JYVÄSKYLÄ STUDIES IN COMPUTING
74

Oleksiy Mazhelis

Masquerader Detection in Mobile Context based on Behaviour and Environment Monitoring

JYVÄSKYLÄN YLIOPISTO

JYVÄSKYLÄ STUDIES IN COMPUTING 74

Oleksiy Mazhelis

Masquerader Detection in Mobile Context based on Behaviour and Environment Monitoring

Esitetään Jyväskylän yliopiston informaatioteknologian tiedekunnan suostumuksella
julkisesti tarkastettavaksi Villa Ranan Paulaharjun salissa
tammikuun 25. päivänä 2007 kello 12.

Academic dissertation to be publicly discussed, by permission of
the Faculty of Information Technology of the University of Jyväskylä,
in the building Villa Rana, Paulaharju Hall, on January 25, 2007 at 12 o'clock noon.

UNIVERSITY OF JYVÄSKYLÄ

JYVÄSKYLÄ 2007

Masquerader Detection in Mobile Context based on Behaviour and Environment Monitoring

JYVÄSKYLÄ STUDIES IN COMPUTING 74

Oleksiy Mazhelis

Masquerader Detection in Mobile Context based on Behaviour and Environment Monitoring

UNIVERSITY OF JYVÄSKYLÄ

JYVÄSKYLÄ 2007

Editors
Seppo Puuronen
Department of Computer Science and Information Systems
Irene Ylönen, Marja-Leena Tynkkynen
Publishing Unit, University Library of Jyväskylä

URN:ISBN:9789513927509
ISBN 978-951-39-2750-9 (PDF)

ISBN 978-951-39-2703-5 (nid.)
ISSN 1456-5390

Jyväskylä University Printing House, Jyväskylä 2007

ABSTRACT

Mazhelis, Oleksiy
Masquerader Detection in Mobile Context based on Behaviour and Environment Monitoring
Jyväskylä: University of Jyväskylä, 2007, 74 p. (+ included articles)
Jyväskylä Studies in Computing,
ISSN 1456-5390; 74
ISBN 978-951-39-2750-9 (PDF), ISBN 978-951-39-2703-5 (nid.)
Finnish summary
Diss.

In recent years, mobile terminals such as mobile phones and PDAs have evolved into functionally powerful devices that can be used to store, process, and communicate valuable information. The access to this information should be properly secured, and hence a great demand for security systems exists. The security issue emphasised in this thesis is the necessity to ensure that the current user of the terminal is its legitimate user. The importance of this issue stems from the fact that a number of mobile terminals are lost or stolen daily: the unauthorised use of such a terminal by a masquerader impersonating the legitimate user may involve abuse of sensitive information kept locally on the terminal or accessible over a network connection. The aim of the reported research is to develop a conceptual basis for differentiating between the legitimate user of the terminal and other individuals by analysing the information about user behaviour and environment, and to address the practical issue of applying it to the problem of mobile-masquerader detection. The main contribution of this thesis is a three-part model of mobile-masquerader detection developed and verified empirically in the thesis. In this model, the problem of mobile-masquerader detection is approached as a classification problem. The first part of the model identifies behavioural and environmental characteristics and measures that can be used for differentiating the user from other individuals. The second part of the model defines how the values of the identified measures can be classified by a set of one-class classifiers each analysing a subset of the measures. The third part addresses the issue of combining the outputs of the classifiers so that accurate final classification can be achieved; a new combining technique is proposed and validated using numerical experiments. Finally, the feasibility of the proposed mobile-masquerader detection model is experimentally validated on a real-world dataset describing the behaviour and environment of smart-phone users.

Keywords: computer security, personal mobile devices, intrusion detection, masquerader detection, continuous identity verification, classification, one-class classification

ACM Computing Review Categories

C.2.1	Computer-Communication Networks: Network Architecture and Design: *Wireless communication*
C.5.3	Computer System Implementation: Microcomputers: *Portable devices (e.g., laptops, personal digital assistants)*
D.4.6	Operating Systems: Security and Protection: *Access controls, Authentication*
I.2.6	Artificial Intelligence: Learning: *Concept learning, Parameter learning*
I.5.1	Pattern Recognition: Models: *Statistical*

Author's address Oleksiy Mazhelis
Dept. of Computer Science and Information Systems
University of Jyväskylä
P. O. Box 35, 40014 Jyväskylä, Finland
mazhelis@it.jyu.fi

Supervisors Prof. Dr. Seppo Puuronen
Dept. of Computer Science and Information Systems
University of Jyväskylä, Finland

Prof. Dr. Jari Veijalainen
Dept. of Computer Science and Information Systems
University of Jyväskylä, Finland

Dr. Alexandr Seleznyov
IT Security
Nokia Group, Finland

Reviewers Prof. Dr. Sokratis K. Katsikas
Dept. of Information & Communication Systems Engineering
University of the Aegean, Greece

Prof. Dr. Sushil Jajodia
Center for Secure Information Systems
George Mason University, Fairfax, Virginia

Opponent Prof. Dr. Steven Furnell
School of Computing, Communications & Electronics
University of Plymouth

ACKNOWLEDGMENTS

First of all, I would like to thank my scientific supervisor, Prof. Seppo Puuronen, for his guidance, help, and moral support throughout the work on the thesis. I am also grateful to Prof. Jari Veijalainen, my second supervisor, for his timely advice at different stages of my research. Many thanks to my third supervisor, Dr. Alexandr Seleznyov, who introduced me to the field of intrusion detection, and whose guidance was especially important during the first steps of my doctoral research.

I am thankful to the external reviewers of my thesis for their valuable comments and suggestions. I would also like to thank Prof. Seppo Puuronen, Prof. Jari Veijalainen, Dr. Jouni Markkula, and Mika Raento for co-authoring the joint publications included in this thesis. I am also thankful to the Context project for making Mobile Communication and Context Dataset available, and especially to Prof. Hannu Toivonen and Mika Raento for their help and support.

I greatly appreciate the support of the COMAS Graduate School which provided funding for this research, and the support of the INFWEST program which provided funding for proofreading of some parts of the thesis. I am also grateful to the Department of Computer Science and Information Systems and the Information Technology Research Institute of the University of Jyväskylä, which offered the facilities for conducting this research, and financially supported numerous conference trips.

I would like to express my gratitude to the staff of the Department for their help and assistance with solving everyday problems. Warm thanks also to Seppo Puuronen, Steve Legrand, and Jari Veijalainen for their efforts during the preparation of this thesis for publishing.

Finally, I wish to thank my family and all my friends for their moral support and interest in my work, especially my dear wife Irina for her forbearance and encouragement.

Jyväskylä
December 19, 2006
Oleksiy Mazhelis

LIST OF FIGURES

LIST OF TABLES

CONTENTS

LIST OF ORIGINAL ARTICLES

I Mazhelis, O. and Puuronen, S. 2006a. A framework for behavior-based detection of user substitution in a mobile context. *Computers & Security* (in press, corrected proof, available online 6 October 2006).

II Mazhelis, O. 2006. One-class classifiers: A review and analysis of suitability in the context of mobile-masquerader detection. *South African Computer Journal. ARIMA & SACJ Joint special issue on advances in end-user data-mining techniques 36*, 29–48.

III Mazhelis, O. and Puuronen, S. 2004. Combining one-class classifiers for mobile-user substitution detection. In I. Seruca, J. Filipe, S. Hammoudi, and J. Cordeiro (Eds.), *Proceedings of the 6th International Conference on Enterprise Information Systems (ICEIS 2004)*, Volume 4. Portugal: INSTICC Press, 130–137.

IV Mazhelis, O., Markkula, J., and Veijalainen, J. 2005. An integrated identity verification system for mobile terminals. *Information Management & Computer Security 13*(5), 367–378.

V Mazhelis, O., Puuronen, S., and Raento, M. 2006b. Evaluating classifiers for mobile-masquerader detection. In S. Fischer-Hübner, K. Rannenberg, L. Yngström, and S. Lindskog (Eds.), *Security and Privacy in Dynamic Environments*, IFIP International Federation for Information Processing, Volume 201. Boston: Springer, 271–283. Proceedings of the IFIP TC-11 21st International Information Security Conference (SEC 2006).

VI Mazhelis, O., Puuronen, S., and Raento, M. 2006a. *Estimating accuracy of mobile-masquerader detection using worst-case and best-case scenario*. In P. Ning, S. Qing, and N. Li (Eds.), *Proceedings of ICICS'06 Eighth International Conference on Information and Communications Security*, Lecture Notes in Computer Science, Volume 4307. Springer-Verlag, 302–321 (in press).

VII Mazhelis, O. and Puuronen, S. 2006b. *Comparing classifier combining techniques for mobile-masquerader detection*. Submitted for publication.

1 INTRODUCTION

This chapter describes the research area of the thesis, introduces the main concepts, and outlines the structure of the thesis.

1.1 Information security issues

Mobile devices have become an indivisible part of our life. They give us an opportunity to have a vast amount of business and personal information at hand, access and process it in a fast and convenient way. According to a survey by Pointsec Mobile Technologies (2005b), smartphones and PDAs are used to store personal and business names and addresses (86% and 81% of users, respectively), to receive and view emails (45%), to store corporate information (27%), etc. This information should be properly secured; therefore, a great demand for security systems exists. These systems are needed to protect the information from disclosure or manipulation and to help to keep computer systems reliable and usable.

Peculiar characteristics of mobile terminals, such as personal use, small size, mobility, and limited battery power, affect the security requirements of these terminals. Meanwhile, the main information security principles and concepts, as well as many of the issues and solution approaches are similar for mobile terminals and traditional computer systems such as networked workstations and servers. Therefore, in the following subsections, main principles and concepts of information security are overviewed.

1.1.1 Security goals, services, and mechanisms

The main goal of information security is protection of the information assets of an organisation so that the business objectives of this organisation could be achieved. This goal can be decomposed into three components (Stoneburner 2001): i) confidentiality of data and system information, ii) system and data integrity, and iii) availability of system and data for the intended use only. The

confidentiality requires that the private or confidential information be disclosed only to authorised system users. The data integrity implies that the data are not modified in an unauthorised way, and similarly the system integrity requires that the functionality of the system be unchanged and free of unauthorised manipulation. The availability ensures that the services provided by the system are not denied to authorised users. It also ensures that the data or the functionality of the system are not employed for unauthorised purposes.

Two additional security subgoals are often added to the above list. These are accountability and assurance (Stoneburner 2001). The accountability allows any action to be traceable back to the entity (an individual, hardware or software) evoking it. The assurance corresponds to continuous verification of how the other security goals are achieved by implemented security measures. It should be noted that the first three subgoals deal with the properties of information being secured, while the assurance and accountability requirements are more closely related to the implementation and management of security measures.

In order to achieve the above security goals, a set of security services should be provided. For example, in the framework of the OSI Reference model (ISO/IEC 7498-2 1989), authentication, access control, and data confidentiality services may be employed for achieving the abovementioned confidentiality goal. Other services specified are data integrity and non-repudiation services. No special-purpose service is proposed for ensuring the availability; however, the authentication and access control services may be employed in order to partly satisfy this requirement.

The security services are, in turn, implemented using specific security mechanisms. The mapping between security services and mechanisms, as well as the mapping between OSI levels and security services and mechanisms is discussed in ISO/IEC 7498-2 (1989). For example, an authentication exchange mechanism may be employed to implement the authentication service. There are also pervasive security mechanisms not specific to any security service. An example of such a mechanism would be an event detection mechanism, which detects violations of security and other security related events.

Security policy of the organisation defines the priorities to be assigned to different security goals. For example, confidentiality is crucial in a military environment, while availability may be most important for a company providing web-services. By identifying the assets to be protected, identifying the threats to these assets and vulnerabilities thereof, and by defining the risks of these threats and their impacts if materialised, the organisation is able to assign the above priorities. Consequently, they are used to define the security services and mechanisms to be implemented.

1.1.2 Preventive and detective security services

Security services can be divided into four categories: deterrence, prevention, detection, and remedies (Straub and Welke 1998)[1]. According to Straub and Welke

[1] Another categorization divides the security services into avoidance (security policy, security awareness, authentication, access control, etc.); assurance (vulnerabilities testing, security reviews, etc.); detection (intrusion detection, fraud detection, proof of wholeness),

(1998), such division can be understood in terms of the general deterrence theory (Pearson and Weiner 1985). Deterrent measures are aimed at making system users aware of details of the security policy in the organization, as well as of certainty and severity of sanctions in case intentional security violations occur (Straub and Welke 1998; Siponen 2000). If the deterrence fails, preventive measures (such as authentication passwords (Summers and Bosworth 2004)) are needed to defend against an abuse. Unfortunately, preventive measures can be compromised or bypassed. The reason for this may be bugs in software, incorrect system configuration, or inappropriate security management, among other things (Sundaram 1996; Krsul 1998; Siponen 2000). Since preventive means cannot be completely unbreakable, the detective means are required to reveal ongoing or succeeded abuse cases. The detective means can be exemplified by intrusion detection systems (Debar et al. 1999; McHugh 2001; Coolen and Luiijf 2002) and virus scanners (Bontchev 1998). Finally, the security system should remedy the damage caused by a successful abuse. In addition, the offenders should be punished to create a deterrence effect.

1.2 Ensuring legitimacy of mobile-terminal users

The generic security principles discussed above are equally applicable in the context of mobile terminals, which may be seen as a special type of computer systems. An important part of security provision in a mobile environment is ensuring that only the legitimate user is allowed to access the resources provided by the terminal. It is a crucial issue since the terminals, due to their small size, are often lost. As the survey by Pointsec Mobile Technologies (2004) reveals, 24% of respondents have experienced a loss or theft of their PDAs; according to another survey, 85 619 mobile phones and 21 460 PDAs/Pocket PCs were lost in Chicago licensed cabs during the six months period (Pointsec Mobile Technologies 2005a).

This section overviews the preventive and detective means that can be employed in order to ensure user legitimacy. The preventive security is supported by the authentication service; in turn, the means of intrusion detection implement the detective security.

The authentication service (more precisely, peer-entity authentication service (ISO/IEC 7498-2 1989)) performs identity verification, i.e., it ensures that the user possesses the claimed identity. In contemporary mobile terminals, the identity verification is usually based on passwords or personal identification numbers (PINs). However, as evidenced by survey results, 44% of users do not use PINs, finding them inconvenient (Clarke et al. 2002). These results are confirmed by a more recent survey (Clarke and Furnell 2005), reporting 34% of mobile phone users disabling PIN authentication. Another survey (Pointsec Mobile Technologies 2003) indicates that one-third of PDA users store corporate and private in-

and recovery (software reinstallation, data recovery) (Stephenson 2000). Here, the means of deterrence are considered as belonging to the group of avoidance services. Assurance services (including vulnerabilities testing, security reviews, etc.) are added; they are aimed at revealing the limitations of current security system implementation.

formation on their PDAs without password protection, and a quarter of the users accessing corporate networks with their PDAs disable the password authentication. Thus, should the legitimate user be substituted, an impostor may easily abuse the information accessible through the terminal.

In order to overcome the limitations of passwords and PINs, some terminals implement also biometrics-based verification (e.g., biometric authentication provided on the DoCoMo's FOMA "9 Series" phones (NTT DoCoMo 2006)). Besides, user verification based on authentication tokens has been proposed (Corner and Noble 2002; Corner and Noble 2003; Kageyama 2006). However, the tokens used can be lost or stolen along with the device being protected. Biometric authentication can also be fooled (Matsumoto et al. 2002; Thalheim et al. 2002; Williams 2002; Chandra and Calderon 2005; Weinstein 2006), and its use often requires additional hardware. Furthermore, the available biometrics-based identity verification implementations produce a considerable rate of false rejection errors (failure to accept the legitimate user) or false acceptance errors (mistakenly accepting illegitimate users) (Phillips et al. 2000; Chandra and Calderon 2005). Thus, the contemporary identity verification means based on passwords, PINs, tokens, or biometrics, when used alone, are not sufficient to provide a high level of security.

The above means of identity verification can be categorised as preventive mechanisms (Straub and Welke 1998). As discussed above, an impostor having substituted the user may break or bypass such identity verification. Consequently, such impostor may illegally use the terminal e.g. to access a corporate database in the name of the legitimate user, or to compromise private data stored on the terminal. The attack consisting in impersonating the legitimate user in order to obtain an unauthorised access to sensitive data or services authorised for that user is referred to as the *masquerade attack* (Anderson 1980). According to the evaluation of security threats and requirements for 3G mobile networks (3GPP 2002), the use of stolen terminals represents a threat of a major impact, and therefore resisting the masquerade attacks in the context of mobile-terminal users is of prime importance.

Since complete attack prevention has so far been unattainable, there is a need to timely identify attacks that have succeeded or are in progress, and, if possible, collect irrefutable evidence of malicious activity for establishing a case in court. For this, the security means belonging to the detection category (Straub and Welke 1998) need to be implemented. Intrusion detection systems (IDSs) are systems intended for performing the task of detecting and registering various types of attacks against computer systems. Their functioning relies on the assumption that attacks can be automatically detected through the analysis of the system audit logs, network packets, and/or other security traces in the system. The IDSs analyse these security traces and detect attacks by identifying the deviations from normal behaviour (the IDSs adopting the so-called *anomaly detection* approach) or by detecting the occurrences of unacceptable behaviour (the IDSs following the so-called *misuse detection* approach) (Kumar 1995; Axelsson 2000). The preventive security means, such as authentication, are often said to implement the first line of defence, while the role of the last line of defence is played by the IDSs (Kumar 1995; Ghosh et al. 1999).

In recent years, the term of intrusion prevention systems (IPS) has been introduced to refer to the systems which are capable of i) on-line detection of ongoing intrusions, and ii) instant automated interruption of the malicious activities thus preventing the attack from successful completion (Wickham 2003). Such IPS should be able to detect attacks extremely quickly and accurately, and they are supposed to be more proactive as compared with traditional IDS which are usually reactive, i.e. merely register occurred violations for further post-mortem analysis. Due to the ability to prevent attacks, the IPS can be classified as preventive rather than detective security means, even though detection mechanisms form the core of the IPSs. Unfortunately, the currently available detection technologies do not provide sufficient detection accuracy, and taking actions based on such inaccurate alarms may be dangerous (Bezroukov 2005; Skoudis and Poor 2005; Info∼Tech Research Group 2006). For instance, in case of a false alarm, the IPS may block traffic from a legitimate host, thus effectively implementing a denial-of-service attack. Therefore, the IPSs for the time being have to be used mainly in a detection mode, and restrict their blocking features only to the most accurately detected attack types.

1.3 Detecting masquerade attacks

As mentioned above, intrusion detection can be based on anomaly detection or misuse detection (Axelsson 2000). In the context of detecting the masquerade attacks, or *masquerader detection*, the anomaly and misuse detection approaches may be realised as:

1. *Continuous verification of user activity or identity.* In this approach, either the description of normal user activity or the description of user identity needs to be established. Deviations from this description are considered as potential masquerade attacks. Therefore, this approach can be seen as anomaly detection since deviations from an established norm are looked for.

2. *Impostor recognition.* This approach is based on detecting predefined patterns associated with impostor activity or identity. Thus, it is aimed at detecting the presence of an impostor, and can be seen as misuse detection.

It may be difficult to implement masquerader detection following the impostor recognition approach. The impostor identity is usually unknown beforehand, and hence cannot be recognised. In turn, determining the patterns of a masquerader's activity requires data describing the masquerader's behaviour to be available. Due to practically infinite space of possible behaviours of a masquerader, the task of collecting the data covering these behaviours is likely to be intractable (Lane 2000). The first approach, on the other hand, only requires the description of a normal activity or the description of an identity for the legitimate user to be provided, and may be easier to implement in practice. Therefore, in masquerader detection the anomaly detection approach is usually followed:

- If the masquerader detection is based on verifying user activities, the norm of the legitimate-user behaviour needs to be established, so that deviations

from this norm can be detected. This norm may cover the normal activities of a particular user of a terminal (Schonlau et al. 2001), or the normal activities of a group of users (Denning 1987). In an extreme case, the normal behaviour of all possible legitimate users would be covered.

- If the masquerader detection is based on user identity verification (e.g. Klosterman and Ganger (2000)), the description of identity of one user only needs to be provided.

Thus, identity verification may be involved in implementing both preventive (authentication) and detective (intrusion detection) security mechanisms. However, the same identity verification methods need not necessarily be employed for both preventive and detective purposes. First, if the preventive and detective mechanisms are considered as distinct lines of defence, using the same identity verification in both lines is unadvisable, since compromising the mechanism in this case may result in compromising both lines of defence. Second, while a detective mechanism should work constantly, providing continuous security, not all identity verification mechanisms can be used continuously. For example, password-protection employed continuously would hinder the user from performing his or her main tasks.

Within the research community, great efforts have been devoted to the problem of detecting masquerade attacks, e.g. (Debar et al. 1992; Anderson et al. 1994; Lee and Stolfo 2000; Seleznyov 2002; Sequeira and Zaki 2002; Lane and Brodley 2003; Shavlik and Shavlik 2004; Ray and Poolsapassit 2005), and a number of IDSs capable of detecting masquerade attacks have been developed. These are, though, aimed at traditional computer systems, and hence do not take into account the peculiarities of mobile terminals. In recent years, attention has also been paid to the problem of repelling masqueraders in the context of mobile terminals (Clarke et al. 2003; Mäntyjärvi et al. 2005; Sun et al. 2006). In particular, the applicability of keystroke dynamics for continuous re-authentication of mobile handset users was studied by Clarke et al. (2003), the use of gait patterns for identifying mobile terminal users was investigated in the recent work of Mäntyjärvi et al. (2005), and analyzing the mobility patterns of a mobile handset for detecting masqueraders was aimed at in the research by Sun et al. (2006). No publicly available research has been found, however, wherein more than one aspect of user behaviour and/or environment would be employed for the detection purposes, and the empirical evidence on mobile-masquerader detection is scarce.

1.4 Outline of thesis

This thesis focuses on the problem of mobile-masquerader detection, and follows the anomaly detection approach. In this approach, continuous verification of user identity is employed as a means of automatic differentiation between the legitimate user of the terminal and other individuals. In the thesis, a conceptual ba-

sis for such differentiation is developed and applied to the problem of detecting masquerade attacks in the context of mobile terminals.

The problem of distinguishing the legitimate user from other individuals is formulated as the problem of classifying the individual characteristics of user behaviour and environment as belonging to the class of the legitimate user or not. The classification is performed by a set of one-class classifiers (Tax 2001), whose classifications are subsequently combined. The thesis considers the characteristics to use in mobile-masqurader detection, the classifiers to analyse them, and the techniques of combining the outputs of these classifiers.

The research can be described in terms of the information systems research framework (March and Smith 1995; Hevner et al. 2004) that includes the development and building process and the justification and evaluating process. During the development and building process, the model of mobile-masquerader detection is constructed, and some components of the model are instantiated. Then, during the justification and evaluating process, the instantiated components of the model are experimentally evaluated using synthetic and real-world data.

The structure of the thesis is as follows. In the next chapter, the work related to the issue of ensuring the legitimacy of the mobile-terminal users is overviewed. Chapter 3 formulates the problem of mobile-masquerader detection as a classification problem. The research objectives and research methods are described in Chapter 4. In Chapter 5, the developed model of masquerader detection is summarised. An overview of the articles included in the thesis is provided in Chapter 6. Finally, the conclusion chapter summarises the contribution and limitations of the thesis and outlines the directions for further research.

2 RELATED WORK

In order to resist masquerade attacks, the mechanisms of authentication as well as detective security mechanisms can be employed. The authentication mechanisms verify that the user possesses the claimed identity (ISO/IEC 7498-2 1989), and they are aimed at the provision of preventive security. Detective security is provided by the mechanisms of intrusion detection capable of detecting the attacks against a protected system that have succeeded or are in progress (Sundaram 1996; Axelsson 2000). In the domain of telecommunication services, the detective security also includes fraud detection which is aimed at revealing a dishonest or illegal use of services, with the intention to avoid service charges (Hollmen 2000). Frauds are often committed by masqueraders, and therefore, some of the masquerade attacks can be detected using fraud detection techniques. In the following sections, a brief overview of the related work in the domains of authentication, intrusion detection, and fraud detection is provided.

2.1 Authentication

Peer-entity authentication verifies that the opposite side (e.g. the user) possesses the claimed identity, i.e. it performs user identity verification. Using the results of the authentication procedure, the access control mechanism decides whether the user with this identity is allowed to access the requested resources.

The approaches to identity verification are usually divided into three groups according to the type of identity proof that a user whose identity claim is verified should be able to present. It is assumed that for other individuals (not possessing this identity), presenting the required proof is difficult or impossible. These three types of identity proofs are based on (NIST FIPS 190 1994): i) knowledge, ii) objects in possession, and iii) user individual physical or behavioural characteristics. They are considered in more detail below.

2.1.1 Knowledge-based identity verification

Knowledge-based identity verification requires that the user possess specific knowledge, usually in the form of a password or Personal Identification Number (PIN). This method is easy to implement and it does not require significant computational resources. Nevertheless, the use of passwords and PINs is often criticised as inconvenient and insufficiently secure (Jermyn et al. 1999; Weinshall and Kirkpatrick 2004). The inconvenience stems from the need to remember passwords or PINs. Some individuals have to memorise five to ten passwords that are needed to access different resources (Summers and Bosworth 2004). Entering passwords or PINs requires specific actions to be performed by the users. As a result, knowledge-based identity verification can hardly be employed continuously, since the user would be constantly disturbed by verification requests. Furthermore, in order to decrease the probability of a password being compromised, the passwords should be changed periodically; this further increases the burden of memorising them. Consequently, users often select easy-to-remember passwords, write them down, or disable the password protection entirely.

A mechanism implementing the knowledge-based verification stores the copies of the password or PIN in a file, and implements the verification by comparing the password against its stored copy. In order to avoid the disclosure of the passwords in case the intruder manages to access the password file, the original passwords are often transformed using a one-way function (hash-function), and the produced values are stored instead of the original passwords. Still, the intruder having got the password file might discover the passwords by utilising automated cracking tools to fit various password candidates to the hash-values in the file (Pinkas and Sander 2002). The time needed for cracking a password depends on the length of the password and on the set of symbols employed in it. Therefore, in order to decrease the probability of revealing the password, the password should be long enough and contain numerical and special symbols; however, even such hardened passwords are susceptible to "smart-dictionary" attacks (Narayanan and Shmatikov 2005). Furthermore, the required minimum length of passwords should increase as the computational power of the computers (and cracking tools) grows. As a result, the use of passwords may become impractical in future.

In order to increase the difficulty of compromising the knowledge used in identity verification, and at the same time to make it easier to remember, other forms of knowledge representation have been proposed. For example, in several works, graphical objects, images, or parts thereof are employed instead of textual passwords (Jermyn et al. 1999; Wiedenbeck et al. 2005; Kirovski et al. 2006).

2.1.2 Token-based identity verification

Token-based verification assumes that an object is possessed by the user with a specific identity. Tokens can be exemplified by traditional door keys; they need to be carried by the user and need to be presented during the identity verification. The tokens employed in computer security are usually in a form of a smart-card capable of storing, processing, and sometimes transmitting identity-related information (RSA Security Inc. 2004; Kageyama 2006). The advantage of

the token-based verification is the potential ability to perform verification continuously and transparently, without any evident user participation (Corner and Noble 2002; Ensure Technologies 2006). The shortcoming of this approach is the need for additional hardware (e.g. a smart-card and a card reader), adding to the costs of the system being protected. Furthermore, in the context of securing a mobile terminal, the token itself can be lost or stolen along with the protected terminal (Bardram et al. 2003).

2.1.3 Identity verification based on physical characteristics

This type of verification relies on the physical characteristics of an individual. Examples of such characteristics are fingerprints, retina, iris and facial characteristics, and hand and palm geometry. These characteristics are highly unlikely to be identical for any two individuals. This property makes them especially useful for identity recognition and verification. The identity verification techniques based on these characteristics are referred to as biometric (Clarke 1994). In addition to personal physical characteristics, biometric identity verification can be based on personal behavioural characteristics discussed in the next subsection.

The use of physical characteristics for identity verification has a number of advantages. They are more convenient for the users than passwords, since no information need to be memorised and typed. As opposed to the tokens that are easy to loose, they cannot be easily made unavailable. Identity verification can sometimes be performed transparently and continuously (Klosterman and Ganger 2000). However, biometric measurements vary in time for the same person. Consequently, the verification based on such biometric measurements may result in a poor accuracy (Chandra and Calderon 2005). For example, the false rejection rate for face recognition is up to 40%, and for fingerprints this error may reach 44% (Phillips et al. 2000). Furthermore, biometrics are not secret, e.g., fingerprints or face characteristics can be relatively easily observed and forged (Riha and Matyas 2000; Matsumoto et al. 2002; Thalheim et al. 2002; Chandra and Calderon 2005). Besides, additional hardware is usually required in order to input biometric data. The verification process is often computationally expensive, especially when the verification is performed continuously.

2.1.4 Identity verification based on behavioural characteristics

Some behavioural characteristics, similarly to physical characteristics, contain regularities which are peculiar for each individual. Among these characteristics are voice (Li et al. 2000), typing rhythms (Clarke et al. 2003; Gunetti and Picardi 2005), and gait (Kale et al. 2003; Mäntyjärvi et al. 2005). Their use for identity verification has the same advantages as the physical characteristics have. Naturally, verification relying on these characteristics can be performed continuously. Moreover, unlike some of the physical characteristics, the behavioural characteristics are hard to forge. However, the values of the measures representing these characteristics vary with time, and, furthermore, the degree of variation varies from one person to another (Verlinde et al. 2000). As a result, the accuracy of verification based on behavioural characteristics may be even worse than the accuracy of

verification based on physical characteristics. Besides, continuous processing of these characteristics tends to be computationally expensive.

2.1.5 Multi-modal identity verification

To improve the accuracy of biometrics-based authentication, multiple biometric modalities are often analysed simultaneously. A number of studies have been devoted to the problem of user authentication based on multiple biometrics referred to as multi-modal user authentication. Most of these studies address the problem of combining visual and acoustic features for identity verification purposes (for example, Ben-Yacoub et al. (1999), Choudhury et al. (1999), Verlinde et al. (2000), Cheng et al. (2005), and Sanderson and Paliwal (2004)). Fierrez-Aguilar et al. (2005) explore the combination of the fingerprint and written signatures. Koreman et al. (2006) use the combination of signature, face, and voice as features for PDA user identity verification. Combinations of face, fingerprint, hand geometry, and speech-based biometrics were investigated at Michigan State University. The reported studies deal e.g. with integrating face and fingerprints (Snelick et al. 2005), fingerprints, face, and speech (Jain et al. 1999), face, fingerprint, and hand geometry (Ross and Jain 2003) within a single authentication approach.

2.1.6 Other types of identity evidences

Clarke (1994) extended the set of biometric characteristics. In addition to physical and behavioural characteristics, three other types of characteristics were considered: appearance, social behaviour, and imposed physical characteristics. The appearance characteristics describing the looks of an individual are exemplified by height, gender, colour of skin, facial hair, etc. The characteristics of social behaviour include e.g. habituated body signals, style of speech, and visible handicaps. These appearance and behavioural characteristics may be used to assist in detecting an impostor; however, they are relatively unreliable and can hardly be employed as identity proofs (Clarke 1994; Ailisto et al. 2004). The imposed physical characteristics such as bracelets, anklets, or embedded micro-chips are similar to the tokens considered above. As opposed to the tokens, the imposed physical characteristics cannot be easily removed. However, user acceptance of the identity verification based on such characteristics is questionable.

2.2 Intrusion detection

Intrusion detection systems (IDSs) are systems intended for performing the task of detecting various types of attacks (intrusions) against computer systems that have succeeded or are in progress, collecting evidence of performed malicious activity, and when possible identifying the intrusions and intruders (Kumar 1995). A computer system may undergo several types of attacks including eavesdropping and packet sniffing, snooping and downloading, tampering with data, spoofing (masquerading is a form of spoofing), flooding, malicious code, exploiting

design and implementation flaws, and cracking passwords and keys (Denning 1997, as referred by Schonlau et al. (2001)).

Approaches to intrusion detection are traditionally categorised into anomaly and misuse detection approaches (Kumar 1995; Axelsson 2000). Anomaly detection assumes that a normal system or user behaviour contains regularities. A profile describing the peculiarities of user or system behaviour is created, and significant deviations from the established norm are flagged as potential attacks (Denning 1987). The misuse detection approaches complement the anomaly detection in that they focus on the patterns of attacks instead of regularities in normal behaviour. In misuse detection, it is assumed that the knowledge about unacceptable behaviour resulting in an attack is obtained beforehand, automatically or with help of security experts, and the occurrences of such unacceptable behaviour are directly looked for (Kumar 1995). Due to the reliance on the previously obtained knowledge these approaches are also called as knowledge-based (Debar et al. 1999) or signature-based (Axelsson 2000).

These two complementary approaches both have their pros and cons. The misuse detection approaches are characterised by relatively high detection accuracy quantitatively measured by the rates of *false acceptance errors*, or *false negatives* (when an attack remains undetected), and *false rejection errors*, or *false positives* (when a normal activity is mistakenly considered as an attack). The employment of misuse detection approaches requires a knowledge base of unacceptable behaviour to be obtained and encoded beforehand. Often, this encoding is done by human experts, and therefore is labour-intensive. Some approaches have been proposed to assist in encoding process (e.g., data-mining intrusion detection (Lee and Stolfo 2000)); however, complete automation has not yet been achieved. Furthermore, a misuse detection system cannot detect a new type of attack before a signature for this attack is discovered and encoded.

The advantage of anomaly detection systems is in their ability to detect new types of attacks. However, anomaly detection assumes no anomalies in legitimate behaviour and implies that all anomalous behaviour represents intrusions, while in fact there is an intersection between legitimate and intrusive behaviour. As a result, the anomaly detection approaches result in a relatively high level of false positives and/or false negatives. Besides, shortcomings of anomaly detection approaches are the difficulty in selecting features to monitor and a considerable computational overhead due to the storage and update of various metrics (Sundaram 1996). In order to improve detection accuracy, a so-called specification-based approach to intrusion detection has been proposed (Sekar et al. 2002). In this approach, the legitimate user or system behaviour should be specified in advance. Provided the knowledge about the legitimate behaviour is available, the use of such specification may reduce the level of false positives. On the other hand, similarly to misuse detection, creating specification involves human expertise, in other words, is time-consuming and costly.

Intrusion detection systems are also divided, according to the source of data being analysed, into host-based and network-based systems (Debar et al. 1999). Host-based IDSs employ system logs and audit trails collected at a host machine, while the primary data source of the network-based IDSs is intercepted network packets. The metrics monitored by IDSs include keystrokes, typed commands,

system calls, processes, statistics of system resources usage (e.g. CPU usage, number of input-output operations), network packets, etc. Not all of these metrics are equally useful for detecting masquerade attacks. For example, it may be more difficult to detect masqueraders by using system calls. The reason is that system calls reflect the program/system behaviour rather than user behaviour. Consequently, the characteristics of these metrics may remain unchanged irrespective of whether the user or an impostor interacts with the system, as long as the programs used are the same.

A number of intrusion detection approaches capable of detecting masquerade attacks have been developed. Some of them, e.g. the approaches based on statistical analysis (Anderson et al. 1994; Schonlau et al. 2001), neural networks (Debar et al. 1992; Ryan et al. 1998), data-mining (Lee and Stolfo 2000), instance-based learning (Lane and Brodley 1999), and hidden Markov models (Yeung and Ding 2003), are considered below.

2.2.1 Masquerader detection based on statistical approach

Statistical approaches are based on the generic model or intrusion detection (Denning 1987) which is independent of the system being secured or of the type of attacks being detected. The model introduces the concepts of metrics and their statistical models that are employed to represent the normal behaviour of subjects with respect to system objects. The model also introduces the concept of an activity profile serving as a structure that keeps the signature of normal activity in terms of the above metrics and statistical models. The statistical models define the normal distribution of the assigned metrics, and anomalies are detected by matching the current metric values against the model. In this model, activity rules are employed in order to react to a detected anomaly or to update the profile.

The statistical approach was followed e.g. in the design of the statistical component of Next-Generation Intrusion Detection Expert System (NIDES) (Anderson et al. 1995), in the works of Shavlik and Shavlik (2004) studying the applicability of the statistical approach for intrusion detection on the Windows platform, and in the research of Schonlau et al. (2001) dealing with the statistical analysis of user commands.

The statistical component of NIDES builds a user profile accumulating various statistics of long-term user behaviour (Javits and Valdes 1993; Anderson et al. 1994; Anderson et al. 1995). Multiple behavioural characteristics including file access, CPU and memory usage, etc. are analysed by the component. The distance between the profile and the statistics of short-term behaviour is calculated, and significant distance values are flagged as potential intrusions. Ye and Chen (2001) and Ye et al. (2002) use a similar approach in order to detect anomalies in the security audit records gathered by the Basic Security Module (BSM) of the Solaris operation system. Shavlik and Shavlik (2004) apply the statistical anomaly detection approach in the context of Windows 2000 workstations. In their work, over 200 Windows properties related to network activity, file access, CPU load, and running programs are continuously monitored. Based on this, approximately

1500 features are derived, and their statistical properties are analysed and used for anomaly detection purposes.

Schonlau et al. (2001) approach the masquerader detection problem by statistically analysing the UNIX commands typed by the users. Among the statistics that have been tried by the authors are the uniqueness of a command (based on the observation that half of the commands are issued by a single user only), a Bayes factor statistics to test the hypothesis that command transition probabilities are consistent with previously established transition matrix, a high-order Markov chain to estimate the probabilities of commands chains, and other statistics (DuMouchel and Schonlau 1999; Schonlau and Theus 2000; Schonlau et al. 2001). To each statistics, a threshold value is assigned, and an alarm is triggered if the current value of the statistics exceeds the threshold.

2.2.2 Masquerader detection based on neural network approaches

Neural networks are networks of interconnected units arranged in one or several layers. These units represent processing elements whose parameters (e.g. weights) can be adjusted using training data. Neural networks can be trained to implement a complex functional mapping between input and output variables. The flexibility and adaptability of neural networks has been successfully used e.g. in the anomaly component of Hyperview intrusion detection system (Debar et al. 1992) and in Neural Network Intrusion Detector, or NNID (Ryan et al. 1998).

The Hyperview intrusion detection system (Debar et al. 1992) consists of two main components, one of which employs an artificial neural network to detect anomalies in the user or system behaviour. The anomaly component implements a recurrent neural network where some of the outputs are connected with the network inputs. It is assumed that user or system behaviour contains multivariate time series, and the recurrent neural network is used to model them. The alarm is raised if the currently observed series of events deviate from the time series learnt by the network.

The NNID (Ryan et al. 1998) uses a backpropagation neural network to identify users based on the frequencies of UNIX commands. The distribution of various commands invoked by the user during a day is used as an input for the neural network. The network is learnt using the data originating from all the system users. It remains unclear, how the detection accuracy of the system depends on the number of users whose data is involved in the learning process.

Clarke and Furnell (2006) have applied neural networks in a mobile environment, in order to continuously re-authenticate users of mobile terminals. The latencies of keystrokes which were entered by the users on a keypad of a mobile handset served as a source data for the networks. In the reported experiments (Clarke and Furnell 2006), the feed-forward multi-layered perceptron networks, radial basis function networks, and generalised regression neural networks were used. The obtained results suggest that the use of keystroke analysis for mobile-masquerader detection is feasible; however, further research is needed in order to improve the accuracy of detection.

2.2.3 Masquerader detection based on data mining

Lee and Stolfo (2000) use a data-mining framework to facilitate the creation of intrusion detection models. The framework is focused on creating models for misuse intrusion detection, but its modified version can be used for creating anomaly detection models capable of detecting masqueraders. In the modification, the user command log is mined for frequent patterns in a form of frequent episodes (Mannila and Toivonen 1996) and association rules (Agrawal et al. 1993). These patterns form the normal usage profile of a user. The current login session is also mined for frequent patterns that are subsequently matched against the profile, and a similarity score is calculated. An alarm is set if the similarity value is less than a threshold.

In the approach of Zhang and Lee (2000; 2003), data-mining techniques are employed for anomaly detection purposes in mobile ad-hoc networks. Specifically, the RIPPER inductive rule generator (Cohen 1995) and Support Vector Machines (Joachims 1999) are used to model the correlations between various features describing local routing information as well as the location and velocity of the user. The deviations from this model are considered as anomalies.

2.2.4 Masquerader detection based on instance-based learning

Lane and Brodley (1999; 2003) employ instance-based learning to analyse the UNIX shell commands typed by users. The authors devised a new similarity measure to compare the sequence of commands against the command history representing normal user behaviour. This measure takes into account the number and the lengths of any identical subsequences found. The calculated similarity score is compared with a threshold, and an alarm is set if this score is less than the threshold. A similar approach is used in the work of Chen et al. (2004), where common subsets of commands between pairs of user sessions are determined, and their length is employed as a similarity measure between these sessions.

Sequeira and Zaki (2002) also used the instance-based learning to classify user shell commands as normal or anomalous. The authors introduced a similarity measure for comparing command sequences, and elaborated a dynamic clustering algorithm to group together similar command sequences. During classification, the similarity between the new command sequence and the closest cluster is determined, and the similarities of last several sequences are used in order to decide whether the new sequence is anomalous.

2.2.5 Masquerader detection based on hidden Markov models

Yeung and Ding (2003) use the ability of hidden Markov models (HMMs) to efficiently model the temporal sequences in order to analyse system calls as well as the shell commands typed by the users. Using HMM, a model of normal sequences of system calls and shell commands is established and subsequently employed for calculating the likelihoods of current sequences. If this probability is lower than a certain threshold, the sequence is treated as an anomaly. Also, mixtures of HMMs have been found useful in detecting masqueraders on the basis of UNIX shell commands (Okamoto et al. 2004; Yamanishi et al. 2005).

Lane and Brodley (2003) also employ the HMMs to model the temporal characteristics of the shell commands and compare their anomaly detection method based on HMM against the anomaly detection based on instance-based learning. As reported by the authors, the detection accuracy of these methods is statistically indistinguishable, while the computational burden of HMM is significantly higher than that of the instance-based learning.

2.2.6 Other approaches to masquerader detection

Maxion and Townsend (2004) use the naïve Bayes classifier to detect masqueraders through the analysis of user shell commands. The dataset of UNIX command lines collected by Schonlau et al. (2001) is employed in order to empirically evaluate the strengths and weaknesses of this approach. Using the same dataset for experimentation, Wang and Stolfo (2003) and Kim and Cha (2005) investigate the applicability of Support Vector Machines (SVM) to detect masqueraders through shell commands analysis. The authors compare the performance of the SVM and the naïve Bayes classifier and conclude that better results can be achieved with the SVM classifier.

In the anomaly component of the Hybrid Intrusion Detection System based on Real-time User Recognition (HIDSUR) (Seleznyov 2002), temporal probabilistic networks are employed to establish the profile of normal user behaviour. The profile takes into account the temporal order of the user actions (processes invoked by the user), as well as the temporal length of these actions and intervals between them. The current sequence of user actions is classified as normal or anomalous by matching it against the profile; an anomaly is registered if a significant deviation from the profile is found.

Sun et al. (2006) apply the anomaly detection scheme derived from a Lempel-Ziv compression algorithm (specifically, LZ78) to detect anomalies in the sequences of cells traversed by mobile-terminal users, and compare this scheme with the detector based on a fixed order Markov model. In the former detection scheme, a mobility trie is built whose nodes represent traversed cells. For each node, its frequency is estimated using the Exponential Weighted Moving Average (EWMA). Using the constructed trie along with the calculated frequencies, the probability of a particular sequence of traversed cells is estimated. The work by Sun et al. (2006) is one of few works which focus on masquerader detection in the context of mobile terminals. However, the proposed schemes have been explored in a simulation study only, and a further study is due to validate the proposed schemes using real-world data.

Also dealing with mobile-masquerader detection is the work of Mäntyjärvi et al. (2005), who attempt to continuously verify the identity of a mobile-handset user through the analysis of the user gait. For this, the forward-backward and the vertical acceleration are continuously measured by using a 3-D accelerometer device. Several approaches to verify user identity are compared in the experiments; these approaches are based on i) correlation coefficients, ii) fast Fourier transform (FFT) coefficients, iii) histograms, and iv) third and fourth moments of the acceleration signal distribution. According to the results of the experiments,

the best verification accuracy is achieved when averaged correlation coefficients are employed.

2.2.7 Combining evidences

Substantial efforts in intrusion detection research have been devoted to combining multiple characteristics, techniques, and their outcomes as a means of improving detection performance. Combining multiple characteristics can be exemplified by the statistical component of NIDES (Anderson et al. 1995), which is capable of monitoring and processing multiple characteristics describing user behaviour. Some approaches combine several anomaly and/or misuse detection techniques within one IDS (Porras and Neumann 1997; Valdes and Skinner 2000; Giacinto et al. 2003). Finally, sizeable amount of work have been dedicated to combining the outcomes (i.e. alerts) of the IDSs. The proposed combining techniques perform *alert aggregation*, *multistep correlation*, *multisensor correlation*, and *filtering* (Haines et al. 2003). Alert aggregation is needed since thousands of alarms may be produced by IDSs daily (Manganaris et al. 2000; Julisch 2003) making their investigation by a human analyst unfeasible. Therefore, the set of alarms should be compressed (aggregated) into a manageable number of reports (Valdes and Skinner 2001; Morin et al. 2002; Porras et al. 2002; Xu and Ning 2004). Alert filtering is justified by the fact that up to 99% of the raised alarms are false positives, i.e. alerts triggered incorrectly (Julisch 2003). Using automatically or manually created rules, these alerts can be filtered out (Clifton and Gengo 2000; Manganaris et al. 2000; Julisch and Dacier 2002; Pietraszek 2004). Often an attack involves several steps each of which can be detected separately. The corresponding alerts should be collected in a single report describing the incident. This is done using multistep correlation (Debar and Wespi 2001; Valdes and Skinner 2001; Cuppens and Miege 2002; Ning et al. 2002a; Ning et al. 2002b; Wang et al. 2005; Chen et al. 2006). Besides, different IDSs may detect different or same steps of an attack. The alerts produced by these IDSs (also referred to as sensors) should be aggregated; this is done through multisensor correlation (Debar and Wespi 2001; Goldman et al. 2001; Valdes and Skinner 2001; Ning et al. 2002a; Han and Cho 2003). In some approaches, several combining techniques are used together (Valeur et al. 2004; Lee et al. 2006).

2.3 Fraud detection in telecommunications

Many fraud detection approaches in the domain of telecommunications are based on information extracted from the so-called Toll Tickets, which are collected by mobile operators for billing purposes (Burge and Shawe-Taylor 1997; Hollmen 2000) and which contain a number of attributes describing the user calling activity. The information in them reflects the behaviour of the user (e.g. time and duration of calls), and is assumed to contain manifestations of fraudulent activity. Reviews of various fraud detection techniques have been published (Hollmen

2000; Bolton and Hand 2002; Kou et al. 2004; Phua et al. 2005). In this section, a brief summary of these techniques is provided.

A number of fraud detection techniques adopt the statistical approach. For instance, Samfat and Molva (1997) employ the profile of user calling activity similar to the profile in (N)IDES (Javits and Valdes 1991; Anderson et al. 1995). The authors use an analogue of the Hotelling's T^2 statistics to estimate the distance between the current vector of measures and the model stored in the profile. Besides, the user's location updates are modelled by a probabilistic graph, and deviations from the model are considered as potential frauds. The approach is validated using simulation experiments; no reported results based on real-world data were found by the author.

The approach of Cahill et al. (2002) relies on assigning call suspicion scores to individual calls. The score calculation procedure takes into account both the similarity of the current behaviour to the fraudulent activities, and dissimilarity to the account signature. The account signature is specific for each user (account) and its core is an estimate of a multivariate probability distribution of a vector of variables describing different aspects of calling behaviour.

Statistical approach is also followed in (Burge and Shawe-Taylor 1997; Burge and Shawe-Taylor 2001), where the Hellinger distance is calculated between the long-term and short-term distributions of various features extracted from Toll Tickets. A great value of this distance indicates a possible fraudulent activity.

Moreau and Vandewalle (1997) and Moreau et al. (1997) apply neural networks approach to differentiate normal and fraudulent calling activities. The authors employed supervised feed-forward networks, which are trained using both normal data and data describing frauds.

The data mining approach is followed by Fawcett and Provost (1996; 1997). Their approach is based on automatically learning the rules discriminating between normal and fraudulent behaviour. The best rules (covering many user accounts) are selected and used to build profiling monitors. The outputs of these monitors are then employed as indicators of fraudulent activity, and are combined into a single measure using a linear threshold unit.

Kim et al. (2003) employ, for fraud detection, ensembles of SVMs which are trained by using a bagging and bootstrapping technique. The outputs of individual SVMs are subsequently aggregated using majority voting, Least Squares Error (LSE) based weighting, and stacked generalisation as aggregation strategy.

Cortes et al. (2001; 2003) build their approach on the observation that fraudsters often keep contacting each other. Using transactional data, the authors dynamically construct a graph modelling connectivity between subscribers (represented by nodes in the graph), and identify the so-called "communities of interests" (COI) as atomic sub-graphs of highly connected nodes in this graph. The COI, according to the authors, may indicate the groups of fraudsters. Therefore, these communities can be used e.g. to recognise recurring impersonation committed by a same fraudster: the calling activity registered for two accounts will correspond to the same COI and hence to the same individual behind the impersonations.

Several fraud detection techniques have been investigated by Hollmen (2000). Some of these techniques detect frauds as anomalies in calling behaviour;

in these techniques, the normal calling activity is modelled using self-organizing maps (Hollmen et al. 1999), or the adaptive Gaussian mixture model (Taniguchi et al. 1998). In Hollmen and Tresp (2000), the hidden Markov model with hierarchical structure of the hidden variable is employed in order to model normal calling activity at different time scales. Several techniques use supervised learning to build the models distinguishing between the normal and fraudulent activity; among them are the techniques based on linear vector quantization (Hollmen et al. 2000), feed-forward neural network, and Bayesian network (Taniguchi et al. 1998).

2.4 Advantages and limitations of existing approaches

When compared with traditional computer workstations, mobile terminals have a number of distinctive peculiar characteristics, among which are i) the limited battery power, ii) rather limited memory and processing capabilities, as well as restricted network bandwidth, iii) the mobility of the terminals, and iv) the personal use of the terminals. The security means aimed at resisting masquerade attacks in the context of mobile terminals should take these peculiarities into account. In addition to the provision of high security level, these means need to be user-friendly, and conservative in the consumption of scarce resources of the terminals (battery, CPU usage, memory, I/O capacity, and network bandwidth usage). In this section, the authentication, intrusion detection, and fraud detection approaches are evaluated from the point of view of how well they meet these requirements.

As described in previous sections, the identity verification approaches include the knowledge-based, token-based, and biometrics-based approaches. The advantage of the knowledge based approaches is their almost perfect accuracy. The false rejection (FR) error rate is usually equal to 0 (provided the user has not forgotten the password and provided the typing errors are excluded). The false acceptance (FA) error is close to 0 and depends on the length of the password and the approach taken to generate it. However, passwords can be relatively easily compromised by using social engineering methods (Mitnick and Simon 2002; Dolan 2004) or sometimes using special cracking tools. Even more importantly, passwords and PINs are often considered as inconvenient by the users, and as a result of lacking user-friendliness, the password protection is often disabled by the users. Furthermore, continuous use of the approach requires user participation and hence is infeasible.

The use of tokens also has the property of good accuracy. Unless the token is damaged or compromised, or the communication link between the token and the terminal is broken, both the FA and FR errors can be kept close to 0. Furthermore, user participation can be minimised, especially if the token is able to transparently communicate with the terminal. A disadvantage of tokens is the need for additional hardware to be implemented. Furthermore, a token represents yet another mobile device to be carried by the user. It therefore may be lost or stolen along with the protected terminal. As such, it is reasonable to employ

tokens in addition rather than instead of other methods. In the approach of Corner and Noble (2002), for example, the token was protected with a separate PIN. An additional protection of the token with passwords or PINs, however, inherits some of the disadvantages of the knowledge-based identity verification.

As compared with passwords, the biometric characteristics, both physical and behavioural, are more convenient for the users and hence support the user-friendliness requirement. As opposed to tokens, biometric characteristics are not easy to lose and cannot be altered without inflicting a physical injury on the user. Many of these characteristics can be monitored continuously and transparently, thus supporting continuous and unobtrusive security. (It should be noted that some biometric identity verification methods, e.g., fingerprint verification, require user participation, and hence are difficult to employ continuously). However, the problem with the biometric methods is their relatively high computational complexity, especially if the verification is performed continuously. For example, continuous face verification imposes 65% processor loading on a workstation with 550 MHz Pentium-III and 128Mb of RAM (Klosterman and Ganger 2000). This is evidently prohibitive in the context of mobile terminals. Besides, similarly to tokens, the biometric methods usually require additional hardware. The possibility of physical characteristics being counterfeited (Matsumoto et al. 2002) and the insufficient accuracy of the verification based on behavioural characteristics (Mäntyjärvi et al. 2005; Clarke and Furnell 2006) are two further shortcomings of the current biometric identity verification methods.

The masquerader detection approaches developed by the intrusion detection community are designed to run continuously and do not require user participation. They may therefore be expected to be suitable for detecting masquerade attacks in the context of mobile terminals, too. However, they are mainly targeted at networked laptops and workstations as well as servers. The peculiarities of mobile terminals are not taken into account in these approaches. Specifically, the limited battery power, memory and processing capabilities, the mobility of the terminals and their personal use are not taken into account. A noticeable exception is the work of Sun et al. (2006) who studied the applicability of analyzing the mobility patterns of a mobile handset for detecting masqueraders; their results, however, lack empirical evidence. The works by Clarke and Furnell (2006) and Mäntyjärvi et al. (2005) dealing with continuous user identify verification based on keystroke dynamics and gait respectively are also tailored to the context of mobile terminals; however, further work is needed in order to improve the accuracy of verification. Some masquerader detection approaches assume a specific user interface, e.g. UNIX command-line interface (Schonlau et al. 2001; Lane and Brodley 2003); such approaches are not applicable in mobile terminals where the user interface is usually different from the user interfaces employed in desktop PCs. Furthermore, the approaches based on anomaly detection may have a high level of resource consumption due to the need to monitor and update multiple behavioural characteristics (Sundaram 1996). Besides, as the characteristics being monitored vary with time, the detection accuracy (in terms of FR and FA errors) of anomaly detection approaches may not be sufficient.

The pros and cons of the approaches to fraud detection in telecommunication are similar to those of intrusion detection approaches. An additional advan-

tage of the fraud detection techniques is their ability to account for user mobility. However, the fraud detection approaches are focused on the use of services, and therefore, are not able to detect masquerade attacks if the services are not used (e.g., if a masquerader attempts to access personal data stored on the terminal).

In summary, the available approaches to intrusion detection, fraud detection, and authentication have several limitations when their suitability to resist masquerade attacks in a mobile context is considered (see also Table 1). The au-

TABLE 1 Advantages and limitations of authentication, intrusion detection, and fraud detection approaches with respect to the mobile-masquerader detection

Security means	Advantages	Limitations
Knowledge-based authentication	Rather high security level Rather small resource consumption	Perceived as inconvenient by users Can be compromised Continuous use is infeasible
Token-based authentication	High security level Little or no user participation Continuous use is possible	Additional hardware needed Token can be lost or stolen
Biometrics-based authentication	Rather user-friendly Cannot be easily 'lost' Some biometrics allow continuous monitoring	Often computationally expensive if used continuously Often additional hardware is needed Can be counterfeited (if physical characteristics are used) Low accuracy (if behavioural characteristics are used)
Intrusion detection	May work continuously No user involvement needed	Assumed source data (e.g. user commands) may be unavailable on mobile terminals Often resource consumption is prohibitive Insufficient detection accuracy or detection time
Fraud detection in telecommunications	May work continuously No user involvement needed Takes into account terminal mobility	Often resource consumption is prohibitive Insufficient detection accuracy or detection time Detection only possible if network services are used

thentication techniques are often difficult to apply continuously, especially on resource-constrained mobile devices. The intrusion detection techniques are not tailored to the mobile and personal nature of mobile terminals. In turn, the techniques of fraud detection do not reveal masquerade attacks while the mobile device is disconnected from the telecommunication network. Additionally, the security level provided by intrusion detection and fraud detection techniques (in terms of accuracy and time of detection) is not always good enough. Thus, there is a need for techniques which are able to detect a user substitution even when the device is disconnected from the telecommunication networks, which are tailored to mobile devices, and which are able to provide a high security level.

3 MASQUERADER DETECTION AS A CLASSIFICATION PROBLEM

The problem of intrusion detection can be formulated as a problem of classifying the system and/or user behaviour into one of N categories $C_1, \ldots, C_N,\ N \geq 2$, or classes (Lee and Stolfo 2000; Barbara et al. 2001). In the context of intrusion detection, one class corresponds to legitimate behaviour, while the other $N-1$ classes correspond to different types of unacceptable behaviour, or to unacceptable behaviour in general, if $N = 2$. It is assumed that the legitimate behaviour and the attacks are manifested in the values of various system features such as service type, service duration, etc. comprising system security traces. Using these security traces as a training dataset, a classification model, or a classifier, can be trained to differentiate between legitimate and unacceptable behaviour. This classifier can then be used to map previously unseen feature values into one of the above categories. Various data-mining algorithms (Fayyad et al. 1996) based on the achievements in the domains of statistics, pattern recognition, machine learning, and databases, can be employed in order to train the classifier.

In a similar manner, the masquerader detection problem is formulated in this thesis as a classification problem, where the object Z (claimant) is to be classified as belonging either to the user class ($Z \in C_U$) or to the class of impostors ($Z \in C_I$), but not to both of them, i.e. $\{Z|Z \in C_U\} \cap \{Z|Z \in C_I\} = \emptyset$. The process of classification consists of the learning phase and the classification phase (Yom-Tov 2004). In the learning phase, using the training set $\mathcal{DS}_T$, a classifier is trained to differentiate the user from the impostors, i.e. it learns a user model. The training set is composed of values of n_f features (*observation vectors*) $(x_1, \ldots, x_{n_\mathrm{f}})_j$ from the feature space $\mathcal{X}$, along with the class labels $y_j,\ j = 1, \ldots, |\mathcal{DS}_T|$. Each feature, in turn, is based on one or several measurable variables (*measures*) whose values can be directly measured in the course of monitoring user behaviour and environment. In the classification phase, the learnt model is used to classify unlabeled observation vectors into the user class or the impostor class.

In the context of mobile-masquerader detection, only the observation vectors belonging to the user class may be available for learning due to privacy concerns, and because it is highly difficult, if at all possible, to obtain observations

covering the whole space of possible behaviours of impostors (Lane 2000). Therefore, the classification problem in the given context represents the one-class classification problem (Tax 2001), where the training process employs observation vectors of only one class. Having been trained, a one-class classifier will classify a new observation vector as either belonging to the learnt class or not.

Analysing the observation vectors with a single classifier carries with it several difficulties for the following reasons. First, the employed features may have a different nature, or different representation. Therefore, the values of these features may be of different type (categorical or numerical) or may have different scale (Xu et al. 1992). Second, due to the curse of dimensionality (Bishop 1995), the complexity of the learning grows exponentially with the number of features involved. Finally, not all feature values may be available at the time when the classification is done. Because of these issues, it is reasonable to split the set of features into several (possibly overlapping) subsets and process these subsets by *individual classifiers* forming a *classifier ensemble*; the *individual classifications* of these classifiers should be subsequently combined so that a final classification would be produced. The structure of such combining approach is presented in Figure 1 and is described below.

The object Z is represented by the set of n_f features $\{x_1, \ldots, x_{n_\mathrm{f}}\}$ from the feature space $\mathcal{X}$. The values of these features are used to initialize the observation vectors of R individual classifiers. Classifier i takes as input the observation vector $\mathbf{x}_i$ composed of the values of $n_{\mathrm{f}i} \leq n_\mathrm{f}$ features: $\mathbf{x}_i \equiv (x_1^{(i)}, \ldots, x_{n_{\mathrm{f}i}}^{(i)})$, where $x_k^{(i)} \in \mathcal{X}_i \subset \mathcal{X}$, $k = 1, \ldots, n_{\mathrm{f}i}$. Outputs of individual classifiers form the vector of individual classifications, or, for short, the classification vector $\mathbf{u} \equiv (u_1, \ldots, u_R)$.

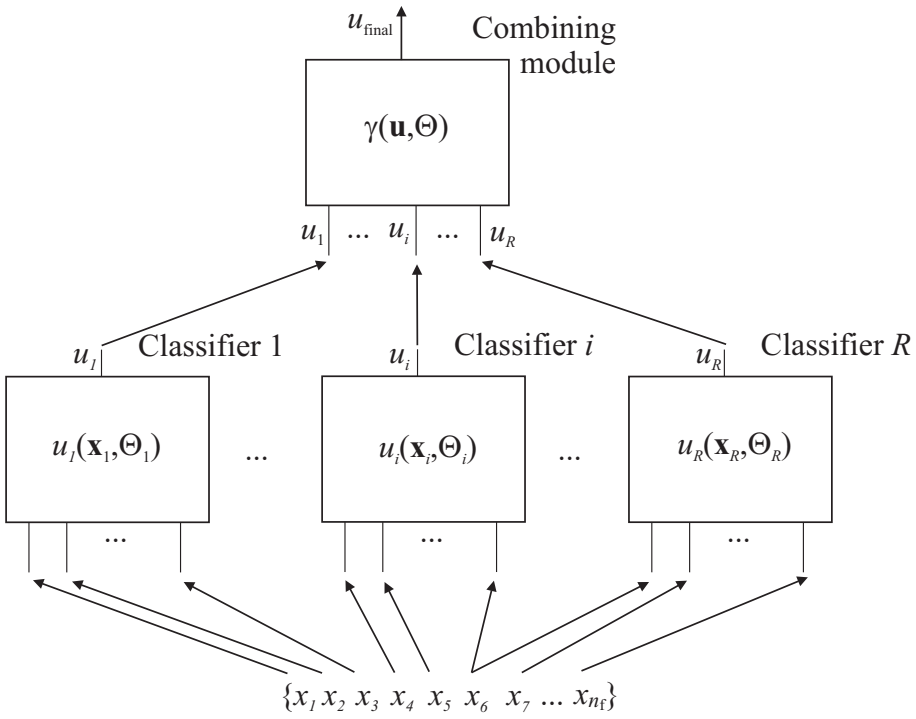

FIGURE 1 Combining one-class classifiers

This classification vector is delivered to the combining module which, using it as input, produces the final classification u_{final}.

The training dataset is the set of observation vectors along with the corresponding class labels $y_j = C_U$: $\mathcal{DS}_T = \{((x_1, \ldots, x_{n_t})_j, y_j)\}$. This dataset is employed in the learning phase in order to estimate, for each classifier i, the set of parameters Θ_i constituting the *model* of this classifier, and in order to estimate the set of parameters Θ determining the behaviour of the combining module. For this, the training dataset is divided into two parts: using the first part, each individual classifier i learns the set of parameters Θ_i, while the second part is employed to estimate the parameters Θ of the combining module.

In the classification phase, given an unlabeled observation vector $\mathbf{x}_i$, each classifier i produces the classification $u_i = u_i(\mathbf{x}_i, \Theta_i)$ indicating the likelihood of the observation vector belonging to the user class, i.e. $Z \in C_U$. For instance, the classifier can output its estimation of class-membership probability $u_i = P(Z \in C_U | \mathbf{x}_i, \Theta_i)$. The individual classifications u_i are delivered by the classifiers to the combining module which, using these classifications as input, produces the final classification u_{final} as a functional mapping $\gamma(\mathbf{u}, \Theta) : \mathbf{u} \mapsto \{C_U, C_I\}$.

In practice, it may happen that not all feature values are available when the classification is made, and therefore the final classification may be required before all individual classifiers have delivered their classifications. Taking the risk of possibly less accurate final classification, the combining module can be modeled as a functional mapping using only the available outputs of individual classifiers.

Above, the use of ensembles of one-class classifiers in mobile-masquerader detection was justified. The following sections outline the methods of one-class classification, and the methods of combining one-class classifiers.

3.1 One-class classification methods

A variety of methods of one-class classification have been developed. Based on the employed internal classification model, these classification methods can be divided into density methods, reconstruction methods, and boundary methods (Tax 2001).

- Density methods (e.g., the method based on the Parzen density estimator) learn from the data the probability density of the feature values, and then make the classification by comparing the estimated probability density of the current observation vector against a predefined threshold.

- Reconstruction methods (e.g. auto-encoders) assume a specific data generation model. The structure of the model is also assumed and the model parameters are estimated from the data. During classification, a reconstruction error reflecting the mismatch between the observation vector and the model is evaluated and compared with a threshold.

- In boundary methods (e.g. k-centres), as the name implies, a boundary around the data is estimated; however, neither the data generation process

is assumed nor is the density estimated. The distance between the observation vector to be classified and the boundary is evaluated and used in classification.

Besides their internal model, one-class classifiers differ in the type of input features (categorical or real-valued), in their ability to reflect temporal relations between features, in their computational and storage requirements, and in other characteristics.

Various one-class classification methods are considered in Article II, *"One-Class Classifiers: A Review and Analysis of Suitability in the Context of Mobile-Masquerader Detection"* (Mazhelis 2006), and their applicability to the problem of mobile-masquerader detection is analysed.

3.2 Methods of combining one-class classifiers

Combining two- or N-class classifiers has been the focus of an extensive research that has resulted in a number of combining methods proposed (Wolpert 1992; Xu et al. 1992; Chan and Stolfo 1993; Dasarathy 1994; Kittler et al. 1998; Merz 1999; Kittler and Alkoot 2000; Alkoot and Kittler 2002). However, for combining one-class classifiers, a relatively small number of methods are available. These include fixed combining schemes and more complex, learnable combining schemes.

Fixed combining schemes can be exemplified by different variations of voting (Xu et al. 1992), as well as by the Product and the Sum rules (Kittler et al. 1998) adapted by Tax and Duin (2001) to the context of one-class classification and referred to as the product of the estimated probabilities (PP) and the mean of the estimated probabilities (MP) rules, respectively. These rules are based on the Bayesian approach and can be derived using the principle of maximum a posteriori probability. In Article III, *"Combining One-Class Classifiers for Mobile-User Substitution Detection"* (Mazhelis and Puuronen 2004), the MP rule is argued to be among the most suitable ones in the context of mobile-masquerader detection, and a modification of the MP rule is proposed.

Some fixed combining methods follow the statistical approach. For example, classifiers' outputs can be mapped on half-normal distribution, and the sum of squares of transformed values may be treated as conforming to chi-square distribution (Anderson et al. 1995).

Learnable combining schemes, as opposed to fixed schemes, can be trained. During training, the parameters Θ of a combining model are estimated from the training data. Such approach is followed in works of Mazhelis (2004) and Mazhelis et al. (2004), where a weighted majority voting is proposed for combining classifiers, and the weights are assigned according to the association rules found between outputs of individual classifiers.

4 RESEARCH OBJECTIVES AND RESEARCH METHODS

In this chapter, the research problem and objectives of the research are stated, and the description of the research methods used is provided.

4.1 Research problem and research objectives

In order to make mobile terminals more secure against masquerade attacks, an arsenal of security measures need to be deployed including preventive measures, detective measures, and response measures, as well as improving user awareness. This research is focused on the detective measures, namely, on the means of mobile-masquerader detection.

Following the categorisation of intrusion detection methods into anomaly detection and misuse detection, two complementary approaches to mobile-masquerader detection may be followed (Section 1.3):

1. The approach involving continuous verification of user activity or identity. It verifies whether the user activity or identity fits to the model kept in a profile and alarms if the verification fails. This is therefore similar to anomaly detection in the sense that deviations from an established norm are looked for.

2. The second approach is complementary to the first one and involves detecting predefined patterns associated with impostor activity or identity. Thus, it is aimed at recognising the presence of an impostor, and is similar to the misuse/abuse detection.

As discussed in Section 1.3, masquerader detection following the impostor recognition approach is difficult to implement because the impostor identity is usually unknown beforehand, and because the task of collecting the data covering practically infinite space of possible behaviours of a masquerader is likely to

be intractable. Therefore, this research concentrates on the first approach involving continuous user activity and identity verification.

Behavioural characteristics are employed in the thesis for the differentiation between the legitimate user and other persons. It is necessary to mention that high-level behavioural characteristics, e.g. taken routes, are employed in the reported research rather than low-level behavioural biometric characteristics, as voice or handwriting, used in authentication. Furthermore, in addition to high-level behavioural characteristics, high-level environmental characteristics, e.g. contacted persons, are employed. These high-level behavioural and environmental characteristics are not unique, and therefore they cannot be used alone as an identity proof. Meanwhile, it may be assumed that these characteristics reflect human personality; the plausibility of this assumption is supported by the Bandura's Social Cognitive Theory (Bandura 1989) stating that human personality, behaviour, and environment are reciprocally determined. Consequently, a combination of high-level characteristics is assumed in this thesis to be peculiar for an individual, and is seen as a high-level biometric characteristic that can be used for distinguishing the legitimate user from other persons.

It is assumed in this thesis that only one person is the legitimate user of the mobile terminal. Therefore, a substitution of this user by another person is assumed to represent a case of a masquerade attack. Thus, the research problem dealt with in this thesis can be defined as *automatically detecting the cases of mobile-user substitution by continuous verification of user identity based on the analysis of user behaviour and environment.*

The task of identity verification is formulated in this thesis as the classification task where the behaviour and environment of the current user of the terminal (claimant) is classified as belonging to either the class of legitimate user or not (cf. Chapter 3). The following objectives are stated:

1. To develop a model of mobile-masquerader detection which includes: i) the part describing the behavioural and environmental characteristics to be used for masquerader detection, as well as relevant measures; ii) the part defining how the values of the above measures can be classified by a set of one-class classifiers as belonging to the user or not, and iii) the part specifying how to combine the outputs of the classifiers so that the accuracy of final classification, and hence, the accuracy of detection would be improved.

2. To develop new technique(s) for combining one-class classifiers to be employed in mobile-masquerader detection, and to evaluate the resulting classification accuracies provided by the technique(s).

3. To elaborate the architecture of a system realizing the mobile-masquerader detection.

4. To demonstrate feasibility of the model by experimenting with a prototype, and to evaluate the detection accuracy and other performance characteristics provided by the prototype.

4.2 Research approaches and research methods

The process of scientific research has been a subject of extensive enquiry within the scientific community; as a result, several research approaches have been identified, and a number of models of research process have been introduced (Wallace 1969; Jenkins 1985; Nunamaker et al. 1991; Hevner et al. 2004; Järvinen 2004).

Hevner et al. (2004) introduced the information systems (IS) research framework combining the behavioural-science and the design-science paradigms. Conducted in a particular environment formed by people, organisations, and technologies, the IS research is aimed at addressing specific issues (business needs), which are relevant in this environment. According to the framework, two complementary phases are needed in such research: the "develop/build" phase and the "justify/evaluate" phase. The behavioural-science research deals with the development and justification of the theories explaining or predicting the phenomena of interest, and is generally aimed at finding truth. On the other hand, the design-science research focuses on the building of artefacts in a form of constructs, models, methods, or instantiations, and the evaluation of their ability to address the perceived business needs. The two research paradigms complement each other. The design-science research is enabled by the knowledge base composed of methodological guidelines and research foundations from reference disciplines, which are accumulated results of behavioural-science research. In turn, the artefacts produced as a result of the design-science research help theories to develop, and are often an object for further behavioural-science research. The results of both the behavioural-science and the design-science IS research are evaluated with respect to their ability to address the identified business needs, and the produced scientific contribution extends the knowledge base of foundations and methodologies. (Hevner et al. 2004)

Järvinen (2004) proposed a taxonomy of research approaches and research methods. In addition to distinguishing between empirical research aimed at utility (i.e. the design-science research) and research aimed at studying reality, the proposed taxonomy introduced the conceptual-analytical research approach, wherein a logical reasoning is employed to build a theory, model, or framework, either by deductively inferring from theoretical assumptions, or by inductively generalising from empirical studies. Below, this taxonomy is mainly used.

Different research approaches are aimed at answering different types of questions, and therefore they require different research methods to address these questions (Järvinen 2004). For instance, the empirical theory testing research approach answers the question of whether a particular theory, model or framework describes accurately a certain part of reality; for answering this question, e.g. controlled experiments can be used.

The research in this thesis concentrates to a considerable extent on answering the questions of whether an innovation (e.g. a model of mobile-masquerader detection) can be built, and how well this innovation can address the practical problem of masquerader detection. The research approach particularly suitable for addressing this type of question is the design-science approach (Nunamaker et al. 1991; Hevner et al. 2004; Järvinen 2004), and therefore it is applied in this

thesis. Meanwhile, since the research problem as formulated in the section above is sufficiently broad, addressing this research problem requires the use of several research approaches and methods.

In the research reported in this thesis, three *research approaches* are used: conceptual-analytical approach, design-science approach, and empirical approach (Järvinen 2004). These approaches are employed in three successive phases, and different *research methods* are applied in different phases:

- In the first phase following the conceptual-analytical approach, based on published theories, models, or frameworks, a model of mobile-masquerader detection is deductively inferred.

- In the second phase, an architecture of the software system implementing this model is developed, and some parts of this system are instantiated as a prototype. This phase therefore follows the design-science approach (artefact-building research) (Hevner et al. 2004; Järvinen 2004).

- In the third phase, performance metrics are defined and used in experiments to assess the validity of the model and to evaluate the performance of the implementation. The research in this phase contains the elements of both the empirical approach (theory-testing research) and the design-science approach (artefact-evaluation research). Here, both the theory-testing research and artefact-evaluation research are studying the same artefact (the mobile-masquerader detection model), but they are attempting to answer different questions: the theory-testing research is answering the question of why the artefact (the model or its instantiation) works, while the artefact-evaluation research is answering the question of how well the artefact works in real settings (March and Smith 1995).

The results of the design-science and empirical research are consequently used to refine the theoretical part, i.e. the mobile-masquerader detection model. The following subsections describe these phases in more detail.

The research phases above can be put in correspondence with the research strategies identified in information systems research (Nunamaker et al. 1991), namely theory building, systems development, experimentation, and observation strategies. The model-building and prototype-instantiation phases above correspond to the Nunamaker's theory building strategy and systems development strategy respectively, while the empirical research in the third phase corresponds to the experimentation strategy.

The above research approaches and research phases can also be expressed in terms of the IS research framework (Hevner et al. 2004). As discussed above, the framework divides the IS research into the phase of development or building, and the phase of justifying or evaluation. The development and justifying of theories, according to the authors, are dealt with mainly by the behavioural-science research aiming at truth, while the building and evaluation of artefacts are the concerns of the design-science research targeting the utility of built artefacts.

The conceptual-analytical research approach in the first phase above can be seen as an integral part of the building activities in the IS research framework. The design-science research approach (including the artefact-building research

in the second phase and the artefact-evaluation research in the third phase) corresponds to the building and the evaluation activities in the framework. The empirical research in the third phase can be seen as belonging to the justification part of the framework (Järvinen 2004).

4.2.1 Conceptual-analytical research

In the first phase, the conceptual-analytical research is conducted. As a result of this phase, based on published theories, models, and frameworks from the domains of machine learning, pattern recognition, statistics, and psychology, a mobile-masquerader detection model is deductively inferred. This model addresses the following questions:

- Which measures describing user behaviour and/or environment should be monitored to distinguish between the legitimate user of a terminal and other persons? In order to identify potentially useful measures, the Royce and Powell's theory of personality and individual differences (Royce and Powell 1983) and Bandura's social cognitive theory (Bandura 1986) are used.
- How can the values of the above measures be used to automatically differentiate the legitimate user and other persons? In addressing this issue, the advances in the domains of machine learning, pattern recognition, and statistics are employed in order to determine potentially useful one-class classifiers and classifier combining techniques.

4.2.2 Artefact-building research

In the second phase, an architecture of the software system implementing the elaborated mobile-masquerader detection model is developed. Furthermore, some parts of this system are instantiated as a prototype.

Two distinct parts having different purposes can be identified in the instantiation; these are the monitoring part and the processing part. The monitoring part is responsible for online monitoring of various measures, and for storing their values in a dedicated database for further processing. The processing part is an implementation of one-class classifiers and combining techniques. For the purposes of the reported research, only the processing part has to be instantiated since the monitoring part has been instantiated and made publicly available by the Context project (Raento et al. 2005).

4.2.3 Theory-testing and artefact-evaluation research

In the third phase, the mobile-masquerader detection model is validated by experimenting with the instantiated prototype, and the performance provided by the prototype is experimentally evaluated. Both numerical experiments end experiments with the real-world data describing the behaviour and environment of mobile-terminal users are conducted.

In the experiments with the real data, the hypothesised behavioural and environmental measures are empirically tested. By assigning these measures to one-class classifiers, the classification accuracies achieved with these measures

and classifiers are estimated; based on the obtained results, the classifiers and measures providing low accuracies are excluded from the model.

The numerical experiments, wherein the data are synthesized, are carried out in order to evaluate the techniques of combining one-class classifiers. The use of synthetic data allows the experimenter to control the properties of these data, and therefore helps in determining the general abilities and shortcomings of the combining techniques. Besides, in order to compare the classification accuracies provided by different combining techniques in the context of mobile-masquerader detection, the experiments with the real data are conducted.

The experiments with the real data are also employed in order to test the feasibility of the elaborated model, to get an understanding of the abilities and shortcomings of the model, and in order to assess the performance characteristics of the implemented prototype, such as the detection accuracy, the required space for both user profile storage and for data processing, the CPU load, and the battery consumption. The design of the experiments with real data, and the details of the dataset used are provided below.

4.2.4 Design of experiments with real-world data

The experiments with real-world data are aimed at the assessment of the classification accuracies provided by different one-class classifiers or combinations thereof and at the comparison of different techniques of combining one-class classifiers. In this subsection, the design of these experiments is briefly described. Further details of the experimental design can be found in (Mazhelis and Puuronen 2006b; Mazhelis et al. 2006b; Mazhelis et al. 2006a).

In order to assess the classification accuracies provided by different one-class classifiers processing distinct measures, or by different ensembles of such classifiers, the holdout cross-validation (Witten and Frank 2000) is used. The classifiers and ensembles are tested by classifying the observation vectors from the classification dataset $\mathcal{DS}_C$ as belonging to the user class or the impostor class. For the results to be more generalizable, the classification dataset $\mathcal{DS}_C$ should include both the observation vectors originated from the user and the observation vectors originated from masqueraders; however, due to unavailability of the masqueraders' data in the dataset used (described below), the other users' data are employed instead.

The data describing the behaviour and environment of each user is gathered in a separate file. For the purposes of the experiments, the data file of each user i is split into two parts in the relation $2:1$. The first part forms the training dataset $\mathcal{DS}_{T_i}$ that is used to train the classifiers for the user i only. The second part is included into the classification dataset $\mathcal{DS}_C$ that is used by a set of classifiers in the classification phase.

The accuracy of classification is assessed by using the Receiver Operating Characteristic (ROC) curve (Egan 1975), which depicts the probability of detection P_D as a function of the probability of false rejection P_{FR}. Furthermore, as a quantitative measure of the classification accuracy, the area under the ROC curve (AUC) (Hanley and McNeil 1982) is employed in the experiments; in general, the greater area corresponds to the classifier with the better accuracy.

When comparing different techniques of combining one-class classifiers, the averaged AUC values obtained with these techniques are compared. In order to determine whether the AUCs for one scheme are on average greater than for another, and whether the difference between them is significant, a parametric test (the t-test for means of two paired samples) and two non-parametric tests (the Wilcoxon Signed Ranks Test and the Sign Test) are performed.

4.2.5 Dataset used in experiments

The dataset used in this thesis was collected during two field studies aimed at the evaluation of a social awareness service (Oulasvirta et al. 2005). The participants of these studies were respectively four members of the same family (a mother and three children), and five high-school students running a small company. The collected dataset[2] registers user communication events (calls and text messages), Bluetooth environment, usage of terminal (active profile, application use, idle and active time, use of charger), as well as the movements of the terminals in terms of GSM cell changes.

In the course of the field studies (Oulasvirta et al. 2005), the use of terminals was continuously monitored, without the need of user interaction, over the period of approximately three months. However, as the terminal could be turned off or the monitoring software disabled, the obtained dataset covers only 55 to 95% of the user activities. Furthermore, the participants were testing a novel application on their terminals, and the terminals themselves were novel for most of the participants; this novelty is likely to affect the behaviour of the participants.

[2] The anonymized version of the dataset is available from http://www.cs.helsinki.fi/group/context/data/.

5 MODEL OF MOBILE-MASQUERADER DETECTION

The mobile-masquerader detection model elaborated in this research, takes as a basis the generic intrusion detection model proposed by Denning (1987). In the Denning's model, the intrusions are detected by matching the observed user behaviour against an activity profile which contains a description of normal behaviour of a user (or a set of users). The current observed behaviour is characterised by statistical metrics, and the norm of user behaviour is represented in the profile by statistical models.

In a similar vein, in the model elaborated in this research, multiple behavioural and environmental aspects are monitored using measurable metrics (measures), and current values of these measures are matched against a profile. Statistical models are used in the profile to describe the norm of user behaviour and environment, although other models such as neural networks or explanation based learning can be used instead. The Denning's model is extended in this thesis with a measure-selection framework, and with methods of combining the evidence obtained from different behavioural and environmental aspects. The proposed model is adjusted to the masquerader detection problem, and it takes into account peculiarities of mobile terminals.

The elaborated model can be conventionally decomposed into three parts: i) the model of user behaviour and environment that relates the user personality to a set of measures, ii) the part specifying how to detect anomalies in the values of these measures by employing one-class classifiers, and iii) the part that, based on the elaborated techniques of combining one-class classifiers, defines how to combine the individual classification results to infer the final classification.

The model is grounded on the assumption that the legitimate user can be differentiated from impostors based on the information about the user behaviour and environment. This assumption can be formulated as follows:

- Some of the characteristics of mobile-user behaviour and environment contain regularities, which reflect the user personality and which keep their individual properties under different circumstances.

- Machine learning and pattern recognition techniques can be applied to automatically reveal the regularities in the above characteristics that can be subsequently coded, stored in the user profile, and used for distinguishing the user from another person.

Figure 2 depicts, in a simplified form, the components involved in the reported research on mobile-masquerader detection. The three parts of the mobile-masquerader detection model are shown by the three leftmost shadowed rectangles. In addition to the model itself, the architecture of the system implementing the model is considered in the research and it is shown in the right part of the figure. This is justified by the need to implement a system prototype, so that the empirical validation of the model using real data would be possible. The three parts of the mobile-masquerader detection model and their validation by experimenting with the prototype are summarised below.

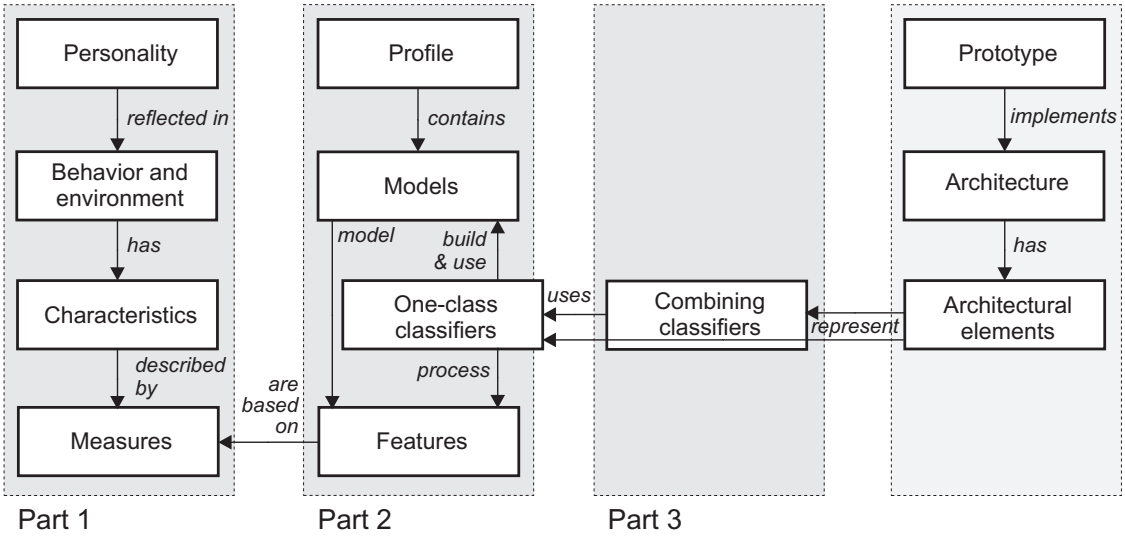

FIGURE 2 Research on mobile-masquerader detection

Model of user behaviour and environment (Part 1). This part addresses the issue of *how user personality is measured.* The personality of a human being is characterised by multiple latent variables studied usually within the psychology domain. For masquerader detection purposes, the indicator variables, or measures, manifesting the corresponding latent personality variables have to be defined. These measures are deductively inferred using theories from the reference discipline of psychology. Royce and Powell's theory of personality and individual differences (Royce and Powell 1983) is used to determine the latent personality variables. Assuming the existence of connections between personality, behaviour, and environment as stated in Bandura's social cognitive theory (Bandura 1986), a set of individual characteristics and measures are hypothesised. The produced descriptive model relating the user's personality with individual behavioural and environmental characteristics provides a conceptual basis for distinguishing between the legitimate user and other individuals; we refer to it as to *the model of*

user behaviour and environment, reflecting the so-called object system which includes the user, his or her personality, and user behaviour and environment. In Article I, *"A framework for behavior-based detection of user substitution in a mobile context"* (Mazhelis and Puuronen 2006a), this conceptual basis is elaborated, and it is applied in order to hypothesize a set of individual characteristics and measures for mobile-masquerader detection. An earlier version of this paper has been published (Mazhelis and Puuronen 2005).

Individual classifiers (Part 2). This part of the model deals with the issue of *how the values of measures are used to differentiate between the user and impostors.* Part 2, together with Part 3, prescribes how mobile-masquerader detection can be implemented relying on the model of user behaviour and environment, and therefore these two parts are referred to as the technical system. Part 2 is based on theoretical foundations from the domain of pattern recognition and machine learning. The one-class classification approach (Tax 2001) is employed. The normal values of measures are modelled by appropriate one-class classifiers. The values of measures for impostors are assumed to deviate from the values learnt by the classifiers; consequently, impostor detection is possible. In Article II, *"One-class classifiers: A review and analysis of suitability in the context of mobile-masquerader detection"* (Mazhelis 2006), in order to define one-class classifiers appropriate for mobile-masquerader detection, the literature survey of one-class classification methods is performed followed by the analysis of their appropriateness for the problem in hand.

Combining the outputs of classifiers (Part 3). The issue of *how the classification results of the individual classifiers are integrated* is addressed by this part. As Part 2, this part is based on theoretical foundations from the domain of pattern recognition and machine learning. Through the literature survey of available techniques, the conceptual basis and formalism for combining one-class classifiers is studied and analysed, and for one of the rules for combining classifiers (the MP rule), a modification (the modMP rule) is proposed in Article III, *"Combining one-class classifiers for mobile-user substitution detection"* (Mazhelis and Puuronen 2004). Using numerical experiments, it is shown in the paper that the proposed modification allows an improvement in classification accuracy to be achieved.

Empirical validation of the model by experimenting with the prototype. The elaborated model of mobile-masquerader detection needs to be empirically validated. For this, an architecture of the software system (technical system) implementing this model has been developed and is presented in Article IV, *"An integrated identity verification system for mobile terminals"* (Mazhelis et al. 2005). Furthermore, for the purposes of the experiments, some parts of the architecture including one-class classifiers and ensembles thereof have been implemented as a prototype. Finally, using the prototype, the elaborated model has been empirically tested in a set of experiments with real-world data.

One of the goals pursued in the experiments is the assessment of the applicability of the behavioural and environmental measures as hypothesised in Article I (Mazhelis and Puuronen 2006a), along with the corresponding one-class

classifiers identified in Article II (Mazhelis 2006), to the problem of mobile-masquerader detection. In order to attain this goal, the classification accuracies achieved with one-class classifiers processing some of the hypothesised measures have been experimentally estimated. The obtained results are reported in Article V, *"Evaluating classifiers for mobile-masquerader detection"* (Mazhelis et al. 2006b). These results are further extended in Article VI, *"Estimating accuracy of mobile-masquerader detection using worst-case and best-case scenario"* (Mazhelis et al. 2006a), where the classification accuracies are estimated by following the worst- and the best-case scenario, for different ranges of the false rejection errors. Besides, other performance characteristics provided by the prototype, such as the required space for both user profile storage and for data processing, the CPU load, and the battery consumption are evaluated (Mazhelis et al. 2006a).

Another goal of the experiments is the evaluation of the techniques of combining one-class classifiers. Therefore, in the experiments, several techniques of combining one-class classifiers (Section 3.2) have been compared on real-world data. Namely, the modMP rule has been compared with the MP and the PP rules in terms of the classification accuracy, and the advantages and limitations of the modMP rule have been investigated. The obtained experimental results are reported in Article VII, *"Comparing classifier combining techniques for mobile-masquerader detection"* (Mazhelis and Puuronen 2006b).

6 SUMMARY OF THE ORIGINAL ARTICLES

In total, seven papers are included in the thesis. This chapter provides the summary of each. For each paper, the addressed research problem is formulated first, followed by the description of the obtained results.

6.1 Article I: "A framework for behavior-based detection of user substitution in a mobile context"

Mazhelis, O. and Puuronen, S. 2006a. A framework for behavior-based detection of user substitution in a mobile context. *Computers & Security* (in press, corrected proof, available online 6 October 2006).

Research problem

This paper elaborates the conceptual basis for mobile-masquerader detection. In the paper, the main focus is on addressing the question of what kind of information about user behaviour and environment can be employed for detecting the cases of masquerading. Thus, the paper concentrates on Part 1 of the masquerader detection model. We consider masquerader detection as a user identity verification problem, and attempt to link behavioural and environmental characteristics to the personality of an individual.

The main assumption of the paper is that cognitive processes are peculiar for each individual. Hence, the factors of personality could be used to differentiate between individuals. However, these factors are latent and cannot be observed directly. Assuming the existence of connections between personality which is latent and the behaviour and environment which are overt (Bandura 1989), the paper aims at identifying the characteristics of user behaviour and environment, which may manifest the above personality factors. It is hypothesized that the set of measures quantitatively describing these characteristics can be used to dif-

ferentiate the user and other individuals. A short earlier version of this paper appeared in Mazhelis and Puuronen (2005).

Results

The paper introduces a general framework of user substitution detection that serves as a conceptual basis for the mobile-masquerader detection model. The focus of the paper is the description of the object system including the user personality, behaviour, and environment. A list of behavioural and environmental aspects that are assumed to reflect the user personality is created and included in the paper. Furthermore, for each of the above aspects, individual characteristics to be used in substitution detection are hypothesized, along with related measures.

Related to the paper is the model of intrusion detection introduced by Denning (1987). This paper extends the Denning's model with the conceptual-theoretical basis for selecting the characteristics to be employed in detection process. Besides, the characteristics identified in the paper are tailored to the problem in hand. Specifically, they are aimed at detecting masquerading rather than detecting all possible types of attack, and they take into account the peculiarity of the behaviour and environment of mobile-terminal users. The limitation of the paper is the lack of empirical evidence that would support or refute the suitability of the hypothesized characteristics and measures.

6.2 Article II: "One-class classifiers: A review and analysis of suitability in the context of mobile-masquerader detection"

Mazhelis, O. 2006. One-class classifiers: A review and analysis of suitability in the context of mobile-masquerader detection. *South African Computer Journal. ARIMA & SACJ Joint special issue on advances in end-user data-mining techniques 36*, 29–48.

Research problem

Based on a literature survey, this paper reviews available one-class classification techniques, and considers their applicability to the problem of masquerader detection in a mobile environment. The design of one-class classifiers to be employed for mobile-masquerader detection is briefly addressed as well. The paper, thus, covers Part 2 of the mobile-masquerader detection model.

The one-class classification techniques are divided into several categories, according to the internal model of the classifier, the ability to classify categorical data, and the ability to take into account temporal regularities present in data. This categorisation is aimed at making the analysis more systematic, and therefore at facilitating the choice of a one-class classifier for a given classification task. Within each category, the classifiers were evaluated along several criteria, such

as robustness, computational and storage requirements, and the number of parameters being estimated.

Results

The advantages and shortcomings of various one-class classification methods were summarised in the paper, in order to determine the applicability of the classification methods to the mobile-masquerader detection problem. In mobile-masquerader detection, one-class classifiers should not be computationally demanding or require a large storage space, and be robust to the noise in training data. The one-class classifiers that meet these requirements are determined in the paper, and the design of one-class classifiers to be employed for mobile-masquerader detection is briefly described.

6.3 Article III: "Combining one-class classifiers for mobile-user substitution detection"

Mazhelis, O. and Puuronen, S. 2004. Combining one-class classifiers for mobile-user substitution detection. In I. Seruca, J. Filipe, S. Hammoudi, and J. Cordeiro (Eds.), *Proceedings of the 6th International Conference on Enterprise Information Systems (ICEIS 2004)*, Volume 4. Portugal: INSTICC Press, 130–137.

Research problem

This paper focuses on the problem of combining the outputs of one-class classifiers (Part 3 of the masquerader detection model). The paper proposes a new modification for the mean of the estimated probabilities (MP) combining rule (Tax and Duin 2001). The MP rule is robust to estimation errors of classifiers and hence is expected to be useful in analysing user behaviour, which is prone to changes over time. In the proposed modification, in order to improve the classification accuracy, the outputs of individual classifiers are made independent of the dimensionality of the features being analysed.

Results

In numerical experiments, three hypothetical one-class classifiers were combined. Using ROC-curve analysis, the proposed modification was compared against the base MP rule as defined by Tax and Duin (2001). The proposed modified MP rule outperformed the base rule, and the difference between them was especially remarkable for low values of FR errors.

Contrary to the base MP rule, the modified rule allows the information about the probabilities $P(u_i|C_I)$, when available, to be taken into account in order to further improve the final classification accuracy. A drawback of both the base and the modified MP combining rule is the ignorance of possible correlations between outputs of individual classifiers. Another limitation of the paper is the lack of experiments with real-world data.

6.4 Article IV: "An integrated identity verification system for mobile terminals"

Mazhelis, O., Markkula, J., and Veijalainen, J. 2005. An integrated identity verification system for mobile terminals. *Information Management & Computer Security 13*(5), 367–378.

Research problem

This paper focuses on the components of a technical system needed for implementing masquerader detection. The problem addressed in the paper can be formulated as the question of what architectural components are needed for mobile-masquerader detection to be implemented, and what is an appropriate placement of these components in a distributed environment.

The problem of masquerader detection is seen in the paper as a user identity verification problem; consequently, the system implementing masquerader detection is considered as an identity verification system. The requirements to an identity verification system are defined, and the selection of architecture components is based on the results of the analysis. Furthermore, various issues affecting the suitability of component distribution between a terminal and a remote server are considered.

The definition of the requirements and architecture components was first reported in an earlier version of this paper that was published in Mazhelis and Markkula (2004). It was extended in Mazhelis et al. (2004) by addressing the issue of architecture component distribution. The current paper represents a revised version of Mazhelis et al. (2004).

Results

An abstract architecture of an integrated identity verification system (IIVS) is introduced in the paper. This architecture integrates the identity verification based on behavioural and environmental characteristics with the identity verification based on other knowledge, token, or biometrics based methods. This integration is aimed at approaching continuous, accurate, and user-friendly verification of user identity. The verification based on behavioural and environmental characteristics is performed by a so-called dynamic identity verifier, which is aimed at the provision of continuous and user-friendly verification. Due to the instability of the user behaviour, dynamic identity verification may result in a considerable level of FR errors. In order to compensate for these errors, the verification failures of the dynamic identity verifier may be confirmed using other, more accurate identity verification methods implemented by a so-called static identity verifier. The components constituting the dynamic and static identity verifier, as well as other required architecture components are specified in the paper.

The components of the architecture may be distributed between a terminal and a server. A number of issues affecting the suitability of a particular distribution are analysed in the paper. These include security and privacy aspects, the

consumption of terminal, server, and network resources, and the availability of identity verification. For each part of the architecture, a placement of the components, which is likely to be suitable, is proposed.

6.5 Article V: "Evaluating classifiers for mobile-masquerader detection"

Mazhelis, O., Puuronen, S., and Raento, M. 2006b. Evaluating classifiers for mobile-masquerader detection. In S. Fischer-Hübner, K. Rannenberg, L. Yngström, and S. Lindskog (Eds.), *Security and Privacy in Dynamic Environments*, IFIP International Federation for Information Processing, Volume 201. Boston: Springer, 271–283. Proceedings of the IFIP TC-11 21st International Information Security Conference (SEC 2006).

Research problem

Based on the publications above and the real-world data collected by the Context project[3] for the research purposes of that project, this paper focuses on the empirical validation of the elaborated mobile-masquerader detection model. The paper is aimed at verifying which of the measures (hypothesized in Article I) are suitable for distinguishing between a mobile-terminal user and masqueraders within the collected dataset. To attain this goal, a set of experiments is conducted, wherein to each of the measures available in the dataset an individual one-class classifier is assigned. In the experiments, i) the classification accuracies achieved by individual classifiers are evaluated, and ii) the individual classifiers which, if used in an ensemble, would improve the final classification accuracy (as compared against single classifiers), are identified. In the ensembles, the modified MP rule (Mazhelis and Puuronen 2004) is used to combine classifiers.

The real-world data used in the experiments reflect the behaviour of two groups of mobile-terminal users (of four and five persons respectively). Due to the absence of data originating from masqueraders, the data of other users belonging to the same group are employed as the impostor's data. In order to evaluate classification accuracies, hold-out cross validation is applied. The area under receiver operating curve (AUC) is used in the experiments as a quantitative measure reflecting the classification accuracies of classifiers and ensembles.

Results

In total, the classification accuracies of nine individual classifiers processing different measures have been experimentally estimated. Based on the results, two of the classifiers along with related measures have been excluded as inaccurate.

In order to determine which of the classifiers are reasonable to use in combination, a number of classifier ensembles have been explored. The accuracies of different classifier combinations have been estimated, and the combinations with

[3] http://www.cs.helsinki.fi/group/context/

superior classification accuracies have been identified. According to the obtained results, better classification accuracy is achieved when the individual classifiers with both high classification accuracy and a small number of non-classifications are used to form the ensemble.

Due to the use of real-world data in the experiments, the obtained results are likely to be generalisable. Meanwhile, the obtained values of accuracies may be underestimated (may represent pessimistic estimates), since the classifiers are distinguishing the users of the same groups, wherein the users are likely to share some of the behavioural or environmental characteristics. Besides, the generalisability may be negatively affected if the data used does not accurately represent the behaviour and environment of mobile-terminal users in general; furthermore, the internal validity of the results may be negatively affected if the behaviour and environment of masqueraders are not accurately approximated by the behaviour and environment of other users.

6.6 Article VI: "Estimating accuracy of mobile-masquerader detection using worst-case and best-case scenario"

Mazhelis, O., Puuronen, S., and Raento, M. 2006a. *Estimating accuracy of mobile-masquerader detection using worst-case and best-case scenario*. In P. Ning, S. Qing, and N. Li (Eds.), *Proceedings of ICICS'06 Eighth International Conference on Information and Communications Security*, Lecture Notes in Computer Science, Volume 4307. Springer-Verlag, 302–321 (in press).

Research problem

The research reported in this paper extends the results presented in Article V. By utilising the collected dataset and assuming that the values of classification accuracy in the previous Article represent pessimistic estimations, the paper seeks answers to the questions of: i) how accurately the classifiers can distinguish the users of different groups, wherein the users are unlikely to share behavioural and environmental characteristics, and ii) how the final classification accuracy of classifier ensembles depends on the range of false rejection rates being considered. As in the previous publication, the modified MP rule (Mazhelis and Puuronen 2004) is employed to combine classifiers in the ensembles.

Similarly to the experiments reported in the previous Article, hold-out cross-validation is used. To estimate the optimistic accuracies, the classifiers attempt to distinguish the users belonging to different user groups. Partial AUCs are used to compare the accuracies of different ensembles for specific ranges of FR rates.

Results

The classification accuracies which are obtained when the classifiers are distinguishing the users of different user groups are remarkably higher than the pes-

simistic accuracy estimation produced when users of the same groups are distinguished. The former can therefore be seen as optimistic accuracy estimates.

The experimental results suggest that different ensembles of classifiers are preferable at different levels of false rejection errors. For small values of FR errors (0.2 and less), a two-classifier ensemble provides the best accuracy; for small and medium FR error values (0.4 and less), the best accuracy is achieved with a three-classifier ensemble; and for all the range of possible FR error values, the best results are produced with a five-classifier ensemble.

The paper also discusses the consumption of the terminal's resources due to the masquerader detection. Based on the analysis of the imposed CPU usage, battery consumption, memory use, and the use of local I/O capacity and network bandwidth, it is concluded that it is feasible to deploy the proposed means of masquerader detection on contemporary smart-phones.

The limitations of this paper include, similarly to the previous publication, potential unrepresentativeness of the employed data which may negatively affect the results' generalisability, and potential negative effect of approximating the behaviour and environment of masqueraders by the behaviour and environment of other users which may threaten the internal validity of the results.

6.7 Article VII: "Comparing classifier combining techniques for mobile-masquerader detection"

Mazhelis, O. and Puuronen, S. 2006b. *Comparing classifier combining techniques for mobile-masquerader detection*. Submitted for publication.

Research problem

This paper continues the empirical validation and analysis of the masquerader detection model in Articles V and VI and employs the same real-world dataset. The paper is aimed at identifying the technique of combining one-class classifiers which provides the best classification accuracy in the context of mobile-masquerader detection. For this, the classification accuracies achieved with different combining rules for the same classifier ensembles are experimentally compared, and then the best rule is determined.

Similarly to the experiments in Articles V and VI, the hold-out cross validation is used. The data of the users belonging to the same group are employed as the impostor's data. As a quantitative measure reflecting the classification accuracies of classifiers as well as ensembles, the total and partial AUCs are used.

Results

Three classifier combining rules have been compared in the experiments: i) the mean of the estimated probabilities (MP) rule (Tax 2001), ii) the modified MP rule (Mazhelis and Puuronen 2004), and iii) the product of the estimated probabilities (PP) rule (Tax 2001). According to the results of comparing the total and

partial AUCs, the classification accuracy achieved with the modMP rule is either better than or approximately equal to the accuracies achieved with the other rules. Based on these results, the conclusion is made that, among the combining rules being compared, the modified MP rule is reasonable to use in mobile-masquerader detection.

In general, the obtained results support the hypothesis in Article III suggesting the superiority of the modMP rule. Meanwhile, the experimental results indicate that the accuracy of the modMP rule depends on the accuracy with which the means of the classifier outputs are estimated. When the estimation is accurate, the modMP rule provides significantly higher classification accuracy than the other rules; on the other hand, should the estimation be inaccurate, the accuracy of modMP rule may yield to the accuracy of the other rules.

In addition to the three combining rules being evaluated in the paper, some other methods of combining one-class classifiers may be applicable in the context of mobile-masquerader detection; however, the experimentation with such combining methods is left for further research. The limitations listed above for the Article V (Section 6.5) are also relevant for this paper.

6.8 About joint publications

The introductory part of the thesis as well as Article II (Mazhelis 2006) were written solely by the author.

The author was the principal author of Article III (Mazhelis and Puuronen 2004). Articlce I (Mazhelis and Puuronen 2006a) and Articles IV–VII (Mazhelis et al. 2005; Mazhelis et al. 2006b; Mazhelis et al. 2006a; Mazhelis and Puuronen 2006b) were written in a close collaboration with other co-authors. The co-authors made contributions to the content and the organisation of the joint papers.

The numerical experiments reported in Article III, as well as the experiments with real-world data in Articles V, VI, and VII were carried out by the author, who also was responsible for the implementation of the software components needed for these experiments.

7 CONCLUSIONS

In this chapter, the contributions of the thesis are summarised, the limitations of the reported research are discussed, and some directions for further research are outlined.

7.1 Contribution of the thesis

Below, the contributions of this thesis are considered in alignment with the four research objectives stated in Section 4.1 on page 39.

The main contribution of the thesis is the elaborated model for mobile-masquerader detection. This model extends the intrusion detection model proposed by Denning (1987) in several ways. Firstly, it includes the conceptual basis for selecting the characteristics to be employed in masquerader detection by relating the behavioural and environmental characteristics of an individual to his or her cognitive personality, and suggests a list of behavioural and environmental characteristics potentially useful for masquerader detection, along with related measures. Secondly, the model describes the one-class classifiers needed to process these measures. Finally, the way of combining the outputs of individual one-class classifiers is specified.

A new rule for combining one-class classifiers based on a variation of the mean of estimated probabilities rule has been introduced; this new rule constitutes the second contribution of the thesis. Included as an integral part of the mobile-masquerader detection model, the rule is aimed at improving the detection accuracy. In numerical experiments and in the experiments with real-world data, the proposed rule was found suitable for combining classifiers in the context of mobile-masquerader detection.

Third, a minor contribution of the thesis is the elaborated architecture of integrated identity verification system where the masquerader detection is integrated with static identity verification in order to achieve accurate, continuous, and unobtrusive verification of user identity.

Fourth, the elaborated masquerader detection model was empirically validated by using real-world data collected through the monitoring of real mobile-terminal users. For validation purposes, a prototype based on the elaborated model was implemented. Through the experimentation with the prototype, its performance characteristics, i.e. the detection accuracy and the computational overhead, were assessed. As a result, the conclusion was made that the model can be used to automatically detect user substitution, and that the model is feasible to deploy on contemporary mobile terminals.

7.2 Limitations and further research

The results of numerical experiments as well as the experiments with real-world data indicate that the elaborated masquerader detection model can be used to automatically differentiate the legitimate user of a terminal from other individuals. Furthermore, results of the experimentation with the implemented prototype suggest that deploying the proposed masquerader detection approach on contemporary mobile terminals is feasible. Meanwhile, these results should be treated as a "proof of concept" only, and extensive further work is needed before the proposed approach can be put in real use. Below, the limitations of this research and some directions for further work are summarized.

Several limitations can be identified in the research reported in this thesis. First, while a number of characteristics and measures have been proposed in Article I (Mazhelis and Puuronen 2006a), only some of them were empirically tested on the real-world dataset. Experimentation with a more extensive dataset is therefore needed in order to test the suitability of other characteristics and measures.

Second, not only the number of empirically tested measures was limited, the number of one-class classifiers applied to analyse these measures was limited as well. With the aim of improving the classification accuracy, the applicability of other classifiers needs to be empirically tested in further research. Alternatively, the design of the same classifiers can be enhanced in the course of further work.

Third, in addition to the proposed combining schemes, other schemes may be applied for combining one-class classifiers. These schemes need to be compared using real data, in order to determine the advantages and shortcomings thereof in the context of mobile-masquerader detection. For example, in Mazhelis et al. (2004) a combining technique has been introduced which provides a superior accuracy as compared with majority voting scheme by taking into account dependencies between classifiers; in further study, this technique needs to be experimentally compared against other combining techniques.

Fourth, the real-world data utilised in the experiments reflects the behaviour of a rather limited number of users. Furthermore, these users might not accurately represent the general population of mobile-terminal users. Therefore, the generalisability of the results may be limited, and further experiments on an independent dataset representing a larger population of mobile-terminal users may be needed in order to validate the achieved results. Besides, it was assumed

in the experiments that the behaviour and environment of masqueraders can be approximated by the behaviour and environment of other legitimate users. Whether this assumption holds needs to be verified in further research.

Besides, the normal user behaviour as well as user environment undergoes gradual changes over time. These changes, referred to as concept drift, need to be taken into account by the mobile-masquerader detection model. Therefore, the issue of concept drift should also be addressed in further research.

Further research is also needed in order to address the issues related to the practical applicability of the proposed mobile-masquerader detection model in real settings. The issues to be addressed include privacy issues, user acceptance, and implementation issues, among other things. From the viewpoint of protecting the user privacy, the implementation of the proposed masquerader detection mechanism needs to ensure that all the personal information collected and stored in the user profile is used for masquerader detection purposes only and cannot be used for other purposes (e.g. retrieved by a masquerader). User acceptance tests need to be conducted, in order to find out whether the users would tolerate, in practice, the false rejection errors triggered by the implementation. Finally, when implementing the proposed mobile-masquerader detection mechanism, the portability of the mechanism across different terminals needs to be provided. This is especially important if the expected lifetime of the mechanism exceeds the average lifetime of mobile terminals, and therefore the mechanism needs to be easily transferable to a newer version of the terminal when it becomes available.

REFERENCES

3GPP 2002. *3G Security; Security Threats and Requirements (Release 4)*. Technical Specification 3GPP TS 21.133, Available from http://www.3gpp.org/ftp/Specs/html-info/21133.htm (read 19.03.2004).

Agrawal, R., Imielinski, T., and Swami, A. N. 1993. Mining association rules between sets of items in large databases. In P. Buneman and S. Jajodia (Eds.), *Proceedings of the 1993 ACM SIGMOD International Conference on Management of Data*. New York, NY, USA: ACM Press, 207–216.

Ailisto, H., Lindholm, M., Mäkelä, S.-M., and Vildjiounaite, E. 2004. Unobtrusive user identification with light biometrics. In A. Hyrskykari (Ed.), *NordiCHI '04: Proceedings of the third Nordic conference on Human-computer interaction*. New York, NY, USA: ACM Press, 327–330.

Alkoot, F. and Kittler, J. 2002. Modified product fusion. *Pattern Recognition Letters 23*(8), 957–965.

Anderson, D., Lunt, T., Javitz, H., Tamaru, A., and Valdes, A. 1994. *Safeguard Final Report: Detecting Unusual Program Behavior Using the NIDES Statistical Component*. Final report, Menlo Park, California: Computer Science Laboratory, SRI International.

Anderson, D., Lunt, T., Javitz, H., Tamaru, A., and Valdes, A. 1995. *Detecting Unusual Program Behavior Using the Statistical Components of NIDES*. SRI Technical Report SRI-CRL-95-06, Menlo Park, California: Computer Science Laboratory, SRI International.

Anderson, J. 1980. *Computer Security Threat Monitoring and Surveillance*. Technical Report 79F296400, Fort Washington, Pennsylvania: James P. Anderson Co.

Axelsson, S. 2000. *Intrusion Detection Systems: A Survey and Taxonomy*. Technical Report 99-15: Chalmers Univ.

Bandura, A. 1986. *Social Foundations of Thought and Action: A Social Cognitive Theory*. Englewood Cliffs, NJ: Prentice Hall.

Bandura, A. 1989. Social cognitive theory. *Annals of Child Development 6*, 1–60.

Barbara, D., Couto, J., Jajodia, S., and Wu, N. 2001. ADAM: a testbed for exploring the use of data mining in intrusion detection. *SIGMOD Rec. 30*(4), 15–24.

Bardram, J., Kjær, R. E., and Pedersen, M. Ø. 2003. Context-aware user authentication – supporting proximity-based login in pervasive computing. In A. K. Dey, A. Schmidt, and J. F. McCarthy (Eds.), *Proc. of UbiComp 2003: Ubiquitous Computing, 5th International Conference*, Lecture Notes in Computer Science, Volume 2864. Germany: Springer, 107–123.

Ben-Yacoub, S., Abdeljaoued, Y., and Mayoraz, E. 1999. Fusion of face and speech data for person identity verification. *IEEE Transactions on Neural Networks 10*(5), 1065–1074.

Bezroukov, N. 2005. Intrusion prevention and detection roadmap for large enterprises in 2005-2007. Unpublished manuscript. Available from http://www.softpanorama.org/Security/Whitepapers/ids_roadmap.shtml (read 05.06.2006).

Bishop, C. M. 1995. *Neural Networks for Pattern Recognition*. Oxford: Oxford University Press.

Bolton, R. J. and Hand, D. J. 2002. Statistical fraud detection: A review. *Statistical Science 17*(3), 235–249.

Bontchev, V. 1998. *Methodology of Anti-Virus Research*. Faculty of Informatics, University of Hamburg, Ph.D. thesis.

Burge, P. and Shawe-Taylor, J. 1997. Detecting cellular fraud using adaptive prototypes. In T. Fawcett (Ed.), *Proceedings AAAI-97 Workshop on AI Approaches to Fraud Detection and Risk Management*. Menlo Park, California: AAAI Press, 9–13.

Burge, P. and Shawe-Taylor, J. 2001. An unsupervised neural network approach to profiling the behavior of mobile phone users for use in fraud detection. *J. Parallel Distrib. Comput. 61*(7), 915–925.

Cahill, M. H., Lambert, D., Pinheiro, J. C., and Sun, D. X. 2002. Detecting fraud in the real world. In J. Abello, P. M. Pardalos, and M. G. C. Resende (Eds.), *Handbook of massive data sets*. Norwell, MA, USA: Kluwer Academic Publishers, 911–929.

Chan, P. K. and Stolfo, S. J. 1993. Toward parallel and distributed learning by meta-learning. In G. Piatetsky-Shapiro (Ed.), *Technical Report of AAAI Workshop in Knowledge Discovery in Databases, WS-93-02*. Menlo Park, CA: AAAI Press, 227–240.

Chandra, A. and Calderon, T. 2005. Challenges and constraints to the diffusion of biometrics in information systems. *Commun. ACM 48*(12), 101–106.

Chen, B., Lee, J., and Wu, A. 2006. Active event correlation in Bro IDS to detect multi-stage attacks. In J. L. Cole and S. D. Wolthusen (Eds.), *Fourth IEEE International Workshop on Information Assurance (IWIA 2006)*. Los Alamitos, CA: IEEE Computer Society, 32–50.

Chen, Y.-r., Åström, M., and Wang, L.-h. 2004. *Session Comparison Measurement and Learning in Masquerading Detection*. Technical Report 2004:14, Luleå, Sweden: Business Administration and Social Sciences / Systems Sciences, Luleå University of Technology.

Cheng, H.-T., Chao, Y.-H., Yeh, S.-L., Chen, C.-S., Wang, H.-M., and Hung, Y.-P. 2005. An efficient approach to multimodal person identity verification by fusing face and voice information. In *IEEE International Conference on Multimedia and Expo (ICME 2005)*. IEEE, 542–545.

Choudhury, T., Clarkson, B., Jebara, T., and Pentland, A. 1999. Multimodal person recognition using unconstrained audio and video. In *The 2nd International Conference on Audio-Visual Biometric Person Authentication*. 176–181.

Clarke, N. L. and Furnell, S. M. 2005. Authentication of users on mobile telephones – A survey of attitudes and practices. *Computers & Security 24*(7), 519–527.

Clarke, N. L. and Furnell, S. M. 2006. Authenticating mobile phone users using keystroke analysis. *International Journal of Information Security* (Published online on August 1 2006), 1–14.

Clarke, N. L., Furnell, S. M., Lines, B., and Reynolds, P. L. 2003. Keystroke dynamics on a mobile handset: A feasibility study. *Information Management and Computer Security 11*(4), 161–166.

Clarke, N. L., Furnell, S. M., Rodwell, P. M., and Reynolds, P. L. 2002. Acceptance of subscriber authentication methods for mobile telephony devices. *Computers & Security 21*(3), 220–228.

Clarke, R. 1994. Human identification in information systems: Management challenges and public policy issues. *Information Technology & People 7*(4), 6–37.

Clifton, C. and Gengo, G. 2000. Developing custom intrusion detection filters using data mining. In *21st Century Military Communications Conference Proceedings (MILCOM 2000)*, Volume 1. IEEE Communications Society, 440–443.

Cohen, W. W. 1995. Fast effective rule induction. In A. Prieditis and S. Russell (Eds.), *Proc. of the 12th International Conference on Machine Learning*. Tahoe City, CA: Morgan Kaufmann, 115–123.

Coolen, R. and Luiijf, H. 2002. *Intrusion Detection: Generics and State-of-the-Art*. Technical Report RTO-TR-049, Neuilly-Sur-Seine Cedex, France: Research and Technology Organisation.

Corner, M. and Noble, B. 2002. Zero-interaction authentication. In I. F. Akyildiz, J. Y. B. Lin, R. Jain, V. Bharghavan, and A. T. Campbell (Eds.), *Proceedings of the Eighth ACM Conference on Mobile Computing and Networking*. New York, NY, USA: ACM Press, 1–11.

Corner, M. D. and Noble, B. D. 2003. Protecting applications with transient authentication. In *The First International Conference on Mobile Systems, Applications, and Services (MobiSys'03)*. New York, NY, USA: ACM Press, 57–70.

Cortes, C., Pregibon, D., and Volinsky, C. 2001. Communities of interest. In F. Hoffmann, D. J. Hand, N. Adams, D. Fisher, and G. Guimaraes (Eds.), *IDA '01: Proceedings of the 4th International Conference on Advances in Intelligent Data Analysis*, Lecture Notes in Computer Science, Volume 2189. Germany: Springer-Verlag, 105–114.

Cortes, C., Pregibon, D., and Volinsky, C. 2003. Computational methods for dynamic graphs. *Journal of Computational and Graphical Statistics 12*(4), 950–970.

Cuppens, F. and Miege, A. 2002. Alert correlation in a cooperative intrusion detection framework. In *Proceedings of 2002 IEEE Symposium on Security and Privacy*. Washington, DC, USA: IEEE Computer Society, 187–200.

Dasarathy, B. V. 1994. *Decision Fusion*. Los Alamitos, CA: IEEE Computer Society Press.

Debar, H., Becker, M., and Siboni, D. 1992. A neural network component for an intrusion detection system. In *IEEE Symposium of Research in Computer Security and Privacy*. Washington, DC, USA: IEEE Computer Society, 240–250.

Debar, H., Dacier, M., and Wespi, A. 1999. Towards a taxonomy of intrusion-detection systems. *Computer Networks 31*(8), 805–822.

Debar, H. and Wespi, A. 2001. Aggregation and correlation of intrusion-detection alerts. In W. Lee, L. Me, and A. Wespi (Eds.), *Recent Advances in Intrusion Detection (RAID 2001)*, Lecture Notes in Computer Science, 2212. Berlin Heidelberg: Springer-Verlag, 85–103.

Denning, D. 1987. An intrusion detection model. *IEEE Transactions on Software Engineering. Special issue on computer security and privacy 13*(2), 222–232.

Denning, D. 1997. Cyberspace attacks and countermeasures. In D. Denning and P. Denning (Eds.), *Internet Besieged: Countering Cyberspace Scofflaws*. Boston, MA: Addison-Wesley Professional, 29–56.

Dolan, A. 2004. *Social Engineering*. SANS InfoSec Reading Room, Available from http://www.sans.org/rr/catindex.php?cat_id=51 (read 11.06.2004).

DuMouchel, W. and Schonlau, M. 1999. A comparison of test statistics for computer intrusion detection based on principal components regression of transition probabilities. In S. Weisberg (Ed.), *Proceedings of the 30th Symposium on the Interface: Computing Science and Statistics*, Volume 30. Interface Foundation of North America, 404–413.

Egan, J. P. 1975. *Signal detection theory and ROC analysis*. New York: Academic Press.

Ensure Technologies 2006. User's Guide for XyLoc Client ver 8.x.x. Available from http://ensuretech.com/software/510-0100-003_rev0_07_Users_Guide_for_XyLoc_Client_ver_8_x_x.pdf (read 9.11.2006).

Fawcett, T. and Provost, F. 1996. Combining data mining and machine learning for effective user profiling. In E. Simoudis, J. Han, and U. Fayyad (Eds.), *Proceedings on the Second International Conference on Knowledge Discovery and Data Mining*. Menlo Park, CA: AAAI Press, 8–13.

Fawcett, T. and Provost, F. J. 1997. Adaptive fraud detection. *Data Mining and Knowledge Discovery 1*(3), 291–316.

Fayyad, U., Piatetsky-Shapiro, G., and Smyth, P. 1996. Knowledge discovery and data mining: Towards a unifying framework. In E. Simoudis, J. Han, and U. Fayyad (Eds.), *Proc. 2nd Int'l. Conf. on Knowledge Discovery and Data Mining (KDD-96)*. Menlo Park, CA: AAAI Press, 82–88.

Fierrez-Aguilar, J., Garcia-Romero, D., Ortega-Garcia, J., and Gonzalez-Rodriguez, J. 2005. Adapted user-dependent multimodal biometric authentication exploiting general information. *Pattern Recogn. Lett. 26*(16), 2628–2639.

Ghosh, A. K., Schwartzbard, A., and Schatz, M. 1999. Learning program behavior profiles for intrusion detection. In *1 st USENIX Workshop on Intrusion*

Detection and Network Monitoring. Berkeley, CA, USA: USENIX Association, 51–62.

Giacinto, G., Roli, F., and Didaci, L. 2003. Fusion of multiple classifiers for intrusion detection in computer networks. *Pattern Recogn. Lett. 24*(12), 1795–1803.

Goldman, R. P., Heimerdinger, W., Harp, S. A., Geib, C., Thomas, V., and Carter, R. L. 2001. Information modeling for intrusion report aggregation. In *Proceedings of the DARPA Information Survivability Conference and Exposition II (DISCEX '01)*, Volume 1. Los Alamitos, California: IEEE Computer Society, 329–342.

Gunetti, D. and Picardi, C. 2005. Keystroke analysis of free text. *ACM Trans. Inf. Syst. Secur. 8*(3), 312–347.

Haines, J., Ryder, D., Tinnel, L., and Taylor, S. 2003. Validation of sensor alert correlators. *IEEE Security & Privacy Magazine 1*(1), 46–56.

Han, S.-J. and Cho, S.-B. 2003. Detecting intrusion with rule-based integration of multiple models. *Computers & Security 22*(7), 613–623.

Hanley, J. A. and McNeil, B. J. 1982. The meaning and use of the area under a receiver operating characteristic (ROC) curve. *Radiology 143*, 29–36.

Hevner, A., March, S., and Park, J. 2004. Design science in information systems research. *MIS Quarterly 28*(1), 75–105.

Hollmen, J. 2000. *User Profiling and Classification for Fraud Detection in Mobile Communications Networks*. Helsinki University of Technology, PhD thesis.

Hollmen, J. and Tresp, V. 2000. Hidden markov model for metric and event-based data. In M. Gabbouj and P. Kuosmanen (Eds.), *EUSIPCO 2000 – X European Signal Processing Conference*. Tampere, Finland: TTKK-Paino, 737–740.

Hollmen, J., Tresp, V., and Simula, O. 1999. A self-organizing map algorithm for clustering probabilistic models. In *Proceedings of the Ninth International Conference on Artificial Neural Networks (ICANN'99)*, IEE Conference Proceedings, Conference Publication No. 470, Volume 2. The IEE, 946–951.

Hollmen, J., Tresp, V., and Simula, O. 2000. Learning vector quantization algorithm for probabilistic models. In M. Gabbouj and P. Kuosmanen (Eds.), *EUSIPCO 2000 – X European Signal Processing Conference*. Tampere, Finland: TTKK-Paino, 721–724.

Info∼Tech Research Group 2006. *Intrusion Prevention Not Ready to Replace Intrusion Detection*. Info-Tech Advisor – Research Note: Available from http://www.infotech.com/Home/ITA/Issues/20060214.aspx (published on February 14, 2006).

ISO/IEC 7498-2 1989. *Information Processing Systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security architecture*. Geneva, Switzerland: International Organization for Standardization. Equivalent to ITU-T Rec. X.800.

Jain, A. K., Hong, L., and Kulkarni, Y. 1999. A multimodal biometric system using fingerprint, face, and speech. In *The 2nd International Conference on Audio-Visual Biometric Person Authentication*. 182–187.

Javits, H. and Valdes, A. 1991. The SRI IDES statistical anomaly detector. In *IEEE Symposium of Research in Computer Security and Privacy*. IEEE Computer Society Press.

Javits, H. S. and Valdes, A. 1993. *The NIDES Statistical Component: Description and Justification*. Technical Report A010, Menlo Park, California: Computer Science Laboratory, SRI International.

Jenkins, A. 1985. Research methodologies and MIS research. In E. Mumford, R. Hirschheim, G. Fitzgerald, and A. Wood-Harper (Eds.), *Research Methods in Information Systems*. Amsterdam: North-Holland, 103–117.

Jermyn, I., Mayer, A., Monrose, F., Reiter, M. K., and Rubin, A. D. 1999. The design and analysis of graphical passwords. In *Proceedings of the 8th USENIX Security Symposium*. USENIX Association, available online at http://www.usenix.org/events/sec99/ (read 9.11.2006).

Joachims, T. 1999. Making large-scale SVM learning practical. In B. Schlkopf, C. Burges, and A. Smola (Eds.), *Advances in Kernel Methods: Support Vector Learning*. MIT Press, 169–184.

Julisch, K. 2003. Clustering intrusion detection alarms to support root cause analysis. *ACM Trans. Inf. Syst. Secur. 6*(4), 443–471.

Julisch, K. and Dacier, M. 2002. Mining intrusion detection alarms for actionable knowledge. In O. R. Zaiane, R. Goebel, D. Hand, D. Keim, and R. Ng (Eds.), *Proceedings of the eighth ACM SIGKDD international conference on Knowledge discovery and data mining*. New York, NY, USA: ACM Press, 366–375.

Järvinen, P. 2004. *On Research Methods*. Tampere: Opinpajan Kirja.

Kageyama, Y. 2006. Cell phone takes security to new heights. The Associated Press. Available from http://hosted.ap.org/dynamic/stories/J/JAPAN_SECURITY_PHONE?SITE=AP&SECTION=HOME&TEMPLATE=DEFAULT (read 04.11.2006).

Kale, A., Cuntoor, N., Yegnanarayana, B., Rajagopalan, A., and Chellappa, R. 2003. Gait analysis for human identification. In J. Kittler and M. S. Nixon (Eds.), *Proceedings of 4th International Conference on Audio- and Video-Based Biometrie Person Authentication, AVBPA 2003*, Lecture Notes in Computer Science, 2688. Berlin Heidelberg: Springer-Verlag, 706–714.

Kim, H.-C., Pang, S., Je, H.-M., Kim, D., and Bang, S. Y. 2003. Constructing support vector machine ensemble. *Pattern Recognition 36*(12), 2757–2767.

Kim, H.-S. and Cha, S.-D. 2005. Empirical evaluation of SVM-based masquerade detection using UNIX commands. *Computers & Security 24*(2), 160–168.

Kirovski, D., sa Jojić, N., and Roberts, P. 2006. Click passwords. In S. Fischer-Hübner, K. Rannenberg, L. Yngström, and S. Lindskog (Eds.), *Security and Privacy in Dynamic Environments*, IFIP International Federation for Information Processing, Volume 201. Boston: Springer, 351–363. Proceedings of the IFIP TC-11 21st International Information Security Conference (SEC 2006).

Kittler, J. and Alkoot, F. 2000. Multiple expert system design by combined feature selection and probability level fusion. In *Proceedings of the Fusion'2000, Third*

International Conference on Information Fusion, Volume 2. France: ONERA, 9–16.

Kittler, J., Hatef, M., Duin, R. P., and Matas, J. 1998. On combining classifiers. *IEEE Transactions on Pattern Analysis and Machine Intelligence 20*(3), 226–239.

Klosterman, A. J. and Ganger, G. R. 2000. *Secure Continuous Biometric-enhanced Authentication*. Technical Report CMU-CS-00-134: Carnegie Mellon University.

Koreman, J., Morris, A., Wu, D., Jassim, S., Sellahewa, H., Ehlers, J., Chollet, G., Aversano, G., Bredin, H., Garcia-Salicetti, S., Allano, L., Ly Van, B., and Dorizzi, B. 2006. Multi-modal biometric authentication on the SecurePhone PDA. In *Second Workshop on Multimodal User Authentication (MMUA 2006)*. Available online at http://mmua.cs.ucsb.edu/MMUA2006 (read 9.11.2006).

Kou, Y., Lu, C., Sirwongwattana, S., and Huang, Y. 2004. Survey of fraud detection techniques. In *Proceedings of the 2004 IEEE International Conference on Networking, Sensing, and Control*, Volume 2. Taiwan: DnE Information Service Net, 749–754.

Krsul, I. 1998. *Software Vulnerability Analysis*. Purdue University, West Lafayette, IN, Ph.D. thesis.

Kumar, S. 1995. *Classification and Detection of Computer Intrusions*. Purdue University, West Lafayette, USA, Ph.D. thesis.

Lane, T. 2000. *Machine Learning Techniques for the Computer Security Domain of Anomaly Detection*. Purdue University, West Lafayette, IN, Ph.D. thesis.

Lane, T. and Brodley, C. E. 1999. Temporal sequence learning and data reduction for anomaly detection. *ACM Transactions on Information and System Security 2*(3), 295–331.

Lane, T. and Brodley, C. E. 2003. An empirical study of two approaches to sequence learning for anomaly detection. *Machine Learning 51*(1), 73–107.

Lee, S., Chung, B., Kim, H., Lee, Y., Park, C., and Yoon, H. 2006. Real-time analysis of intrusion detection alerts via correlation. *Computers & Security 25*(3), 169–183.

Lee, W. and Stolfo, S. 2000. A framework for constructing features and models for intrusion detection systems. *ACM Transactions on Information and System Security (TISSEC) 3*(4), 227–261.

Li, Q., Juang, B.-H., Zhou, Q., and Lee, C.-H. 2000. Automatic verbal information verification for user authentication. *Transactions on Speech and Audio Processing 8*(5), 585–596.

Manganaris, S., Christensen, M., Zerkle, D., and Hermiz, K. 2000. A data mining analysis of RTID alarms. *Computer Networks 34*(4), 571–577.

Mannila, H. and Toivonen, H. 1996. Discovering generalized episodes using minimal occurrences. In E. Simoudis, J. Han, and U. M. Fayyad (Eds.), *Knowledge Discovery and Data Mining*. Cambridge, MA: AAAI Press, 146–151.

March, S. T. and Smith, G. F. 1995. Design and natural science research on information technology. *Decis. Support Syst. 15*(4), 251–266.

Matsumoto, T., Matsumoto, H., Yamada, K., and Hoshino, S. 2002. Impact of artificial gummy fingers on fingerprint systems. In R. L. van Renesse (Ed.), *Proceedings of SPIE*, Volume 4677, Optical Security and Counterfeit Deterrence Techniques IV. Bellingham, WA: SPIE - The International Society for Optical Engineering, 275–289.

Maxion, R. and Townsend, T. 2004. Masquerade detection augmented with error analysis. *IEEE Transactions on Reliability 53*(1), 124–147.

Mazhelis, O. 2004. *Using Meta-Learning to Reveal Dependencies between Errors in Mobile User Substitution Detection*. Computer science and information systems reports, working papers WP-39: University of Jyväskylä. 65 p.

Mazhelis, O. 2006. One-class classifiers: A review and analysis of suitability in the context of mobile-masquerader detection. *South African Computer Journal. ARIMA & SACJ Joint special issue on advances in end-user data-mining techniques 36*, 29–48.

Mazhelis, O. and Markkula, J. 2004. An integrated identity verification system for mobile terminals: Requirements and architecture components. In C. Branki, J. F. Hampe, R. Helfrich, K. Kurbel, G. Schwabe, F. Teuteberg, S. Uellner, R. Unland, and G. Wanner (Eds.), *Multikonferenz Wirtschaftsinformatik MKWI 2004, Techniques and Applications for Mobile Commerce (TAMoCO)*, Volume 3. Köln, Germany: Akademische Verlagsgesellschaft Aka, 216–227.

Mazhelis, O., Markkula, J., and Veijalainen, J. 2004. An integrated identity verification system for mobile terminals: System components and their distribution. In S. M. Furnell and P. S. Dowland (Eds.), *Proceedings of the Fourth International Network Conference*. United Kingdom: University of Plymouth, 353–360.

Mazhelis, O., Markkula, J., and Veijalainen, J. 2005. An integrated identity verification system for mobile terminals. *Information Management & Computer Security 13*(5), 367–378.

Mazhelis, O. and Puuronen, S. 2004. Combining one-class classifiers for mobile-user substitution detection. In I. Seruca, J. Filipe, S. Hammoudi, and J. Cordeiro (Eds.), *Proceedings of the 6th International Conference on Enterprise Information Systems (ICEIS 2004)*, Volume 4. Portugal: INSTICC Press, 130–137.

Mazhelis, O. and Puuronen, S. 2005. Characteristics and measures for mobile-masquerader detection. In P. Dowland, S. Furnell, B. Thuraisingham, and X. S. Wang (Eds.), *Proc. IFIP TC-11 WG 11.1 & WG 11.5 Joint Working Conference on Security Management, Integrity, and Internal Control in Information Systems*. USA: Springer Science+Business Media, 303–318.

Mazhelis, O. and Puuronen, S. 2006a. A framework for behavior-based detection of user substitution in a mobile context. *Computers & Security* (in press, corrected proof, available online 6 October 2006).

Mazhelis, O. and Puuronen, S. 2006b. *Comparing classifier combining techniques for mobile-masquerader detection*. Submitted for publication.

Mazhelis, O., Puuronen, S., and Raento, M. 2006a. Estimating accuracy of mobile-masquerader detection using worst-case and best-case scenario. In P. Ning, S. Qing, and N. Li (Eds.), *Proceedings of ICICS'06 Eighth International Conference on Information and Communications Security*, Lecture Notes in Computer Science, Volume 4307. Springer-Verlag, 302–321 (in press).

Mazhelis, O., Puuronen, S., and Raento, M. 2006b. Evaluating classifiers for mobile-masquerader detection. In S. Fischer-Hübner, K. Rannenberg, L. Yngström, and S. Lindskog (Eds.), *Security and Privacy in Dynamic Environments*, IFIP International Federation for Information Processing, Volume 201. Boston: Springer, 271–283.

Mazhelis, O., Puuronen, S., and Veijalainen, J. 2004. Modelling dependencies between classifiers in mobile masquerader detection. In J. Lopez, S. Qing, and E. Okamoto (Eds.), *Proceedings of the 6th International Conference on Information and Communications Security (ICICS 2004)*, Lecture Notes in Computer Science, Volume 3269. Berlin Heidelberg: Springer-Verlag, 318–330.

McHugh, J. 2001. Intrusion and intrusion detection. *International Journal of Information Security 1*(1), 14–35.

Merz, C. J. 1999. Using correspondence analysis to combine classifiers. *Machine Learning 36*(1-2), 33–58.

Mitnick, K. and Simon, W. L. 2002. *The Art of Deception*. Indianapolis, Indiana: Wiley Publishing.

Moreau, Y. and Vandewalle, J. 1997. Fraud detection in mobile communications using supervised neural networks. In B. Kappen and S. Gielen (Eds.), *Proceedings of SNN'97: Europe's Best Neural Networks Practice*. Singapore: World Scientific, 149–152.

Moreau, Y., Verrelst, H., and Vandewalle, J. 1997. Detection of mobile phone fraud using supervised neural networks: A first prototype. In W. Gerstner, A. Germond, M. Hasler, and J.-D. Nicoud (Eds.), *Proceedings of ICANN International Conference on Artificial Neural Networks*, Lecture Notes in Computer Science, Volume 1327. Berlin Heidelberg: Springer-Verlag, 1065–1070.

Morin, B., Mé, L., Debar, H., and Ducassé, M. 2002. M2D2: A formal data model for IDS alert correlation. In A. Wespi, G. Vigna, and L. Deri (Eds.), *Recent Advances in Intrusion Detection (RAID 2002)*, Lecture Notes in Computer Science, Volume 2516. Berlin Heidelberg: Springer-Verlag, 115–137.

Mäntyjärvi, J., Lindholm, M., Vildjiounaite, E., Mäkelä, S.-M., and Ailisto, H. 2005. Identifying users of portable devices from gait pattern with accelerometers. In *Proc. Of IEEE International Conference on Acoustics, Speech, and Signal Processing*, Volume 2. 973–976.

Narayanan, A. and Shmatikov, V. 2005. Fast dictionary attacks on passwords using time-space tradeoff. In *CCS '05: Proceedings of the 12th ACM conference on Computer and communications security*. New York, NY, USA: ACM Press, 364–372.

Ning, P., Cui, Y., and Reeves, D. S. 2002a. Analyzing intensive intrusion alerts via correlation. In A. Wespi, G. Vigna, and L. Deri (Eds.), *Recent Advances in*

Intrusion Detection (RAID 2002), Lecture Notes in Computer Science, Volume 2516. Berlin Heidelberg: Springer-Verlag, 74–94.

Ning, P., Cui, Y., and Reeves, D. S. 2002b. Constructing attack scenarios through correlation of intrusion alerts. In S. Jajodia, R. Sandhu, and V. Atluri (Eds.), *Proceedings of the 9th ACM conference on Computer and communications security*. New York, NY, USA: ACM Press, 245–254.

NIST FIPS 190 1994. *Guideline for the Use of Advanced Authentication Technology Alternatives*. Springfield, VA: National Institute of Standards and Technology (NIST).

NTT DoCoMo 2006. Docomo to unveil new eight foma "9 series" phones. Press Release Article. Available from http://www.nttdocomo.com/pr/2006/001266.html (read 05.06.2006).

Nunamaker, J., Chen, M., and Purdin, T. D. 1991. Systems development in information systems research. *Journal of Management Information Systems 7*(3), 89–106.

Okamoto, T., Watanabe, T., and Ishida, Y. 2004. Mechanism for generating immunity-based agents that detect masqueraders. In M. G. Negoita, R. J. Howlett, and L. C. Jain (Eds.), *Proceedings of the 8th International Conference on Knowledge-Based Intelligent Information and Engineering Systems (KES 2004), Part II*, Lecture Notes in Computer Science, Volume 3214. Germany: Springer, 534–540.

Oulasvirta, A., Raento, M., and Tiitta, S. 2005. ContextContacts: Re-designing smartphone's contact book to support mobile awareness and collaboration. In M. Tscheligi, R. Bernhaupt, and K. Mihalic (Eds.), *Proceedings of the 7th International Conference on Human Computer Interaction with Mobile Devices and Services, MOBILEHCI'05*. New York: ACM Press, 167–174.

Pearson, F. and Weiner, N. 1985. Toward an integration of criminological theories. *Journal of Criminal Law and Criminology 76*(Winter), 116–150.

Phillips, P., Martin, A., Wilson, C., and Przybocki, M. 2000. An introduction evaluating biometric systems. *IEEE Computer 33*(2), 56–63.

Phua, C., Lee, V., Smith, K., and Gayler, R. 2005. A comprehensive survey of data mining-based fraud detection research. *Submitted to Artificial Intelligence Review*, available from http://www.bsys.monash.edu.au/people/cphua/ (read 9.11.2006).

Pietraszek, T. 2004. Using adaptive alert classification to reduce false positives in intrusion detection. In E. Jonsson, A. Valdes, and M. Almgren (Eds.), *Proceedings of the 7th International Symposium on Recent Advances in Intrusion Detection (RAID 2004)*, Lecture Notes in Computer Science, Volume 3224. Germany: Springer, 102–124.

Pinkas, B. and Sander, T. 2002. Securing passwords against dictionary attacks. In S. Jajodia, R. Sandhu, and V. Atluri (Eds.), *Proceedings of the 9th ACM conference on Computer and communications security*. New York, NY, USA: ACM Press, 161–170.

Pointsec Mobile Technologies 2003. *Stolen PDAs provide open door to corporate networks*. Pointsec News Letter 3, Available from http://www.pointsec.com/news/mediakit/ (read 09.02.2006).

Pointsec Mobile Technologies 2004. *Half of All Corporate PDAs Unprotected Despite Employer Risk*. Pointsec News Letter 2, Available from http://www.pointsec.com/news/mediakit/ (read 09.02.2006).

Pointsec Mobile Technologies 2005a. *Confidential Data Gets Taken for a Ride*. Pointsec News Letter 1, Available from http://www.pointsec.com/news/mediakit/ (read 09.02.2006).

Pointsec Mobile Technologies 2005b. *IT Professionals Turn Blind Eye to Mobile Security as Survey Reveals Sloppy Handheld Habits*. Pointsec news releases, Available from http://www.pointsec.com/news/release.cfm?PressId=108 (read 09.02.2006).

Porras, P. A., Fong, M. W., and Valdes, A. 2002. A mission-impact-based approach to INFOSEC alarm correlation. In A. Wespi, G. Vigna, and L. Deri (Eds.), *Recent Advances in Intrusion Detection (RAID 2002)*, Lecture Notes in Computer Science, 2516. Berlin Heidelberg: Springer-Verlag, 95–114.

Porras, P. A. and Neumann, P. G. 1997. EMERALD: event monitoring enabling responses to anomalous live disturbances. In *Proc. 20th NIST-NCSC National Information Systems Security Conference*. 353–365.

Raento, M., Oulasvirta, A., Petit, R., and Toivonen, H. 2005. ContextPhone, a prototyping platform for context-aware mobile applications. *IEEE Pervasive Computing 4*(2), 51–59.

Ray, I. and Poolsapassit, N. 2005. Using attack trees to identify malicious attacks from authorized insiders. In S. de Capitani di Vimercati, P. Syverson, and D. Gollmann (Eds.), *Proceedings of ESORICS 2005*, Lecture Notes in Computer Science, Volume 3679. Germany: Springer-Verlag, 231–246.

Riha, Z. and Matyas, V. 2000. *Biometric Authentication Systems*. FI MU Report Series FIMU-RS-2000-08, Brno, Czech Republic: Masaryk University.

Ross, A. and Jain, A. 2003. Information fusion in biometrics. *Pattern Recognition Letters 24*(13), 2115–2125.

Royce, J. R. and Powell, A. 1983. *Theory of personality and individual differences: factors, systems and processes*. Englewood Cliffs, NJ: Prentice Hall.

RSA Security Inc. 2004. RSA SecurID Authentication. Available from http://www.rsasecurity.com/products/securid/ (read 07.06.2004).

Ryan, J., Lin, M.-J., and Miikkulainen, R. 1998. Intrusion detection with neural networks. In M. I. Jordan, M. J. Kearns, and S. A. Solla (Eds.), *Advances in Neural Information Processing Systems*. Cambridge, MA, USA: The MIT Press, 943–949.

Samfat, D. and Molva, R. 1997. IDAMN: An intrusion detection architecture for mobile networks. *IEEE Journal on Selected Areas in Communications 15*(7), 1373–1380.

Sanderson, C. and Paliwal, K. K. 2004. Identity verification using speech and face information. *Digital Signal Processing 14*, 449–480.

Schonlau, M., DuMouchel, W., Ju, W., Karr, A., Theus, M., and Vardi, Y. 2001. Computer intrusion: Detecting masquerades. *Statistical Science 16*(1), 58–74.

Schonlau, M. and Theus, M. 2000. Detecting masquerades in intrusion detection based on unpopular commands. *Information Processing Letters 76*(1-2), 33–38.

Sekar, R., Gupta, A., Frullo, J., Shanbhag, T., Tiwari, A., Yang, H., and Zhou, S. 2002. Specification-based anomaly detection: a new approach for detecting network intrusions. In S. Jajodia, R. Sandhu, and V. Atluri (Eds.), *Proceedings of the 9th ACM conference on Computer and communications security*. New York, NY, USA: ACM Press, 265–274.

Seleznyov, A. 2002. *An Anomaly Intrusion Detection System Based on Intelligent User Recognition*. Department of computer Science and Information Systems, University of Jyväskylä, Finland, Ph.D. thesis.

Sequeira, K. and Zaki, M. 2002. ADMIT: anomaly-based data mining for intrusions. In D. Hand, D. Keim, and R. Ng (Eds.), *Proceedings of the eighth ACM SIGKDD international conference on Knowledge discovery and data mining*. Edmonton, Alberta, Canada: ACM Press, 386–395.

Shavlik, J. and Shavlik, M. 2004. Selection, combination, and evaluation of effective software sensors for detecting abnormal computer usage. In R. Kohavi, J. Gehrke, W. DuMouchel, and J. Ghosh (Eds.), *Proceedings of the 2004 ACM SIGKDD international conference on Knowledge discovery and data mining*. New York: ACM Press, 276–285.

Siponen, M. T. 2000. Critical analysis of different approaches to minimizing user-related faults in information systems security: implications for research and practice. *Information Management & Computer Security 8*(5), 197–209.

Skoudis, E. and Poor, M. 2005. On the line. *Information Security magazine*. Available online from http://www.toplayer.com/pdf/IS_110105.pdf (read 05.06.2006).

Snelick, R., Uludag, U., Mink, A., Indovina, M., and Jain, A. 2005. Large-scale evaluation of multimodal biometric authentication using state-of-the-art systems. *IEEE Transactions on Pattern Analysis and Machine Intelligence 27*(3), 450–455.

Stephenson, P. 2000. Intrusion management: A top level model for securing information assets in an enterprise environment. In U. E. Gattiker (Ed.), *EICAR 2000 Best Paper Proceedings*. New Orleans, LA: EICAR, 287–298.

Stoneburner, G. 2001. *Underlying Technical Models for Information Technology Security*. NIST Special Publication MD 20899-8930, Gaithersburg: National Institute of Standards and Technology.

Straub, D. W. and Welke, R. J. 1998. Coping with systems risk: Security planning models for management decision making. *MIS Quarterly 22*(4), 441–469.

Summers, W. C. and Bosworth, E. 2004. Password policy: the good, the bad, and the ugly. In *Proceedings of the winter international symposium on Information and communication technologies*. Dublin: Trinity College, 1–6.

Sun, B., Yu, F., Wu, K., Xiao, Y., and Leung, V. C. M. 2006. Enhancing security using mobility-based anomaly detection in cellular mobile networks. *IEEE Transactions on Vehicular Technology 55*(3), 1385–1396.

Sundaram, A. 1996. An introduction to intrusion detection. *ACM Crossroads 2*(4), 3–7.

Taniguchi, M., Haft, M., Hollmen, J., and Tresp, V. 1998. Fraud detection in communications networks using neural and probabilistic methods. In *Proceedings of the 1998 IEEE International Conference in Acoustics, Speech and Signal Processing (ICASSP'98)*, Volume 2. USA: Omnipress, 1241–1244.

Tax, D. 2001. *One-class classification*. Delft University of Technology, Ph.D. thesis.

Tax, D. M. J. and Duin, R. P. W. 2001. Combining one-class classifiers. In J. Kittler and F. Roli (Eds.), *Proceedings of MCS 2001, Multiple Classifier Systems, Second International Workshop*, Lecture Notes in Computer Science, 2096. Berlin Heidelberg: Springer-Verlag, 299–308.

Thalheim, L., Krissler, J., and Ziegler, P.-M. 2002. Body check: Biometrics defeated. Reprinted with permission from c't Magazine, translated from the German by Robert W. Smith. Available from http://www.extremetech.com/article/0,3396,s=1024&a=27687,00.asp; see also http://www.heise.de/ct/english/02/11/114/ (read 05.06.2006).

Valdes, A. and Skinner, K. 2000. Adaptive, model-based monitoring for cyber attack detection. In H. Debar, L. Me, and F. Wu (Eds.), *Recent Advances in Intrusion Detection (RAID 2000)*, Lecture Notes in Computer Science, 1907. Berlin Heidelberg: Springer-Verlag, 80–92.

Valdes, A. and Skinner, K. 2001. Probabilistic alert correlation. In W. Lee, L. Me, and A. Wespi (Eds.), *Recent Advances in Intrusion Detection (RAID 2001)*, Lecture Notes in Computer Science, 2212. Berlin Heidelberg: Springer-Verlag, 54–68.

Valeur, F., Vigna, G., Kruegel, C., and Kemmerer, R. 2004. Comprehensive approach to intrusion detection alert correlation. *IEEE Transactions on Dependable and Secure Computing 1*(3), 146–169.

Verlinde, P., Chollet, G., and Acheroy, M. 2000. Multi-modal identity verification using expert fusion. *Information Fusion 1*(1), 17–33.

Wallace, W. L. 1969. *Sociological theory*. Chicago: Aldine.

Wang, K. and Stolfo, S. J. 2003. One class training for masquerade detection. In *ICDM Workshop on Data Mining for Computer Security (DMSEC)*. Available from http://www.cs.fit.edu/~pkc/dmsec03/dmsec03notes.pdf (read 20.10.2005).

Wang, L., Liu, A., and Jajodia, S. 2005. An efficient and unified approach to correlating, hypothesizing, and predicting intrusion alerts. In S. de Capitani di Vimercati, P. Syverson, and D. Gollmann (Eds.), *Proceedings of ESORICS*

2005: 10th European Symposium on Research in Computer Security, Lecture Notes in Computer Science, Volume 3679. Berlin Heidelberg: Springer, 247–266.

Weinshall, D. and Kirkpatrick, S. 2004. Passwords you'll never forget, but can't recall. In E. Dykstra-Erickson and M. Tscheligi (Eds.), *Extended abstracts of the 2004 conference on Human factors and computing systems*. New York, NY, USA: ACM Press, 1399–1402.

Weinstein, L. 2006. Fake id: batteries not included. *Commun. ACM 49*(4), 120.

Wickham, T. 2003. *Intrusion Detection Is Dead. Long Live Intrusion Prevention!* Computer security white papers, available from http://www.sans.org/reading_room/whitepapers/detection/ (read 9.11.2006): SANS InfoSec Reading Room.

Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A., and Memon, N. 2005. Authentication using graphical passwords: effects of tolerance and image choice. In *SOUPS '05: Proceedings of the 2005 Symposium on Usable Privacy and Security*. New York, NY, USA: ACM Press, 1–12.

Williams, J. M. 2002. Biometrics or ... biohazards? In C. Serban, C. Marceau, and S. Foley (Eds.), *NSPW '02: Proceedings of the 2002 workshop on New security paradigms*. New York, NY, USA: ACM Press, 97–107.

Witten, I. H. and Frank, E. 2000. *Data Mining: Practical Machine Learning Tools and Techniques*. Morgan Kaufmann Publishers.

Wolpert, D. H. 1992. Stacked generalization. *Neural Networks 5*(2), 241–259.

Xu, D. and Ning, P. 2004. Alert correlation through triggering events and common resources. In *ACSAC '04: Proceedings of the 20th Annual Computer Security Applications Conference (ACSAC'04)*. Washington, DC, USA: IEEE Computer Society, 360–369.

Xu, L., Krzyzak, A., and Suen, C. Y. 1992. Methods for combining multiple classifiers and their applications to handwriting recognition. *IEEE Transactions on Systems, Man, and Cybernetics 22*(3), 418–435.

Yamanishi, K., ichi Takeuchi, J., and Maruyama, Y. 2005. Data mining for security. *NEC Journal of Advanced Technology 2*(1), 63–69.

Ye, N. and Chen, Q. 2001. An anomaly detection technique based on a chi-square statistic for detecting intrusions into information systems. *Quality and Reliability Engineering International 17*(2), 105–112.

Ye, N., Emran, S. M., Chen, Q., and Vilbert, S. 2002. Multivariate statistical analysis of audit trails for host-based intrusion detection. *IEEE Transactions on Computers 51*(7), 810–820.

Yeung, D.-Y. and Ding, Y. 2003. Host-based intrusion detection using dynamic and static behavioral models. *Pattern Recognition 36*(1), 229–243.

Yom-Tov, E. 2004. An introduction to pattern classification. In O. Bousquet, U. von Luxburg, and G. Rätsch (Eds.), *Advanced Lectures on Machine Learning*, Lecture Notes in Computer Science, Volume 3176. Heidelberg: Springer Berlin, 1–20.

Zhang, Y. and Lee, W. 2000. Intrusion detection in wireless ad-hoc networks. In R. Pickholtz and S. K. Das (Eds.), *The Sixth Annual International Conference on Mobile Computing and Networking (MobiCom'2000)*. New York: ACM Press, 275–283.

Zhang, Y. and Lee, W. 2003. Intrusion detection techniques for mobile wireless networks. *Wireless Networks 9*(5), 545–556.