Physical Weaponization of a Smartphone by a Third Party

Juhani Rauhala

University of Jyväskylä, jussi@ieee.org

Abstract In the literature and media, the treatment of the dangers and exposures posed by smartphones has generally focused on information security or privacy concerns. There have also been reports of fires, explosions, electric shocks, or loss of phone functionality due to faulty design or manufacture. This article provides an overview of acute physical and physiological dangers of smartphones that can be induced or triggered by a third party. It proposes a categorical discussion framework to describe and define the dangers in terms of attack vectors, effects on the smartphone, harms, and potential culprits/instigators. Counterfeit smartphones are themselves a significant potential threat in this context. Finally, some possible solutions and mitigation are suggested as preventive measures. Some templates for threat assessment forms are also proposed.

Keywords: technology acceptance, smartphone dangers, technology abuse, unorthodox weaponization

1 Introduction

It may soon be possible to remotely "self-destruct" a smartphone (Hsu, 2017). Previous reports have shown that ISPs and mobile operators may soon be able to disable smartphones remotely (FoxNews, 2012). Smartphone self-destruction differs from remote disablement in that consumers are not only able to disable their device (similar to PIN locking) but also destroy device data and even components at the hardware level (Hughes, 2017). Self-destruction would make the device unusable for a thief, even if a sophisticated thief could override a disabled state to reactivate the device. User data cannot be physically restored.

A common signal-initiated (or software-based) disablement that can be activated by a user or operator is different from self-destruction. With software-based disabling, a smartphone's memory cards and chips remain intact, so data may be recoverable. In the self-destruction method described in Hughes (2017), the system data

or hardware of the device would be destroyed, making reactivation, data recovery, and use of the device impossible.

The problems and threats related to malicious software and hardware hacking are well known in the cybersecurity community. Connected devices such as computers and even automobiles have been hacked remotely. Such hacking has been done for eavesdropping, remote control of functions, or other purposes. Smartphone cameras and microphones have been activated remotely, and recent WikiLeaks revelations show that remote hacking is possible, at least on Android and iPhone devices (WikiLeaks, 2017a). It was revealed that it is possible for an intelligence agency to override smartphone firmware in the supply chain (Durden, 2017). Android and Apple smartphones have also been subject to malware attacks by actors such as individual hackers who are not affiliated with any government (Brewster, 2015; Eadicicco, 2017). In addition, there are software methods that allow complete remote control of some iPhone and Android phones by a third party (Pagliery, 2015; Wikileaks, 2017a).

This chapter deals with hypothetical actions that are intended to impact the owner of a given smartphone, or more precisely, the primary user (either as an actual or misidentified target, either by design or coincidence). The use of the smartphone by the primary user is assumed to be typical, i.e., users use their devices in ordinary ways. The literature seems to lack an overview of potential third-party induced acute direct manipulations of smartphone hardware that result in physical or psychological threats and dangers. Our intention is to draw attention to the issue, *hoping* that such attention will catalyze preventive and mitigating measures by stakeholders. We attempt to present a discussion framework outlined by a profile of potential threats. Profiling is done by characterizing potential threat vectors, potential third-party actors or culprits, and estimated consequences for the user.

In this work, we do not address certain non-physical dangers posed by weaponized smartphones, such as fraud, privacy threats, security threats, financial loss, or identity theft. Nor do we deal with the weaponization of information, such as an attack on a user by software, messages, or signaling designed to manipulate the user. The misuse of smartphones to trigger the detonation of externally connected explosives (e.g., a roadside bomb to which the phone is connected) is also excluded. We do not treat the abuse of smartphones as blunt force instruments or projectiles. We do not deal with technical details.

The terms “smartphone”, “phone” and “device” are used interchangeably.

2 Remote Destruction of the Smartphone

Researchers have developed a method to remotely trigger the destruction of a smartphone by directing power from the smartphone battery to heat and expand the phone material. The material expands to physically destroy some critical hardware, rendering device data physically unrecoverable and the phone useless (Hughes, 2017). While the remote destruction capability of a smartphone is legal and useful

under the intended use scenario, it may lead to more severe and damaging results that can extend far beyond the small integrated circuits and components of the target device. Every smartphone has a battery, a lithium cell, designed to store enough energy to run the device for as long as possible. With the development of battery technology, it has been possible to design and manufacture more efficient batteries. Lithium-ion batteries commonly used in smartphones have a very high energy density (CEI, 2021) and are around 90% efficient (Xiong, 2019). A typical smartphone battery contains about 5 Wh of energy, which is equivalent to 18,000–20,000 J. Utilizing information from Herskowitch (1963) and Wikipedia (2020), this can be calculated to be roughly equivalent to the energy of five grams of TNT or about two M-80 firecrackers (Fig. 1).

Fig. 1. M-80 firecracker (Wikipedia, 2020)

These small and efficient batteries are not always harmless. Problems with the design or manufacture of the battery can cause malfunctions that result in fires or explosions. Some battery issues can be caused by smartphone design, user operations, or software errors. Explosions in a smartphone battery have been sufficient to cause a short-term shock, injury, or fire (Brown, 2013; Kerr, 2013). In cases where the user does not suffer physical harm, many users consider the loss of a smartphone alone to cause almost as much stress as the threat of terrorism (PhySoc, 2017).

A smartphone is typically owned and used by a single individual. Most people carry their smartphones with them or keep them close all day. Once a person and their smartphone are identified, it is reasonably sure that most of the day the person will carry the smartphone with them, the person will handle it, or it will be close to them. It is conceivable that techniques similar to those described by Hughes (2017) (which trigger a rapid rise in the internal temperature of the device with battery electrodes) could be applied to rapidly cause an uncontrolled thermal reaction of the battery. This in turn can result in a fire or explosion. Thus, it may be possible for a remote hacker to attack a device, causing physical harm to the user. For example, unauthorized tampering with the device firmware or operating system can cause a

fire in the device or an explosion of the battery. Hacking could also cause the device to malfunction, which drains the battery very quickly. Indeed, there are smartphone apps freely available that are designed to cause rapid but safe battery discharge (Kushwaha, 2020).

High ambient temperature is one factor known to cause battery fires (Chen & Goode, 2016). Overcharging, abnormally rapid discharge, or short circuiting can cause the smartphone components to overheat, heating the battery, which in turn can cause an explosion or fire. Alternatively, firmware hacking can result in activity that could cause the battery to explode or catch fire. Explosive destruction of the phone battery can even result in the death of the user, see Fig. 2 (Beschizza, 2007; India, 2019; DailyMail, 2009; Prabhu, 2018; Stewart, 2019; Zamfir, 2018). At least one death has been reported due to electric shock when the phone was connected to a charger (Azman, 2019). It should be noted that some of the reported deaths or injuries due to smartphone explosions appear to be hoaxes (Ram, 2014; Yarow, 2010).

Fig. 2. This explosion caused a user's death (CEN, 2018)

Battery-powered devices that are frequently used with smartphones may also pose threats. Smartphone accessories, such as headphones, are known to overheat or explode, causing burns to the user's face, see Fig. 3 (FoxNews, 2016; Olding, 2017). Even if smartphone batteries are designed to withstand hacking (e.g., with robust short-circuit protection), hacking into any of the user's battery-powered accessories can still pose a danger. Such accessories can be wireless headphones (Olding, 2017) or a Bluetooth earpiece that is used very close to the ear. Bluetooth speakers are also known to burst into flames (Strahan & Novini, 2017).

Fig. 3. Battery-operated headphones exploded while the passenger was listening to music (ATSB, 2017)

Hackers or culprits who produce and distribute malware or commit cyberattacks can be individuals or organizations. Recent WikiLeaks documents have revealed the extensive hacking capabilities of a national intelligence agency (WikiLeaks, 2017a). Hacking against smart TVs was developed in cooperation with intelligence agencies in different nations (Wikileaks, 2017b). Some governments around the world are certainly able to develop and implement such hacking or install backdoor capabilities on after-market devices. This ability could give powerful bad actors a personal level "kill switch" to an affected smartphone or accessory. The device could be disabled or destroyed by causing a fire or explosion in the battery. Bad actors could also develop a program or hack that causes the device to emit radiofrequency (RF) radiation at high levels. If the user becomes aware of such an attack, they may feel psychological distress. The distress would depend on their concern about possible radiation exposure and where they usually keep the device relative to their body.

3 Categorical Framework for Smartphone Dangers

Various threat modeling techniques and frameworks exist, but many of them are intended to model threats to large organizations or other high-stakes targets. Examples of such models are listed by Shevchenko (2018). Some of these techniques can be applied, perhaps in awkward ways, to model the threats to individual smartphone users. Based on the author's literature review, there are currently no threat modeling techniques designed to model the specific threats that this chapter focuses on.

3.1 Characteristics of Attack Effect

To assess the potential harm caused by a third-party, we propose the following parameters to facilitate categorization, discussion, and thus understanding:

- Acute vs. chronic,
- Sudden vs. long-term,
- Obvious/salient vs. hidden/obscured,
- Catastrophic vs. undetectable:,
- Maintained functionality vs. compromised functionality vs. eliminated functionality.

Is the effect sudden or long-term? This applies to the first two parameters. For example, a battery explosion will have sudden consequences while increased radio frequency emissions will have a long-term effect. The effect is obvious to the user, for example, when the phone overheats or ignites. An example of a non-obvious effect would be intensified radio frequency emissions. The catastrophic effect significantly impairs the functionality of the smartphone and threatens the user's well-being. Otherwise, the user will not detect any inconvenience or danger during normal use.

An example of the effect of maintaining functionality (excluding battery life) is the increase in radio frequency emissions. Compromised functionality is a scenario in which some functions, such as an Internet connection or a camera/gallery or other function, are forced off, but other important functions, such as the ability to make a call, remain. Eliminated functionality means a case where the smartphone is completely disabled or “bricked.”

3.2 Attack Vectors

Different attack vectors can be used to carry out a smartphone attack:

- Implanted software,
- Voluntarily downloaded software,
- Hijacked default or hijacked downloaded software,
- Implanted firmware,
- Update with malicious firmware,
- Rogue or fake cell towers,
- Using a counterfeit smartphone.

Implanted software is malware or other software that is designed to cause a particular effect through an embedded payload. Voluntarily downloaded software is malware that a user has intentionally downloaded from the Internet. Hijacked default or hijacked downloaded software is firmware or apparently legitimate software that has been infected with a payload of malware. Implanted firmware is firmware that has malware embedded on it when it comes from the factory. Update with malicious firmware occurs when a user updates his/her device with malware-embedded firmware. The user has obtained it from a malicious website or elsewhere.

Rogue or fake cell towers spoof an authentic operator tower. This vector enables communication monitoring of connected devices and the sending of spoofed text

messages to these devices (Leiva-Gomez, 2014). Thus, it is possible to organize SMS-based hacking from a fake tower to the victim, such as receiving an image as a text message as described by Pagliery (2015). When using a counterfeit smartphone, the user is using an unauthorized copy of the branded smartphone product. The device manufacturer has not been authorized to manufacture this device and may not be known.

3.3 Attack Perpetrators

The culprit/perpetrator/source of the attack may be

- Single hacker,
- Hacker group,
- Nation state actor,
- Private company,
- Criminal gang/organization.

The perpetrator of an attack may be an individual using one of the attack vectors. In the case of a group of hackers, the attack is carried out in cooperation by several hackers. A national state actor is any entity with the resources and operational support of a national government. A private company refers to a criminal company or part of a private company that makes an attack. A criminal gang/organization is an organized criminal group that carries out an attack, perhaps as part of a turf war or through proxies.

3.4 Weaponizable Components

A weaponizable component can be one of the following:

- RF transmitter,
- Battery,
- User interface (UI) function.

An RF transmitter is a (radio frequency) hardware module that could transmit electromagnetic signals abnormally. The battery inside the smartphone may be damaged. The interactive UI components of the device may start to malfunction.

3.5 Attack Effects

Effects of an attack on a smartphone can be

- Device heating/overheating,
- Battery swelling,
- Battery fire,
- Battery explosion,
- Excessive abnormal radiation from the device,
- Disabling the device,
- Destruction of the device.

As a result of the attack, the device may become hot or overheated. The battery generates enough heat to cause injury to the user and damage the smartphone. Swelling of the battery will damage the operation of the smartphone due to physical damage to the device. When a battery catches fire, it causes (typically) a hot and rapid fire in the smartphone. Explosive energy from the battery can cause injury to the user but may not necessarily destroy data on the device or its functions.

An attack may cause excessive abnormal radiation from the device. In this case, the device's RF modules and antennas emit abnormally high levels of electromagnetic radiation. This can cause the battery to discharge quickly as well as distress to the user. A direct or indirect (timed or user-triggered) disablement of the device by a remote/third party will cause some or all of the device's functions to stop. The functions that are disabled may be critical for a particular user. The remote/third party may cause the device to be destroyed so that no operations can be performed and all data is destroyed. This could be accomplished by a battery explosion or by less visible means, e.g., expansion of a polymer layer that destroys essential components, as described by Hughes (2017).

The harm caused to the user by an attack can be physical. For example, the user suffers from a burn or physiological shock. Psychological consequences can include distress, anxiety, or emotional shock.

In addition to the acute effects, the realization of an attack may have significant secondary effects. Consider a passenger flight. Nearly every passenger carries a battery-powered device. If the battery of the passenger’s device burns or explodes during a flight, the flight may be disrupted. Secondary social impacts may include decreased user confidence in smartphone technology and willingness to use smartphones. Some people who have learned of the incident, and especially its victims and witnesses, may become reluctant to fly.

A hypothetical assessment of weaponizable smartphone components can be found in Table 1 in the Appendix. Using Tables 2, 3, and 4 in the Appendix, a researcher or threat analyst can cross-reference the above parameters against each other to analyze threats. The cells in the tables can be filled with a suitable scale parameter, such as a number ranging from zero to ten. For example, 0 means no threat is detected, and 10 means that the combination has a certain or current manifestation. The tables can also be applied to the analysis of other types of threat scenarios.

4 Nation State as a Bad Actor

Advances in technology have made it possible for various entities to abuse technology. Such entities include nation-states with significant sovereign authority and access to substantial resources. Because of the scale of the influence of nation states, the potential abuse of technology by them is a threat to human rights. Determination and awareness of the threats of abuse often follow mass adaption to new technology.

WikiLeaks' Vault 7 revelations have revealed state-sponsored hacking and malware used on smartphones. NightSkies 1.2, designed to enable complete remote control and management of iPhones, has apparently been implanted in devices during the product supply chain (Durden, 2017). With RoidRage software, a third party can monitor the device's RF functions and SMS messages (Paganini, 2017). The Vault 7 revelations were released in 2008 and comprised only 1% of the leaks (Wikileaks, 2017c). Thus, there is no doubt that more sophisticated hijacking and surveillance tools exist today.

Apps such as TikTok and at least one private technology company that manufactures smartphones have been accused of being channels for international espionage (Kaska et al., 2019; Ryan et al., 2020). The benefits and risks of remotely activated self-destruction of a smartphone should be thoroughly considered for possible abuse. The damaging effects of unethical or illegal hacking on a smartphone battery could be prevented by physical protection measures during design and manufacture. However, manufacturers of counterfeit smartphones, batteries, and accessories may not implement all of the safety features of copied products.

5 Counterfeit Smartphones

Arguably, one of the most significant risk factors for the threats described in this chapter is the widespread availability of counterfeit smartphones. The counterfeit electronics industry as a whole is in the order of US$100 billion and it is estimated that 10% of the world's electronics are counterfeit (Spiegel, 2009). Counterfeit smartphones are relatively cheap to buy, widely available online, and compose a US$48 billion market (Gilchrist, 2017). Authorities have fought against such trafficking (HK-CED, 2018; US-CBP, 2019). A carefully manufactured counterfeit smartphone may appear nearly identical to authentic ones (Evans, 2019). Thus, some consumers may not be able to distinguish counterfeit smartphones. Consumers may also knowingly use a counterfeit without much concern for the risks involved. A study by Liao and Hsieh (2013) found that consumers agreed with the perceived risks of buying counterfeit (or "grey-market") smartphones. However, they only slightly disagreed with the idea or intention of purchasing them: the mean user response was 2.78 on the Likert scale (from 1 = strongly disagree to 5 = strongly agree).

It can be extremely difficult for a consumer to discover or begin to suspect hidden functionalities or backdoors that can be designed for any smartphone. Counterfeit smartphones pose additional risks (Evans, 2019). Detecting malicious or exploitable features that can be embedded in tiny integrated circuits used in smartphones can require considerable technical expertise and expensive sophisticated equipment. At the technology level, counteracting the use of counterfeit smartphones, batteries, and accessories can be difficult. It requires a great deal of involvement from the original manufacturers. One measure to prevent the use of counterfeit batteries has required advanced cryptographic security-based technology (Bush, 2014). Counterfeit devices are often designed and manufactured in areas where government quality control, regulations, and policies are questionable.

In addition to counterfeit smartphones, counterfeit batteries and chargers are widely available. The varying quality of these devices poses its own danger (Best, 2017). With modern technology, it is possible to embed concealed electronics or functionality in a counterfeit product housing, including smartphone accessories. As the Vault 7 revelations suggest, very sophisticated concealed functionality can be embedded in legal and authentic devices. Hidden functionalities could also be embedded in authentic batteries or accessories. One possible scenario is a counterfeit battery installed in an authentic smartphone (or an authentic battery in a counterfeit smartphone) that, together with a malware app, can cause unexpected or dangerous damage. In other words, a malware app or firmware could perform as Hsu (2017) suggests but in a malicious way, weaponizing the smartphone by causing an explosive reaction in the battery. Alternatively, the malware app or firmware may act as a malicious variation of the battery drainage app (Kushwaha, 2020), causing a rapid drainage and (assuming the battery has sufficient charge) a significant temperature rise inside the device. This could also pose a danger to the device and the user.

The use of smartphones is very widespread. Globally, about 6.4 billion people use smartphones (O'Dea, 2021). Entities that can control remote connections to such devices generally have, figuratively speaking, the vicinity of each smartphone user in a wireless tether. The vicinity is either the user's pocket, hand, handbag, nightstand and so on.

6 Discussion

When considering a potential threat posed by a remote-weaponized smartphone, the cybersecurity officer should take security measures as appropriate. For example, for high-profile or VIP personnel gatherings or meetings, a protocol can be implemented that requires attendees to hand over their smartphones to a separate and secure location. Alternatively, guests may be asked to remove the batteries from their phones (which is unfortunately impossible on most modern smartphones). Another possible security measure would be to prevent potential wireless signal triggers by creating an RF interference field around the secured area. RF jamming can

also block connections from fake cell towers. During the jamming, smartphones are also rendered incapable of normal wireless communication.

Prevention of the described hypothetical threats can be promoted by advising smartphone users to avoid downloading unknown or unauthorized apps and opening suspicious messages from unknown senders. However, compliance with the advice is not effective against modified firmware embedded in a supply chain or against text message hacking that is activated merely upon delivery. If a bad actor has significant technology resources and expertise at its disposal, threat prevention can be difficult or impossible. Such actors may include a manufacturer of counterfeit phones under the control of a criminal organization or an arm of an authoritarian regime.

Designers could choose materials and configuration models for the smartphone chassis so that the smartphone body would withstand a catastrophic battery fire or explosion. This would provide the user with some protection from injury. This mitigation is problematic in the case of counterfeit phones – not to mention phones specifically designed to be weaponized.

Further research could focus on analyzing suspected counterfeit smartphones and batteries for malicious or dangerous functions. The analyses should include studies of whether such functions are designed or coincidental, whether they are in the smartphone ICs or battery, and whether they are pre-programmed into software or firmware. If a physically harmful function is found, the analyzes should try to determine its triggering mechanisms.

7 Conclusion

The pervasive use of smartphones creates a potentially highly vulnerable target for those malicious parties with sufficient technical means. The technology developed to enable remote-triggered self-destruction of a smartphone could be maliciously abused by a third party to cause catastrophic battery fires and explosions. For the victim, severe heating or explosion of the device can cause distress (about the destruction of the device and the data contained in it and possible thermal damage to property), injury or, at worst, death. The widespread availability of counterfeit devices makes it more difficult to combat such threats. Simply disabling the smartphone can cause significant stress to the victim. A third party guilty of physical weaponization of a smartphone can be any actor, including a nation state-sponsored actor, organization, mafia, company, criminal gang, hacker group, or individual hacker. Regardless of possible culprits, authorities should consider the interests of citizens and fundamental human rights, the role of regulators, and the interests of operators and the high-tech industry when proactively assessing the potential threats and preventive measures.

By no means does the author imply or suggest that any individual or organization was or will be involved as a perpetrator or culprit for any of the hypothetical malicious attack scenarios described. The author is also not aware of any realizations of the attack scenarios that are the focus of this chapter.

References

ATSB (2017). Battery explosion mid-flight prompts passenger warning. Australian Transport Safety Bureau, https://www.atsb.gov.au/media/news-items/2017/battery-explosion-mid-flight/

Azman, K. K. (2019). Man dies of electrocution after his counterfeit phone charger caused an explosion. Says, https://says.com/my/news/man-dies-of-electrocution-after-his-counterfeit-charger-caused-an-explosion

Beschizza, R. (2007). Man killed by exploding cell phone. Wired, https://www.wired.com/2007/07/man-killed-by-e/

Best, S. (2017). Use an iPhone? Check your charger NOW: Study finds 98% of fake Apple power leads risk causing fatal `electric shocks or house fires'. MailOnline, https://www.dailymail.co.uk/sciencetech/article-5155765/98-fake-iPhone-chargers-users-risk-DEATH.html

Brewster, T. (2015). Stagefright: It only takes one text to hack 950 million Android phones. Forbes, https://www.forbes.com/sites/thomasbrewster/2015/07/27/android-text-attacks/

Brown, H. (2013). Student's cell phone battery explodes, starts a fire. CBS Minnesota, http://minnesota.cbslocal.com/2013/02/21/students-cell-phone-battery-explodes-starts-a-fire/

Chen, A., & Goode, L. (2016). The science behind exploding phone batteries. The Verge, http://www.theverge.com/2016/9/8/12841342/why-do-phone-batteries-explode-samsung-galaxy-note-7

CEI (2021). Lithium-ion battery. Clean Energy Institute, University of Washington. https://www.cei.washington.edu/education/science-of-solar/battery-technology/

DailyMail (2009). Man killed after his mobile phone explodes, severing an artery in his neck. Daily Mail, http://www.dailymail.co.uk/news/article-1134838/Man-killed-mobile-phone-explodes-severing-artery-neck.html

Durden, T. (2017). Wikileaks releases "NightSkies 1.2": Proof CIA bugs "factory fresh" iPhones. The Liberty Beacon, https://www.thelibertybeacon.com/wikileaks-releases-nightskies-1-2-proof-cia-bugs-factory-fresh-iphones/

Eadicicco, L. (2017). Watch out for this iPhone-crashing text message. Time, https://time.com/4637574/iphone-crash-text-2017/

Evans, C. (2019). From the depths of counterfeit smartphones. Trail of Bits, https://blog.trailofbits.com/2019/08/07/from-the-depths-of-counterfeit-smartphones/

FoxNews (2012). Wireless providers to disable stolen phones. Fox News, http://www.foxnews.com/politics/2012/04/10/wireless-providers-to-disable-stolen-phones.html

FoxNews (2016). Cell phone battery catches fire aboard Delta Air Lines flight to Atlanta. Fox News, http://www.foxnews.com/travel/2016/09/16/cell-phone-battery-catches-fire-aboard-delta-air-lines-flight-to-atlanta.html

Gilchrist, K. (2017). Fake smartphone sales cost global industry $48 billion. CNBC, https://www.cnbc.com/2017/02/28/fake-smartphone-sales-cost-global-industry-48-billion.html

Herskowitch, J. (1963). The combustion of a granular mixture of potassium perchlorate and aluminum considered as either a deflagration or a detonation. Technical report, 3063. Picatinny Arsenal, Dover, NJ, https://apps.dtic.mil/sti/pdfs/AD0296417.pdf

HK-CED (2018). Hong Kong Customs combats sale of suspected counterfeit smartphones and accessories. Press release, Customs and Excise Department, Government of the Hong Kong

Special Administrative Region of the People's Republic of China, https://www.customs.gov.hk/en/publication_press/press/index_id_2372.html

Hsu, J. (2017). Self-destructing gadgets made not so mission impossible. IEEE Spectrum, https://spectrum.ieee.org/tech-talk/consumer-electronics/gadgets/selfdestructing-gadgets-made-not-so-mission-impossible

Hughes, O. (2017). Mission possible: Self-destructing phones are now a reality. International Business Times, http://www.ibtimes.co.uk/mission-possible-self-destructing-phones-are-now-reality-1605897

India (2019). 22-year-old man dies as mobile phone explodes while charging. India News, https://www.india.com/technology/22-year-old-man-dies-as-mobile-phone-explodes-while-charging-3840866/amp/

Kaska, K., Beckvard, H., & Minárik, T. (2019). Huawei, 5G and China as a security threat. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE).

Kerr, D. (2013). Samsung cell phone battery explodes in man's pocket. CNET, https://www.cnet.com/news/samsung-cell-phone-battery-explodes-in-mans-pocket/

Kushwaha, N. (2020). 6 best free battery drain apps for Android. List Of Freeware. https://listoffreeware.com/free-battery-drain-apps-for-android/

Leiva-Gomez, M. (2014). Everything you need to know about fake cell towers. Make Tech Easier, https://www.maketecheasier.com/fake-cell-towers/

Liao, C.-H., & Hsieh, I.-Y. (2013). Determinants of consumer's willingness to purchase gray-market smartphones. *Journal of Business Ethics*, 114(3), 409–424. Doi: 10.1007/s10551-012-1358-7.

O'Dea, S. (2021). Number of smartphone users worldwide from 2016 to 2026 (in billions). Statista. https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

Olding, R. (2017). Safety warning after passenger's headphones explode on Beijing to Melbourne flight. The Sydney Morning Herald, https://www.smh.com.au/technology/safety-warning-after-passengers-headphones-explode-on-beijing-to-melbourne-flight-20170315-guy6va.html

Paganini, P. (2017). WikiLeaks Vault 7 data leak: Another earthquake in the intelligence community. Infosec Resources, https://resources.infosecinstitute.com/topic/wikileaks-vault-7-data-leak-another-earthquake-intelligence-community/

Pagliery, J. (2015). Android phones can be hacked with a simple text. CNN Business. https://money.cnn.com/2015/07/27/technology/android-text-hack/index.html

PhySoc (2017). Stress in modern Britain. The Physiological Society, https://static.physoc.org/app/uploads/2020/02/20131612/Stress-in-modern-Britain.pdf

Prabhu, A. (2018). Cradle Fund CEO killed by smartphone explosion. Gizbot, https://www.gizbot.com/mobile/news/smartphone-explosion-kills-ceo-cradle-fund-051647.html

Ram, S. (2014). This FB post about a boy getting killed due to an exploding phone is a hoax. Says, https://says.com/my/tech/explosion-of-exploding-phone-that-killed-10-year-old-boy-is-a-hoax

Ryan, F., Fritz, A., & Impiombato, D. (2020). TikTok and WeChat: Curating and controlling global information flows. Australian Strategic Policy Institute, https://www.aspi.org.au/report/tiktok-wechat

Shevchenko, N. (2018). Threat modeling: 12 available methods. Carnegie Mellon University, https://insights.sei.cmu.edu/sei_blog/2018/12/threat-modeling-12-available-methods.html

Spiegel, R. (2009). Counterfeit components remains a huge electronics supply chain problem. Engineering Design News, https://www.edn.com/counterfeit-components-remains-a-huge-electronics-supply-chain-problem/

Stewart, W. (2019). Girl, 14, killed in her sleep 'by exploding phone' after going to bed listening to music while device was charging. The Sun. https://www.thesun.co.uk/news/10032279/schoolgirl-14-killed-sleep-exploding-smartphone-listening-music-device-charging/?utm_campaign=sunmainfacebook300919&utm_medium=Social&utm_source=Facebook#comments

Strahan, T. & Novini, R. (2017). Bluetooth speaker starts smoking on bed, bursts into flames. NBC New York, http://www.nbcnewyork.com/news/local/Bluetooth-Speaker-Bursts-into-Flames-Seen-Smoking-on-Bed-Sources-417596643.html

US-CBP (2019). Philadelphia CBP seizes nearly $1 million in counterfeit smartphones from China. United States Customs and Border Protection, https://www.cbp.gov/newsroom/local-media-release/philadelphia-cbp-seizes-nearly-1-million-counterfeit-smartphones-china

WikiLeaks (2017a). Vault 7: CIA hacking tools revealed. WikiLeaks, https://wikileaks.com/ciav7p1/

Wikileaks. (2017b). Weeping angel (extending) engineering notes. In Vault 7: CIA Hacking Tools Revealed. WikiLeaks, https://wikileaks.org/ciav7p1/cms/page_12353643.html

WikiLeaks (2017c). WikiLeaks has released less than 1% of its #Vault7 series in its part one publication yesterday `Year Zero'. Twitter, https://twitter.com/wikileaks/status/839475557721116672

Wikipedia (2020). M-80 (explosive). Wikipedia, Retrieved September 2, 2020, from https://en.wikipedia.org/wiki/M-80_(explosive)

Xiong, S. (2019). A study of the factors that affect lithium ion battery degradation. M.Sc. thesis, University of Missouri-Columbia. https://mospace.umsystem.edu/xmlui/bitstream/handle/10355/73777/Xiong-Shihui-Research.pdf?sequence=1&isAllowed=y

Yarow, J. (2010). The Droid phone that exploded and blew up a guy's ear? It was just dropped, says Motorola source. Business Insider. https://www.businessinsider.com/droid-phone-explosion-motorola-2010-12?international=true&r=US&IR=T

Zamfir, G. (2018). Girl, 18, killed when mobile phone explodes while she is chatting to relative. Mirror, https://www.mirror.co.uk/news/world-news/girl-18-killed-mobile-phone-12215521

Appendix: Threat analysis

Table 1. Threat analysis of third-party induced weaponization of a smartphone, a hypothetical example

Component/module	Potential result	Attack vector / trigger
RF transmitter	Unnecessary exposure to higher than normal levels of RF radiation	Firmware programming (call to certain number, opening of certain website [malicious code in the site, firmware sniffing for opening of the site,…]
	Heating	Firmware trigger for permanent abnormally excessive transmission strength with every activity that requires a transmission.
		Firmware trigger for maximum transmission power during mundane background transmission activity and/or disabling of OLPC (open-loop power control).
Battery	Swelling	Remote activation
	Fire	Firmware programming (Timer, push-button sequence, phone call, download, malicious app [malware, …]
	Explosion	
UI functionality	Stress and distress to users via disabling of partial or all functionality.	Firmware (implanted during manufacture, or malicious update)
		Malware/virus
		Fake cell tower (via malicious or rogue (hacked) base station)
		Physical damage (via “self-destruct” or battery damage hack)
		Rogue operator employee

Table 2. Threat assessment table: Threat vs. potential culprit

		Culprit				
		Hacker	**Nation-state actor(s)**	**Private corporation**	**Criminal gang/organization**	**Hacker group**
Threat	Device emits excessive heat / overheats					
	Battery swelling					
	Battery fire					
	Battery explosion					
	Abnormal RF emissions					
	Remotely induced disablement of device					
	Remotely induced destruction of device					

Table 3. Threat assessment table: Threat vs. potential trigger/attack vector

		Potential trigger/attack vector						
		Implanted software	Voluntarily downloaded software	Hijacked default or hijacked downloaded software	Implanted firmware	Updated with malicious firmware	Rogue or fake cell towers	Using a counterfeit smartphone
Threat	Device emits excessive heat / overheats							
	Battery swelling							
	Battery fire							
	Battery explosion							
	Abnormal RF emissions							
	Remotely induced disablement of device							
	Remotely induced destruction of device							

Table 4. Threat assessment table: Potential trigger/attack vector vs. potential culprit

		Potential culprit				
		Hacker	Nation-state actor(s)	Private corporation	Criminal gang/organization	Hacker group
Potential trigger/attack vector	Implanted software					
	Voluntarily downloaded software					
	Hijacked default or hijacked downloaded software					
	Implanted firmware					
	Updated with malicious firmware					
	Rogue or fake cell towers					
	User is using a counterfeit smartphone					
	User is using a counterfeit battery/accessory					