sustainablySMART

Sustainable Smart Mobile Devices Lifecycles through Advanced Re-design, Reliability, and Re-use and Remanufacturing Technologies

Project Duration: **01/09/2015 - 31/10/2019**

Deliverable No.: **5.2**

Deliverable Title: **Solid state memory data erasure: Guidance**

Version Number: 2.0

Due Date for Deliverable: **31/08/2018**

Actual Submission date: **19/12/2018**

Lead Beneficiary: **Lead Partner**

Lead Author: Juho Pörhönen

Deliverable Type: R

R = Document, report
DEM = Demonstrator, pilot, prototype, plan designs
DEC = Websites, patent filing, press & media actions, videos, etc.

Dissemination Level: PU

PU = Public
CO = Confidential, only for members of the consortium, including the Commission Services

Coordinator contact: Karsten Schischke
Fraunhofer IZM
phone +49.30.46403-156
e-mail schischke@izm.fhg.de

Contributing Partner:

Blancco Technology Group Ltd.

Disclaimer

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 680604

Document version history:

Date:	**Author:**	**Notes:**
31.10.2018	J. Pörhönen	The first draft version.
17.12.2018	J. Pörhönen	The final document version.

Contents

Summary

Presented report is the outcome of sustainablySMART project that is focused on the research and development of technologies to promote the cascade reuse of smartphone and tablet devices on the product and printed circuit board level. The project encompasses a wide-reaching and ambitious program of development that includes: advanced disassembly and remanufacturing technologies; the development of new product design approaches and new re-/de-manufacturing processes; environmental goals to improve the efficient use of components and better material recycling. The project has received funding from the EU through the Horizon 2020 initiative and involves 17 partners across a variety of disciplines.

One fundamental aspect when considering the repurposing of technology is to ensure that data privacy and protection requirements are observed to prevent an unwanted data breach. The reuse of devices with storage components requires a sound process for data sanitization. Moreover, the sanitization process for flash-based memories can be hindered by the added complexity due to data management processes on a device.

Blancco Technology Group is leading the data security aspect of the project with the primary aim of identifying and disseminating the processes required to enable secure disposal or repurposing of memory components. This report aims to provide recommendations for different entities such as recyclers, companies, governmental organizations and individuals on secure end of lifecycle actions for mobile storage technologies. Additionally, the guidance report gives recommendation to the memory OEMs on actions to be taken to facilitate secure storage sanitization. Presented report is intended for those who are not the experts in data security and, therefore, gives a deep overview of mobile and storage technologies, risks and threats of insecure media sanitization as well as present the analysis on various options for data destruction.

SECTION 1: Introduction

1.1 Rationale

Rapid development of mobile phone technologies has revolutionised the concept of phone, redefined consumers' experiences (GSMA, 2015) and made smartphone an integral part of modern life. Radical changes happened for the past 10 years enriched mobile devices with more functionality and superior performance. Mobile industry continues to scale rapidly driven by the increase adoption of smartphones and other connected devices (GSMA, 2015). Mobile is a heart of new digital ecosystem and a major driver of economic progress globally, generating 3.8% of global GDP and estimated to reach 4.2% by 2020 (GSMA, 2015). The capabilities of nowadays phones and tablets generally rivals mid-range desktop computers (Computer Hope, 2018). Moreover, smartphones have already surpassed desktops and laptops not only by functionality, but also by the volume of units shipped reaching the highest year-over-year growth in 2018 (Gartner, 2017). Significant performance improvements have also enabled the extended range of smartphone usage such as bank account management, online payments, social media surfing and business tasks' management. According to the research undertaken by Blancco Technology group, 20% of smartphone users are likely to use their mobile devices exclusively for browsing and shopping and 21% access financial information and make mobile payments (Blancco Technology Group, 2015). Moreover, it has been noted that organisations in the public and private sectors are increasingly using smartphones to store the data related to business operation, employees or customers (Jones, 2008). Consequently, the range of data stored on mobile devices is not any more limited to personal and includes work-related content. This tendency has been supported by becoming increasingly popular Bring Your Own Device (BYOD) policy taken in use by many companies. BYOD allows employees to use their personal devices for work purposes instead of using company-owned devices (French, et al., 2014). Despite of associated security and privacy risks, BYOD usage is gradually growing. According to the research conducted by Tech Pro Research, 74% of respondents are saying that their organization is using or planning to use BYOD (ZDNet, 2015). Besides the mix of personal and business data that can be found on modern smartphones. Introduction of new features and applications increase the amount and diversity of stored information: geo location history, health tracking, IoT connected devices, credentials, browser history (Mahalik, et al., 2016). Additional factor that influenced wide adoption of the smartphones is increasing affordability of devices expressed in diversification of smartphones segments such as low-end to flagship models and related to them broad range of price categories. All these aspects have contributed to smartphones becoming a huge repository of sensitive data.

Another consequence of the smartphone technology improvements is skyrocketing rate at which devices are purchased, used and discarded (Green Aliance, 2015) (Challen, et al., 2014). Thereby, 35% of smartphone users trade, sell or donate their devices every two to three years and 17% do so every year or whenever the new model is released (Blancco Technology Group, 2015). As a result, short product lifecycle and high environmental footprint of smartphone production have negatively affected sustainability index of smartphones and tablets. For instance, the latest Apple iPhone X (64 GB) generates 63.2 kg CO2 per kg of smartphone (Apple, 2017) compared to 6,7 kg CO2 per kg of Citroen C1 (The Guardian, 2010). This high carbon footprint is accumulating after 2 or 3 years as the smartphone reaches end-of-life and even under optimal material recycling conditions only a small fraction can be recovered. Only complete rethinking and redesigning the way smartphones are used and retired will make continuous improvement on the invested resources and emitted greenhouse gases. Consequently, a circular economy approach for smart mobile devices must focus with priority on lifetime extension of products and components. Implementation of circular economy approach aims to shift from linear view, where resources are disposed once they reach end-of life, to closed loop through redesigning the devices and enhancing durability and easier repair, re-use of smartphones, their components and material recovery. The European Commission defines a circular economy as a set of activities in which "the value of products, materials and resources is maintained in the economy for as long as possible and the generation of waste minimised" (European Comission, 2015).

To support green initiative many companies are engaging into take-back and buy-back programmes. Currently smartphones refurbishing, and resale are the most common ways of smartphone lifespan expansion applied in practice. The market perspectives indicate that we only see the beginning of a larger wave of discarded units (Maytom, 2014). According to IDC (IDC, 2016), the growth of second-hand phone market is forecasted to reach 222.6 million units by 2020. One fundamental aspect when considering the reuse of technology such as resell of device or re-purposing of its memory storage is to ensure that data privacy and protection requirements are observed to prevent an unwanted data breach. From customer perspective, data privacy on donated resold or other way disposed asset is significant barrier to recycling and re-use of mobile devices. With getting increasingly popular online commerce, social media, gaming and other activities, consumers are increasingly voicing privacy concerns and demanding better protection of their data (GSMA, 2015). Moreover, non-sanitized or improperly sanitised storage media has a high risk to be a subject of a data acquisition attack that could be performed by different parties with various motivation, technical capabilities and funding. These threats are interested in unauthorised access to user data from smartphone device. Successful data acquisition attack can lead to data breach and various unpleasant legal and financial consequences. Data security is also an integral part of EU GDPR legislation introducing the "right to be forgotten" and mandating the organizations handling the data of EU citizens to "erase personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data" (EU GDPR, 2016). Therefore, the

reuse of devices with storage components requires a sound process for data sanitization. Presented secure data sanitization guidance aims eliminate this barrier and increase user awareness about data security and privacy as well as provide the recommendations to secure device disposal.

1.2 Scope and focus of research

The market for mobile communications technologies is characterized by a large and constantly growing number of smartphones, a diversity of different platforms and an array of different technologies underpinning the hardware used in a device. Among many factors contributing to the growth of the smartphone market, the key one is large number of smartphone manufacturers, providing a greater variety of devices more tailored to local needs and preferences (GSMA, 2016). Factoring in these permutations means adjusting the scope of research activities appropriately, as testing every model on the market today is simply not feasible. Therefore, the carried-out work is focused on two key facets of a mobile device:

1. The memory storage technology used to store data in smartphones

   The way in which data is handled and erased from the physical storage medium is a key concern for data sanitization.

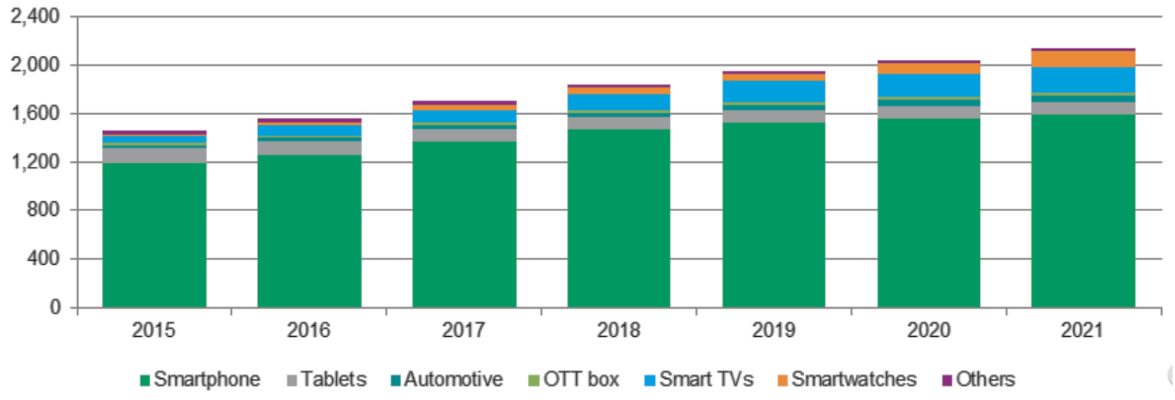
2. Platform/operating system deployed on a device.

   The operating system provides the layer of abstraction between the user and the data stored on the medium and is, therefore, of critical importance.

Smartphone Storage Technologies

Undertaken research has identified that the primary memory storage technology used in most modern smartphones is eMMC, which stands for embedded Multi Media Card. eMMC combines a NAND flash memory chip and an integrated controller in a single package. This technology is quite mature in nature and has historically had a high rate of adoption. eMMC has been by far the dominant technology used in smartphones to date due to satisfactory performance and low-price characteristics, and it has saturated the market. Therefore, the major share of the smartphone devices in circulation today use eMMC to store data. Its key benefits include low energy consumption, small size factor and most importantly low cost. Due to advances in many areas of smartphone technology, the storage used in devices (particularly for flagship smartphones) must adapt to keep pace with the demands of increased speed and storage capacity. Nonetheless, eMMC is projected to continue to be widely utilized in low-end smartphones in the coming years, as the technology goes up in the value chain resulting in decreasing prices and improved performance and functionality. Referenced chart is showing eMMC deployment - presence in smartphones

Figure 1: eMMC deployment in smartphones (IHS Markit, 2017).



Universal Flash Storage (UFS) is a recently developed specification for flash storage posited for consumer electronic devices. With higher speed, command queuing and other functionality, this is currently considered as a direct replacement for eMMC inside smartphones and, since it is still expensive in comparison, is mainly used for high-end devices. However, the constant enhancements in areas such as photo and video quality, gaming and internet use are raising the requirements for smartphone storage, creating a greater demand for UFS and, potentially, a wider spread across devices.

Considering the above, the primary focus of the research will be on eMMC storage due to its availability, maturity, continued and presence in the majority of devices. Since both eMMC and UFS deploy the use of flash as the actual physical storage medium, the findings from researching eMMC will likely apply to UFS.

Smartphone Operating Systems

There is a vast array of hardware technologies found in smartphones and a high number of associated OEMs packaging and deploying these into commercial products. However, not every smartphone OEM internally develops its own Operating System to provide fundamental functionality on a device. The list below details the most commonly used/known mobile Operating Systems during the last few years, the company behind the OS and whether they are open or closed source.

- Android OS (Google Inc.)
  - Open source - adopted and adapted by various OEMs
- BlackBerry OS (Research In Motion)
  - Closed source - used on Blackberry devices only
- iPhone OS / iOS (Apple)
  - Closed source - used on Apple devices running iOS only
- Windows Phone (Windows Phone 7)
  - Closed source - used on Windows devices only

While the market has fluctuated over the years, two Operating Systems have emerged that cover a clear majority of devices in circulation today. The table below illustrates this point by showing the deployed mobile OSes in devices globally in 12 months across 2015 and 2016.

Table 1: Smartphone operating systems (IDC, 2017).

Period	Android	iOS	Windows Phone	Others
2016 Q1	83.4%	15.4%	0.8%	0.4%
2016 Q2	87.6%	11.7%	0.4%	0.3%
2016 Q3	86.8%	12.5%	0.3%	0.4%
2016 Q4	81.4%	18.2%	0.2%	0.2%
2017 Q1	85.0%	14.7%	0.1%	0.1%

Of the two major players, Android has a clear lead as its freely available source code is adopted and used by many different smartphone OEMs, e.g. Samsung and Sony, while Apple's iOS is proprietary and exclusive to their own devices. Due to the closed nature of Apple products, the ability to analyse and modify security functions is limited. This, is coupled with encryption deployed by default on Apple smartphones, leads to problems when attempting to verify data sanitization. The factors above have led to the conclusion that the Android Operating System will be the sole mobile OS under scrutiny for the research.

1.3 Research gap

***Note**: Definitions for different sanitization methods are addressed later in section 5.2. In this chapter the term "erasure" is used interchangeably with the term "sanitization" in the context of flash memory.*

Amount of data generated and stored on modern smartphone devices demands security being a necessary component of design requirements. Keeping track of the user data security includes utilizing the proper methods to remove that data from the device. Reliable and irretrievable data erasure of storage media is a critical component of secure data management and a fundamental aspect of device disposal. Secure erasure of flash memories is one of the most unclear and misunderstood concepts, where very little progress has been made despite of all the focus on data privacy and security (Datalight, 2015). Unlike the days of rotating media, securely erasing data from flash media requires additional steps and knowledge (Datalight, 2016). In contrast to older technology such as hard disk drives, for which appropriate data erasure process is well established and well-understood, erasure of flash memories such eMMC has to be done differently and might be hindered by the proprietary design of the memory semiconductors. It has been proven, that the tools and techniques used for traditional hard drives do not work on solid state drives (Singh, et al., 2016). The differences in erasure process can be explained by significant differences in internal architecture, physical storage principles and algorithms to manage and access data. These peculiar properties of flash-based memories can potentially lead to a dangerous misunderstanding that the data are left recoverable remaining on the drive and requiring only moderate sophistication to extract (Wei, et al., 2011).

Although solid-state drives have strong advantage over hard disk drives, flash memories that they use are subject to finite erase cycles and erase-before-write limitations. Flash memory is programmed electronically and consists of pages that are grouped into blocks. Page is the minimum unit for read and write operations, while block is the minimum erase unit. Erasure, being more complicated operation than read or write, significantly degrades the storage. After the maximum erase limit is reached (typically 10,000 to 100,000 times), the block becomes unreliable. (Singh, et al., 2016)

Moreover, solid state memories are characterised by indirection between the logical block addresses, that computer systems use to access data, and the physical block addresses that identify physical storage. This helps to enhance storage performance and reliability by hiding flash memory's idiosyncratic interface and managing its limited lifetime. (Wei, et al., 2011)

Allocation schemes, aiming at even wear-out of the flash memory, may also hide the fact that data were supposed to be erased permanently, when they were actually only moved (Datalight, 2015). The data that are left behind on invalid pages after an out-of-place update also complicates the secure deletion task (Singh, et al., 2016). Typical flash-based system will state that all data have been erased when they were merely deallocated, which indicates potential recoverability of the data until the explicit erasure (Datalight, 2015).

Though, there have been research done on SSD, UV EPROM, EEPROM, NAND and other flash media erasure, understanding on eMMC erasure is still underdeveloped. According to research done by the University of California, San Diego (Wei, et al., 2011), only a comprehensive and secure erase and overwrite of the entire flash media destroy data. Another research undertaken by University of Cambridge (Skorobogatov, 2005) concludes that even the data that have been erased or overwritten can be prone of data remanence which is also explained by the internal structure of the flash memory. In non-volatile flash memories bits are stored as charge in the floating gates of a transistor. Consequently, this means that data or their parts can still be extracted even after erasure. This represents a serious threat to any security system.

1.4 Need for data sanitization

The importance of secure and irrecoverable data sanitization is well-recognized, it is always among the highest priorities for any companies as well as individuals. However, when it comes to the end-of-life of technology asset, what happens to them is rarely at the top of the list being typically summarized in one sentence similar to "Retired equipment must be disposed in a secure and environmentally friendly manner" (CIO, 2018). Nowadays companies are becoming more concerned about how data protection and how security mechanisms affect their business performance. With data now moving freely among mobile devices, today's rapidly evolving threat landscape demands a more comprehensive approach to protecting sensitive information assets. For any organization data is invaluable asset, containing information on products, services, customers and suppliers, financial data. Any asset used for business development should be protected by security mechanism (Inspired Techs, 2017). These data must not be disclosed to unauthorized individuals in any manner, as the data is considered a company intellectual asset.

National legislation and regulation acts as well as corporate policies are determining assets to be securely erased before decommissioning. Reliable asset sanitization can provide security and privacy of the user data and ensure confidentiality of the information stored by the previous owner. Well-established data protection mechanism is a cornerstone of any risk management process. Not being able to provide data security may lead to disclosure of sensitive information and data breach and associated potential legal fees, fines, auditing services, repaying customers and other financial losses. If a company suffers a data breach, it must deal with a wide range of consequences it is not likely prepared for. In the recent past, a number of companies have had their databases attacked and their customer information compromised. The leakage of information assets unavoidably ruins the trust to the company and results in negative publicity and decrease of customers due to inability to protect their confidential information. Typically, customers migrate to another supplier. In addition, they can sue the company, which could result in punitive damages and court fees.

Table 2: Data erasure benefits.

Factor	Impact of data erasure	Description
Likelihood of data breach	↓	Violation of information privacy and disclosure of confidential data.
Reputation and trust	↑	Reputational losses are decreasing the trust to the company which makes it less attractive for existing and potentially new customers.
Risks	↓	Some business data are used for risk mitigation, business optimization and overall business improvement. The loss of these data can cause increase of risks they have been mitigating.
Business disruption	↓	Significant violation of business processes and company's operation.
Cost savings	↑	Minimization or avoidance of extra costs related to the consequences of data leakage, law suits, legislation penalties or company's liabilities.
Overall security and status of organization	↑	Indicates the reliability of the company as a supplier and helps to build trust and good reputation.
Regulatory compliance and auditing	↑	State and international legislation demand IT assets to be erased prior to disposal.
IT environmental footprint	↓	Securely sanitized devices can be further re-used and recycled, therefore, extending IT product lifecycle and reducing the consumption of raw materials.

For many companies, data assets are leveraged as risk mitigation instruments. Thus, the loss of data previously used to mitigate certain risks makes the company more vulnerable to threats. These may have negative long-term consequences not only for IT systems, but for the company as whole including disturbed business continuity, disruption of business processes and worsened company's overall performance, decrease of share price and increased liabilities. As infrastructure expands to meet the needs of new services and technologies, companies must focus more on improving overall data privacy and addressing and managing the significant enterprise risk that is data security. Besides the fact that robust and reliable data destruction process improves overall data security of organization, it also enables assets reuse and recycling, therefore, supporting green initiative and enabling Circular Economy. Extended lifecycle of IT assets reduces the need for raw materials, which significantly decreases negative environmental impact.

The last but not the least, sound data erasure process helps to be compliant with state regulations concerning data privacy This has become a topic of discussion for all the companies handling the data of EU citizen in the light of EU GDPR regulation. The key points are summarized as following (EU GDPR, 2016):

- Applicability

Both data collectors and data processors, and both businesses and governmental organizations are subject to the new legislation; adjustments are made for micro small and medium-sized businesses.

- Right to be forgotten

The legislation also preserves the right to have personal data erased "without undue delay" under certain circumstances.

- Withdrawal consent

Prior to giving consent, data subjects must always be informed of their right to withdraw consent.

- Breach notification

Supervisory authorities must be notified within 72 hours of learning of a data breach; impacted individuals must be notified "without undue delay".

- Fines

The maximum fines will be set at 4% of an organisation's worldwide turnover, or 20 million euros, whichever is higher. Infractions will be grouped into ties, attracting different maximum fines levels.

The EU GDPR is forcing organizations globally to rethink and redesign the whole process of how data are being collected, handled and destroyed. GDPR compliance requires end-to-end data lifecycle management, transparent processes and customer communications on methods for data removal, and finally, improving data security. (Blancco Technology Group, 2016)

1.5 Structure of the document

Data protection has long relied on risk management as a critical tool for complying with data protection laws and ensuring that data are processed appropriately (CIPL, 2014). Presented document utilizes risk-based approach and is relying on existing ISO risk management standards such as ISO 31 000 and ISO 27 001 to build a foundation for the guidelines. ISO 31000:2018 Risk Management Guidelines is an international standard that provides principles and guidelines for effective risk management. It is not specific to any industry or sector and can be applied to any kind of risk and any kind of organization. It provides the principles and guidelines of mapping the risk in systematic and transparent way and credible manner and within any scope and context.

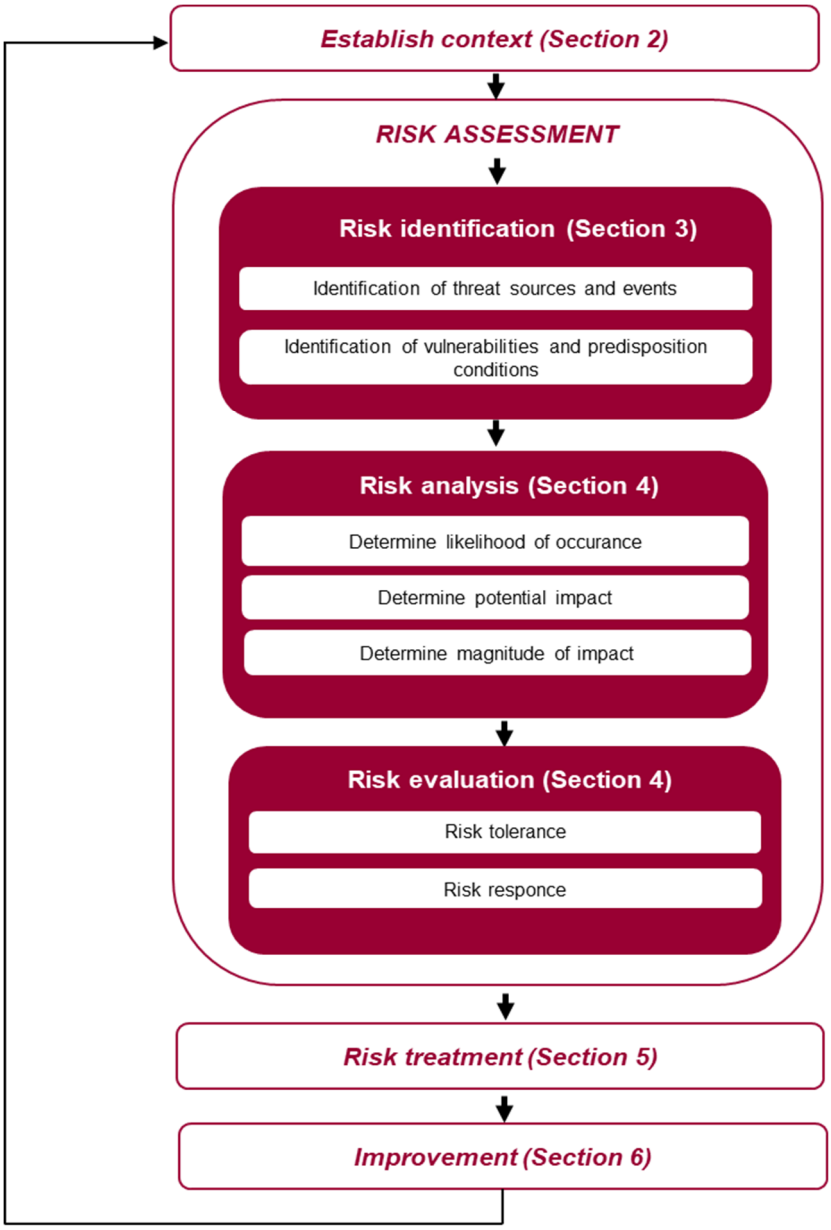
Implementation of the risk-based approach allows identification and evaluation of potential risks and development of a risk management plan to minimize or avoid potential negative consequences these risks can bring. Risk management involves three key elements — (1) the systematic process of identifying and assessing harms and other negative impacts, (2) avoiding or mitigating those that cannot be justified by the benefits and other positive impacts, and then (3) accepting and managing the remaining risks (CIPL, 2014).

Risk management is a valuable tool for calibrating the implementation of and compliance with privacy requirements, prioritising action, raising and informing awareness about risks, identifying appropriate mitigation measures (CIPL, 2014).

Figure 2 presents risk management process and corresponding Sections of this document. Risk-based approach starts from setting up the context and providing background information. In case of smartphone devices, the context is device's End-Of-Life (EOL), the time when IT asset is retired, or the ownership is changed. The context boundaries are determined by software that smartphones are running on and hardware underpinning internal storage technology. Section 2 gives an in-depth view on drivers of smartphones development and related to them changes in mobile storage requirements. Is also presents the essentials of Android OS and internal flash memory storage types. Threat intelligence analysis described in the Section 3 provides knowledge on sources of threats, their capabilities and attack vectors. These are later used to determine the likelihood of attack and estimate potential impact and magnitude in case of risk materialization (Section 4). Risk identification and analysis help to design appropriate response based on value of the data that can be compromised by an unauthorised user. The organization can then determine risk tolerance level and risk mitigation plan. In the context of data sanitization, it would mean selection of appropriate data destruction method (Section 5).

Continuous improvement, being an integral part of overall process, is focused on enhancing the security management system needed to achieve improvements in overall security performance consistent with the organization's security policy (ISO 28000:2007(en), 2007). Recommendations provided in the Section 6 contain guidelines on secure smartphones sanitization before their disposal. Risk management process is not linear but rather continuous process which means its elements should be reviewed regularly to identify any possible changes in the context, identify new risks or redefine risk tolerance levels.

Figure 2: Document structure.



Application of risk-based approach brings the following advantages (Baich, 2012):

- Ability to build a more in-depth view on threat environment and own strengths and vulnerabilities.
- Gather actionable risk intelligence
- Determine the value and risk-related significance of categories of data, prioritize and protect them accordingly
- Develop cyber intelligence
- Understand the organization's susceptibility to persistent, sustained access by cyber criminals

One of the most important benefits of risk-based management is ability to foresee the risks and identify and prevent them before they occur. This enables to switch from responding to incidents to proactive risk approach. Without that companies are not able to prioritize security threats understand their motivation and techniques, detect and respond to attack. Risk management is critical for any organization to deliver their strategies, initiatives and goals as well as to meet business requirements for information security. (Durbin, 2016)

There is value to be added by an effective risk management process and by having efficient risk monitoring resources. A risk monitoring process, if well thought-out and executed, will help line management operate their business processes with added efficiency.

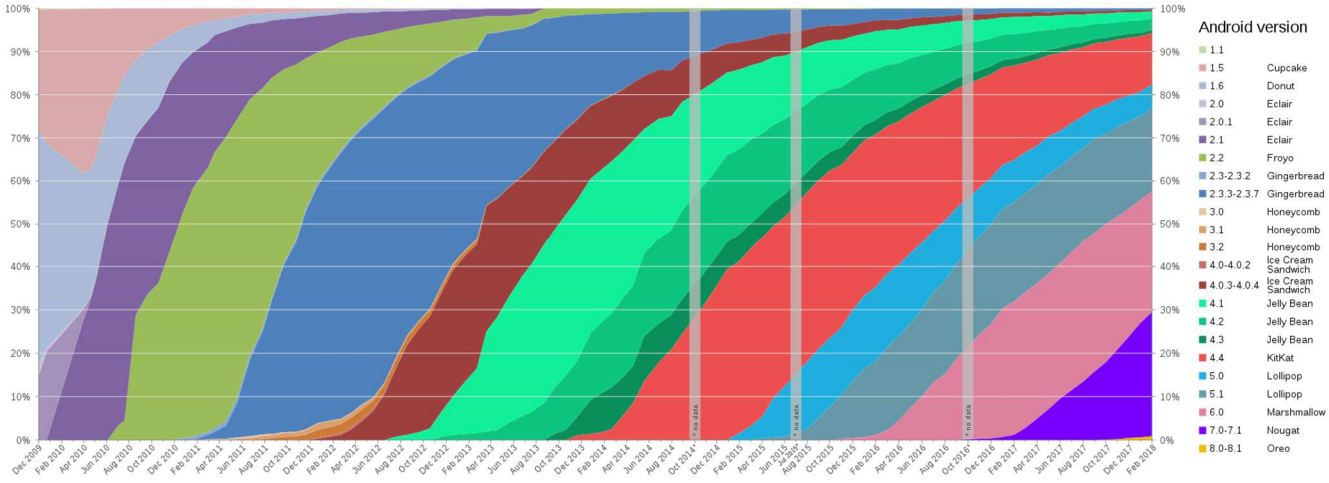
SECTION 2: Erasure in context

2.1. Android platform

Versions

Android OS remains highly fragmented, following its official release in 2008 (Amadeo, 2012), new versions have been coming every year followed by minor updates including bug fixes and security patches. From Android version 1.5, Google started using alphabetical code name with Android "Cupcake". The latest version at the time of this report is Android "Oreo" (version 8.0 – 8.1) and a new version, Android "P", is coming in late 2018. When a new version is released, only the devices manufactured by Google get updated immediately. Because other manufacturers need time to adjust the core OS to fit their own product line, it takes time until the new version arrives to the rest of the devices. In some cases, older devices are abandoned out of update cycle and keep running old OS version. Figure 3 illustrates the distribution of all Android versions throughout the years since 2009. Right now, in 2018, KitKat, Lollipop, Marshmallow and Nougat are the most common Android versions. However, due to the lack of updates coming to older devices, there is still at least 1% of market share per each old Android version starting from "Gingerbread" 2.3.

Figure 3: Android historical version distribution (Erikrespo, 2018).



In Table 3, we studied and singled out the most significant changes among Android versions regarding user's privacy and security (Wikipedia, 2018). On versions prior to 3.0, Android updates were focusing on core features and improving system performance. From Android 3.0, some new features related to user's privacy and storage interface performance were added: enable SELinux, restrict access of new user profiles, add *fstrim* system feature which allows storage address instant remapping.

Encryption is one of the key features when it comes to data security. Android version 3.0, Honeycomb, is the first version where user data security becomes a highlight with the introduction of full-system encryption. Full-system encryption offers optional user data encryption in the kernel. In Android 5.0, Lollipop, data encryption is updated with the addition of Full-disk encryption that uses a single key to protect the whole device's user data partition. The key for full-disk encryption is protected with user's password, so user needs to enter the password before being able to access anything on the device. Initially, full-disk encryption is supposed to be enforced by default on all devices released with Android 5.0. However, due to the drop of performance, Google only makes it default for devices with strong enough hardware. Android 7.0, Nougat, is the version with the announcement of file-based encryption. File-based encryption encrypts different files with different keys that can be unlocked independently.

To control individual application Android has a permission control policy. There are 2 levels of permission, system level permissions and normal permissions. System level permissions can only be granted to the *system applications*. In version 4.3, Android separates the real system applications from the bloatware (pre-installed) applications from manufacturers by adding the *"system/priv-app"* director. Only those applications installed in the specified directory can have access to the system level permissions. Normal permissions are granted to the apps by user either at the time of installation (Android 5.1.1 and earlier) or at run-time (Android 6.0 and later). In 4.3, Gingerbread, Google added a hidden feature called *App Ops* which allows user to enable\disable permissions individually for each application. This feature has been removed from the system in Android 4.4.2 update due to potential bugs. From Android 6.0 Marshmallow, the ability to grant permissions individually has returned in a different form. In this new version, user grants permission to the application at run time one-by-one and has access to an official permission setting menu.

Table 3: Android version changelog.

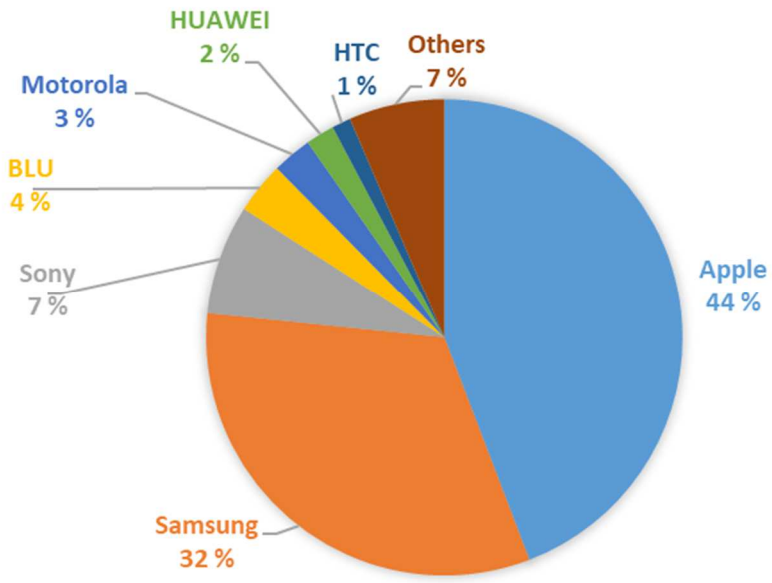
Version	Highlight features
3.0 (Honeycomb)	Ability to encrypt all user data (full-system encryption)
4.3 (Gingerbread)	• SELinux on Android is enabled by default • Restricted access mode for new user profiles • Improve file system performance by running *fstrim* when device is idle • Devide system application into 2 types with addition of *system/priv-app* directory • 'Hidden' *App Ops* feature to control granting of application permission individually
4.4 (Kitkat)	• Restriction for applications when accessing external storage except for their own directories • Enforcing SELinux • Android 4.4.2, remove *App Ops* feature due to potential bugs
5.0 (Lollipop)	Enforce user data encryption by default (Full-disk encryption) for devices that have suitable hardware
6.0 (Marshmallow)	• Enforce user data encryption by default for all devices • Adoptable external storage to behave like internal storage • Return of individual application permission granting (*App Ops*)
7.0 (Nougat)	Announcement of File-based encryption

Smartphone manufacturers

Similarly to OS version diversity, there is extremely high fragmentation in terms of smartphone manufacturers. For instance, in 2015 there has been over a thousand brands that manufactured more than 24 000 devices (OpenSignal, 2015). Android even helped to develop a segment of low-cost smartphones in the range of 100-500$ (Hoffman, 2014) that did not exist before, resulting in widening the options for every preference, budget and taste.

In our research, we have analysed Blancco internal data gathered from almost 190 000 devices that have been sent to recycling facilities for re-use or mechanical destruction in Europe in between 2015 and 2017. These data served as a base for selecting the devices for our internal testing and shed some light on the situation in the second-hand market. Thus, we could distinguish the main manufacturers in European market and their share. The market share of major smartphone manufacturers has been presented in Figure 4. Excluding Apple devices which are not part of the scope of this research, the rating of top Android smartphone makers is headed by Samsung. The next major ones include Sony, BLU (mainly present in UK), Motorola, Huawei and HTC. Each of these manufacturers hold less than 10% of the market. Other vendors account for less than 1% of the market and are grouped into "Others" category.

Figure 4: Vendor distribution of erased devices in Europe.



Openness of Android platform gives phone manufacturers freedom to change the OS according to their requirements. Therefore, smartphones coming from different vendors deliver unique experience due to modifications phone makers are introducing to the OS. Based on a degree of these modifications we can classify the devices into several categories:

- Zero degree of modification (aka Vanilla / Stock / Pure Android)

  These devices are running on the version of Android that is directly provided by Google without any modifications. Examples of these smartphones are Google Nexus devices. Stock Android is coming only with important applications and tools that are needed to run the OS or which Google considers important for its users (no extra skin or bloatware over). All other than Nexus devices come with skinned Android OS which is based on pure Android (Soutiyal, 2016).

- Slight modifications

  Such devices are heavily based on pure Android and introduce some superficial changes released in interface modifications and small amount of pre-installed apps. These are typically entry-level and mid-range smartphones.

- Heavily modified

  The Android OS on these devices has been significantly changed resulting in a large number of pre-installed apps as well as incorporation of deep changes. For example, stock Android reserves a space for the phone manufacturer within factory reset section which gives a full freedom in the way the process is performed. Thus, some vendors, for instance, provide an option to keep the multimedia content or erase the whole storage space. Devices that are running on deeply modified Android OS include the ones of the big vendors such as Samsung, Sony, LG.

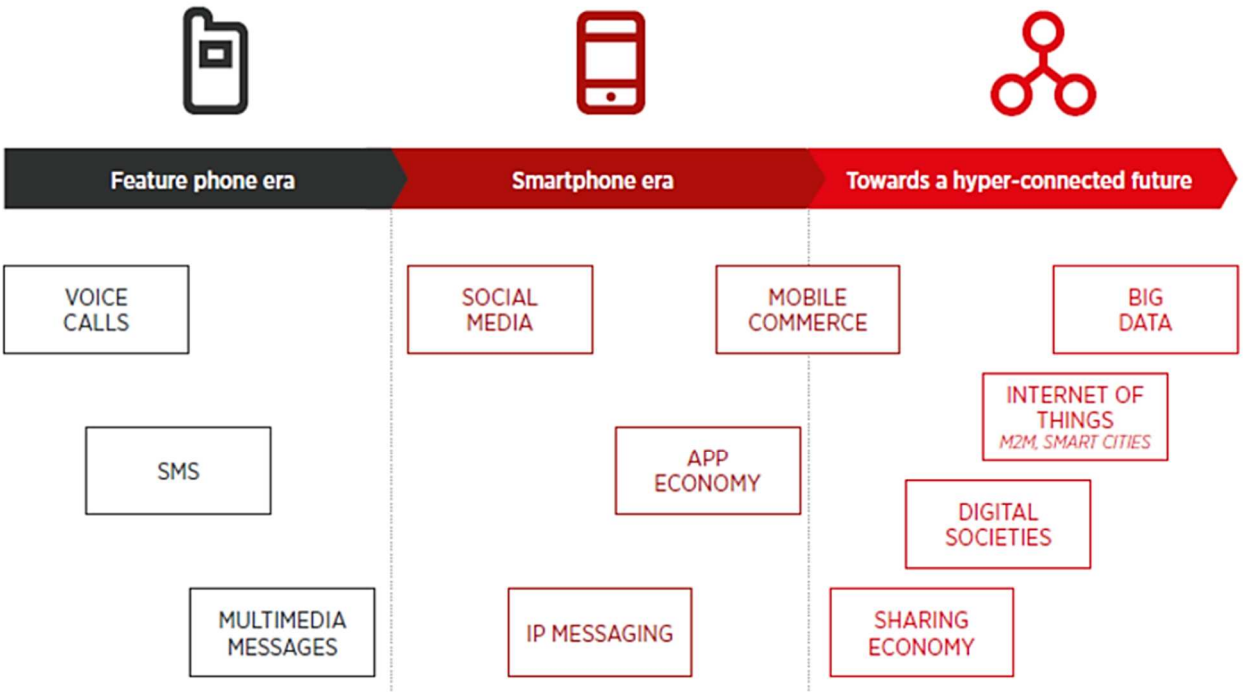
Besides improving user experience and differentiation, phone manufacturers are customizing Android OS to enable support of phone hardware and make most out of it. For example, Samsung flagships have ab iris scanner which Android stock versions are not equipped to make any use of (Android Authority, 2016). Therefore, Samsung has to make a unique version of Android to utilize the capabilities of an iris scanner.

2.2 Storage technologies

Evolution of mobile memory storage

Gradually growing sophistication of mobile phones and constant technical and feature improvements are determining the need for more advanced memory technology utilized on modern devices. Mobile phones initially used solely for calling and SMS/MMS exchanging evolved into mini computers and primary communication mean with extended functionality going beyond traditional phone's limits (Figure 5). Therefore, the requirements for memory storage have also changed dramatically. Improving performance of smartphones required a bigger capacity and faster memory combined with small form factor, low energy consumption and attracting pricing.

Figure 5: Evolution of mobile devices (GSMA, 2016).

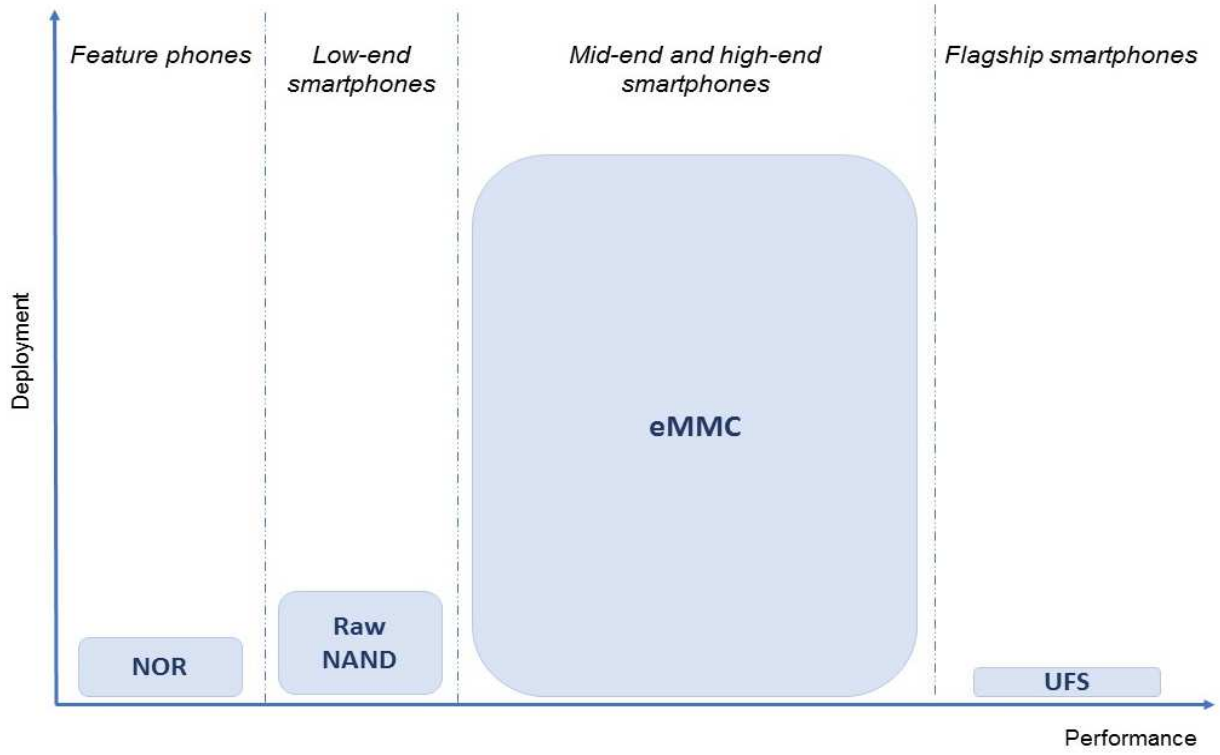


Considering implementation of different memory storage technologies across the whole spectrum of mobile devices and the fact that mobile devices vary greatly in terms of their functionality and performance influencing heavily the memory storage requirements, we have analysed the distribution of the device across the market segments and storage platforms. The size of the rectangles represents the quantity of the devices running on certain storage platform. Feature phones, having a strong price advantage, offer a fixed set of functions beyond calling and messaging, for instance, Web browsing and e-mail, but they generally cannot download apps from an online marketplace (PCMagazine, 2017). Technical characteristics of such devices are very basic, often they even don't have a camera. Therefore, they don't store much of a content and do not require extensive storage.

Low-end also called as entry-level smartphone is usually intended for users with average technical skills. Such devices are equipped with less powerful hardware, smaller memory and lower storage capacity. An entry-level smartphone is the cheapest model of its class, or the base model. They may share the same design as high-end ones, but with fewer advanced features. (Techopedia, 2017)

The mid-end and high-end category represent the intermediate smartphones, the models that are between the most basic and the most complete. Generally, they are built with good materials and components, have decent characteristics, are close to the best in the market and the price is higher than the low-end. These devices are designed for more complex tasks such as playing heavy games, editing photos and videos, using the device as a router etc. All these functions rise the bar for memory storage both in terms of speed and capacity and make eMMC preferred storage technology.

Figure 6: Memory storage in relation to smartphone categories.



The flagship smartphones represent the best devices phone maker has to offer, featuring the top-notch specs and new features that improve user experience. These devices are also equipped with the latest memory storage technology that exhibits high memory performance and capacities and are designed for technically advanced users who are ready to pay the premium. As time goes by, new technologies evolve and surpass the already existing ones resulting in changes of classification (Chibueze, 2016) and storage platform preferences.

Overview of internal memory storage technologies for smartphones

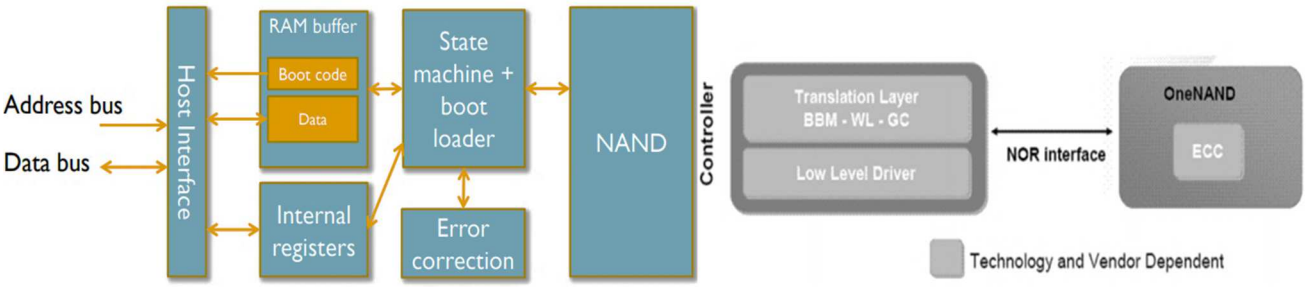
NOR vs NAND

Before the era of smartphones NOR flash used as a primary non-volatile storage technology for feature phones. NOR flash has been designed as a replacement for read only memory (ROM), erasable programmable read-only memory (EPROM), and EEPROM non-volatile memory (Whitaker, 2015). The key advantages of such technology were fast random access and byte write capability (Cooke, 2006). On the drawbacks was very slow erasure speed, which was not that big of a problem as long as performed infrequently (Whitaker, 2015), which in the end determined its wide adoption on feature phones. However, expanding functionality of phones and new features targeted on generation and storage of multimedia content such as pictures, videos, music raised the bar for memory storage requirements. The need for higher density and capacity made NAND flash more attractive alternative than NOR. NAND has become an optimal solution for low-cost applications offering high-density and fast erase.

The larger capacity of NAND, required by modern consumer market applications including smartphones, has been provided by a smaller cell size. NAND's multiplexed interface represents a similar pin-out for all recent devices and densities, which gives more flexibility to designers when migrating to larger densities bypassing any hardware changes on the PCB (Printed Circuit Board) (Cooke, 2006)

NAND flash requires a controller, either internal or external, specific firmware for error code correction (ECC), bad block management (BBM), and wear leveling (WL), Flash Translation Layer (FTL). (Micron, 2018). First NAND flash architecture (i.e. raw NAND / pure NAND) had the lowest cost per GB among NAND flash (Micron, 2018), consisting of a memory unit directly managed by a host (Cooke, 2006). One step towards managed NAND was taken by Samsung who has introduced a new memory device OneNAND™. It has incorporated high-speed data read function of NOR Flash and high speed write capability of NAND (Fiorillo, 2009). OneNAND has a NOR interface and contains a NAND flash and RAM and is classified as a raw NAND due to FTL being manage by host controller.

Figure 7: OneNAND architecture (Fiorillo, 2009) (Boukhobza & Rubini, 2012).



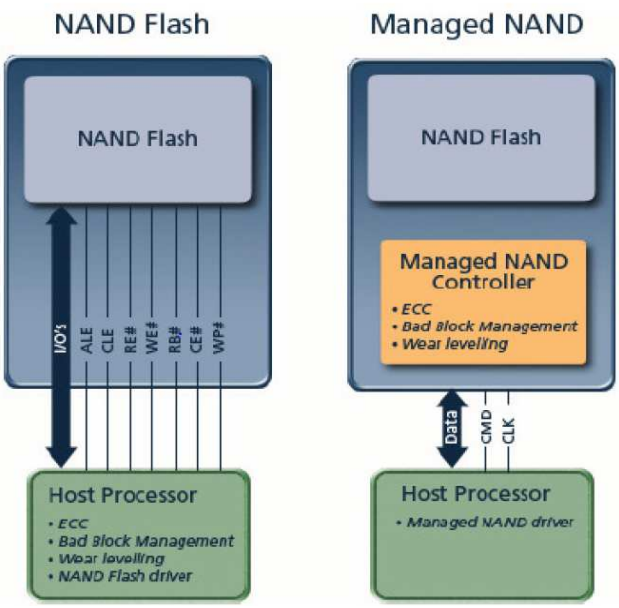
eMMC

The next stage of NAND flash-based storage evolution started from the release of advanced managed NAND – eMMC (embedded multi-media chip). This chip contains NAND flash memory and an embedded controller in an industry-standard BGA package (Whitaker, 2015). All the flash management operations are handled by on-chip controller internally which removes the workload from the host controller and allows device to run faster. The eMMC architecture allows simplification of application interface design and release the host processor from low-level flash memory management. The host processor sends the commands through the MMC Bus without any additional considerations, such as Error Correction Code (ECC), Wear-Leveling (WL) and Bad Block Management (BBM), which are performed by the on-chip controller. Accommodating the complexities of flash technology into a convenient plug-and-play package eMMC greatly reduces time and effort for developers.

Following its launch in the year 2008, eMMC has quickly become a preferred flash storage type in portable consumer electronics such as smartphones, tablets, navigation/GPS devices, digital book readers, digital cameras (PRWeb, 2015). The eMMC format has added new dimensions to the basic function of mass storage, and the current version eMMC 5.1 comes with several innovative features such as up to 400 Mb/s data transfer rates, enhanced strobe and command queuing to augment the already established image of eMMC in its end-use verticals.

As mobile devices have been constantly becoming more complex, there has been a need for improved storage performance which resulted in release of several eMMC versions based on JEDEC standards (developer of open standards for microelectronics industry). This has resulted in many flavours of the eMMC that can be found on different mobile phones. The overview of versions history is presented in Table 6. Every next eMMC version is characterised by faster random and sequential read and write speed as well as higher storage capacity. Moreover, newer versions have been focused more on improving data security features, for example, introducing Sanitize, TRIM Secure Erase and Secure TRIM operations. Significant changes have been introduced starting from eMMC v.5.x resulted in introduction of firmware update feature and health report. Firmware (FW) refers to the program helping eMMC to operate the way it is supposed to. Whenever the manufacturer makes improvements to the programs that run the storage a new FW update is released. A new FW version aims to boost the device performance and / or fix the bugs. However, it's worth mentioning that eMMC FW update is a complex and manual process accessible mainly to the technically advanced users.

Figure 8: Raw vs managed NAND (Whitaker, 2015).



Starting from version 5.x eMMC start containing health report information that has been designed to indicate an estimated life time (in percentage) of the chip calculated as a ration of averaged wear out of memory to its maximum estimated device life time.

Table 4: eMMC versions comparison (Datalight, 2016)

Functionality/ Version	4.3	4.4	4.41	4.5	4.51	5.X
Read block	x	x	x	x	x	x
Write block	x	x	x	x	x	x
Reliable write	x	x	x	x	x	x
Write protect		x	x	x	x	x
TRIM		x	x	x	x	x
High Priority Interrupt		x	x		x	x
Sanitize				x	x	x
Enhanced Partition types				x	x	x
Firmware update						X
Device Health Report						x

Besides the variety of eMMC versions there are also various packaging alternatives such as Embedded Multi-Chip Package (eMCP). Flash sizes have been shrinking alongside constant miniaturization of communication devices, which forced the memory manufacturers to integrate several components (typically SRAM, DRAM and eMMC) into one eMCP package (Whitaker, 2015). This design allows significant size reduction due to vertical stacking, which enables development of thinner and smaller devices (PRWeb, 2015). Besides flexibility in various physical sizes of any smartphone design and space allocation advantage eMCP organization provides significant cost benefits (SK Hynix, 2017).

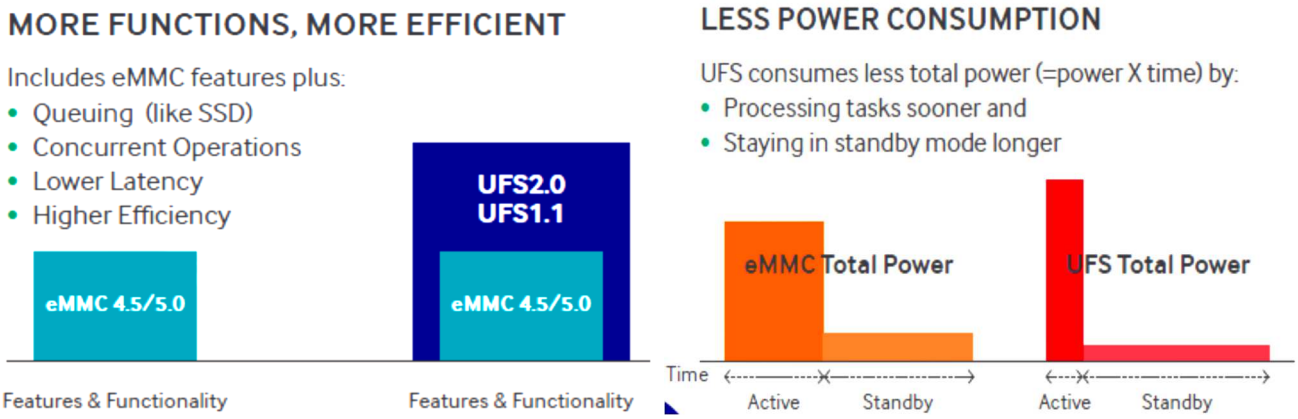
UFS

The explosive growth of mobile devices over the past decade continues to challenge manufacturers requiring them to meet the following basic criteria (Design&Reuse, 2016):

- High bandwidth
- High capacity
- Low power consumption
- Low cost

Flash storage technology and standards have been evolving rapidly over the years to meet these requirements, which resulted in development of Universal Flash Storage (UFS) to satisfy the demands for high performance and low power consumption. UFS has been termed SSD for Mobile (Design&Reuse, 2016). Even though eMMC is remaining a dominant storage technology for smartphones, newly developed UFS is gradually gaining wider adoption being primarily used in flagship smartphone devices. UFS is the next generation of high-performance non-volatile storage standard. It is intended to be a replacement for eMMC which is cheaper and easier to implement but is significantly slower (PhoneArena, 2017). UFS brings together the high sequential read/write speed of SSD and low power consumption of eMMC (UFSA, 2013).

Figure 9: UFS vs eMMC (Kathy , 2013)

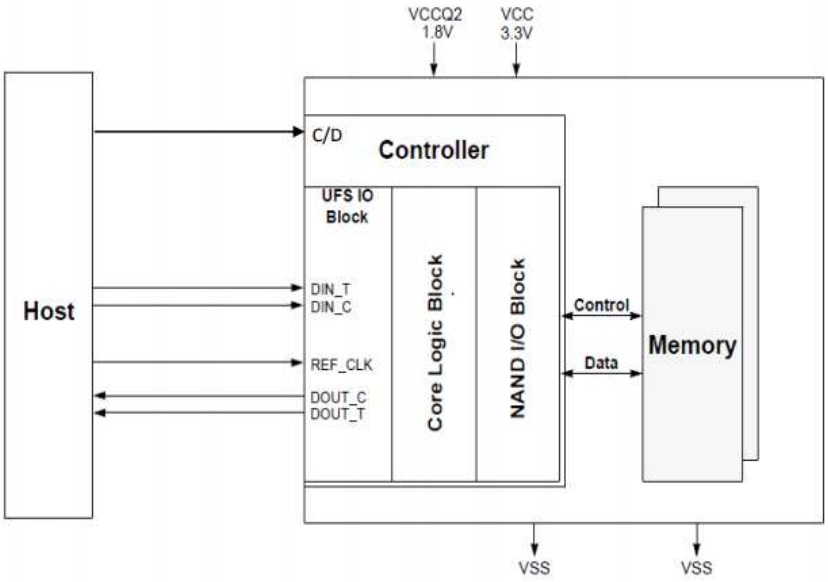


Faster storage determines better overall performance (Figure 9), and while eMMC is still fast enough for general use, it could prove a bottleneck in more resource-intensive use cases such as, for instance, recording high-bitrate 4K videos (PhoneArena, 2017). The difference between eMMC and UFS is tremendous especially in high densities (128 GB 256 GB and 512 GB) which is critical in multi-tasking and multimedia operations (PR Newswire, 2017). Therefore, strong UFS performance makes it preferable technology for the next generation smartphones. Among key benefits is faster application load times and boot up, multi-tasking responsiveness that allows quicker switch between the applications. Higher memory interface bandwidth improves camera performance when shooting multiple photos or panorama pictures. Faster read/write UFS characteristics enable seamless HD streaming and better graphical content which improves gaming experience (Micron, 2016).

UFS has significantly improved performance due to 2 main factors. Firstly, UFS has a LVDS (Low-Voltage Differential Signaling) serial interface which incorporates separately dedicated read/write paths (Figure 10). This allows two-way interaction (full duplex) which means that UFS can read and write simultaneously which is critical when the device is under load. On the contrary, eMMC has a parallel interface which allows data traffic only in one direction at a time, e.g. either read or write.

Secondly, UFS has a Command Queue (CQ), which sorts out the commands that needs to be performed. In this case, multiple commands can be carried out at the same time and the order of tasks can be changed accordingly. In its turn, eMMC (up to v.5.0) has to wait until previous command is completed before sending a new one. The combination of these two advantages allows UFS to have a sequential read speed, sequential write speed, random read speed and random write speed much faster than eMMC.

Figure 10: UFS architecture (JEDEC standard, 2016)



Furthermore, despite of strong performance of the latest UFS 2.1 development of the next 3.0 version is already ongoing. The new chip is promised to be 1.5 times faster than the previous version and offer reduced power consumption. Overall, there's going to be 30% increase in performance (Singh, et al., 2016)

The adoption of new storage technology such as UFS is steadily growing but is slow, therefore, allowing eMMC to remain an industry standard for mobile storage. First reason is introduction of eMMC v.5.x series which has significantly improved its performance characteristics in comparison with v.4.5 (Figure 11). High transfer speed and first time implemented command queuing feature (Android authority, 2015) makes eMMC 5.1 competitive with UFS. Secondly, due to UFS's entirely different overall structure and design, it will take a long time for application processors' manufacturers to support a new standard. Thirdly, development costs of UFS particularly for the controller part are significantly higher. Slowing down innovation in high-end devices and noticeable advancements in mid- and low-end smartphones mean that UFS can only compete with eMMC in high end markets with not many chances to become a mainstream in the long-term perspective.

Figure 11: UFS vs eMMC performance (Micron, 2016).

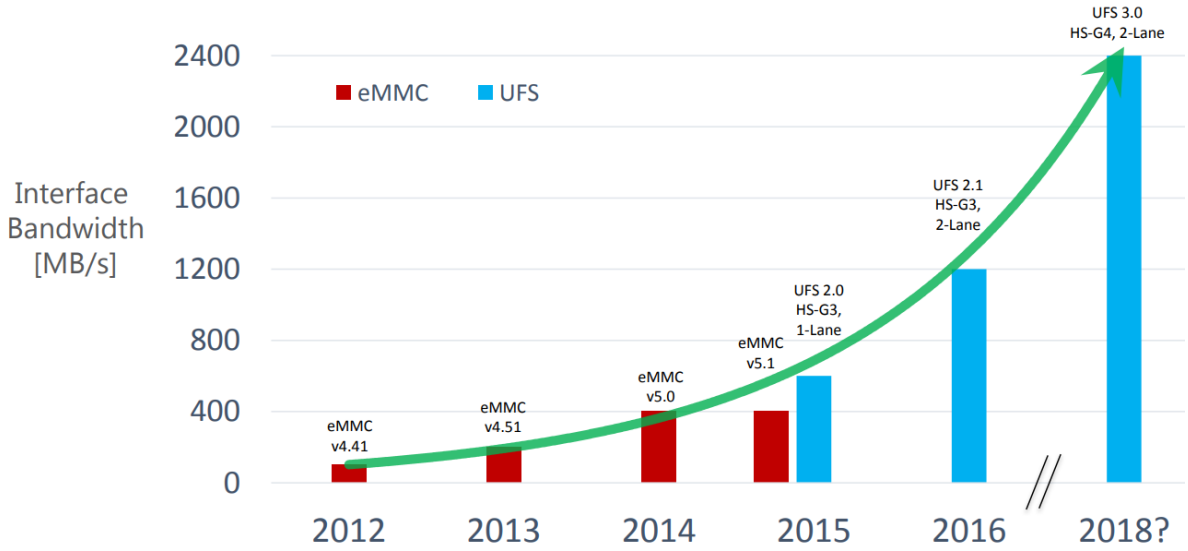
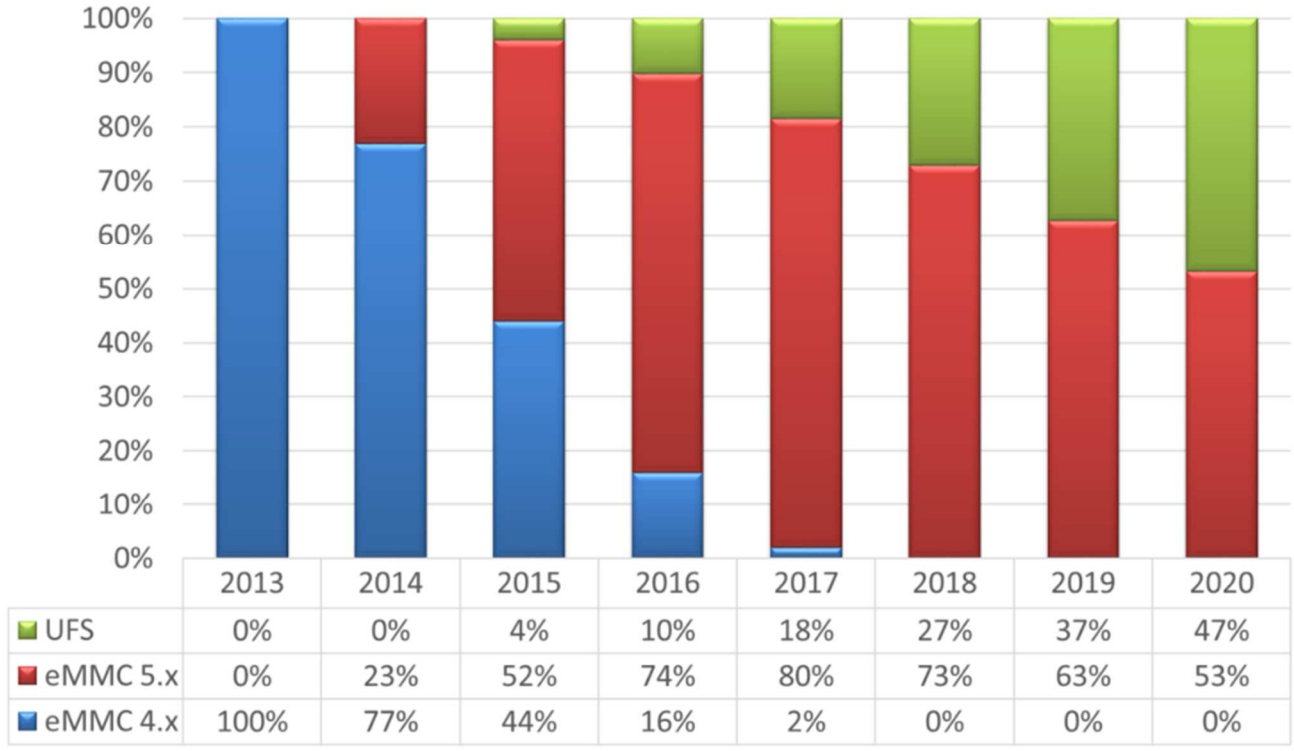


Figure 12: eMMC vs UFS forecast (IHS Markit, 2017).



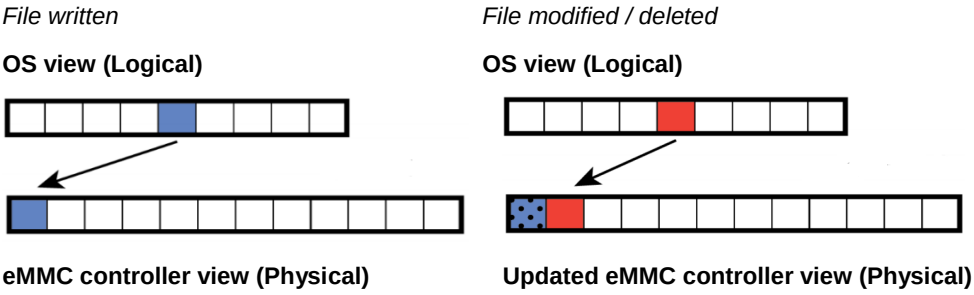
	2013	2014	2015	2016	2017	2018	2019	2020
UFS	0%	0%	4%	10%	18%	27%	37%	47%
eMMC 5.x	0%	23%	52%	74%	80%	73%	63%	53%
eMMC 4.x	100%	77%	44%	16%	2%	0%	0%	0%

Smartphones and tablets are typically using eMMC storage to store information, however, a transition is under way towards Universal Flash Storage (UFS) as the future of flash memory (Figure 12). The JEDEC-defines UFS mobile-centric storage standard addressing next-generation mobile performance and scalability, offering high performance characteristics that are essential for mobile phones. (IHS Markit, 2017)

Flash data management and security concerns

There are different ways of how the OS and a built-in controller see the storage space. Internally, eMMC controller is responsible for establishing the link between addressable (logical) space and physical blocks on the chip (Figure 13) (Afonin & Katalov, 2016). For the purpose of hiding all the complex data management of memory and making addressing more flexible and simpler, a logical block address is remapped to a physical block address. This way complex low-level data management happening on a flash storage becomes invisible for high levels that consume its service (Flashdba, 2014). Thus, OS has no idea about real location of data. In this case, the host (application + OS) addresses the flash system via logical addresses, memory controller will allocate the data to a certain location on storage and map a logical address to corresponding physical addresses (Boukhobza & Rubini, 2012). Whenever that data gets modified controller will keep the old data and create a copy where the changes will be saved (Figure 13). Similarly, if the file gets deleted controller will remove the index to the physical location, adding a physical block to the "*to be erased*" list and remap the logical address to a clean physical location (Afonin & Katalov, 2016). Notably, the controller may or may not decide to push a newly released physical block out of the addressable space, resulting the content of deleted block to be potentially recoverable (Afonin & Katalov, 2016). Actual deletion will happen later, on all the locations marked as deleted. Also, because it is impossible to re-write the data in a page (min programmable unit) that is already programmed before prior erase and the min erasable flash unit is 16-512 blocks (comprised of pages), controller will duplicate the active data (data not marked as deleted) of the block to another location and then erase the whole block. Therefore, the files that have been deleted by the user (removed from the logical level) can still be potentially recoverable. This is the first key limitation of eMMC storage, impossibility to perform *in-place data updates* (before performing any write on location already storing some data, this area has to be erased first) (Boukhobza & Rubini, 2012).

Figure 13: Memory blocks seen by OS and flash controller.



Another limitation of flash memory is *wear* (flash cells can only sustain certain number of write/erase operations, after which the cell becomes unusable). The exact limit of write/erase operations is determined by employed NAND flash and varies from 5 000 to 100 000 cycles (Boukhobza & Rubini, 2012). To combat these issues and prolong the life span of the memory storage controller performs a set of complex operations to maintain optimal operation of the memory cells. These operations include “Bad Block Management” (identification of bad blocks and excluding them from storing data), “Wear Levelling” (averaging of read/write cycles to prevent the concentration of operations on one block), and “Garbage Collection” (cleaning the memory of invalid pages).

Controller operations

As mentioned before, the number of write/erase (w/e) operations is limited for each cell. Therefore, eMMC controller ensures NAND flash is used efficiently performing *wear levelling*. Wear levelling ensures that write operations are evenly distributed across the whole memory (Toshiba, 2016). eMMC controller keeps track of which cells are receiving a high number of writes and which cells are sitting relatively idle. Then it rotates the used pages on the NAND flash around so that the cells hosting static files are swapped with cells holding active files. The goal is to ensure that no pages are singled out with more writes, and that all the cells age through their allotted lifespan of writes at roughly the same pace (Hutchinson, 2012). In order to successfully rotate the content around flash, there is a need for a buffer area which has been released in a form of *overprovisioning space*.

Overprovisioning

Overprovisioning is the inclusion of extra memory capacity that is not directly accessible by the user and does not form a part of indicated volume of the storage. Consequently, eMMC ships (as well as any solid-state media) have more actual capacity than they advertise (Afonin & Katalov, 2016). The extra physical space is non-addressable until called by the controller and non-visible for the OS. The amount of overprovisioned space varies from one device to another and is only accessible by a controller and memory manufacturer.

As has been mentioned earlier, flash cells are subject of wearing out and as soon as the block gets a broken cell it will be marked as *bad block* and considered unusable: it produces erroneous data that cannot be repaired by the drive using error correction techniques. In this case, the reliability of the data read from that block cannot be guaranteed. Bad blocks are present in a device since it is first shipped, and the number increases over time, as the eMMC is used and begins to gradually wear out. When a block contains bad cells, it is moved to the overprovisioned space and gets replaced by another one taken from a spare pool. If there is active data stored on a block that becomes ‘bad’, it is copied to a new location on the device and the mapping table (Flash Translation Layer) is updated to reflect its new location (the data on the now considered bad block is not removed).

Address spaces

Furthermore, besides the complexity of in-built controller data management, there are several address spaces that are not addressable by the OS but are visible for the chip controller. The JEDEC Standard No. 84-B51 for eMMC defines the following address spaces:

- Mapped Host Address Space
    - Usable space by the host software
- Private Vendor Specific Address Space
    - Cannot be accessed by read command from the host

- Contains vendor specific internal management data
- No host data

- Unmapped Host Address Space

  - Cannot be accessed by a read command from the host
  - Excludes private vendor specific address space
  - May contain old host data or copies

JEDEC standard determines 2 areas that are not accessible by the host. Vendor specific space is reserved for memory manufacturers to store firmware and mapping tables for the controller. This area can be filled during production of the chip or later during its operation. This area does not contain any user generated data. The other non-accessible by the host area is unmapped host address space which does not contain any vendor specific information but may still store user data which can be potentially recoverable.

Secure data erasure considerations

eMMC controller actively and independently manages data stored on the chip, often hiding the result of its actions from the view of the host and, therefore, the user. It may even perform the operations without any commands being sent by the host. On-chip controller contains many complex algorithms that are designed to ensure the reliability of data; maintain fast operation speeds; maximize flash lifetime preventing from premature wear of flash cells; offer the host a simplified way to interact with the storage. However, these controller management complexities combined with flash specific properties are creating certain barriers on the way of secure erasure process (Table 5).

Table 5: The barriers to secure data erasure.

	Impact on secure data erasure
Logical and physical addressing	Deleted data or the duplicates of users' data can still reside on physical memory level. Some data that have been marked as deleted will be placed in a queue for the controller to actually erase it and meanwhile will remain recoverable from unallocated space.
Overprovisioning	Extra memory capacity that used for relocating the data across NAND memory is not accessible for the OS.
Bad blocks	Retired blocks that are no longer write reliable can still be readable.
Unmapped host addressed space	The area is not accessible by the OS but may still store user data.

Due to the advanced operations of the controller chip, a significant disconnect is created between what the user can see on the drive and the physical reality i.e. what is present on the memory chips. The differences in the logical and physical memory views result in hiding the content that has been modified or deleted. Therefore, the data that are invisible for the OS may still be accessible to the flash controller at least for some time before actual execution of erase commands.

The implications the overprovisioning has for erasure are also significant. The allocation of extra memory locations that cannot be addressed at the logical level results in a kind of black box situation as only the eMMC controller can manage the content of the NAND flash directly.

Bad blocks are the blocks that contains one or more invalid bits whose reliability is not guaranteed. They represent worn out flash cells that cannot be programmed anymore and, therefore, are taken out of use. Bad blocks may be present when the devices are shipped or developed during devices usage. However, it is conceivable that the data stored on the block (before it was marked as bad) can still be read and be recoverable in full or fragmentarily. Furthermore, unmapped host address space that is not addressable by the host but accessible by the controller can potentially store user data. All these factors determine the possibility for data recovery from flash storage and require reliable erasure process to combat these issues.

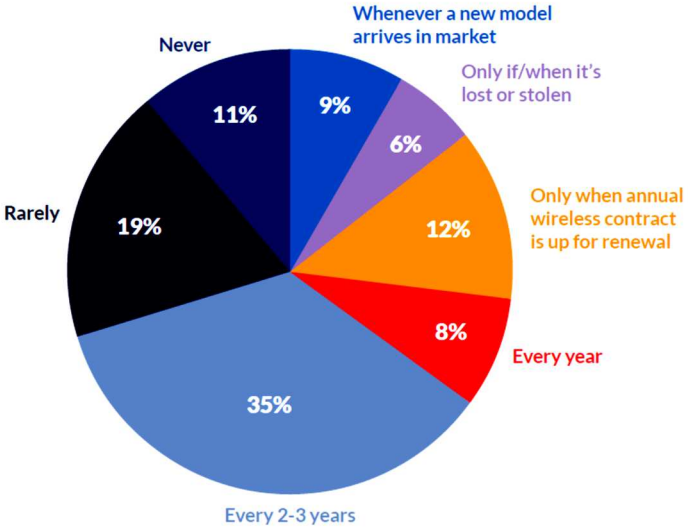
2.3 Device end-of-life

It has been observed that smartphone users are fully dependent on their devices and are passionate about gadget upgrades. Excitement and rush for new smartphone models is what drives the demand for smartphone renewal. This is what motivates people to replace their existing devices with newer, flashier and higher priced models. Notably, this is what drove more than 4 million pre-orders for the iPhone 6 and iPhone 6 plus within 24 hours of the process opening on September 12, 2014, just

seven days before the official launch date (Apple, 2014). According to Blancco Technology Group study (Blancco Technology Group, 2015), the replacement cycle for mobile devices is getting shorter and shorter. In fact, 35 percent of respondents reported that they recycle, trade in, sell or donate their mobile devices every two to three years. Meanwhile, another 17 percent do so either every year or whenever a new model debuts in the marketplace (Figure 14).

Considering the growing number of different smartphone applications that carry personal data and various services that are accessible through the mobile phone, smartphones are storing mission-critical data. And all the smartphones will reach end of life, at which they will be resold, recycled, donated to charity or discarded. The diversity of the data stored on the device and its amount is huge which makes any of us concerned about potential data leakage.

Figure 14: How often the smartphones are trade in, recycled, sold or donated (Blancco Technology Group, 2015).



However, not many smartphone users realize that manual deletion of the information or physical damage will not provide reliable data security in case of highly motivated and skilful threats. For example, in our research we have investigated 2 cases (Table 6, Table 7) where the smartphones had severe physical damage, which resulted in devices not being operational. In both cases, Android devices were not able to be booted and accessed by any software methods. Therefore, in the first case eMMC chip has been desoldered from the device motherboard and read through special chip reader. The results of performed data extraction and analysis are presented in Table 6. To perform the test on the second Android device, motherboard has been disassembled from the remaining parts of the device and the memory content has been read through ISP (in-system programming interface). Table 6 summarizes the type and amount of data found using 3 different Forensics Tools.

Table 6: Data read through chip-off.

Artefact	Cellebrite	Oxygen	Axiom
WhatsApp messages	1097	0	12257
Call Logs	229	0	0
SMS	372	0	1
MMS	1	0	0
Skype messages	1	0	5
Images	4988	1002	19989
Contacts	0	0	0
Video	0	22	271
Audio	0	660	11
Potential passwords	0	3	0
Web (cookies, history)	0	0	1684
Email	0	0	161

Table 7: Data read through ISP.

Artefact	Cellebrite	Oxygen	Axiom
WhatsApp messages	≈10 000	0	1 799
Call Logs	388	0	0
SMS	3573	0	3 192
Skype conversations	11	0	8
Snapchat	0	0	109
Images	1701	24 731	66 238
Camera pictures	632	0	0
WhatsApp images	332	0	0
Contacts	928	0	0
Audio	207	210	208
Video	1	372	1
Documents	3	0	177
Emails	120	0	648
Internet of Things	0	0	3
Web related	14	868	10 981
Calendar	0	0	751

SECTION 3: Threat modelling

3.1 Threat landscape and data breach

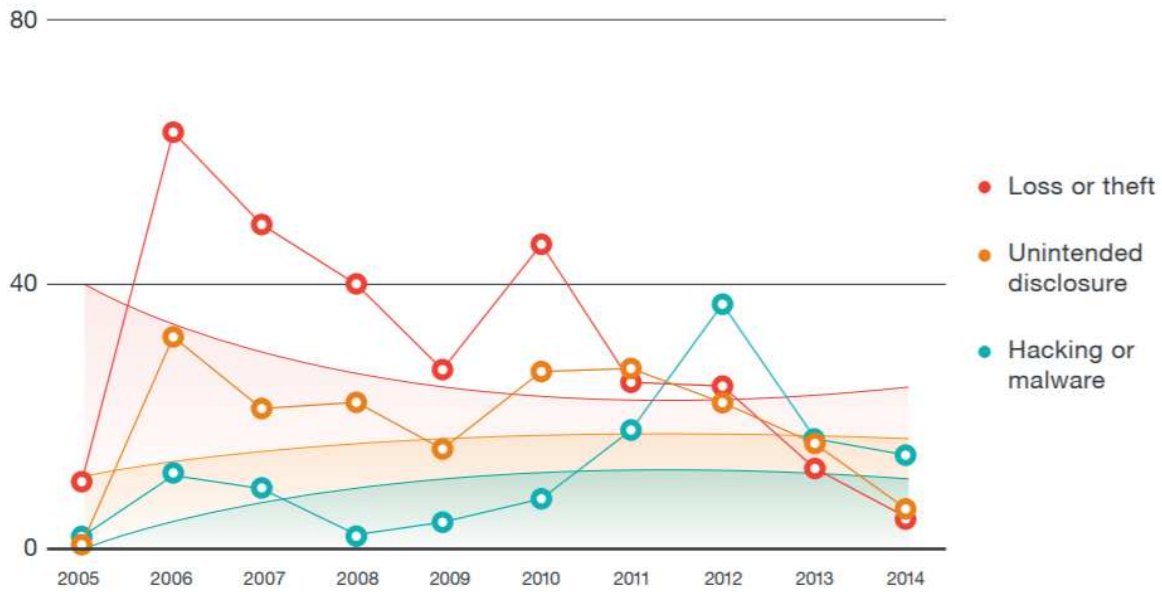
Increasing digitalization, the growth of connected device and amount of data generated and stored on smartphones today are making communication easier and more convenient than ever before. Consequently, this attracts threat actors of all kinds seeking to steal personal and corporate data, intellectual property and other sensitive information. There is, and always will be a permanent race between attackers and defenders, where it is impossible to protect against threats without having deep understanding on their motivation, targets and attack methods (ENISA, 2012).The businesses are facing the problem of data breaches despite of audits and being compliant with security standards (Uceda Velez & Morana , 2015). The emergence of new types of malicious actors coupled with more advanced attack methods constitute a menace to existing risk management programs. Hence, understanding threats is a vital element towards protecting assets that needs to be in the focus of information security professionals (ENISA, 2012). Building a detailed profile of the potential threat vectors, their motivation and capabilities as well as attack techniques will provide organizations with a clear understanding of the threat environment, enable anticipation and diminish future attacks based on detailed knowledge about these threats.

According to research undertaken by Ponemon Institute (2014), average organization has 23 000 mobile devices in use including personally owned smartphones, tables and other devices, out of which roughly 37% containing organisation's sensitive data. Due to the wide adoption of mobile computing, the probability of data loss (potentially sensitive data) is also increasing. According to ENISA threat landscape research (ENISA, 2012):

- Data breaches today have become more targeted
- More than 9 out of 10 breaches would have been prevented

Though it might look that data security considerations are mainly relevant to organizations, individual users are also at risk of their data being leaked. One of the ways users lose their data is due to devices being lost or stolen. Statistics shows that 70 million smartphones are lost every year and 4.3 percent of company-issued smartphones are lost or stolen every year (Hom, 2017). Ten years analysis (2005 - 2015) on data breaches (Huq, Numaan, 2015) identified that portable devices loss or theft is a major contributing factor in the leakage of sensitive data that remain the constant threat over the years. On the side, the number of hacking attempts steadily increases. Another identified risk is increasing insider threat for organizations. As for governmental organizations, lost or stolen portable devices was the biggest contributing factor in data breaches (Huq, Numaan, 2015). Unintended disclosure of sensitive data through mistakes or negligence is another major problem followed by hacking or malware attacks.

Figure 15: Causes of data breach for governmental organizations (Huq, Numaan, 2015).



Given the significant impact of smartphones in particular, it is important to assess the privacy and security risks associated with these devices. In this chapter we introduce basic definitions of terms related to risk:

- *Threat* - "any circumstance or event with the potential to adversely impact an asset through unauthorized access, destruction, disclosure, modification of data, and/or denial of service" (ENISA).

These cases are the perfect examples of how much data can be accumulated in a phone for 1-2 years of usage and how much can be recovered if the device is not properly sanitized. The right tools in right hand will most probably be able to recover the user data partly or fully. Therefore, reliable and verifiable data erasure of user generated content should be applied to ensure secure data sanitization.

- *Asset* - “anything that has value to the organization, its business operations and their continuity, including Information resources that support the organization's mission.” (ISO/IEC 13335-1:2004)

- *Risk* – “The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization” (ENISA). In the context of information security *risk* is calculated probability of a threat agent causing impact on an asset by exploiting vulnerability (Uceda Velez & Morana , 2015).

- *Attack vector* is a way threat can compromise the security and gain the access to the assets to leverage own interests (ENISA, 2010).

- The *likelihood* of threat depends on a relative ease to perform the attack and attractiveness of the assets (ENISA, 2010).

- *Impact* of a threat is the result of an unwanted incident determined by the value of the assets affected by attack (ENISA, 2010).

- *Incident* - An event that has been assessed as having an actual or potentially adverse effect on the security or performance of a system (ENISA, 2017).

- *Vulnerability* - The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the computer system, network, application, or protocol involved (ENISA, 2017).

3.2 Categorization of users and associated risks

Since smartphones are widely used in different scenarios and by different type of users, it is critical to understand what the users’ groups are. Use cases determine the type of data stored on the devices, level of information sensitivity and the party responsible for keeping data secure. Therefore, the likelihood, impact and risk will vary accordingly. Such classification of users is helpful to further define the requirements for secure storage sanitization. Since approaches for defining users and usage scenarios in mobile phone security context vary across countries and regions, this document uses classification developed by European Agency for Network and Information Security (ENISA), a centre of expertise for cyber security in Europe. Each user group is characterized by degree of interest from potential threats, amount of data being stored and data sensitivity. *Data sensitivity* can be classified according to the following levels:

1. **Restricted**: High sensitivity data that would results in catastrophic impact on the organization or individual(s), in case of unauthorised access or disclosure. These data include personal information, financial records, legal data, business data such as intellectual property, authentication data, etc. (IMPERVA, 2018). According to EU (Article 4(13), (14) and (15) and Article 9 and Recitals (51) to (56) of the GDPR), the following personal data is considered ‘sensitive’ and is subject to specific processing conditions:

    - personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs;
    - trade-union membership;
    - genetic data, biometric data processed solely to identify a human being;
    - health-related data;
    - data concerning a person’s sex life or sexual orientation.

2. **Private data**: Data are for internal use only. If compromised or destroyed, would not have a catastrophic impact on the organization or individual(s). Examples of medium sensitivity data are emails and documents that do not include confidential data. (IMPERVA, 2018)

3. **Public**: data is for public use. Examples include press releases, marketing materials, website content.

In its turn, security breach related to unauthorised information disclosure can have different *impact levels*: **low, moderate, and high** (FIPS PUB 199 , 2004):

1. Low impact level

Adverse impact on organizational operations, assets and individuals is limited. It might be released in a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions. Other consequences include minor damage to assets, minor financial loss or minor harm to individuals. Minor harm to individuals would not cause harm greater than inconvenience, such as, for instance, changing a telephone number.

2. Moderate impact level

Negative impact on organization is moderate in terms of normal operation, financial losses and harm to individuals. However, harm to individuals doesn't involve life threatening or serious injuries. The types of harm for individuals would include financial loss due to identity theft or denial of benefits, public humiliation, discrimination, and the potential for blackmail.

3. High impact level

Severe or catastrophic impact on organizational operations, assets and individuals. Harm at the high impact level involves serious physical, social, or financial harm, resulting in potential loss of life, loss of livelihood, or inappropriate physical detention.

It is important to note that the impact level depends on several factors which should be into account. The difference in the impact levels of the factors can significantly influence the total impact level. Factors with high impact level typically override the ones with smaller one, therefore, increasing the final score. The first factor determining the impact level is *identifiability*. This means how easily the individual or organization can be directly identified (e.g. names, fingerprints, social security numbers can directly identify an individual, while zip codes do not provide the same accuracy). *Quantity* stands for how many individuals can be identified in the information. Breaches of 35 records and 35 million records will have different impact level. The third factor is data filed *sensitivity*. For instant, medical history or financial account information is generally considered more sensitive than an individual's phone number. Organizations often require the PII confidentiality impact level to be set at least to moderate if a certain data field, such as SSN, is present. Organizations may also consider certain combinations of PII data fields to be more sensitive, such as name and credit card number, than each data field would be considered without the existence of the others. Data fields may also be considered more sensitive based on potential harm when used in contexts other than their intended use. For example, basic background information, such as place of birth or parent's middle name, is often used as an authentication factor for password recovery at many web sites. (NIST 800-122, 2010)

Based on the aforementioned criteria, smartphone users can be classified into the following groups (ENISA, 2010), characterised by the amount and sensitivity of their data, attractiveness to potential adversaries and responsibility for the IT retirement:

- **Case 1: Individual (consumer)**

The phone represents an integral part of personal life storing such data as, for instance, call logs, data from social networks and banking applications, messaging, gaming, geolocation and tracking, photos, videos, audio files, web history, emails, copy of identity and other documents, health data. These data can be used for identity stealing and unauthorised access to monetary funds. The responsibility for retirement and disposal of a smartphone devices lies entirely on individual, if not transferred to the 3rd party for further disposal.

- **Case 2: Corporate user (employee)**

The phone is used by an employee in a business or both business and private context. Besides personal data device also contains business related information such as calls history, corporate email communication, corporate specific application (e.g. expense and travel management, customer relationship management, business social networking), video conferencing, tasks management, corporate documents. Attackers are highly attracted to gaining the access to these data for monetary gain and leverage of corporate secrets and internal knowledge. Due to high security concerns, these devices are subject of IT security policy, therefore, corporate IT officers are responsible for their retirement and disposition.

- **Case 3: Governmental / high official** (ENISA, 2010):

The cybersecurity of governments and high officials represent a huge problem considering the amount of interest from threats and nation states towards getting the access to information. Also, the volume of data is huge, while the consequences of data breach are dangerous for national security. Smartphones are used by high or top-level officials in a business or governmental context. In addition to the use scenario explained above, smartphone is used for handling sensitive information and/or tasks. Consequently, smartphones are the subject of security policies, their functionality can be customised or restricted.

Likewise, the *likelihood* of threat will also vary across smartphones and device use care, i.e. whether the device is used by individual customer, within the organisational or governmental context. For instance, for certain employees the breach of contacts can reveal customer details while in context of individual users it will show only phone numbers of family and friends.

Thanks to the growing awareness of identity theft many individuals and organisations apply data erasure or physically destroy the assets before the decommissioning (ENISA, 2010). This approach is widely implemented and well-defined for computers, but not for the smartphone device. At the same time, number of retired smartphones is constantly growing.

Table 8: Likelihood of data breach (ENISA, 2010).

	Likelihood	Impact	Risk
Individual	Medium	Medium	Medium
Corporate employee	High	High	High
Governmental / High official	Medium	Very high	High

Thanks to the growing awareness of identity theft many individuals and organisations apply data erasure or physically destroy the assets before the decommissioning (ENISA, 2010). This approach is widely implemented and well-defined for computers, but not for the smartphone device. At the same time, number of retired smartphones is constantly growing. Table 8 explains the likelihood of risk occurrence for different use case scenarios where the smartphone was not properly sanitised after decommissioning and data have been present on the device allowing the attacker to access the stored information. The likelihood of attack is high for individual users due to unawareness of the threats and attack methods. This is different for other use cases, because users are more aware and protective measures have been taken to protect the data. The impact of information exposure is higher for employees and high officials due to sensitivity of information stored on their devices. The same pattern is followed by risk.

3.4 Threat background and associated attacks against secure sanitization

In the race between attackers and defenders it is impossible to protect assets against cyber-threats without having a thorough understanding on their motives, capabilities and attack methods (ENISA, 2012). Therefore, threat analysis is a vital element of information security that needs to be in the focus for security professionals. It is possible to recover data from storage in mobile technology that has not been erased properly. The densities of modern memory technology mean that there exists the potential for significant volumes of data to remain on small parts of a storage device. The data held on devices may be attractive to certain threat actors for different reasons. The effort employed to recover data will scale with the perceived importance of the data stored on a device.

Besides being more active, threats are also improving technical capabilities and become more sophisticated too (IBM, 2015).The effectiveness of an attack (determined by expressed by probabilities of success) is defined by the capability of the threat actor and the sophistication of attack methods. The data recovery techniques employed by a threat actor can vary and are relative to the amount of financial and other resources deployed. For example, some resources are readily available in the public domain with little or no investment required. Noteworthy, some data recovery techniques will require low levels of technical knowledge while others require specific expertise. Commercial tools proliferate the market and there is an active hacking community that provide a knowledge base for those who wish to develop the skills and expertise required to use such products making them easier to deploy and available to a wider pool of potential threats.

Table 9 defines different approaches to recovering data from improperly sanitized mobile devices. Included are the associated approaches to accessing data stored on a device from the normal user interface (i.e. via the phone's Operating System) through to the most advance known tactics. Additional consideration is given toward tactics that are unknown and wielded by agencies who have significant funding and access to bespoke technologies that are not available in the mainstream as COTS (Commercial off-the shelf) tools. Table 9 highlights the difference between the amount of time and effort that could be employed and outlines the type of adversary expected, according to a specified threat level. More detailed description of certain attacks is given below the table.

Table 9: Threat matrix.

Capability level	Threat	Description	Target	Motive	Associated attack
Low	Individuals	Individuals such as specific person or a group could act their own not being the member of any actor threat category and not having any particular motivation. (SurfWatch Labs, 2015) (SANS Institute, 2003) (NIST , 2002)	No specific	Curiosity, challenge, ego	*Non-invasive:* acquiring data without damaging or making any harm to the device. Access can be achieved via existing interface or free (low-cost) software tools (ENISA, 2017).
	Employees	This group includes staff, contractors, operational staff or security guards of a company. Even though they typically don't have high capabilities, employees possess insider information and significant amount of knowledge along with access to company's resources. This can potentially allow them to perform activities against the assets of their organisation, often without arousing suspicion. (ENISA, 2012) (SANS Institute, 2003) (New Zealand Government, 2014)	Corporate secrets, insider information	Revenge, financial gain, satisfying curiosity	
Medium/Low	Corporations	Some corporations (organizations/enterprises) can be considered as threat agents and be involved in offensive tactics for the purpose of acquiring confidential information of other companies. Their capabilities and level of motivation depends on their size and sector, however, generally corporations have significant capabilities, varying from technology up to human engineering intelligence, especially in their area of expertise. (ENISA, 2012)	Confidential information of other companies	Gaining competitive advantage, disrupt new product development, product copying.	*Non-invasive:* using COTS tools. Does not require in-depth knowledge, not sophisticated equipment. Though some product training is beneficial. These are the tools that typically used by police and law enforcement organizations, though some are available for business usage. The key limitation is low accessibility of forensic equipment: very few providers, some sell exclusively for police and criminal investigators.
	Investigative journalists	In their search for sensational news journalists can potentially apply data extraction techniques to make confidential information belonging to individuals or corporations or public organizations public. (Deloitte & Touche LLP, 2012)	Any information with a potential for sensation	Hot-news discovery.	
	Academia and research	The individual or a group which conducts research in the area of Information Security, data recovery, data erasure or any other related fields can potentially identify and/or implement new data extraction procedures. Thus, the result of academic research can be considered as the (non-malicious) Threat Source. (Deloitte & Touche LLP, 2012)	Exploration of new ways/methods for data extractions, back doors, vulnerabilities	Identification and performing new methodologies and techniques for data recovery, new knowledge generation	

Capability level	Threat	Description	Target	Motive	Associated attack
Medium	Hacktivists	Hacktivists are individuals (or groups) who apply digital tools for cyber-attacks to obtain personal information and internal organizational data or to protest / promote their opinion regarding certain social events (free speech or human rights). (SANS Institute, 2014) (ENISA, 2012) (SurfWatch Labs, 2015)	Corporations, intelligence agencies and military institutions	Political, ideological, social, religious, cultural beliefs, demonstration against authorities	Methods vary from non-invasive to semi-invasive: *Non-invasive*: Android physical acquisition based on firmware update protocols. A physical acquisition of Android smartphones can be achieved using the flash memory read command by reverse engineering the firmware update protocol in the boot loader. (Yang,, et al., 2015) *Semi - invasive* (eMMC chip is accessed through TAP (Test Access Points) to communicate with chip and issue read commands. These interfaces are used by manufacturers during production and testing for boundary scans and solderless IC components' re-programming. Besides physical connection to the interface a separate programmer (a.k.a. flasher box/ hex dumping tool) is required to execute the commands on eMMC chip. Examples of such approaches are UART, JTAG, eMMC ISP.
	Skilled hackers	Skilled hackers are very similar to hacktivists in their behaviour and utilized tools and methodologies, however, they aim to get monetary gain when performing the attack. Their target is to steal users' data in return of payment. (SANS Institute, 2003) (NIST , 2002)	Bank and card credentials, bank accounts, information systems	Monetary gain, extortion, challenge, ego, thrill of the chase, addiction	
Medium / high	Cyber criminals	Cyber criminals' hacks are hostile by nature and characterized by being organized in large communities (local, national or even international level with a certain degree of networking), well-funded (or state sponsored), patient and persistent. Financially driven cyber criminals are described to be less persistent than espionage motivated ones whose goal is to control the object in the long run. (SANS Institute, 2014) (ENISA, 2012)	Bank and card credentials, bank accounts, information systems, confidential data	Monetary profit (e.g. credit card numbers, bank information) or espionage (e.g. social media and email account information). Acquired data can be further sold on the black market	*Invasive*: these methods involve desoldering the components, which requires advanced equipment and skilled attackers. Commonly used method is *chip-off*, when the memory IC is removed from the motherboard and reworked to be further read through a chip reader or via direct wire soldering. This approach is typically the last resort in case other methods failed or severe physical damage of the device. The shortcoming is technical complexity caused by multiple thermal operations while IC desoldering. In addition, ICs commonly apply underfilling which makes save chip removal even harder. Another example is microprobing and direct raw NAND flash read.
	Crackers	These are type of hackers that posse good technical knowledge to commit crimes such as vandalism, destruction of property, fraud, theft, corporate or government espionage, and terrorism. They understand that act illegally and attempt to enter systems undetected and leave minimum evidence. This makes them very difficult to identify and catch (MHEducation, 2016) (NIST , 2002)	Secret information, trade and military secrets	Financial gain, corporate or government espionage, stealing intellectual property, trade and military secrets, challenge, ego, thrill of the chase, hack addiction	

Capability level	Threat	Description	Target	Motive	Associated attack
High	State Sponsored Threat Actors / Nation States	State sponsored threat actors have almost unlimited technical capabilities, highly resourced and sophisticated, deploy tactics unknown in the field being well financed and organized and act in very large number of attackers. These attackers are individuals who have been hired by state agencies. They aim to perform cyber espionage, compromise data, sabotage computer systems, and in certain circumstances to even commit cyber warfare. (SANS Institute, 2014)	Commercial and/or government systems, credentials data, internal organizational data, trade secrets, system information.	Espionage and political reasons, compromise data, cyber war.	*Invasive*: Extensive attacks of the highest sophistication that can be performed on extremely damaged, partially destroyed storage media. Techniques vary from all the mentioned above to currently unknown developed by highly resourced and sophisticated intelligence agencies. (CESG, 2014) Example: Micro Read. These methods involve the use of a high-powered microscope to view the physical state of gates (NIST, 2014).During micro-read the chip is removed and is then read by carefully removing the top layers of silicon. The reading is performed through exposed interfaces directly from the raw NAND bypassing the controller. Alternatively, the gates are read manually one at a time and the binary data is converted to hex. The resulting hex can then be converted to data blocks. This process is expensive and time-consuming. Also, it requires an ample knowledge of hardware and file systems. This is the most time-consuming method known. (NIJ, 2014).
	Terrorists	Capabilities of terrorist vary from low to high, however, terrorist organizations being characterized by high level of organization and management have expanded significantly together with their area of performing activities which now also covers cyber-attacks.	Military and commercial secrets, governmental information, confidential information	Potential targets are critical infrastructures such as e.g. public health, energy production, telecommunication due to great impact of failure of these on society and government. The performed activities are undertaken to cause alarm or panic.	

UART (Universal Asynchronous Receiver/ Transmitter): This attack involves communicating through UART interface to issue read commands to the flash memory. Some manufacturers enable UART connection through switching a headphone jack into a serial connector (Munro, 2014), others via USB port (multiplex attack) (Ossmann & Osborn, 2013) Connection to the UART interface is also possible through dedicated UART ports on the PCB, which requires a pinout for specific device model. The main drawback of data read through UART is extremely slow speed due to the fact that this interface is not intended to be used for data acquisition but for hardware and components testing and debugging. Moreover, the interface can be purposely disabled by the manufacturer, which represents another limitation of this method.

JTAG (Joints Test Access Group): JTAG is another type of debugging interface, which allows communication with a memory and further data read through the JTAG port. Although it takes long to dump the memory content, the benefit of this approach as well as UART is potential opportunity to keep the device in a working condition (if only the access to JTAG ports doesn't require breakage of device, since many phones are now glued). Additionally, these methods can be applied if the device has been damaged (e.g. battery fault, cracked screen) but PCB stayed functional. Access to the JTAG points can be provided either by soldering or, for certain phones, by attaching the JTAG adapter to the PCB.

Since both UART and JTAG can be accessed through soldering to the TAPs or connected to the adapter, these methods can be both non-invasive or semi-invasive. UART and JTAG ports are only the access points to the device internals, the actual communication with the internal memory is done through e.g. hex dumping tools.

eMMC ISP (In-system programming) is flash programming interface allowing direct communication with eMMC chip through the test points on the PCB. This type of data transfer is significantly faster than UART or JTAG. However, eMMC ISP pinout for every variation of the device model is required to perform data read. Complexity of this approach is also released in physical location of the pins on the PCB: they may be hidden under other ICs and, therefore, inaccessible. Certain manufacturers feature double-sided pinouts (pins located on both sides of the mother board), making access more difficult. Same as UART and JTAG, a programmer is required

Hex Dumping tools (a.k.a. boot loaders): connecting the mobile device to the forensic workstation through flasher box and JTAG / ISP interface of mobile device PCB. They dump the memory from the device to the computer. Flasher boxes communicate directly with mobile memory storage avoiding interaction with mobile operating system. Importantly, the phone should be started via operation of external or non-device resident start-up program, not the phone's firmware. If bootloaders are configured wrong or improperly they can permanently damage a phone. The process is inexpensive and allows recovery of deleted data. Due to the reason that acquired data raw image is in a binary format, certain technical expertise is mandatory to undertake analysis. (NIJ, 2014)

Chip-off: The chip-off is invasive data recovery approach that requires de-soldering of the memory chip(s) from the circuit. In this case, the microscope is required to remove the chips from the device without any damage. Additionally, certain skills and experience are needed to mitigate the risks associated with mistakes that can result in permanent loss of all the data on the device. As soon as the chips are successfully extracted the data they store can be read. The de-soldering of eMMC chips is not an easy task due to multiple connectors on the underneath (BGA) that are directly soldered onto the motherboard. Chip-off extraction provides a very comprehensive view of the information stored in the device. However, data interpretation may be challenging and time consuming. Often, manual reverse-engineering is required. (Data Recoup, 2016) (NIJ, 2014).

Microread with fine electrodes - attaching microscopic needles onto the internal wiring of a chip, eavesdropping on signals inside a chip injection of test signals and observing the reaction. Can be used to read internal secrets that are not intended to leave the chip, fault attacks or extraction of secret keys and memory contents limited use for 0.35µm and smaller chips. (Skorobogatov, 2011) (TUM, 2014)

Direct raw NAND flash read: According to the recent research performed by Rusolut (Rusolut, 2016) (Rusolut, 2018), among all the pins present on the eMMC chip there are vendor proprietary pins for communication with the raw NAND of the eMMC through NAND interface. Research done within our project shows that these pins are often hidden deeper in the eMMC structure under protective layers (coating).

3.5 The rise of threats and cyber security challenges

According to Bruce Schneier, a world-renowned industry expert, the cyber security adversaries may be categorized as follows (Schneier, 2000):

- Hackers
- Lone Criminals
- Malicious Insiders
- Industrial Espionage
- Press
- Organized Crime
- Police
- Terrorists
- National Intelligence Organizations
- Infowarriors

Even though many years have passed since writing the book, the list is still quite accurate. Mr. Schneier states, that the main attack types are criminal attacks, privacy violations and publicity attacks (Schneier, 2000). We will scrutinize these threats and adversaries in greater detail in the following paragraphs.

Several of the listed adversaries would be interested in the contents of a mobile phone that has reached the end of its lifespan in the hands of the original owner. For example, lone criminals and organized crime would be interested in credit card information stored in the phone, while individuals who operate in the field of industrial espionage are interested in any kind of corporate secrets.

Peoples use patterns change, and it becomes more common to do things with smartphones, and thus the attackers also change their attack patterns. For example, identity theft is a real threat, if a smartphone end up in criminal hands with all its data intact. According to Javelin Research's, 16.7 million US consumers were victims of identity fraud in 2017 (Pasqual at al., 2018). The study claims that the fraudsters stole 16.8 billion US dollars from the victims.

According to another source, Internet of Things devices are the biggest technology crime driver in 2018 (Morgan, 2017). It is common that people manage the IoT devices with their mobile phones, and thus if someone can for example phish the account data and passwords from someone's smartphone, that may allow other kinds of crime – for example remotely opening the intelligent locks of a house to let the thieves in, when the smart systems of the house have first detected that the family is not present in the house.

According to Irish Examiner article, cybercrime is bigger than global drug trade (Hoare, 2017). The article quotes Europol statement that global impact of cybercrime has risen to $3 trillion, making it more profitable than global trade of marijuana, cocaine and heroin combined.

SECTION 4: Risk evaluation

4.1 Potential impact of risk materialisation

The negative consequences that can occur due to improperly sanitized devices are (Ponemon Institue, 2014):

- Leakage of information assets

  Information assets may contain wide variety of data, from customer-related information to strategic assets of a company. Realising the extent of a leak, verifying the leaked data and restoring and securing data storage is time-consuming, disruptive and costly operation.

- Reputation damage

  Reputation of a company or organization is a perceived value defined by public based on available information and actions of said company or organization, so damage to reputation is similarly based on public view on incident, and communication and actions related to incident. Reputation damage usually affects adversely to operation, causing unnecessary difficulties to normal operation. Further, reputation damage alone may impair goodwill of the company, resulting in diminished balance sheet value and depreciated stock price.

- Business disruption.

  A leak causes business disruption due to resource diversion. Varied amount of resources from within a company or organisation and possibly paid external resources are needed to assess the situation after the leak,and are tied to plan and execute corrective actions needed to rectify the situation for normalizing operation. These resources are limited or exempt from day-to-day operations of a company or organization.

- Damage of IT system

  Damage caused to IT systems may include reassessing operating procedures, revaluation of service provider contracts, renewal of IT assets, training of personnel and possible relocation to operating premises.

- Customer turnover

  Customer turnover may be affected, if leaked assets contain business-critical information related to customers. These may contain for example RFTs, RFQs, and other internal financial information, trade secrets, IP etc. Having these in public knowledge have adverse effect to customer turnover as increasing number of customers take their business to another company.

- Regulatory actions or lawsuits

  Usually companies are liable for the data entrusted with them. If data breach occurs, companies or organizations may face penal obligation to compensate the damages caused by an incident to contractual parties. After GDPR compensation obligation of up to 4% of annual global turnover is extended to anyone whom the incident affects (in EU countries). This may have severe implications to the extent of liabilities and amount of compensations.

- Costs of consultants and experts

  Solving the incident may need additional expertise in form of hired consultants and experts, which adds unnecessary cost outside of a budgeted amount, which in turn may be detrimental to an operation of a company or organization.

4.2 Risk tolerance

Risk tolerance means comparing risk assessment to the gained benefit in spite of risk realization. If the benefits outweigh possible consequences of risk realization, it can be said risks are tolerable. If not, then risk tolerance cannot be achieved. Risk assessment for the individuals may differ greatly from risk assessment of corporate and institutional entities, latter being more uniform and parallel to each other, than in the case of former group, where tolerance factors may even be exclusive between individuals. Risk tolerance can be increased via inventing or using methods, which reduce accompanied risks, or by increasing the value of benefits compared to risks and possible consequences. It may also be feasible to use damage control methods and elements after risk realization in order to counter the negative effects, but usually it is better to decrease the risks, and their consequences beforehand.

4.3 Risk mitigation

Information security starts with proper data handling policies, which benefit both organizations and companies, as well as individuals. Consistent policies and procedures minimize the risk of data breach, and proactive measures are vastly better than reactive measures. Such policies should consider at least the following points:

- Restricting the amount of data in device (store only necessary data on device, otherwise store it in data repositories)
- Usage of data repositories away from mobile device (maximizing the usage of e.g. cloud services to access data, when needed)
- Proper storage of devices (for restricting outsider access to device)
- Usage of strict authentication methods (for restricting outsider access to device)
- Enabling device encryption (limiting usability of in case of breach)
- Removal of data after the intended usage period (limit the time window of data exposure)

Risk mitigation follows simple rules, which are based on controlling the visibility of data exposed via mobile devices, and the smaller the window of opportunities is, the lesser the accumulated risk of a breach are.

SECTION 5: Evaluation of existing data erasure solutions for smartphones

5.1 Level of media sanitization

To understand different levels of media sanitization, it is good to first review the different attack capabilities of various threat actors. Lowest level of attack sophistication is just browsing through files, trying to find something interesting. At this level of attack sophistication, the attacker does not use any kind of software or hardware tools to find data, they just use the device as any normal user would.

Next level of attack is often called “keyboard attack”. It means using commercial off-the shelf software (COTS) solutions to find erased files. Executing this kind of attack requires some understanding about the underlying technology and some money, although many COTS data recovery software solutions can be bought from the internet relatively cheap or even for free.

The highest data recovery level is often called “laboratory attack”. This attack level actually consists of several sublevels, but common to all of them is that they require high level of technical knowledge and modest to high level funding to execute. Laboratory attack may for example consist of removing the flash chips from the device and reading their contents with a special chip reader or using JTAG analyser to get direct access to the data stored in the device.

NIST Special Publication 800-88 Revision 1 defines erasure levels in the following way (NIST SP 800-88, 2014):

> Clear applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques; typically applied through the standard Read and Write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported).
>
> Purge applies physical or logical techniques that render Target Data recovery infeasible using state of the art laboratory techniques.

The “clear” and “purge” are the two industry-standard levels of media sanitization. Each device sanitization method should be evaluated, as to define whether that method offers clear of purge level security. Depending on the sensitivity of data a device contains, clear level solution may be good enough (if the device did not contain anything very sensitive to begin with). However, if in doubt, purge level solutions are always considered safer than clear level solutions.

5.2 Overview of erasure options

As described in the previous chapter, each sanitization method should be defined whether it offers clear of purge level security. In this chapter we address this topic in more detail and introduce the methods that can be used to achieve data sanitization. The categorization of sanitization methods in the below table is based on the definition of International Data Sanitization Consortium (IDSC, 2018) in context of NIST SP 800-88.

Table 10: Categories of sanitization methods.

Level of sanitization, according to NIST SP 800-88	Sanitization method	What is does	Challenges
N/A	Data deletion	Hiding data on a storage device, whereby the data is available for overwrite. Until the data has been overwritten, the data is still easily recoverable.	Data easily recovered.
	Reformatting	Reformatting is performed on a working disk drive to eliminate its contents. By formatting, it leaves most, and sometimes all, existing data on the storage device.	Data easily recovered.
	Factory reset	Removes all user data and restores a device back to factory settings, providing the device is not rooted.	Data exposed on Android OS.
Clear	Data wiping	Process of overwriting data, without verification that the overwriting was successful in overwriting all sectors of the storage device.	No verification of the result, does not produce a certified report.
	File shredding	Destroying data on individual files and folders by overwriting the space with a random pattern of 1s and 0s.	No verification of the result, does not produce a certified report.
Purge	Data erasure	Securely overwriting data from any data storage device using zeros and ones onto all sectors of the device.	Requires use of a third party data erasure software and information on the storage device so that appropriate erasure standard may be applied.
	Crypto Erasure	The process of using encryption software (either built-in or deployed) on the entire data storage device, and erasing the key used to decrypt the data.	Practical only on self-encrypting drives, unless a third party encryption software is used.
	Degaussing	Physical destruction whereby data is exposed to the powerful magnetic field of a degausser and neutralized, rendering the data unrecoverable.	Degaussing can only be achieved on hard disk drives (HDDs) and most tapes.
Destroying	Physical desctruction	Shredding hard drives, smartphones, printers, laptops and other storage media into tiny pieces.	The storage device is lost in the process.

Many national authorities provide more detailed instructions on how to sanitize storage media. Further, some organizations maintain their own specifications or standards on how to perform overwriting in order to achieve compliance. As an example, the following guidelines are from IT Media Sanitization publication (ITSP.40.006 v2), issued under the authority of the Chief, Communications Security Establishment, CSE (Government of Canada, 2017).

a) SANITIZING ENCRYPTED IT MEDIA

Apart from self-encrypting drives, encryption can be instituted for other Media as well; such encryption can assist departments to provide for continuing protection of the data beyond the life cycle of the media.

A wide range of data storage devices, including high-end smartphones and tablets, are able to support the encryption of all user data that is stored in their memory. Devices encrypted throughout their life cycle using CSE-recommended solutions are easily sanitized and decommissioned.

The CE requires the encryption key or key-encryption key to be stored in a known location (e.g. Trusted Platform Module (TPM) chip, removable hardware token, smartcard) where it can be targeted for erasure and verification. Even in cases where key erasure cannot be positively verified (e.g. because it is stored with the user data in flash-based media that does not include a verifiable key-erase function), CE is still used but should also be followed by clearing all data. This is an additional safeguard against the possibility of forensic recovery of the key following disposal.

The sanitization steps for encrypted media include:

1. Erasing the key (or re-encrypting with a strong key then erasing the key used for re-encryption.)
2. Clearing the Media as an additional step when key erasure is not verifiable
3. Removing external markings or labels that indicate government ownership or data sensitivity
4. Documenting sanitization steps performed
5. Disposing of the Media through controlled channels

a.1. CRYPTO ERASE (CE)

Sanitization of Media using CE is the practice of securely deleting the encryption key used to encrypt the data on the Media. Although the encrypted data remains on the Media, without the encryption key the data on the Media is unrecoverable and the Media is sanitized.

Media sanitization using CE is suitable for sanitizing encrypted HDDs, solid-state drives, and other flash-based storage devices – providing that encryption has been used from the beginning of the Media's life cycle. When used for sanitization as follows, CE is equivalent to overwriting and SE, whether it is a self-encrypting drive or has after-market whole-drive encryption:

1. Use of FIPS 140-2 validated cryptography
2. Employ encryption throughout the life cycle of the Media
3. Securely manage the password and encryption key
4. Reliably destroy or securely delete the password and encryption key

An enhanced version, CE Enhanced, involves re-encrypting all of the data on the Media with a strong, random, one-time key that is securely deleted after use. To ensure that cryptographic keys can be reliably erased, they should be stored in the Trusted Platform Module (TPM), which is available on fixed platforms such as desktop or laptop computers, or in a removable hardware token or smartcard, as in the case of portable devices such as smartphones and tablets.

Following the CE procedure, an additional step can be followed to clear the Media by overwriting or securely erasing all accessible storage locations. The combination of CE and clearing is particularly useful for flash-based drives because they are more difficult to analyse in order to verify the results of CE or clearing.

b) SANITIZING NON-ENCRYPTED IT MEDIA

Decommissioning procedures for Media that pre-dates or does not fall within the scope of current departmental encryption policies include:

1. Overwriting or securely erasing the device to overwrite all accessible storage locations with a known pattern

2. Verifying the results by representative sampling with media analysis tools to confirm the presence or absence of any data other than the expected pattern

3. Removing external markings or labels that indicate government ownership or data sensitivity

4. Documenting sanitization steps performed

5. Disposing of end-of-life Media through controlled channels

b.1. ERASE AND RESET TO FACTORY DEFAULT

Erasing and Resetting are logical methods that may be available as a product feature in many storage-capable devices (e.g. cell phones, tablets, routers). Normally, the data is not truly erased, or it might not be possible to verify its erasure. Erase and resetting to factory default settings makes the data inaccessible through the device's standard user interface, which serves to protect the data against passive or casual access. This method may be suitable for sanitizing devices such as network routers, basic cell phones and Voice over Internet Protocol (VoIP) phones that contain limited amounts of low-sensitive configuration or user data.

The erase-and-reset steps for selected Media include:

1. Revoking, removing or replacing any cryptographic certificates

2. Using the built-in erase feature to delete pointers to user data or (in the case of encrypted data) to delete cryptographic keys

3. Resetting the device to factory default

4. Removing organization markings and labels

5. Disposing through controlled channels

b.2. OVERWRITING AND SECURE ERASE (SE)

Overwriting and digital SE are methods to sanitize data storage media for reuse or disposal. They are used to sanitize media containing low-to-medium sensitive data; they are also used in conjunction with physical destruction for Media containing highly sensitive data.

Overwriting and SE are:

1. Very effective for magnetic media

2. Ineffective or unreliable for many flash-based media (but may be effective for some)

3. Not used for optical media

For solid-state drives, a double overwrite-pass or a single SE process is recommended – if either function is adequately supported by the design of the particular device, and if the device does not have retired “bad blocks” that may contain sensitive unencrypted data.

Positive verification of results is essential to provide the needed degree of security, especially for medium sensitive data and solid-state media. Data removal processes must be verified in each case in order to confirm the presence or absence of the expected sanitization data values across a wide sampling of all data-storage areas.

Departments should select overwrite products that are independently evaluated (e.g. Common Criteria), with user feedback features to help assess the success or failure of erasure tasks. Separate tools should be chosen and used for the verification step.

c) DESTRUCTION METHODS

Physical destruction methods commonly available to departments are not recommended as a stand-alone sanitization method. Their effectiveness is becoming less effective due to the advent of Media with smaller and denser physical memory components, combined with technological advancement in the ability to recover non-sanitized data from memory remnants. Destruction should be preceded by best-effort encryption or erasure (to ensure that Media fragments cannot be read), and removal of external labels and identifiers (to reduce unwanted attention to the Media remnants). Media disposal should only be processed through controlled channels (refer to Annex B - Sanitization Standards for RCMP destruction standards for Media).

Destruction is the final step for declassification of media that:

1. Has no donation or commercial re-use value

2. Contains medium-sensitive data that failed sanitization efforts or sanitization verification

3. Contains high-sensitive data, whether or not it is sanitized

Requirements for media destruction are based on IT security factors such as data erasure prior to destruction and the assessed level of residual sensitivity following erasure. This also includes environmental factors such as the through-put rate, noise, and harmful dust generation associated with the destruction product being used.

5.3 Performance Evaluation of Factory Reset

According to Khramova & Martinez, the factory reset function built into Android operating system seems to be good enough to protect against casual browsing of the data without use of any kind of data recovery software (Khramova & Martinez, 2018). With increasingly advanced attack methods, more data was recovered from the tested phones. Table 11 illustrates the rate of data recovery with different tools.

Table 11: Results from a study by Khramova & Martinez, where data recovery techniques of different sophistication were used to restore user data from second-hand smartphones (Khramova & Martinez, 2018).

The level of sophistication	Technique/tools	Sample size	Units failed
Low	Manual inspection	68	0
Low-Medium	Forensic imagining (COTS tools)	62	12
Medium-High	JTAG/eMMC ISP/Chip-Off	12	1
High	Bespoke tools	1	1

The main contribution of the study (Khramova & Martinez, 2018) was that while factory reset is good enough to protect against manual inspection of a smartphone, more advanced techniques can still recover data from phones that have been erased with factory reset.

Data Recovered with COTS Tools (Forensic Imagining)

Research (Khramova & Martinez, 2018) used several commercial off-the-shelf (COTS) mobile forensic tools such as Magnet Axiom (demo), Oxygen Forensic Detective (full version) and Cellebrite: UFED Touch and Physical Analyser (demo). The amount of recovered data varies depended on many factors such as the memory type, phone model, Android OS version, manufacturer, etc. The findings suggest that factory reset process is more prone to improper data sanitization in older versions of Android OS. Still, it was shown that user data is recoverable with COTS tools at least up to OS version 4.4. The recovered user data included for example multimedia files, documents, emails, messages, contacts, call logs and browser history. In addition, metadata such as folder path, time stamp, author and even geo location were recoverable in some cases. Below image shows an example of data recovered with COTS tools (Khramova & Martinez, 2018).

Figure 16: Examples of user data recovered from a second-hand smartphone (Khramova & Martinez, 2018).

Data Recovered with Advanced Tools

The research (Khramova & Martinez, 2018) was able to recover user data directly from the eMMC chip of one of the smartphones running on an older Android OS by using advanced ISP and JTAG methods. More importantly, the research was also able to recover multiple text messages from one phone running on Android OS version 5.0.1 by using a very advanced methodology and bespoke tools. This would suggest that factory reset might still fail to permanently erase user data even on later Android versions. Below image shows an example of the data recovered by using this very advanced methodology, which involved removing the eMMC chips and reading their contents directly using special tools and software.

Figure 17: Text message recovered from a second-hand smartphone (Khramova & Martinez, 2018).

Number	Deleted	Read	Type	Folder	Timestamp (UTC+0)	From	To	
1	yes	no	SMS	Inbox	09.04.2018 6:36:07	+35840021[redacted]		Message 2: received
2	yes	yes	SMS	Sent	09.04.2018 6:34:59		040021[redacted]	Monday message 2 to[redacted]
3	yes	yes	SMS	Outbox	09.04.2018 6:34:57		040021[redacted]	Monday message 2 to[redacted]
4	yes	yes	SMS	Sent	09.04.2018 6:31:22		040021[redacted]	Monday message to[redacted]
5	yes	yes	SMS	Sent	09.04.2018 6:31:21		040021[redacted]	Monday message to[redacted]
6	yes	yes	SMS	Sent	06.04.2018 7:15:38		+35841[redacted]	To have the .db files with some info
7	yes	yes	SMS	Sent	06.04.2018 7:15:37		+35841[redacted]	To have the .db files with some info
8	yes	yes	SMS	Sent	06.04.2018 7:15:12		+35841[redacted]	Simply logs
9	yes	yes	SMS	Sent	06.04.2018 7:15:10		+35841[redacted]	Simply logs
10	yes	yes	SMS	Drafts	06.04.2018 7:05:35			Drive[redacted] Samsung Galaxy S4
11	yes	yes	SMS	Drafts	06.04.2018 7:05:08			Drive[redacted]Galaxy S4
12	yes	yes	SMS	Drafts	06.04.2018 7:04:22			Drive[redacted]S4
13	yes	yes	SMS	Drafts	06.04.2018 7:03:41			Drive[redacted]

Conclusions on Effectiveness of Factory Reset

As Khramova & Martinez state, factory reset is not effective enough to protect against advanced data recovery methods. While no user data was found by simply navigating the user interfaces of the tested phones, the more advanced attacks were still efficient in recovering data after factory reset.

Among the data recovered in the study (Khramova & Martinez, 2018) were Google account passwords, photos, SMS messages and other personal information. The main finding of the study was that factory reset is not good enough to protect valuable data held in the smartphone. This is especially true if the phone was in company use, so that it contains company secrets, or in a case when the phone contains some other highly valuable data.

Google's design document for Android 6.0 states that devices must use full disk encryption, with some caveats (Android 6.0 Compatibility Definition 2015). This is important, because recovering data from device which uses full disk encryption is much more difficult by using advanced chip-off methods. However, the document states that if the device has AES encryption performance below 50 MiB/sec, or if the device does not have a lock screen, it is allowed to ship to the customers without full disk encryption. Also, if the device was shipped with an older Android version, and updated to Android 6.0 or later, it is also allowed to not have full disk encryption. These statements can be compared to Android 9.0 design document [https://source.android.com/compatibility/android-cdd.pdf], which outlines how full disk encryption must be implemented, if the device supports it; however, that latest document does not explicitly define the rules for when full disk encryption must be implemented.

Due to these caveats, it is possible that some smartphones sold today may not have full disk encryption on by default. In those cases, they are vulnerable to advanced chip-off techniques. This fact makes this research paper relevant to even those cases when the smartphone is modern and comes with a current Android version.

5.4 Data sanitization methods with regard to threats and compliance

This chapter will tie together some of the topics in previous chapters. First, the data security threats that were divided into three categories in section 3.4 are linked to the sanitization methods described preceding in chapters 5.1 and 5.2. The goal is to describe the appropriate methods that could be used to counter the threat in each case. Second, the sanitization methods are considered in terms of data sensitivity addressed in section 3.2.

Low capability level threats

As described in previous chapters, curious outsiders that are not members of any larger organization could pose a low-level threat to information security. Further, company employees with no particular skill, but access to insider information could also pose this sort of a threat. The methods this sort of actors would typically employ are non-invasive and typically limited to simply browsing through files existing on the device or using a commercial off-the shelf software (COTS) solutions to find erased files.

Some organizations, such as small-size companies and motivated individuals with resources, such as investigative journalists or academia researchers might apply data extraction techniques to access confidential information. However, actors such as these are likely limited to non-invasive methods due to limited accessibility to forensic equipment.

This sort of low-level threats may be countered by any clear or purge level sanitization methods or physical destruction of the storage media, as described in previous chapters. In particular, this may be done by sanitization methods that include either changing the decryption key of an encrypted drive or overwriting the space. Simply deleting the files might leave the data recoverable by COTS tools.

Medium capability level threats

Other organizations, such as big corporations and highly-skilled individuals, such as hacktivists and cyber criminals might employ invasive methods involving de-soldering the memory chips and accessing their contents by using a chip reader. While very few manufacturers sell equipment such as this for use outside law enforcement, some laboratories provide commercial data recovery services. Further, given enough funding, knowledge and motivation, it may possible to build a setup capable of invasive data recovery from commercially available equipment.

While clear level solutions are sufficient to sanitize logical data, some data may still be left recoverable on the physical level. Consequently, medium-level threats posed by actors such as those described above, may only be countered by purge level sanitization methods or physical destruction of the storage media, as described in previous chapters. In particular, this may be done by verified methods that include either changing the decryption key of an encrypted drive or overwriting all addressable space. The distinction to solutions including clear level overwriting methods is that overwriting is done in accordance with a specified standard and that sanitization result is verified, which is usually evidenced by a certificate.

High capability level threats

High-level threat actors are typically state-sponsored and characterized by almost unlimited technical capabilities and resources. These actors are capable of very sophisticated invasive methods that may be performed on extremely damaged and partially destroyed storage media. Consequently, physical destruction of the storage media alone may not be sufficient if not done efficiently. For example, shredding of each flash memory chip would have to be ensured. In conclusion, this sort of high-level threat actors are best countered by purge level sanitization methods.

Regulatory compliance of data sanitization methods

In terms of regulatory compliance, an organization needs to consider the type of data that is being stored on the storage media. In section 3.2 data sensitivity was classified into three categories: Restricted, Private and Public. Different regulation may be applied, depending on the sensitivity of data. In case of a data breach, sensitivity of the data has an influence on the resulting fines and damages.

As described in section 3.2, data revealing personal information is considered restricted data, which is subject to specific processing conditions, in accordance with the EU General Data Protection Regulation (GDPR): Organizations that collect, store and use this sort of data are accountable for responsible data management (Blancco Technology Group, 2016). While GDPR does not impose any particular sanitization method at the end of data lifecycle, complying with the accountability requirement may be evidenced by using verifiable sanitization method, such as any purge level method, according to section 5.2.

As described further in section 3.2, data including trade secrets, such as intellectual property, financial records or legal data, is also considered restricted. Fines for data breach of this sort of information may depend on national legislation, however, more importantly the company may be liable to compensate for the damages caused by the breach. As described in section 4.1, the negative consequences caused by improperly sanitized devices may be massive. Consequently, implementing at least a clear level data sanitization method, according to section 5.2, or physically destroying the storage media is highly recommended to prevent easy data recovery by curious outsiders, grudged company employees or investigative journalists.

Section 6: Guidelines

6.1 Recommended action to secure data

About data classification

In section 3.2 data sensitivity was classified into three categories: Restricted, Private and Public. However, there are many definitions on this topic, as almost every country has its own data classification guidelines. Many of these guidelines are themselves classified and hence not available to the general public. One of the publicly available classification guides, for example, is UK "Cabinet Office Government Security Classifications, May 2018", which defines three possible classifications.

Table 12: Classification of documents, according to "Cabinet Office Government Security Classifications, May 2018".

Classification	Definition
Official	The majority of information that is created or processed by the public sector. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile.
Secret	Very sensitive information that justifies heightened protective measures to defend against determined and highly capable threat actors. For example, where compromise could seriously damage military capabilities, international relations or the investigation of serious organized crime.
Top Secret	HMG's most sensitive information requiring the highest levels of protection from the most serious threats. For example, where compromise could cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations.

Data may later be unclassified, which means that it is no longer considered to be sensitive enough to warrant any special actions to limit its use or availability.

Companies and individual users generally do not classify their data, but still they should think about how sensitive the material is that they have in their smartphones. For example, a phone that contains some corporate plans and work-related e-mail messages might be considered a container for "secret" data, if releasing that information to general public or the competitors could cause problems to the company's operations.

Individual Users

For an average person, the most sensitive items held in a smartphone are probably the personal information such as names, addresses, opinions stated in e-mails and SMS messages and other similar items. Additionally, it is likely that the phone contains credit card information, login details for different services, and other data that might be used for fraud or identity theft.

An average user cannot be required to classify the sensitivity of the data their smartphone contains. Instead, they should always assume that their phone contains at least some data that they do not wish to disclose to third parties. Also, an average user probably is not aware whether their phone encrypts the data or not. Thus, they should assume that their model does not feature data encryption.

Based on these assumptions, the safest course of action when repurposing the old smartphone is to sanitize the phone using some trustworthy software for data sanitization: The software should employ at least a clear level method, as described in section 5, and overwrite the data and/or perform crypto erase – just doing factory reset is not safe enough practice.

Companies and Governmental Organizations

The IT departments of companies and governmental organizations probably have the ability to evaluate how sensitive data some employee's smartphone contains. A good practice is to have guidelines for the employees stating that the employees should avoid storing sensitive data on their phones, if that is feasible. When purchasing the phones for the employees, the companies and governmental organizations should make sure that the phone models use intrinsic full-disk encryption, because that effectively protects against advanced chip-off attacks.

For companies and governmental organizations, the ability to prove that an asset was sanitized before it was repurposed is highly important. For this reason, they should use software that generates a digitally signed report, which proves that the asset was correctly processed. Even when the smartphones use intrinsic full-disk encryption, it is better to use software that either overwrites the storage or performs crypto erase in addition to doing factory reset.

Recommended action for disposing non-functional devices

As discussed in section 5.4, data may be recovered from damaged and partially destroyed devices by invasive methods that access the memory chip directly. Consequently, partial physical destruction of the device is not sufficient to eliminate the risk of user data being recovered. Examples of partial physical destruction methods are “hammering” or partial shredding of the device hardware. In case damaged or otherwise non-functional device may still store highly sensitive information, shredding of each flash memory chip would have to be ensured to safeguard this information.

Recycling Plants

IT Asset Disposal (ITAD) companies do not know what information the phones they process contain. However, in most cases their customers require some particular level of safety (for example, employing a “purge” level sanitization method), or the customers demand that the assets are processed according to some guidelines (for example NIST 800-88 R1). For this reason, ITAD customers should use software that offers several well-established erasure methods.

Additionally, it is essential for recycling industry that they can prove smartphones were erased properly, for example, if the audit scheme employed by a customer so requires. For this reason, ITAD companies need to use software that is able to generate a digitally signed erasure report.

Actions for Those Using Only Chips

If some company uses recycled chips, they should require that the phones were properly sanitized before the chips were removed from them. This is important, because if some previous users’ data were found from a device that uses recycled components that would create unnecessary problems for the company and the user whose data was not properly sanitized.

While requiring erasure reports to be attached to every recycled component might not be feasible, the companies using recycled components should require audits to be held in the companies providing the chips. Those audits should make sure that phones are properly sanitized, using a software that generates digitally signed reports.

Memory Manufacturers and Phone Vendors

At this point in time, using intrinsic full-disk encryption that is always on is the best protection against advanced chip-off techniques. This is feasible in all modern phones, provided that the memory chips and the processors used in the phones are able to access the encrypted memory without too big of an impact on the phone performance.

For this reason, the memory manufacturers should make sure that their memory chips are fast enough to cater for using intrinsic full-disk encryption. Luckily this is the case with most modern memory chips. On the other hand, the phone vendors should make sure that the processors are able to perform AES encryption, which is the de-facto standard in data encryption, at a reasonable speed. This may be done for example by including an AES co-processor in the phone processor.

Phone vendors should also try to improve the quality of their factory reset. The quality may be tested, for example, by first filling the phone with suitable data, then performing a factory reset and finally sending the phone to some commercial data recovery company. If the data recovery company is not able to find any data, then it is likely that the factory reset is working reasonably well, although later enhancements in data recovery technology might still be able to recover previously unrecoverable data.

6.2 Procedures for dealing with future technology

Storage technology trending recap

From our overview report section on mobile storage technologies, eMMC is currently the dominant technology with cheap price, capable performance and simple communication interface. The eMMC standard itself is still getting performance and security improvement updates over the versions (latest version is eMMC 5.1 released in 2015). Previously, we also mentioned UFS as an emerging technology starting to take some percentage of the market. UFS has the edge over eMMC on much faster performance, larger maximum capacity, lower power consumption.

Will eMMC get completely replaced by UFS? The answer is no, simply because of the price difference, eMMC is still the perfect choice for manufacturers aiming for the mid/low-end of the mobile phone market. A similar situation can be demonstrated by the state of the Hard disk drives market where HDD and SSD co-exist and serve individual purpose. However, our prediction is UFS would continue the current trend of gaining more popularity and remain a respectable potion of the market share.

Brief introduction to the functionality of UFS

Definition:
Universal Flash Storage (UFS) is a simple, high performance, mass storage device with a serial interface. It is primarily for use in mobile systems, between host processing and mass storage devices.

Key features of UFS include the following:

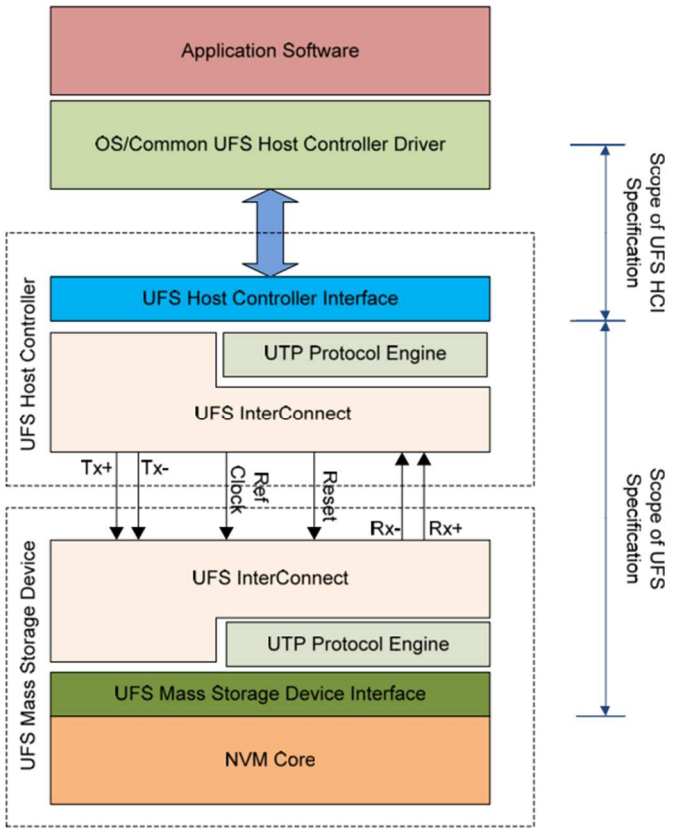
- UFS provides a number of features to support either embedded or removable storage.
- Embedded memory features: Capability to partition device's storage into multiple logical units with full management of partition attributes
- Command queue: Supporting multiple commands with command queue. This enables multi thread computing
- Supports well-known SCSI command set
- Simplified host controller interface (UFSHCI): Allowing greater flexibility in system design.
- Extendable performance with low power through significant reduction in power consumption
- Background operations mode: Granting devices time to execute flash management tasks (e.g. wear leveling, bad block management, wipe and garbage collection)
- Dynamic device capacity: The host has the ability to dynamically re-purpose used blocks into spared blocks.
- Security: UFS security features include: Secure mode operation, data and register protection, RPMB and reset

Structure of UFS

There are 2 levels when it comes to communicating with a UFS device: UFS Host Controller and UFS Mass Storage Device (shown in Figure 18 below).

The UFS Host Controller is responsible for managing the interface between host SW and UFS device and the data transfer. The UFS Device is the mass storage unit.

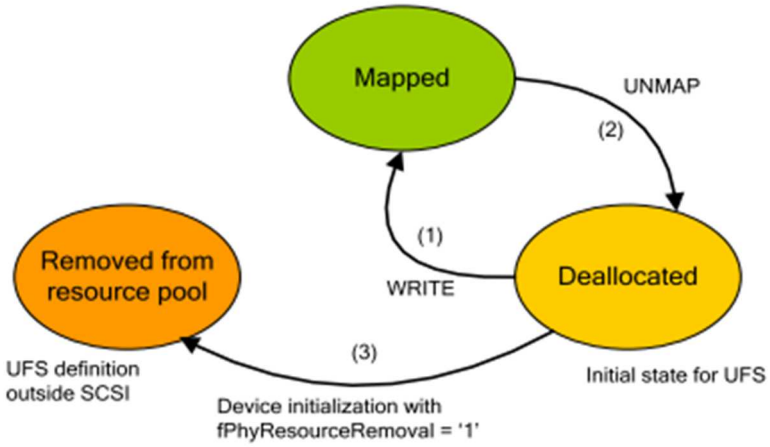
Figure 18: UFS Mass Storage Device.



Data arrangement

Figure 19 below shows a state machine diagram for the physical memory state. In addition to the "Mapped" state and the "Deallocated" state, there is the "Removed from the resource pool" state.

Figure 19: State machine diagram for the physical memory state.



Data manipulation operations:

(1) Write operation: Physical memory resource from the resource pool is mapped to LBA containing valid data.

(2) UNMAP operation for erase/discard: Physical memory resource is unmapped (de-allocated) from LBA and returned to the resource pool. Residual data in un-mapped physical memory resource is not valid.

(3) Device re-initialization causes some physical memory resources to be removed from the resource pool servicing the logical address space. After conversion, the amount of physical memory resources remaining in the resource pool of each logical unit is updated.

UFS characteristics regarding data security

This section describes the security features that are mandatory for all UFS memory chip. These features include: replay protected memory block (RPMB), secure mode and different types of logical unit write protection.

- *Secure mode:* the UFS device provides a way to remove the data permanently from the device when requested, ensuring that it cannot be retrieved using reverse engineering on the memory device. In the secure mode all operations that result in the removal or retiring of information on the device will purge this information in a secure manner. The secure mode is applied at the logical unit level, so different logical unit (partition) may have different secure mode. The data can be removed securely from the device through various methods

- *Device Data Write Protection:* UFS device data content can be protected at the logical unit level. The following write protection modes shall be available: permanent write protection, power on write protection, and secure write protection

- *RPMB:* A signed access to a RPMB is provided. This function provides means for the system to score data to the specific memory area in an authenticated and replay. The contents of the RPMB well known logical unit can only be read or written via a successfully authenticated read and write accesses. The data may be overwritten by the host but can never be erased.

In addition to these secure features, devices that utilize UFS memory chip is still under effect of security flaws coming from the operating system. From the perspective of Android OS, the necessity actions still need to be considered when erasing user data from the device.

References

Afonin, O. & Katalov, V., 2016. Practical Steps to Android Acquisition. In: *Mobile Forensics - Advanced Investigative Strategies.* Birmingham - Mumbai: Packt Publishing, pp. 65-137.

Amadeo, R., 2012. *A History of Pre-Cupcake Android Codenames.* [Online] Available at: http://www.androidpolice.com/2012/09/17/a-history-of-pre-cupcake-android-codenames/

Amadeo, R., 2012. *A History of Pre-Cupcake Android Codenames.* [Online] Available at: http://www.androidpolice.com/2012/09/17/a-history-of-pre-cupcake-android-codenames/

Android authority, 2015. *Samsung announces faster eMMC 5.1 flash memory chips.* [Online] Available at: http://www.androidauthority.com/samsung-emmc-5-1-flash-memory-588143/

Android Authority, 2016. *What is Android fragmentation, and can Google fix it?.* [Online] Available at: http://www.androidauthority.com/android-fragmentation-google-fix-it-713210/

Android 6.0 Compatibility Definition. 2015. [Online] Available at: https://source.android.com/compatibility/6.0/android-6.0-cdd

Apple, 2014. *Apple Announces Record Pre-orders for iPhone 6 & iPhone 6 Plus Top Four Million in First 24 Hours.* [Online] Available at: https://www.apple.com/uk/newsroom/2014/09/15Apple-Announces-Record-Pre-orders-for-iPhone-6-iPhone-6-Plus-Top-Four-Million-in-First-24-Hours/

Apple, 2017. *iPhone X: Environmentla Report.* [Online] Available at: https://images.apple.com/environment/pdf/products/iphone/iPhone_X_PER_sept2017.pdf

Baich, R., 2012. *A Risk-Based Approach to Combating Cyber Crime.* [Online] Available at: http://deloitte.wsj.com/cio/2012/07/18/cyber-crime-adopting-a-risk-based-approach-to-security/

Blancco Technology Group, 2015. *It's Complicated: Mobile Frustrations & Churn.* [Online] Available at: https://www.blancco.com/press-releases/blancco-technology-group-study-reveals-faulty-mobile-devices-ineffective-care-play-integral-role-in-mobile-carrier-oem-churn/

Blancco Technology Group, 2016. *EU GDPR: A Corporate Dilemma.* [Online] Available at: http://www.blancco.com/wp-content/uploads/2016/07/eu_gdpr_-_a_corporate_dilemma_rs.pdf

Blancco Technology Group, 2018. *State of Mobile Device Repair & Security Report.* [Online] Available at: https://www.blancco.com/resources/rs-state-of-mobile-device-repair-security/

Blancco, 2015. *Risky Mobile Business - Study of Mobile User's Views on Data Privacy & Security.* [Online] Available at: https://www.slideshare.net/BlanccoTechnologyGroup/risky-mobile-business-study-of-mobile-users-views-on-data-privacy-security-55686666

Boukhobza, J. & Rubini, S., 2012. *Flashing in the Memory Hierarchy.* [Online] Available at: https://www.lip6.fr/public/2012-11-15_Boukhobza_Flash_Final.pdf

CESG, 2014. *HMG IA Standard No. 5. Secure Sanitisation.,* s.l.: s.n.

Challen, G. et al., 2014. *The Mote is Dead. Long Live the Discarded Smartphone.* Santa Barbara, California , ACM.

Chibueze, E., 2016. *How do YOU Define Smartphone Brackets (Mid-range, etc)? Price, or Specs?.* [Online] Available at: https://www.xda-developers.com/how-do-you-define-smartphone-categories-price-or-specs/

CIO, 2018. *Data security + IT asset disposition: Avoiding a costly breach.* [Online] Available at: https://www.cio.com/article/3256908/leadership-management/data-security-it-asset-disposition-avoiding-a-costly-breach.html

CIPL, 2014. *The role of risk management in data protection.* [Online] Available at: https://www.google.fi/url?sa=t&rct=j&q=&esrc=s&source=web&cd=12&cad=rja&uact=8&ved=0ahUKEwik35L93ObaAhWGIpoKHa34CLM4ChAWCDkwAQ&url=https%3A%2F%2Fwww.informationpolicycentre.com%2Fuploads%2F5%2F7%2F1%2F0%2F57104281%2Fwhite_paper_2-the_role_of_risk_manageme

Computer Hope, 2018. *Computer vs Smartphone.* [Online] Available at: https://www.computerhope.com/issues/ch001398.htm

Cooke, J., 2006. *Flash memory 101: An Introduction to NAND flash.* [Online] Available at: http://www.eetimes.com/document.asp?doc_id=1272118&

Data Recoup, 2016. *Specialist data extraction tools for mobile phones and tablets.* [Online] Available at: https://www.datarecoup.com/blog/data-recovery/specialist-data-extraction-tools-for-mobile-phones-and-tablets

Datalight, 2015. *A Comparative Study of Flash Storage Technologies for Embedded Devices.* [Online] Available at: http://www.logic.nl/Site_files/Logic/9b/9b9af430-9379-44a7-9650-984adbcb2e08.pdf

Datalight, 2016. *Comparing Secure NAND Erase MEthods.* [Online] Available at: https://www.farelettronica.it/web/wp-content/uploads/2016/02/Comparing-Secure-NAND.pdf

Datalight, 2016. *eMMC Version Comparison.* [Online] Available at: https://www.datalight.com/solutions/technologies/emmc/emmc-feature-comparison-by-version

Deloitte & Touche LLP, 2012. *Risk assessment in practice.* [Online] Available at: http://www.coso.org/documents/COSOAnncsOnlineSurvy2GainInpt4Updt2IntrnlCntrlIntgratdFrmwrk%20-%20for%20merge_files/COSO-ERM%20Risk%20Assessment%20inPractice%20Thought%20Paper%20OCtober%202012.pdf

Design&Reuse, 2016. *UFS Goes Mainstream.* [Online] Available at: https://www.design-reuse.com/articles/38226/ufs-goes-mainstream.html

Durbin, S., 2016. *What a Risk-Based Approach to Security Means for Your Business.* [Online] Available at: http://www.infosecisland.com/blogview/24778-What-a-Risk-Based-Approach-to-Security-Means-for-Your-Business.html

ENISA, 2010. *Smartphones: Information security risks, opportunities and recommendations for users.* [Online] Available at: https://www.enisa.europa.eu/publications/smartphones-information-security-risks-opportunities-and-recommendations-for-users

ENISA, 2012. *Threat Landscape: Responding to the Evolving Threat Environment.* [Online] Available at: https://www.google.fi/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjWrpWxrtfZAhWLkiwKHVzMCdoQFggoMAA&url=https%3A%2F%2Fwww.enisa.europa.eu%2Fpublications%2FENISA_Threat_Landscape%2Fat_download%2FfullReport&usg=AOvVaw1Lhrgs8dZca3xVrpc

ENISA, 2017. *European Union Agency for Network and Information Security.* [Online] Available at: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary

ENISA, 2017. *Hardware Threat Landscape and Good Practice Guide.* [Online] Available at: https://www.enisa.europa.eu/publications/hardware-threat-landscape

Erikrespo, 2018. *Historical Android version distribution according to Android Market/Play Store usage, summing up data since December 2009.* [Online] Available at: https://en.wikipedia.org/wiki/Android_version_history#/media/File:Android_historical_version_distribution_-_vector.svg

EU GDPR, 2016. *GDPR Key Changes.* [Online]
Available at: https://www.eugdpr.org/key-changes.html

European Comission, 2015. *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS,* s.l.: s.n.

Fiorillo, S., 2009. *Theory and practice of flash memory mobile forensics.* Perth, s.n.

FIPS PUB 199 , 2004. *Standards for Security Categorization of Federal Information and Information Systems.* [Online]
Available at: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

Flashdba, 2014. *Understanding Flash: The Flash Translation Layer.* [Online]
Available at: https://flashdba.com/2014/09/17/understanding-flash-the-flash-translation-layer/

French, A. M., Guo, C. & Shim, J., 2014. Current Status, Issues, and Future of Bring Your Device (BYOD). *Communications of the Association for Information Systems,* 11, 35(10), pp. 191-198.

Gartner, 2017. *Gartner Says Worldwide Device Shipments Will Increase 2 Percent in 2018, Reaching Highest Year-Over-Year Growth Since 2015.* [Online]
Available at: https://www.gartner.com/newsroom/id/3816763

Government of Canada, 2017. *IT MEDIA SANITIZATION ITSP.40.006 V2.* [Online]
Available at: https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsp-40-006v2-eng_1.pdf

Green Aliance, 2015. *A circular economy for smart devices Opportunities inthe US, UK and India..* [Online]
Available at: http://www.green-alliance.org.uk/resources/A%20circular%20economy%20for%20smart%20devices.pdf

GSMA, 2015. *GSMA Mobile Economy 2015.* [Online]
Available at: https://www.gsma.com/mobileeconomy/global/2015/

GSMA, 2016. *GSMA Mobile Economy 2016.* [Online]
Available at: https://www.gsma.com/mobileeconomy/2016/global/

Hoare, P. 2017. Cybercrime is ‘bigger than global drug trade’. [Online] Available at: https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf

Hoffman, C., 2014. *Why You Don’t Need an Expensive Smartphone Anymore.* [Online]
Available at: https://www.howtogeek.com/196500/why-you-dont-need-an-expensive-smartphone-anymore/

Hom, E. J., 2017. *Mobile Device Security: Startling Statistics on Data Loss and Data Breaches.* [Online]
Available at: http://www.channelpronetwork.com/article/mobile-device-security-startling-statistics-data-loss

Huq, Numaan, 2015. *Follow the Data: Analyzing Breaches by Industry,* s.l.: s.n.

Hutchinson, L., 2012. *Solid-state revolution: in-depth on how SSDs really work.* [Online]
Available at: https://arstechnica.com/information-technology/2012/06/inside-the-ssd-revolution-how-solid-state-disks-really-work/5/

IBM, 2015. *Staying ahead of threats with global threat intelligence and automated protection.* [Online].

IDC, 2016. *Worldwide Market for Used Smartphones Forecast to Grow to 222.6 Million Units in 2020, According to IDC.* [Online]
Available at: https://www.idc.com/getdoc.jsp?containerId=prUS41929916

IDC, 2017. *Smartphone OS Market Share, 2017 Q1.* [Online]
Available at: https://www.idc.com/promo/smartphone-market-share/os

IDSC, 2018. Data Sanitization Terminology and Definitions. [Online]
Available at: https://www.datasanitization.org/data-sanitization-terminology/

IHS Markit, 2017. *IHS Mobile and Embedded Memory Market Tracker Q4 2016.* [Online] Available at: http://www.gosemiandbeyond.com/system-level-test-essential-for-fast-growing-embedded-nand-market/

IHS Markit, 2017. *Mobile and Embedded Memory Market Tracker.* [Online] Available at: https://technology.ihs.com/594195/mobile-and-embedded-memory-market-tracker-q2-2017

IMPERVA, 2018. *Data Classification.* [Online] Available at: https://www.imperva.com/data-security/data-security-101/data-classification/

Inspired Techs, 2017. *Why Data Security is So Important to Businesses of all Sizes.* [Online] Available at: http://www.inspiredtechs.com.au/why-data-security-is-so-important-to-businesses-of-all-sizes/

ISO 28000:2007(en), 2007. *Specification for security management systems for the supply chain.* [Online] Available at: https://www.iso.org/obp/ui/#iso:std:iso:28000:ed-1:v1:en

ISO/IEC 13335-1:2004, n.d. *IT Security techniques.* [Online] Available at: https://www.iso.org/standard/39066.html

JEDEC standard, 2016. *Universal Flash Storage (UFS) versoi 2.1.* [Online] Available at: https://www.jedec.org/system/files/docs/JESD220C.pdf

Jones, A. V. C. S. I., 2008. Analysis of Information Remaining on Hand Held Devices Offered for Sale on the Second Hand Market. *Journal of Digital Forensics, Security and Law,* 3(2), pp. 55-70.

Kathy , C., 2013. *Flash Storage A True Mobile Catalyst,* Santa Clara, CA, USA: Flash Memory Summit 2013.

Khramova, M & Martinez, S. 2018. Analysis of data remanence after factory reset, and sophisticated attacks on memory chips. *Presented at Going Green – CARE INNOVATION 2018 conference and exhibition on Electronics and the Environment*.

Mahalik, H., Tamma, R. & Bommisetty, S., 2016. *Practical Mobile Forensics.* Second ed. Birmingham: Packt Publishing.

Maytom, T., 2014. Four Connected Devices per Person Worldwide by 2020. *Mobile Marketing Magazine.*

MHEducation, 2016. *Understanding hackers and how they attack.* [Online] Available at: http://books.mcgraw-hill.com/downloads/products/0072133686/0072133686_ch01.pdf

Micron, 2016. *3-D NAND and UFS: Optimized Mobile Storage.* [Online] Available at: https://www.flashmemorysummit.com/English/Collaterals/Proceedings/2016/20160811_S301I_Christensen.pdf

Micron, 2018. *Choosing the Right NAND.* [Online] Available at: https://www.micron.com/products/nand-flash/choosing-the-right-nand

Morgan, S. 2017. 2017 Cybercrime Report. [Online] Available at: https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf

Munro, K., 2014. Android scraping:accessing personal data on mobile devices. *Network Security,* Issue 11, pp. 5-9.

New Zealand Government, 2014. *Risk Assessment Process. Information security.* [Online] Available at: https://www.ict.govt.nz/assets/ICT-System-Assurance/Risk-Assessment-Process-Information-Security.pdf

NIJ, 2014. *Cell Phone Forensics In a Correctional Setting: Guidebook,* s.l.: s.n.

NIST , 2002. *Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology.* [Online] Available at: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

NIST 800-122, 2010. *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).* [Online] Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf

NIST 800-88, 2006. *Guidelines for Media Sanitization ,* Washington: National Institute of Standards and Technology.

NIST, 2014. *NIST Special Publication 800-101. Guidelines on Mobile Device Forensics,* s.l.: s.n.

OpenSignal, 2015. *Android Fragmentation (August 2015).* [Online] Available at: https://opensignal.com/reports/2015/08/android-fragmentation/

Ossmann, M. & Osborn, K., 2013. *Multiplexed Wired Attack Surfaces.* [Online] Available at: https://www.google.fi/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=2ahUKEwjr172xx9jcAhVrD5oKHbL2C6sQFjABegQICRAC&url=https%3A%2F%2Fmedia.blackhat.com%2Fus-13%2FUS-13-Ossmann-Multiplexed-Wired-Attack-Surfaces-WP.pdf&usg=AOvVaw1B82pglNVyZZWti

Pascual A., Marchini K., Miller S. 2018 Identity Fraud: Fraud Enters a New Era of Complexity. [Online] Available at: https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity

PCMagazine, 2017. *Definition of: feature phone.* [Online] Available at: https://www.pcmag.com/encyclopedia/term/62894/feature-phone

PhoneArena, 2017. *UFS 2.1 explained: the storage technology in today's top Android phones.* [Online] Available at: https://www.phonearena.com/news/UFS-2.1-explained-the-storage-technology-in-todays-top-Android-phones_id95180

Ponemon Institue, 2014. *The Cost of Insecure Mobile Devices.* [Online] Available at: https://www.ponemon.org/local/upload/file/AT%26T%20Mobility%20Report%20FINAL%202.pdf

PR Newswire, 2017. *New UFS controller family enables next-generation high-performance, high-capacity embedded memory solutions for mobile devices.* [Online] Available at: http://www.prnewswire.com/news-releases/new-ufs-controller-family-enables-next-generation-high-performance-high-capacity-embedded-memory-solutions-for-mobile-devices-300418259.html

PRWeb, 2015. *Robust Growth in Mobile Device Sales Drives the Global Embedded Multimedia Card (eMMC) Market, According to a New Report by Global Industry Analysts, Inc..* [Online] Available at: http://www.prweb.com/releases/emmc_market/ufs_market/prweb12604646.htm

Rusolut, 2016. *SMS recovery from NAND memory of erased eMMC chip.* [Online] Available at: https://www.flashmemorysummit.com/English/Collaterals/Proceedings/2017/20170808_S102A_Sheremetov.pdf

Rusolut, 2018. *THE ULTIMATE CHIP-OFF MOBILE FORENSICS: DATA RESURRECTION FROM DEAD EMMC CHIPS.* Myrtle Beach, SC USA, s.n.

SANS Institute, 2003. *Ghosts in the machine: The who, why, and how of attacks on information security.* [Online] Available at: https://www.sans.org/reading-room/whitepapers/awareness/ghosts-machine-who-why-attacks-information-security-914

SANS Institute, 2014. *Creating a Threat Profile for Your Organization.* [Online] Available at: https://www.sans.org/reading-room/whitepapers/threats/creating-threat-profile-organization-35492

Schneier, B. 2000. Secrets and Lies: Digital Security in a Networked World.

Singh, B., Saharan,, R., Somani, G. & Gupta, G., 2016. Secure File Deletion for Solid State Drives. In: *Advances in Digital Forensics XII: 12th IFIP WG 11.9 International Conference.* New Delhi: s.n., pp. 345-362.

SK Hynix, 2017. *Multichip Package.* [Online] Available at: https://www.skhynix.com/eng/product/multiPackage.jsp

Skorobogatov, S., 2005. *Data Remanence in Flash Memory Devices.* [Online] Available at: https://www.cl.cam.ac.uk/~sps32/DataRem_CHES2005.pdf

Skorobogatov, S., 2011. *Fault attacks on secure chips: from glitch to flash.* Albena, Bulgaria, Design and Security of Cryptographic Algorithms and Devices (ECRYPT II).

Soutiyal, A., 2016. *What is Stock Android, Vanilla Android & Pure Android, Benefits.* [Online] Available at: https://www.xyztimes.com/6517/what-is-stock-android-vanilla-android-pure-android-benefits.html

SurfWatch Labs, 2015. *Cyber threat intelligence.* [Online] Available at: https://www.surfwatchlabs.com/threat-categories

Techopedia, 2017. *Entry-Level Smartphone.* [Online] Available at: https://www.techopedia.com/definition/30931/entry-level-smartphone

The Guardian, 2010. *What's the carbon footprint of ... a new car?.* [Online] Available at: https://www.theguardian.com/environment/green-living-blog/2010/sep/23/carbon-footprint-new-car

Toshiba, 2016. *EMBEDDED MULTIMEDIA CARD" E•MMCTM MEMORY: ENABLING A WORLD OF "THINGS" TO THINK SMARTER,* s.l.: s.n.

TUM, 2014. *Invasive Attacks.* [Online] Available at: https://www.sec.ei.tum.de/en/research/invasive-attacks/

Uceda Velez, T. & Morana , M., 2015. *Risk centric threat modeling. Process for attack simulation and threat analysis..* Hoboken, New Jersey: Wiley.

UFSA, 2013. *Introduction to the Universal Flash Storage Assocation.* [Online] Available at: https://ufsa.org/wp-content/uploads/2011/06/1306_UFSA_White_Paper.pdf

Wei, M., Grupp, L., Spada, F. & Swanson, S., 2011. *Reliably Erasing Data From Flash-Based Solid State Drives.* [Online]
Available at: https://www.usenix.org/legacy/event/fast11/tech/full_papers/Wei.pdf

Whitaker, K., 2015. *A Comparative Study of Flash Storage,* s.l.: s.n.

Wikipedia, 2018. *Android version history.* [Online] Available at: https://en.wikipedia.org/wiki/Android_version_history

Yang,, . S., Choi, J., Kim,, K. & Chang,, T., 2015. New acquisition method based on firmware update protocols for Android smartphones.. *Digital Investigation ,* Volume 14, pp. 68-76.

ZDNet, 2015. *Research: 74 percent using or adopting BYOD.* [Online] Available at: http://www.zdnet.com/article/ces-2015-gogoro-unveils-urban-battery-swapping-infrastructure-and-connected-smartscooter/