Computer Security and Mobile Security Challenges

Nikola Zlatanov*

Preface

Computer security, also known as **cybersecurity** or **IT security**, is the protection of **information systems** from theft or damage to the **hardware**, the **software**, and to the **information** on them, as well as from **disruption** or **misdirection** of the services they provide.[1] It includes **controlling physical access** to the hardware, as well as protecting against harm that may come via **network access**, **data** and **code injection**,[2] and due to malpractice by operators, whether **intentional**, **accidental**, or due to them **being tricked** into deviating from secure procedures.[3]

The field is of growing importance due to the increasing reliance on computer systems in most societies.[4] Computer systems now include a very wide variety of "smart" devices, including smartphones, **televisions** and tiny devices as part of the **Internet of Things** – and networks include not only the **Internet** and private data networks, but also **Bluetooth**, **Wi-Fi** and other **wireless networks**.

Vulnerabilities and attacks

A vulnerability is a system susceptibility or flaw, and many vulnerabilities are documented in the **Common Vulnerabilities and Exposures** (CVE) database and vulnerability management is the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities as they are discovered. An *exploitable* vulnerability is one for which at least one working attack or "**exploit"** exists.

To secure a computer system, it is important to understand the attacks that can be made against it, and these **threats** can typically be classified into one of the categories below:
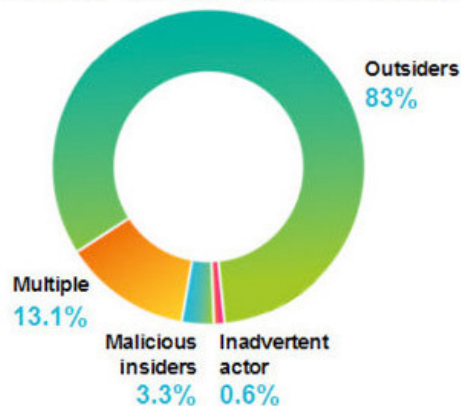
Backdoors

A **backdoor** in a computer system, a **cryptosystem** or an algorithm, is any secret method of bypassing normal authentication or security controls. They may exist for a number of reasons, including by original design or from poor configuration. They may also have been added later by an authorized party to allow some legitimate access, or by an attacker for malicious reasons; but regardless of the motives for their existence, they create a vulnerability.
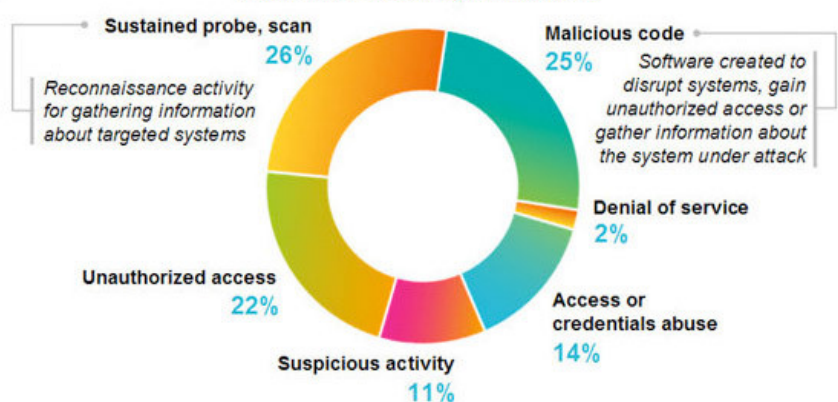
Denial-of-service attack

Denial of service attacks are designed to make a machine or network resource unavailable to its intended users. Attackers can deny service to individual victims, such as by deliberately entering a wrong password enough consecutive times to cause the victim account to be locked, or they may overload the capabilities of a machine or network and block all users at once. While a network attack from a single IP address can be blocked by adding a new firewall rule, many forms of Distributed denial of service (DDoS) attacks are possible, where the attack comes from a large number of points – and defending is much more difficult. Such attacks can originate from the zombie computers of a **botnet**, but a range of other techniques are possible including **reflection and amplification attacks**, where innocent systems are fooled into sending traffic to the victim.

Retail Security Threats: Types of Attackers

Outsiders
83%

Multiple
13.1%

Malicious insiders
3.3%

Inadvertent actor
0.6%

Methods Used by Attackers

Sustained probe, scan
26%
Reconnaissance activity for gathering information about targeted systems

Malicious code
25%
Software created to disrupt systems, gain unauthorized access or gather information about the system under attack

Denial of service
2%

Access or credentials abuse
14%

Suspicious activity
11%

Unauthorized access
22%

Source: 2013 IBM Cyber Security Intelligence Index for Retail

Direct-access attacks

An unauthorized user gaining physical access to a computer is most likely able to directly download data from it. They may also compromise security by making **operating system** modifications, installing software **worms**, **keyloggers**, or **covert listening devices**. Even when the system is protected by standard security measures, these may be able to be bypassed by booting another operating system or tool from a **CD-ROM** or other bootable media. **Disk encryption** and **Trusted Platform Module** are designed to prevent these attacks.

Eavesdropping

Eavesdropping is the act of surreptitiously listening to a private conversation, typically between hosts on a network. For instance, programs such as Carnivore and **NarusInsight** have been used by the **FBI** and **NSA** to eavesdrop on the systems of **internet service providers**. Even machines that operate as a closed system (i.e., with no contact to the outside world) can be eavesdropped upon via monitoring the faint **electro-magnetic** transmissions generated by the hardware; TEMPEST is a specification by the NSA referring to these attacks.

Spoofing

Spoofing of user identity describes a situation in which one person or program successfully masquerades as another by falsifying data.

Tampering

Tampering describes a malicious modification of products. So-called **"Evil Maid" attacks** and security services planting of surveillance capability into routers[5] are examples.

Privilege escalation

Privilege escalation describes a situation where an attacker with some level of restricted access is able to, without authorization, elevate their privileges or access level. So for example, a standard computer user may be able to fool the system into giving them access to restricted data; or even to "**become root**" and have full unrestricted access to a system.

Phishing

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details directly from users. Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Preying on a victim's trusting, phishing can be classified as a form of social engineering.

Clickjacking

Clickjacking, also known as "UI redress attack or User Interface redress attack", is a malicious technique in which an attacker tricks a user into clicking on a button or link on another webpage while the user intended to click on the top level page. This is done using multiple transparent or opaque layers. The attacker is basically "hijacking" the clicks meant for the top level page and routing them to some other irrelevant page, most likely owned by someone else. A similar technique can be used to hijack keystrokes. Carefully drafting a combination of stylesheets, iframes, buttons and text boxes, a user can be led into believing that they are typing the password or other information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

Social engineering and Trojans

Social engineering aims to convince a user to disclose secrets such as passwords, card numbers, etc. by, for example, impersonating a bank, a contractor, or a customer.[6]

Systems at risk

Computer security is critical in almost any industry which uses computers.[7]

Financial systems

Web sites that accept or store credit card numbers and **bank account** information are prominent hacking targets, because of the potential for immediate financial gain from transferring money, making purchases, or selling the information on the **black market**. In-store payment systems and ATMs have also been tampered with in order to gather customer account data and **PINs**.

Utilities and industrial equipment

Computers control functions at many utilities, including coordination of telecommunications, the power grid, **nuclear power plants**, and valve opening and closing in water and gas networks. The Internet is a potential attack vector for such machines if connected, but the **Stuxnet** worm demonstrated that even equipment controlled by computers not connected to the Internet can be vulnerable to physical damage caused by malicious commands sent to industrial equipment (in that case uranium enrichment centrifuges) which are infected via **removable media**. In 2014, the Computer Emergency Readiness Team, a division of the Department of Homeland Security, investigated 79 hacking incidents at energy companies.[8]

Aviation

The aviation industry is very reliant on a series of complex system which could be attacked.[9] A simple power outage at one airport can cause repercussions worldwide,[10] much of the system relies on radio transmissions which could be disrupted,[11] and controlling aircraft over oceans is especially dangerous because radar surveillance only extends 175 to 225 miles offshore.[12] There is also potential for attack from within an aircraft.[13]

The consequences of a successful attack range from loss of confidentiality to loss of system integrity, which may lead to more serious concerns such as exfiltration of data, network and **air traffic control** outages, which in turn can lead to airport closures, loss of aircraft, loss of passenger life, **damages on the ground** and to transportation infrastructure. A successful attack on a **military aviation** system that controls munitions could have even more serious consequences.

Consumer devices

Desktop computers and laptops are commonly infected with malware either to gather passwords or financial account information, or to construct a **botnet** to attack another target. Smart phones, **tablet computers**, smart watches, and other mobile devices such as **Quantified Self** devices like **activity trackers** have also become targets and many of these have sensors such as cameras, microphones, GPS receivers, compasses, and accelerometers which could be exploited, and may collect personal information, including sensitive health information. Wi-Fi, Bluetooth, and cell phone network on any of these devices could be used as attack vectors, and sensors might be remotely activated after a successful breach.[14] **Home automation** devices such as the **Nest thermostat** are also potential targets.[14]

Large corporations

Large corporations are common targets. In many cases this is aimed at financial gain through identity theft and involves **data breaches** such as the loss of millions of clients' credit card details by Home Depot,[15] **Staples**,[16] and **Target Corporation**.[17]

Not all attacks are financially motivated however; for example security firm HBGary Federal suffered a serious series of attacks in 2011 from hacktivist group **Anonymous** in retaliation for the firm's CEO claiming to have infiltrated their group, [18][19] and Sony Pictures **was attacked in 2014** where the motive appears to have been to embarrass with data leaks, and cripple the company by wiping workstations and servers.[20][21]

Automobiles

If access is gained to a car's internal controller area network, it is possible to disable the brakes and turn the steering wheel.[22] Computerized engine timing, **cruise control**, anti-lock brakes, seat belt tensioners, door locks, **airbags** and **advanced driver assistance systems** make these disruptions possible, and self-driving cars go even further. **Connected cars** may use Wi-Fi and Bluetooth to communicate with onboard consumer devices, and the cell phone network to contact concierge and emergency assistance services or get navigational or entertainment information; each of these networks is a potential entry point for malware or an attacker.[22] Researchers in 2011 were even able to use a malicious **compact disc** in a car's stereo system as a successful attack vector,[23] and cars with built-in voice recognition or remote assistance features have onboard microphones which could be used for eavesdropping.

A 2015 report by U.S. Senator Edward Markey criticized manufacturers' security measures as inadequate, and also highlighted privacy concerns about driving, location, and diagnostic data being collected, which is vulnerable to abuse by both manufacturers and hackers.[24]

Government

Government and **military** computer systems are commonly attacked by activists[25][26][27][28] and foreign powers.[29][30][31][32] Local and regional government infrastructure such as **traffic light** controls, police and intelligence agency communications, **personnel records** and financial systems are also potential targets as they are now all largely computerized.

Impact of security breaches

Serious financial damage has been caused by security breaches, but because there is no standard model for estimating the cost of an incident, the only data available is that which is made public by the organizations involved. "Several computer security consulting firms produce estimates of total worldwide losses attributable to **virus** and **worm** attacks and to hostile digital acts in general. The 2003 loss estimates by these firms range from $13 billion (worms and viruses only) to $226 billion (for all forms of covert attacks). The reliability of these estimates is often challenged; the underlying methodology is basically anecdotal."[33]

However, reasonable estimates of the financial cost of security breaches can actually help organizations make rational investment decisions. According to the classic **Gordon-Loeb Model** analyzing the optimal investment level in information security, one can conclude that the amount a firm spends to protect information should generally be only a small fraction of the expected loss (i.e., the **expected value** of the loss resulting from a cyber/information security breach).[34]

Attacker motivation

As with **physical security**, the motivations for breaches of computer security vary between attackers. Some are thrill-seekers or **vandals**, others are activists or criminals looking for financial gain. State-sponsored attackers are now common and well resourced, but started with amateurs such as **Markus Hess** who hacked for the **KGB**, as recounted by **Clifford Stoll**, in *The Cuckoo's Egg*.

A standard part of threat modelling for any particular system is to identify what might motivate an attack on that system, and who might be motivated to breach it. The level and detail of precautions will vary depending on the system to be secured. A home **personal computer**, **bank**, and **classified** military **network** face very different threats, even when the underlying technologies in use are similar.

Computer protection (countermeasures)

In computer security a countermeasure is an action, device, procedure, or technique that reduces a **threat**, a **vulnerability**, or an **attack** by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.[35][36][37]

Security measures

A state of computer "security" is the conceptual ideal, attained by the use of the three processes: threat prevention, detection, and response. These processes are based on various policies and system components, which include the following:

- User account **access controls** and **cryptography** can protect systems files and data, respectively.

- Firewalls are by far the most common prevention systems from a network security perspective as they can (if properly configured) shield access to internal network services, and block certain kinds of attacks through packet filtering. Firewalls can be both hardware- or software-based.

- Intrusion Detection System (IDS) products are designed to detect network attacks in-progress and assist in post-attack forensics, while **audit trails** and logs serve a similar function for individual systems.

- "Response" is necessarily defined by the assessed security requirements of an individual system and may cover the range from simple upgrade of protections to notification of legal authorities, counter-attacks, and the like. In some special cases, a complete destruction of the compromised system is favored, as it may happen that not all the compromised resources are detected.

Today, computer security comprises mainly "preventive" measures, like firewalls or an exit procedure. A firewall can be defined as a way of filtering network data between a host or a network and another network, such as the **Internet**, and can be implemented as software running on the machine, hooking into the network stack (or, in the case of most UNIX-based operating systems such as **Linux**, built into the operating system kernel) to provide real time filtering and blocking. Another implementation is a so-called physical firewall which consists of a separate machine filtering network traffic. Firewalls are common amongst machines that are permanently connected to the **Internet**.

However, relatively few organizations maintain computer systems with effective detection systems, and fewer still have organized response mechaniSMS in place. As result, as Reuters points out: "Companies for the first time report they are losing more through electronic theft of data than physical stealing of assets".[38] The primary obstacle to effective eradication of cybercrime could be traced to excessive reliance on firewalls and other automated "detection" systems. Yet it is basic evidence gathering by using **packet capture appliances** that puts criminals behind bars.

Reducing vulnerabilities

While **formal verification** of the correctness of computer systems is possible,[39][40] it is not yet common. Operating systems formally verified include seL4,[41] and **SYSGO**'s **PikeOS**[42][43] – but these make up a very small percentage of the market.

Cryptography properly implemented is now virtually impossible to directly break. Breaking them requires some non-cryptographic input, such as a stolen key, stolen plaintext (at either end of the transmission), or some other extra cryptanalytic information.

Two factor authentication is a method for mitigating unauthorized access to a system or sensitive information. It requires "something you know"; a password or PIN, and "something you have"; a card, dongle, cellphone, or other piece of hardware. This increases security as an unauthorized person needs both of these to gain access.

Social engineering and direct computer access (physical) attacks can only be prevented by non-computer means, which can be difficult to enforce, relative to the sensitivity of the information. Even in a highly disciplined environment, such as in military organizations, social engineering attacks can still be difficult to foresee and prevent.

It is possible to reduce an attacker's chances by keeping systems up to date with security patches and updates, using a security scanner or/and hiring competent people responsible for security. The effects of data loss/damage can be reduced by careful **backing up** and **insurance**.

Security by design

Security by design, or alternately secure by design, means that the software has been designed from the ground up to be secure. In this case, security is considered as a main feature.

Some of the techniques in this approach include:

- The **principle of least privilege**, where each part of the system has only the privileges that are needed for its function. That way even if an **attacker** gains access to that part, they have only limited access to the whole system.

- **Automated theorem proving** to prove the correctness of crucial software subsystems.

- **Code reviews** and **unit testing**, approaches to make modules more secure where formal correctness proofs are not possible.

- **Defense in depth**, where the design is such that more than one subsystem needs to be violated to compromise the integrity of the system and the information it holds.

- **Default secure settings**, and design to "fail secure" rather than "fail insecure". Ideally, a secure system should require a deliberate, conscious, knowledgeable and free decision on the part of legitimate authorities in order to make it insecure.

- **Audit trails** tracking system activity, so that when a security breach occurs, the mechanism and extent of the breach can be determined. Storing audit trails remotely, where they can only be appended to, can keep intruders from covering their tracks.

- **Full disclosure** of all vulnerabilities, to ensure that the "**window of vulnerability**" is kept as short as possible when bugs are discovered.

Security architecture

The Open Security Architecture organization defines IT security architecture as "the design **artifacts** that describe how the security controls (security countermeasures) are positioned, and how they relate to the overall information technology architecture. These controls serve the purpose to maintain the system's quality attributes: confidentiality, integrity, availability, accountability and **assurance services**".[44]

Techopedia defines security architecture as "a unified security design that addresses the necessities and potential risks involved in a certain scenario or environment. It also specifies when and where to apply security controls. The design process is generally reproducible." The key attributes of security architecture are:[45]

- the relationship of different components and how they depend on each other.

- the determination of controls based on risk assessment, good practice, finances, and legal matters.

- the standardization of controls.

Hardware protection mechaniSMS

While hardware may be a source of insecurity, such as with microchip vulnerabilities maliciously introduced during the manufacturing process,[46][47] hardware-based or assisted computer security also offers an alternative to software-only computer security. Using devices and methods such as **dongles**, trusted platform modules, intrusion-aware cases, drive locks, disabling USB ports, and mobile-enabled access may be considered more secure due to the physical access (or sophisticated **backdoor access**) required in order to be compromised. Each of these is covered in more detail below.

- USB **dongles** are typically used in software licensing schemes to unlock software capabilities,[48] but they can also be seen as a way to prevent unauthorized access to a computer or other device's software. The dongle, or key, essentially creates a secure encrypted tunnel between the software

application and the key. The principle is that an encryption scheme on the dongle, such as **Advanced Encryption Standard** (AES) provides a stronger measure of security, since it is harder to hack and replicate the dongle than to simply copy the native software to another machine and use it. Another security application for dongles is to use them for accessing web-based content such as cloud software or Virtual Private Networks (VPNs).[49] In addition, a USB dongle can be configured to lock or unlock a computer.[50]

- Trusted platform modules (TPMs) secure devices by integrating cryptographic capabilities onto access devices, through the use of microprocessors, or so-called computers-on-a-chip. TPMs used in conjunction with server-side software offer a way to detect and authenticate hardware devices, preventing unauthorized network and data access.[51]

- **Computer case intrusion detection** refers to a push-button switch which is triggered when a computer case is opened. The firmware or BIOS is programmed to show an alert to the operator when the computer is booted up the next time.

- Drive locks are essentially software tools to encrypt hard drives, making them inaccessible to thieves.[52] Tools exist specifically for encrypting external drives as well.[53]

- Disabling USB ports is a security option for preventing unauthorized and malicious access to an otherwise secure computer. Infected USB dongles connected to a network from a computer inside the firewall are considered by the magazine Network World as the most common hardware threat facing computer networks.[54]

- Mobile-enabled access devices are growing in popularity due to the ubiquitous nature of cell phones. Built-in capabilities such as **Bluetooth**, the newer **Bluetooth low energy** (LE), **Near field communication** (NFC) on non-iOS devices and **biometric** validation such as thumb print readers, as well as **QR code** reader software designed for mobile devices, offer new, secure ways for mobile phones to connect to access control systems. These control systems provide computer security and can also be used for controlling access to secure buildings.[55]

Secure operating systems

One use of the term "computer security" refers to technology that is used to implement secure **operating systems**. In the 1980s the **United States Department of Defense** (DoD) used the **"Orange Book"**[56] standards, but the current international standard ISO/IEC 15408, "**Common Criteria**" defines a number of progressively more stringent **Evaluation Assurance Levels**. Many common operating systems meet the EAL4 standard of being "Methodically Designed, Tested and Reviewed", but the **formal verification** required for the highest levels means that they are uncommon. An example of an EAL6 ("Semiformally Verified Design and Tested") system is Integrity-178B, which is used in the **Airbus A380**[57] and several military jets.[58]

Secure coding

In software engineering, **secure coding** aims to guard against the accidental introduction of security vulnerabilities. It is also possible to create software designed from the ground up to be secure. Such systems are "**secure by design**". Beyond this, **formal verification** aims to prove the **correctness** of the algorithms underlying a system;[59] important for **cryptographic protocols** for example.

Capabilities and access control lists

Within computer systems, two of many **security models** capable of enforcing privilege separation are **access control lists** (ACLs) and **capability-based security**. Using ACLs to confine programs has been proven to be insecure in many situations, such as if the host computer can be tricked into indirectly allowing restricted file access, an issue known as the **confused deputy problem**. It has also been shown that the promise of ACLs of giving access to an object to only one person can never be guaranteed in practice. Both of these problems are resolved by capabilities. This does not mean practical flaws exist in all ACL-based systems, but only that the designers of certain utilities must take responsibility to ensure that they do not introduce flaws.

Capabilities have been mostly restricted to research **operating systems**, while commercial OSs still use ACLs. Capabilities can, however, also be implemented at the language level, leading to a style of

programming that is essentially a refinement of standard object-oriented design. An open source project in the area is the E language.

The most secure computers are those not connected to the Internet and shielded from any interference. In the real world, the most secure systems are **operating systems** where **security** is not an add-on.

Response to breaches

Responding forcefully to attempted security breaches (in the manner that one would for attempted physical security breaches) is often very difficult for a variety of reasons:

- Identifying attackers is difficult, as they are often in a different **jurisdiction** to the systems they attempt to breach, and operate through proxies, temporary anonymous dial-up accounts, wireless connections, and other anonymizing procedures which make backtracking difficult and are often located in yet another jurisdiction. If they successfully breach security, they are often able to delete logs to cover their tracks.

- The sheer number of attempted attacks is so large that organizations cannot spend time pursuing each attacker (a typical home user with a permanent (e.g., **cable modem**) connection will be attacked at least several times per day, so more attractive targets could be presumed to see many more). Note however, that most of the sheer bulk of these attacks are made by automated **vulnerability scanners** and **computer worms**.

- **Law enforcement officers** are often unfamiliar with **information technology**, and so lack the skills and interest in pursuing attackers. There are also budgetary constraints. It has been argued that the high cost of technology, such as **DNA** testing, and improved forensics mean less money for other kinds of law enforcement, so the overall rate of criminals not getting dealt with goes up as the cost of the technology increases. In addition, the identification of attackers across a network may require logs from various points in the network and in many countries, the release of these records to law enforcement (with the exception of being voluntarily surrendered by a **network administrator** or a **system administrator**) requires a **search warrant** and, depending on the circumstances, the legal proceedings required can be drawn out to the point where the records are either regularly destroyed, or the information is no longer relevant.

Notable computer security attacks and breaches

Robert Morris and the first computer worm

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers – the first internet "**computer worm**".[60] The software was traced back to 23-year-old **Cornell University** graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.[60]

Rome Laboratory

In 1994, over a hundred intrusions were made by unidentified crackers into the **Rome Laboratory**, the US Air Force's main command and research facility. Using **Trojan horses**, hackers were able to obtain unrestricted access to Rome's networking systems and remove traces of their activities. The intruders were able to obtain classified files, such as air tasking order systems data and furthermore able to penetrate connected networks of NASA's Goddard Space Flight Center, Wright-Patterson Air Force Base, some Defense contractors, and other private sector organizations, by posing as a trusted Rome center user.[61]

TJX loses 45.7m customer credit card details

In early 2007, American apparel and home goods company **TJX** announced that it was the victim of an **unauthorized computer systems intrusion**[62] and that the hackers had accessed a system that stored data on **credit card**, **debit card**, **check**, and merchandise return transactions.[63]

Stuxnet attack

The computer worm known as **Stuxnet** reportedly ruined almost one-fifth of Iran's nuclear centrifuges[64] by disrupting industrial **programmable logic controllers** (PLCs) in a targeted attack generally believed to have been launched by Israel and the United States[65][66][67][68] although neither has publicly acknowledged this.

Global surveillance disclosures

In early 2013, massive breaches of computer security by the NSA were revealed, including deliberately inserting a backdoor in a NIST standard for encryption[69] and tapping the links between **Google**'s data centers.[70] These were disclosed by NSA contractor **Edward Snowden**.[71]

Target and Home Depot breaches

In 2013 and 2014, a **Russian/Ukrainian** hacking ring known as "Rescator" broke into **Target Corporation** computers in 2013, stealing roughly 40 million credit cards,[72] and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers.[73] Warnings were delivered at both corporations, but ignored; physical security breaches using self-checkout machines are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee – meaning that the heists could have easily been stopped by existing antivirus software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

Ashley Madison breach

In July of 2015, a hacker group known as "The Impact Team" successfully breached the extramarital relationship website Ashley Madison. The group claimed that they had taken not only company data but user data as well. After the breach, The Impact Team dumped emails from the company's CEO, to prove their point, and threatened to dump customer data unless the website was taken down permanently. With this initial data release, the group stated "Avid Life Media has been instructed to take Ashley Madison and Established Men offline permanently in all forms, or we will release all customer records, including profiles with all the customers' secret sexual fantasies and matching credit card transactions, real names and addresses, and employee documents and emails. The other websites may stay online." [74] When Avid Life Media, the parent company that created the Ashley Madison website, did not take the site offline, The Impact Group released two more compressed files, one 9.7GB and the second 20GB. After the second data dump, Avid Life Media CEO Noel Biderman resigned, but the website remained functional.

Legal issues and global regulation

Conflict of laws in cyberspace has become a major cause of concern for computer security community. Some of the main challenges and complaints about the antivirus industry are the lack of global web regulations, a global base of common rules to judge, and eventually punish, cyber crimes and cyber criminals. There is no global cyber law and cybersecurity treaty that can be invoked for enforcing global cybersecurity issues.

International legal issues of cyber attacks are complicated in nature. Even if an antivirus firm locates the cyber criminal behind the creation of a particular virus or piece of **malware** or form of cyber attack, often the local authorities cannot take action due to lack of laws under which to prosecute.[75][76] Authorship attribution for cyber crimes and cyber attacks is a major problem for all law enforcement agencies.

"[Computer viruses] switch from one country to another, from one jurisdiction to another — moving around the world, using the fact that we don't have the capability to globally police operations like this. So the Internet is as if someone [had] given free plane tickets to all the online criminals of the world."[75] Use of dynamic DNS, **fast flux** and **bullet proof servers** have added own complexities to this situation.

Government

The role of the government is to make **regulations** to force companies and organizations to protect their systems, infrastructure and information from any cyber attacks, but also to protect its own national infrastructure such as the national power-grid.[77]

The question of whether the government should intervene or not in the regulation of the **cyberspace** is a very polemical one. Indeed, for as long as it has existed and by definition, the cyberspace is a virtual space free of any government intervention. Where everyone agree that an improvement on cybersecurity is more than vital, is the government the best actor to solve this issue? Many government officials and experts think that the government should step in and that there is a crucial need for regulation, mainly due to the failure of the private sector to solve efficiently the cybersecurity problem. **R. Clarke** said during a panel discussion at the **RSA Security Conference** in **San Francisco**, he believes that the "industry only responds when you threaten regulation. If industry doesn't respond (to the threat), you have to follow through."[78] On the other hand, executives from the private sector agree that improvements are necessary, but think that the government intervention would affect their ability to innovate efficiently.

Actions and teams in the US

Legislation

The 1986 **18 U.S.C. § 1030**, more commonly known as the **Computer Fraud and Abuse Act** is the key legislation. It prohibits unauthorized access or damage of "protected computers" as defined in **18 U.S.C. § 1030(e)(2)**.

Although various other measures have been proposed, such as the "Cybersecurity Act of 2010 – S. 773" in 2009, the "International Cybercrime Reporting and Cooperation Act – H.R.4962"[79] and "Protecting Cyberspace as a National Asset Act of 2010 – S.3480"[80] in 2010 – none of these has succeeded.

Executive order 13636 *Improving Critical Infrastructure Cybersecurity* was signed February 12, 2013.

Agencies

Homeland Security

The **Department of Homeland Security** has a dedicated division responsible for the response system, **risk management** program and requirements for cybersecurity in the United States called the **National Cyber Security Division**.[81][82] The division is home to US-CERT operations and the National Cyber Alert System.[82] The National Cybersecurity and Communications Integration Center brings together government organizations responsible for protecting computer networks and networked infrastructure.[83]

FBI

The third priority of the **Federal Bureau of Investigation** (FBI) is to: *"Protect the United States against cyber-based attacks and high-technology crimes"*,[84] and they, along with the **National White Collar Crime Center** (NW3C), and the **Bureau of Justice Assistance** (BJA) are part of the multi-agency task force, The **Internet Crime Complaint Center**, also known as IC3.[85]

In addition to its own specific duties, the FBI participates alongside non-profit organizations such as **InfraGard**.[86][87]

Department of Justice

In the **criminal division** of the **United States Department of Justice** operates a section called the **Computer Crime and Intellectual Property Section**. The CCIPS is in charge of investigating computer crime and **intellectual property** crime and is specialized in the search and seizure of **digital evidence** in computers and **networks**.[88]

USCYBERCOM

The United States Cyber Command, also known as USCYBERCOM, is tasked with the defense of specified Department of Defense information networks and *"ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries."*[89] It has no role in the protection of civilian networks.[90][91]

FCC

The U.S. **Federal Communications Commission**'s role in cybersecurity is to strengthen the protection of critical communications infrastructure, to assist in maintaining the reliability of networks during

disasters, to aid in swift recovery after, and to ensure that first responders have access to effective communications services.[92]

Computer Emergency Readiness Team

Computer Emergency Response Team is a name given to expert groups that handle computer security incidents. In the US, two distinct organization exist, although they do work closely together.

• **US-CERT**: part of the **National Cyber Security Division** of the **United States Department of Homeland Security**.[93]

• **CERT/CC**: created by the Defense Advanced Research Projects Agency (DARPA) and run by the **Software Engineering Institute** (SEI).

International actions

Many different teams and organizations exist, including:

• The Forum of Incident Response and Security Teams (FIRST) is the global association of CSIRTs.[94] The US-CERT, **AT&T**, **Apple**, Cisco, McAfee, **Microsoft** are all members of this international team.[95]

• The **Council of Europe** helps protect societies worldwide from the threat of cybercrime through the Convention on Cybercrime.[96]

• The purpose of the Messaging Anti-Abuse Working Group (MAAWG) is to bring the messaging industry together to work collaboratively and to successfully address the various forms of messaging abuse, such as spam, viruses, denial-of-service attacks and other messaging exploitations.[97] France Telecom, **Facebook**, **AT&T**, **Apple**, Cisco, Sprint are some of the members of the MAAWG.[98]

• ENISA : The European Network and Information Security Agency (ENISA) is an agency of the European Union with the objective to improve network and **information security** in the **European Union**.

Europe

CSIRTs in Europe collaborate in the **TERENA** task force TF-CSIRT. **TERENA**'s Trusted Introducer service provides an accreditation and certification scheme for CSIRTs in Europe. A full list of known CSIRTs in Europe is available from the Trusted Introducer website.

National teams

Here are the main **computer emergency response teams** around the world. Most countries have their own team to protect network security.

Canada

On October 3, 2010, Public Safety Canada unveiled Canada's Cyber Security Strategy, following a Speech from the Throne commitment to boost the security of Canadian cyberspace.[99][100] The aim of the strategy is to strengthen Canada's "cyber systems and critical infrastructure sectors, support economic growth and protect Canadians as they connect to each other and to the world."[101] Three main pillars define the strategy: securing government systems, partnering to secure vital cyber systems outside the federal government, and helping Canadians to be secure online.[101] The strategy involves multiple departments and agencies across the Government of Canada.[102] The Cyber Incident Management Framework for Canada outlines these responsibilities, and provides a plan for coordinated response between government and other partners in the event of a cyber incident.[103] The Action Plan 2010–2015 for Canada's Cyber Security Strategy outlines the ongoing implementation of the strategy.[104]

Public Safety Canada's Canadian Cyber Incident Response Centre (CCIRC) is responsible for mitigating and responding to threats to Canada's critical infrastructure and cyber systems. The CCIRC provides support to mitigate cyber threats, technical support to respond and recover from targeted cyber attacks, and provides online tools for members of Canada's critical infrastructure sectors.[105] The CCIRC posts regular cyber security bulletins on the Public Safety Canada website.[106] The CCIRC also operates an online reporting tool where individuals and organizations can report a cyber incident.[107] Canada's Cyber

Security Strategy is part of a larger, integrated approach to critical infrastructure protection, and functions as a counterpart document to the National Strategy and Action Plan for Critical Infrastructure.[102]

On September 27, 2010, Public Safety Canada partnered with STOP.THINK.CONNECT, a coalition of non-profit, private sector, and government organizations dedicated to informing the general public on how to protect themselves online.[108] On February 4, 2014, the Government of Canada launched the Cyber Security Cooperation Program.[109] The program is a $1.5 million five-year initiative aimed at improving Canada's cyber systems through grants and contributions to projects in support of this objective.[110] Public Safety Canada aims to begin an evaluation of Canada's Cyber Security Strategy in early 2015.[102] Public Safety Canada administers and routinely updates the GetCyberSafe portal for Canadian citizens, and carries out Cyber Security Awareness Month during October.[111]

China

China's network security and information technology leadership team was established February 27, 2014. The leadership team is tasked with national security and long-term development and co-ordination of major issues related to network security and information technology. Economic, political, cultural, social and military fields as related to network security and information technology strategy, planning and major macroeconomic policy are being researched. The promotion of national network security and information technology law are constantly under study for enhanced national security capabilities.

Germany

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) **Nationales Cyber-Abwehrzentrum** located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) **Bundesamt für Sicherheit in der Informationstechnik**, BKA (Federal Police Organization) **Bundeskriminalamt (Deutschland)**, BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) **Amt für den Militärischen Abschirmdienst** and other national organizations in Germany taking care of national security aspects. According to the Minister the primary task of the new organization founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like **Stuxnet**.

India

Some provisions for cybersecurity have been incorporated into rules framed under the Information Technology Act 2000.
The **National Cyber Security Policy 2013** is a policy framework by Department of Electronics and Information Technology (DeitY) which aims to protect the public and private infrastructure from cyber attacks, and safeguard "information, such as personal information (of web users), financial and banking information and sovereign data".
The **Indian Companies Act 2013** has also introduced cyber law and cyber security obligations on the part of Indian directors.

Pakistan

Cyber-crime has risen rapidly in Pakistan. There are about 30 million internet users with 15 million mobile subscribers in Pakistan. According to Cyber Crime Unit (CCU), a branch of Federal Investigation Agency, only 62 cases were reported to the unit in 2007, 287 cases in 2008, ratio dropped in 2009 but in 2010, more than 312 cases were registered. But unreported incidents of cyber-crime are huge in numbers.[112] The first ever pertinent law, i.e. "Pakistan's Cyber Crime Bill 2007", which focuses on electronic crimes, i.e. cyber terrorism, criminal access, electronic system fraud, electronic forgery, misuse of encryption etc. has been there.[113]
National Response Centre for Cyber Crime (NR3C) - FIA is a law enforcement agency dedicated to fight cyber crime. Inception of this Hi-Tech crime fighting unit transpired in 2007 to identify and curb the phenomenon of technological abuse in society.[114] However along with that certain private firms are also working in cohesion with Govt to work towards cyber security and curb cyber attacks[115]

South Korea

Following cyberattacks in the first half of 2013, when government, news-media, television station, and bank websites were compromised, the national government committed to the training of 5,000 new

cybersecurity experts by 2017. The South Korean government blamed its northern counterpart for these attacks, as well as incidents that occurred in 2009, 2011,[116] and 2012, but Pyongyang denies the accusations.[117]

Other countries

- CERT **Brazil**, member of FIRST (Forum for Incident Response and Security Teams)
- CARNet CERT, **Croatia**, member of FIRST
- AE CERT, **United Arab Emirates**
- SingCERT, **Singapore**
- CERT-LEXSI, **France**, **Canada**, **Singapore**

Modern warfare

Cybersecurity is becoming increasingly important as more information and technology is being made available on cyberspace. There is growing concern among governments that cyberspace will become the next theatre of warfare. As Mark Clayton from the *Christian Science Monitor* described in an article titled "The New Cyber Arms Race":

In the future, wars will not just be fought by soldiers with guns or with planes that drop bombs. They will also be fought with the click of a mouse a half a world away that unleashes carefully weaponized computer programs that disrupt or destroy critical industries like utilities, transportation, communications, and energy. Such attacks could also disable military networks that control the movement of troops, the path of jet fighters, the command and control of warships.[118]

This has led to new terms such as *cyberwarfare* and *cyberterrorism*. More and more critical infrastructure is being controlled via computer programs that, while increasing efficiency, exposes new vulnerabilities. The test will be to see if governments and corporations that control critical systems such as energy, communications and other information will be able to prevent attacks before they occur. As Jay Cross, the chief scientist of the Internet Time Group, remarked, "Connectedness begets vulnerability."[118]

The cyber security job market

Cyber Security is a fast-growing[119] field of **IT** concerned with reducing organizations' risk of hack or data breach. Commercial, government and non-governmental organizations all employ cybersecurity professionals. However, the use of the term "cybersecurity" is more prevalent in government job descriptions.[120]

Typical cybersecurity job titles and descriptions include:[121]

Security Analyst

Analyzes and assesses vulnerabilities in the infrastructure (software, hardware, networks), investigates available tools and countermeasures to remedy the detected vulnerabilities, and recommends solutions and best practices. Analyzes and assesses damage to the data/infrastructure as a result of security incidents, examines available recovery tools and processes, and recommends solutions. Tests for compliance with security policies and procedures. May assist in the creation, implementation, and/or management of security solutions.

Security Engineer

Performs security monitoring, security and data/logs analysis, and forensic analysis, to detect security incidents, and mounts incident response. Investigates and utilizes new technologies and processes to enhance security capabilities and implement improvements. May also review code or perform other **security engineering** methodologies.

Security Architect

Designs a security system or major components of a security system, and may head a security design team building a new security system.

Security Administrator

Installs and manages organization-wide security systems. May also take on some of the tasks of a security analyst in smaller organizations.

Chief Information Security Officer (CISO)

A high-level management position responsible for the entire information security division/staff. The position may include hands-on technical work.

Chief Security Officer (CSO)

A high-level management position responsible for the entire security division/staff. A newer position now deemed needed as security risks grow.

Security Consultant/Specialist/Intelligence

Broad titles that encompass any one or all of the other roles/titles, tasked with protecting computers, networks, software, data, and/or information systems against viruses, worms, spyware, malware, intrusion detection, unauthorized access, denial-of-service attacks, and an ever increasing list of attacks by hackers acting as individuals or as part of organized crime or foreign governments.

Student programs are also available to people interested in beginning a career in cybersecurity.[122][123] Meanwhile, a flexible and effective option for **information security** professionals of all experience levels to keep studying is online security training, including webcasts.[124][125][126]

Terminology

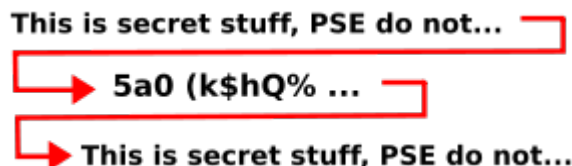The following terms used with regards to engineering secure systems are explained below.

- Access **authorization** restricts access to a computer to group of users through the use of **authentication** systems. These systems can protect either the whole computer – such as through an interactive **login** screen – or individual services, such as an **FTP** server. There are many methods for identifying and authenticating users, such as **passwords**, identification cards, and, more recently, **smart cards** and biometric systems.

- Anti-virus software consists of computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious software (**malware**).

- **Applications** with known security flaws should not be run. Either leave it turned off until it can be patched or otherwise fixed, or delete it and replace it with some other application. Publicly known flaws are the main entry used by **worms** to automatically break into a system and then spread to other systems connected to it. The security website Secunia provides a search tool for unpatched known flaws in popular products.

- **Authentication** techniques can be used to ensure that communication end-points are who they say they are.

- **Automated theorem proving** and other verification tools can enable critical algorithms and code used in secure systems to be mathematically proven to meet their specifications.

- **Backups** are a way of securing information; they are another copy of all the important computer files kept in another location. These files are kept on hard disks, **CD-Rs**, **CD-RWs**, **tapes** and more recently on the cloud. Suggested locations for backups are a fireproof, waterproof, and heat proof safe, or in a separate, offsite location than that in which the original files are contained. Some individuals and companies also keep their backups in **safe deposit boxes** inside **bank vaults**. There is also a fourth option, which involves using one of the **file hosting services** that backs up files over the **Internet** for both business and individuals, known as the cloud.

Backups are also important for reasons other than security. Natural disasters, such as earthquakes, hurricanes, or tornadoes, may strike the building where the computer is located. The building can be on fire, or an explosion may occur. There needs to be a recent backup at an alternate secure location, in case of such kind of disaster. Further, it is recommended that the alternate location be placed where the same disaster would not affect both locations. Examples of alternate disaster recovery sites being compromised by the same disaster that affected the primary site include having had a primary site in **World Trade Center** I and the recovery site in **7 World Trade Center**, both of which were destroyed in the 9/11 attack, and having one's primary site and recovery site in the same coastal region, which leads

to both being vulnerable to hurricane damage (for example, primary site in New Orleans and recovery site in Jefferson Parish, both of which were hit by **Hurricane Katrina** in 2005). The backup media should be moved between the geographic sites in a secure manner, in order to prevent them from being stolen.

- Capability and **access control list** techniques can be used to ensure privilege separation and mandatory access control. **This section** discusses their use.

- **Chain of trust** techniques can be used to attempt to ensure that all software loaded has been certified as authentic by the system's designers.

- **Confidentiality** is the nondisclosure of information except to another authorized person.[127]

- **Cryptographic** techniques can be used to defend data in transit between systems, reducing the probability that data exchanged between systems can be intercepted or modified.

- Cyberwarfare is an Internet-based conflict that involves politically motivated attacks on information and information systems. Such attacks can, for example, disable official websites and networks, disrupt or disable essential services, steal or alter classified data and cripple financial systems.

- **Data integrity** is the accuracy and consistency of stored data, indicated by an absence of any alteration in data between two updates of a data record.[128]

This is secret stuff, PSE do not... →

→ 5a0 (k$hQ% ... →

→ This is secret stuff, PSE do not...

Cryptographic techniques involve transforming information, scrambling it so it becomes unreadable during transmission. The intended recipient can unscramble the message; ideally, eavesdroppers cannot.

- **Encryption** is used to protect the message from the eyes of others. **Cryptographically** secure **ciphers** are designed to make any practical attempt of **breaking** infeasible. **Symmetric-key** ciphers are suitable for bulk encryption using shared keys, and public-key encryption using digital certificates can provide a practical solution for the problem of securely communicating when no key is shared in advance.

- Endpoint security software helps networks to prevent exfiltration (data theft) and virus infection at network entry points made vulnerable by the prevalence of potentially infected portable computing devices, such as laptops and mobile devices, and external storage devices, such as USB drives.[129]

- Firewalls are an important method for control and security on the Internet and other networks. A network firewall can be a communications processor, typically a router, or a dedicated server, along with firewall software. A firewall serves as a gatekeeper system that protects a company's intranets and other computer networks from intrusion by providing a filter and safe transfer point for access to and from the Internet and other networks. It screens all network traffic for proper passwords or other security codes and only allows authorized transmission in and out of the network. Firewalls can deter, but not completely prevent, unauthorized access (hacking) into computer networks; they can also provide some protection from online intrusion.

- **Honey pots** are computers that are either intentionally or unintentionally left vulnerable to attack by crackers. They can be used to catch crackers or fix vulnerabilities.

- Intrusion-detection systems can scan a network for people that are on the network but who should not be there or are doing things that they should not be doing, for example trying a lot of passwords to gain access to the network.

- A **microkernel** is the near-minimum amount of software that can provide the mechaniSMS to implement an operating system. It is used solely to provide very low-level, very precisely defined machine code upon which an operating system can be developed. A simple example is the early '90s GEMSOS (Gemini Computers), which provided extremely low-level machine code, such as "segment" management, atop which an operating system could be built. The theory (in the case of "segments") was that—rather than have the operating system itself worry about mandatory access separation by means of

military-style labeling—it is safer if a low-level, independently scrutinized module can be charged **solely** with the management of individually labeled segments, be they memory "segments" or file system "segments" or executable text "segments." If software below the visibility of the operating system is (as in this case) charged with labeling, there is no theoretically viable means for a clever hacker to subvert the labeling scheme, since the operating system *per se* does **not** provide mechaniSMS for interfering with labeling: the operating system is, essentially, a client (an "application," arguably) atop the microkernel and, as such, subject to its restrictions.

- **Pinging** The ping application can be used by potential crackers to find if an IP address is reachable. If a cracker finds a computer, they can try a port scan to detect and attack services on that computer.

- Social engineering awareness keeps employees aware of the dangers of social engineering and/or having a policy in place to prevent social engineering can reduce successful breaches of the network and servers.
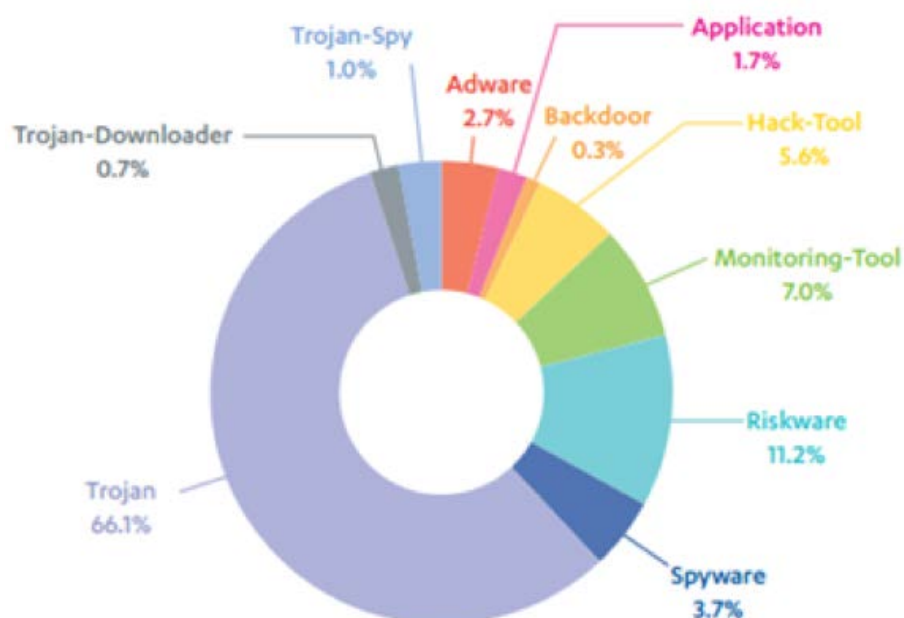
Mobile security

Mobile security or **mobile phone security** has become increasingly important in **mobile computing**. Of particular concern is the **security** of personal and business information now stored on smartphones.

More and more users and businesses employ smartphones as communication tools, but also as a means of planning and organizing their work and private life. Within companies, these technologies are causing profound changes in the organization of information systems and therefore they have become the source of new **risks**. Indeed, smartphones collect and compile an increasing amount of sensitive information to which access must be controlled to protect the **privacy** of the user and the **intellectual property** of the company.

All smartphones, as computers, are preferred targets of attacks. These attacks exploit weaknesses related to smartphones that can come from means of communication like **Short Message Service** (SMS, aka text messaging), **Multimedia Messaging Service** (MMS), Wi-Fi networks, **Bluetooth** and **GSM**, the de facto global standard for mobile communications. There are also attacks that exploit software vulnerabilities from both the web browser and operating system. Finally, there are forms of **malicious software** that rely on the weak knowledge of average users.

Different security counter-measures are being developed and applied to smartphones, from security in different layers of software to the dissemination of information to end users. There are good practices to be observed at all levels, from design to use, through the development of **operating systems**, software layers, and downloadable apps.

Challenges of mobile security

Threats

A smartphone user is exposed to various threats when they use their phone. In just the last two quarters of 2012, the number of unique mobile threats grew by 261%, according to **ABI Research**.[1] These threats can disrupt the operation of the smartphone, and transmit or modify user data. For these reasons, the **applications** deployed there must guarantee **privacy** and **integrity** of the information they handle. In addition, since some apps could themselves be **malware**, their functionality and activities should be limited (for example, restricting the apps from accessing location information via **GPS**, blocking access to the user's address book, preventing the transmission of data on the **network**, sending **SMS** messages that are billed to the user, etc.).

There are three prime targets for attackers:[2]

- **Data**: smartphones are devices for data management, therefore they may contain sensitive data like credit card numbers, authentication information, private information, activity logs (calendar, call logs);

- **Identity**: smartphones are highly customizable, so the device or its contents are associated with a specific person. For example, every mobile device can transmit information related to the owner of the mobile phone contract, and an attacker may want to steal the identity of the owner of a smartphone to commit other offenses;

- **Availability**: by attacking a smartphone one can limit access to it and deprive the owner of the service.

The source of these attacks are the same actors found in the non-mobile computing space:[2]

- **Professionals**, whether commercial or military, who focus on the three targets mentioned above. They steal sensitive data from the general public, as well as undertake industrial espionage. They will also use the identity of those attacked to achieve other attacks;

- **Thieves** who want to gain income through data or identities they have stolen. The thieves will attack many people to increase their potential income;

- **Black hat hackers** who specifically attack availability.[3] Their goal is to develop **viruses**, and cause damage to the device.[4] In some cases, hackers have an interest in stealing data on devices.

- **Grey hat hackers** who reveal vulnerabilities.[5] Their goal is to expose vulnerabilities of the device.[6] **Grey hat** hackers do not intend on damaging the device or stealing data.[7]

Consequences

When a smartphone is infected by an attacker, the attacker can attempt several things:

- The attacker can manipulate the smartphone as a **zombie machine**, that is to say, a machine with which the attacker can communicate and send commands which will be used to send unsolicited messages (**spam**) via **SMS** or **email**;[8]

- The attacker can easily force the smartphone to make **phone calls**. For example, one can use the **API** (library that contains the basic functions not present in the smartphone) PhoneMakeCall by **Microsoft**, which collects telephone numbers from any source such as yellow pages, and then call them.[8] But the attacker can also use this method to call paid services, resulting in a charge to the owner of the smartphone. It is also very dangerous because the smartphone could call emergency services and thus disrupt those services;[8]

- A compromised smartphone can record conversations between the user and others and send them to a third party.[8] This can cause user privacy and industrial security problems;

- An attacker can also steal a user's identity, usurp their identity (with a copy of the user's **sim** card or even the telephone itself), and thus impersonate the owner. This raises security concerns in countries where smartphones can be used to place orders, view bank accounts or are used as an identity card;[8]

- The attacker can reduce the utility of the smartphone, by discharging the battery.[9] For example, they can launch an application that will run continuously on the smartphone processor, requiring a lot of

energy and draining the battery. One factor that distinguishes mobile computing from traditional desktop PCs is their limited performance. Frank Stajano and Ross Anderson first described this form of attack, calling it an attack of "battery exhaustion" or "sleep deprivation torture";[10]

• The attacker can prevent the operation and/or starting of the smartphone by making it unusable.[11] This attack can either delete the boot scripts, resulting in a phone without a functioning **OS**, or modify certain files to make it unusable (e.g. a script that launches at startup that forces the smartphone to restart) or even embed a startup application that would empty the battery;[10]

• The attacker can remove the personal (photos, music, videos, etc.) or professional data (contacts, calendars, notes) of the user.[11]

Attacks based on communication

Attack based on SMS and MMS

Some attacks derive from flaws in the management of **SMS** and **MMS**.

Some mobile phone models have problems in managing binary SMS messages. It is possible, by sending an ill-formed block, to cause the phone to restart, leading to denial of service attacks. If a user with a **Siemens S55** received a text message containing a Chinese character, it would lead to a denial of service.[12] In another case, while the standard requires that the maximum size of a Nokia Mail address is 32 characters, some Nokia phones did not verify this standard, so if a user enters an email address over 32 characters, that leads to complete dysfunction of the e-mail handler and puts it out of commission. This attack is called "curse of silence". A study on the safety of the SMS infrastructure revealed that SMS messages sent from the **Internet** can be used to perform a **distributed denial of service (DDoS)** attack against the mobile telecommunications infrastructure of a big city. The attack exploits the delays in the delivery of messages to overload the network.

Another potential attack could begin with a phone that sends an MMS to other phones, with an attachment. This attachment is infected with a virus. Upon receipt of the MMS, the user can choose to open the attachment. If it is opened, the phone is infected, and the virus sends an MMS with an infected attachment to all the contacts in the address book. There is a real world example of this attack: the virus Commwarrior [11] uses the address book and sends MMS messages including an infected file to recipients. A user installs the software, as received via MMS message. Then, the virus began to send messages to recipients taken from the address book.

Attacks based on communication networks

Attacks based on the GSM networks

The attacker may try to break the encryption of the mobile network. The **GSM** network encryption algorithms belong to the family of algorithms called **A5**. Due to the policy of **security through obscurity** it has not been possible to openly test the robustness of these algorithms. There were originally two variants of the algorithm: **A5/1** and **A5/2** (stream ciphers), where the former was designed to be relatively strong, and the latter was designed to be weak on purpose to allow easy cryptanalysis and eavesdropping. ETSI forced some countries (typically outside Europe) to use **A5/2**. Since the encryption algorithm was made public, it was proved it was possible to break the encryption: **A5/2** could be broken on the fly, and **A5/1** in about 6 hours .[13] In July 2007, the 3GPP approved a change request to prohibit the implementation of **A5/2** in any new mobile phones, which means that is has been decommissioned and is no longer implemented in mobile phones. Stronger public algorithms have been added to the **GSM** standard, the A5/3 and A5/4 (**Block ciphers**), otherwise known as **KASUMI or UEA1**[14] published by the **ETSI**. If the network does not support A5/1, or any other A5 algorithm implemented by the phone, then the base station can specify A5/0 which is the null-algorithm, whereby the radio traffic is sent unencrypted. Even in case mobile phones are able to use **3G** or **4G** which have much stronger encryption than 2G **GSM**, the base station can downgrade the radio communication to 2G **GSM** and specify A5/0 (no encryption) .[15] This is the basis for eavesdropping attacks on mobile radio networks using a fake base station commonly called an **IMSI catcher**.

In addition, tracing of mobile terminals is difficult since each time the mobile terminal is accessing or being accessed by the network, a new temporary identity (TMSI) is allocated to the mobile terminal. The TSMI is used as identity of the mobile terminal the next time it accesses the network. The TMSI is sent to the mobile terminal in encrypted messages.

Once the encryption algorithm of **GSM** is broken, the attacker can intercept all unencrypted communications made by the victim's smartphone.

Attacks based on Wi-Fi
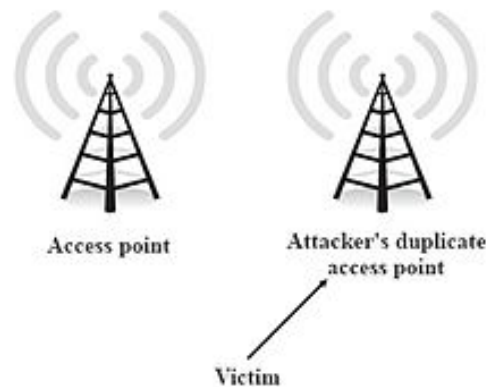
An attacker can try to eavesdrop on **Wi-Fi** communications to derive information (e.g. username, password). This type of attack is not unique to smartphones, but they are very vulnerable to these attacks because very often the Wi-Fi is the only means of communication they have to access the internet. The security of wireless networks (WLAN) is thus an important subject. Initially wireless networks were secured by **WEP** keys. The weakness of WEP is a short encryption key which is the same for all connected clients. In addition, several reductions in the search space of the keys have been found by researchers. Now, most wireless networks are protected by the **WPA** security protocol. WPA is based on the "**Temporal Key Integrity Protocol** (TKIP)" which was designed to allow migration from WEP to WPA on the equipment already deployed. The major improvements in security are the dynamic encryption keys. For small networks, the WPA is a "**pre-shared key**" which is based on a shared key. Encryption can be vulnerable if the length of the shared key is short. With limited opportunities for input (i.e. only the numeric keypad) mobile phone users might define short encryption keys that contain only numbers. This increases the likelihood that an attacker succeeds with a brute-force attack. The successor to WPA, called **WPA2**, is supposed to be safe enough to withstand a brute force attack.

As with GSM, if the attacker succeeds in breaking the identification key, it will be possible to attack not only the phone but also the entire network it is connected to.

Many smartphones for wireless LANs remember they are already connected, and this mechanism prevents the user from having to re-identify with each connection. However, an attacker could create a WIFI access point twin with the same parameters and characteristics as the real network. Using the fact that some smartphones remember the networks, they could confuse the two networks and connect to the network of the attacker who can intercept data if it does not transmit its data in encrypted form.[16][17] [18]

Lasco is a worm that initially infects a remote device using the **SIS file format**.[19] SIS file format (Software Installation Script) is a script file that can be executed by the system without user interaction. The **smartphone** thus believes the file to come from a trusted source and downloads it, infecting the machine.[19]

Principle of Bluetooth-based attacks

Security issues related to **Bluetooth** on mobile devices have been studied and have shown numerous problems on different phones. One easy to exploit **vulnerability**: unregistered services do not require authentication, and vulnerable applications have a virtual serial port used to control the phone. An attacker only needed to connect to the port to take full control of the device.[20] Another example: a phone must be within reach and Bluetooth in discovery mode. The attacker sends a file via Bluetooth. If the recipient accepts, a virus is transmitted. For example: **Cabir** is a worm that spreads via Bluetooth connection.[11] The worm searches for nearby phones with Bluetooth in discoverable mode and sends itself to the target device. The user must accept the incoming file and install the program. After installing, the worm infects the machine.

Attacks based on vulnerabilities in software applications

Other attacks are based on flaws in the OS or applications on the phone.

The mobile web browser is an emerging attack vector for mobile devices. Just as common Web browsers, **mobile web** browsers are extended from pure web navigation with widgets and plug-ins, or are completely native mobile browsers.

Jailbreaking the **iPhone** with firmware 1.1.1 was based entirely on vulnerabilities on the web browser.[21] As a result, the exploitation of the vulnerability described here underlines the importance of the Web browser as an attack vector for mobile devices. In this case, there was a vulnerability based on a stack-based buffer overflow in a library used by the web browser (**Libtiff**).

A vulnerability in the web browser for **Android** was discovered in October 2008. As the iPhone vulnerability above, it was due to an obsolete and vulnerable **library**. A significant difference with the iPhone vulnerability was Android's **sandboxing** architecture which limited the effects of this vulnerability to the Web browser process.

Smartphones are also victims of classic piracy related to the web: **phishing**, malicious websites, etc. The big difference is that smartphones do not yet have strong **antivirus** software available.

Operating system

Sometimes it is possible to overcome the security safeguards by modifying the operating system itself. As real-world examples, this section covers the manipulation of **firmware** and malicious signature certificates. These attacks are difficult.

In 2004, vulnerabilities in virtual machines running on certain devices were revealed. It was possible to bypass the bytecode verifier and access the native underlying operating system. The results of this research were not published in detail. The firmware security of Nokia's **Symbian** Platform Security Architecture (PSA) is based on a central configuration file called SWIPolicy. In 2008 it was possible to manipulate the Nokia firmware before it is installed, and in fact in some downloadable versions of it, this file was human readable, so it was possible to modify and change the image of the firmware.[22] This vulnerability has been solved by an update from Nokia.

In theory smartphones have an advantage over hard drives since the **OS** files are in **ROM**, and cannot be changed by **malware**. However, in some systems it was possible to circumvent this: in the Symbian OS it was possible to overwrite a file with a file of the same name.[22] On the Windows OS, it was possible to change a pointer from a general configuration file to an editable file.

When an application is installed, the **signing** of this application is verified by a series of **certificates**. One can create a valid **signature** without using a valid certificate and add it to the list.[23] In the Symbian OS all certificates are in the directory: c:\resource\swicertstore\dat. With firmware changes explained above it is very easy to insert a seemingly valid but malicious certificate.

Attacks based on hardware vulnerabilities

Electromagnetic Waveforms

In 2015, researchers at the French government agency **ANSSI** demonstrated the capability to trigger the voice interface of certain smartphones remotely by using "specific electromagnetic waveforms".[24] The

exploit took advantage of antenna-properties of headphone wires while plugged into the audio-output jacks of the vulnerable smartphones and effectively spoofed audio input to inject commands via the audio interface.[24]

Juice Jacking

Juice Jacking is a method of physical or a hardware vulnerability specific to mobile platforms. Utilizing the dual purpose of the USB charge port, many devices have been susceptible to having data ex-filtrated from, or malware installed on to a mobile device by utilizing malicious charging kiosks set up in public places, or hidden in normal charge adapters.

Password cracking

In 2010, researcher from the **University of Pennsylvania** investigated the possibility of **cracking a device's password** through a **smudge attack** (literally imaging the finger smudges on the screen to discern the user's password).[25] The researchers were able to discern the device password up to 68% of the time under certain conditions.[25]

Malicious software (malware)

As smartphones are a permanent point of access to the internet (mostly on), they can be compromised as easily as computers with malware.[26] A **malware** is a computer program that aims to harm the system in which it resides. **Trojans**, **worms** and **viruses** are all considered malware. A Trojan is a program that is on the smartphone and allows external users to connect discreetly. A worm is a program that reproduces on multiple computers across a network. A virus is malicious software designed to spread to other computers by inserting itself into legitimate programs and running programs in parallel. However, it must be said that the malware are far less numerous and important to smartphones as they are to computers.
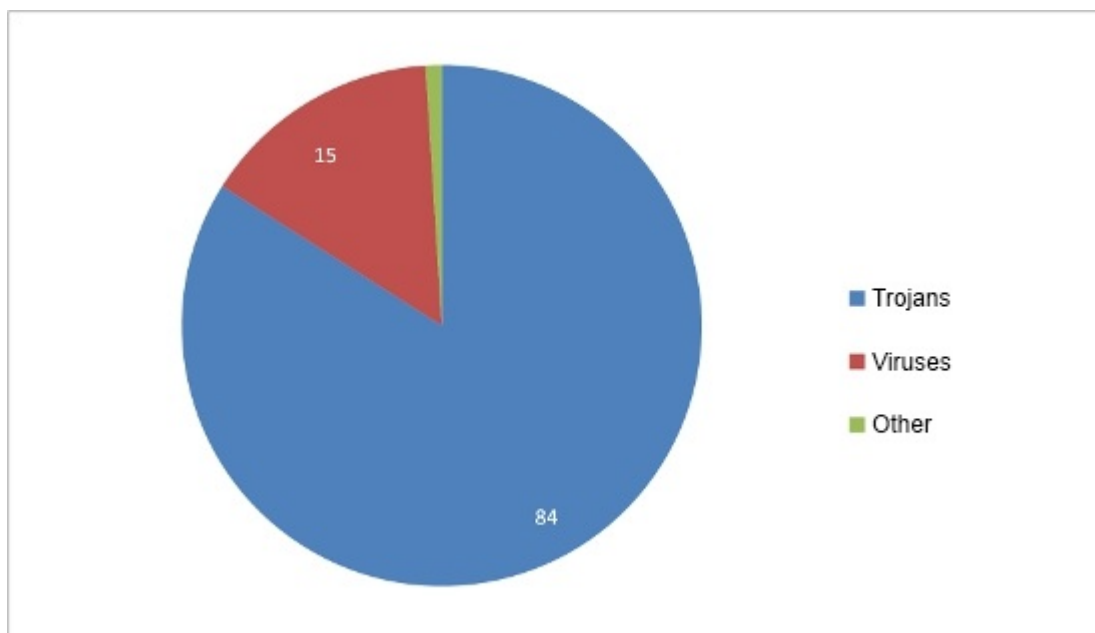
Nonetheless, recent studies show that the evolution of malware in smartphones have rocketed in the last few years posing a threat to analysis and detection.[28]

The three phases of malware attacks

Typically an attack on a smartphone made by malware takes place in 3 phases: the infection of a host, the accomplishment of its goal, and the spread of the malware to other systems. Malware often use the resources offered by the infected smartphones. It will use the output devices such as Bluetooth or

infrared, but it may also use the address book or email address of the person to infect the user's acquaintances. The malware exploits the trust that is given to data sent by an acquaintance.

Infection

Infection is the means used by the malware to get into the smartphone, it can either use one of the faults previously presented or may use the gullibility of the user. Infections are classified into four classes according to their degree of user interaction:[29]

Explicit permission

The most benign interaction is to ask the user if it is allowed to infect the machine, clearly indicating its potential malicious behavior. This is typical behavior of a **proof of concept** malware.

Implied permission

This infection is because the user has a habit of installing software. Most Trojans try to seduce the user into installing attractive applications (games, useful applications etc.) that actually contain malware.

Common interaction

This infection is related to a common behavior, such as opening an MMS or email.

No interaction

The last class of infection is the most dangerous. Indeed, a worm that could infect a smartphone and could infect other smartphones without any interaction would be catastrophic.

Accomplishment of its goal

Once the malware has infected a phone it will also seek to accomplish its goal, which is usually one of the following: monetary damage, damage data and/or device, and concealed damage:[30]

Monetary damages

The attacker can steal user data and either sell them to the same user, or sell to a third party.

Damage

Malware can partially damage the device, or delete or modify data on the device.

Concealed damage

The two aforementioned types of damage are detectable, but the malware can also leave a **backdoor** for future attacks or even conduct wiretaps.

Spread to other systems

Once the malware has infected a smartphone, it always aims to spread one way or another:[31]

- It can spread through proximate devices using Wi-Fi, Bluetooth and infrared;

- It can also spread using remote networks such as telephone calls or SMS or emails.

Examples of malware

Here are various **malware** that exist in the world of **smartphones** with a short description of each.

Viruses and Trojans

- **Cabir** (also known as **Caribe**, **SybmOS/Cabir**, **Symbian/Cabir** and **EPOC.cabir**) is the name of a computer worm developed in 2004 that is designed to infect mobile phones running Symbian OS. It is believed to be the first computer worm that can infect mobile phones

- **Commwarrior**, found March 7, 2005, is the first worm that can infect many machines from **MMS**.[11] It is sent in the form of an archive file COMMWARRIOR.ZIP that contains a file COMMWARRIOR.SIS. When this file is executed, Commwarrior attempts to connect to nearby devices by **Bluetooth** or infrared under a random name. It then attempts to send MMS message to the contacts in the smartphone with different header messages for each person, who receive the MMS and often open them without further verification.

- **Phage** is the first **Palm OS** virus that was discovered.[11] It transfers to the Palm from a PC via synchronization. It infects all applications that are in the smartphone and it embeds its own code to function without the user and the system detecting it. All that the system will detect is that its usual applications are functioning.

- **RedBrowser** is a **Trojan** which is based on java.[11] The Trojan masquerades as a program called "RedBrowser" which allows the user to visit WAP sites without a WAP connection. During application installation, the user sees a request on their phone that the application needs permission to send messages. Therefore, if the user accepts, RedBrowser can send SMS to paid call centers. This program uses the smartphone's connection to social networks (**Facebook**, **Twitter**, etc.) to get the contact information for the user's acquaintances (provided the required permissions have been given) and will send them messages.

- **WinCE.PmCryptic.A** is a malicious software on Windows Mobile which aims to earn money for its authors. It uses the infestation of memory cards that are inserted in the smartphone to spread more effectively.[32]

- **CardTrap** is a virus that is available on different types of smartphone, which aims to deactivate the system and third party applications. It works by replacing the files used to start the smartphone and applications to prevent them from executing.[33] There are different variants of this virus such as **Cardtrap.A** for SymbOS devices. It also infects the memory card with malware capable of infecting **Windows**.

- **Ghost Push** is a malicious software on Android OS which automatically root the android device and installs malicious applications directly to system partition then unroots the device to prevent users from removing the threat by master reset (The threat can be removed only by reflashing). It cripples the system resources, executes quickly, and harder to detect.
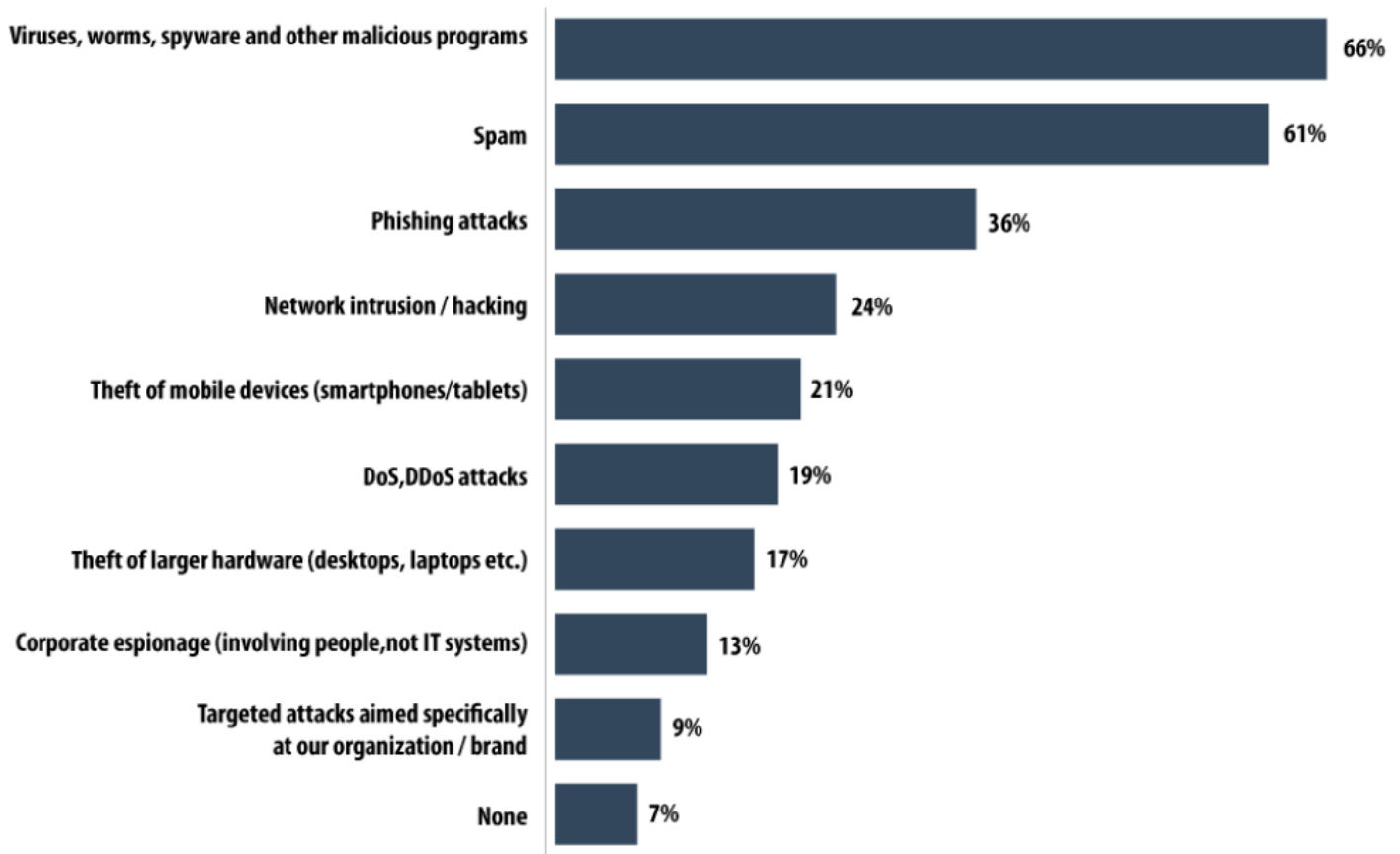
Ransomware

Mobile ransomware is a type of malware that locks users out of their mobile devices in a pay-to-unlock-your-device ploy, it has grown by leaps and bounds as a threat category since 2014.[34] Specific to mobile computing platforms, users are often less security-conscious, particularly as it pertains to scrutinizing applications and web links trusting the native protection capability of the mobile device operating system. Mobile ransomware poses a significant threat to businesses reliant on instant access and availability of their proprietary information and contacts. The likelihood of a traveling businessman paying a ransom to unlock their device is significantly higher since they are at a disadvantage given inconveniences such as timeliness and less likely direct access to IT staff.

Spyware

- **Flexispy** is an application that can be considered as a Trojan, based on Symbian. The program sends all information received and sent from the smartphone to a Flexispy server. It was originally created to protect children and spy on adulterous spouses.[11]

Number of malware

Below is a diagram which loads the different behaviors of smartphone malware in terms of their effects on smartphones:[27]

Category	Percentage
Viruses, worms, spyware and other malicious programs	66%
Spam	61%
Phishing attacks	36%
Network intrusion / hacking	24%
Theft of mobile devices (smartphones/tablets)	21%
DoS,DDoS attacks	19%
Theft of larger hardware (desktops, laptops etc.)	17%
Corporate espionage (involving people,not IT systems)	13%
Targeted attacks aimed specifically at our organization / brand	9%
None	7%

Effects of Malware

We can see from the graph that at least 66% malwares are the majority that exhibits no negative behavior, except their ability to spread.[27]

Portability of malware across platforms

There is a multitude of malware. This is partly due to the variety of operating systems on smartphones. However, attackers can also choose to make their malware target multiple platforms, and malware can be found which attacks an OS but is able to spread to different systems.

To begin with, malware can use runtime environments like **Java virtual machine** or the **.NET Framework**. They can also use other libraries present in many operating systems.[35] Other malware carry several executable files in order to run in multiple environments and they utilize these during the propagation process. In practice, this type of malware requires a connection between the two operating systems to use as an attack vector. Memory cards can be used for this purpose, or synchronization software can be used to propagate the virus.

Countermeasures

The security mechaniSMS in place to counter the threats described above are presented in this section. They are divided into different categories, as all do not act at the same level, and they range from the management of security by the operating system to the behavioral education of the user. The threats prevented by the various measures are not the same depending on the case. Considering the two cases mentioned above, in the first case one would protect the system from corruption by an application, and in the second case the installation of a suspicious software would be prevented.

Security in operating systems

The first layer of security within a smartphone is at the level of the **operating system (OS)**. Beyond the usual roles of an operating system (e.g. resource management, scheduling processes) on a smartphone, it must also establish the protocols for introducing external applications and data without introducing risk.

A central idea found in the mobile operating systems is the idea of a **sandbox**. Since smartphones are currently being designed to accommodate many applications, they must put in place mechaniSMS to ensure these facilities are safe for themselves, for other applications and data on the system, and the user. If a malicious program manages to reach a device, it is necessary that the vulnerable area presented by the system be as small as possible. Sandboxing extends this idea to compartmentalize different processes, preventing them from interacting and damaging each other. Based on the history of operating systems, sandboxing has different implementations. For example, where **iOS** will focus on limiting access to its public API for applications from the **App Store** by default, Managed Open In allows you to restrict which apps can access which types of data. Android bases its sandboxing on its legacy of **Linux** and **TrustedBSD**.

Rootkit Detectors

The intrusion of a **rootkit** in the system is a great danger in the same way as on a computer. It is important to prevent such intrusions, and to be able to detect them as often as possible. Indeed, there is concern that with this type of malicious program, the result could be a partial or complete bypass of the device security, and the acquisition of administrator rights by the attacker. If this happens, then nothing prevents the attacker from studying or disabling the safety features that were circumvented, deploying the applications they want, or disseminating a method of intrusion by a rootkit to a wider audience.[36][37] We can cite, as a defense mechanism, the **Chain of trust** in iOS. This mechanism relies on the signature of the different applications required to start the operating system, and a certificate signed by Apple. In the event that the signature checks are inconclusive, the device detects this and stops the boot-up.[38] If the Operating System is compromised due to **Jailbreaking**, root kit detection may not work if it is disabled by the Jailbreak method or software is loaded after Jailbreak disables Rootkit Detection.

Process isolation

Android uses mechaniSMS of user process isolation inherited from Linux. Each application has a user associated with it, and a tuple (**UID**, **GID**). This approach serves as a **sandbox**: while applications can be malicious, they cannot get out of the sandbox reserved for them by their identifiers, and thus cannot interfere with the proper functioning of the system. For example, since it is impossible for a process to end the process of another user, an application can thus not stop the execution of another.[36][39][40][41][42]

File permissions

From the legacy of Linux, there are also **filesystem permissions** mechaniSMS. They help with sandboxing: a process cannot edit any files it wants. It is therefore not possible to freely corrupt files necessary for the operation of another application or system. Furthermore, in Android there is the method of locking memory permissions. It is not possible to change the permissions of files installed on the SD card from the phone, and consequently it is impossible to install applications.[43][44][45]

Memory Protection

In the same way as on a computer, **memory protection** prevents **privilege escalation**. Indeed, if a process managed to reach the area allocated to other processes, it could write in the memory of a process with rights superior to their own, with root in the worst case, and perform actions which are beyond its permissions on the system. It would suffice to insert function calls are authorized by the privileges of the malicious application.[42]

Development through runtime environments

Software is often developed in high-level languages, which can control what is being done by a running program. For example, **Java Virtual Machines** continuously monitor the actions of the execution threads they manage, monitor and assign resources, and prevent malicious actions. Buffer overflows can be prevented by these controls.[46][47][42]

Security software

Above the operating system security, there is a layer of security software. This layer is composed of individual components to strengthen various vulnerabilities: prevent malware, intrusions, the identification of a user as a human, and user authentication. It contains software components that have learned from their experience with computer security; however, on smartphones, this software must deal with greater constraints.

Antivirus and firewall

An **antivirus software** can be deployed on a device to verify that it is not infected by a known threat, usually by signature detection software that detects malicious executable files. A **firewall**, meanwhile, can watch over the existing traffic on the network and ensure that a malicious application does not seek to communicate through it. It may equally verify that an installed application does not seek to establish suspicious communication, which may prevent an intrusion attempt.[48][49][50][37]

Visual Notifications

In order to make the user aware of any abnormal actions, such as a call they did not initiate, one can link some functions to a visual notification that is impossible to circumvent. For example, when a call is triggered, the called number should always be displayed. Thus, if a call is triggered by a malicious application, the user can see, and take appropriate action.

Turing test

In the same vein as above, it is important to confirm certain actions by a user decision. The **Turing test** is used to distinguish between a human and a virtual user, and it often comes as a **captcha**.

Biometric identification

Another method to use is **biometrics**.[51] Biometrics is a technique of identifying a person by means of their **morphology**(by recognition of the eye or face, for example) or their behavior (their signature or way of writing for example). One advantage of using biometric security is that users can avoid having to remember a password or other secret combination to authenticate and prevent malicious users from accessing their device. In a system with strong biometric security, only the primary user can access the smartphone.

Resource monitoring in the smartphone

When an application passes the various security barriers, it can take the actions for which it was designed. When such actions are triggered, the activity of a malicious application can be sometimes detected if one monitors the various resources used on the phone. Depending on the goals of the malware, the consequences of infection are not always the same; all malicious applications are not intended to harm the devices on which they are deployed. The following sections describe different ways to detect suspicious activity.[52]

Battery

Some malware is aimed at exhausting the energy resources of the phone. Monitoring the energy consumption of the phone can be a way to detect certain malware applications.[36]

Memory usage

Memory usage is inherent in any application. However, if one finds that a substantial proportion of memory is used by an application, it may be flagged as suspicious.

Network traffic

On a smartphone, many applications are bound to connect via the network, as part of their normal operation. However, an application using a lot of bandwidth can be strongly suspected of attempting to communicate a lot of information, and disseminate data to many other devices. This observation only allows a suspicion, because some legitimate applications can be very resource-intensive in terms of network communications, the best example being **streaming video**.

Services

One can monitor the activity of various services of a smartphone. During certain moments, some services should not be active, and if one is detected, the application should be suspected. For example, the sending of an SMS when the user is filming video: this communication does not make sense and is suspicious; malware may attempt to send SMS while its activity is masked.[53]

The various points mentioned above are only indications and do not provide certainty about the legitimacy of the activity of an application. However, these criteria can help target suspicious applications, especially if several criteria are combined.

Network surveillance

Network traffic exchanged by phones can be monitored. One can place safeguards in network routing points in order to detect abnormal behavior. As the mobile's use of network protocols is much more constrained than that of a computer, expected network data streams can be predicted (e.g. the protocol for sending an SMS), which permits detection of anomalies in mobile networks.

Spam filters

As is the case with email exchanges, we can detect a spam campaign through means of mobile communications (SMS, MMS). It is therefore possible to detect and minimize this kind of attempt by filters deployed on network infrastructure that is relaying these messages.

Encryption of stored or transmitted information

Because it is always possible that data exchanged can be intercepted, communications, or even information storage, can rely on **encryption** to prevent a malicious entity from using any data obtained during communications. However, this poses the problem of key exchange for encryption algorithms, which requires a secure channel.

Telecom network monitoring

The networks for SMS and MMS exhibit predictable behavior, and there is not as much liberty compared with what one can do with protocols such as **TCP** or UDP. This implies that one cannot predict the use made of the common protocols of the web; one might generate very little traffic by consulting simple pages, rarely, or generate heavy traffic by using video streaming. On the other hand, messages exchanged via mobile phone have a framework and a specific model, and the user does not, in a normal case, have the freedom to intervene in the details of these communications. Therefore, if an abnormality is found in the flux of network data in the mobile networks, the potential threat can be quickly detected.

Manufacturer surveillance

In the production and distribution chain for mobile devices, it is the responsibility of manufacturers to ensure that devices are delivered in a basic configuration without vulnerabilities. Most users are not experts and many of them are not aware of the existence of security vulnerabilities, so the device configuration as provided by manufacturers will be retained by many users. Below are listed several points which manufacturers should consider.

Remove debug mode

Phones are sometimes set in a debug mode during manufacturing, but this mode must be disabled before the phone is sold. This mode allows access to different features, not intended for routine use by a user. Due to the speed of development and production, distractions occur and some devices are sold in debug mode. This kind of deployment exposes mobile devices to exploits that utilize this oversight.[54][55]

Default settings

When a smartphone is sold, its default settings must be correct, and not leave security gaps. The default configuration is not always changed, so a good initial setup is essential for users. There are, for example, default configurations that are vulnerable to denial of service attacks.[36][56]

Security audit of apps

Along with smart phones, appstores have emerged. A user finds themselves facing a huge range of applications. This is especially true for providers who manage appstores because they are tasked with examining the apps provided, from different points of view (e.g. security, content). The security audit should be particularly cautious, because if a fault is not detected, the application can spread very quickly within a few days, and infect a significant number of devices.[36]

Detect suspicious applications demanding rights

When installing applications, it is good to warn the user against sets of permissions that, grouped together, seem potentially dangerous, or at least suspicious. Frameworks like such as Kirin, on Android, attempt to detect and prohibit certain sets of permissions.[57]

Revocation procedures

Along with appstores appeared a new feature for mobile apps: remote revocation. First developed by Android, this procedure can remotely and globally uninstall an application, on any device that has it. This means the spread of a malicious application that managed to evade security checks can be immediately stopped when the threat is discovered.[58][59]

Avoid heavily customized systems

Manufacturers are tempted to overlay custom layers on existing operating systems, with the dual purpose of offering customized options and disabling or charging for certain features. This has the dual effect of risking the introduction of new bugs in the system, coupled with an incentive for users to modify the systems to circumvent the manufacturer's restrictions. These systems are rarely as stable and reliable as the original, and may suffer from phishing attempts or other exploits.

Improve software patch processes

New versions of various software components of a smartphone, including operating systems, are regularly published. They correct many flaws over time. Nevertheless, manufacturers often do not deploy these updates to their devices in a timely fashion, and sometimes not at all. Thus, vulnerabilities persist when they could be corrected, and if they are not, since they are known, they are easily exploitable.[57]

User awareness

Much malicious behavior is allowed by the carelessness of the user. From simply not leaving the device without a password, to precise control of permissions granted to applications added to the smartphone, the user has a large responsibility in the cycle of security: to not be the vector of intrusion. This precaution is especially important if the user is an employee of a company that stores business data on the device. Detailed below are some precautions that a user can take to manage security on a smartphone.

A recent survey by internet security experts BullGuard showed a lack of insight into the rising number of malicious threats affecting mobile phones, with 53% of users claiming that they are unaware of security software for Smartphones. A further 21% argued that such protection was unnecessary, and 42% admitted it hadn't crossed their mind ("Using APA," 2011). These statistics show consumers are not concerned about security risks because they believe it is not a serious problem. The key here is to always remember smartphones are effectively handheld computers and are just as vulnerable.

Being skeptical

A user should not believe everything that may be presented, as some information may be phishing or attempting to distribute a malicious application. It is therefore advisable to check the reputation of the application that they want to buy before actually installing it.[60]

Permissions given to applications

The mass distribution of applications is accompanied by the establishment of different permissions mechaniSMS for each operating system. It is necessary to clarify these permissions mechaniSMS to users, as they differ from one system to another, and are not always easy to understand. In addition, it is rarely possible to modify a set of permissions requested by an application if the number of permissions is too great. But this last point is a source of risk because a user can grant rights to an application, far beyond the rights it needs. For example, a note taking application does not require access to the geolocation service. The user must ensure the privileges required by an application during installation and should not accept the installation if requested rights are inconsistent.[61][56][62]

Be careful

Protection of a user's phone through simple gestures and precautions, such as locking the smartphone when it is not in use, not leaving their device unattended, not trusting applications, not storing sensitive data, or encrypting sensitive data that cannot be separated from the device.[63][64]

Ensure data

Smartphones have a significant memory and can carry several gigabytes of data. The user must be careful about what data it carries and whether they should be protected. While it is usually not dramatic if

a song is copied, a file containing bank information or business data can be more risky. The user must have the prudence to avoid the transmission of sensitive data on a smartphone, which can be easily stolen. Furthermore, when a user gets rid of a device, they must be sure to remove all personal data first.[65]

These precautions are measures that leave no easy solution to the intrusion of people or malicious applications in a smartphone. If users are careful, many attacks can be defeated, especially phishing and applications seeking only to obtain rights on a device.

Centralized storage of text messages

One form of mobile protection allows companies to control the delivery and storage of text messages, by hosting the messages on a company server, rather than on the sender or receiver's phone. When certain conditions are met, such as an expiration date, the messages are deleted.[66]

Limitations of certain security measures

The security mechaniSMS mentioned in this article are to a large extent inherited from knowledge and experience with computer security. The elements composing the two device types are similar, and there are common measures that can be used, such as **antivirus** and **firewall**. However, the implementation of these solutions is not necessarily possible or at least highly constrained within a mobile device. The reason for this difference is the technical resources offered by computers and mobile devices: even though the computing power of smartphones is becoming faster, they have other limitations than their computing power.

- **Single-task system:** Some operating systems, including some still commonly used, are single-tasking. Only the foreground task is executed. It is difficult to introduce applications such as antivirus and firewall on such systems, because they could not perform their monitoring while the user is operating the device, when there would be most need of such monitoring.

- **Energy autonomy:** A critical one for the use of a smartphone is energy autonomy. It is important that the security mechaniSMS not consume battery resources, without which the autonomy of devices will be affected dramatically, undermining the effective use of the smartphone.

- **Network** Directly related to battery life, network utilization should not be too high. It is indeed one of the most expensive resources, from the point of view of energy consumption. Nonetheless, some calculations may need to be relocated to remote servers in order to preserve the battery. This balance can make implementation of certain intensive computation mechaniSMS a delicate proposition.[67]

Furthermore, it should be noted that it is common to find that updates exist, or can be developed or deployed, but this is not always done. One can, for example, find a user who does not know that there is a newer version of the operating system compatible with the smartphone, or a user may discover known vulnerabilities that are not corrected until the end of a long development cycle, which allows time to exploit the loopholes.[55]

Next Generation of mobile security

There is expected to be four mobile environments that will make up the security framework:[68]

Rich operating system

In this category will fall traditional Mobile OS like Android, iOS, Symbian OS or Windows Phone. They will provide the traditional functionality and security of an OS to the applications.

Secure Operating System (Secure OS)

A secure kernel which will run in parallel with a fully featured Rich OS, on the same processor core. It will include drivers for the Rich OS ("normal world") to communicate with the secure kernel ("secure world"). The trusted infrastructure could include interfaces like the display or keypad to regions of PCI-E address space and memories.

Trusted Execution Environment (TEE)

Made up of hardware and software. It helps in the control of access rights and houses sensitive applications, which need to be isolated from the Rich OS. It effectively acts as a firewall between the "normal world" and "secure world".

Secure Element (SE)

The SE consists of tamper resistant hardware and associated software. It can provide high levels of security and work in tandem with the TEE. The SE will be mandatory for hosting proximity payment applications or official electronic signatures.

References

Books

1. *Bishop, Matt (2004). Introduction to Computer Security. Addison Wesley Professional.* **ISBN 978-0-321-24744-5**.
2. *Dunham, Ken; Abu Nimeh, Saeed; Becher, Michael (2008).* **Mobile Malware Attack and Defense**. *Syngress Media.* **ISBN 978-1-59749-298-0**.
3. *Rogers, David (2013).* **Mobile Security: A Guide for Users**. *Copper Horse Solutions Limited.* **ISBN 978-1-291-53309-5**.

[1] **"Air Traffic Control Systems Vulnerabilities Could Make for Unfriendly Skies [Black Hat] - SecurityWeek.Com"**.

[2] **"Hacker Says He Can Break Into Airplane Systems Using In-Flight Wi-Fi"**. *NPR.org. 4 August 2014.*

[3] *Jim Finkle (4 August 2014).* **"Hacker says to show passenger jets at risk of cyber attack"**. *Reuters.*

[4] **"Is Your Watch Or Thermostat A Spy? Cybersecurity Firms Are On It"**. *NPR.org. 6 August 2014.*

[5] *Melvin Backman (18 September 2014).* **"Home Depot: 56 million cards exposed in breach". CNN Money**.

[6]**"Staples: Breach may have affected 1.16 million customers' cards"**. *Fortune.com. December 19, 2014*. Retrieved *2014-12-21*.

[7] **"Target security breach affects up to 40M cards"**. *Associated Press via Milwaukee Journal Sentinel. 19 December 2013*. Retrieved *21 December* 2013*.

[8] *Bright, Peter (February 15, 2011).* **"Anonymous speaks: the inside story of the HBGary hack"**. *Arstechnica.com*. Retrieved *March 29,* 2011.

[9] *Anderson, Nate (February 9, 2011).* **"How one man tracked down Anonymous—and paid a heavy price"**. *Arstechnica.com*. Retrieved *March 29,* 2011.

[10] *Palilery, Jose (December 24, 2014).* **"What caused Sony hack: What we know now"**. *CNN Money*. Retrieved *January 4,* 2015.

[11] *James Cook (December 16, 2014).* **"Sony Hackers Have Over 100 Terabytes Of Documents. Only Released 200 Gigabytes So Far". Business Insider**. Retrieved *December 18,* 2014.

[12] *Timothy B. Lee (18 January 2015).* **"The next frontier of hacking: your car"**. *Vox.*

[13] **http://www.autosec.org/pubs/cars-usenixsec2011.pdf**

[14] **http://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf**

[15] **"Internet strikes back: Anonymous' Operation Megaupload explained"**. *RT. January 20, 2012.* **Archived** *from the original on May 5, 2013*. Retrieved *May 5,* 2013.

[16] **"Gary McKinnon profile: Autistic 'hacker' who started writing computer programs at 14"**. *The Daily Telegraph (London). 23 January 2009.*

[17] **"Gary McKinnon extradition ruling due by 16 October"**. *BBC News. September 6, 2012*. Retrieved *September 25,* 2012.

[18] *Law Lords Department (30 July 2008).* **"House of Lords – Mckinnon V Government of The United States of America and Another"**. *Publications.parliament.uk. Retrieved 30 January* 2010.

[19] **"NSA Accessed Mexican President's Email"**, October 20, 2013, Jens Glüsing, Laura Poitras, Marcel Rosenbach and Holger Stark, spiegel.de

[20] *Sanders, Sam (4 June 2015).* **"Massive Data Breach Puts 4 Million Federal Employees' Records At Risk"**. *NPR. Retrieved 5 June* 2015.

[21] *Liptak, Kevin (4 June 2015).* **"U.S. government hacked; feds think China is the culprit"**. *CNN*. Retrieved *5 June* 2015.

[22] *Sean Gallagher.* **"Encryption "would not have helped" at OPM, says DHS official"**.

[23] Cashell, B., Jackson, W. D., Jickling, M., & Webel, B. (2004). The Economic Impact of Cyber-Attacks. Congressional Research Service, Government and Finance Division. Washington DC: The Library of Congress.

[24] *Gordon, Lawrence; Loeb, Martin (November 2002). "The Economics of Information Security Investment". ACM Transactions on Information and System Security* **5** *(4): 438–457.* **doi:10.1145/581271.581274**.

[25] **RFC 2828** Internet Security Glossary

[26] **CNSS Instruction No. 4009** dated 26 April 2010

[27] **"Firms lose more to electronic than physical theft"**. *Reuters*.

[28] *Harrison, J. (2003). "Formal verification at Intel": 45–54.* **doi:10.1109/LICS.2003.1210044**.

[29] **Formal verification of a real-time hardware design**. Portal.acm.org (1983-06-27). Retrieved on April 30, 2011.

[30] **"Abstract Formal Specification of the seL4/ARMv6 API"** *(PDF). Retrieved May 19,* 2015.

[31] Christoph Baumann, Bernhard Beckert, Holger Blasum, and Thorsten Bormer **Ingredients of Operating System Correctness? Lessons Learned in the Formal Verification of PikeOS**

[32] **"Getting it Right"** by Jack Ganssle

[33] **Definitions: IT Security Architecture**. SecurityArchitecture.org, Jan, 2006

[34] *Jannsen, Cory.* **"Security Architecture"**. *Techopedia. Janalta Interactive Inc*. Retrieved *9 October* 2014.

[35] **"The Hacker in Your Hardware: The Next Security Threat"**. *Scientific American*.

[36] *Waksman, Adam; Sethumadhavan, Simha (2010),* **"Tamper Evident Microprocessors"** *(PDF), Proceedings of the IEEE Symposium on Security and Privacy (Oakland, California)*

[37] **"Sentinel HASP HL"**. *E-Spin. Retrieved 2014-03-20*.

[38] **"Token-based authentication"**. *SafeNet.com. Retrieved 2014-03-20*.

[39] **"Lock and protect your Windows PC"**. *TheWindowsClub.com. Retrieved 2014-03-20*.

[40] *James Greene (2012).* **"Intel Trusted Execution Technology: White Paper"** *(PDF). Intel Corporation*. Retrieved *2013-12-18*.

[41] **"SafeNet ProtectDrive 8.4"**. *SCMagazine.com. 2008-10-04. Retrieved 2014-03-20*.

[42] **"Secure Hard Drives: Lock Down Your Data"**. *PCMag.com. 2009-05-11*.

[43] **"Top 10 vulnerabilities inside the network"**. **Network World**. *2010-11-08. Retrieved 2014-03-20*.

[44] **"Forget IDs, use your phone as credentials"**. **Fox Business Network**. *2013-11-04. Retrieved 2014-03-20*.

[45] Steve Lipner, "The Birth and Death of the Orange Book," *IEEE Annals of the History of Computing* 37 no. 2 (2015): 19-31

[46] *Kelly Jackson Higgins (2008-11-18).* **"Secure OS Gets Highest NSA Rating, Goes Commercial"**. *Dark Reading. Retrieved 2013-12-01*.

[47] **"Board or bored? Lockheed Martin gets into the COTS hardware biz"**. *VITA Technologies Magazine. December 10, 2010*. Retrieved *9 March* 2012.

[48] *Sanghavi, Alok (21 May 2010). "What is formal verification?". EE Times_Asia.*

[49] Jonathan Zittrain, 'The Future of The Internet', Penguin Books, 2008

[50] **Information Security**. United States Department of Defense, 1986

[51] **"THE TJX COMPANIES, INC. VICTIMIZED BY COMPUTER SYSTEMS INTRUSION; PROVIDES INFORMATION TO HELP PROTECT CUSTOMERS"** (Press release). The TJX Companies, Inc. 2007-01-17*. Retrieved *2009-12-12.*

[52] **Largest Customer Info Breach Grows**. MyFox Twin Cities, 29 March 2007.

[53] **"The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought"**. *Business Insider. 20 November 2013.*

[54] *Reals, Tucker (24 September 2010).* **"Stuxnet Worm a U.S. Cyber-Attack on Iran Nukes?"**. *CBS News.*

[55] *Kim Zetter (17 February 2011).* **"Cyberwar Issues Likely to Be Addressed Only After a Catastrophe"**. *Wired.* Retrieved *18 February* 2011*.

[56] *Chris Carroll (18 October 2011).* **"Cone of silence surrounds U.S. cyberwarfare"**. *Stars and Stripes.* Retrieved *30 October* 2011*.

[57] *John Bumgarner (27 April 2010).* **"Computers as Weapons of War"** (PDF). IO Journal*. Retrieved *30 October* 2011*.

[58] **"New Snowden Leak: NSA Tapped Google, Yahoo Data Centers"**, Oct 31, 2013, Lorenzo Franceschi-Bicchierai, mashable.com

[59] *Seipel, Hubert.* **"Transcript: ARD interview with Edward Snowden"**. *La Foundation Courage.* Retrieved *11 June* 2014*.

[60] *Michael Riley, Ben Elgin, Dune Lawrence, Carol Matlack.* **"Target Missed Warnings in Epic Hack of Credit Card Data - Businessweek"**. *Businessweek.com.*

[61] **"Home Depot says 53 million emails stolen"**. *CNET. CBS Interactive. 6 November 2014.*

[62] *Mansfield-Devine, Steve (2015-09-01).* **"The Ashley Madison affair"**. *Network Security* **2015** *(9): 8–16.* **doi:10.1016/S1353-4858(15)30080-5.**

[63] **"Mikko Hypponen: Fighting viruses, defending the net"**. *TED.*

[64] **"Mikko Hypponen – Behind Enemy Lines"**. *Hack In The Box Security Conference.*

[65] **"Ensuring the Security of Federal Information Systems and Cyber Critical Infrastructure and Protecting the Privacy of Personally Identifiable Information"**. *Government Accountability Office.* Retrieved *November 3,* 2015.

[66] *Kirby, Carrie (June 24, 2011).* **"Former White House aide backs some Net regulation / Clarke says government, industry deserve 'F' in cybersecurity"**. *The San Francisco Chronicle.*

[67] **"Text of H.R.4962 as Introduced in House: International Cybercrime Reporting and Cooperation Act – U.S. Congress"**. *OpenCongress.* Retrieved *2013-09-25.*

[68] **"National Cyber Security Division"**. *U.S. Department of Homeland Security.* Retrieved *June 14,* 2008.

[69] **"FAQ: Cyber Security R&D Center"**. *U.S. Department of Homeland Security S&T Directorate.* Retrieved *June 14,* 2008.

[70] AFP-JiJi, "U.S. boots up cybersecurity center", October 31, 2009.

[71] **"Federal Bureau of Investigation – Priorities"**. *Federal Bureau of Investigation.*

[72] **"Infragard, Official Site"**. *Infragard.* Retrieved *10 September* 2010*.

[73] **"Robert S. Mueller, III -- InfraGard Interview at the 2005 InfraGard Conference"**. *Infragard (Official Site) -- "Media Room".* Retrieved *9 December* 2009*.

[74] U.S. Department of Defense, Cyber Command Fact Sheet, May 21, 2010 **http://www.stratcom.mil/factsheets/Cyber_Command/**

[75] *"Speech:".* Defense.gov. Retrieved *2010-07-10.*

[76] Shachtman, Noah. **"Military's Cyber Commander Swears: "No Role" in Civilian Networks"**, **The Brookings Institution**, 23 September 2010.

[77] *Verton, Dan (January 28, 2004).* **"DHS launches national cyber alert system"**. *Computerworld (IDG).* Retrieved *2008-06-15.*

[78] **"Government of Canada Launches Canada's Cyber Security Strategy"**. *Market Wired. 3 October 2010.* Retrieved *1 November* 2014*.*

[79]**"Canada's Cyber Security Strategy"**. *Public Safety Canada. Government of Canada*. Retrieved *1 November* 2014*.*

[80] **"Action Plan 2010–2015 for Canada's Cyber Security Strategy"**. *Public Safety Canada. Government of Canada*. Retrieved *3 November* 2014*.*

[81] **"Cyber Incident Management Framework For Canada"**. *Public Safety Canada. Government of Canada*. Retrieved *3 November* 2014*.*

[82] **"Action Plan 2010–2015 for Canada's Cyber Security Strategy"**. *Public Safety Canada. Government of Canada*. Retrieved *1 November* 2014*.*

[83]**"Canadian Cyber Incident Response Centre"**. *Public Safety Canada*. Retrieved *1 November* 2014*.*

[84] **"Cyber Security Bulletins"**. *Public Safety Canada*. Retrieved *1 November* 2014*.*

[85] **"Report a Cyber Security Incident"**. *Public Safety Canada. Government of Canada*. Retrieved *3 November* 2014*.*

[86] **"Government of Canada Launches Cyber Security Awareness Month With New Public Awareness Partnership"**. *Market Wired (Government of Canada). 27 September 2012*. Retrieved *3 November* 2014*.*

[87] **"Cyber Security Services Pakistan"**. *Tier3 - Cyber Security Services Pakistan.*

[88] *"South Korea seeks global support in cyber attack probe". BBC Monitoring Asia Pacific. 7 March 2011.*

[89] *Kwanwoo Jun (23 September 2013).* **"Seoul Puts a Price on Cyberdefense"**. *Wall Street Journal. Dow Jones & Company, Inc*. Retrieved *24 September* 2013*.*

[90] Clayton, Mark. **"The new cyber arms race"**. *The Christian Science Monitor*. Retrieved *16 April* 2015*.*

[91]**"The Growth of Cybersecurity Jobs"**. *Mar 2014*. Retrieved *24 April* 2014*.*

[92] *de Silva, Richard (11 Oct 2011).* **"Government vs. Commerce: The Cyber Security Industry and You (Part One)"**. *Defense IQ*. Retrieved *24 Apr* 2014*.*

[93] **"(Information for) Students"**. *NICCS (US National Initiative for Cybercareers and Studies)*. Retrieved *24 April* 2014*.*

* Mr. Nikola Zlatanov spent over 20 years working in the Capital Semiconductor Equipment Industry. His work at Gasonics, Novellus, Lam and KLA-Tencor involved progressing electrical engineering and management roles in disruptive technologies. Nikola received his Undergraduate degree in Electrical Engineering and Computer Systems from Technical University, Sofia, Bulgaria and completed a Graduate Program in Engineering Management at Santa Clara University. He is currently consulting for Fortune 500 companies as well as Startup ventures in Silicon Valley, California.