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. It includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data and code injection, and due to malpractice by operators, whether intentional, accidental, or due to them being tricked into deviating from secure procedures.

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 â€“ 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.

If access is gained to a car's internal controller area network, it is possible to disable the brakes and turn the steering wheel. 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 wifi 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. Researchers in 2011 were even able to use a malicious compact disc in a car's stereo system as a successful attack vector, and cars with built-in voice recognition or remote assistance features have onboard microphones which could be used for eavesdropping.

However, relatively few organisations maintain computer systems with effective detection systems, and fewer still have organised 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". The primary obstacle

to effective eradication of cyber crime 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.

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" 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 and several military jets.

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.

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.

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,

APPROVED
By Guest at 3/25/2024 6:14:02 PM

CONFIDENTIAL
By Guest at 3/25/2024 6:14:06 PM

NOT APPROVED
By Guest at 3/25/2024 6:14:09 PM

RECEIVED
By Guest at 3/25/2024 6:14:14 PM

REVIEWED
By Guest at 3/25/2024 6:14:20 PM

REVISED
By Guest at 3/25/2024 6:14:27 PM

SIGN HERE

APPROVED

CONFIDENTIAL

INITIAL HERE

WITNESS

COMPLETED

DRAFT

FINAL

FOR COMMENT

FOR PUBLIC RELEASE

INFORMATION ONLY

NOT APPROVED

NOT FOR PUBLIC RELEASE

PRELIMINARY RESULTS

VOID

activated after a successful breach.

computer can be tricked into indirectly allowing restricted file access, an issue known as the confu. It h t t ving access to an object to only one pe nt p me st in responsibility to ensure that they do not introduce flaws [citation needed]

er cr Laboratory, the US Air Force's main command and research facility. Using trojan horses, le co ng 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 National Aeronautics and Space Administration'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.

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 â€œAvid 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.â€ 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.

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." 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.

On October 3, 2010, Public Safety Canada unveiled Canadaâ€™s Cyber Security Strategy, following a Speech from the Throne commitment to boost the security of Canadian cyberspace. The aim of the strategy is to strengthen Canadaâ€™s "cyber systems and critical infrastructure sectors, support economic growth and protect Canadians as they connect to each other and to the world." 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. The strategy involves multiple departments and agencies across the Government of Canada. 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. The Action Plan 2010â€“2015 for Canada's Cyber Security Strategy outlines the ongoing implementation of the strategy.

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.

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.

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."

While hardware may be a source of insecurity, such as with microchip vulnerabilities maliciously introduced during the manufacturing process, 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.

Public Safety Canadaâ€™s Canadian Cyber Incident Response Centre (CCIRC) is responsible for mitigating and responding to threats to Canadaâ€™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 Canadaâ€™s critical infrastructure sectors. The CCIRC posts regular cyber security bulletins on the Public Safety Canada website. The CCIRC also operates an online reporting tool where individuals and organizations can report a cyber incident. 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.

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."

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. On February 4, 2014, the Government of Canada launched the Cyber Security Cooperation Program. The program is a $1.5 million five-year initiative aimed at improving Canadaâ€™s cyber systems through grants and contributions to projects in support of this objective. Public Safety Canada aims to begin an evaluation of Canada's Cyber Security Strategy in early 2015. Public Safety Canada administers and routinely updates the GetCyberSafe portal for Canadian citizens, and carries out Cyber Security Awareness Month during October.

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 by passed 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.

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.

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 â€“ the first internet "computer worm". 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'.

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, and then Home Depot computers in 2014, stealing between 53 and 56 million credit card numbers. 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 â€“ 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.

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 fÃ¼r Sicherheit in der Informationstechnik, BKA (Federal Police Organisation) Bundeskriminalamt (Deutschland), BND (Federal Intelligence Service) Bundesnachrichtendienst, MAD (Military Intelligence Service) Amt fÃ¼r den MilitÃ¤rischen Abschirmdienst and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like Stuxnet.