6 Cyber Security

Introduction

6.1.1 A Brief History

The Internet was launched in the 1960s when researchers were working on packet switching networks such as the Advanced Research Projects Agency Network (ARPANET) as well as the protocol for Inter-networking. Security threats were not high on the list then as the focus was on having a robust, fault-tolerant and distributed computer network.

Computer misuse was controllable since interconnected systems were sparse and well within the border of organisations. Access to devices was limited to only the researchers and scientists or those with the right funding.

In the 1980s, access to ARPANET was expanded, partly due to the National Science Foundation's development of the Computer Science Network (CSNET). Around the same time, the Internet Protocol Suite (TCP/IP), as we know it today, was standardised; the concept of a worldwide network of fully interconnected networks was introduced and the Internet was born.

A series of events that followed saw the rapid commercialisation of the Internet which has been growing at an exponential rate. Every day, new services that have the potential of changing and impacting culture, values and the inter-operation of societies are created. These developments have made the Internet an integral part of our lives today.

The association of the Internet with infocomm technology (ICT) has given rise to the term, "cyberspace." The United States National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD23) defines "cyberspace" as the interdependent network of information technology infrastructures which includes the Internet, telecommunications networks, computer systems, embedded processors and controllers in critical industries.[1]

ICT touches almost everything and everyone in the modern world. In cyberspace, we are so interconnected digitally that people, both good and bad actors,[2] separated miles apart, are just a few clicks away. The current economic value and dependency on cyberspace have reached a level that exploitation, even in a limited form, can yield enormous returns and impact. Part of this realisation is reinforced by the increased activity of technology-enabled crimes.

Technology-enabled crimes are also known as high-tech crime, computer crimes or cybercrime. They include crimes committed directly against computers and computer systems, as well as the use of technology to commit or facilitate the commission of traditional crimes, bringing unique challenges to law enforcement.

---

1 United States Army Combined Arms Center. Cyberspace. [Online] Available from: http://usacac.army.mil/cac2/call/thesaurus/toc.asp?id=9140 [Accessed 9th July 2012].

2 "Actors" refer to "participants or perpetrators." This and other terms will be referred to frequently in the discussion on cyber security.

IT security in ICT, with the association of the Internet, has evolved into cyber security as we know it today.

Security is an integral part of any technology trend and includes related issues such as incident response process and security personnel proficiency. An IT security incident refers to an event that has the potential to impact the confidentiality, availability or integrity of an entity's IT resources.[3] An incident response process includes discovery, documentation, notification, acknowledgement, containment, investigation, resolution and closure. Apart from process and procedure, the human element in security maintenance and management is critical to the containment of the security threat. In this regard, the competence and professionalism of security personnel is an important element of IT security.

6.1.2 Five Cyber Security Incidents

Defence: RSA Security Breach - March 2011

On 7 March 2011, RSA Security reported a security breach, the result of an "extremely sophisticated" attack.[4] In June 2011, RSA confirmed that stolen data about the company's SecurID authentication token was used in an attack against defence contractor, Lockheed Martin. RSA believed that the likely motive was to take data that could be used against defence contractors rather than against financial institutions or to steal personal information. The initial RSA breach was described by the company as an Advanced Persistent Threat (APT) that targeted information related to the SecurID two-factor authentication product. Researchers believe that a keystroke logger was placed on a computer used for remote log-in, possibly through a spear-phishing attack, and was able to steal a user ID, PIN and several one-time passcodes.

E-mail: Epsilon Security Breach - April 2011

Epsilon, the largest distributor of permission-based e-mail in the world and an online marketing unit of Alliance Data that had some 2,500 clients, suffered a security breach on 4 April 2011 that exposed the e-mail addresses of 2% of its customers that included some of the largest companies in the USA such as Barclays Bank, Walt Disney, Marriott, Ritz-Carlton, College Board, JP Morgan Chase, CitiBank and Target.[5]

The breach was significant and was described as a "massive haemorrhage," leading to immediate customer alerts by banks and retailers worried about a surge in phishing attacks that could steal personal information like bank account numbers or passwords. Epsilon's customers who were affected by the breach feared the possibility of cyber criminals linking addresses with names and businesses such as banks and thereafter, devising highly customised attacks to trick people into disclosing more confidential information.

---

[3] http://www.it.ufl.edu/policies/security/uf-it-sec-incident-response.html

[4] William Jackson. RSA confirms its tokens used in Lockheed hack. [Online] Available from: http://gcn.com/articles/2011/06/07/rsa-confirms-tokens-used-to-hack-lockheed.aspx [Accessed 9th July 2012].

[5] Miguel Helft. After Breach, Companies Warn of E-Mail Fraud. [Online] Available from: http://www.nytimes.com/2011/04/05/business/05hack.html?_r=1 [Accessed 9th July 2012].

This spear-phishing possibility was perceived as being more dangerous than traditional phishing attacks because it would be more targeted, using personal names and associations, thus gaining greater credibility from potential victims.

Gaming: Sony's Two Security Breaches - 16-19 April 2011

On 3 May 2011, Sony admitted that 25 million customers who played games on its Sony Online Entertainment (SOE) PC games network had had their personal details stolen on 16 and 17 April 2011. The names, addresses, e-mail, birth dates, phone numbers and other information from PC games customers were taken before the theft of another 77 million users' details on the Playstation Network (PSN) from 17 to 19 April 2011.[6]

The global reach of the second breach extended to 23,400 people outside the USA. This number included 10,700 direct debit records for customers in Austria, Germany, the Netherlands and Spain.

The SOE network hosted games played on PCs over the Internet and was separate from the PSN which connects PlayStations online. The latter enabled gamers to download software and compete with other members. PSN's biggest market included North America and Europe, home to almost 90% of the users of the network.

The SOE network was taken down on 2 May 2011 and Sony suspended its SOE games on Facebook because of "microtransactions" online – it was afraid that the sale of virtual goods, if subverted, could be used by hackers to make illicit transactions.

On 23 May 2011, Sony estimated that direct costs from the PSN hack would total US$171 million.[7] This included estimates for an identity theft program and costs for a “Welcome Back” package but excluded outcomes of potential class action suits. On 23 October 2012, the class action suit against Sony was dismissed by a US District Court judge, clearing it of any major wrongdoing (including negligence, unjust enrichment, bailment and violations of California consumer protection statutes) in the case.[8]

Retail: The Zappos Security Breach - January 2012

In an incident reminiscent of the Epsilon security breach in April 2011, Zappos Retail Inc, an Amazon Inc unit and one of the world's largest online footwear and accessories sellers with 24 million customers, suffered a data breach when cyber thieves obtained “one or more” elements of customers' personal data, including names, e-mail addresses, billing and

---

[6] Charles Arthur and agencies. Sony suffers second data breach with theft of 25M more user details. [Online] Available from: http://www.guardian.co.uk/technology/blog/2011/may/03/sony-data-breach-online-entertainment [Accessed 9th July 2012].

[7] Mark Hachman. PlayStation Hack to Cost Sony $171M; Quake Costs Far Higher. [Online] Available from: http://www.pcmag.com/article2/0,2817,2385790,00.asp [Accessed 9th July 2012].

[8] Sony data breach lawsuit largely dismissed. [Online] Available from: http://www.infosecurity-magazine.com/view/28945/sony-data-breach-lawsuit-largely-dismissed [Accessed 3rd November 2012].

shipping addresses, and phone numbers, along with the last four digits of credit card numbers.[9]

This incident was "bad news" for merchants because it told them that scrupulously following the Payment Card Industry Data Security Standard guidelines was no longer sufficient protection against hackers seeking other types of stored customer information useful for perpetrating fraud.

Online retailers are learning that they might need to consider encrypting all types of customer data, not just payment card data, to prevent the occurrence of e-mail or telephone scams that might attempt to use data obtained in the breach to extract further data for fraudulent purposes.

Social Networks: LinkedIn Breach – June 2012

LinkedIn, a business-focused social network with 161 million users worldwide as of 31 March 2012,[10] suffered a major breach of its password database when it experienced a hacking of 6.46 million encrypted passwords in June 2012.

An online forum in Russia featured a file containing the leaked passwords shortly thereafter. The file contained passwords that were hashed using the SHA-1 algorithm and did not include user names or other data. However, the breach was so serious that security professionals and LinkedIn advised affected users to change their LinkedIn passwords immediately.

The risk is that hackers who know that the password is hashed with the SHA-1 algorithm will be able to quickly uncover some of the more basic passwords that people commonly use. LinkedIn responded by "salting" the passwords, a process that adds random bits ("salt") to the hash so as to make it more difficult to guess the output.

Online users who have the habit of using the same passwords for different sites, including mobile banking, e-commerce, e-mail and social networks, should learn to use different, unique passwords so that a "break-in" does not compromise the security of all their online correspondences and transactions.

6.1.3 Cyber Security – A Growing Concern

The security of the cyberspace or cyber security is such a critical concern that it is projected to be among the fastest growing segments of the Information Technology (IT) sector in the next three to five years. The growth is due to significant investments from companies trying to secure their computing environments.

---

[9] Kate Fitzgerald. Zappos Breach: When Good Data Security Wasn't Good Enough. [Online] Available from: http://www.americanbanker.com/issues/177_11/zappos-shoe-data-breach-pci-1045779-1.html [Accessed 9th July 2012].

[10] Ian Paul. Update: LinkedIn Confirms Account Passwords Hacked. [Online] Available from: http://www.pcworld.com/article/257045/update_linkedin_confirms_account_passwords_hacked.html [Accessed 9th July 2012].

Fuelling the rise further is the increasing adoption of cloud computing, new networks, bigger data centres and mobile wireless communication devices. Services increasingly required are in the area of security installations, security operations, managed security services and consulting services.

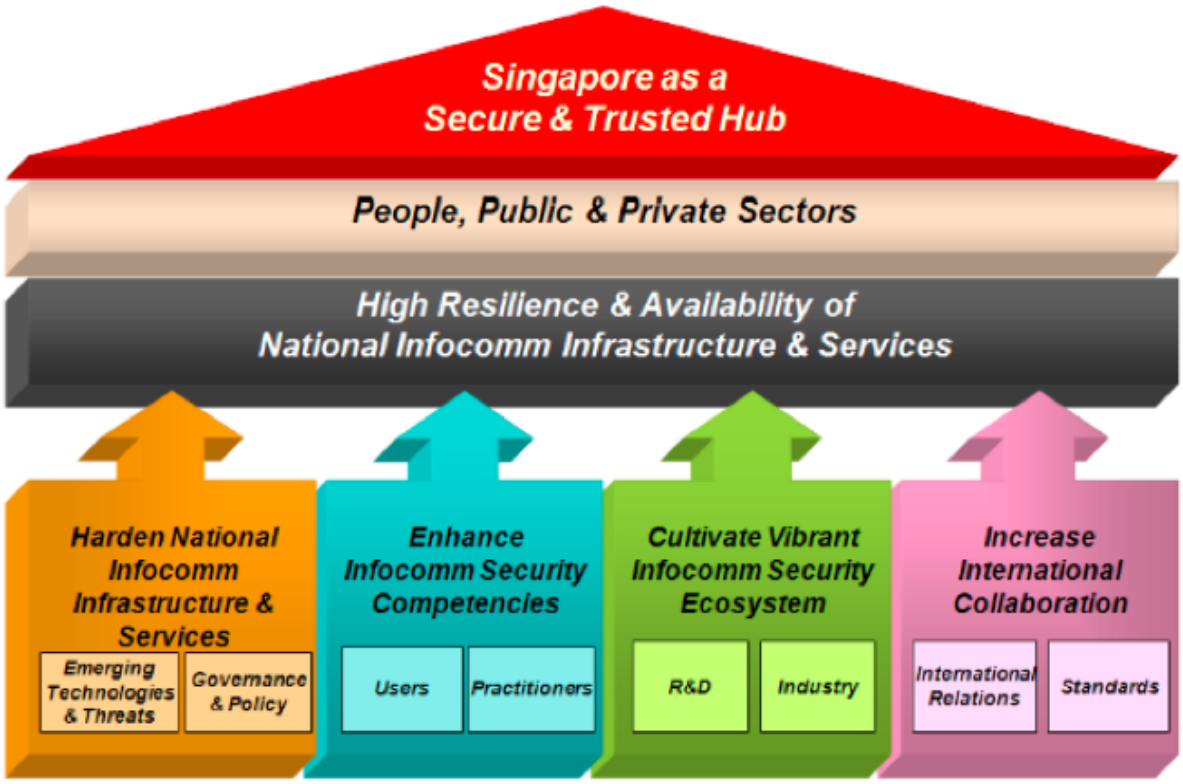
Cyber security providers are offering systematic processes and protection to guarantee that vulnerabilities are managed and threats are blocked at each layer through the application of industry-compliant security products and services; they routinely work on the concept of defence-in-depth.

In 2011, the cyber security market was worth US$63.7 billion. It is expected to grow to about US$120.1 billion by 2017, at a compound annual growth rate (CAGR) of 11.3% from 2012 to 2017. The markets in Western Europe and APAC are estimated to grow at a CAGR of 10.1% and 13.4% respectively, from 2012 to 2017, reaching US$28.1 billion and US$25.9 billion respectively by 2017.[11]

Singapore's Cyber Security Strategy

Under the guidance of the National Infocomm Security Committee, Master Plan 2 (MP2), IDA is bringing the public, private and people sectors to work closer together to secure Singapore's cyberspace. The framework for MP2, shown in the figure below, depicts the vision, coverage, strategic outcome and supporting strategic thrusts. Four strategic thrusts have been identified to support MP2's aim of attaining high resilience and securing the availability of the nation's infocomm infrastructure and services:

[11] MarketsandMarkets: Global Cyber Security Market worth $120.1 Billion by 2017. [Online] Available from: http://www.marketsandmarkets.com/PressReleases/cyber-security.asp [Accessed 9th July 2012].



Strategic Thrust 1: Harden national infocomm infrastructure and services. This strategic thrust aims to enhance the resilience of our underlying foundation to combat cyber threats with Singapore's "hardened" national infocomm infrastructure and services.

Strategic Thrust 2: Enhance infocomm security competencies. This thrust looks at enhancing the security competencies of infocomm users and infocomm security practitioners in managing infocomm security risks.

Strategic Thrust 3: Cultivate a vibrant infocomm security ecosystem. A vibrant infocomm security ecosystem strengthens Singapore's capability to protect our national infocomm infrastructure and services. An active infocomm security research and development (R&D) scene would ensure that a variety of up-to-date infocomm security solutions is available to counter evolving infocomm security threats.

Strategic Thrust 4: Increase international collaboration. As cyber threats are borderless, it is important to continue to work closely with our international counterparts. MP2 also focuses on exchanging best practices in infocomm security and exploring collaboration in this area.

Trends

With the proliferation of the Internet, rise of social networking, consumerisation of IT, exponential growth of mobile devices and the many new services that leverage the omnipresence of the Internet, cyber security is an issue which every user must be aware of.

Several sub-trends within the mega trends mentioned above are highlighted by threat events that occurred in the past few years. These events will be discussed in more detail in the following sections. The incidents helped escalate the issue of cyber security and influenced the underlying technologies required for the protection, detection, remediation and management of cyber security implementations.

6.3.1 Cyber Espionage and Cyber Weapon: Stuxnet and Flame

In June 2010several reports indicated that the Iranian systems that controlled and monitored industrial processes for nuclear facilities were the target of a specially crafted worm called Stuxnet. Later analysis of the worm shown that it might have been developed and dispersed "in the wild" as early as 2009. It is the first malware used to subvert operating systems.

While it infects Windows systems, the cyber worm, unlike most malware, does not slow computers down or damage computer systems. Eventually it became clear that Stuxnet had a very specific target. It was found to be activated only in the presence of a certain configuration of controllers, namely the Siemens supervisory control and data acquisition (SCADA) systems.

Stuxnet infects Siemens Programmable Logic Controllers (PLCs) by subverting the Step-7 software application or the thematic manager that is used to re-program these devices. An in-depth knowledge of the product and environment, as well as a great deal of detailed planning, would have to be factored into the creation of Stuxnet in order for it to achieve the precise damage it creates. This reinforced the notion of a deliberate targeted attack.

The Stuxnet[12] attacks proved that specific cyber activities could be now used to inflict direct damage on the physical world and into critical infrastructures that provide essential services. In addition, it also demonstrated that systems that are not connected to the Internet and that operate under restricted and controlled environments remain vulnerable.

Later, in September 2011, the Laboratory of Cryptography and System Security (CrySyS Lab) of the Budapest University of Technology and Economics in Hungary found the first offspring or variance of Stuxnet and named it Duqu.

Like Stuxnet, Duqu attacks Microsoft Windows systems using zero-day vulnerability. The first-known installer (or dropper) file recovered and disclosed by CrySyS Lab uses a Microsoft Word (.doc) that exploits the Win32k TrueType font parsing engine and allows further execution.

Duqu's purpose is not to be destructive; the known components are trying to gather information, such as keystrokes and system information that could be especially useful in attacking industrial control systems. Based on the modular structure of Duqu, special payloads could be used to attack any type of computer system by any means. This made Duqu a malware toolkit.

---

[12] Microsoft. Win32/Stuxnet. [Online] Available from: http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Win32/Stuxnet [Accessed 9th July 2012

The coverage of the executables have been found in a limited number of organisations, including those involved in the manufacture of industrial control systems, thus indicating the extent of the targets of interest.

Around mid 2012, the Iranian Computer Emergency Response Team (MAHER), Kaspersky Lab and CrySyS Lab claimed to have discovered a new targeted malware in Iran dubbed "Flame."

Flame (also known as Flamer or Skywiper[13]) was found to be created around the same time as Stuxnet.[14] Flame[15]is potentially more potent and complex with as many as 20 times more code than Stuxnet. It is able to trick systems running Windows as their operating system (OS) into accepting malicious code via Windows updates. This means that for almost any system it encountered, Flame could infect it without being detected, even if the computer were a fully patched Windows 7 machine. This indicated that zero-day vulnerabilities[16] are increasingly being used in unlawful exploitation.

These events led to the realisation of a new threat called *Advanced Persistent Threats (APTs)* and *Subversive Multi-Vector Threats (SMTs).* APTs are considered to be:

- Highly customised and intrusion techniques with very specific details and technological requirements;
- Stealthy, patient and persistent for the maximum amount of time so as to extract valuable intelligence;
- Targeted at high-value objectives such as military, political or economic intelligence, organisations of strategic importance, government agencies and their support chain operators shown in Duqu malware.

[13] Laboratory of Cryptography and System Security (CrySyS Lab). sKyWIper (a.k.a. Flame a.k.a. Flamer): A complex malware for targeted attacks. [Online] Available from: http://www.crysys.hu/skywiper/skywiper.pdf [Accessed 9th July 2012].

[14]In fact, Kaspersky researchers believe the Flame platform predates the Stuxnet platform. The Flame code was found in a platform component - "resource 207" - included in earlier versions of Stuxnet collected in 2009. The code was removed from later versions of Stuxnet once the malware was able to achieve the same capabilities using different components. [Online] Available from: http://arstechnica.com/security/2012/06/zero-day-exploit-links-stuxnet-flame/ [Accessed 3rd November 2012].

[15] Kim Zetter. Meet 'Flame,' The Massive Spy Malware Infiltrating Iranian Computers. [Online] Available from: http://www.wired.com/threatlevel/2012/05/flame/all/1 [Accessed 9th July 2012].

[16]According to Symantec, "zero-day vulnerabilities" are associated with "zero-day attacks" or threats that exploit previously unknown vulnerabilities or security holes in a computer application or software. Uses of zero-day attacks can include infiltrating malware, spyware or allowing unwanted access to user information. The term "zero day" refers to the unknown nature of the security hole to those outside of the hackers, more specifically the developers who, once the vulnerability becomes known, usually scramble to protect users. The Stuxnet malware that sabotaged Iranian nuclear facilities relied on five zero days. [Online] Available from: http://www.pctools.com/security-news/zero-day-vulnerability/ [Accessed 3rd November 2012].

Taking APTs several steps further, SMTs refer to highly sophisticated, well-crafted and well-executed attacks designed to use and exploit as many possible threat vectors as necessary to accomplish the mission's milestones.[17]

The main difference between SMTs and other threats is the willingness of SMTs to utilise people, process and technology weaknesses in order to meet their ends. These threats are designed in a dynamic fashion: to place a greater or less amount of effort and emphasis in one area versus another over time, as dictated by the mission's goals and the leadership behind them. SMTs resemble, to a large extent, conventional military operational principles.

With the strengthening of the critical system, attackers are now looking outward across the supply and service chain for potential re-entry into the system.

6.3.2 Hacktivists

In 2007, a national level distributed denial of service (DDOS) attack took the entire Republic of Estonia offline for more than a week, affecting every connected website, from commercial to government.

The attack was sparked off by a single social event - the uprooting of a bronze statue in Tallinn, the capital of Estonia. Thereafter, a series of events, from rioting to protests by local citizens as well as foreign nations, culminating in cyber attacks, led Estonia to cut itself off from the rest of digital world in order to recover itself.[18]

The aftermath highlighted the difficulty of identifying the source of the attacker as botnets were involved ("herded" by their bot master). In addition, "script kiddies" using prepared toolkits, together with hackers, under the cover of the attack, broke into sites and inflicted greater damage by corrupting data and destroying records.

From citizen revolts to the toppling of governments (the "Arab Spring"), the impact of the Internet and social networks on the social fabric emerged as a significant trend in 2011.

Activists are now using cyberspace to promote their political agenda, uphold freedom of speech, declare their commitment to human rights and register their protest. The exploitation of cyberspace and IT systems has given rise to the term, "hacktivists."

Rather than using malware, many of the hacktivists target Web application vulnerabilities which give them direct access to Web servers behind the website itself. Web applications were the third most common attack vector overall in 2011 and were associated with over a

---

[17] Will Gragido. Subversive Multi-Vector Threats. [Online] Available from: http://cassandrasecurity.com/?p=960 [Accessed 9th July 2012].

[18] Joshua Davis. Hackers Take Down the Most Wired Country in Europe. [Online] Available from: http://www.wired.com/print/politics/security/magazine/15-09/ff_estonia [Accessed 9th July 2012].

third of total data loss. According to the 2012 Verizon Data Breach Investigations Report (DBIR) statistics, Web applications were the route used in 56% of large business breaches.[19]

Hacktivists are using cyberspace, in near real time, in every way, to communicate and coordinate their activities. Irrespective of their motivation, hacktivists are a force to contend with.[20]

One such category of hacktivists is "Anonymous," a loosely organised group using underground chats, bulletin boards, social networks and other means of communication to achieve its goals.

When given state support, hacktivists can move into or join forces with cyber armies, causing new threats or cyber event escalation that may result in physical conflict. Depending on the classification and definition, some of these activities might be considered as cyber-terrorism or cyber-espionage.

The following diagram demonstrates the possible workflow of hacktivist activities (we may never understand fully the elements in hactivist groups).

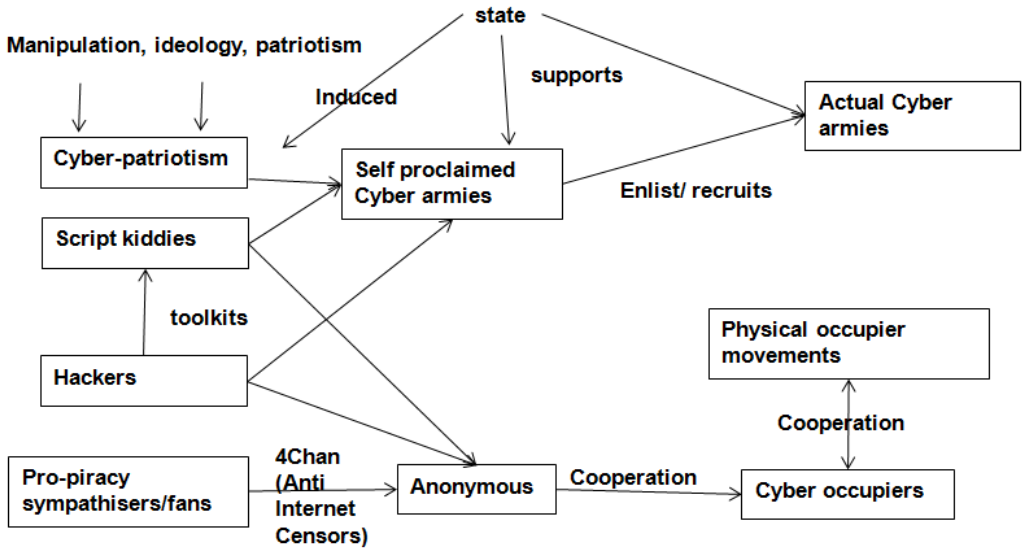


Figure 2: Hacktivist workflow

Source: Mcafee 2012 Threats Predictions

[19] Verizon. 2012 Data Breach Investigations Report. [Online] Available from: http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf [Accessed 9th July 2012].

[20] In 2011, 79% of attacks represented in Verizon DBIR 2012 statistics were opportunistic and many involved hacktivists. [Online] Available from: http://searchsecurity.techtarget.com/news/2240147299/2012-Verizon-DBIR-Hacktivists-make-impact-on-data-breach-statistics [Accessed 3rd November 2012].

6.3.3 Cyber Conflicts

Throughout the history of mankind, conflicts that lead to confrontation and eventual war are events we cannot ignore. New technology, environments ("theatres") and frontiers are constantly being explored and exploited to gain advantages and ensure survival, as well as mobilise defence.

The Economist describes this exploitation as "the fifth domain of warfare" after land, sea, air and space.[21] In the book, Cyber War by Richard A Clarks, "cyberwarfare" is defined as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption."

As in any operational preparation, both offensive and defensive, cyber readiness is essential and cyber weapons are being developed secretly, without discussion of how and when they might be used. Nobody knows their true power so countries can only, and must, prepare for the worst case scenario.

Operations are technically sophisticated, compounded by the speed of the execution and extensive areas involved. An exploitation can be used both offensively and defensively, changing roles quickly. A sector can be deceptively involved in a matter of seconds while work is in progress on another sector.

Adding to the risk is anonymity that mistakes, misattributes and miscalculates, leading to a final military escalation mixing with conventional conflicts.[22]

In 2009, US President Barack Obama declared America's digital infrastructure to be a "strategic national asset." In May 2010, the Pentagon set up its new US Cyber Command (USCYBERCOM)[23] while in Europe, the European Union launched the European Network and Information Security Agency (ENISA) and the United Kingdom, the Government Communications Headquarters (GCHQ), its cyber security and operations centre.

All these events signify the natural interest of states in assuring their self-preservation and testify to their realisation that threats to national survivability are taking on a new scale and dimension.

6.3.4 Cybercrime

---

[21] The Economist. Cyberwar. [Online] Available from: http://www.economist.com/node/16481504?story_id=16481504&source=features_box1 [Accessed 9th July 2012].

[22] Robert K. Knake. Internet Governance in an Age of Cyber Insecurity. [Online] Available from: http://www.cfr.org/terrorism-and-technology/internet-governance-age-cyber-insecurity/p22832 [Accessed 9th July 2012].

[23] U.S. Department of Defense. Cyber Security. [Online] Available from: http://www.defense.gov/home/features/2010/0410_cybersec/ [Accessed 9th July 2012].

Cybercrime is different from traditional crime in that it creates impacts that are closer (in space), wider (in reach) and faster (in time) while recognising no boundaries.

Cybercrime has become the occupation of choice for smart criminals because it offers fairly low risk in the conduct of their operations and potentially higher reward for the work done.

While national legal authorities are bounded by borders, the Internet is not. Criminals exploit this fact by carrying out cybercrime in one country from the safe confines of another, preferably one with weak laws and limited enforcement, investigation or prosecutorial capabilities. Using proxies and anonymising networks such as botnets where the actual sources of the activities are more difficult to locate, cyberspace offers infinitely more impenetrable "hide-outs" for cyber criminals. This is why, in one sense, cyberspace is perceived as the new frontier.

In September 2011, the Norton Cybercrime Report noted that in 2010, cybercrime damage, based on money and time lost, amounted to US$388 billion[24] globally. On 5 September 2012, Norton released the findings of its 2012 Norton Cybercrime Report which calculated the direct costs associated with global consumer cybercrime at US$110 billion over the past one year.[25]

Combating cybercrime, therefore, requires all countries to pass legislation that makes international cybercrime, including activities for extortion and the sabotage of systems, illegal. Countries would require developing mechanisms to stop, investigate, and prosecute attacks originating in one country that target victims in another. Collaboration among states is essential as failure could potentially seem to be supportive to the acts and considered as hostile.

On the ground, online users, including corporate users, need to build security into their IT culture, improve the quality and quantity of published information, and increase channels of communication and collaboration.

Cyber Wellness

There is a need for a more proactive and coordinated cyber defence system in view of the fact that cyber defence today seems to be founded on *ad hoc*, manual processes while cyber attacks seem to be well-organised, with "a systematic escalation path beginning with reconnaissance activities and extending to gaining entry, establishing persistence, setting up external communications pathways, and conducting attack operations."[26]

---

[24] [Online] Available from: http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02 [Accessed 3rd November 2012].

[25] [Online] Available from: http://www.symantec.com/about/news/release/article.jsp?prid=20120905_02 [Accessed 3rd November 2012].

[26] US Department of Homeland Security. Enabling Distributed Security in Cyberspace: Building a healthy and resilient cyber system with automated collective action. [Online] Available from: http://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf [Accessed 9th July 2012].

Besides cybercrime, there is potential for state-sponsored attacks on the national infrastructure or the use of the Internet by terrorists for recruitment and radicalisation.

The concept of wellness in cyberspace is founded on the notion of a "healthy" cyber ecosystem that can provide security, safety and resilience to Internet users worldwide. An ecosystem comprises players that are interdependent, interactive and adaptable. It is recognised that the diverse participants in cyberspace include public and private sectors, individuals, and even processes and cyber devices such as computers, software and communications technologies.

A "healthy" cyber ecosystem works across boundaries (institutional, cultural, national and systemic) and in real time to "anticipate and prevent cyber attacks, limit the spread of attacks, minimize the consequences of attacks, and recover to a trusted state."[27]

The US Department for Homeland Security has identified three building blocks as the foundation for a healthy cyber ecosystem: automation, interoperability, and authentication. The metaphor of the human body's immune system is used to highlight the instinctive and spontaneous auto-responses triggered by attacks to the system, a process cyber defence proponents hope online networks will emulate.

For example, when malicious code or viruses intrude into the computer systems, automated defences could be effectively deployed at the early and even later stages of a cyber attack to prevent fraud, denial of service attacks, identity and data theft, and other threats that attempt to exploit unauthorised access to intellectual property, personal data and sensitive information.

Interoperability can broaden and strengthen collaboration, create new intelligence, accelerate and distribute learning, and improve situational awareness. Three types of interoperability – semantic (that is, shared lexicon based on common understanding), technical, and policy – have been identified as fundamental to integrating disparate cyber participants into a comprehensive cyber defence system.

Identification and authentication technologies that can deliver across five operational objectives - security, affordability, ease of use and administration, scalability, and interoperability – will greatly enhance the resilience of the cyber defence system. There is a need for strong standards-based device authentication, including for software, handheld devices, and small, often wireless, devices composing massively scalable grids.

In Singapore, the Media Development Authority (MDA), together with schools and the local community, are delivering cyber wellness awareness programmes to young children (including preschoolers), taking on issues such cyberbullying and cyber baiting.

Ultimately collaboration and sharing of information, and the coordination of reporting and response systems are key to the creation of a strong and "healthy" cyber ecosystem.

---

[27] US Department of Homeland Security. Enabling Distributed Security in Cyberspace: Building a healthy and resilient cyber system with automated collective action. [Online] Available from: http://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf [Accessed 9th July 2012].

Maintaining cyber wellness is a continuous process that takes into account trends, new technologies, and new exploitation.

6.4.1 Mobile device computing

Mobile devices such as laptops, tablets and smartphones enable users to access information anywhere and anytime through their constantly connected and powerful processing capabilities.

Boosted by powerful processors and graphics processing units, abundant flash-based storage for applications and media files, high-resolution screens and multi-touch capabilities, each smartphone today has more computing power than what the US National Aeronautics and Space Administration (NASA) had of computing capabilities during its moon landing missions.

An estimated 659.8 million[28] units of smartphones will be shipped by end 2012; by 2016, there will be approximately 5 billion mobile device users.

Fundamentally a Linux-based system, the mobile device OS of both the Android and iOS have in-built security components such as in-device encryption and sandboxing or virtualised application running environments. The architecture of both systems can be compared in Figures 3 and 4.

[28] IDC Worldwide Smartphone 2012-2016 forecast and Analysis

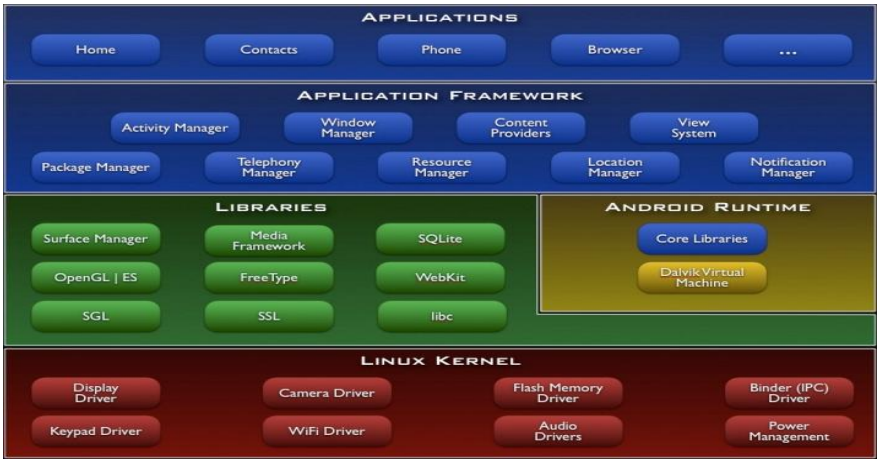


Figure 4: Android Architecture

(**Android. Android Security Overview. [Online] Available from: http://source.android.com/tech/security/index.html [Accessed 9th July 2012].**)

However, the presence of programming vulnerabilities allows users and hackers to "jail break" the phones, circumventing all security barriers and making the phones even more vulnerable to security threats such as malware. Using mobile phones to access Quick Response (QR) codes can also exposes the devices to malware and malicious URLs.[29] A January 2012 report from AVG indicates that malware spread by QR codes is expected to increase in 2012 and likens the practice of scanning QR codes on mobile phones with running an unknown executable on the computer.[30]

The mobility of the devices also makes it easier for users to lose them and with the devices, essential data.

Next, the proliferation of mobile banking and use of digital wallets provides another enticement to bad actors. It is thus no surprise that mobile computing risks top the list among new risks that have been identified.[31]

6.4.2 Consumerisation of IT, Cloud and BYOD

[29] Matthew DeCarlo. AVG: QR code-based malware attacks to rise in 2012 [Online] Available from: http://www.techspot.com/news/47189-avg-qr-code-based-malware-attacks-to-rise-in-2012.html [Accessed 3rd November 2012].

[30] AVG: Community Powered Threat Report – Q4 2011, page 24. [Online] Available from: http://aa-download.avg.com/filedir/press/AVG_Community_Powered_Threat_Report_Q4_2011.pdf [Accessed 3rd November 2012].

[31] Survey shows mobile computing is top security concern: Survey done by FishNet Security also finds cloud computing rising in risk profile. [Online] Available from: http://finance.yahoo.com/news/survey-shows-mobile-computing-top-120000899.html [Accessed 3rd November 2012].

There is a growing tendency for new IT products and services to gain a foothold in the consumer market before “infiltrating” into the enterprise, business and government space. This growing tendency is termed the “consumerisation” of IT, indicating the shift of IT industry innovation and market demands from the consumer space into institutional markets. The use of the Worldwide Web started this shift with the use of free, advertisement-based services such as e-mail and searches; with lighter Web protocols, consumers are able to access services that were once limited to enterprise IT.

With virtualisation and the eventual migration to the cloud, large-scale computing is changing to support these demands with bigger and larger data centres. These data centres are more efficient than general big enterprises because of the massive size of the consumer-driven volume.

In these data centres, scale and efficiencies take on a new level, with simple and low-cost commodity server system resilience creating better use of computation power. The cost-averaging effect of these cloud providers should give a better security infrastructure. With more systems, applications and data creating a large attack surface, the security compromise might be nullified.

Another concern and contention now rests on privacy issues such as loss of data ownership, responsibilities due to failure of services, as well as massive information leakage from a single break-in. Hacking is still possible as program vulnerability is not totally eliminated from these clouds.

At the other end, devices are being built for the consumption of content provided by these services. With personal devices getting more powerful and affordable and access to consumer services becoming easier, enterprise IT continues to lag behind (or even fail) in the provision of devices or services for daily use. Employees trying to enhance their productivity have reached out to external resources or even bring their own devices to work, setting the stage for the Bring Your Own Devices (BYOD) phenomenon.

The BYOD events are forcing enterprise IT to re-think its work and support models as the events bring about new security challenges.

6.4.3 Rise of Malware

Malware are malicious programs that include computer viruses, worms, Trojan horses, spyware, adware, most rootkits and any other program that can be used as a computer contaminant to cause harm. The objective of harm would be to steal sensitive information for the benefit of others, to gain access and to disrupt computer systems.

Early malware creations in the form of viruses and worms are used more as pranks or acts of vandalism. With more computer systems connected to the Internet, malware evolved to try to extract profit out of the ecosystem.

Exploitation of system vulnerabilities and defects, herding zombie computers into botnets, spamming other systems so as to expand the herds, coordinating denial of services for ransom, and using social engineering to trick users into enlisting their systems are some common ways of putting the ecosystem into the control of bad actors.

Malware toolkits and malware-as-a-service are widely on sale in the black market, offering proof-of-concept and service level assurance just like well-furnished commercial services. New business models are changing with malware programmers and other bad actors constantly competing for profits. This competitive landscape promotes innovation and enables new lethal tools to evolve, giving better value for money to their owners.

For example, the banking Trojans, SpyEye and Zeus, have dropped their prices from US$4,000 and US$10,000 to around US$600 and less than US$400 respectively.[32] These lower prices provide fairly low start-up costs and access for interested parties to join the "game."

Malware variants are pushing the limits of anti-virus or anti-malware programs by loading their reference databases and making detection harder while using up much required resources.

The presence of zero-day malware or malicious software that exploits unannounced vulnerabilities on applications, systems and mobile devices will continue to increase. Like a vicious, insidious virus that mutates, the tools of cyber criminals adapt and change constantly, rendering the latest defences useless.

Enterprises need to adapt quickly to respond to malware as well as the tactics of organised crime and foreign adversaries.

6.4.4 Web Development

The ever-increasing presence of Web applications has been one of the key factors driving the popular usage of the Internet. It has also triggered the consumerisation of IT and several other trends such as mobile connectivity and the use of smartphones.

Among all Web programming languages, HTML5 is the new "it" protocol on the Internet.[33] It is an alternative to Adobe Flash in the display of content through a Web browser. The emergence of HTML5 standards enables programming inside a browser and this is what makes HTML5 attractive to developers. The development processes also place the end user at the centre, allowing for the creation of more relevant and user-centric applications and services.

HTML5 includes features that allow the control and storage of offline data within the browser using client-side JavaScript, consequently facilitating the creation of offline mobile Web applications across platforms. Without HTML5, the development process would require installed applications, for example, an application that can download articles for later reading or a data capture application that can work offline and upload when the user is online.

---

[32] EMC^2. RSA 2012 Cybercrime Trends Report. [Online] Available from: http://www.rsa.com/products/consumer/whitepapers/11634_CYBRC12_WP_0112.pdf [Accessed 9th July 2012].

[33] Network Computing. Rise of HTML5 Brings with It Security Risks. [Online] Available from: http://www.networkcomputing.com/next-gen-network-tech-center/232500303?pgno=1 [Accessed 9th July 2012].

The standardisation of HTML5 will make the browser programming trend even more pronounced. While the standard is not yet finalised, support for these offline features is available and ready for use. As the Web evolves, so too do the ways it is used. The support of dedicated user interfaces for mobile devices is growing quickly.

The security concern over implementation is that each browser's implementation of HTML5 varies so it would be hard to generalise about its security enhancements and limitations. HTML5 contains new security features but present many new issues.

Bad actors who spread malware or steal user information on the Web will continue to seek new ways to exploit HTML5.

6.4.5 Embedded Device Exploitation

Embedded systems are computer systems designed to perform a specific task. These systems generally consist of basic processing cores that are typically either micro-controllers or digital signal processors (DSP) with memory spaces as well as IO and communication interfaces.
By contrast, a general-purpose computer, such as a personal computer (PC), is designed to be flexible and to meet a wide range of end user needs.

Large computer systems such as PCs consist of several other smaller embedded systems designed for specific control functions. At times, these systems, often including hardware and mechanical parts, are embedded as part of the complete device.

Since the embedded system is dedicated to specific tasks, it can be optimised to reduce the size and cost of the product while increasing reliability and performance. Certain embedded systems are mass-produced, benefiting from economies of scale.

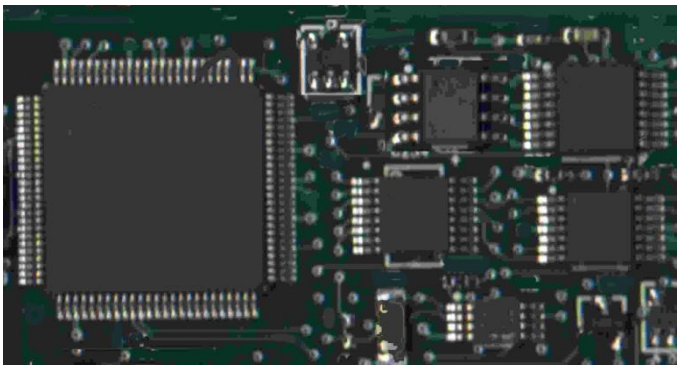


Figure 5: Embedded System Board (Source: IDA)

As the building block of other devices, embedded systems control many devices ranging from printers, routers, digital watches and MP3 players, to large stationary installations such as traffic lights, factory controllers and systems controlling nuclear power plants. They also include medical equipment, mobile phones, avionics and automatic safety systems spanning all aspects of modern life.

These systems are so common and insignificant that they are simply overlooked most of the time. Many such systems run relatively in isolation and are thus protected from a wide range of security threats. However, many other embedded systems are directly or indirectly

connected to the cyber world. These devices are not designed to enable secure connections or include any of the security components as these add up to the costs of production.

Other devices built with security considerations are still exploitable as design failures are the starting point for exploitation, leading mainly to software level attacks.

With the increasing use of sensory devices in smart cities and smart grids, and the extensive use of anti-malware applications, malware writers are seeking new ground for their exploitations. They are exploring different concepts such as having code that alter the OS boot order and using embedded hypervisors.

Sophisticated attackers know that controlling hardware, in addition to operational and application levels, is a new key to their success since it will provide greater control and maintain longer access to the system and its data.[34]

Opportunities

The use of the Internet and IT has created many new trends such as the Internet of Things, BYOD, Big Data and greater mobility.

As security cuts across all levels and layers, there is a need to provide confidentiality, integrity and availability as well as protection in these areas.

6.5.1 International Cooperation

Globally, there is room for more work in cross-border mutual cooperation and assistance because malicious activities on the Internet do not recognise borders. National cyber security events or crises would generate both technological and political responses.

The European Union's Convention on Cybercrime, also known as the Budapest Convention, is the first and only binding international treaty designed specifically to address cybercrime by harmonising national laws, improving investigative techniques and increasing cooperation among nations. As of 28 October 2010, 30 states had signed, ratified and acceded to the Convention while a further 16 states had signed the convention but not ratified it.[35]

Though the Budapest Convention has helped to develop an international standard for criminalising cybercrime, it has not led to an appreciable reduction in cybercrime. The mechanisms for international cooperation developed by the Convention are bilateral and prosecutorial, providing no conduits to coordinate law enforcement activity across borders or for network security professionals to coordinate technical solutions when attacks occur.

---

[34] Bruce Schneier. Schneier on Security. [Online] Available from: http://www.schneier.com/blog/archives/2012/05/backdoor_found.html [Accessed 9th July 2012].

[35] Council of Europe. Convention on Cybercrime. [Online] Available from: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=28/10/2010&CL=ENG [Accessed 9th July 2012].

Gaps and issues still exist in the treaty and adding signatories to this particular document is neither necessary nor sufficient to reduce cross-border cyber criminal activity. Many proposals to add to a more comprehensive and globally acceptable cybercrime treaty have been submitted but none has been accepted to date.

Nonetheless, other international efforts to encourage collaboration and dialogue continue.[36]

6.5.2 National Awareness

With undesirable events happening in cyberspace and political leaders feeling the impact of cyber security events in their different manifestations, national interests and safety can be compromised. The focus would have to shift to the more pragmatic field of response and command and control; this would include enhancing the development of secure computer systems, networks and applications. Within these parameters, research and development (R&D) linking industry, research centres and academic institutions can be better leveraged to avoid duplication of effort and optimise efficiency.

Changes would have to be directed toward the encouragement of security innovation and applications in the face of increasing demand for security technologies. As awareness and demand coalesce, technologies would be the main "push" factor while processes are being worked out and human capital enhanced.

6.5.3 Technology innovation

Many of the modern issues surrounding cyber security are not something new, even if the technologies are newly emerging. Some, such as the basic TCP/IP protocol, are legacy issues. Other issues are caused by poor programming techniques and languages.

Experience with IT security indicates that security has not been able to attain best of breed standard as many are simply patch works reacting to inherent weaknesses in the architecture and programming circumstances.

Challenges

While we seek out technology and innovation to resolve our problems, we must realise that many of these issues require policy, education, awareness, institutional support and even behavioural changes, as in the case of cyber bullies.

"Cyberbullying involves the use of information and communication technologies to support deliberate, repeated, and hostile behaviour by an individual or group, that is intended to harm others." (Bill Belsey)[37]

Another definition of cyberbullying would be when a child or group of children (under the age of 18) intentionally intimidates, offends, threatens or embarrasses another child or

---

[36] Georgetown University. International Engagement in Cyberspace 2012. [Online] Available from: http://lsgs.georgetown.edu/events/internationalengagement2012/ [Accesed 9th July 2012].

[37] Cyberbullying.org. Cyberbullying. [Online] Available from: http://www.cyberbullying.org/ [Accessed 9th July 2012].

group of children specifically through the use of IT, such as a website or chat room on the Internet, a cellular telephone or another mobile device.[38]

Not only has this behaviour within the physical world been modelled into the cyber world, other socially related behavioural patterns have found their way into cyberspace, aided by technology.

When cyber incidents occur, all too often states will claim no responsibility and offer "patriotic" hackers who cannot be identified or controlled as the likely culprits. These countries will likely refuse investigators access to potential suspects or to systems involved in the incidents on the grounds that doing so would violate national sovereignty.

Technologies alone cannot address these national sovereignty issues even if there are capabilities to accurately pinpoint the source of the attack.

With more devices connected and an increase in interactions between human-to-machine and machine-to-machine, cyber traffic increases, creating the Big Data and Internet of Things trends that are both useful and challenging

In addition, the dimensions of cyber incidents are so encompassing that they span both the physical and cyber worlds, and across different silos and departments within enterprises, businesses and governments. This, however, does not account for deceptive activities during an attack operation.

Increase in high speed broadband and wireless network penetration are transforming threats that were trivial in the past into more lethal attacks, e.g., Denial of Service (DOS) incidents. The wide scope and form of cyber attacks creates enormous challenges for both protectors and investigators. No single entity would be able to face these security challenges alone.

Technology Outlook

The initial focus of the Internet is on interoperability within a closed network environment. Access is tightly controlled with trusted users but that focus is now shifting to security as the Internet was not built and designed for the way it is used today.

At the same time, systems connecting to the Internet continue to have programming vulnerabilities as there are no clear restrictions and requirements over the outcome of those vulnerabilities.

Every system or device, regardless of technology or process, has a vulnerability that can be potentially exploited. Within these systems are resources and data that some cyber criminals may want.

The 2003 US National Strategy to Secure Cyberspace[39] identified vulnerabilities within three essential Internet protocols:

---

[38] Ipsos. One in Ten (12%) Parents Online, Around the World Say Their Child Has Been Cyberbullied, 24% Say They Know of a Child Who Has Experienced Same in Their Community. [Online] Available from: http://www.ipsos-na.com/news-polls/pressrelease.aspx?id=5462#.Tw6exyC2__s.twitter [Accessed 9th July 2012].

1. the Internet Protocol which guides data movement from source to destination across the Internet;
2. the Domain Name System which translates IP numbers into recognisable Web
addresses and
3. The Border Gateway Protocol which provides the connection between networks to create bonding between them. This protocol is the source of the greatest risk among the three domains.

For example, IPv6, while having improvements over the older IPv4 in term of security, does not totally address the issues related to dual stacking, header manipulation, man-in-the middle, Address Resolution Protocol (ARP) table overflow[40]and mobility.[41]

Traditional IT security technologies such as risk assessment and assurance, detection and protection will continue to evolve to manage new security vulnerabilities and keep pace with trends and challenges.

Special focus will be on the Web-based ecosystem and context-aware computing. Examples would be adaptive strong multi-factor authentication and an authorisation provisioning system to provide both better usability and protection.

A new category of security technology coined by Gartner, Operational Technology (OT) security, is emerging to harmonise a wide spectrum of products, solutions and services to ensure operational protection and continuity. This security technology is essentially found on systems such as SCADA and systems that operate critical information infrastructures.

Big Data for data analysis, together with multi intelligence feeds for correlation, could be used in the detection of simple malware and APTs. Cloud and virtualisation security that use strong encryption, provisioning and control would better facilitate collaboration.

Innovation in mobile device security for use in enterprises will have to be stepped up as awareness of the issues takes centrestage.

Security is gradually being embedded in design, down at the chip level, and is no longer something that is an afterthought.

---

[39] The White House, Washington. The National Strategy to Secure Cyberspace. [Online] Available from: http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf [Accessed 9th July 2012].

[40] National Institute of Standards and Technology, U.S. Department of Commerce. Guidelines for the Secure Deployment of IPv6. [Online] Available from: http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf [Accessed 9th July 2012].

[41] Samuel Sotillo. IPv6 Security Issues. [Online] Available from: http://www.infosecwriters.com/text_resources/pdf/IPv6_SSotillo.pdf [Accessed 9th July 2012].

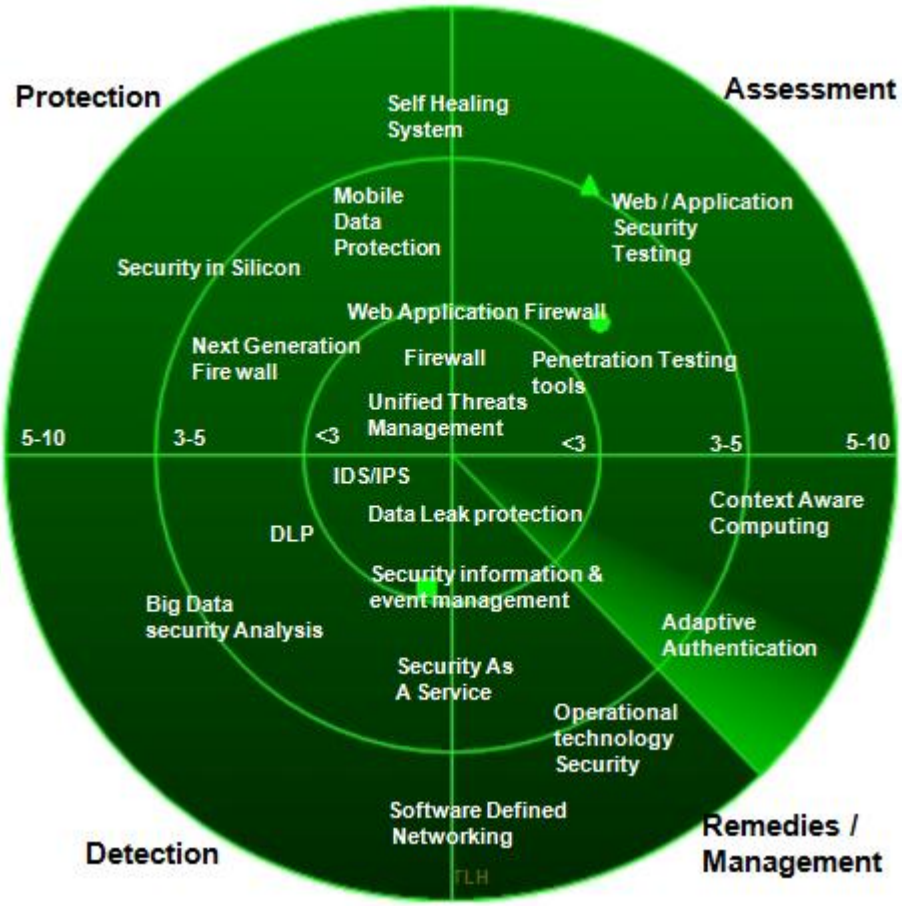


Figure 6: Technology Radar

6.7.1 Less than three years

Unified threat management (UTM)

A unified threat management (UTM) system is an all-inclusive security product that is able to perform multiple security functions within one single appliance with network firewalling, network intrusion prevention and gateway anti-virus (AV), gateway anti-spam, VPN, content filtering, load balancing, data leak prevention and on-appliance reporting.

One key motivation of having a single device to cover all security functions is that it simplifies administrative functions and gives a much smaller footprint compared to handling and having multiple products. In addition, UTM systems are generally better integrated with the functions offered.

However, running multiple functions require critical resources such as a Central Processing Unit (CPU) and memory, especially if deep packet inspection is involved, and this makes performance the Achilles heel of UTM.

Large enterprises tend to deploy separate devices that are dedicated to certain security functions or at times, combinations of not more than three functions. That would make UTM more suitable for smaller branches, remote offices or event smaller organisations.

UTM remains an important consideration since hardware performance is constantly improving while UTM vendors are getting better at integrating and tuning the functions.

Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)

The Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) are two mature technologies that kick in after the firewall. Instead of access control, IDS/IPS inspects the packet for signs of abnormality using sets of pre-defined rules, sometimes known as signatures or filters.

IDS/IPS has two advantages in that it can be network-based or host-based. Network-based IDS/IPS works together with the firewall in any architecture setup and can be used either as software or as an appliance. Host-based IDS/IPS comprises agents that run in systems, intercepting traffic moving through the TCP/IP stack.

The difference between IDS and IPS is that IPS is in line with the traffic flow and is able to block access when an abnormality, e.g., DOS, is detected while IDS would only alert the administrator or other management system to take further action.

The challenges for IDS/IPS lie in the bandwidth of the traffic and the analysis of that traffic. The inspection of the traffic would also post issues to the network-based IDS/IPS because of more encrypted data flow. Host-based IDS/IPS would be able to intercept the data within the host once it is decrypted.

Like the firewall, IDS/IPS would remain an integrated part of network security solutions if not subsumed as part of the firewall product. IDS/IPS could also be used to create data for correlation under security information and event management (SIEM) as well as to overcome SIEM's tendency for false positives.

Security Information and Event Management (SIEM)

Security information and event management (SIEM) technology provides two main capabilities, namely security information management (SIM) and security event management (SEM).

SIM provides log management where the log data is collected, analysed and used to generate reports. SIM is used mainly to support regulatory compliance reporting, internal threat management and resource access monitoring.

SEM processes event data from security and network devices, and systems and applications in near real time for security monitoring, event correlation and incident response.

Using correlation rules and wide data sources, SIEM can be used to discover activity associated with a targeted attack or security breach, and to satisfy regulatory requirements, mainly in the USA. In Asia Pacific, SIEM deployments are primarily used for threat monitoring.

The rise in targeted attacks is driving many organisations to adopt SIEM to improve external and internal threat-monitoring capabilities. In these situations, information from user activity and resource access monitoring for host systems, and real-time event management for network security, is fed into the system.

Used as a platform or as part of a service, SIEM provides additional assessment, direct monitoring, end-point control, or management dashboard and risk assessment functions. These use cases are the result of adoption of SIEM technology by a broad set of companies.

Just as enterprises are singularly distinct and different, each SIEM technology is singular and unique, corresponding to event type, usage patterns, network and system configuration as well as business needs.

Users of SIEM must learn to temper their expectations. SIEM – in spite of configuration, tuning and maintenance - cannot resolve every security issue.

Nonetheless, a well set-up and configured SIEM can work remarkably well in supporting the external and internal threat-monitoring activities of IT security systems, improving incident management capabilities, and fulfilling the reporting needs of internal audit and compliance organisations.

Penetration (P-) Testing tools

Vulnerability assessment is a proactive process whereby a system or network is checked for potential vulnerability while penetration testing (P-testing) extends vulnerability assessment by assuming an attacker-oriented approach. Vulnerability assessment is typically broad and shallow while P-testing is deep and narrow.

P-testing will move from finding a vulnerability to taking exploitable actions so as to determine whether deeper access can be accomplished. The outcome of the test and assessment is to establish weak points at the time of testing so that they can be strengthened or hardened. Hence the exploitation can be achieved by a possible hacker.

P-testing tools, be they open source or paid products, enable enterprises to perform the tests themselves. The same set of tools is used by external consultancies engaged by enterprises to do vulnerabilities assessment and P-testing.

P-testing products have gotten easier to use; badly “excited” testing can have a nasty impact on operational systems and give a lot of false positives.

Preparation, as well as engaging external services for enterprises that do not have the technical skills but need to regularly perform P-testing, is critical for any successful testing exercise.

The technology for P-testing and vulnerabilities assessment tools will continue to improve in tandem with known security issues and open exploitation incidents . These tools will need to be updated at least quarterly for assessment, given the rapid changing cyber security landscape.

Mobile data protection (MDP)

Mobile data protection requires:

- encryption and authentication to protect the stored data on mobile devices;

- evidence that the protection is working.

Mobile devices are moveable devices such as notebooks, smartphones, tablets and removable media. The main protection is for moveable storage found on these mobile devices. Similar technology can be applied to the moveable storage of desktops and servers.

Enterprise IT would have some processes and support for mobile devices such as laptops, PCs or mobile workstations while workstations' mobile protection requirements are mostly served by end protection products which have several security functions such as enterprise anti-virus, personal firewall and host IPS on top of storage encryption.

Encryption with 256 or 128-bit Advanced Encryption Standard (AES) with Federal Information Processing Standards (FIPS) 140-2 validated cryptographic library, and Common Criteria Evaluation Assurance Level (EAL) 4+ certification are the common security requirements. This type of encryption is one of the overlapping security features provided by OS vendors such as Bitlocker from Microsoft.

Mobile device protection technology is an exciting new development poised for growth in the next five years as convergence takes place. Endpoint protection product vendors will be pushing toward more device coverage of smartphones and tablets as well as the security functions on these devices. In the process of the convergence, mergers and acquisitions (M&As) between these vendors and those providing the Mobile Device Management (MDM) suites would be expected.

Mobile OS providers will improve their security feature offering as users' awareness of the threats within the changing cyber landscape increases and they demand more protection using their consumer power.

Mobile manufacturers will include some security enhancements such as the Trusted Platform Module (TPM) into their hardware. This would provide a Trusted Execution Environment and Mobile Trusted Platform.

Smartphones and tablets

MDP has a significant role to play is in smartphones and tablets where there are opportunities for both basic and new requirements. Today, OS providers are starting to incorporate security features into these devices. One such development is the implementation of Address Space Layout Randomisation (ASLR)[42] in the Android's latest Jelly Bean.[43]

ASLR is a technique designed to make malware-based attacks more difficult. It shuffles the pack and position of libraries, heaps and stacks in a process's address space. This means that even if hackers find any vulnerability in a device, they will have a far greater problem locating

[42] Jon Oberheide. Exploit Mitigations in Android Jelly Bean 4.1. [Online] Available from: https://blog.duosecurity.com/2012/07/exploit-mitigations-in-android-jelly-bean-4-1/ [Accessed 9th July 2012].

[43] Dan Goodin. Serial hacker says latest Android will be "pretty hard" to exploit. [Online] Available from: http://arstechnica.com/security/2012/07/android-jelly-bean-hard-to-exploit/ [Accessed 9th July 2012].

the infected shell code in a stack, making it much harder for them to craft a working exploit. ASLR is often combined with other memory protection techniques, such as non-executable memory protection.

ASLR has been a mainstay of security defence in desktop machines for years, appearing in Windows Vista and Mac OS X since 2007. It was featured in iOS 4.3, released in March 2011, marking its migration into smartphones and, more recently, in Android 4.0.

Mobile Device Management (MDM)

Used mainly in enterprise level protection, MDM comprises a suite of software to secure, monitor, manage and support mobile devices, mainly smartphones and tablets.

Part of the MDM capabilities is to control these mobile devices remotely Over-The-Air (OTA) so that they can be updated and managed without any need for physical connections.

With this capability, devices can be locked or data remotely removed when devices are lost or stolen. Software updates can be pushed to mobile device users so they can keep the devices well updated with the latest MDM patches. Self-service Web portals, support of in-house developed mobile software and enterprise mobile app stores are other capabilities that can enhance the MDM environment.

6.7.2 Three to five years

Firewalls

A firewall, whether it is software or hardware-based, analyses data packets and is used mainly as a control over incoming and outgoing network traffic. It would then determine whether access should be granted, based on a predetermined rule set.

Generally, there are two main locations where a firewall is used – in the network and the system.

The network firewall connects between a trusted and secure network to other networks that it deems as neither secure nor trusted. A system firewall is a software-based firewall running in its hosts as a protected domain in relation to the network that the system is connected to.

Firewalls have been evolving since the late 1980s, from basic packet filters to stateful and application layer firewalls. Even with the changing trends, firewalls will remain in the mainstream and as a required component in the security control system. Several variants of firewalls are branching off; these include the Web Application firewall and XML firewall.

As a network firewall, the stateful firewall uses the history and characteristics of a connection, in addition to traditional firewall methods, to control traffic. Instead of using only the IP address source, the destination and ports, using “state” imparts better security knowledge about how the connection is being used. This has made stateful firewall the most common type of firewall and a well-established technology. Almost every enterprise uses state-based network firewalls at the Internet and/or in the data centre and branch offices.

Stateful firewalls will eventually evolve into, and be subsumed by, next-generation firewalls (NGFWs) which offer software and appliance-based services.

Since perimeter and segregation of domains continue to be a constant requirement, such access control safeguards will remain intact.

Firewall technology will adapt continually to respond to new threats but the basic concept will remain unchanged.

When deploying a firewall, users should take note that newer variants of firewalls exist. Care should to be taken not to label traditional, stateful firewalls as NGFWs or any other type of firewall without substantive improvements.

Web application firewalls

A Web application firewall (WAF) is intended to protect applications accessed via HTTP and HTTPS against possible attacks. WAFs primarily focus on Web server protection at Layer 7, the application layer. However, they may include safeguards against attacks at other layers.

WAFs do not typically protect against unpatched vulnerabilities, the domain of networks and host-based intrusion prevention systems (IPS). Instead, they focus on vulnerabilities in configuration or in custom-developed code that makes Web applications subject to attacks, such as cross-site scripting, directory traversal and forced URL browsing.

A WAF operates like a shield and does not fix the underlying vulnerability, even as it is reportedly being used as a guide to what requires remediation. As a shield, WAFs are most often expected to be deployed in front of Web servers.

WAF capabilities are required for most leading application delivery controllers (ADCs) to improve behavioural detection engines and larger e-commerce websites.

A pure WAF product market will remain small because of the varying growth of ADCs and the competing market for application scanners. However, the Payment Card Industry Data Security Standard (PCI DSS) standard continues to drive WAF use. Companies where a scanner is already in use, or cannot or will not be used, will also need WAFs.

As individual products mature, market choices would likely contract as a result of consolidation via M&As. However, the WAF market will continue to grow because of the need to respond to new risks introduced (at times) by the Web applications themselves.

Even when the best way to secure Web applications is to ensure that they have checked negative for vulnerabilities before running in production, WAFs are still valuable as an added protection since they address gaps or failure in the checks as well as possible new vulnerabilities.

XML firewalls

XML firewalls are sometimes called "Web services security gateways" or “Web service proxies.” They provide security functionality and an enforcement point mainly for Web services traffic, often based on Representational State Transfer (REST), Simple Object Access

Protocol (SOAP) and Extensible Markup Language(XML). XML firewalls are developed in concert with service-oriented architecture (SOA).

Usually deployed in demilitarised zones (DMZ), these XML firewalls generally perform at Layer 7, providing XML threat protection, Web Services Description Language/XML/SOAP schema validation, data transformation and payload schema validation.

However, XML firewalls can also be used internally where security concerns are high. In many cases, security-related functions are packaged with other SOA support functions. XML firewall technology providers are increasingly providing functionality for the creation, importation, administration, versioning and enforcement of policies.

The difference between XML firewalls and WAFs is that the XML/SOAP firewall enables Layer 7 filtering on any content, metadata or network variable in a message while WAFs offer security threat mediation and content processing for other URL-encoded, HTTP-based applications, HTTP protocol and method filtering, and session handling policies.

XML firewalls offer significant security value for Web services deployments, especially for processing transactions that have high financial value, intellectual property considerations or privacy restrictions pertaining to both security and traffic management.

These firewalls may be used in line with WAFs, or as a converged product in the near future.

Next Generation Firewalls (NGFWs)

Next-generation firewalls (NGFWs),[44] also known as application-aware firewalls, usually have the traditional ports and protocol analysis capabilities of a traditional, stateful firewall and can also evaluate traffic, based on the applications that generate the packets crossing the wire, using some level of deep packet inspection. This capability has become critical in recent years with the explosion of Web-based applications that most stateful firewalls can only identify as HTTP traffic headed for Port 80.

Gartner's position for the past few years has been that NGFWs are the future of the firewall industry.

NGFWs should not be confused with a standalone network IPS, a commodity or non-enterprise firewall, or a firewall and IPS that are not closely integrated in the same appliance.

Leading firewall products and first-generation IPS products are converging toward NGFWs as they begin to integrate IPSs and firewalls with limited capability. The NGFW market will likely overtake the standalone IPS appliance market at the enterprise level as firewall vendors remain slow to innovate and increasingly face competition from niche players.

NGFWs often include advanced inspection such as application control and reputation-based feeds, and better controls such as Active Directory integration. Some NGFWs include firewall,

---

[44] Shamus McGillicuddy. Magic Quadrant: Next-generation firewalls are mainstream. [Online] Available from: http://searchnetworking.techtarget.com/news/2240113743/Magic-Quadrant-Next-generation-firewalls-are-mainstream [Accessed 9th July 2012].

IPS and possibly URL filtering as product offerings. These have given rise to another branch of products called unified threat management (UTM).

Data Leak Prevention (DLP)

It is a serious concern when sensitive data is disclosed maliciously or unintentionally to unauthorised personnel, both inside and outside of an organisation. Depending on the organisation, that data can range from credit card data, patient information and intellectual property to corporate correspondence by top executives.

Data breaches would require that the incident be handled quickly and in a timely fashion, ensuring the prevention of further data loss during use, in motion or transit, and at rest. To address this requirement, it is necessary for organisations to have the Data Leak Protection or Data Loss Protection (DLP) defence layer.

During use, endpoint agents can be used to monitor a specific order of data according to the required usage policy. Files can be embedded with watermark or rights, subject to usage policy.

With data in motion, network-based detection can be effected through the use of IDS/IPS or specific DLP devices to tackle potential violation of security policies.

When dealing with data at rest, encryption is used and additional data extrication monitoring is executed by the DLP agent. Encryption is not a foolproof solution as over time, better algorithms can be found to break the encryption method, using vulnerabilities in the method or better factorial algorithms.

DLP agents can only address the majority of data leakages. Any more advanced forms of data exfiltration would either circumvent the agents or simple bypass the whole prevention process.

The challenge of DLP deployment lies in the definition of rules and fine-tuning as there is a tendency toward the yield of false positives and negatives. DLP is an important layer of defence in the overall security setup.

The key application of DLP technology is in areas where data leaks need to be critically addressed.

Trusted Platform Module (TPM)

Since 2006, many laptop computers have been sold with a Trusted Platform Module (TPM) chip built into the motherboard. The following figure presents TPM as part of the overall architecture of a PC.

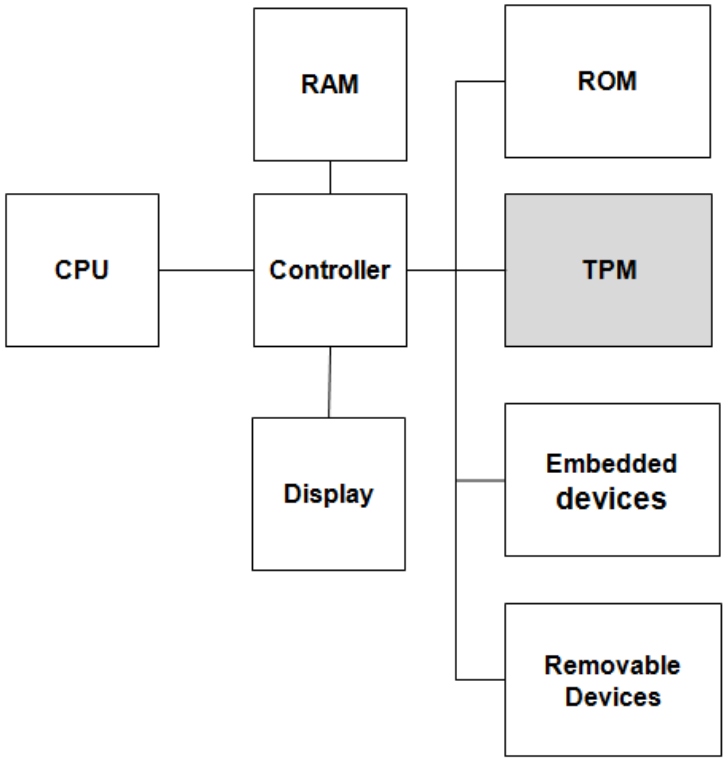


Figure 7: PC Platform Containing a Trusted Platform Module (TPM)

The Trusted Platform Module (TPM) is the general name of a specification, often called the "TPM chip" or "TPM Security Device" by the Trusted Computing Group (TCG), as well as the published specification that details a secure crypto-processor that can store cryptographic keys for the protection of information.

On 18 May 2009, TCG managed to achieve standardisation for their TPM specifications:

- ISO/IEC 11889-1:2009 Information technology—Trusted Platform Module—Part 1: Overview
- ISO/IEC 11889-2:2009 Information technology—Trusted Platform Module—Part 2: Design principles;
- ISO/IEC 11889-3:2009 Information technology—Trusted Platform Module—Part 3: Structures;
- ISO/IEC 11889-4:2009 Information technology—Trusted Platform Module—Part 4: Commands.

As published on 3 March 2011, the current version of TPM specifications is 1.2 Revision 116. The next figure shows the internal components of the TPM.[45] The IO interface with the external world with the cryptographic co-processor implements cryptographic operations such as Asymmetric key generation (RSA), Asymmetric encryption/decryption (RSA), Hashing (SHA-1) and Random Number Generation (RNG).

[45] Trusted Computing Group, Inc. TPM Main: Part 1 Design Principles. [Online] Available from: http://www.trustedcomputinggroup.org/files/static_page_files/72C26AB5-1A4B-B294-D002BC0B8C062FF6/TPM%20Main-Part%201%20Design%20Principles_v1.2_rev116_01032011.pdf [Accessed 9th July 2012].

The TPM uses these operations to generate random data and asymmetric keys, for signing and maintaining the confidentiality of stored data. The TPM can also implement other asymmetric algorithms such as Digital Signature Algorithm (DSA) or elliptic curve.

The Hash-based Message Authentication Code (HMAC) engine provides two pieces of information to the TPM: proof of knowledge of the Authentication Data (AuthData) and proof that the request arriving is authorised and has had no modifications made to the command in transit. The SHA-1 engine is primarily used by the TPM as it is a trusted implementation of a hash algorithm.

The power detection component manages the TPM power states in conjunction with platform power states. TCG requires that the TPM be notified of all power state changes. The Opt-In component provides mechanisms and protection to allow the TPM to be turned on/off, enabled/disabled, and activated/de-activated. The Opt-In component also maintains the state of persistent and volatile flags, and enforces the semantics associated with these flags.

The TPM provides an option via hardware-based protection for encryption and authentication keys, machine identity and integrity. Protection, e.g., pre-boot and OS integrity testing through the use of certificate keys and hash verification, can be done at a much lower level.

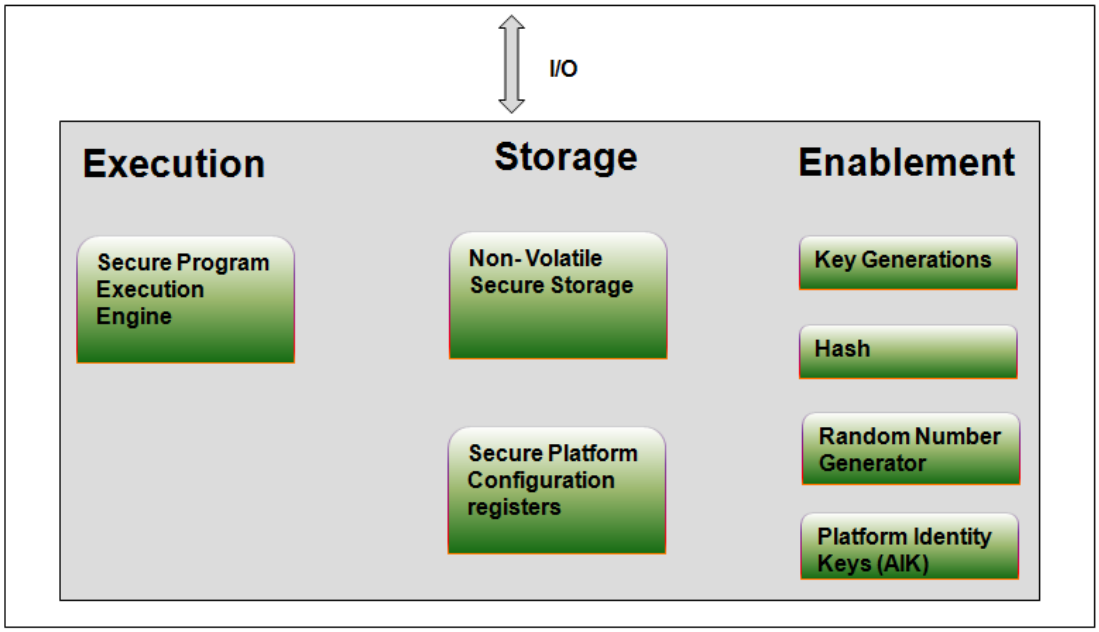


Figure 8: Trusted Platform Module (TPM) Components

The TPM would be expected to be integrated into other parts of the computer system such as the Ethernet chip, as well as into mobile devices. It is only to be expected that the TPM would be included as a *de facto* component in motherboards in time to come.

Security-As-a-Service

Security-as-a-service is an outsourcing model for security management and typically involves applications such as anti-virus software delivered over the Internet, and Web and e-mail

security offerings through the cloud. It also can refer to security management provided in-house by an external organisation.
Gartner predicted that cloud-based security controls for messaging applications (such as anti-malware and anti-spam programs) would generate 60% of the revenue in that industry sector by 2013, up from 20% in 2008.[46]

The use of such services might require that network traffic be redirected to the provider networks for sanitation.

Organisations with limited in-house security resources which use security-as-a-service might find that the cost of the service may not necessarily be lower than in-house support. The main advantage with this model is that it frees up resources to deal with other issues.

Another consideration is that providers can have a better appreciation of the security situation, relative to the awareness of individual customers, due to its customer coverage.

Adaptive Authentication

Adaptive authentication is a risk-based authentication and identification platform that tries to balance security, usability and functionality.

It is designed to customise the required authentication levels, depending on the authenticating of the user's risk score, with the ability to calculate the risk of an access request, an event or a transaction, and determine proper outcomes to prevent fraud and misuse.

Part of the risk evaluation is devoted to verifying a user's identity and determining if the activity is suspicious. Once the suspicious activity is determined by the calculation of the user risk score, different authentication methods can be used. This could range from direct user/password to further challenges such as One-Time-Password (OTP) or two-factor authentication.

Additional post-authentication processes can be set up as well to quicken the next authentication process. This can be done using security tokens placed with the users, in the same way an ultraviolet sensitive stamp can be verified for multiple entries.

With adaptive authentication, the authentication levels of different risk requirements can be managed with better user experience. However, more consideration would be needed to improve the setup process and access authentication method.

Adaptive authentication is a step closer toward the provision of context-aware security.

Context-aware Security

As we work with IT systems, we expect them to provide the required challenge and determine the right responses so as to grant the resource for use.

---

[46] Margaret Rose. Security as a Service (SaaS). [Online] Available from: http://searchsecurity.techtarget.com/definition/Security-as-a-Service [Accessed 9th July 2012].

The issue over this arrangement is that the policy that determines the required challenge applied to the resource is fixed without, or with limited, consideration of other factors such as location, time, roles and work patterns.
With connectivity and constant interaction with IT systems, it is expected that the interaction is more flexible or friendly while still maintaining a high level of security.

The IT system must have some kind of realisation of the state of the user when trying to access the resources and the security profile of the resources in relation to that state, as well as the interaction between the two objects, namely the user and the resource. The realisation of these states is equivalent to the IT system's awareness of the context states, profiles and conditions.

The state of the user can considered as the local and global contexts of who, what, where, when, and how. The security profile of the resource can be considered by its classification of low or high priority, very high risk and so on.

The interaction between the two objects can be smooth or interrupted. An example of a local interaction would be when users try to access different files of different security profiles at the same time and starting or failing to access files of high security profiles. An example of a global interaction would be when several users fail in attempting to access multiple objects with the same or different high security profile.

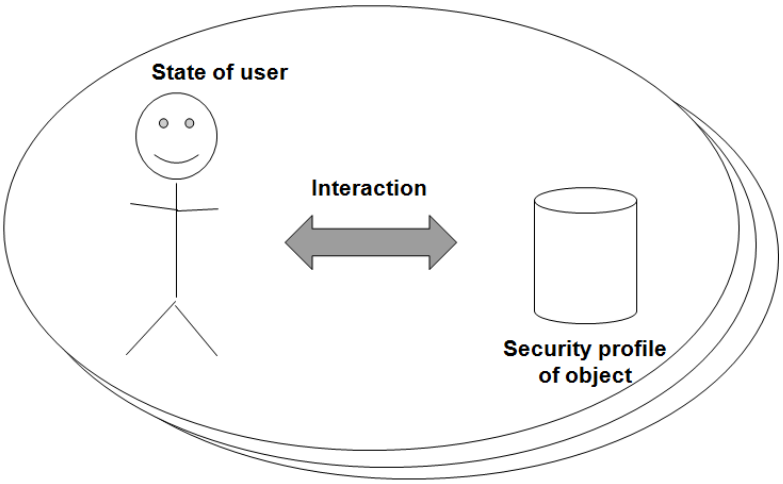


Figure 9: Overall context-aware condition

Using high-level policies on the context awareness obtained, adaptive authentication can be applied accordingly or environmental conditions altered to confirm the acceptance of the access.

With regard to the two examples of interaction, administrators can create policy to intelligently detect abnormal conditions such that the user is adaptively authenticated with a stricter realm or routed to a separate system with additional monitoring capability until s/he is correctly identified.

Alternatively, the user authentication can be simplified to the lowest acceptable realm for normal working conditions, giving a better and smoother experience.

In this way, context-aware security, by correlating all the contexts - locally and/or globally, with enforcement based on a user's identity and state - is able to bring a more complete picture of the required security posture, with deeper insight and more effective security.

Context-aware security not a totally new technology but an evolved policy-based control technology. However, more features and richer policy language will enable administrators to express policies in the language of business constructs so as to improve operational efficiency.

Self-healing System

Self-healing is a capability taken for granted in the biological world. The human body has a series of monitoring systems that detect when there is an abnormal situation such a cut in the skin which subsequently triggers a change in the electrical state near the cut, alerting pain receptors that drive the body to start its repair and protection.

Self-healing in IT requires tightly integrated and managed sensory feedback, controls for recovery and effective communication between the components and decision programs.
Sensory feedback would detect fault points, identify early failure parameters and engage in active sensing during the recovery while the decision program would use the feedback to control recovery.

From a wider system implementation view, self-healing is not limited to IT systems and can be seen in mission-critical systems such as in-flight control systems (IFSCs) on planes. During a failed event, an IFSC would try to determine the best possible adjustment to recover from that incident so that the pilot can regain flight control.

In the IT world, the mainframe reflects some of those resiliencies but work is still required so as to reach a parallel capability in the system type and network. Self-healing systems, infrastructures and networking induce a much needed stability, resilience and robustness under the component of security.

One example of self-healing is in data storage. In data storage systems, the disk arrays are constantly monitored and there is little or no maintenance required. Once a fault or error is detected, repair over the bad sector is attempted by the data storage system.

If the repair fails, the affected data is reconstructed and re-mapped on the virtual spare capacity. Similarly with the failure of a disk drive. As long as there is enough virtual spare capacity, the storage can be maintained at working state, demonstrating storage resilience for usage availability.

Using similar decision control and other available technologies such as virtualisation, systems can become self-healing.

Cloud Computing Security

Cloud computing is rapid evolving with new innovations and capabilities created regularly. This section would broadly discuss security technology concerns as well as opportunities over the security-ass-a-service platform and it underlying ecosystem. The full details of cloud computing is covered under section 5 of the ITR.

Cloud computing is not a single technology but a combination of many existing technologies fostered by the use of virtualisation. Virtualisation provides the abstraction of computing resources from application and the service user.

Virtualisation also enables applications to utilise the underlying computing resource on demand, according to its load from its service user, up to the maximum provision that the whole infrastructure can provide. It is hence considered a form of elasticity. Services rendered by these applications are not limited by a single system resource or capacity.

With the underlying infrastructure spanning across multiple data centres globally, availability for applications in these infrastructures is high as the application can be moved across the infrastructure and provide a good level of resilience.

Both the elasticity as well as resilience augur well for the provision of service. However, once the cloud system or infrastructure is compromised due to inherent flaws from the fostering technologies or the abstraction layer, the potential damage to applications or the receiving victims is unimaginable.

The large computational resources could be used to create large scale DOS attacks, with a reasonable assurance of resilience, over a wide range of targets,. As traditional control and mitigation measures start to melt down, the amount of data in these clouds as well as the dependence of the data create considerable issues that have to be dealt with.

Similarly, the security of the virtualisation abstraction layer, as well as an area that needs "hardening," would be targeted. The hypervisors are driven by codes and vulnerabilities for exploitation.

Application and resource partitioning would be greatly enhanced through the use of strong encryption and enhancement of identity and access control management in the best case scenario of isolations.
More work on cloud computing security needs to be done and it requires a shift in mindsets, architecture changes and security approach.

6.7.3 Five years or more

Big Data security analytics

Big Data refers to the volume, velocity, variety and complexity of large amounts of unstructured and semi-structured data that an enterprise creates. Big Data would take too much time and cost too much money to load into a relational database for analysis. The term, "Big Data," is often used when in the range of petabytes and exabytes of data or beyond.

The primary goal for looking at Big Data is to discover repeatable business patterns. It is generally accepted that unstructured data, most of it located in text files (and in social media and smartphone content), accounts for at least 80% of an organisation's data.

Big Data analytics requires analysis of large data sets in near real time, using frameworks like MapReduce to distribute the work among tens, hundreds or even thousands, of commodity computers.

Given the large amount of data collected, it is possible to extract event patterns for security-related incidents from any device that creates data other than traditional log sources such as IDS, anti-virus or firewalls. In this way, even the detection of potential APTs is possible from Big Data security analytics.

Gartner predicated that by 2016, 40% of enterprises, led by the banking, insurance, pharmaceutical and defence industries, will actively analyse patterns using datasets of at least 10 terabytes, in order to flag potentially dangerous activity.[47]

Big Data security analytics is to be expected to drive the next generation of SIEM (SIEM is limited to handling normalised data instead of raw transactions).

However, Big Data security analytics will not be a standalone product but will be packaged as part of the larger business intelligence for IT product range where Big Data will be mined for related business information and insights.

Security in Silicon

Intel's acquisition of McAfee for US$7.7 billion, completed in February 2011[48] after its July 2009 purchase of Wind River, a software company dealing with embedded and mobile software, indicated a trend of combining and aligning security software and hardware to take on the mobile and embedded device markets.

Like the TPM, this technology trend brings security onto the chip and hence, to some level, into embedded devices. Unlike the TPM which is a crypto co-processor, security in silicon refers to a more general state where different security functions are included in various deployable chipsets.

For example, a single chip can be used only for the byte-wide keystream of the C4 stream cipher algorithm in hardware implementation of WEP or TLS/SSL applications.

At the other end, an anti-virus engine can be placed in the hardware with signatures separately located to check for malware during boot time or program scanningfor access to the hardware resources. Since the engine is in the hardware, it cannot be easy disabled or re-programmed.

Working at the hardware level would also dictate that the program is less dependent on the changes, restrictions and vulnerabilities created by the OS and applications.

---

[47] Eric B. Parizo. Gartner: Big data security will be a struggle, but necessary. [Online] Available from: http://searchsecurity.techtarget.com/news/2240157901/Gartner-Big-data-security-will-be-a-struggle-but-necessary [Accessed 9th July 2012].

[48] Suzy Greenberg. Intel Completes Acquisition of McAfee. [Online] Available from: http://newsroom.intel.com/community/intel_newsroom/blog/2011/02/28/intel-completes-acquisition-of-mcafee [Accessed 9th July 2012].

Another advantage of having the security program in silicon form is that performance is greatly enhanced which is vital as scanning and the cryptographic process generally require a considerable amount of processing resources.

This development indicates that security is now being considered and designed in the basic core of the IT system. Essentially, building security functions and features into hardware instead of software saves power - a particularly valuable advantage on battery-powered devices such as smartphones.

Web Application Security Testing

With the Internet and rise of Web usage, Web application security breaches are among the most common security risk, threatening millions of users' data with exposure and highlighting the quality of Web application configuration and security.

After a Web application is set up, it is only prudent that it is tested thoroughly to expose any security shortcomings. Generally, automated Web application testing can divided into two main technology groups: Static Application Security Testing (SAST) and Dynamics Application Security Testing (DAST), with a third group, a hybrid of the two termed Interactive Application Security Testing (IAST).

SAST consists of a set of technologies designed to analyse application source code, byte code and binaries for coding and design conditions that are indicative of security vulnerabilities. SAST solutions analyse an application from the "inside out" in a non-running state so as to identify code weakness and poor coding practices.

In contrast, DAST technologies are designed to test an application from the "outside in," to detect conditions indicative of security vulnerability in an application in its running state. DAST is useful as a simulation of near real life attacks.

IAST is an application security testing solution combining dynamic and static techniques to improve the overall quality of the testing results. The information gathered by this instrumentation agent gives the hybrid solution an inside-out view that complements the outside-in view of a purely DAST solution.

Driving the need for SAST, DAST or IAST is awareness that Web application testing throughout the software development life cycle would help remove any vulnerability that could give rise to bigger security issues later.

The best solution would be to have both automated as well as manual testing applied into the Web application development life cycle.

For manual testing, good practices and standards, e.g., from the Open Web Application Security Project (OWASP),[49] can be used.

Operational Technology security

[49] OWASP. About the Open Web Application Security Project. [Online] Available from: https://www.owasp.org/index.php/About_OWASP [Accessed 9th July 2012].

Gartner defines operational technology (OT) as a collection of industrial technologies consisting of networks, systems, data and applications that support the operational systems in industries such as energy, manufacturing, utilities and transportation.

These technologies can be used in specialised or specific areas such as SCADA and in the introduction of “smartness” into underlying systems, as in the case of smart grids.

The evolution of OT and the emergence of attacks on targeted critical infrastructures and systems (e.g., SCADA and critical information infrastructures) have given rise to a category of products and services that provides security to, and protection of, these OT platforms and software.

New threats have made many OT enterprises realise they are relatively unprepared to cope with the risks and escalated the demand for security and governance in these areas

Software-defined networking security

Within the IT network environment, the routing or switching devices’ data and control planes are located in the devices as a proprietary closed system. This limits the flexibility of extending the network as well as restricts the network's capability to handle the complexity in network elements.

Elastic cloud architectures and dynamic resource allocation, combined with the growth of mobile devices, have highlighted the inadequacy of closed platform networking in dealing with the security challenge. There is thus a requirement for an open and flexible networking environment and the development of Software Defined Networking (SDN).

In the SDN architecture, shown in the figure below, the control and data planes are decoupled. The two planes communicate via the Openflow protocol tunnelled via SSL. Business applications that use and manage network intelligence and states are logically centralised, with the underlying network infrastructure abstracted from the applications.

As a result, enterprises and carriers gain unprecedented programmability, automation, and network control, enabling them to build highly scalable, flexible networks that readily adapt to changing business needs.

The key application and adoption of SDN would be in the consolidation of large data centres, carriers’ networks and possible self-healing networks and the provision of Infrastructure as a Service (IaaS).

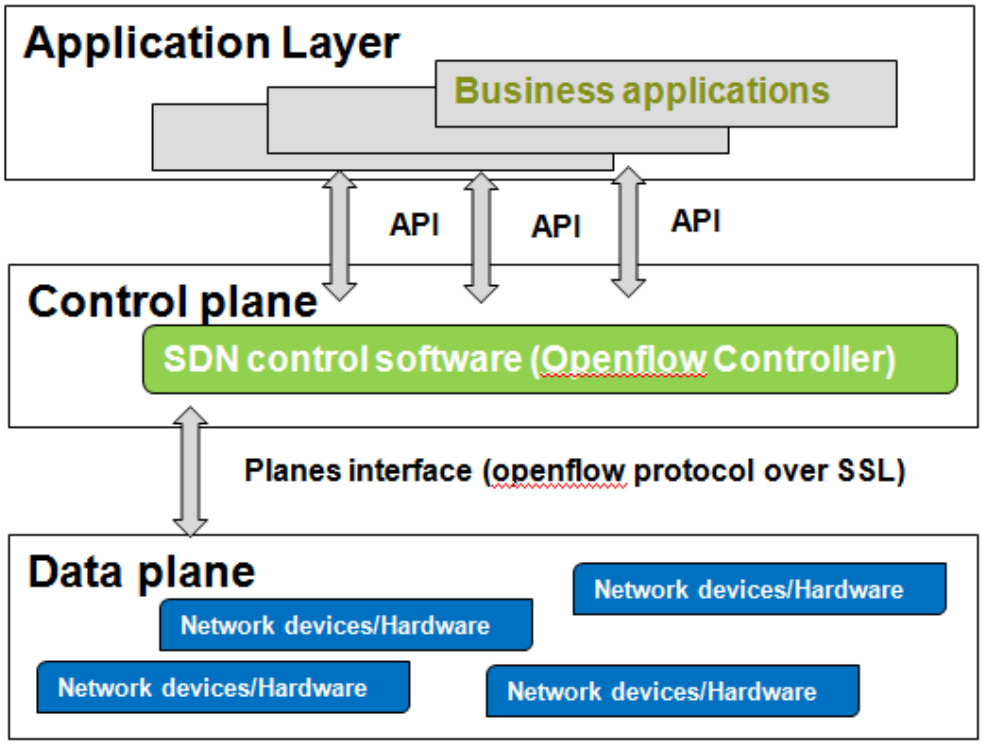


Figure 10: Software Defined Networking Architecture

Market Applications/ Opportunities

Security provides certain levels of assurance to the users of services and products. The increasing use of the Internet and the hyper-connectivity of networks in cyberspace create even more opportunities for security incidents and events. The public needs to be better educated and more aware of the need for stronger cyber protection and security. Opportunities for cyber security technologies and solutions would be in great demand in the years to come.

6.8.1 User authentication and authorisation

Having the user properly authenticated so that the correct authorisation can be given is an essential component of cyber security. Basic user and password authentication in the form of single-factor authentication is no longer adequate as a guarantee of cyber security. Users now need to have more complex and different passwords for different accounts and adhere to a policy of changing passwords several times a year.

The vulnerability lies in the human element – careless users can weaken and compromise the entire security process. Adaptive and context-aware authentication or usable security would be an important application in this market .

6.8.2 Digital records and transactions

Data today is being transformed in the digital realm and transacted in cyberspace. With the physical and at times, logical boundaries dissolving, data protection during creation, in

transit and at rest is a significant and important part of cyber security. Applications can range from banking and financial transactions, mobile eWallets to digital cheques and signatures.

Privacy enhancement is an essential requirement for protection in sensitive areas such as patient health records. It is not uncommon to hear of "database kidnapping" and the extortion of money for the recovery of medical records. A recent case of a ransom demand for the key or password to a specially encrypted healthcare database in the USA[50] highlights the vulnerability of the healthcare system to such cases of cyber crime. It would seem that cyber criminals are now getting more "creative" with their methods and demands. Not content only with data breaches and selling the stolen data on the black market, cyber criminals are now moving into the realm of blackmail and extortion.

Fraud and counterfeit would be another area where the authenticity of digital records and transactions could be challenged and solutions provided.

Embedded security solutions, working together with other security technologies such as certificates and strong cryptography, are only one of the many methods to respond to the need for greater digital records security.

6.8.3 Critical and essential infrastructure

Energy generation and distribution, water supply, public transport and signalling systems are the types of critical and essential infrastructure that would merit greater attention in the cyber security space today.

With the increasing use of smart-grids and interconnected networks, these infrastructures are vulnerable to acts of cyber terrorism which can shut down critical systems, compromise national security, and threaten economies and political stability. Because of the nature of cyber networks and the use of interconnected systems in cyberspace, the impact of such acts would be devastating.

Conclusion

Cyber security is at a crucial point of development. ICT products and services are expected to incorporate security elements to manage malicious activity carried out by criminals, spies and other bad actors that threaten the economic growth and efficiency that a single, global, interoperable network has brought us.

In effect, APTs are simply a wake-up call that tells us that the bad actors are not another Chicken Little story that security practitioners have been warning us about. These actors have been with us since the initial creation of the digital world and operate with relatively unchanged motivation.

[50] In August 2012, hackers penetrated the computer network of a small medical practice in a wealthy suburb of northern Illinois, The Surgeons of Lake County, and broke into a server containing e-mail and e-medical records. They encrypted the data and posted a message demanding a ransom payment in exchange for the pasword. OWASP. Adam Levin. For ransom: Your medical records. [Online] Available from: http://abcnews.go.com/Business/ransom-medical-records/story?id=17051612#.UJVTs7Q29IA [Accessed 3rd November 2012].

As the number of cyber incidents increase because of our heightened intimacy with cyberspace and attacks grow increasingly sophisticated, stakeholders, from political leaders to businesses and the public, will naturally demand, and expect more of, cyber security.

Demand for better security will continue to drive technology innovation so that security can be better integrated and more seamless in its implementation. Eventually, cyber security will reach a state that resembles our immune system, living among us, protecting us - in silence.