Emerging Cyber-Security Threats in Cloud Computing

Author: James Truckle

We review the increasing need to focus time and energy to threats in cyber space facing both the government and private sector. We begin by introducing the emerging concept of cloud computing and follow by introducing cyber threats. In particular, we describe and review the threat to critical infrastructures that pose an even greater danger than nuclear warheads. This is followed with a review of espionage conducted in cyber space and the specific areas of concern. We conclude by pointing to where focus needs to be placed and continue by suggesting methods to improve the current defense process. We have pointed to threats that we see to be of highest concern. Our review of this rapidly evolving threat demonstrates that current defense mechanisms are not sufficient in protecting systems from high intensity cyber-attacks.

Keywords – *Cloud computing, critical infrastructure, cyber-attacks, cyber espionage, Industrial Computer System*

1 Introduction

As the internet has expanded and improved over the last decade, a new concept of data storage has emerged that utilizes the internet to provide technology enabled services to people and organizations [1]. Cloud computing is being promoted as the 5th utility service after water, electricity, gas and telephony. Its infrastructure is leased and the needs of specific enterprises are met by the service provider. By converting capital expenditure of an organization into operational expenditure, costs are cut. No maintenance cost is involved because this, as well as securing data centers, is the responsibility of the service provider. Remote servers are accessed through new web-based applications and are placed in extremely safe and secure data centers [1],[2]. The cloud systems are extremely flexible, meaning they can be scaled up or down, they can have basic security or high-level protection, and most aspects of the package can be adjusted as and when required based on the customers' needs [3].

In cloud computing there are three types of services that can be provide [1].

Software as a Service (SaaS): Software is provided to customers as a service according to their specific needs. Customers have access to the services that are hosted on the cloud server.

Platform as a Service (Paas): Customers are provided access to platforms, allowing them to provide their own software and other applications on clouds.

Infrastructure as a Service (Iaas): Storage systems, processing, network capacity and all basic computing resources are rented. This enables customers to manage all aspects of their computing.

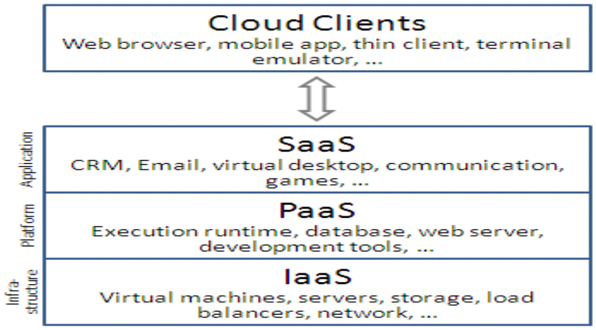
Cloud Clients
Web browser, mobile app, thin client, terminal emulator, ...
SaaS
CRM, Email, virtual desktop, communication, games, ...
PaaS
Execution runtime, database, web server, development tools, ...
IaaS
Virtual machines, servers, storage, load balancers, network, ...
Application
Platform
Infra-structure

Figure 1 shows the types of cloud computing - Wikipedia

From this emerging technology, there is a consensus that security is the primary challenge which could hinder its development. Current users are not happy with the current level of security that is in place. Information security can be specified as ensuring the availability, integrity, and confidentiality of information. Information needs to be accessible when needed, without undetected corruption, and withheld from unauthorized personnel. These challenges present difficulties to the adoption of cloud computing and are the reason that it has been inhibited to a great extent [1] [2]. These security challenges can be further described as aggressive action in cyber space, which can be further articulated as cyber-attacks. In this paper, we will review cyber-attacks on critical infrastructure and espionage in cyber space as a result of the development of cloud computing. We will emphasize SCADA control systems and valuable research and development technology.

2 Cyber Attacks

The emergence of cloud computing has increased reliance of the internet and the need for effective security. Both in the industrialized private sector and in state governments the same unprecedented threat to security and economic well-being exists. For the private sector, the threat is clear; competitors could use industrial espionage for economic gain where technological progress has been achieved. For states, cyber terrorism has the potential to damage critical infrastructures that are required to keep the populous safe and secure. These infrastructures include banking and finance, electric power, information and communications, oil and gas production, transportation, water supply, emergency services, and the continuity of government services [4].

During the remainder of this paper, similarities will be drawn between the threats to the private sector and the threats to states. Because of this, the term ‘cyber terrorism’ may not always apply. Cyber terrorism is designed to instill terror among a target population [5]. It is the use of computer networks in order to disrupt or destroy human life. While addressing these threats is central to the continued protection of a nation, they do not include the attacks carried out by any group that has the intent to increase knowledge through espionage in cyberspace. Therefore, the term cyber-attacks and the threat of the utilization of aggressive cyber capability will replace cyber terrorism.

2.1 Infiltrating Critical Infrastructure

With the growing interconnectedness of critical infrastructures, attacks at the right node have devastating potential. According to the Information Management Journal, cyber space threats pose the highest risks alongside terrorism, an international military crisis, or a natural emergency, ahead of the second tier threats that include nuclear attack. For this reason, increasing focus on protection of these systems has to be a priority of government defense agencies.

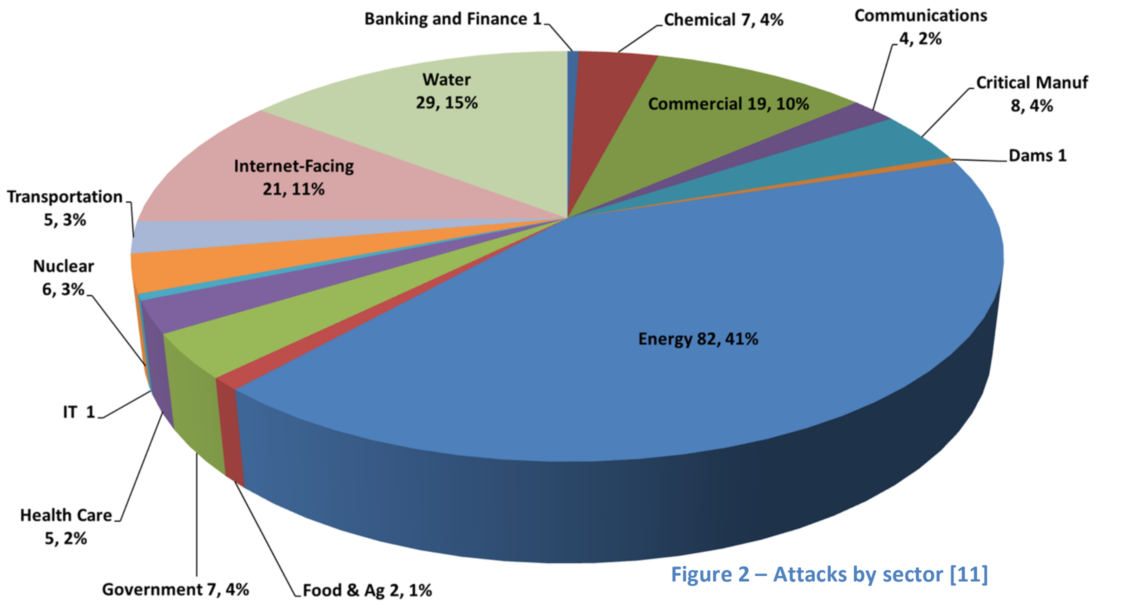

Figure 2 – Attacks by sector [11]

The effects of infrastructure attacks are deterrent. This was shown in 2009 when the United States became aware that its electricity network had been hacked into. Allegedly, parts of the network could be shut down whenever the hacker wished to do so. This attack was traced to China and is a clear indicator that the United States could have a serious problem protecting itself from an ambitious Chinese cyber program [6].

2.11 Areas of Highest Concern

Most critical infrastructure is monitored and controlled via an ICS or an Industrial Computer System. If this system were to be penetrated by a malicious user, they would have control over all aspects of the utility, service, or process.

According to the Industrial Control Systems Cyber Emergency Response Team [11], in 2012 over 40% of all incidents reported were attacks against the energy sector. The penetrating attacks target information that could facilitate remote access and unauthorized operation.

Disruptions to any one of these infrastructures would have devastating effects on the people who rely on them. One component of critical infrastructure systems being threatened are SCADA systems. [7] A SCADA system is an Industrial Computer System (ICS) for monitoring and controlling a critical infrastructure process.

The processes include manufacturing, energy utilities, refining, oil and gas pipelines and large communication infrastructure. Cyber threats to ICS's are growing [7]. The CIA confirmed a cyber-attack caused power outages in multiple cities including New Orleans in 2008. Unlike other attacks, attacks to SCADA systems are intent on disabling operations and are meant to destroy not just disrupt. This makes their protection an absolute priority.

2.12 SCADA Vulnerabilities

There are numerous threats to Industrial Control Systems and specifically processes controlled by SCADA [7]. One serious incident that could endanger human life is interference with operation of safety systems.

Another would be the unauthorized changes to instructions, commands, or alarm thresholds, which could damage, disable, or shut down equipment, creating environmental impacts in addition to endangerment of human lives.

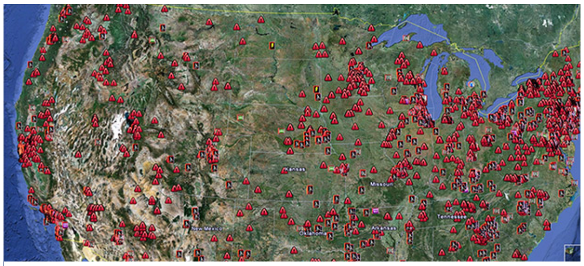

Figure 3- The Department of Homeland Security released this map showing the locations of 7,200 key industrial control systems that appear to be directly linked to the Internet and vulnerable to attack.

SCADA systems typically have a shelf life of 10-20 years. Some older systems were designed with little or no notion of cyber security. This, in addition to the increasing use of common operating systems and the Internet makes systems much more difficult to secure and much more vulnerable to intrusion attacks. Unauthorized changes pose the greatest threat to national infrastructure. ICS software or configuration settings can be modified, or software can be infected with malware. The countermeasure to these intrusions is the development of intrusion detection systems (IDS).

Since most critical infrastructures are now privately owned, companies are in a precarious position. The well-being of society depends on the effectiveness of the private sector's protection system. This situation presents a complex problem for states across the globe on how best to protect their citizens. Should it be left in the hands of the private sector, or does its importance merit substantial government support? The private sector is critical to successfully combating aggressive cyber capability, but training, education, and a push towards a more secure and safer internet must all be initiated by the government. They are responsible for protecting the people. With regards to SCADA technology (technology used to manage critical infrastructure) the US Department of Homeland Security needs to recognize the vulnerability and take urgent action perhaps in partnership with private enterprise.

2.2 Industrial and State Espionage in cyber space

As we move away from the concept of using cyber-space as a weapon of destruction used to cause harm on society, we approach a second, possibly more immediate, threat concerning the emergence of cloud technology and the continued reliance on the internet.

According to Symantec Internet Security Threat Report, the number of targeted attacks on industry increase from 77 per day in 2010 to 82 per day in 2011. Targeted attacks are attacks using customizable malware and refined social engineering to obtain sensitive information without authorized access. Refined social engineering refers to the art of manipulating people into performing actions or divulging confidential information.

It is clear from the results indicated in the graph that attacks on governments and corporations aimed at stealing information are inevitably increasing. A reported attack in 2011 resulted in the theft of 24,000 files belonging to a US defense contractor for a weapons system

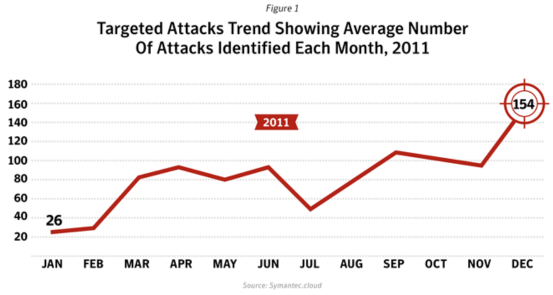

Figure 3 - Symantec Internet Security Threat Report

belonging to the US Department of Defense [8]. Another challenging aspect of cyber infiltration is the unidentified source. The US faces threats from peer nations, trading partners, hostile countries, non-state actors, terrorists, organized crime, insiders, and teenage hackers [6].

2.21 Areas of Highest Concern

Similar to attacks on critical infrastructure, attacks concerning information in cyber space are not isolated to governmental agencies. It is a threat that concerns the private sector in addition to states. Targeted attacks affect all sectors of the economy. Figure 3 illustrates this. This clearly indicates that foreign intelligence services and corporations conducting cyber espionage are interested in two specific fields: strategic economic strength and military capability intelligence [9].

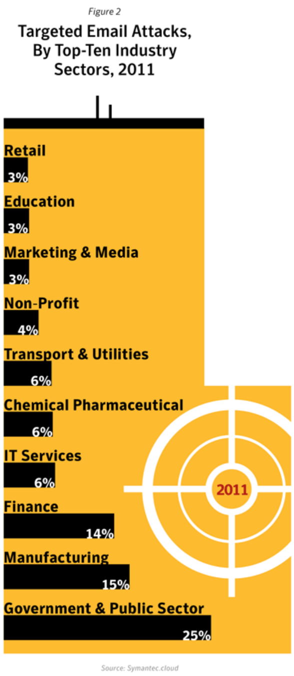

Figure 5 – Symantec Security Report

Strategic economic strength can be associated with aspects related to manufacturing and production processes in addition to aspects related to important infrastructures. Important areas for concern would be in science and technology academia. Protecting national and corporation internal research and developments against foreign countries or competitors is an important task [9].

Technology relating to military capability intelligence is an area where enemy armies may have a specific focus, in addition to collecting information on military capabilities. These target fields show that applied science research and technology are focal points for espionage in general.

2.22 Specific Threats relating to Espionage – *Social Engineering and Intrusion Attacks*

Refined targeting using social engineering has evolved to the point where victims are researched in advanced and specifically targeted [8]. In the past, these techniques have been used to steal customer data for financial gain. However, advanced persistent threats use targeted attacking as part of a longer- term campaign targeting high-value information in government and industry. A common example of social engineering would be where a hacker sends an email to an employee, claiming to be an administrator who needs the employee’s password to do some work. Social engineering attacks are easy ways for hackers to gain access to corporate data with very little work. These attacks can be minimized and prevented by creating security aware users. Taking the time to run a short and simple user awareness program will decrease liability significantly.

Intrusion attacks are more refined and more difficult to prevent. Much like penetrating attacks to SCADA systems, hackers use known vulnerabilities in the network in gain access. Some examples of intrusion attacks are viruses, worms, and Trojan horses.

A hacker can develop harmful code known as a virus [12]. They can then use password-cracking techniques to gain access to a system and plant the virus. Malicious programs or software code can be hidden inside what looks like a normal program, this is called a Trojan. When a user runs the program it can cause damage to the computer. Worms are programs that run independently and travel from computer to computer across network connections.

Corporations and governments need to design protocols to protect from both intrusion attacks and social engineering. A good hacker will use both to steal information. By using impersonation in email they can plant their Trojan. This will then leave data unprotected and technology will be shared.

3 Conclusion

Cyber-attacks pose threats to national security and economic well-being, and we have only just begun to realize the depth and extreme nature of the threat. We have reviewed critical infrastructures and SCADA system vulnerabilities within them. We have also reviewed intrusion attacks and social engineering attacks to conduct espionage in cyber space. Without a doubt, we are seeing parallels between the two issues: attacks on critical infrastructure and espionage in cyber space. It is clear from analysis that the number of threats is rising with the continued growth of technology and the inter-connectedness of the internet. It has also been suggested that there is an equal magnitude of threat facing the private sector in addition to the government sector. These two entities should be encouraged to work together for the benefit of all.

To protect our nation's critical infrastructure, valuable corporate technology, and state R&D further cyber defense mechanisms need to be implemented. [10] The state of cyber defense today could be significantly improved if every vendor, owner, and operator of information technology systems and networks would implement what is already known about mitigating threats. Taking this concept further, if individuals and organizations worked collectively to adopt the best practices cyber security would be improved. State defense agencies need to work with private-sector experts to address the problem as one. According to the National Research Council report, today's state of knowledge does not include defense against a high level cyber threat to ICS systems originating from a major nation state. Research needs to be conducted to place an emphasis on these high-level threats. We have made analysis to determine the areas where high level threats will likely be executed. These areas of concern are Industrial Control Devices, manufacturing processes, and military intelligence.

No one solution exists that will prevent a hostile party from destructive behavior. There are numerous techniques to implement intrusion techniques which are evolving in sophistication every day. As humans, in order to counter the progression of social engineering our best defensive techniques must involve inducing people to behave in a way that does not compromise security. Education can teach people not to fall victim to fish-hooking emails, intended to obtain login names and passwords. Monitoring internet use can encourage people to not use information technology in ways that may leave the organization vulnerable to attacks. These methods can only be successful in preventing attacks some of the time. Intrusion Detection Systems need to be developed in conjunction with education. These systems need to be developed by the leading experts in both corporations and government agencies. Knowledge on detection needs to be shared so it can then be implemented in all organizations.

Even with a solid defense mechanism no one technological advance, or one strategy, or one control agreement will result in a safer and secure cyber space [10]. With the plethora of attackers (hostile countries, terrorists, insiders, organized crime, and individual hackers) and the rapid pace of technology that is occurring before our eyes, progress related to security will likely be incremental and slow. Presently, responsible nations need to apply what they know and seek to develop new options for protecting themselves against cyber conflict.

Acknowledgment

The author would like to thank Professor Tom Akbari and Undergraduate Elena Losada for helping in the process of writing.

References

[1] Shaikh, F.B.; Haider, S., "Security threats in cloud computing," *Internet Technology and Secured Transactions (ICITST), 2011 International Conference for* , vol., no., pp.214,219, 11-14 Dec. 2011

[2] Khan, A.U.; Oriol, M.; Kiran, M.; Ming Jiang; Djemame, K., "Security risks and their management in cloud computing," *Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference on* , vol., no., pp.121,128, 3-6 Dec. 2012

[3] Behl, A., "Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation," *Information and Communication Technologies (WICT), 2011 World Congress on* , vol., no., pp.217,222, 11-14 Dec. 2011

[4] Frank Cilluffo, Paul Byron Pattak. "Cyber threats: Ten Issues to Consider" *Georgetown Journal of International Affairs*, Volume 1, Number 1, Winter/Spring 2000

[5] Ahmad, R.; Yunos, Z.; Sahib, S., "Understanding cyber terrorism: The grounded theory method applied," *Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on* , vol., no., pp.323,328, 26-28 June 2012

[6] Hjortdal, Magnus. "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence." *Journal of Strategic Security* 4 (2011): 1-25. Print.

[7] *Information Management Journal*; Jul2002, Vol. 36 Issue 4, p10, 2/3p, 1 Color Photograph

[8] "Internet Security Threat Report | Symantec." *Endpoint, Cloud, Mobile & Virtual Security Solutions | Symantec*. N.p., n.d. Web. 27 Mar. 2013. <http://www.symantec.com/threatreport>.

[9] Dirk Thorleuchter, Dirk Van den Poel. "Protecting research and technology from espionage" *Expert Systems with Applications*, Volume 40, Issue 9, July 2013, Pages 3432–3440 <http://0-dx.doi.org.ilsprod.lib.neu.edu/10.1016/j.eswa.2012.12.051>

[10] Lin H. A virtual necessity: Some modest steps toward greater cybersecurity. *Bulletin Of The Atomic Scientists* [serial online]. September 2012;68(5):75-87. Available from: Academic Search Premier, Ipswich, MA. Accessed March 27, 2013.

[11] "ICS CERT Monitor ." *Industrial Control Systems Cyber Security Response Team,* October (2012): 1-15. Web.

[12] "Security Threats." *Resources and Tools for IT Professionals | TechNet*. N.p., n.d. Web. 3 Apr. 2013. <http://technet.microsoft.com/en-us/library/cc723507.aspx#XSLTsection12612