Abstract

The rampant fleshing out of "The World Wide Web" has become the home of knowledge for both philosophising and contemplating. Albeit parents take pride that their kids are more informed than them in various fields. People face hardships and grievous situations like cyberbullying, harassments, assaults, false identification, terrorism and money laundering hoots called businesses because of the same Cyber. Since Cyber has become a great influencer and another world “The E world”. Its our hardware, software, our laptops and desktops, cellphones and smartphones that have intertwined in every aspect of our life. It’s the broadband network beneath us and the wireless signals around us, the local networks in our schools, hospitals, businesses are the massive grids that power the nation. It’s the classified military and Intelligence works that keeps us safe. It’s the world wide web that has interconnected us humans more than ever in the human history. So Cyber space is real and so are the risks that come with it. Since Cyber has become a great influencer and another world “The E world”. It’s our hardware, software, our laptops and desktops, cellphones and smartphones that have intertwined in every aspect of our life. It’s the broadband network beneath us and the wireless signals around us, the local networks in our schools, hospitals, businesses are the massive grids that power the nation. It’s the classified military and Intelligence works that keeps us safe. It’s the world wide web that has interconnected us humans more than ever in the human history. So cyber space is real and so are the risks that come with it. Its the great irony of our Information Age E that very technologies that empower us to create and to build also empower those who would disrupt and destroy. And this paradox is something we experience everyday”. (Obama,2009) It has become a responsibility to provide security to this Virtual World.

Introduction

Our society, economy and critical infrastructures have become completely reliable on networks and Information Technologies and Information Communication Technologies. Cyber attacks have become more attractive and potential threats as our resources have been flooded. According to the Symantec’s CyberCrime Report published in April, 2012. Cyber attacks cost USD $114 billion each year. Victims of cyber attacks are also significantly growing based on the survey conducted by Symantec which involved interviewing 20,000 people across 24 countries, 69% reported being the victim of Cyber attack in their life time.

I. Cyber Security

Cybersecurity concerns with the undersanding of surrounding issues of diverse cyber attacks and devising defense strategies (i.e., countermeasures) that preserve confidentiality, integrity and availability of any digital and information technologies [18].

• Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems.
• Integrity is the term used to prevent any modification/deletion in an unauthorized manner.
• Availability is the term used to assure that the systems responsible for delivering, storing and processing information are accessible when needed and by those who need them.

II. A Fine Balance

It is widely accepted in industrial security analysis that the security risk faced by an organization is a function of both the Likelihood of Successful Attack (LAS) against an asset or an act to hide a negative imprint and illegitimate process. The second variable, Consequence, while highly site specific, is generally the easiest to get an understanding of. Often it can be estimated in terms of financial loss, acute health effects or environmental impacts; concepts well understood from years of safety analysis of hazardous processes.

Estimating the Likelihood of Successful Attack is far more difficult. Threat (T): Any indication, circumstance, or event with the potential to cause
the loss of, or damage to an asset. Vulnerabilities (V): Any weakness that can be exploited by an adversary to gain access to an asset. Target Attractiveness (AT): An estimate of the value of a target to an adversary.

These terms are more difficult to estimate, particularly with respect to cyber security.

This difficulty is largely because we have little reliable historical or statistical data to work with. The details of safety related incidents have been recorded for over a century, while cyber security incidents have risk, with the potential cost of an event occurring. To do so we need to understand the variables at play in defining the cyber security risk for an industrial facility. Furthermore, we need to continuously monitor the risk variables to determine if they are changing. To be effective from both a technical and cost perspective, our mitigation response must adapt to changes in Threats, Vulnerabilities or Target Attractiveness. The consequences of successful attacks are not insignificant less than two decades of occurrence, never mind record keeping. Furthermore, most organizations are highly reluctant to report security incidents as they are viewed as potential embarrassments. In fact, many organizations have denied that there even is a risk to industrial systems never mind record keeping. Furthermore, most organizations are highly reluctant to report security incidents as they are viewed as potential embarrassments. In fact, many organizations have denied that there even is a risk to industrial systems from cyber attack. For example, as recently as March 2002 an article in CIO Magazine entitled “Debunking the Threat to Water Utilities” stated there was no credible risk to SCADA systems from a network-based attack:

“Most public utilities rely on a highly customized SCADA system. No two are the same, so hacking them requires specific knowledge.”[3]

There is obviously some security risk faced by industrial control systems and, as difficult as it is to estimate, we still need to understand it. We can’t ignore the risk still we also can’t afford the infinite cost of perfect security.

III. Emerging threats

Cyber attacks on cyberspace evolve through time capitalizing on new approaches. Most times, cyber criminals modify the existing malware signatures to exploit the flaws in the new technologies. In other cases, they explore unique characteristics of the new technologies to find loopholes to inject malware. Taking advantages of new Internet technologies with millions and billions of active users, cyber criminals utilize these new technologies to reach out vast numbers of victims quickly and efficiently. We select such upcoming technology advancements: social media, smartphone technology, and critical infrastructure, as illustrative examples to explore the threats in these technologies. We discuss unique characteristics of each of the emerging technologies and analyze number of common attack patterns presented in them.

A. Social media

Social media, such as Facebook and Twitter, has shown explosive growth in recent years. At the end of 2012, there are 450 million active users in Twitter while the number grows exponentially in Facebook reaching almost a few hundred billions. Social networking sites also have raised the stakes for privacy protection because of the centralization of massive amounts of user data, the intimacy of personal information collected, and the availability of up-to-date data which is consistently tagged and formatted. This makes social networking sites an attractive target for a variety of organizations seeking to aggregate large amounts of user data, some for legitimate purposes and some for malicious ones. In most cases, extracting data violates users’ expectations of privacy. Protecting user’s private data kept in the social networking service providers has been explored data using clientside JavaScript. Privacy wizard, the wizard iteratively asks the user to assign privacy “labels” to selected friends, and it uses this input to construct a classifier, using a machine learning model.

B. Smartphones

Smartphones, coupled with improvement in wireless technologies, have become an increasingly sophisticated computer and communication device that is readily carried by individuals throughout the day. The convergence of increasing computing power, personalization and mobility makes them an attractive means of planning and organizing work and private life of individuals. According to [16], the sheer volume of mobile phone users around the world indicates a current need for proactive mobile security measures. It is assumed that over 4.5 billion use a cell phone every day and an estimated 2 billion smartphone will be deployed by 2013.
Going beyond the simple SMS messaging, increasing level of sensitive information is stored in smartphones. Within companies, these technologies are causing profound changes in the organization of information systems and therefore have become the source of new risks. As smartphones collect and compile increasing amount of sensitive information, the access must be controlled to protect the privacy of the user and the intellectual property of the company.

These staggering growths in mobile technology have created an attractive target for cyber criminals. Security concerns in mobile are different from the traditional security problems in PC and enterprise computing due to their embedded nature and different operational environment. Mulliner [119] listed the following features unique to mobile computing.

- **Mobility**: This is the most important characteristic of the mobile phones. Since mobile users can take them to anywhere.
- **Technology Convergence**: Today numerous functional features are integrated in the mobile phones, for example gaming, video and data sharing, and Internet browsing.
- **Limited Resources and Reduced Capabilities**: Comparing with stationary devices, mobile devices have four major limitations:
  - a) limited battery life, b) limited computing power, c) very small display screen size, and d) very small sized keys for inputs. These limits bring the challenges in building mobile security technology.

IV. Long term impact

National security breaches (e.g. the incident in 2010 where classified/confidential government information was leaked to Wikileaks).

Social discontent and unrest (e.g. loss of public confidence in the government even if the actual damage caused by the cyber criminal activities was minimal).

Loss of intellect property, which can affect the long-term competitiveness of businesses and governments in industrial and military espionage incidents.

The million-dollar question is “How prevalent is financially-motivated cyber criminal activity such as unauthorized access, online extortion and Distributed Denial of Service (DDoS) attacks?”. Official crime statistics compiled by law enforcement, prosecution and other government agencies, and private sector agencies are unlikely to indicate the entire cyber threat landscape. For example, victims were not aware that their organizations had experienced one more cyber security incidents, and therefore indicated that they had not experienced any such incidents when asked. In addition, victimized organizations may be reluctant to report breaches due to a range of reasons, such as believing the incident was not serious enough to warrant reporting it to law enforcement and other competent agencies, believing that there is little chance of a successful prosecution, fearing negative publicity and that reporting would result in a competitive disadvantage (Richards, 2009).

The concern of cyber crime is not only perceived by computer scientists and ICT professionals, but politicians also understand its potential impact as well (Obama, 2009).

V. Cyber crime prevention strategies:

Various crime prevention practices are generally based on actor choice (cf. neo-classical deterrence theory). The Routine Activity Theory (RAT), for example, proposes that crime occurs when a suitable target is in the presence of a motivated offender and is without a capable guardian (Cohen and Felson, 1979).

The theory draws on rational exploitation of 'opportunity'
in the context of the regularity of human conduct to design prevention strategies, especially where terrestrial interventions are possible e for example in the transit of goods. It assumes criminals are rational and appropriately resourced actors that operate in the context of high-value, attractive targets protected by weak guardians (Felson, 1998; Yar, 2005).

In the context of cyber crime, an assumption is that cyber criminals are (1) criminally and/or financially-motivated that seek out (2) opportunities provided by cyberspace such as anonymity and no geographical limitations, acquire the necessary resources for cyber crime by (inter alia) using delinquent/rogue IT professionals and (3) targeting weakly protected systems/networks and exploiting situations where law enforcement agencies are being hampered by jurisdictional, legislative and evidentiary issues, particularly in cross-border cyber criminal cases (Broadhurst and Choo, 2011).

There are a number of ways that criminological theories such as RAT can be applied to reduce the risk of cyber crime. Cyber crime prevention strategies using RAT, for example, target each of these areas e (1) increasing the effort required to offend; (2) increasing the risk of getting caught; and (3) reducing the rewards of offending e see

No single entity “owns” the issue of cyber security. While governments cannot completely delegate the role of securing cyberspace, governments cannot work in isolation.

VI. Conclusion

While cyber criminal and security risks may be seen by some as an extension of existing threats to cyber and national security, the threat landscape is an extremely fast-moving environment. Only seven years ago, several criminologists warned that ‘those who fail to anticipate the future are in for a rude shock when it arrives’ (Smith et al., 2004: 156). It is essential for our society to be prepared and for our businesses, governments and research institutions to innovate faster than criminals and other actors with malicious intentions.

VII. References


2011 [Date last accessed: 06.07.11.]