CRITICAL NATIONAL NEED IDEA

ADVANCED RISK MODELS
FOR EVALUATING CRITICAL INFRASTRUCTURE CYBER SECURITY
THREATS, EXPLOITS, VULNERABILITIES, INCIDENTS, AND RESPONSES

Submitting Organization: The United States Cyber Consequences Unit

Contributing Organizations: N/A

Contact Information:

C. Warren Axelrod, Ph.D.
Research Director for Financial Services
The United States Cyber Consequences Unit
P.O. Box 234030
Great Neck
New York 11023

Telephone No: **917-670-1720**

E-mail Address: warren.axelrod@usccu.us

Key Words:

cyber security
risk
critical infrastructure
threats
exploits
vulnerabilities
incidents
responses

ADVANCED RISK MODELS FOR EVALUATING CRITICAL INFRASTRUCTURE CYBER SECURITY THREATS, EXPLOITS, VULNERABILITIES, INCIDENTS, AND RESPONSES

INTRODUCTION

This document is in response to the NIST TIP (Technology Innovation Program) request for White Papers on Areas of Critical National Need. TIP was established by the America COMPETES Act (PL 110-69) for the purpose of assisting United States organizations, including nonprofit research institutes, to support, promote, and accelerate innovation in the United States through high-risk, high-reward research in areas of critical national need.

AN AREA OF CRITICAL NATIONAL NEED (CNN)

The area selected as the Critical National Need is "Advanced Risk Models for Evaluating Infrastructure Cyber Security Threats, Exploits, Vulnerabilities, Incidents, and Responses." This CNN was selected from a larger field, including critical infrastructure protection, information security economics, and risk analysis. It was selected on the basis that current models are woefully inadequate as illustrated by the clearly apparent lack of preparation for major attacks and the knee-jerk reactions when attacks do occur. The need is for a better understanding of what is at risk, the likelihood of adverse events and the most appropriate investments to mitigate the most critical risks. Inputs regarding potential areas of CNN were obtained from the following publications:

- **Defending America's Cyberspace: National Plan for Information Systems Protection, Version 1.0 An Invitation to a Dialogue**, The White House, 2000. May be downloaded from link at www.libertysecurity.org/article729.html
- **National Infrastructure Protection Plan**, 2006. Links available at www.dhs.gov/xprevprot/programs/editorial_0827.shtm
- **FSSCC (Financial Services Sector Coordinating Counsel for Homeland Security and Critical Infrastructure Protection) Research Agenda**, September 2008. Available at www.fsscc.org/fsscc/reports/2008/RD_Agenda-FINAL.pdf
- **INFOSEC Research Council (IRC) Hard Problem List**, November 2005. Available at www.cyber.st.dhs.gov/docs/IRC_Hard_Problem_List.pdf
- Various **NIST Special Publications (800 Series),** available at http://csrc.nist.gov/publications/PubsSPs.html including:
  - SP 800-12 **An Introduction to Computer Security: The NIST Approach**, October 1995
  - SP 800-14 **Generally Accepted Principles and Practices for Securing Information Technology Systems**, September 1996
  - SP 800-83 **Guide to Malware Incident Prevention and Handling**, November 2005
  - SP 800-80 **DRAFT Guide for Developing Performance Metrics for Information Security**, May 2006
  - SP 800-100 **Information Security Handbook: A Guide for Managers**, October 2006

- SP 800-39 **DRAFT Managing Risk from Information Systems: An Organizational Perspective**, April 2008

- Various **FFIEC Information Technology Examination Handbook** booklets, available at www.ffiec.gov/ffiecinfobase/html_pages/lt_01.html including:
  - Information Security
  - Management
  - Business Continuity Planning
  - Development and Acquisition

The output of the work proposed here is a series of implementable, usable, and accurate models for determining the risk to the critical infrastructure resulting from the successful exploitation of cyber vulnerabilities and inadequate responses to actual incidents. Current risk models, while reasonably well developed for a limited range of existing and potential threats, vulnerabilities and incidents, do not provide sufficient accuracy and are not convincing enough for decision makers. Given this situation and the continuing and accelerating seriousness of threats and exploits, as attackers evolve from recreational hackers to organized criminals to hostile terrorists and nation states, the creation of accurate, effective and reasonably easy-to-use models requires a leap in technology that can only be acquired through transformative research, rather than continued incremental advances of the current state of the art.

The need for advanced cyber security risk models is *national* because every component of the nation's public and private critical infrastructure is subject to the risks of cyber attacks. The need is *critical* because the national infrastructure is more subject to increasingly severe attacks with each passing day and the means of predicting the impact of the attacks and anticipating them by providing suitable mitigating strategies prior to their occurrence.

MAGNITUDE OF THE PROBLEM

The size of the problem is enormous and growing rapidly with the critical infrastructure and the economy as a whole becoming increasingly dependent on software and computer systems. The potential impact of a major successful attack on banking and commerce could run into the hundreds of billions of dollars, if not trillions of dollars. The recent credit freeze and trillion dollar bailout provides some indication of the cost of a loss of confidence in global financial markets due to cyber attacks. Attacks on other components of the critical infrastructure, such as telecommunications, electrical power and transportation, could also result in hundreds of billions of dollars of losses due to denial of service and secondary effects on other segments of the economy.

Until fairly recently, cyber security was viewed as secondary to physical security and was significantly underfunded. However several notable major incidents, such as the cyber attacks on the countries of Estonia and Georgia, have raised the priority of cyber security as it relates to national security. As this recognition of the importance of cyber security pervades government and, to a lesser extent, the private sector, it has become much more apparent that existing risk analysis and management tools are not up to the task of providing substantive information for deciding how to deploy the additional monies that are forthcoming for reducing the risks and losses that might result from significant incursions by cyber attackers.

One of the concerns is that there is not only insufficient understanding of the risks relating to exploits of the cyber vulnerabilities that exist in current computer systems and networks, but there is a lack of understanding of the structures and processes that these systems and networks support. This type of lack of knowledge has been painfully illustrated by the ongoing global financial crisis resulting from an underassessment of the risks related to obscure financial instruments and ignorance about how the various components of the economy are interrelated. In the cyber security space, there is a frightening misjudgment in the scope and intensity of potential cyber events, which could easily exceed the horrendous prospective impact of a pandemic, and a distressing lack of understanding of how systems and networks interact and the extent to which they are interdependent.

SOCIETAL CHALLENGES

Societal challenges related to cyber attacks and any resulting disastrous consequences will significantly affect the overall function and quality of life of the nation in a very detrimental manner if they are not addressed immediately. In fact the negative consequences of recent and current cyber attacks are already having a major impact. In order to address the CNN of increasing exposure to cyber attacks and their potential damage and destruction, there are several Societal Challenges that need to be overcome, including:

- General collaboration on cyber security between the public and private sectors, particularly as it relates to the critical infrastructure
- Sharing of information between, among and within the public and private sectors regarding threats, exploits, vulnerabilities and incidents
- The monetization of cyber risk to make for appropriate expenditures on security measures and determination of potential reallocation of cyber liabilities using insurance and other mechanisms
- The role of government in regulating cyber risk using such approaches as incentives and disincentives (such as through the purchasing power of the government), direct regulation, creation of a marketplace for trading risk, and so on

This document focuses on the challenges of modeling the risks related to cyber incidents and increasing our understanding of the dependencies and interdependencies of the various segments of our public and private critical infrastructure. This focus was based in the size and complexity of the challenges and the expected benefits if these challenges are surmounted.

Data Collection Issues

There is a dearth of accurate and applicable data relating to cyber attacks and the economic impact of those attacks, both in the public and private sectors. This is, in part, due to few in the private sector having the necessary clearances to be briefed on threats and incidents occurring in the public sector. Likewise, the private sector is unwilling to share such information within and among industries for reasons of reputation and competition, and with government due to fear of public disclosure (e.g., because of FOIA) and government interference and intervention, particularly with respect to law enforcement agencies.

There has been a degree of information sharing through the establishment of industry and government information sharing and analysis centers (ISACs), such as those for financial services, information technology and multi-state, and organizations such as InfraGard, which was established by the FBI to work with the private sector. However, such information dissemination is very limited in scope and coverage.

The challenge is to develop much more extensive and representational means of collecting and sharing data on threats, exploits, vulnerabilities and, in particular, actual incidents and responses to those incidents. A related challenge is to ensure that such information is protected so that the security and integrity of the critical infrastructure and the nation are not compromised as a result of disseminating data to untrusted entities and individuals.

Monitoring Issues

The collection of useful cyber security data is highly contingent upon the ability to monitor and measure the sources of such information. In addition to the practical issues of filtering huge amounts of data to arrive at actionable information, there are numerous privacy issues that are raised when far-reaching data collection methods, such as the Carnivore system, are proposed.

Methods need to developed that will allow for the anonymizing of data so as not to infringe on individuals' rights to privacy while still providing information that enables appropriate protective measures to be taken.

Risk Model Issues

It is clear from the continued under-spending in protective security measures that the quality of cyber risk models is inadequate for their purpose, which is to justify such spending. Also, because so many of the costs and benefits, which are related to cyber security, are intangible or difficult to determine, even well founded risk models provide unsatisfactory results.

A major effort is needed to evolve risk assessment and management models so that they encompass many more of the relevant factors surrounding cyber risk and then use improved data collection and analysis methods and tools to enhance the quality of the results.

Interaction of Critical National Need and Societal Challenges

The societal challenges – improvements needed in data collection, monitoring and risk model development, particularly as they relate to the public and private components of the critical infrastructure – can be better addressed through a commitment to focus attention and resources on developing the governance structure, tools and techniques, and procedures for implementing the results of the risk analyses.

While some progress has been made through the establishment of ISACs and the direct participation of government and private entities in attempting to address cyber risk and security issues, the sophistication and resolve of the attackers is advancing more quickly than our ability to defend against them.

It is clear from many recent presentations and publications that there is general agreement among security professionals that cyber attackers are evolving from recreational hackers seeking peer approval through to organized criminals looking for financial gain. There is increasing concern that we are entering a new phase, where terrorists and hostile nation states are using the Internet to launch cyber attacks. [Jakobsson 2008]

Defenders are seen to be lagging well behind attackers. This is in part due to it being so much more difficult to defend than to attack. After all, defenders must secure ***all*** attack points, whereas an attacker need find only ***one*** chink in the armor. Also, attackers, who are looking to gain money or other assets, enhance their reputation and/or acquire destructive capability, are usually considerably more highly motivated than defenders who, if successful, get to keep their jobs.

While attackers and defenders are clearly jockeying to attain the upper hand, there are additional external factors, which are also changing rapidly. These latter factors include technical advances, competitiveness, and legal and regulatory environments. Introducing new technologies creates unprecedented exposures. Competition with other organizations and with other intra-company projects limits the quantity of resources assigned to security activities. Government legislators and regulators and internal and external auditors are continually coming up with new requirements and restrictions in an attempt to mitigate the risks of activities that they believe result in insecure or unsafe consequences.

The purpose here is to examine the dynamics of the attack-defense interaction and come up with a model that will lead to optimal funding and prioritization of security projects based on the threats, exploits, vulnerabilities and incidents that various sectors and organizations are experiencing. The difficult and significant challenge, which is presented to the reader, is to develop real-world numbers for the model so that one can determine how much to invest in cyber security, which projects should receive priority, when to begin the project and how quickly it should be completed.[1]

The Attack-Defense Interaction

The threat-exploit-defense-response interaction has been extensively documented. The process usually follows a well-defined path. Someone will find some vulnerability or other, either as a result of an organized search, from a reliable source, or by chance. That person, or an associated group, being aware of the associated threat, will then work to determine whether an exploit can be developed to take advantage of the vulnerability and whether such an exploit can be implemented before systems can be patched or otherwise protected. Interestingly, black, white and gray hats all get involved in this endeavor, even though their motivations will vary considerably. Sometimes a critical vulnerability might be common knowledge, either by accident or on purpose (or "accidentally, on purpose"), as with the July 2008 DNS cache-poisoning situation. Whenever the threat of an impending attack evolves into a proven exploit or proof of

[1] This set of decisions is common to virtually all situations. For example, it is explicitly stated in [Allen, 2008] with regard to software assurance.

concept, there is a rush to come up with and implement an effective defense strategy, such as a patching program. However, it can take a fair amount of time to develop and test patches or fixes, so that there is a period of vulnerability during which successful attacks may be launched against undefended victims. In other cases, the defenders do not even know that the vulnerability exists, and an attacker can then operate with impunity until or unless the exploitation of the vulnerability is noticed or disclosed and work is initiated to defend against it.

There is clearly value in defending against an attack. That value might result from tangible and intangible costs stemming from the direct loss of funds and other resources, diminution of reputation, payment of regulatory fines, and so on. It will vary over time depending upon one's expectations of threats, exploits, vulnerabilities and the ability to withstand and respond to them. The value will vary with the type and effectiveness of a specific attack and the extent to which an entity might be exposed, even if they have some defenses in place.

For example, a major denial-of-service attack prevents online commerce to continue and the interchange of goods and services between an organization and its customers, partners, and service providers. It will likely have a significant financial impact over a specific period of time based upon an immediate loss of business and the long-term potential of lost customers. The costs of remediation are not particularly clear as many different approaches can be applied. For example, redundancy of networks and systems can increase resiliency, or a third-party service might be engaged to scrub transmissions "in the cloud." Mitigating possibilities tend to be longer term and to include infrastructure redesign, reduced dependency on the Internet, and so on. These require careful planning and significant expenditures over an extended period of time.

On the other hand, the impact of phishing or the surreptitious installation of malware, will have a significant impact on customers, and may therefore lead to loss of business and reputation, but the full impact may not be knowable unless identity theft is involved and the entity must advise customers and offer them credit checking services, and the like. The fixes for malware are often far more complex. Short term preventative measures might involve patching vulnerabilities in software, updating intrusion detection and prevention systems, and responding to the immediate impact of an attack depending on who is affected and to what extent. Longer term there will likely be the need for major redesigns of systems and processes.

While there is certainly a need to respond to a successful attack, it is far better to have in place the protective mechanisms that ***avoid*** having to deal with the adverse consequences of such an attack. If the form and nature of potential attacks are known in advance, then it is reasonable to expect potential victims to plan and implement appropriate protective or responsive measures. If one cannot predict a specific form of attack, but are reasonably sure that an attack of a general nature may be in the offing, then it is reasonable to establish some level of general defense or the type of defensive mechanism. Such a system can respond in some behavioral sense to an attack that is generically similar to some that may have been experienced in the past. As Nassim Nicholas Taleb points out [Taleb 2007], the way to prepare for major destructive incidents is not to try to anticipate what particular events might occur and when they might happen, but to prepare to respond to a range of possible, though unlikely, events.

There are a series of sequenced events related to the typical development of threats, exploits, vulnerabilities, protective measures, incidents and responses.

The attack and defense sequences can vary significantly with respect to timing. For example:

- A patch or other mitigating action may become available before or after an exploit is released and in the wild, with very different consequences
- A patch may have been available but not have been applied in many cases.
- The defenders may not be aware of a vulnerability until an incident occurs.
- A vulnerability may be known to the world at large but a viable exploit may be too difficult or costly to develop and implement for the "benefit" that could be derived from incidents.
- A threat may be known but there may not yet be a viable defense, so that it becomes a race between the exploit developers and mitigation groups.
- A vulnerability may be known by some and not shared with others, and those with the knowledge may focus their attacks on select targets so that the advent of the attacks are not generally known about, and no general defenses are developed and distributed.

As can be seen from the above examples, not every stage in the timeline is realized in all cases. Also, the relative timing can be different for each of the two tracks. For example, an exploit might be developed and released either before or after a patch has been made available, with very different consequences. As a result, the value of the defense mechanisms will vary from case to case and particularly with respect to the different timing of events. In part, this has to do with the perceived risk relating to attacks and the time and effort it takes to develop exploits and defenses. The enthusiasm for such development will vary based on the expectation of returns from exploitation and the losses due to inadequate protection. Consequently a series of different scenarios can be envisaged, each showing different cost and value profiles.

The model described in this paper clearly still requires polishing. There is a myriad of different situations, including those outlined here, that must be accounted for and injected into the model.

However, a much greater challenge is in:

- determining the potential for exploit development and successful use
- obtaining the values of security measures in the context of many different scenarios, and
- arriving at an optimal portfolio of measures and the times of implementation that will yield the highest overall net value.

MAPPING TO NATIONAL OBJECTIVES

It is clear from the documents mentioned in the CNN section above that the need to develop advanced risk models and to populate them with accurate and complete data maps well into national objectives, Congressional testimony, and NIST's core competencies.

Recent Presidential directives and Congressional approvals have focussed on the need for greater protection of the nation's cyberspace. In order to accomplish this there is an underlying need to develop meaningful risk models.

NIST has done significant research and published commendable guidance on information security. This work represents a critical foundation to the advancement of cyber risk models.

MEETING TIMELY NEEDS NOT MET BY OTHERS

Overview

TIP is directed to fund research areas that are not currently being adequately addressed by others. Given the scale and importance of the problem of securing our nation's critical cyber infrastructure, it is not surprising that others are aware of the issues and are looking to address the problem. However, it is apparent that all of these efforts combined fall far short of the needs of an increasingly hazardous cyber space.

TIP's role

In general, the public and private sectors have significant knowledge gaps and their tools for cyber risk evaluation and decision-making are severely lacking. While there may be point solutions to individual aspects of the problem, there is not a fully coordinated, well-funded effort to meet the challenges. This is in contrast to the efforts of highly motivated and well-funded attackers. Transformative impacts on the security of the critical cyber infrastructure are therefore expected to be limited. TIP is in a position to remedy this increasingly dangerous threat to the economic and social future of our nation.

CONCLUSION

Improved cyber risk models and a major enhancement of monitoring and data collection capabilities can lead to vastly improved risk evaluation and decision making, which in turn will greatly enhance the security and safety of the public and its public and private institutions.

The vision for this funding opportunity is:

- To develop advanced cyber risk models that will provide appropriate representation of the threats, exploits, vulnerabilities, incidents, and responses as they relate to the security and integrity of the nation's critical cyber infrastructure which is essential for the economic, social and cultural health of the nation, its economy, and its citizens.
- To develop advanced monitoring and data collection capabilities that will not infringe upon individuals' privacy rights but will provide the necessary inputs to the cyber risk models so that the results from running the models will be meaningful, actionable and will provide timely and effective protection against the growing threat environment.

References

[Allen 2008]
Allen, J.H, et al. Software Security Engineering: A Guide for Project Managers. Boston: Addison-Wesley, 2008.

[Jakobsson 2008]
Jakobsson, M. and Raman, Z. *Crimeware: Understanding New Attacks and Defenses*. Boston: Addison-Wesley, 2008.

[Taleb 2007]
Taleb, N.N. *The Black Swan: The Impact of the Highly Improbable*. New York, Random House, 2007.