CSC 893 Report: Science of Security

Magreth Mushi

August 17, 2013
1 Abstract

This report is basically a literature review of some papers and reports concerning science of security; and it is compiled to fulfill a requirement for completion of CSC 893–Supervised Doctoral Research course. This report gives an overview of current computer–related attack trend in the U.S, and discuss major efforts put by the research community to minimize the risks of this trend to systems and critical infrastructure. As the report shows, there have been increase in computer–related attack trends as indicated by several government agencies like Government Accountability Office (GAO), U.S. Computer Emergency Readiness Team (US-CERT), and Industrial Control System–Cyber Emergency Response Team (ICS–CERT). These trends calls for immediate response from the research and industry community in order to minimize (or possibly halt) the risk posed to our systems and critical infrastructure. As detailed below, there are several initiatives around the nation giving their best efforts to secure tomorrow’s systems and infrastructure, such efforts includes TRUST, DETERLab, and NSA SoS lablets among others. This report also summarize the eleven (11) cyber-security hard problem as identified by Department of Homeland Security (DHS), and it is expected that these problems and many others will form areas of focus for the science of security research; as it has already been realized by the NCSU SoS lablet.

2 Introduction

For the past 10 years, the world has experience dramatic increase in computer-related attacks causing damage ranging from web page modification to serious loss of critical infrastructure and life, United states is not an exception to this trend. According to the National Preparedness Report (NPR), the US-CERT reported an over 650-percent increase in the number of cyber incidents reported by federal agencies over a five-year period, from 5,503 in FY 2006, to 41,776 in FY 2010[2]. At the same time ICS-CERT reported that U.S. critical infrastructure companies saw a dramatic increase in the number of reported cyber-security incidents from 9 in 2009 to 198 in 2011[4].

In the 2012 U.S Government Accountability Office (GAO) report[3], the Director of Information Security Issues Gregory C. Wilshusen said

“*The number of cybersecurity incidents reported by federal agencies continues to rise, and recent incidents illustrate that these pose serious risk. Over the past 6 years, the number of incidents reported by federal agencies to the federal information security incident center has increased by nearly 680 percent.*”

Looking at the 2012 Cyber Attacks Timeline Master Index, cyber attacks are gaining popularity in main sectors especially government and banks.
An extract of recent (October 2012) cyber attacks statistics is shown below and more details and statistics can be found in the website [http://hackmageddon.com/2012-cyber-attacks-timeline-master-index/](http://hackmageddon.com/2012-cyber-attacks-timeline-master-index/). All these statistics call for proper significant effort in securing critical systems and infrastructures.

![Daily Trend of Attacks](image.png)

**Figure 1: Daily attacks trend for October 2012**

Current practice in dealing with security problems is based on engineering solutions such as Internet protocol security (IPSec) suites, Rivest-Shamir-Adleman (RSA) systems, and cryptography, to mention a few, which basically rely on infrastructure; and according to the statistics above, these solutions have not been successful in dealing with day to day sophistication of attacks. However, scientific solutions to security emerge where the available infrastructure does not suffice for security. In his paper entitled “On bugs and elephants: Mining for science of security”, Pavlovic[6] put it this way.

> “Conjoining cyber, physical, and social spaces by networks gives rise to new security problems that combine computational, physical, and social aspects. They cross the boundaries of the disciplines where security was studied before, and require new modeling tools, and a new, unified framework, with a solid scientific foundation, and empiric methods to deal with the natural and social processes on which security now depends. In many respects, a scientific foundation for the various approaches to security would have been beneficial even before; but now it became necessary.”

### 3 Current State of Research

Since the idea of Science of Security was envisaged, several researchers in the government, academia and industry have shown interest to push it forward.
There are many initiatives going on in different places, but in this section few major research initiatives will be discussed.

3.1 Team for Research in Ubiquitous Secure Technology (TRUST)

TRUST was established as a National Science Foundation Science and Technology Center to address technical, operational, legal, policy, and economic issues affecting security, privacy, and data protection as well as the challenges of developing, deploying, and using trustworthy systems. This team is comprised of researchers from Carnegie Mellon University, Cornell University, San Jose State University, Stanford University, University of California, Berkeley, and Vanderbilt University. In support of SoS initiative, TRUST researchers are developing a science base for security, with hopes to ultimately leverage these views in revising course content and embodying this theory in tools for system developers; and the expectation is that, this science can become a basis for an engineering discipline (http://www.truststc.org/).

3.2 cyber-DEFense Technology Experimental Research laboratory testbed (DETERlab)

This is the primary shared facility for scientists engaged in research, discovery, development, experimentation, and testing of new cyber-security technology. The lab is an open, remotely accessible, shared network research lab which allow researchers in the academia, government and industry to run different experiments on new security technologies. The lab is very crucial to foster SoS initiatives since researchers will be able to test different new technologies in order to come up with reliable and sustainable science of security (http://www.deter-project.org/deterlab-cyber-security-science-facility).

3.3 NSA Science of Security Lablets Research Initiative

As part of the effort to securing tomorrow’s systems, NSA started the initiative to fund SoS lablets which are expected to form the creation of a unified body of knowledge that can serve as the basis of a trust engineering discipline, curriculum, and rigorous design methodologies. The results of SoS Lablet research will be extensively documented and widely distributed through the SoS Virtual Organization. Currently, NSA is funding three lablets at North Carolina State University, University of Illinois at Urbana-Champaign, and Carnegie Mellon University (http://cps-vo.org/node/5253). This initiative has received substantial approval from several research groups such as Science of Security group, which is an online community (under the Cyber Physical Systems Virtual Organization (CPS-VO)) looking forward to advance cyber-security science. Under the same initiatives, NSA is funding several SoS projects such as Game and Abstraction: The Science of Cybersecurity; and GLASS (http://cps-vo.org/node/5991).
The first annual Science of Security (SoS) Community Meeting will be held on November 29-30, 2012 at the Gaylord National Hotel and Convention Center in National Harbor, Maryland to discuss foundations for security science and ways individual elements can contribute to a general framework that supports the principled design of trustworthy systems, which may include multi-disciplinary contributions from mathematics, computer science, behavioral science, economics, physics, as exemplars.

4 Lessons From Other sciences

The main goal of this section is to show how science of security can relate to other existing sciences; what lessons can we learn from them; and what we should expect as we develop science of security. As discussed in JASON report on Science of Cyber–security [5], the emphasis is in the sciences that resemble cyber–security, for instance with active agents, or those in which things change over time.

Economics: As a social science explicitly concerned with competing agents, it has a deep mathematical component, and used to make specific predictions. Many of the predictions are more like tendencies, and the record of success is mixed. However, economics plays an important role in that its considerations can shape the expectations of adversaries.

Meteorology: is the science that studies atmospheric phenomena, especially those that relate to weather, and it is based entirely on physics. By using science, this field has been successful in making weather forecast, but the forecasting has not been very accurate. For a long time this field is expecting to use models based on physics to make more accurate prediction of weather, though this have not been realized yet. In fact here, the issue of the limits of predictability are as important as the fundamental description of various physical processes. In addition, it is well known that there are extreme events that are very difficult to predict with accuracy but their existence requires that plans be put into place to deal with their consequences.

Medicine: This field is primarily organized with science-based tools. Based on these tools, some diseases have been eliminated completely, many are treated fairly successfully, but some diseases, like influenza, are only managed, killing tens of thousands each year despite all the efforts put to eliminate them. In addition, the basic science of how cells work, or how the body reacts to specific molecules, is still lacking. There are no fully quantitative measures of health, although there are quantitative test results. Nor can the health of individuals be compared; one cannot say I am 6 dB (or Pasteurs) healthier than you.
Agriculture: In agriculture we have crops that are grown and pests that attacks the crops. Over the years, scientific methods have been used to deal with this problem such as modifying the crops to be more resistant to pests, use of pesticides, or other biological controls. But, without continual attention (or even with it sometimes) the pests come back.

The above understanding of other fields of science, gives us an insight of how the science of security will develop and what it will look like, at least for the near future.

5 Science of Security Areas of Focus

Areas of focus discussed in this section are based on the DHS November 2009 roadmap for cybersecurity research where eleven(11) hard problems were identified to be of priority. This section is meant to be a brief summary of the problems, mainly focusing on the challenge to be addressed; current state of practice and research; and major research gaps identified in each of the eleven problems. For more details on these problem areas, the DHS report[1] should be consulted.

Scalable trustworthy systems: The problem being addressed here is how to build systems (or create systems and applications from components) which are trustworthy and scalable including system architectures and requisite development methodology. By trustworth it means the system which fulfill each of its specified requirements; and by scalability it means the systems ability to satisfy specified requirements as it expands in functionality, capacity, complexity and scope of trustworthiness. Composability of systems is critical to determining its trustworthy and scalability. By composability it generally means the ability to make a complete system and applications from components, subsystems, and other systems. We believe that the foundation of trustworthy scalable systems is established by the underlying hardware architecture, and therefore adequate hardware protection is necessary; and most hardware architectures does not have the required capabilities, for example fine-grain memory protection. However, hardware vendors have made significant investment in dealing with hardware problems, and this approach can be extended to software as well, but additional approaches may be necessary to ensure that the software problems are dealt with properly. In addition to this, more techniques are needed to address how software/hardware interaction affect the overall system trust level. Unfortunately, there is no existing significant investment during software development to ensure scalable trustworthiness, consequently, those interactions issues are generally not adequately addressed. Research is needed to es-
establish proper hardware protections necessary for system trustworthiness since it is unlikely that software alone will ever fully compensate for lack of hardware protections. DHS identified major research gaps in this area including, but not limited to understanding of composability and how it relates to security and trustworthiness, how to apply and combine specific solutions to specific security problems to produce trustworthy systems, and lack of methods for analyzing how even a small change to systems affect their trustworthiness.

**Enterprise-level metrics:** The problem being addressed here is how to define effective metrics for information security in the enterprise, these metrics are different from system- and component-level metrics. Generally speaking, we do not have well defined metrics for systems security in the enterprise to help us answer questions like “how secure is my organization?”, and therefore can not measure progress in security measures and compare between systems/organizations for security. Current approaches to measure security is ad hoc and metric selection mostly subjective, example evaluation of compliance with Sarbanes-Oxley. Most of measurements such as size and scope of botnets and number of infections are not related to fundamental characteristics of systems, but rather measurements about adversaries. There are several on going initiatives to improve metrics of the security domain, such as several government documents and efforts (e.g NIST SP800-55), Red teaming, heuristic approaches (e.g measure of password strength). In the research arena there are initiatives aimed at developing new approaches to identifying metrics, some of these initiatives are based on applying tools and techniques from other disciplines, while others are looking into new directions. More details on these initiatives can be found in the DHS report. Major research gaps identified includes lack of universally agreed-upon methodologies to address the fundamental question of how to quantify system security.

**System evaluation life cycle:** The problem in this area is lack of methods to systematically and cost-effectively evaluate products (security artifacts) in the security field in a timely manner including approaches for sufficient assurance. Lack of these methods resulted into challenges to measure progress toward handling security threats. According to DHS, security evaluation in the SDLC involves four major areas; developing explicit requirements and specifications for systems; understanding whether a product meets its specification with respect to a security policy that it is suppose to enforce; understanding whether a product can be successfully attacked or bypassed by testing it in each phase of its development life cycle, either in a testbed or through a mathematical model or simulation; and developing system evaluation processes whereby incremental changes can be tracked and rapidly reevaluated without having to repeat the entire process. Evaluation of secu-
curity artifacts is still ad hoc, though some methodologies have been discussed and proposed as detailed in the report, they are basically reemphasizing many of the tools and methods that have been unsuccessful in the past. Currently, evaluation of products is done in-house by vendors using different tests that are not known to the public. This approach is not successful either, since real evaluation is supposed to be done in customer environment by collecting periodic statistics. In terms of research, relatively little has been done on system evaluation methods, since researchers are concentrating on novel defenses and attacks. Major research gaps identified in this area includes lack of knowledge and understanding of the threat domain needed to develop realistic security requirements to be designed, implemented and evaluate; lack of understanding of which evaluation methods work for which threats; no peer review mechanism to review and validate evaluation mechanisms or proposals; and many others as detailed in the report.

Combating insider threats: The main challenge being addressed here is how to deal with threats posed by trusted untrustworthy individuals inside an organization. These individuals abuse granted privileges and they are the sources of many losses and harm in the organizations and the nation as a whole. There are different kinds of insiders who have different privileges to computing resources, but of particular concern here are trusted insiders who design, maintain, and manage critical information systems because they possess the skills and access necessary to engage in serious abuse or harm. Current practice in dealing with insider threats are based on procedures such as awareness training, identity management, and user authentication access control etc. However, these procedures are not consistently applied mainly due to their limited effectiveness. There are research initiatives going on currently, but some of them still rely on research on access controls dating back as many as 40 years. Refer DHS report for details about ongoing research work in this area. Thirteen major research gaps were identified in this area, prioritized ones being automated checking; response strategy and privacy protection for falsely accused insider abuses; and behavior-based access control.

Combating malware and botnets: The challenge being addressed here is how to deal with malware that attack and expose systems to the benefit of an adversary. Of a particular interest is “Bot” malware program that are installed on a system allowing an unauthorized user to remotely control the compromised machine for a variety of malicious purposes. Several machines compromised by a bot malware and so are under an adversary control form a botnet. These systems are source of many security challenges such as Distributed Denial of Service (DDoS) attack where an adversary can flood a network with traffic and therefore deny service to legitimate users. Several solutions have been devised, such as antiviruses, and Intru-
sion Detection Systems/Intrusion Prevention Systems (IDS/IPS), but they are becoming obsolete since malware are becoming more and more sophisticated. Currently, research does not address adequately this sophistication of malware such as malware code encryption and packing, and malware polymorphism. Therefore, in order to keep pace with adversaries and secure our systems we need more sophisticated solutions. Unfortunately, we are still counting on static signatures antiviruses, IDS/IPS, and system patching which are easily bypassed by sophisticated malware. However, there are research initiatives going on mainly centered around virtualization and honeynets; they have potential in short term malware detection, analysis, and response, but in the long run more sophistication is needed since bad guys are gaining understanding of these solutions and come up with ways to circumvent around them. Major research gaps identified in this area includes lack of understanding the agility and polymorphisim of malware, since current approaches (AV and IDS/IPS) are becoming less effective as malware become increasingly sophisticated. Another areas are lack of adequate taxonomy of malware and botnets; and attacker/defender asymmetry.

**Global-scale identity management:** The problem being addressed here concerns identifying and authenticating entities such as people, hardware devices, software applications etc when accessing critical infrastructure technology systems from anywhere. It should also be clear that the global nature of this problem raises many issues relating to international laws and regulations that must be considered. There are many potential threats in relation to identity management such as Identification and Authentication systems attacks, and because of lack of proper identity management, it is often extremely difficult to identify the misuser. Current approaches (discussed in the roadmap) to identity management lacks interoperability with other required services, not scalable, or limited in other ways. Major research gaps in this area includes lack of transparent, fine-grained, strongly typed control of identities, roles, attributes, and credentials; solutions based on authenticating only the would-be identities of users, not transactions, applications,or systems; lack of understanding of cultural and social implication of identity management and privacy among most citizens; difficult in maintaining consistency of reputations over time across identities; and past efforts to impose national standards for identity management have met considerable resistance.

**Survivability of time-critical systems:** The problem being addressed here is the capability of time-critical systems to fulfill their mission in a timely manner, in the presence of attacks, failures, or accidents. Time-critical system basically means a system that require fast response on non-human timescales to continue operation under relevant challenges. Examples of such systems are electric power grid, and regional transportation systems.
It is worth noting that, this sections pay more attention on systems which impaired survivability would have large-scale consequences, particularly in terms of the number of people affected. Current metrics for survivability of time-critical systems are focusing on the occurrence of natural random failures and therefore ignore occurrence of intentional attacks. However, due to criticality of these systems, the possibility of intentional attacks should not be ignored. There are existing research initiatives in this area such as DARPA’s OASIS, and several testbeds such as DETER and ORBIT, but still more effort is required to ensure survivability of these systems. Major research gaps identified in this area includes the absence of meaningful requirements for survivability. We need to understand the mission and risks of these systems; we also need survivability architectures, methods, and tools protection that does not involve human interaction; and lastly we need realistic testbeds to test survivability of the systems in the wide variety of adversaries and attacks.

**Situational understanding and attack attribution:** The problem being addressed here is how to understand different systems situations and identify which ones are attacks and which ones are not; and also be able to accurately tell who is the attacker. However, there are challenges in doing this, first, adversaries may be able to exfiltrate sensitive data over period of time, again without actually taking down the targeted system; second, some cyber attacks occur faster than human response time; and lastly, low and slow, and possibly stealthy attacks that break the attack sequences into a series of small steps spread over a long time period. Currently, situational understanding is done through IDS/IPS with much of the analysis done through manual perusal of log files despite existence of visualizations and analysis tools for large data. Major research gaps identified in this area includes needed improvement to IDS/IPS to deal with more sophisticated attacks; detection of attacks within encrypted payloads; sophisticated attribution mechanisms because it is still hard to do as it touches on privacy, legal, and forensic issues; more sophisticated tools since adversaries are becoming more intelligent and increasingly use new techniques.

**Provenance:** The problem being addressed here is understanding of sources and intermediate processors of shared computer-related resources in order to assess resource’s trustworthiness and reliability. With respect to data, provenance is concerned with the integrity and reliability of the information and meta-information rather than just the information content. It can also be used to track modification of information such as history through successive versions, transformation of content, and change of format. Currently provenance practice is very basic (such as change-tracking feature in documents, and version control systems) compared with what is needed to be able to rely on provenance collection and maintenance. There are several
research work going on related to information and resource provenance such as the myGrid system; ESSW; and other provenance-aware storage systems such as Lineage File System (LFS); and pedigree management such as Pedigree Management and Assessment Framework (PMAF). There are major research gaps identified by DHS in this area such as lack of taxonomy of provenance which means lacking appropriate definition and means for manipulating meaningful granularity of information provenance marking; and lack of confidential and anonymous provenance to protect sources of information.

Privacy-aware security: The problem being addressed here is how to overcome the challenges and provide approaches to technological means for safely controlling access to, and use of private information. Currently there are no formal uniform frameworks for enforcing protection requirements for private information while enabling sharing for legitimate purposes. On the technology side there has been progress in the privacy enhancing technologies such as access controls, encryption, and anonymous credential systems which authorize without necessarily revealing identity. There is a considerable amount of privacy-related work going on such as NSF trustworthy computing program, Microsoft research database privacy, and many others in U.S and outside U.S as detailed in the report. Major research gaps identified in this area includes lack of sound bases for selective disclosure and privacy-aware access; lack of techniques to share data sets while reducing the likelihood that arbitrary users can infer individual identification; and lack of enough research in policy and procedures to support privacy.

Usable security: The problem being addressed here is how to enforce security without compromising system usability. Security must be usable by persons ranging from non technical users to experts and system administrators, while at the same time systems be usable while maintaining security. Currently the problem of usable security is more challenging because security is poorly understood by non-experts; and technology developers are paying more attention to security in their products and systems rather than in usability; therefore, usability of systems tends to decrease as security tends to increase. Current research is focusing on usable authentication, example virtual passwords; user security projects such as CMU Cylab usable security and security laboratory (CUPS) and Stanford university work on web integrity. Major research gap in this area have been discussed in the report and all are based on lack of the science of usability as applied to security.
6 NCSU Science of Security Lablet

In March 2012, North Carolina State University, together with University of Illinois at Urbana-Champaign and Carnegie Mellon University received a grant from National Science Foundation (NSA) to stimulate the creation of a more scientific basis for the design and analysis of trusted systems. All three universities involved in this research are implementing Science of Security virtual lablets intended to create a unified body of knowledge and analytics methods and tools that can serve as the basis of a trust engineering discipline, curriculum, and rigorous design methodologies. The results of SoS lablet research are to be extensively documented and widely distributed through the use of a new, network-based collaboration environment. The intention is for that environment to be the primary resource for learning about ongoing work in security science, and to be a place to participate with others in advancing the state of the art (http://news.ncsu.edu/releases/wms-williams-nsa-lablet/).

The NCSU SoS lablet is a virtual lab involving faculty and students in the field of security. The lablets work is expected to draw on several fundamental areas of computing research and on the related analytics such as fault-tolerance computing, control theory, game theory and decision theory principles, formal methods, and from other areas of mathematics, statistics and engineering as well.

Currently identified areas of research focus for the NCSU lablet are mainly on scalability, analytics, and resiliency. As detailed by the principal researcher of the NCSU lablet, problem areas needing particular attention include:

Composability. When system components are combined, the aggregate must be evaluated as a whole. An aggregate analysis ideally would be based on and simplified by the prior independent analyses of the component, without the need for re-evaluation of the components.

Usability. Systems developers come from diverse technical backgrounds, so that design models and metaphors are graspable by a broad base of professionals. Additionally, approaches must be structured so that increments of effort by developers are rewarded by increments of value back to them in the form of enhanced productivity or accretion of measurable evidence in support of some assurance claim.

Analytics. Secure analytics focuses on making analytics processes and methods secure, privacy-preserving, and auditable to protect both the subject(s) of analytics and those engaged in analytics, while not restricting the ability to effect in-depth and mission-supporting analyses and a broad range of related activities. Security analytics, on the other hand, is about use of state-of-the-art analytics methods and approaches to assuring security of a wide range of software-based systems by analyzing both static and dynamic characteristics of the systems, large-scale data-streams, and human
behaviors.

**Human factors.** The analysis of potential security breaches requires sifting through enormous volumes of log data. A promising approach uses virtual representation of large complex datasets with respect to security, with an eye towards supporting an analyst. By focusing on how the low-level human virtual system "sees" basic properties of an image, and how anomalies are recognized, one can construct visualizations and analytics algorithms that are perceptually and psychologically sound and tuned for a particular analyst, and therefore allow an analyst to perform very rapid and accurate data exploration and discovery.

**Resiliency.** The complexity of software systems ensures that there will almost always be errors that can be exploited for penetration. Crucially needed are foundational principles for designing systems that anticipate penetration, contain it and limit its effects, even if the penetration is undetected. A science behind resilient secure systems may be approached by extending ideas of resiliency in the face of hardware and software errors; the key (but important) difference is that faults are security breaches. The key (but important) commonality is to approach the problem from the point of view of limiting the propagation of faults. Resiliency may be approached by extending techniques from a variety of mathematical modeling disciplines, including faulty-tolerant systems, control theory, game and decision theory, formal methods, and stochastic end-to-end system analysis.

### 7 Conclusion

There have been an upward trend of attacks as seen in most of the reports from public and private sectors, and the trend is showing significant increase on daily basis. Researchers are putting more efforts to secure systems and infrastructure by coming up with new solutions, forming research groups, and developing testbeds. Since the current state of using engineering solutions to attack security challenges have proved inefficient, researchers are looking forward to develop science of security in order to deal with this problem in a scientific way. In order to successful develop a science of security, we believe that other science disciplines have a role to play in helping us understand and shape the science of security as described in section 4 above.

In 2009, DHS prepared a roadmap identifying major problems in security and in which researchers should base in solving the current problems facing the nation; and therefore we expect that these areas will be some of the many areas of focus for science of security research. NSA has started to put more effort in developing this science by funding three universities to start science of security tablets where research about science of security will be done and shared. These tablets have their own areas of focus in research.
References


