Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security

Research and Development Committee

Research Agenda for the Banking and Finance Sector

September 2008

Overview

The Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC) supports research and development initiatives to protect the physical and electronic infrastructure of the Banking and Finance Sector, and to protect its customers by enhancing the Sector's resilience and integrity.[1] The FSSCC established the Research and Development Committee ("R&D Committee") in 2004 as a standing committee to identify priorities for research, promote development initiatives to significantly improve the resiliency of the Financial Services Sector, engage stakeholders (including academic institutions and government agencies), and coordinate these activities on behalf of the Banking and Finance Sector.[2] This research agenda is intended as a "living" document and has been updated to reflect advances in technology and the changing threat environment. The R&D Committee revised the priorities paper in early 2008 by consolidating nine research and development challenges into seven, re-evaluating the priority order, and seeking input from experts in academia, government, financial services and information technology communities.[3]

The R&D Committee believes that much of the financial sector's R&D needs are unique to the Banking and Finance Sector. However, the Committee believes other critical infrastructure sectors would also benefit from investments in R&D directed at the financial services industry. The FSSCC R&D Committee is working with the Treasury and Department of Homeland Security to identify funding mechanisms to address the priorities identified by the FSSCC. Treasury and Homeland Security are working with the financial sector, academia, and other government agencies to focus on cyber security concerns.

The information security industry has grown rapidly to mitigate risks by providing a myriad of products and services, including firewalls, access controls, anti-virus and anti-spyware programs, audits, standards (e.g., Common Criteria), and software patches. Financial institutions have responded by establishing governance models that include chief information security officers who manage information security risks by applying the appropriate mix of technology, processes, and expertise to safeguard data and information systems. Ongoing research and development is vital to supplement these advances, and to securing the economic well-being of the United States.

Discussions with academic institutions, however, reveal funding is very limited to conduct priority research. Financial institutions are battling new and constantly changing threats with old technologies and processes. Nevertheless, the Banking and Finance Sector is capable of

[1] The FSSCC is a private sector organization of more than 45 financial sector association and financial institutions representing all of the financial associations and major operators. The FSSCC was created in 2002 to work with US government on matters related to the National Response Framework (NRF). As per the NRF, the designated agency on the government side of this communication is the U.S. Department of Treasury (Treasury). Treasury is also responsible for coordinating the financial services sector's contribution to the NRF, or the "sector-specific plan." The NRF requires that all sectors include Research & Development efforts in their sector specific plans. To this end, the FSSCC created an R&D Committee in 2004. The mission of the FSSCC R&D Committee is to support research and development initiatives to ensure the protection and resilience of the physical and electronic infrastructure of Banking and Finance activities that are vital to the nation's economic well-being. More information on the FSSCC is available at http://www.fsscc.org.

[2] Appendix A provides a list of current R&D Committee members.

[3] The 2006 version of the Challenges is based on a paper entitled *Closing the Gap: A Research and Development Agenda to Improve the Resiliency of the Financial and Banking Sector*, by Dr. Jerrold M. Grochow of the MITRE Corporation and the Massachusetts Institute of Technology, with the support of officials from the U.S. Department of the Treasury, Office of Critical Infrastructure Protection and Compliance Policy. In updating the paper, the R&D Committee received very positive comments on the draft from experts from academia, government and the technology and financial services communities in terms of the paper's depth and breath. Reviewers suggested that the Committee narrow the list of priorities, list more specific R&D projects that have clear independent and dependent variables, focus on risk measurement and how R&D outcomes would result in risk reduction, and include more examples to explain why projects are important to the banking and finance sector.

coordinating research and programs to address its priorities. Coordination would drive efficiencies and help direct available research investments. Therefore, increasing and sustaining funding levels for R&D is critical. This might be possible by using a translational research model that partners researchers with stakeholders, has clear goals, a mechanism of technology transfer that includes intellectual property ownership resolution, and metrics to gauge the effectiveness of the R&D solutions.

The R&D Committee has identified four major gaps in financial sector R&D:

1. Greater transparency is needed to make key stakeholders (financial institutions, academia and government) aware of each other's R&D efforts and needs.

2. Better coordination is needed to facilitate activities among stakeholders in the US, as well as coordination with international organizations, subject to legal and regulatory restrictions and national security interests. Better coordination would drive efficiencies, help direct available research investments, and help achieve common goals more effectively.

3. Academics seek access to sensitive data of financial institutions. However, access to data is a major concern for financial institutions. In general, financial institutions are reluctant to provide data given the sensitivity of data and the potential for misuse.

4. Funding for R&D by the federal government and private sector is inadequate to meet the critical needs of the Banking and Finance Sector. Additional funding is necessary to meet current and emerging challenges.

In response to several of these gaps, in 2007 the FSSCC established a program to connect experts within the Banking and Finance Sector with researchers in academia: the Subject Matter Advisory Response Team (SMART) Program. The program assists research and development organizations working on critical infrastructure protection projects by providing subject matter expertise from financial institutions necessary to facilitate their research and development endeavors.

The committee has identified seven priority areas for R&D. Each of these seven challenges is important, but this should not be considered an all-inclusive list. The Committee has ranked these in order of importance recognizing that there are divergent views as to the appropriate order.

Executive Summary

The following are the top priorities of the Research and Development Committee of the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security.

Advancing the State of the Art in Designing and Testing Secure Applications. Software applications are complex and often insecure and thus introduce vulnerabilities. Historically, acquisition requirements have favored functionality over security which has led to a state of software development that often does not emphasize security. Financial institutions have begun demanding more secure application development. Because financial institutions often cannot be sure that their applications are secure, they must develop and implement costly and inefficient compensating controls. Financial institutions need a robust, effective, affordable, and timely security testing methodology, and practice to gain the confidence required to deploy application software into sometimes-hostile environments for purposes of practical and appropriate risk management. Research is needed to develop effective procurement standards, software developer education, and testing guidelines. In addition, research is needed to develop tools for producing, measuring and testing secure application software.

More Secure and Resilient Financial Transaction Systems. The Financial Services industry is dependent upon information technology infrastructure, much of which is owned and operated by third parties outside the financial services industry. This infrastructure is constantly under attack by hackers and identity thieves who seek to exploit vulnerabilities in networks, devices and applications for financial gain. Research is needed to better understand these threats, improve the security and resiliency of the financial transaction infrastructure, enhance the protections available to prevent the increasingly common downloads of malware by criminal elements that bypass existing defenses such as anti-virus and anti-spyware, and to develop metrics to evaluate the resiliency of the information technology infrastructure.

Enrollment and Identity Credential Management. The financial services industry depends on the ability of financial institutions to identify, authenticate and authorize customers before accessing information and conducting transactions through remote channels where direct human interaction is not possible. Inadequate controls can leave financial institutions and their customers vulnerable to attacks. Research is needed to study how to make the identity management process better and less susceptible to social engineering attacks.

Understanding the Human Insider Threat. Financial institutions must trust employees who have access to sensitive personal and financial information. Current strategies for identifying trustworthy candidates rely upon historical methods such as background and credit history checks as well as identity confirmation. Such methods often do not sufficiently identify insider-fraud perpetrators ahead of time and can be costly to maintain. Research is needed to develop holistic solutions to the insider-authentication problem, including the development of a data frame to predict the likelihood of insider attacks based on differing scenarios, or the development of continuous, unobtrusive monitoring to reduce the risks posed by insiders.

Data Centric Protection Strategies. To maintain trust and the integrity of data, financial institutions must protect sensitive data but also share it with third parties, such as merchants and processors. Increasingly, devices and networks are vulnerable to malicious code or data breaches. Research is needed to develop secure data file and document tagging technologies to classify information, and to enforce rules on access so that sensitive information is protected as intended by its original owner, regardless of where it traverses.

Better Measures of the Value of Security Investments. Traditionally, investment decisions surrounding security implementations have followed a “Return on Investment” (ROI) decision making process. The ROI model does not always fit well into the security space because it can be difficult to quantify hypothetical losses averted through increased security. The creation of cost-benefit models for security spending might be more appropriate because they would take into account intangible benefits such as increased customer confidence and decreased brand exposure. Research is needed to quantify the costs and benefits of security investments using models that are understood by financial risk managers.

Development of Practical Standards. The financial services industry relies on numerous standards and practices but has not succeeded in developing quantifiable measures for how these standards and practices reduce risk and enhance resiliency of critical infrastructures. Research is needed to measure the impact of standards and practices.

Table of Contents

Challenge 1: Advancing the State of the Art in Designing and Testing Secure Applications

The Situation

Information technology vulnerabilities emanate from two primary sources: (1) software flaws, and (2) inadequate patching and configuration practice—and therefore require two different threads of thinking about research. Across the entire financial services industry, the information protection and risk management community is generally not well equipped to accurately or completely define, specify, estimate, calculate, and measure how to design and test secure application software. Although continued mitigations against network vulnerabilities remain important, an increasing number of attacks are against software applications. However, financial institutions typically spend more to mitigate network vulnerabilities than software application vulnerabilities. Business requirements and risk assessments should drive resource allocations. Risks are driven by complex applications developed in-house and by partners, extension of powerful business applications to vulnerable customers, and increasingly organized criminal attacks (e.g., SQL injections to steal copies of data bases, cross-site scripting). To be effective, application security strategies must incorporate development standards and training, automated and manual code reviews, and penetration testing with and without design specifications or source code of the applications being tested. Some financial regulators have issued supervisory guidance on risks associated with web-based applications, urging banks to focus adequate attention on these risks and appropriate risk management practices.[4]

The testing of financial institution applications for security vulnerabilities stemming from software flaws is often inadequate, incomplete, or non-existent. Whether commercial off-the-shelf (COTS) applications are used stand-alone or integrated into custom-built applications, financial institutions cannot gain the confidence that is needed to deploy business-critical software without some proof of evaluation for obvious application security flaws (e.g., un-validated user input, buffer-overrun conditions). Without this confidence, financial institutions are forced to develop countermeasures and compensating controls to counter these unknown potential threats and undocumented features of the software. While functional testing by development teams and outside software developers is necessary, it is insufficient without explicit security assurance testing and corresponding evidence of testing results. Financial institutions need a robust, effective, affordable, and timely security testing methodology and practice to gain the confidence required to deploy application software into sometimes hostile environments for purposes of practical and appropriate risk management.

To minimize vulnerability, financial institutions have urged major software providers to improve the quality of their software development and testing processes for utility software, such as operating systems, but are only beginning to urge application software developers to do the same. Major software companies and outsourcing providers are responding by developing more secure code. However, while these are important and worthwhile efforts, the financial services industry (and other users of software) remains at risk from fundamental software development practices that produce vulnerable software in the very beginning stages of development. This vulnerable software has, in turn, resulted in substantial increase in application-level attacks. Risk managers in financial institutions continue to look for solutions.

[4] See *OCC Bulletin 2008-16 Guidance on Application Security* (http://www.occ.treas.gov/ftp/bulletin/2008-16.html).

The financial services industry needs research on how to specify, design, and implement secure software and measure its associated lifecycle costs and the benefits of the various information security technologies and processes. The industry would benefit from better understanding of how to develop, test, and measure secure application software.

Impact and consequences

The cost to the industry of maintaining, upgrading, and patching software has grown to the point that it is impeding the ability of the industry to add needed new functionality. In the short run, software flaws are fixed via patches, but in the long run, better coding practices will reduce the number of flaws. However, the inability to keep abreast with the growing vulnerabilities of application software and to keep up with remediating these vulnerabilities is leading to an increase in the likelihood of catastrophic failures, unacceptable service disruptions, and highly publicized losses due to fraud, errors, and misuse of data.

Cyber security breaches are a risk in today's interconnected world with its ever expanding flow of data. The financial and business impact of unauthorized intrusions can be damaging. Financial institutions experience a continuing onslaught of malware, Trojans, worms, viruses, spyware, and the resulting fraud and loss of privacy, in addition to the fear of malicious cyber attacks that can disrupt or preclude access to a web service. Every day, an organization's information system is at risk of attack from insecure software applications. And while many of these attacks are little more than harmless pranks, other more insidious assaults can wreak significant economic and operational damage.

Desired Functionality

A clear and accepted methodology to design, implement, measure and test application software to assure that application software is secure from attack and hack. This would include the ability to:

1 Provide software security testing and certification methodologies and standards that are relevant and immediately useful to the financial industry. The results of this research should:
   - 1.1 Evaluate the commercial effectiveness of existing software security certification and testing programs (e.g., Common Criteria).
   - 1.2 Explore more effective ways to design, test, and measure software during its development to minimize errors, reduce software vulnerabilities, and provide guidance to developers on how to remediate discovered vulnerabilities.
   - 1.3 Work with the information technology industry and others to apply concepts from the Trusted Computing Initiative from the Trusted Computing Group (https://www.trustedcomputinggroup.org/home) to build and protect a core "Trusted Financial Service Processing Layer" upon which our applications can safely be built, and upon which the financial industry can rely on to provide a continuous level of financial services at some minimum essential level in the face of massive failure, attack, or successful fraud.
   - 1.4 Develop a standardized methodology for designing, implementing, testing, and measuring application software to be less vulnerable to attack. Such a methodology should include the ability to accurately measure and forecast the security of application code.
   - 1.5 Educate software developers on secure development techniques because better coding practices are needed to reduce the number of software flaws in the long term.

Potential Research Projects

Research to support this challenge is needed to:

- Develop cost effective design principles for secure application designs that can reliably rank and distinguish the relative levels of security of different software products.
- Develop tools for developing, measuring, and testing secure software to a higher degree of accuracy.
- Develop strategies and tools for making/transforming existing or legacy software applications to a more secure state by adding layers of protection.
- Anticipate and predict future software attacks, exploits that could detect known vulnerabilities, and variance to known vulnerabilities via simulation models in order to better anticipate threats. Simulation models include tabletop games and computer modeling.
- Allocate more equitable liability for software vulnerabilities to create better incentives for responsible parties to implement appropriate controls including testing, user training, and standard configuration.
- Develop effective procurement standards, software developer education, and testing guidelines.
- Design diversity and resiliency in software to make it more robust and resistant to attack.
- Understand the interaction of software and their vulnerabilities.
- Develop a standard for secure software development (e.g., review and revamp of ISO/IEC 12207 and linkage to ISO 17799) that integrates security requirements and principles in each phase of the software development life cycle.
- Develop a standard for software procurement (to mitigate adhesion contracts) that clearly establishes the security requirements for custom-developed software, COTS, and embedded (including network devices) software.
- Develop tools (e.g., IDE plug-in, etc.) to automatically scan and enforce security principles based on a centralized policy server as the software is being coded. This tool should also provide and enforce the use of security API (similar to OWASP ESAPI) for common validation routines.
- Develop a methodology and tools to evaluate software security within short timeframes, and in an economically efficient manner by considering real-life deployment/usage scenarios. Also develop accompanying star ratings (1 through 5) that are easily understandable by a purchaser.
- Make the Common Criteria commercially viable for research efforts in developing and validating already-developed evaluation criteria that is meaningful for the Banking and Finance Sector.
- Develop a “self-healing" framework and utilities that would automatically adapt to defend against the potential exploits of code vulnerabilities or security weaknesses of underlying services.
- Research the application of Six Sigma, CMM, and other quality-enhancing practices to software development.

Challenge 2: More Secure and Resilient Financial Transaction Systems

The Situation

The Banking and Finance Sector relies on an information technology infrastructure, including computing hardware, software, and telecommunications networks. Some of this infrastructure is owned and operated by financial institutions and some is provided by third party service providers in the US and around the globe. This infrastructure is probed and attacked by a variety of adversaries, including criminal elements and nation-states. These adversaries exploit vulnerabilities in people, processes, and technologies and perpetrate attacks for financial gain, to steal proprietary information, or to undermine consumer confidence in the financial services industry and US economy. Threats from adversaries are increasing, raising concerns over the integrity of devices, networks, and applications. The infrastructure is also vulnerable to natural disasters, pandemics, and other outages. Although the financial services, information technology, and telecommunications industries have responded to these challenges with initiatives to address security, integrity, and resiliency, significant risks remain in terms of security breaches, fraud (including identity theft), service disruptions, and data integrity.

The key to maintaining the integrity of the financial services industry is more secure and resilient financial transaction systems. It must resist interception and tampering over an increasingly vulnerable environment in which the trustworthiness of networks and devices is uncertain. One facet is ensuring that networks and devices are “clean” when restoring service after an interruption. Reconstitution of data after an attack requires an additional step: decontamination, which is the process of distinguishing a clean system state (unaffected by the intruder) from the portions of infected system state, and eliminating the causes of those differences. Because system users would prefer as little good data as possible be discarded, this problem is quite difficult. Also of primary importance is the retention and reconstruction of transaction history while simultaneously being fully engaged in business continuity operations and executing a recovery plan. Other sectors have expressed concerns about extending their continuity plans to include vital information found on remote workstations. The possibility of this dislocation of normal corporate boundaries could be strained when relying on a distributed computing model.

Remote access is necessary for enhancing productivity and as a tool for business continuity planning purposes. For example, financial institutions have developed business continuity plans to ensure employees can access networks if core facilities are not available. The most significant outcome of the FSSCC/FBIIC pandemic planning exercise in 2007 was the heavy reliance by multiple industries on the Internet as the backup communication channel to support business continuity. Use of company-owned devices in conjunction with personally-owned devices introduces serious security challenges. Issues arise regarding the downloading, printing, and storage of sensitive customer and company information; potential data loss as a result of theft of mobile and personally-owned devices; introduction of malicious code into the corporate network from the personally-owned devices or company devices that are not managed as strongly as desktop systems; remote support issues; compliance with regulatory requirements; and the ability to reroute phone calls and faxes, etc.

The challenge is in finding the right mix of hardware and software that gives employees the ability to conduct their work off-site while still adhering to all of the controls and monitoring afforded by corporate facilities, and without introducing the company and the data to excessive

incremental risk. It should also provide employees the ability to seamlessly move from one location to another while retaining their "session state" and desktop customization.

Impact and Consequences

The impact and consequences of attacks or operational failures on the transactions could cause serious service disruptions to customers resulting in losses, liquidity problems, and lack of market and consumer confidence due to concerns about data integrity. This could lead to severe market disruptions, economic disruptions, and public panic. Also, credible threats of service disruptions could lead to situations where adversaries could blackmail, extort, or coerce financial institutions in ways that could be detrimental to individual firms and the overall economy.

Desired Functionality

2a More secure and resilient financial transaction systems that enable transacting parties (e.g., between financial institutions, and between institutions and customers) to securely exchange financial information and commands (e.g. account information, payment instructions, etc.) with confidence even though the message protocol traverses untrustworthy communications networks and computing nodes. The protocols should:
- 2a.1 Reliably and unambiguously identify the originator of a message.
- 2a.2 Ensure only the intended recipient(s) is able to receive and understand the message
- 2a.3 Protect message content against tampering and identify any attempt to modify message content.
- 2a.4 Promote interoperability among financial institutions by use of existing or enhanced industry standards to encode and encrypt message content.
- 2a.5 Support use as a service among diverse financial service applications.
- 2a.6 Scale to support very high transaction rates, on a scale exceeding hundreds of millions of transactions per day, operating globally, 24x7.
- 2a.7 Motivate migration to more secure protocols and tamper proof records.
- 2a.8 Anticipate threat evolution and evolve ahead of them (e.g., flexible responses to chameleon automated attacks introduced by organized crime, technology that would provide a tamper-proof record of document access for auditing /monitoring multiple secure email systems).

2b The architecture of a more secure, more resilient, and more flexible financial transaction system infrastructure should:
- 2b.1 Address secure data replication in large quantities across great distances.
- 2b.2 Shift load from congested or compromised facilities to other available facilities with care not to create a data replication issue.
- 2b.3 Provision public networks or endpoints (i.e. banks) to dedicate secure bandwidth to financial services transactions.
- 2b.4 Support the creation of shared capacity able to absorb demand displaced by a wide variety of incidents (e.g., pandemic requiring massive work-from-home scenario), and engineer a protected service that would give priority access when there is congestion.
- 2b.5 Extend connectivity to areas in which basic services are unavailable using local power generation, rapid deployment of wireless communications, mobile kiosks, or other innovative techniques.
- 2b.6 Leverage the economic efficiency provided by public communications networks and commercial off-the-shelf (COTS) computer systems.

2b.7 Provide sufficient redundancy and flexibility to continue operation without significant degradation of services while under cyber and physical attack, or during natural disasters.

2b.8 Reduce dependencies on the critical infrastructure provided by other industries.

2c Develop more resiliency for the telecommunications and processing capabilities required by the financial industry, and define alternative communications channels that are less reliant on any particular Internet connectivity channel:

2c.1 Prioritize in favor of commercial and critical telecommunication traffic from casual and critical use to improve quality of service and maintain resiliency.

2c.2 Increase resiliency of connectivity between continents and countries (e.g., Internet cable cuts).

2c.3 Provide incentives to business partners to meet the necessary security and resiliency needs of the Banking and Finance Sector.

2c.4 ROI for more secure protocols.

2c.5 Provide secure hardware and software that can connect securely to the customer without relying on their ability to configure devices.

2c.6 Apply top level domain or high assurance certificates that can be used for priority handling.

2c.7 Improve rapidly deployable emergency communications.

2c.8 Prioritization by addresses versus content.

2d Enhance the protections available to prevent the increasingly common downloads of malware created by criminal elements (i.e., "crimeware") that bypass existing PC defenses such as anti-virus and anti-spyware. The criminal element uses crimeware, among other things, to capture consumer information (e.g., via the "Silent Banker" malware) or use the end user's PC as a node in a botnet.

2e Improve the level of defenses available to prevent malicious downloads of software.

2f Minimize the amount of proactive interaction required by users, particularly consumer-type users utilizing home-based PCs, to protect their computers against crimeware.

2g Develop a platform-independent transaction system that maintains adequate integrity even when an endpoint is compromised.

2g.1 Ensure that transactions are delivered to the bank exactly as entered by the customer, without change, addition, or deletion.

2g.2 Maintain the customers' ability to transact business using any platform other than that of their choice.

2g.3 The transactional system should be independent of any specific platform.

Potential Research Projects

Research to support this challenge is needed to:

- Better understand the changing threats and develop strategies to adapt to them.
- Design better protocols that can operate with un-trusted devices and vulnerabilities in software and hardware.
- Develop metrics to evaluate the resiliency of an enterprise in a way that permits continuous improvement.
- Reduce the cost and improve the usability of industry standard cryptographic solutions.
- Explore the application of advanced encryption such as quantum cryptography and steganographic[5] techniques to the secure and resilient transaction system problem.

[5] Steganography is the art and science of writing hidden messages in such a way that no one apart from the sender and intended recipient even realizes there *is* a hidden message. By contrast, cryptography obscures the meaning of a message, but it does not conceal the fact that there *is* a message. (Wikipedia)

- Improve the underlying trust models by developing novel processes and technologies.
- Develop tools, in the form of simulation models, for the system and network infrastructure as well as for information and transaction processing. Such models will enable financial institutions to evaluate the impact of incidents and develop contingency and response plans if attacks, natural disasters, or other events were to disrupt the flow of information and transactions.
- Use integrated multi-channel transaction protocols to enhance diversity and resiliency.
- Identify feasible alternatives to the current financial transaction systems.
- Analyze how a top level domain (TLD) for the banking and finance sector could enhance resiliency and mutual authentication. For example, the Internet Corporation for Assigned Names and Numbers (ICANN) offers a means whereby key sectors can establish criteria for a TLD. Research is needed to understand how such means would address the security concerns of the financial services industry, what ground rules would need to be established, and what the potential benefits might be in terms of enhanced security and reduced fraud. This includes whether a sector specific TLD would be a marketing differentiator and thus worth the investment beyond the security and fraud savings. Further research is necessary to understand the following: (a) assurance levels of parties; (b) how to treat financial institutions and service providers on a global basis; (c) consumer education; (d) transition costs; (e) impact to brand and marketing; and (f) impact on reducing denial of service attacks on individual financial institutions and the entire sector.
- Analyze how data tagging and application security could enable computing in environments where the trustworthiness of networks and devices is questionable (in conjunction with challenge #5 on “data centric protection strategies”).
- Identify mechanisms for more effective automatic network load shifting.
- Research approaches for a system to adapt around disruptions, including shifting operation to a minimum essential mode that allows the continuation of critical services in the face of reduced capacity, communications, and resources.
- Create new decontamination approaches for discarding as little good data as possible, and for removing active and potential infections, on a system that cannot be shut down for decontamination.
- Research alternative organizational and operational modes that can allow the operation of loosely coupled, decentralized locations with minimum connectivity and communications.
- Improve communication protocols that could free additional bandwidth or allow bandwidth switching during a crisis.
- Develop strategies to overcome vulnerabilities of transcontinental cables and route diversity constraints.
- Develop strategies to identify, segregate and route traffic based on bandwidth requirements of applications.
- Research capabilities to use low bandwidth mobile devices as alternatives.
- Understand minimum, essential financial operational procedures and processes that are capable of operating with minimal survivable communications and processing capacity.
- Understand how desktop virtualization, suspend/resume processing, message compression algorithms, transmission optimization for performance enhancement and capacity optimization, validation of software components, both local and remote, data integrity, etc. can enhance security and resiliency.
- Research self-executing (i.e., require little to no interaction with PC users to operate), commercially reasonable mechanisms that improve on currently available PC defenses to prevent the download of crimeware.

Challenge 3: Enrollment and Identity Credential Management

The Situation

A secure financial infrastructure requires reliable and unambiguous identification of all parties involved in a transaction and non-repudiation of authorized transactions. Current technologies offer "spot" solutions that secure an aspect of identity management; however, many vulnerabilities remain. Although strong authentication credentialing technology exists, the initial identification of and linkage to an individual's identity to an authentication credential and the need to replace lost or stolen credentials remain weak links. Financial institutions rely on the individual's possession of knowledge that can be stolen, or by biometrics that can be spoofed, and may not scale up to millions of individuals without sacrificing performance. Moreover, the lack of strong mutual authentication allows for, among other things, the ability for the launching of successful man-in-the-middle attacks.[6] Financial institutions typically rely on "spot" authentication in which the financial institution authenticates customers before a transaction. Research is needed to develop more continuous authentication and credentialing.

Impact and Consequences

There are widely varying estimates of losses due to identity-based financial fraud. A public perception of widespread risk of identity-based financial fraud has led to declining consumer confidence in online financial services, further resulting in a loss of potential customer adoption. This perception could also increase the risk of new laws, regulations, and supervisory requirements that yield sub-optimal solutions and new compliance costs without tangible results in terms of reduced losses and higher customer satisfaction. The absence of agreed-upon architectural solutions, and strong, affordable, well-accepted, easy to use identification and mutual authentication means that vulnerabilities will persist, especially as criminal elements perpetrate financial fraud through attacks on identity management systems.

Desired Functionality

3 Define the architecture of an 'identity layer' suitable for incorporation in all financial services protocols and communications. This identity layer should:
- 3.1 Provide secure and reliable identification of all parties.
- 3.2 Provide strong mutual authentication of all parties using existing authentication methods such as biometrics or new methods to be developed that minimize customer inconvenience, are well-accepted, and minimize personal intrusion and interaction.
- 3.3 Provide a reasonable level of non-repudiation of financial transactions undertaken by authenticated participants.
- 3.4 Preserve identity across all interfaces and protocols.
- 3.5 Develop a capability for continuous authentication throughout the entire transaction interaction.
- 3.6 Include procedures that verify an applicant's right to enroll under a particular identity.

[6] In cryptography, the man-in-the-middle, or bucket-brigade, attack (often abbreviated MITM) is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all messages going between the two victims and inject new ones, which is straightforward in many circumstances (for example, the owner of a public wireless access point can, in principle, conduct MITM attacks on the users). A man-in-the-middle attack can only be successful when the attacker can impersonate each endpoint to the satisfaction of the other. Most cryptographic protocols include some form of endpoint authentication specifically to prevent MITM attacks. For example, SSL authenticates the server using a mutually trusted certification authority. (Wikipedia)

3.7 Support new approaches to strengthening enrollment procedures, including new knowledge-based identification approaches, and investigating and developing new, stronger approaches to identity verification, including the use of biometrics.
3.8 Provide flexibility to incorporate improved methods for an individual or enterprise who has verified identity with a financial institution to use that identity in dealings with other institutions – financial or non-financial – including 'trust models' that address liability issues.
3.9 Improve the scalability of any solution and issues related to preserving end-to-end identity management in systems comprising many subsystems.

Potential Research Projects

Research to support this challenge is needed to:

- Integrate national security-based identification standards (e.g., REAL ID) into mature and robust access control technology.
- Protect the privacy and confidentiality of identity data and identity management artifacts, such as enrollment questions, throughout the identity management domain.
- Incorporate appropriate privacy and confidentiality protections into the identity management process.
- Understand the social and psychological issues that affect whether a solution is acceptable to the public, including the factors that make a security procedure "feel" intrusive versus reassuring to the public, and methods to present security enhancements in a way that enhances public confidence without causing resentment.
- Document risks inherent in advances in identity management and methods of mitigating and managing these risks.
- Quantify current vulnerabilities and losses and the effect of solutions in eliminating or reducing these risks.
- Develop a framework with more precise terminology to better understand the nature of Identity Management and the distinctions between identification, verification, authentication, and authorization, including a more fine-grained approach to establishing and managing identity claims and authorizations.
- Understand how to implement cost effective and customer-accepted authentication and identification technologies, such as continuous physiological and biometric indicators.
- Test the effectiveness of technologies that protect consumers against social engineering attacks such as phishing, vishing, or smsing.
- Apply novel methods of zero-knowledge challenges and continuous authentication monitoring.
- Apply advanced behavioral monitoring, including anomaly pattern detection integrated with physiological monitoring.
- Research methods to integrate effective methods of multi-channel authentication.
- Apply metrics that evaluate and compare various authentication technologies and identity management schemes.

Challenge 4: Understanding the Human Insider Threat

The Situation

Financial institutions grant access to confidential information to authorized parties. To establish and maintain trust in this access granting process, financial institutions use a variety of tools and controls to identify, verify, authenticate, and authorize trustworthy individuals and contractors. Measures include background checks, credit history checks, and other historical data checks. The insider threat problem is a particularly difficult because of the interplay between technical, legal, managerial, and ethical issues. Financial institutions recognize that current measures provide only a "coarse-grained" screening for obvious human threats to begin the access granting process; individuals are granted access to networks, systems, databases, applications, and ultimately customer and business information based on their job or role in the institution. The process is enforced via a highly complex set of overlapping operational and technical controls, which requires that a large percentage of each financial institution's total information protection budget is dedicated to access management, control, and reporting.

Despite the pre-employment/engagement checking processes, and the layering of costly operational and technical controls, financial institutions continue to experience damage from the unprofessional, malicious, or criminal activities committed by individuals with authorized access, sometimes in coordination with external individuals, criminal organizations, or terrorists. Current approaches suggest adding additional layers – technological or procedural – of surveillance processes to detect, identify, and help stop the unwanted activities of authorized individuals. However, such approaches, while they may reduce undesirable activities, add substantial operating costs to an already costly access management approach.

Financial institutions currently have tools that could be useful in determining improper behavior of insiders. Many of these tools are based on physical and logical access but are typically not integrated. Improvements in security information management are needed to detect and prevent improper insider behavior. A critical component of improving security information management is ensuring that appropriate controls are in place to address privacy and other human resource protections.

Impact and consequences

Events where authorized access has been exploited within individual financial institutions can damage the reputation of the institution and, taken as a group, can degrade customer confidence in the entire financial infrastructure. Continued problems could cause a downward confidence spiral in which internal attacks could become increasingly effective at reducing customer confidence. The human threats problem appears to be growing despite increased funding and oversight within financial institutions and from financial regulators. While most attacks by insiders are for financial gain, there is concern of a potential terrorist threat to the national financial infrastructure from coordinated insider attacks by individuals with access to multiple institutions.

Desired Functionality

4 Bring together a research team with wide ranging skill sets to accurately and thoroughly identify, measure, and document personal/behavioral, operating process/procedural, technical/technological policies and the financial aspects of this problem. The research should:

- 4.1 Review the scope of operating issues faced by individual financial institutions, including defining the problem in terms of a coordinated attack on the National Financial Infrastructure.
- 4.2 Provide a framework for describing and understanding the totality of the human threat, and produce or advance a common language for describing the problem in its various forms.
- 4.3 Provide conclusions about the nature, scope, size, extent, and direction of movement so that financial institutions' decision-makers can understand their place in the problem on both an individual and national basis.
- 4.4 Describe a set of workable tactical solutions that could be implemented individually by financial institutions to decrease the risk of threats from an authorized user.
- 4.5 Investigate technologies such as behavioral modeling and social network analysis, as well as advanced methodologies for sharing the results.
- 4.6 Track and provide auditable records of what subsequent actions were taken and by whom.
- 4.7 Investigate application of sensors for monitoring and surveillance of, for example, critical financial and banking center operations. Sensors can control doors, tag computers, and operate cameras and other monitoring devices to provide security information remotely.

Potential Research Projects

Research to support this challenge is needed to:

- Develop a holistic approach for authorizing insiders at all phases of the authorization lifecycle, given that threats can change faster than layers of control and surveillance complexity can be added to respond.
- Develop data to frame the likelihood of the insider threat.
- Identify tactical solutions for identifying and responding to the human threat that automatically terminates access rights, including (but not limited to) behavior and physiological modeling; better means of continuous psychological and background testing that is more predictive; application of social network analysis; effective sensor techniques for monitoring behavior; and monitoring technologies to detect when a trusted insider is doing something that is deemed a threat to the institution.
- Balance privacy rights with identity mechanisms.
- Measure the effectiveness of new approaches to reducing incidents and the likelihood of human insider fraud.
- Improve the automated aspects of audit log review and activities.
- Develop an incentive structure to help manage the threat.
- Measure the effectiveness of new approaches to reducing the number of incidents and the likelihood of insider fraud. Thereafter, use the usual audit rule; the set up changes should require more than one person.

Challenge 5: Data Centric Protection Strategies

The Situation

Even if the financial services industry builds a more secure and resilient infrastructure to protect financial transactions (as addressed in Challenge #2), it is still vulnerable to having sensitive information stolen by criminal elements and other adversaries who attack less secure systems outside the financial services industries' secure transaction infrastructure with whom we share portions of this information (e.g. merchants and third party vendors). Preserving the integrity of each transaction involves identification, authentication, and authorization of each transaction to ensure that counterparties are not criminals or money-launderers, and that sensitive information is protected and its loss, copying, or tampering is detected. While financial institutions have tools that protect data while it resides in a certain environment, these tools are not effective when the data is taken out of that controlled environment (e.g., when a user cuts and pastes in another form). A key challenge is focusing on metadata to understand when data is accessed, updated, or copied.

Impact and consequences

The result of these trends, if not checked, would be for customers to lose confidence in the banking system, which has become increasingly dependent on these computer networks and systems. If this situation is not addressed, the banking and financial services industry will face critical brand erosion and significant loss of customers, as well as financial losses realized by both their customers and themselves. Increasing incidents of privacy breaches will lead to a loss of consumer confidence in online financial services. Theft of sensitive data can also provide the information needed to launch more successful denial-of-service attacks.

Desired Functionality

5 Define the architecture of a financial information system that provides a comprehensive privacy and security model. Such a system should:
- 5.1 Provide strong access, authentication, and entitlement controls.
- 5.2 Provide a means or mechanism (e.g., "tagged" data elements or metadata stored in a data dictionary) that enables a rules-based model where data protection, based on established control requirements, is automatically enforced by the infrastructure to prevent unauthorized access or modification while preserving the principles of Discretionary Access Controls.
- 5.3 Track information across its entire life-cycle, requiring institutions to:
  - 5.3.1 Track and provide auditable records of who accessed what information and when.
  - 5.3.2 Track and provide auditable records of how the information was used and what actions were taken.
  - 5.3.3 Track and provide auditable records indicating whether the information or derivatives of this information were shared, with whom it was shared, when, and where.
  - 5.3.4 Track and provide auditable records of what subsequent actions were taken and by whom.
  - 5.3.5 Determine how to detect when data has been tampered with.
- 5.4 Explore how to develop data dictionaries in which transactions that identify data are classified and encrypted.

5.5 Provide alerts and the ability to set and enforce unified data-centric policies to prohibit and constrain attempts at using or sharing information in ways that violate policies established for the data.
5.6 Provide warning indicators when usage and access is not normal.
5.7 Accommodate remote access of enterprise information and processing resources.
5.8 Accommodate personally-owned devices used by employees and contractors.
5.9 Address the security implications of Web 2.0.
5.10 Increase scale to economically support hundreds of billions of records.
5.11 Interoperate with a system that makes information securely accessible across untrustworthy communications networks and computing nodes (see Challenge #1).
5.12 Provide advanced analytics and simulation tools for accurate fraud and attack forecasting.

Potential Research Projects

Research to support this challenge is needed to:

- Develop secure data file and document tagging technologies that provide audit trails of access.
- Develop effective digital data tagging technologies that provide for enforcement of access/authentication and authorization rules across any application or access point used to access the information.
- Develop standards and best practices to classify and tag data.
- Develop enforcement requirements for compliance with data classification practices.
- Automate processes where multiple parties provide data and control decision points.
- Preserve accountability through data ownership and control.
- Investigate feasibility of “rights management” technology as a means of enforcing policies governing access to information and how it is used, as well as providing alerts when violations are attempted or detected.
- Allocate more equitable liability for software vulnerabilities to create better incentives for responsible parties to implement appropriate controls including testing, user training, and standard configuration.

Challenge 6: Better Measures of the Value of Security Investments

The Situation

The financial industry seeks research on the life-cycle costs of security technologies that support critical infrastructure protection, and the creation of cost-benefit models that can be adopted within institutions and across the industry. One of the key issues in the adoption of improved protective technologies and processes is the ability of the purchasing organizations to fully understand the costs and benefits of security technologies. Information protection organizations, as part of their regular business, can effectively evaluate specific cost elements for various protective programs in terms of operating cost, contracting costs, and the cost of purchasing the needed technology for an organization. However, information protection organizations typically do not have good estimates of the total lifecycle costs of the protective programs on the business lines that are asked to implement, own, and manage these protective programs over the long-term. Across the entire Banking and Finance Sector, the information protection and risk management community is generally not well-equipped to accurately or completely define, estimate, calculate, measure, or communicate the benefits that result from protective programs. Further exacerbating this issue is that the "benefits" of security are often intangible and often relate more to loss avoidance, making traditional return-on-investment (ROI) calculations difficult. There needs to be a stronger correlation between security investment and the reduction of risk and subsequent loss. Some methods used today to justify security investments may not align or be equivalent with methodologies under Generally Accepted Accounting Principles (GAAP). Research is needed to establish a baseline risk and to understand changes from the baseline that result from investment. This research also could benefit the broader risk management community.

Impact and consequences

The Sector continues to focus on security processes rather than security outcomes, and as a result, there is scant knowledge of which security investments and practices have an effect on security outcomes. A clear and accepted methodology to accurately measure both costs and benefits would speed the deployment of improved security technologies within organizations and across the Industry. There is a need for a disciplined approach based on clear outcome definitions combined with a causality oriented learning and improvement feedback loop; a standard language and financially certifiable methodology to define, estimate, measure, and communicate costs and benefits would assist all institutions. The sooner the industry adopts a standard cost-to-benefit approach, the more rapidly information protection will be integrated into financial institutiono priorities.

Desired Functionality

6 Develop a standardized methodology for calculating ROI for critical infrastructure protection (CIP) and security technology that is relevant to the financial industry. Such a methodology should:

- 6.1 Develop cost-benefit models describing the costs and benefits of improved CIP and security technology. The output of this research should result in agreement from participating institutions and the industry at large for adoption of these models and approaches. This model should include data that are appropriate to estimate the total lifecycle cost when implementing individual information protection programs, and form a repository for case studies that may be accessed and used by other institutions.

6.2 Develop common mathematics and rules for estimating program deployment costs that allow Institutions to “plug-in” their specific costs, and that are open to varied implementation approaches.
6.3 Quantify the costs/benefits for information protection as mandated by the Sarbanes-Oxley and Gramm-Leach-Bliley Acts, and link to an overall approach to provide reporting to meet SOX, GLBA, and other legal and regulatory requirements.
6.4 Establish commonly acceptable cost-to-benefit estimation, measurement, and communication processes and methods for the financial industry.
6.5 Focus on security outcomes rather than security processes to determine what security investments and practices have an effect on security outcomes.

Potential Research Projects

Research to support this challenge is needed to:

- Identify financial modeling methodologies that:
  - Quantify the costs and direct and indirect benefits of security software.
  - Are sufficiently close to existing ROI models as to be understood easily by financial institutions’ senior and executive management.
  - Are sufficiently consistent with existing accounting principles to be both acceptable to and understood by FI’s financial staffs.
- Develop tools to better understand the cost-benefit trade-offs and methods to quantify levels of investment and set priorities.

Challenge 7: Development of Practical Standards

The Situation

One of the prevailing techniques for closing the gap between state-of-the-art and state-of-the-practice is the development of practical standards and suggested practices. In an attempt to further the protection of the banking and finance critical infrastructures, numerous documents outlining suggested practices have been developed, most addressing a closely circumscribed segment of banking and finance systems and practices. Standards such as COBIT, ISO 27002, PCI-DSS, and the NIST Special Publications 800 series are in development or have been issued. While efforts to promulgate these documents and encourage adoption of these standards have been uneven, this challenge continues to consistently score near the top whenever these R&D opportunities are prioritized. Part of the problem is that, to date, the industry has been unable to quantitatively correlate best practices with reduced risk. If such a relationship could be determined and quantified, financial institutions would have the tools needed to justify risk management and risk reduction measures. This analysis could, in turn, assist the industry in agreeing on a common and consistent set of practices. A related question is how practitioners and regulators should adopt or consider these in developing robust and resilient infrastructures vis-à-vis the confusion caused by so many different best practices guides and standards. .

Impact and consequences

It typically takes a long period of time and involves a lot of costly trial and error to develop best practices in response to changing regulatory requirements. This process is inefficient and costly to financial institutions as well as to the regulators. Inaccessible or uncoordinated standards and best practices, and unclear return on investment (ROI) measurements, contribute to the gap between state-of-the-art and state-of-the-practice. In this space there are many chronically missed opportunities and the potential for substantial gains based on a modest investment.

Desired Functionality

7 Create a practical standards repository and incident database available for members of the Banking and Finance Sector to enable research into the effectiveness and correlation of effective practices that improve risk management. Industry, enterprise, system, and process practices and standards should be sought out, summarized, categorized, indexed, and made available to the community. The Department of Justice standards registry is an example of this (http://it.ojp.gov/jsr/public/index.jsp). Such a repository could include the following:

- 7.1 A database for use by academicians through which they can develop a correlation of existing standards, the risks each correlated set of standards addresses, the level of protection, and limits to protection each correlated set of standards provides.
- 7.2 Standards for integrating physical and logical security systems.
- 7.3 Standards across network connections that ensure security across wired and wireless devices with particular concern to interoperability and privacy.
- 7.4 Voice and video conferencing for VOIP over data networks.
- 7.5 Standards for access control.
- 7.6 Standards for outsourcing critical functions, particularly those related to networks and information systems, that address the implications for cyber security, business continuity, and overall risk management.

7.7 Standards for business continuity planning, including methods for determining the minimal operational requirements of an organization, strategies for achieving these requirements after a contingency event, selecting recovery time objectives (RTO) and recovery point objectives (RPO) for data replication, considering the distance between operational locations, the nature of critical business processes, cost, and sound business practices
7.8 Standards regarding the ability of key components of the Banking and Finance Sector to establish and maintain communication between their various primary and alternate facilities with the capability to conduct transactions at a sufficient volume and level of accuracy.
7.9 Practices regarding the verification and preservation of physical diversity of telecommunications routing
7.10 Practices in code development.
7.11 Identification of the key elements of secure software code/products.
7.12 Quantifying the impact of “safe practices” on reducing exposure.
7.13 Practices of shared responsibilities that lead to better security controls.
7.14 Practices in data replication that increase resiliency by seamlessly providing redundant services and processing capabilities across multiple operations centers.

This endeavor should also investigate new, innovative technologies that might improve the current state of best practices.

Potential Research Projects

Research to support this challenge is needed to:

- Correlate the impact of standards and practices on the actual state of security.
- Review laws and regulations (e.g., Bank Secrecy Act, Gramm-Leach-Bliley, Sarbanes-Oxley) and analyze the period of time it took to develop a standardized best practices approach within the industry to implement the new regulations.
- Develop approaches that would be more cost-effective and efficient for financial institutions to comply with requirements.
- Build models of disaster situations and then play interactive tabletop game to simulate various scenarios.

Appendix A: Members of the FSSCC R&D Committee

C. Warren Axelrod, Financial Services Technology Consortium
Andy Bach, Securities Industry Automation Corporation
John Carlson, BITS/Financial Services Roundtable (Chairman)
Frank Castelluccio, The Options Clearing Corporation
Dan DeWaal, The Options Clearing Corporation
Eric Guerrino, Bank of New York Mellon Corporation
Mark Merkow, American Express Company
William Nelson, Financial Services Information Sharing and Analysis Center
Dan Schutzer, Financial Services Technology Consortium

Public Sector Representatives: Brian Peretti, U.S. Department of the Treasury

In addition to the above R&D Committee members, Paul Smocer, Ann Patterson, Matt Ribe and Ryan Waggoner of BITS/Financial Services Roundtable provided substantive comments and edits on this draft of the report. Jennifer Bayuk, formerly with Bear Stearns & Co, served as the chair of the R&D Committee from 2006 until February 2008 and contributed to the development of this paper.