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

Research Challenges for the Financial Sector

DHS S&T PI Meeting

September 18, 2013

Dan Schutzer, co-Chair FSSCC R&D Committee and

CTO, The Financial Services Roundtable/BITS

dan@fsround.org

The Financial Services Sector

- Public and private institutions involved in carrying out the primary sector functions of depositing funds, making payments, providing credit and liquidity, investing, and transferring financial risk (taken from http://www.fsscc.org/fsscc/reports/2011/SAR-2011.pdf)
- Sector covers different organization types, further broken down into 157 specific business functions:
  - Types: Clearinghouses; Commercial banks; Credit rating agencies; Payment companies; Exchanges; Financial advisory services; Financial utilities; Government and industry regulators; Insurance firms; Investment banks; Retail banks
  - Functions: Transaction processing, bank deposit programs, loan origination and management, stock/bond trading and lending

Unique Characteristics

- High demanding transaction rates
  - 10,000 Worldwide Card Transactions Occur Very Second, http://www.transactionworld.net/articles/2007/August/washOut1.asp
  - Transaction processing needs to be Atomic (all or nothing occurs)
- Few key critical players
  - But tens of thousands of organizations
- Large customer base
  - Larger institution banks serving tens of millions of retail consumers
- Huge legacy investment
  - Hard to migrate from
  - Usually back-ending web
  - Regulation complicates cost, complexity and difficulty of migration

Changing Environment

- Advances in mobile, social, cloud, others (IoT):
  - Breaks down business silos
  - Blurs physical/cyber boundaries
  - Enables new threat vectors as systems become perimeter-less
  - Increases competition, putting further pressure on profit margins, accelerating change, and requiring faster decision-making
- Growing complexity
  - Increasingly real-time and inter-dependent
- Threats growing in sophistication and lethality

Changing Workplace Environment

- Employees bringing consumer technology into the workplace
  - Smart phones, tablets, wearables
  - Intermixing of personal consumer apps with business functionality
- The movement of business and consumer data to the cloud
  - Creates large stores of important data and processing resources that will lure attackers
  - Requires rethinking end point perimeter security
  - Could evolve to a future infrastructure characterized by a small number of large silo'd network/cloud alliances that although it has its advantages, isn't without its own risks

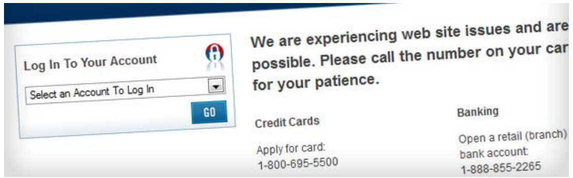
Changing Threat – Various Motivations

Hacktivism
Fraud
National Agendas

- Criminals seeking financial gain
- Theft of intellectual property
- Politically-motivated Hacktivism
- National agendas and resources
  - Disruption of Critical Infrastructure

- In the near future, prudent to also expect:
  - Control information to influence what users believe and where they go on the web
  - Tamper and manipulate data for disruption of critical infrastructure
  - Disrupt to distract the attention from coordinated attacks aimed at committing fraud
  - Cyber-attacks that could disrupt or take down targeted physical equipment, or take lives

Changing Threat – Increasingly Lethal and Sophisticated



We are experiencing web site issues and are possible. Please call the number on your car for your patience.

Credit Cards

Apply for card:
1-800-695-5500

Banking

Open a retail (branch)
bank account:
1-888-855-2265

DDoS on Steroids

- **Targeted** – from attacks of opportunity to personalized and dedicated to a target
- **Persistent** – attacking a specified target can last for months and years
- **Ability to harness huge resources** – botnets and server farms
- **Adaptive and dynamic** – change approaches, tactics and tools in response to the defense
- **Hold unknown vulnerabilities in reserve** – large database of zero day exploits created and held in reserve until needed
- **Compromise of the Supply Chain** – poisoning components during production and transport - hard to detect, expensive to defend against

Changing Regulatory Environment

- Executive Order 136361 – Improving Critical Infrastructure Cybersecurity
  - Information Sharing
  - Cybersecurity Standards
- Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience
  - All hazards situational awareness
  - Prioritize critical infrastructure

Potential for Cybersecurity Legislation

- Information sharing with liability protections
  - H.R. 624, Cybersecurity Intelligence Sharing and Protection Act (CISPA) passed House April 18
- Updates to criminal codes
- International law enforcement collaboration
- Funding for cyber research and development
  - H.R. 756, Cybersecurity Enhancement Act passed House April 16

Needs

- Better knowledge of the threat
  - Improve Information sharing and analysis
  - Achieve right balance between privacy and security
  - Better able to anticipate and respond to future threat
- More effective risk management and countermeasures
  - Earlier identification of anomalies to detect and respond to the threat
  - Cyber war and Active/Passive defense debate
  - Dependency of the Financial Sector on other Critical Industries
- Better cyber security education and awareness
- Define and transition to a new more secure architecture, processes and testing
  - Migration is hard

Research Agenda for the Banking and Finance Sector

(http://www.fsscc.org/fsscc/news/2013/FSSCC RD Agenda April 24 2013.pdf)

1. **Identity assurance** – Identify and authenticate people, organizations, devices, services, application software in real-time, at level of assurance commensurate with the risk, at order of magnitude greater than currently

2. **Security analysis and intelligence** – More effective real-time identification of malware, infected devices, and suspicious activities of people and organizations; capable of forecasting, learning and adapting to changing threats and tactics; employing real-time and after-the-fact forensic analysis.

3. **Transaction protocols** – Core transaction protocol layer, integrated with transaction systems and processes, easy to use and customize by verified users and devices, near impossible to access, modify and tamper with by any non-verified user or device, able to handle loads of hundreds of millions of financial transactions per day.

**Ten Focus areas, not listed in any order of importance*

Research Agenda for the Banking and Finance Sector

(http://www.fsscc.org/fsscc/news/2013/FSSCC RD Agenda April 24 2013.pdf)

4. **Risk management** – Common framework and set of metrics and processes; cyber risk identified, assessed and managed against other financial risks such as credit and market risk; taking into account that we are dealing with intelligent adversaries – intelligent adversaries are not random
5. **Human behavior** – Better integrate humans into the Financial Services Sector risk management, information security and physical security programs
6. **Proactive measures** – Suite of proactive measures that provides demonstrative success over current purely defensive measures, including a set of tools and analyses that justify these measures, taking into account the unique regulatory and compliance environment of the financial services sector.

Research Agenda for the Banking and Finance Sector

(http://www.fsscc.org/fsscc/news/2013/FSSCC RD Agenda April 24 2013.pdf)

7. **Software technology assurance** – Application software development tool sets and processes that enable financial applications to be developed and maintained with measureable improvement in their ability to operate in the face of successful attacks; includes ability to spot counterfeit or tampered devices and software in real-time, with traceability back to source of creation or tampering.

8. **Testing financial applications** – Methods of testing and assessing the security, resilience and resistance to attack of financial applications and systems that provide measurable improvement in ability to both identify vulnerabilities, along with comprehensive analyses of areas needing improvement.

9. **Training** – Training methodology that demonstrates measureable improvement in security skills and readiness of personnel and customers, taking into account unique systems architecture, vulnerability and regulatory compliance requirements of the financial services industry

Research Agenda for the Banking and Finance Sector

(http://www.fsscc.org/fsscc/news/2013/FSSCC RD Agenda April 24 2013.pdf)

10. **Internet ecosystem architecture** – Formal and/or informal models of the Internet Ecosystem that allow a plug-and-play approach to modeling proposed security advances in ecosystem components, able to forecast the impact of proposed improvement deployments.

* Need to improve transition of research to practice

- R&D presentations
- Workshops
- Pilots
- Address barriers to adoption
- Resources applied to transition to practice