The E-Commerce Security

Part 1 of 2

Paul I-Hai Lin, Professor
http://www.etcs.ipfw.edu/~lin
A Specialty Course for
M.S. in Technology IT/Advanced Computer Applications Program
Purdue University Fort Wayne Campus

References

- Google Hacks, 100 Industrial-Strength Tips and Tools, by Tara Calishain and Rael Dornfest, from O’Reilly, 2003
- Web Security, by Lincoln D. Stein, from Addison-Wesley, 1998
Topics

- Cyberwar: Mutually Assured Destruction (MAD)
- The E-Commerce Security Environment
- Security Threats in the E-Commerce Environment
- Technology Solutions for Site Security
- Management Policies, Business Procedures, and Public Laws
- E-Commerce Payment Systems
- E-Billing Presentment and Payment
- Case Study

Cyberwarfare

Mutually Assured Destruction (MAD)

- State sponsored activities
- China vs. Google (Email services and Google Talk features), May 2011
  - Google says China blocking its email services, abc News, [link](http://abcnews.go.com/Technology/wireStory?id=13182824)
  - Beijing Fires Back at Google, [link](http://online.wsj.com/article/SB10001424052702304563104576361300123816450.html)
- U.S. public web, air-traffic control systems, healthcare, telecommunication services, electric power grid
Cyberwarfare
Mutually Assured Destruction (MAD)

- U.S. public web, air-traffic control systems, healthcare, telecommunication services,

- Electric power grid cyber attack threats

Stuxnet

- Attack industrial machines, facilities
- Stuxnet worm used against Iran was tested in Israel, by William Broad, John Markoff and David Sanger, 2011/1/16, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all
- How Stuxnet Spreads: A Study of Infection Paths in Best Practice Systems, by Eric Byres, Andrew Ginter and Joel Langill, ICSJWG 2011 Spring Conference
Cyberwarfare
Mutually Assured Destruction (MAD)

- RustockB
  - Botnet – a collection of compromised computers connected to the Internet, each of which is called a ‘bot’
  - DDoS (Distributed Denial of Service) attack

- CAIDA (Cooperative Association for Internet Analysis), http://www.caida.org/home/


Cyber Storm II

- MAD 2.0


**Cyberwarfare**

**Mutually Assured Destruction (MAD)**

- Hacking and cyberwar? Difference.
- Why has cyberwar become more potentially devastating in the past decade?
- What percentage of computers have been compromised by stealth malware programs?
- Will a political solution to MAD 2.0 be effective enough?

---

**The E-Commerce Security Environment**

- **Players**
  - Customers: Law-abiding citizens
    - Global marketplace
    - Privacy, Integrity, Authentication, Non-repudiation
  - For Criminals
    - Less risky to steal online

- **Cybercrime**
  - Bot networks, DDoS attacks, Trojans, Phishing, Data theft, Identity theft, Credit card fraud, Spyware

- **Technology and Infrastructure**
  - E-commerce web sites, Social network, Smartphones and Mobile devices, Payment systems, Databases

- **Law Enforcement Agencies**
The E-Commerce Security Environment

- Internet Information
  - Personal Identifiable Information
  - Personal Health Information

- Internet Information Security and Enforcement Agencies
  - Identity Theft Resource Center (ITRC), http://www.idtheftcenter.org/
  - Internet Crime Complaint Center (IC3), http://www.ic3.gov/default.aspx
    - CSI Reports, http://gocsi.com/members/reports

Figure 5.1 Types of Attacks Against Computer Systems (Cybercrime), page 264
What is Good E-Commerce Security?

- To achieve highest degree of security
  - New technologies
  - Organizational policies and procedures
  - Industry standards and government laws

- Other factors
  - Time value of money
  - Cost of security vs. potential loss
  - Security often breaks at weakest link

Figure 5.2 The E-Commerce Security Environment, page 267
Security Threats in the E-Commerce Environment

- Three key points of vulnerability in E-Commerce environment
  1. Client
  2. Server
  3. Communication pipeline (Internet communications channels)
Figure 5.3 A Typical E-Commerce Transaction

Figure 5.4 Vulnerable Points in an E-Commerce Transaction
Most Common Security Threats in the E-Commerce Environment

- Malicious code (malware)
  - Viruses
  - Worms
  - Trojan horses
  - Bots, botnets

- Unwanted programs
  - Browser parasites
  - Adware
  - Spyware

Most Common Security Threats in the E-Commerce Environment (cont.)

- Social engineering

- Phishing
  - Deceptive online attempt to obtain confidential information
    - E-mail scams
    - Spoofing legitimate Web sites
    - Use of information to commit fraudulent acts (access checking accounts), steal identity
Most Common Security Threats in the E-Commerce Environment (cont.)

- **Hacking**
  - Hackers vs. crackers
  - Types of hackers: White, black, grey hats

- **Cybervandalism:**
  - Intentionally disrupting, defacing, destroying Web site

- **Data breach**
  - When organizations lose control over corporate information to outsiders

- **Credit card fraud/theft**
  - Hackers target merchant servers; use data to establish credit under false identity

- **Spoofing**
  - Misrepresenting oneself by using fake e-mail addresses or masquerading as someone else

- **Pharming – spoofing a web site**

- **Spam/junk Web sites**

- **Denial of service (DoS) attack**
  - Hackers flood site with useless traffic to overwhelm network

- **Distributed denial of service (DDoS) attack**
Sony: Press the Reset Button (Class Discussion)

- What organization and technical failures led to the April 2011 data breach on the PlayStation Network (PSN)?
- Can Sony be criticized for waiting 3 days to inform the FBI?
- Have you or anyone you know experienced data theft?

Most Common Security Threats in the E-Commerce Environment (cont.)

- **Sniffing**
  - Eavesdropping program that monitors information traveling over a network
- **Insider jobs**
- **Poorly designed server and client software**
- **Social network security**
- **Mobile platform threats**
  - Same risks as any Internet device
  - Malware, botnets
Think Your Smartphone is Secure?

- What types of threats do smartphones face?
- Are there any particular vulnerabilities to this type of device?
- What did Nicolas Seriot’s “Spyphone” prove?
- Are apps more or less likely to be subject to threats than traditional PC software programs?

Technology Solutions

- Protecting Internet communications
  - Encryption
- Securing channels of communication
  - SSL, VPNs
- Protecting networks
  - Firewalls
- Protecting servers and clients
Security Software, Tools and Information

E-Commerce Vulnerabilities & Security Reports and Study


E-Commerce Laws

- USA PATRIOT ACT
- 1978 Foreign Intelligence Surveillance Act (FISA)
- Protect America Act 2007
- The Communications Assistance for Law Enforcement Act (CALEA)
Summary