Identity Theft Prevention Workshop

Washington DC

April 26, 2006

Agenda

- 8:30-8:45 Welcome and Overview
- 8:45-11 The Identity Crime Spectrum
  - 8:45-9:15 The Legislative Landscape, Mary Ellen Callahan, Hogan & Hartson
  - 9:15-9:45 Law Enforcement Perspective, Raul Roldan, Chief Cyber Security, FBI
  - 9:45-10:15 Identity Technology, Purdue University
  - 10:15-10:30 Coffee Break
  - 10:30-11 Identity Best Practices, Jonathan Rusch, US Department of Justice

Agenda (cont)

- 11-12 Deployment Case studies
  - 11-11:30 Paul Biciunas, Fidelity Investments
  - 11:30-12 Darrell Shull, BIPAC
- 12-1 Lunch, Sponsored by ChoicePoint
- 1-3:45 Workshops
  - Best Practices in Identity, facilitated by Christine Varney
  - Identity Technology, facilitated by Purdue University
- 3:45-4:30 Reconvene and Next Steps

Introduction to Liberty Alliance

- An industry alliance to drive open, neutral, federated standards for digital identity, authentication and authorization
  - September 2001, 14 co-founders (+2)
  - More than 150+ members
- Liberty Approach
  - Distributed architecture (federation)
  - Business oriented
  - Policy/privacy focused
  - Based on the most common standards
    - HTTP, SOAP, XML, SAML, etc.
  - Multi-platforms
    - Java, .Net, Open Source initiatives

Liberty Vision

> Liberty envisions a networked world across which individuals and businesses can engage in virtually any transaction without compromising the privacy and security of vital identity information.

Identity Theft Working Group

- Liberty Special Interest Group in March 2005
- Make recommendations on policy, business, and technology
  - Enhance specifications
  - Enhance best practices work
  - Explore new solution areas
- Work closely with other orgs to drive solutions and awareness

LIBERTY ALLIANCE PROJECT

Objective - Obtain Individual Identity

Type	Attack	Description	Mitigations
Technical	Trojan/Keystroke Logging	Spyware/malware placed via hacking, as payload in a virus, or downloaded from an attacker's Web site	1, 3, 4
	Wireless Intercept	Open access points, AirSnarfing, "Evil Twin"	5, 6
	Pharming	DNS spoofing, DNS cache poisoning, proxy attacks	23
	Scrape Web Site	Gather personal data from Web sites to use as verifiers	
	Network Sniffing	Collect targeted network packets	7, 23
Physical	Theft	Stolen mail, wallets/purses, laptops	2, 5, 6
	Shoulder Surfing	Direct observation of personal, confidential information	2
	Dumpster Diving	Gather discarded documents or hardware (disks)	2, 8
	Trusted Insiders	Identity information misused by individuals with access	5, 9, 10
Social Engineering	Phishing	Luring individuals to reveal confidential information	1, 20
	Family Members	Identity information misused by family members	2
	Legal Identity Sources	Obtain identity information fraudulently from credit bureaus, government agencies, etc.	1, 2
	"419" Scams	Obtain money and/or account information	2
	Trusted Insiders	Obtain identity information from service providers (doctors, dentists, lawyers, etc.)	1, 2, 21, 22

LIBERTY ALLIANCE PROJECT

Objective - Obtain Multiple Identities

Type	Attack	Description	Mitigations
Technical	Hacking	Gain privileged access for further attacks and/or data harvesting	10, 12, 13, 14, 15, 16, 17
	Data Attacks	SQL injection, XSS attacks	7, 18, 19
	Database Attacks	Login attacks, inference attacks, SQL scanners	1, 5, 15
	Password Cracking	Acquire admin passwords to servers	1, 15
Physical	Theft and Loss	Backup data, tapes, disks, laptops, etc.	5, 7, 11
	Firewall Breaches	Connect and map internal network(s)	15, 16
	Dumpster Diving	Obtain discarded documents, disks, systems, etc.	8
	Trusted Insiders	Access individuals take data with removable media, e-mail	1, 2, 21, 22
Social Engineering	Gain Physical Access	Computer rooms, server farms, wiring closets, switches, routers	1, 2
	Trusted Insiders	DBAs, employees, contractors, individuals with access	1, 2, 21, 22
	Phone Requests	Obtain confidential information to facilitate attacks	2

Mitigations and Compensating Controls

1. Multi-factor authentication
2. User education
3. Anti-virus package(s)
4. Anti-spyware package(s)
5. Encryption
6. Secure configuration
7. Encrypted payload
8. Shredding
9. Enforce need-to-know
10. Access controls and user privileges
11. Policy and enforcement
12. n-tier architecture
13. Real-time monitoring
14. Honey pots/honey nets
15. HIPS (Host Intrusion Protection Systems)
16. NIDS (Network Intrusion Detection Systems)
17. Well-configured firewall(s)
18. Server-side validation
19. Secure coding techniques
20. Browser toolbars
21. Separation of duties
22. Audit controls
23. SSL/TLS