Identity Theft Prevention Workshop

Washington DC
April 26, 2006
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
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 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
<table>
<thead>
<tr>
<th>Type</th>
<th>Attack</th>
<th>Description</th>
<th>Mitigations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical</td>
<td>Trojan/Keystroke Logging</td>
<td>Spyware/malware placed via hacking, as payload in a virus, or downloaded from an attacker’s Web site</td>
<td>1, 3, 4</td>
</tr>
<tr>
<td></td>
<td>Wireless Intercept</td>
<td>Open access points, AirSnarfing, “Evil Twin”</td>
<td>5, 6</td>
</tr>
<tr>
<td></td>
<td>Pharming</td>
<td>DNS spoofing, DNS cache poisoning, proxy attacks</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td>Scrape Web Site</td>
<td>Gather personal data from Web sites to use as verifiers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network Sniffing</td>
<td>Collect targeted network packets</td>
<td>7, 23</td>
</tr>
<tr>
<td>Physical</td>
<td>Theft</td>
<td>Stolen mail, wallets/purses, laptops</td>
<td>2, 5, 6</td>
</tr>
<tr>
<td></td>
<td>Shoulder Surfing</td>
<td>Direct observation of personal, confidential information</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Dumpster Diving</td>
<td>Gather discarded documents or hardware (disks)</td>
<td>2, 8</td>
</tr>
<tr>
<td></td>
<td>Trusted Insiders</td>
<td>Identity information misused by individuals with access</td>
<td>5, 9, 10</td>
</tr>
<tr>
<td>Social</td>
<td>Phishing</td>
<td>Luring individuals to reveal confidential information</td>
<td>1, 20</td>
</tr>
<tr>
<td>Engineering</td>
<td>Family Members</td>
<td>Identity information misused by family members</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Legal Identity Sources</td>
<td>Obtain identity information fraudulently from credit bureaus, government agencies, etc.</td>
<td>1, 2</td>
</tr>
<tr>
<td></td>
<td>“419” Scams</td>
<td>Obtain money and/or account information</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Trusted Insiders</td>
<td>Obtain identity information from service providers (doctors, dentists, lawyers, etc.)</td>
<td>1, 2, 21, 22</td>
</tr>
</tbody>
</table>
# Objective - Obtain Multiple Identities

<table>
<thead>
<tr>
<th>Type</th>
<th>Attack</th>
<th>Description</th>
<th>Mitigations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical</td>
<td>Hacking</td>
<td>Gain privileged access for further attacks and/or data harvesting</td>
<td>10, 12, 13, 14, 15, 16, 17</td>
</tr>
<tr>
<td></td>
<td>Data Attacks</td>
<td>SQL injection, XSS attacks</td>
<td>7, 18, 19</td>
</tr>
<tr>
<td></td>
<td>Database Attacks</td>
<td>Login attacks, inference attacks, SQL scanners</td>
<td>1, 5, 15</td>
</tr>
<tr>
<td></td>
<td>Password Cracking</td>
<td>Acquire admin passwords to servers</td>
<td>1, 15</td>
</tr>
<tr>
<td>Physical</td>
<td>Theft and Loss</td>
<td>Backup data, tapes, disks, laptops, etc.</td>
<td>5, 7, 11</td>
</tr>
<tr>
<td></td>
<td>Firewall Breaches</td>
<td>Connect and map internal network(s)</td>
<td>15, 16</td>
</tr>
<tr>
<td></td>
<td>Dumpster Diving</td>
<td>Obtain discarded documents, disks, systems, etc.</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>Trusted Insiders</td>
<td>Access individuals take data with removable media, e-mail</td>
<td>1, 2, 21, 22</td>
</tr>
<tr>
<td>Social Engineering</td>
<td>Gain Physical Access</td>
<td>Computer rooms, server farms, wiring closets, switches, routers</td>
<td>1, 2</td>
</tr>
<tr>
<td></td>
<td>Trusted Insiders</td>
<td>DBAs, employees, contractors, individuals with access</td>
<td>1, 2, 21, 22</td>
</tr>
<tr>
<td></td>
<td>Phone Requests</td>
<td>Obtain confidential information to facilitate attacks</td>
<td>2</td>
</tr>
<tr>
<td>Mitigations and Compensating Controls</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Multi-factor authentication</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. User education</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Anti-virus package(s)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Anti-spyware package(s)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Encryption</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Secure configuration</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Encrypted payload</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. Shredding</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9. Enforce need-to-know</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10. Access controls and user privileges</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11. Policy and enforcement</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12. n-tier architecture</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13. Real-time monitoring</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14. Honey pots/honey nets</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15. HIPS (Host Intrusion Protection Systems)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16. NIDS (Network Intrusion Detection Systems)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17. Well-configured firewall(s)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18. Server-side validation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19. Secure coding techniques</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20. Browser toolbars</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21. Separation of duties</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>22. Audit controls</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>23. SSL/TLS</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>