Computer Security and Data Privacy

Eric White
IFD&TC 2007
Why do we care?

- Ethical Reasons
  - Honor commitment to respondents
  - Sensitive data could be used against respondents if released
What to do?

- Security = risk management
  - Risk = likelihood of a threat exploiting a vulnerability and the seriousness of a successful attack
  - All about tradeoffs

- Risk assessment
  - http://www.cramm.com/
  - http://www.cert.org/octave/
  - http://rusecure.rutgers.edu/sec_plan/risk.php
Security Models

• Data
  • CIA - Confidentiality, Integrity, Availability
  • Parkerian Hexad – Confidentiality, Possession of Control, Integrity, Authenticity, Availability, Utility

• Threat Vectors
  • TPS – Technological, Physical, Social
Escape Routes

- Tech Vector
  - Network
  - Servers & PCs
  - Mobile Devices
- Physical Vector
- Social Vector
Tech Vector – The Network

- **Threats**
  - Theft over the wire or air
  - Want to keep the bad guys out

- **Security Measures**
  - Secure communication with VPNs, SSL, WPA(2) or other encryption
  - Firewalls block traffic in and out
  - Monitor volume and type of network traffic
Tech Vector - Servers & PCs

- Threats
  - User account compromised
  - Errors in configuration exploited
  - Application flaw exploited
  - OS flaw exploited
  - Malware installed (viruses, trojans, etc.)
  - Data leakage (IM, email, etc.)

- Security Measures
  - Restrict local and remote user access
  - Software restrictions
  - Security scans (nmap, Nessus)
  - Restrict local device access
  - Patch management
  - Anti-virus and anti-spyware software
  - Principle of least privilege
  - Encryption
  - Content monitoring and filtering
Tech Vector – Mobile Devices & Media

• Threats
  • Theft or loss of device
  • Theft over air or wire

• Security Measures
  • Keep private data off device
  • Encryption for data storage and communication
  • Power-on password
Physical Vector

• Threats
  • Unauthorized Access
  • Theft

• Security Measures
  • Locked and secure workspace
  • Locked server space
  • Secure storage (paper documents, laptops, etc.)
  • Security camera
  • Inventory control system
  • Key and access revocation policy
Social or Personal Vector

• Threats
  • Encryption not used
  • Secure communication channels bypassed
  • Social engineering / phishing / spam
  • Passwords exposed or unprotected
  • Malicious intent

• Security Measures
  • Clear and sensible policy
  • Principle of least privilege
  • User-friendly software and support
  • Education and training
Conclusion

• Data security is a lot of work
  • Good tools being developed
  • “Baked in” in future products
• Security = Risk Management
  • Look at the big picture
  • Make rational decisions
• Don’t underestimate the social aspect
  • Behavior ≥ technology