Security Concerns with Remote Access

Karen Scarfone, NIST

Overview

- Definition/Scope
- Trends
- Vulnerabilities
- Threats
- Security Controls and Recent NIST Publications

Remote Access

- Defined as “the ability of an organization’s users to access its nonpublic computing resources from locations other than the organization’s facilities” (NIST SP 800-114)
- Access to public resources out of scope
- Access between an organization’s facilities out of scope

Remote Access Trends

- Increasingly popular because of widespread availability of Internet access and mobile computing devices
- More applications and other resources available through remote access
- Wide variety of client devices, including many outside the organization's control
- Client devices in many types of environments

Remote Access Vulnerabilities

- Remote access client devices generally have weaker protection than standard client devices
  - Many devices not managed by the enterprise
  - No enterprise firewalls, antivirus, etc.
  - Lack of physical security controls
- Remote access client devices may be used in hostile environments but not configured for them
- Remote access communications are carried over untrusted networks

Remote Access Threats

- Communications monitoring and manipulation
  - Deployment of rogue wireless access points
- Exploitation of remote access client devices and users
  - Phishing, keyloggers, etc. to collect credentials and other sensitive data
  - Unauthorized access to resources
- Loss or theft of remote access client devices

Remote Access Security

- General remote access security
  - SP 800-46, *Security for Telecommuting and Broadband Communications*
- Use virtual private networks
  - SP 800-77, *Guide to IPsec VPNs*
  - SP 800-113 (Draft), *Guide to SSL VPNs*
- Secure remote access client devices
  - SP 800-114, *User's Guide to Securing External Devices for Telework and Remote Access*
  - SP 800-111, *Guide to Storage Encryption Technologies for End User Devices*
  - National Checklist Program, Security Content Automation Protocol (SCAP)

Remote Access Security (cont.)

- Understand wireless networking security concerns
  - SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*
  - SP 800-48 (Draft), *Wireless Network Security for IEEE 802.11a/b/g and Bluetooth*
- Test the security of remote access methods
  - SP 800-115 (Draft), *Technical Guide to Information Security Testing*

Links

- Computer Security Resource Center
  http://csrc.nist.gov/
- Special Publications
  http://csrc.nist.gov/publications/PubsSPs.html
- Draft Publications
  http://csrc.nist.gov/publications/PubsDrafts.html

Questions?

karen.scarfone@nist.gov