Network Security Controls

Tom Kelliher, CS 325

Nov. 29, 2007

1 Administrivia

Announcements

Assignment

Read Chapter 8 for Monday's exercise.

From Last Time

Problems and solutions for several networking protocols.

Outline

1. Controls.
2. Vulnerability points.

Coming Up

Lab day to begin your voting system analysis work.

2 Controls for Problems Discussed Last Class

1. DNS
   (a) Keep named up to date.

   (b) Use authentication techniques to verify source of query replies.

2. SMTP
   (a) Disable relaying for hosts outside your domain.

   (b) Use greylisting and Bayesian techniques to reduce SPAM.

   (c) SPF protects `Return-Path` (envelope address). What about `From` and `Sender` headers? — Not used by mail handling software.

3. XDMCP
   (a) Block at external firewall.

   (b) Use tcpd or tcpwrappers as an additional layer of defense, and to limit internal use.

   (c) Do not disable built-in protection, regardless of DNS problems.

3 Networking Weak Points and Controls

A summary of controls:

1. Design and implementation — segmented networks and services. Redundancy. Eliminating single points of failure.

2. Encryption. Link-level. End-to-end. VPNs. Signed code.

3. Data integrity. ECC. Cryptographic checksum.

4. Strong authentication. One-time passwords. Challenge-response systems. Distributed authentication.

5. Access controls. ACLs on routers. Firewalls.

6. Alarms and alerts. IDS at system- and network-levels.

7. Honeypots.

   Traffic flow security. Onion routing.

Threats to mediate:

1. Intercepting data in traffic.

2. Accessing programs or data at remote hosts.

3. Modifying programs or data at remote hosts.

4. Inserting communications.

5. Impersonating a user.

6. Inserting a repeat of a previous communication.

7. Blocking selected traffic.

8. Blocking all traffic.

9. Running a program at a remote host.