Introduction, Continued

Tom Kelliher, CS 325

Feb. 1, 2010

1 Administrivia

Announcements

Perl resources pointed to on class Web site.

Assignment

2.1–2.4 will be assigned once we finish our Perl introduction.

Write and run a small, standalone Perl program on phoenix, to familiarize yourself a bit with Perl and re-familiarize yourself with phoenix.

From Last Time

Introduction.

Outline

1. Introduction, continued.
2. Discussion/exercises.

Coming Up

Cryptography, Perl CGI and file I/O.

2 Introduction, Continued

2.1 Defense Mechanisms

1. Prevent. Block attack (firewall) or close vulnerability (load new kernel).
2. Deter. Make attack harder (use weak encryption).
3. Deflect. Make another target more attractive (honeypot).
4. Detect. At time of attack or later (intrusion detection).
5. Recover. From the attack (backups).

2.2 Controls

1. Encryption. Basic tool. Clear text; cipher text.
2. Software controls:
   (a) Internal security controls. Authentication and views within a DBMS. Apache global and local controls.
   (b) Operating system and network controls. Traditional authentication and access measures. SE Linux. TCP wrappers.
   (c) Independent control programs. John the Ripper, TripWire, ipChains, PAM.
   (d) Development controls. Software design standards and methodologies.
3. Hardware controls.

(a) Hardware encryption engines.

(b) Smart cards for authentication; biometrics.

(c) Locks and chains.

(d) Firewalls, bandwidth regulation systems, intrusion detection systems, network partitioning.

4. Policies.

   Policies for programmers, administrators, and users.

5. Physical controls.

   Controlled access to computing systems.

How do these relate to defense mechanisms?

2.3 Effectiveness of Controls

1. Awareness of the problem.

2. Likelihood of Use.

   Principle of effectiveness.

3. Overlapping controls.

4. Periodic review.

   Principle of weakest link.

3 Discussion/Exercises

1. Do you currently use any computer security control measures? If so, what? Against what attacks are you trying to protect?

2. When you say that software is of high quality, what do you mean? How does security fit into your definition of quality? Can an application be insecure and still be good?

3. Cite a recent report of a security failure that exemplifies one or more of the principles we've discussed: easiest penetration, adequate protection, effectiveness, weakest link.