Lecture 2: Vulnerabilities and Standards

Summary

We finish-off the material from Chapter 1 of P&P with a discussion of vulnerabilities; this segues into a more detailed description of software vulnerabilities from Section 3.1. Lastly, we introduce three important standards organizations — we will encounter publications from these organizations throughout the semester.

Vulnerabilities

Reference: P&P, Sections 1.3 and 3.2

Types of Vulnerabilities

Relate classification of attacks (interception, interruption, modification, fabrication) to system assets (hardware, software, and data)

Hardware

A *hardware* vulnerability may *expose* software or data, e.g. TEMPEST Demo http://www.csee.umbc.edu/~cmarron/cmsc426-626/lectures/SecTEMPEST.ogg

Data

Can a *data* vulnerability *expose* software or hardware to attack?

Software

Can a *software* vulnerability *expose* hardware or data to attack?

Software Modification

This means more than just changing the bits of an executable file — also includes modification of program execution or causing a program to run in a way that was not intended. Many important vulnerabilities are of this type.

Buffer Overflow Attack (we'll go into this in-depth in Lectures 4 and 5)

What is it?

http://www.csee.umbc.edu/~cmarron/cmsc426-626/lectures/buffer_overflow_overview.pdf

Give an example.

How do you prevent it?

Incomplete Mediation

What is it?

Give an example.

How do you prevent it?

Time-of-check to Time-of-use Errors (or *Race Errors*)

What is it?

Give an example.

How do you prevent it?

Timing Attacks

What is it?

Give an example.

Here's one: http://codahale.com/a-lesson-in-timing-attacks/

A more complicated example:
http://crypto.stanford.edu/~dabo/papers/ssl-timing.pdf

How do you prevent it?

Major Standards Organizations

Why standards? Interoperability, assurance of market share.

More important for security *because it is hard!*

The Internet Organization

Internet Architecture Board

Internet Engineering Steering Group

Internet Engineering Task Force (IETF)

Internet Drafts are proposed standards; Requests for Comment (RFCs) are published standards.

RFCs — not just security, but many Internet standards

http://www.ietf.org/rfc.html

Examples:

1883 — IPv6 Specification
2065 — DNS Security Extensions
3711 — Secure Real-time Transport Protocol (SRTP)
4250 - 4254 — Secure Shell (SSH)

National Institutes of Standards and Technology (NIST)

Publish Federal Information Processing Standards (FIPS) and Special Publications (SP)

Examples:

FIPS 186-4 — Digital Signature Standard
FIPS 197 — Advanced Encryption Standard
SP 800-90 — Random Number Generation
SP 800-82 — Industrial Control System Security

International Telecommunications Union (ITU)

"is responsible for studying technical, operating, and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis."

Examples:

X.509 Public Key Certificates
X.800 Security Architecture for Open Systems

Exercises

P&P, Chapter 1, exercises 14, 17-21