# Security and Standards

Or, What Should This System Do
and
How Well Does It Do That?

# The Problem

Vendor: “This system is designed and built using standard industrial software engineering techniques”
Customer: “We installed and run this following the vendor’s instructions”

- Took 5 minutes to gain illicit, unauthorized access to system
- Took 10 minutes to compromise system’s functioning so it reported incorrect results
- Took 20 minutes to find all “hidden” passwords embedded in programs

Moral: current software and systems are not secure!

# What Is Security?

- No intrinsic meaning
- Defined by a statement of requirements and rules called a *security policy*
  - Policies vary among organizations
  - Often informal, sometimes unwritten—which leads to confusion and disputes
- Definition depends on what the system is to do and where (how) it is to function
  - Network systems: protect both network messages *and end, intermediate systems*

# Role of Standard

- Presents definition and/or method of measurement
  - Measurement may be quantitative or qualitative
- Aspects of security standards
  - Functionality: what should it do?
  - Assurance: how do we know it does it?

# Assurance

Confidence that an entity meets its security requirements
– Based on specific evidence and applying assurance techniques

Depends on environment as well as system itself

Vendors, users, operators may help supply evidence, but independent experts do the analysis and evaluation

# Security = Functionality + Assurance

- Windows 2000 “achieves highest level of security evaluation” (Microsoft)
  - Common Criteria assurance rating EAL4
- But what is the functionality?
  - Protection Profile: CAPP
    - Assumes trusted environment, users; no determined and/or hostile attackers
    - Assumes nothing installed on system beyond what it is delivered with
  - Translation: don’t install anything and don’t hook it up to a network
    - Especially not the Internet!

# Getting Assurance

For the developer/vendor: Did they validate that the system as delivered meets the requirements?

For the purchaser/installer: Is it installed correctly and does everything works together?

From the maintainers and operators: Do the procedures enforce the security policy?

Most importantly: do they provide evidence that independent experts can (and do) assess?

# Penetration Testing

- Goal: violate security policy to determine effectiveness of security controls
- Rules
  - What information should testers be given?
  - How do you know when test succeeds?
  - What are testers *not* allowed to do?
  - Who should know about test?
- All this must be in writing and signed by whomever has authority to approve tests
  - Severe legal consequences possible if this is not done

# Questions? Answers?

Matt Bishop
*email*: bishop@cs.ucdavis.edu
Dept. of Computer Science
University of California, Davis
One Shields Ave.
Davis, CA 95616-8562