CS 166 Lecture Notes for 8/26/2014

teodoro.cipresso@sjsu.edu

1.2.1 Confidentiality, Integrity and Availability

- Confidentiality: Prevent unauthorized reading of data.
- Integrity: Detect unauthorized writing (or modification) of data.
- Availability: Prevent denial of service attacks.

1.2.2 Beyond CIA

- Authentication: local and network are 2 different problems.
  - With local, crypto is used to verify the password and that's it.
  - With network, we're vulnerable to multiple attacks that don't occur on local.
  - Trudy can intercept, modify, insert, or replay messages to pose as Bob.
  - Authentication over a network requires protocols.
  - Security protocols define how to compose and order exchanged messages.
  - Crypto plays an important role in security protocols.
  - One Bob is authenticated his actions need to be restricted (Authorization).
  - Bob shouldn't be able to read Charlie's balance.
  - Authorization restricts actions on authenticated users.
  - Authentication + Authorization = Access Control
- Security is implemented in software, microcode, or firmware.
  - Real world software is large + complex with millions of lines of code.
    - The lines harbor bugs yet to be discovered.
  - Bugs can cause security vulnerabilities (defensive programming?)
  - Malware is software written with the *intent* to do wrong.

1.3.1 Cryptography

- Cryptography "secret codes" are a fundamental security tool.
- Crypto is used to provide confidentiality (ciphertext is unreadable).
- We start with classic cipher systems. Even though these systems are no longer used, the principles and techniques are still used in modern ciphers.
- We then move to study modern crypto.
- Symmetric key and Public Key Crypto play major roles in information security.
  - So each gets its own chapter.
- Hash functions are also very important tools. They are used in many different ways.
- Cryptanalysis, "Breaking Ciphers".

1.3.2 Access Control

- Deals with Authentication and Authorization.
- Passwords are used because they are cheap—not because they are the most secure option.
- Weak passwords are a major vulnerability in most systems.
- Alternatives to passwords include biometrics and smartcards.
- Authorization deals with restricting a user's actions once they are authenticated. Two classic methods for enforcing those restrictions are Access Control Lists and Capabilities.
- Authorization leads to a few specialized topics.
  - Multilevel security (and the related topic of compartments).
  - U.S. Military has TOP SECRET and SECRET information. Some users can see both, one, or none of these. If both types of info are stored on the same system, enforcing these restrictions is challenging.
- Multilevel security leads to security modeling.
  - Layout the security requirements of a system (essential elements).
  - Test the system to see if it satisfies an existing model.
  - If the system satisfies an existing model then it inherits all of the security properties known to hold for that model.
  - We'll look at two of the simplest models.
- Multilevel security provides for discussing Covert Channels and Inference Control.
  - Covert Channels are unintended channels of communication. These are common.
  - Inference Control: limit the amount of sensitive information that can leak out of a system through valid, normal DB queries.
- Firewalls are a form of access control for networks, however attacks occur and Intrusion Detection Systems (IDS) can detect attacks in progress.

1.3.3 Protocols

- First we consider authentication over a network. Replay is a critical problem.
- Cryptography is essential in authentication protocols.
  - Symmetric and Public Key Crypto are covered.
  - Hash Functions are also important.
- A small change to a protocol can completely change its security.
- SSL is an elegant an efficient protocol.
  - SSL vs. IPSec. IPSec is over-engineered.
  - Despite lengthy open development process IPSec is complex and has security issues.
  - Kerberos follows a much different approach than either SSL or IPSec.
- WEP and GSM are wireless security protocols with many flaws. We'll discuss these.

1.3.4 Software

- Extremely large topic that we just scratch the surface of.
- We'll discuss security flaws and malware.
- SRE (deconstruct software without access to source code)
- Trusted OS? (Microsoft)

1.4 The People Problem

- Security can be broken due to user error(s). For example:
  - Ignoring warnings
  - Weak passwords
  - Strong passwords?
    - They often get written down to remember them.