LECTURE 1

Introduction

1 The Goals

After a successful completion of this course, the student should be able to understand

- The IT weaknesses that exist in an organization
- How these are typically exploited
- The resources that are at stake
- Available methods to protect these resources
- The legal and ethical issues involved

When there is a security breach at a business and systems are halted either by damage inflicted to the production systems or through a denial of service (DOS) attack, there is loss of business, loss of intellectual/proprietary assets such as source code of programs, and reputation. Loss of reputation is one of the primary reasons why business hush up IT attacks. This combined with the fact that the federal government does not classify IT crimes separately, make the task of putting a dollar figure on the losses due IT security breaches very difficult. The figure is estimated to be between $300M and $500B. The government systems are also exposed to IT attacks. National defense labs hold important military secrets relating missile technologies that are of great importance to national security.

2 Who Understands What

The owner certainly understands what is at stake, i.e. the value of what is being guarded. Developer is typically concerned with the functionality of the application that is being built; Security is secondary. Until it is pointed out that not checking array bounds for example can make the application susceptible to buffer-overflow attacks, the developer does not pay attention to such matters. Q/A staff might be aware of security holes that they discover during testing. Normally the IT staff is tasked with guarding the information technology assets, i.e. computer hardware,

access to server rooms, tapes used to back up data and code, network devices such as routers and firewalls, scanners and printers. The IT staff is expected to have a good understanding of overall security. But the mechanics of buffer overflow or email viruses is outside their domain of expertise.

The one who understands the entire security landscape is the hacker. A good hacker has a very thorough understanding of what is at stake, how programs run, inner working of various operating systems, networking protocols, databases and human psychology. Some example facts that were used in previous attacks:

- C does not do array-bound checking
- Some UNIX utilities, written in C, give a temporary root privileges to normal users
- People can remember only a few different passwords
- People tend to pick words that are easy to remember for passwords making the words susceptible to dictionary attacks
- Having a catchy subject heading in an email virus gets people to open the email containing a virus
- Network packet-source information can be modified so that it appears to be originating from another location

3 Who are These People That Breach Computer Security?

Amateurs

- Have a poor understanding of security
- Accidentally discover that they have access to something of value. They might take advantage of that.
- Have a temporary incentive to commit this kind of a crime, e.g. a disgruntled employee might attempt to damage to get “even” with management

Crackers

- Students/juveniles
- Seen by them as victimless crime
- Absence of explicit warning not to trespass is taken as permission for entry
- Status among other hackers -- The hackers hall of fame contains many very talented technical people like Richard Stallman, Dennis Ritchie and Ken Thompson, among others who committed crimes including one who was on the FBI “most wanted” list, Kevin Mitnick. Many times these juveniles are looking for an identity and a status that they might not be getting at school.

Tsutomu Shimomura, an experimental physicist from San Diego supercomputing center, wrote an account of how he trapped Mitnick in a book. This book makes an interest reading for this class.

Career Criminals

- The underground criminals hire these criminals
- Might belong to special interest/extremist groups
- Might come from "enemy" nations

4 The Three Aspects of Security

These three goals are conflicting, i.e. strengthening availability might compromise confidentiality.

Confidentiality

- Only authorized people can see protected data
- Who decides who is "authorized"?
- How does one determine the person claiming to be is really that person? (Nonrepudiation)

Integrity

- Precise
- Accurate
- Unmodified
- Modified in acceptable ways by authorized people
- Consistent

Availability

- Timely response
- Fair Allocation
- Fault tolerant
- Full functional

Easy to understand when a resource is not available. Lack of VPN might prevent employees to telecommute, MS outlook features are not all available when accessed from the web, attempting to login incorrectly 3 times might disallow an

authorized user, securing a web page might encrypt images and make the download too slow to be acceptable.

In class exercise: (Exercise 1.5, page 15 of Gollmann)

Bank customers can withdraw cash from automated teller machines (ATMs) using a cash card and a personal identification number (PIN). Conduct a risk and threat analysis for this application, both from the customers' and the banks' viewpoints.