95-753

Lecture 3

Secrets & Lies

1. The Landscape

Richard J. Orgass
Heinz School
Carnegie Mellon University

1. Introduction

- First seven days of March 2000
  - News Events
    - b-to-b website for SaleGate.com -- 3,000 Customer Records Stolen
    - Intuit Personal Web site leaks
    - Kevin Mitnick testifies before Congress
      - "social engineering" is major security vulnerability
      - often gets passwords and other secrets by pretending to be someone else and asking
    - Gallup poll -- third of all asked less likely to make on-line purchase because of breakins
    - Personal data from people who ordered Playstation 2 were leaked to their customers by Sony
    - Amazon.com pays commissions to third-party web sites for referrals. Program to manage is subverted enabling anyone to channel information to anyone
    - CIA director denies US engages in economic espionage but doesn't deny that ECHELON is used
    - Nine more security related items.....

1. Introduction -- II

- First Seven Days of March (continued)
  - Software vulnerabilities reported
    - MS Internet Explorer 5.0 (win 95, 98, NT, 2000) allows attacker to set up a web page that gives him the ability to execute any program on a visitors machine
    - By modifying URL attacker completely bypasses authentication mechanisms protecting remote-management screens of the Axis StarPoint CD-ROM servers
    - If attacker sends Netscape Enterprise Server 3.6 a certain type of long message, a buffer overflow crashes a particular process; attacker then executes arbitrary programs on the server.
    - Can launch denial of service and CGI script attacks so that the Internet Security System's RealSecure Network Intrusion Detection software does not detect
    - Sending URL to server running Allaire's ColdFusion product, attacker can receive an error message giving physical paths to various files.
    - Eight additional new vulnerabilities reported....
    - 65 web sites known to have been defaced

1. Introduction -- III

- First Seven days of March 2000 (continued)
  - Attacks against a home computer
    - twenty-six scans looking for vulnerabilities to exploit
    - four particularly determined attempts at breaking into the computer
      - basic vulnerability
      - scans
      - piles of other crafty cracker tricks
- Systems
  - Much more complex than programs
  - Security much more difficult because no one understands whole system

1. Introduction -- IV

- Four types of Issues
  - Complex
    - Win 2000 Active Directory security problems can be traced to complexity of any computer-based directory
  - Interactive
    - Interaction between software on Intuit's Web sit and software that double click uses to display ads to Web users resulted in information leaking between users
  - Emergent
    - Sony programmers had no idea why credit card information leaked from one user to another. It just happened.
  - Bug Ridden
    - Bug in Netscape Enterprise Server 3.6 was caused by programming bug.

2. Digital Threats

- Largely the same as other threats
  - Main difference is that it's now economical to look for very simple but hard to find holes.
- Automation is Cracker's friend
- Can defraud or steal from a distance -- presence is no longer necessary so it's safer for thief.
- Technique propagation
  - Programs can be
    - distributed to other crackers
    - combined with other programs with a GUI so skill required for theft is negligible

3. Attacks

- Criminal Attacks
- Publicity Attacks
- Legal Attacks

3. Attacks -- II

- Criminal Attacks
  - Fraud
  - Scams
  - Destructive Attacks
  - Intellectual Property Theft
  - Identity Theft
  - Brand Theft
  - Surveillance
  - Databases
  - Traffic Analysis
  - Massive Electronic Surveillance
    - ECHELON
    - CARNIVORE

3. Attacks -- III

- Publicity Attacks
  - Berkeley Students crack Netscape Navigator encryption
  - Customers may desert site that has be damaged for publicity
    - DVD security issues are an example
  - Every US Government Web Sit probably damaged
  - Denial of Service Attacks

3. Attacks -- IV

- Legal Attacks
  - Steal from Bank Account via ATM
  - Owner of Account prosecuted for fraud because bank system is secure
    - bank has no security management
    - never any external security assessment for software
    - disputed withdrawals were never investigated
    - Customer acquitted
  - Attacks using legal system are hardest to protect against

4. Adversaries

- Crackers or, in newspaper terms, hackers
- Lone Criminals
  - Trojan horse ATM
- Malicious Insiders
- Industrial Espionage
- Press
- Organized Crime
- Police
- Terrorists
- National Intelligence Organizations
- Infowarriors

5. Security Needs

- Privacy
- Multilevel Security
  - some things lightly protected
  - some things extremely heavily protected
- Anonymity
  - Commercial Anonymity
  - Medical Anonymity
- Privacy and the Government
- Authentication
- Integrity
- Audit
- Electronic Currency
- Operative Solutions