Threats to Information Systems

Providing Critical Services

New Risks and Threats

- **Vulnerability stems from easy accessibility to Infrastructures via Internet**
- **Tools to do harm are widely available and do not require a high degree of technical skills**
- **Globalization of infrastructures increases exposure to potential harm**
- **Interdependencies of systems make attack consequences harder to predict and perhaps more severe**

Our Data Represents the Best that we Have

CIA, NSA

FBI, USSS

CIAO

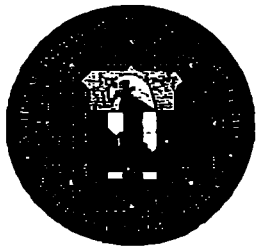
DoD

etc…….use picture instead

Goals

To Share What We Know and Don't Know about Threats to Banking and Finance Infrastructure

Enhance Relationship



Motivation

- **Ego**
- **Competitive Hacker Atmosphere**

  Ample Targets of Opportunity
- **No System is Totally Secure**
- **Low Overhead for the attacker**

  Low risk of Detection

  Low risk of reporting
- **High Potential Reward**

Typical Attack Scenario

- Identify Victim
- Exploit Internet Vulnerability
- Gain Superuser Status
- Modifies System to Hide Tracks
- Launch to other Systems
- Advertises compromised site

Challenges

- **Cyber vulnerability stems from :**
  - **Easy access to infrastructures via Internet and Public Switched Telecommunication Network**
  - **Readily available tools and recipes for new cyber weapons**
  - **Countless players with diverse motives**
  - **New cyber threats outpace defensive measures**

Countless Players with Diverse Motivations

- **Insiders**
- **Hackers / Hacktivists**
- **Organized Crime Syndicates**
- **International / Domestic Terrorists**
- **Foreign Intelligence Agencies / Industrial Spies**
- **Information Warriors**

Insiders

- **Employees, Contractors and Service Providers**

  Most dangerous and most overlooked

- **Special knowledge or access to confidential information**

  Carte blanche to wreak damage and destruction

  Self - motivated

  Personal vendetta or retaliation

Insiders

Shahuntla Devi Singla

- July 1997, former federal government employee accessed Guard personnel data systems.
- Issued commands that caused the data systems to crash
- Required over 1800 hours to recover and re-enter the lost data data
- Plead guilty to accessing a federal computer
- Sentenced to 5 months in prison and to repay $35,000 in restitution
- Demonstrated a classic "disgruntled" employee situation

Hackers

- **Individuals who break into information systems remotely using actions such as denial of service attacks, mail bombs and penetration of secure areas by subverting security measures**
  - **They attempt feats just to see if they can do it**
  - **Most visible and most reported**
  - **Unskilled to highly sophisticated**
  - **Typically motivated by ego**

Hacktivists

- **Individuals who violate computer systems to impart their political agenda through the media**
- **Highly motivated to disrupt the flow of information in an arena that is politically charged**

Hacktivists

Electronic Disturbance Theater

- Interested in electronic civil disobedience
- Focused their actions against Mexican and U.S. governments to draw attention to the plight of the Zapatistas
- Recently increased their protest activities U.S. government entities
- Lack sophistication and organization

Organized Crime

- **Moving into computer crimes as a direct source of illegal income**
- **An organized crime family set up what appeared to be a legitimate consulting firm to fix computer software glitches, but in reality, they were redirecting payments from businesses to mob - controlled accounts**
- **Exploiting the banking infrastructure by laundering drug money**

Organized Crime

Ivey James Lay

"Knightshadow"

- 1994 - Stole over 100,000 telephone calling card numbers
- Supplied these numbers to an international crime ring operating in major U.S. cities as well as in Spain and Germany
- Numbers were then sold to Europeans, who used them to make long distance calls totaling at least $50 million
- Lay was sentenced to serve 3 years and 2 months

USSS case

Unclassified

Spies

✵ Foreign Intelligence Groups & Industrial Spies

- U.S. reliance on computer networks makes us the most vulnerable

- Vulnerable to computer network exploitation across all sectors

- Availability of open source information exacerbates compromises

Social Engineering

- **Technique to verbally coerce people into revealing logins passwords to allow an intruder access to an individual's computer/network**

- **Methods include phone scams, posing as technician / fellow employee.**

- **Potential victims include switchboard operators, help desk, and computer operators**

Hacker Tools Availability

- **Internet newsgroups, web home pages, and IRC channels include**
  - **Automated attack tools**
  - **Attack methodologies**
  - **System vulnerabilities**
- **Software Tools**
  - **War Dialers (password guessing)**
  - **Sniffers (capture password / log-on)**
  - **Rootkits (mask intrusion)**
  - **Network Analyzers (SATAN)**
  - **Spoofing (smurfing)**
  - **Trojan Horses**
  - **Viruses or Logic Bombs**

Why Would Our Infrastructures be Targeted for attack?

- **National Security**
  Reduce U.S. ability to act in its own self interest

- **Public Welfare**
  Erode confidence in the critical services

- **Economic Strength**
  Damage American economic competitiveness

How Big is the Problem ?

- **1998 Computer Security Institute/FBI Study**

  - **64% of companies polled reported information system security breaches - 16% increase from 1997**

  - **Total financial losses from 241 organizations was $ 136.8M - 36% increase from 1997**

- **1997 COMDISCO survey surmises less than 50% of business have disaster recovery plans**

What Your Local FBI Agent Can Do for You ?

- Combine technical skills and investigative experience
- National and global coverage
- Apply more traditional investigative techniques
- Long-term commitment of resources
- Integration of law enforcement and national security concerns
- Pattern analysis
- Can provide deterrent effert ... even if hacker not prosecuted

What the FBI Will NOT Do !

- **Take over your system**
- **Provide information beyond your need to know**
- **Share proprietary information with competitors**
- **Become involved in civil action**
- **May not keep you advised of status of investigation**
- **Provide investigation - related information to the media**
- **Provide access to national security information/intelligence gathering techniques**
- **May not react wit the speed you want or expect**

Before Become a Victim Consider the Following

- Maintain backups of original OS software
- Maintain backups of ALL important data
- Develop a solid, well - thought out business security recovery plan ... one accepted by and involving all necessary levels of management
- Acquire some level of intrusion detection and audit capability
- Ensure audit logs turned on
- Consider "warning banner" to notify users they may be monitored
- Have key recovery/response personnel predetermined
- Routinely test system vulnerabilities
- Cancel ex-employee logins/passwords upon their termination
- Minimize number of modems on system