Cyber-Terrorism

Use of Mass Media in Today’s Info war
Safety Considerations: None
Risk Assessment Level: Low
Environmental Considerations: None
Evaluation: In class student checks and discussions.
Objective

• Action: Identify specific threats and weaknesses in regards to Cyber-Terrorism
• Conditions: Given student handouts
• Standards: Identified specific threats and weaknesses in regards to Cyber-Terrorism
Agenda

- Definitions
- History
- Types of Cyber-terrorism
- Vulnerabilities
- Counter-measures
- Summary
Cyber-Terrorism

• **Definition**: The premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by sub national groups or clandestine agents. (FBI)
Cyber-Terrorist

• **Definition:** Can be domestic or international terrorists. Cyber terrorists may be classified as such whether they solely rely on cyber terrorism to further their cause, or whether they use cyber terrorism in addition to other more conventional forms of terrorism. (FBI)
• **Cyber-utilization**: The use of on-line networks or data by terrorist organizations for supportive purposes.

• **Cyber-crime**: The deliberate misuse of digital data or information flows.
Hackers (MGM/UA, 1995)

War Games (MGM/UA, 1983)

The Net (Columbia Pictures, 1995)

Sneakers (Universal Pictures, 1992)
“My Crime is Curiosity”

• “Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for. I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all...” *The Hacker’s Manifesto, 1986.*
History of Hacking & Cyber-Terrorism
Sophistication of Cyber-Crime

- Simple Unstructured: Individuals or groups working with little structure, forethought or preparation
- Advanced Structured: Groups working with some structure, but little forethought or preparation
- Complex Coordinated: Groups working with advance preparation with specific targets and objectives.
Attack Sophistication vs. Intruder Technical Knowledge

- High Intruder Knowledge
- Low Intruder Knowledge

- Attack Sophistication
  - 1980
  - 1985
  - 1990
  - 1995
  - 2000

- Tools
  - Auto Coordinated
  - Staged

- Cross site scripting
  - "stealth" / advanced scanning techniques
  - www attacks
  - distributed attack tools
  - automated probes/scans
  - GUI

- packet spoofing
  - denial of service
  - network mgmt. diagnostics
  - GUI

- back doors
  - disabling audits
  - hijacking
  - sessions

- self-replicating code
  - password cracking
  - exploiting known vulnerabilities

- password guessing
  - burglaries

- sweepers
  - packet spoofing

- sweepers
  - denial of service

- back doors
  - network mgmt. diagnostics

- back doors
  - GUI

- back doors
  - Swing

- back doors
  - Swing

- back doors
  - Swing

- back doors
  - Swing
The First Computer?

What did it take to get from this...

Electronic Numerical Integrator and Computer (ENIAC)
...to this?

Altair 8800
Student Check

Q: What does ENIAC stand for?
A: Electronic Numerical Integrator and Computer

Q: What was the name of the world's first “micro computer”?
A: The Altair 8800
The 414 Gang, 1982

Los Alamos National Laboratory
The Morris Worm

Cornell University student Robert T. Morris
Other Acts of Cyber-Terrorism

- 1997: Hacker disabled the traffic control tower at a Mass. Airport. No accidents were caused, but service was affected.
Continued

- 2001: Treasury Dept. bank systems cracked, personal I.D. numbers accessed
Types of Cyber-Terrorism
Viruses

- Same concept as a biological virus
  - Self-replicating
  - Damages host (computer program)
  - Host then infects other applications
- Not all are destructive
- Many have delayed payload
- Some (very rare) actually improve programs
Worms

• Similar to a Virus
  – Self-replicating
  – Self-contained
    • **DOES NOT** need to be part of another program

• Deletes files from host

• Sends secure info (credit card #'s) from host to outside party

• Can severely slow down networks
Trojan Horses

• Different from viruses and worms
  – Does not attach to other files or programs
  – Does not self-replicate
  – Does not transmit on its own
    • Must be transferred & run by user deliberately

• Appears to be harmless

• Deletes files

• Reconfigures settings
Spyware

• A form of Trojan Horse
  – Does not attach to existing files
  – Does not self-replicate
  – Sends user info to outside source
  – Can reconfigure computer settings
    • Stealth dialers

• Does not damage computer, in general

• User usually never knows it is there
Spam

- Generally harmless to computer itself
- Several side effects
  - Overcrowded In-boxes
  - Pop-up windows
  - Lost time
Student Check

Q: How are viruses and worms similar?

A: They are both self-replicating.

Q: How are they different?

A: Worms don’t need to be a part of another program, viruses do.
What Are Our Vulnerabilities?
Banking Industry

• Financial ruin for individual
• Hard to reverse
• 80% of incidents go unreported
  – Bad for bank’s reputation
  – Loss of customer trust
  – Loss of business
Travel Industry

• Well trained, well motivated
  – Under right circumstances this person can do **HEAVY** damage

• Does not just apply to air travel
  – Trains as well
Financial Markets

- "United Loan Gunmen take control of NASDAQ stock market."
  - False story posted on NASDAQ Website by hacker group

- Can play on the public’s sense of fear of a crashing market
Computer Networks

• Consists of hundreds of computers
  – Big businesses and the Federal Government use networks
• One infected system can bring down a network.
• Not all viruses get caught by Anti-virus software
Student Check

Q: What percentage of computer crimes in the banking industry go unreported?  
A: 80%

True or False: The “United Loan Gunmen” took control of NASDAQ stock market.  
A: False
How Do We Stop Him?
Online Banking & Shopping

• Make sure bank/merchant takes adequate security precautions
  – Secure Sockets Layer
  – Other encryption methods
• Do research to ensure your protection
Anti-Virus Software

- Several very reliable packages available
- Different packages for different uses
- Free and easy updates available.
Persistence

• Destroy important documents
  – Shred or burn account numbers, credit card bills, bank statements, etc.

• Update anti-virus software regularly

• Don’t open strange e-mails, even from “friends”
Summary

• Definitions
• History
• Types of Cyber-terrorism
• Vulnerabilities
• Counter-measures
• Summary
Bottom Line
Questions???