# The Art of Tech Support John Abbott College

### InfoSec for Tech Support -- Part 1

M. E. Kabay, PhD, CISSP Director of Education, NCSA President, JINBU Corp

Copyright © 1997 JINBU Corp.
All rights reserved

ATS 6 - 1

# Security for Technical Support Personnel

- Basic concepts of security
- Information Warfare
- Hardware security
- Software security
- Communications security
- Problems for People
- Operations Security
- Solutions

ATS 6 - 2

#### **Definitions**

Classical definitions

- "Protection of information from unauthorized or accidential modification, destruction and disclosure."
- C I A: "InfoSec protects confidentiality, integrity and availability of data."

ATS 6 - 3

#### **Definitions (cont'd)**

Donn B. Parker's Hexad

- Confidentiality and possession
- Integrity and authenticity
- Availability and utility



ATS 6 - 4

#### Confidentiality

Restricting access to data

- Protecting against unauthorized disclosure of existence of data
  - E.g., allowing industrial spy to deduce nature of clientele by looking at directory names
- Protecting against unauthorized disclosure of details of data
  - E.g., allowing 13-yr old girl to examine HIV+ records in Florida clinic



Possession

Control over information

- Preventing physical contact with data
  - E.g., case of thief who recorded ATM PINs by radio (but never looked at them)
- Preventing copying or unauthorized use of intellectual property
  - E.g., violations by software pirates

ATS 6 - 6



#### Integrity

Internal consistency, validity, fitness for use

- Avoiding physical corruption
  - E.g., database pointers trashed or data garbled
- Avoiding logical corruption
  - E.g., inconsistencies between order header total sale & sum of costs of details

ATS 6 - 7



#### **Authenticity**

Correspondence to intended meaning

- Avoiding nonsense
  - E.g., part number field actually contains cost
- Avoiding fraud
  - E.g., sender's name on e-mail is changed to someone else's



ATS 6 - 8

#### **Availability**

Timely access to data

- Avoid delays
  - E.g., prevent system crashes & arrange for recovery plans
- Avoid inconvenience
  - E.g., prevent mislabelling of files



ATS 6 - 9

#### Utility

Usefulness for specific purposes

- Avoid conversion to less useful form
  - E.g., replacing dollar amounts by foreign currency equivalent
- Prevent impenetrable coding
  - E.g., employee encrypts source code and "forgets" decryption key



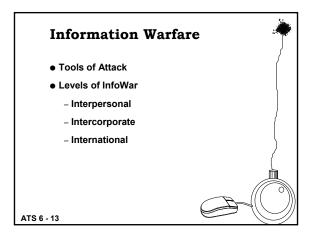
ATS 6 - 10

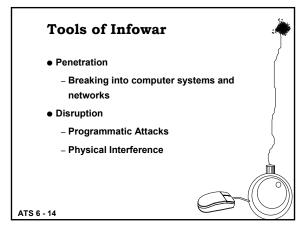
# Rough Guesses About Damage to Computer Systems & Data Fire Water Dishonest Outsider ATS 6 - 11

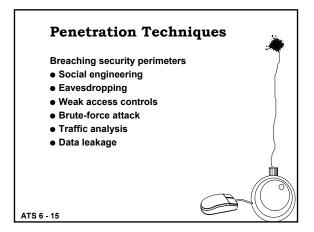
Take detailed notes on the following video and submit a onepage or longer summary covering the six case studies and what lesson you learned from each. Submit your report as part of your homework.

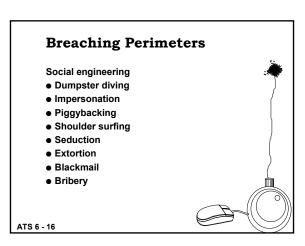
# VIDEO: Locking the Door

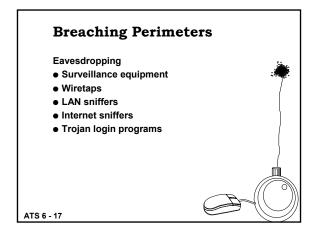
Commonwealth Films Boston, MA

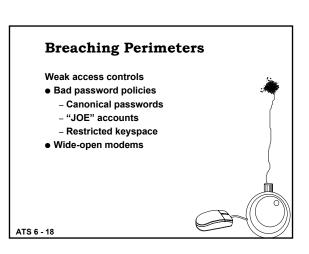


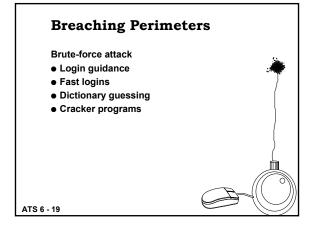


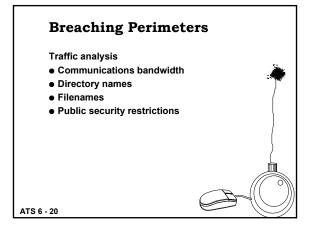


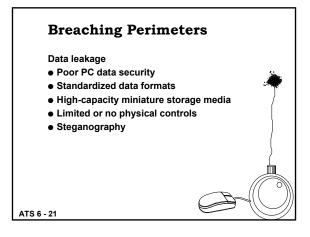


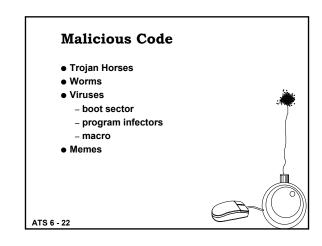


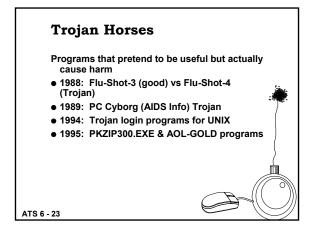


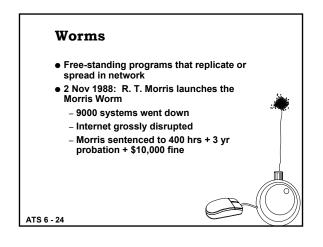


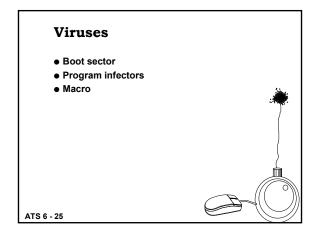


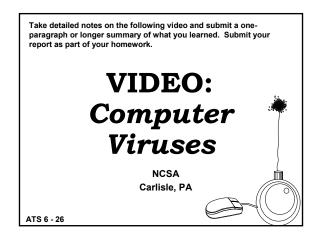


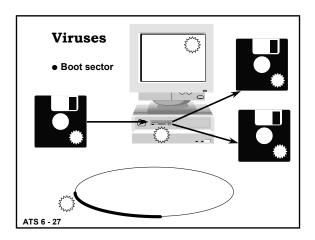


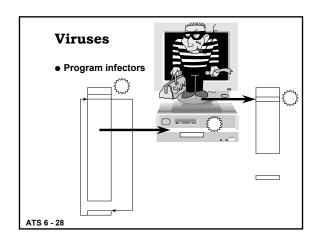


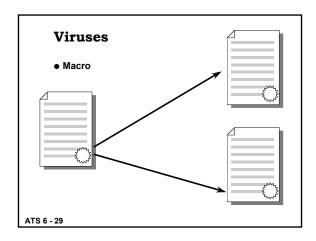




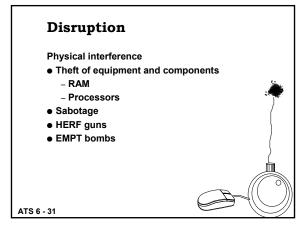


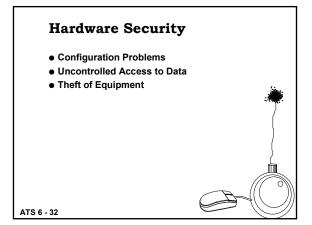


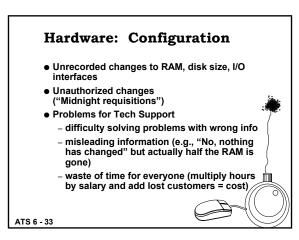


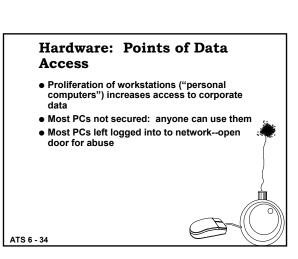




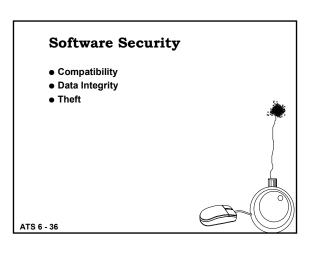








#### 



#### Software: Compatibility

- . Many different software tools in use
- Each has different schedule of patches, upgrades and new versions
- Major logistics nightmare to keep all systems up to date
- Incompatibilities lead to difficulties
  - persistence of tech support problems that have been solved by new versions
  - interference with problem solution because of faulty assumptions about
  - repeated extra work to convert files for interchange among users

ATS 6 - 37

#### **Software: Data Integrity**

- Errors creep into data during data entry
  - people don't verify their data
  - do not permit transcription of data
- Multiple copies of data tend to diverge
  - e.g., spreadsheets may use data from different dates
  - can cause embarrassment and serious error
- Accidental errors can change information
- Deliberate damage to data by angry employees or by outsiders

ATS 6 - 38



- Intellectual property rights frequently violated
- Software purchased from vendor is usually a license to use a specific number of copies in a particular way on particular machines
- Making copies without authorization is potentially a felony (jail time)
- Upgrades to existing copies do not entitle licensee to give away or sell copies of previous version
- More on this topic in section on Ethics

ATS 6 - 39

#### **Communications Security**

- Non-encrypting LANS
  - sniffers pick up data in the clear
- Modems
  - don't usually encrypt data
  - provide uncontrolled
  - disable auto-answer until required
- Wireless technology broadcasts data
  - radio
  - cellular
  - fundamentally insecure

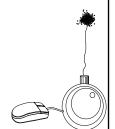
**Internet: Sniffing** 

ATS 6 - 40

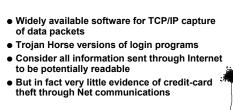


#### **Internet Security**

- Sniffing
- Spoofing
- Denial of Service
- Attacks on Web Sites



ATS 6 - 42





#### **Internet: Spoofing**

Anonymity and pseudonymity account for most problems on the Net

- No requirement at present for strong identification and authentication
- Many ISPs allow pseudonyms for e-mail
- Often impossible to track down anonymous or pseudonymous abusers of the Net
- Criminal hackers almost universally use pseudonyms
- Some criminal hackers and some spammers alter e-mail headers

ATS 6 - 43

#### **Internet: Denial of Service**

Serious problem facing the Net

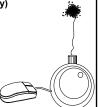
- Mail-bombing (e.g., vs Canter & Siegel)
- USENET subscription bombing (e.g, Johnny [X]chaotic)
- Syn-flooding (e.g., PANIX)
- JAVA and JAVAscript bugs (e.g., multiple windows page)
- ActiveX bugs (e.g., crashing Windows95)



ATS 6 - 44

## Internet: Attacks on Web Sites

- Vandals deface public Web pages
- Poor security over files
- Recent highly-publicized cases:
  - Department of Justice (swastikas, porn)
  - CIA (Central Stupidity Agency)
- Political sites at risk



ATS 6 - 45

#### **Problems for People**

- Multiple systems
- Multiple logons
- Multiple passwords
- Lack of coordination
- Corporature culture vs politeness



ATS 6 - 46

#### **Operations Security**

- Version control--see above in Software Compatibility
- License control--see above in Software Theft
- Audit trails--need to track access and changes
- Quality control--verify that programs working as planned



ATS 6 - 47

#### Homework: Readings in Wilson's text

- Read Chapter 7, "A User's Guide to Tech Support" and prepare a summary of the key points in this chapter
- Answer all the review questions from the instructor
- Submit your chapter summaries, video summaries (2) and review questions after the quiz at the start of lecture 7

ATS 6 - 49		