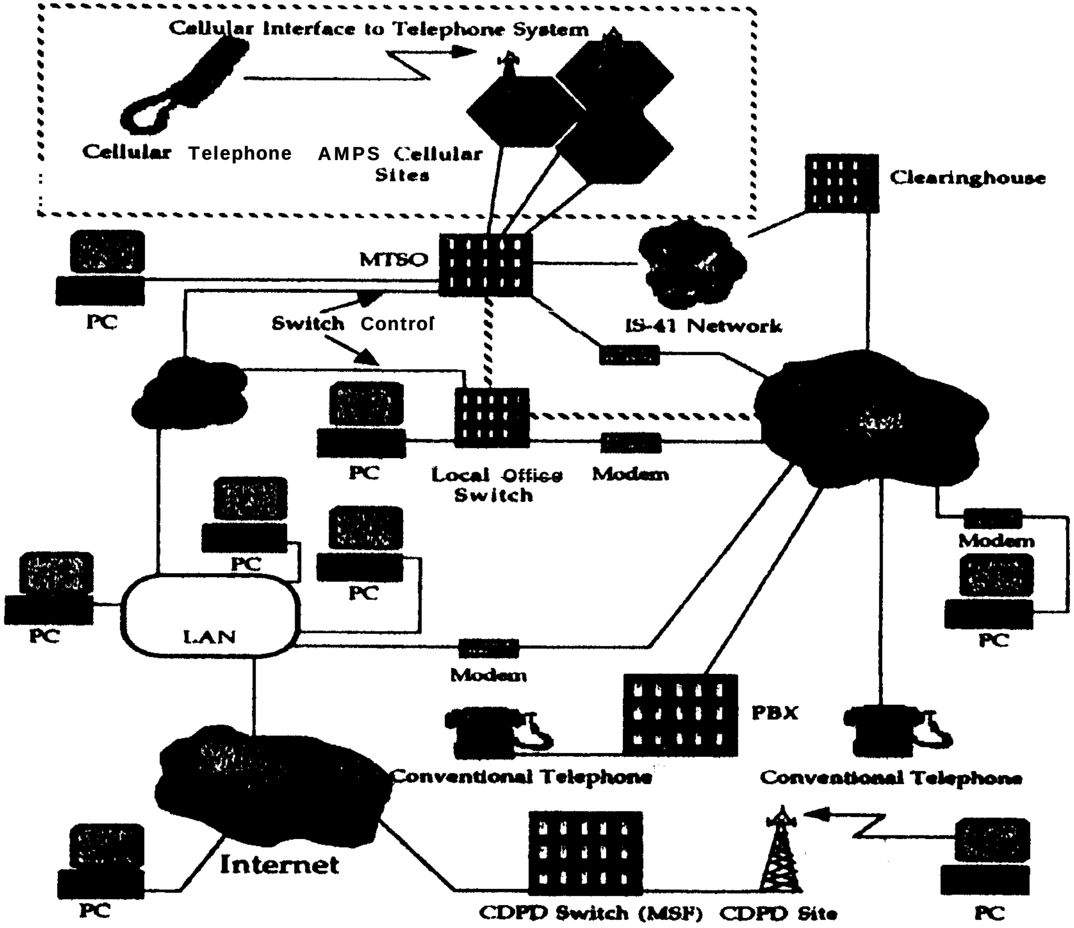
Attacks on Cellular Systems

Robert A. McKosky, Ph.D., CISSP
Chris Carroll, Co-Principal Investigator
Hai-Ping Ko, Ph.D. (Speaker)

November 13, 1996

Overview


Cellular Interface to Telephone System
Cellular Telephone
AMPS Cellular Sites
Clearinghouse
MTSO
PC
Switch Control
IS-41 Network
PC
Local Office Switch
Modem
PC
PC
Modem
PC
LAN
PC
Modem
PBX
Conventional Telephone
Conventional Telephone
Internet
PC
CDPD Switch (MSF)
CDPD Site
PC

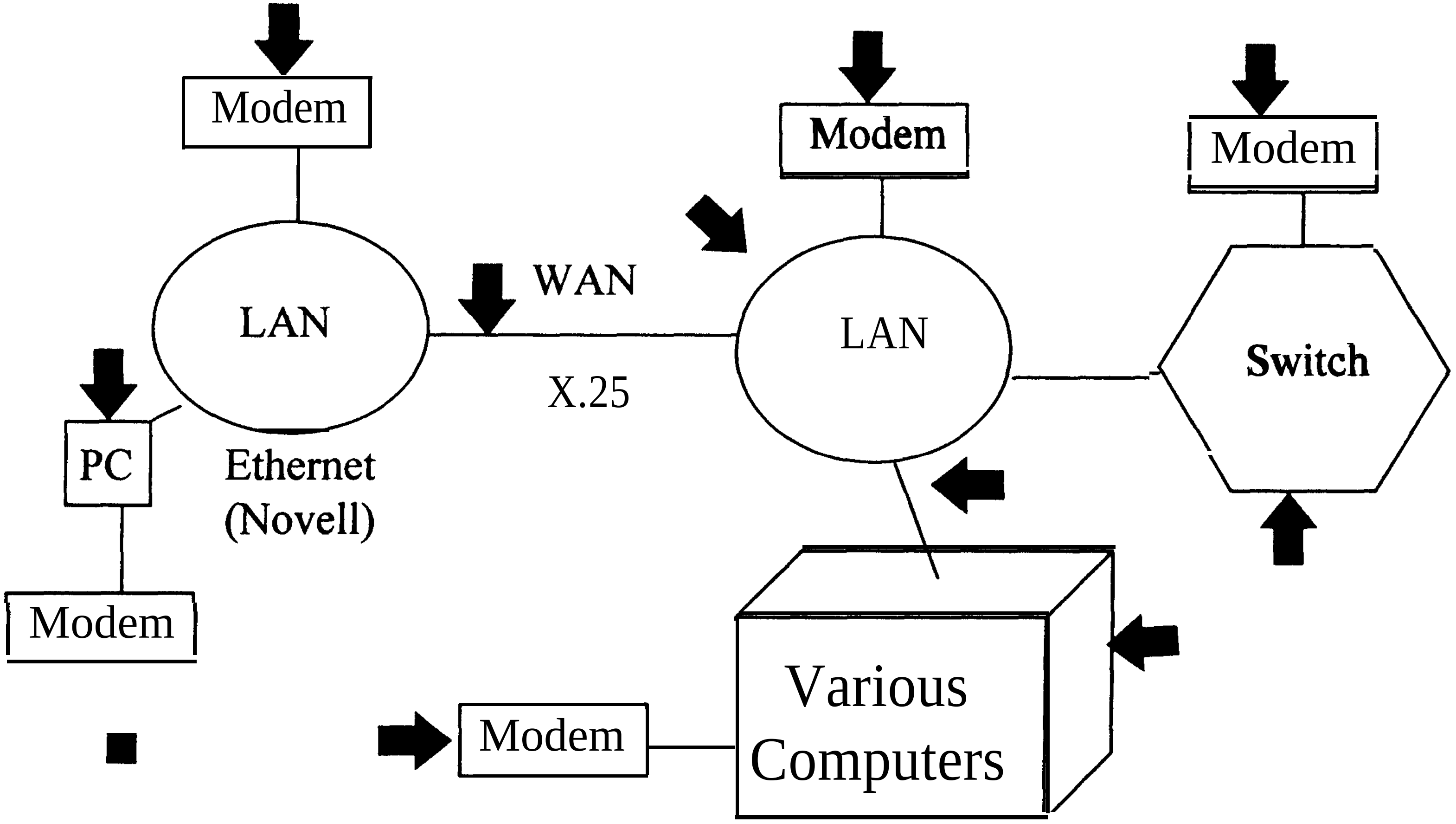
Types of Attack

- $600M Loss Per Year -

- Air
  - Human Fraud or Hijack
  - Clone (Tumbling, Simple, Tumbler)
    - ESN (Electronic Serial Number)
    - MIN (Mobile Identification Number)
- Land
  - Network Attack on Multiple Points
    - Switch
    - Modem, LAN, WAN, PC, various computers

Attack Points

⬇ Indicated possible point of attack



Land Tiger Team Results

- remote access to the switch computer
  - obtained /etc/passwd, MINs/EINs, billing, ...
- physical access to offices, computer room,...
- beat SecureID
- clone phone
- Trojan Horse on a PC
- NOT DETECTED

Comments

- "Our biggest problem is the access from the business systems."
- "Our biggest problem is access from personal modems."
- "We try to do a good job here of controlling access, but other areas of the company are not as conscientious."

Comments (Cont.)

- “I don’t know who I would call if we had a security problem.”
- “Nobody looks at the log on a regular basis.”
- “We only look at the logs when we think there has been a problem.”
- “I didn’t know you could do that!”

Comments ...

- "The modem thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than a bomb . . . To date, we have been remarkably lucky . . . (A)s far as we can tell, there has been no systematic attempt to subvert any of our critical computing systems. Unfortunately, there is reason to believe that our luck will soon run out."
  - National Research Council, 199 l

- "Neither AT&T, nor the local exchange telephone companies, nor anyone else can tell you what is connected to the public network fabric today."
  - John C. Wohlstetter, 1993

- "If [senior management] really understood the potential liability and the potential risks to corporate assets and to their reputations, they might shut down all networks and computer centers."
  - Kenneth Weiss, chairman of the computer security division of the American Defense Preparedness Association

Solutions (Partial)

- Air
  - Authentication, Encryption, Clone Detection
- Land
  - Security Owner
  - Security Policy
  - Training
  - Enhanced Audit
  - Encryption