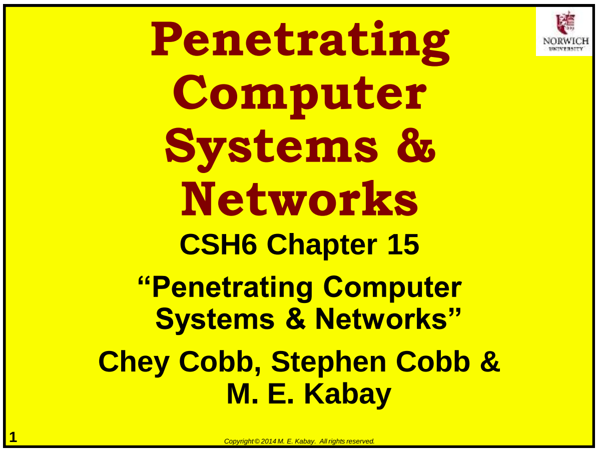


Penetrating Computer Systems & Networks

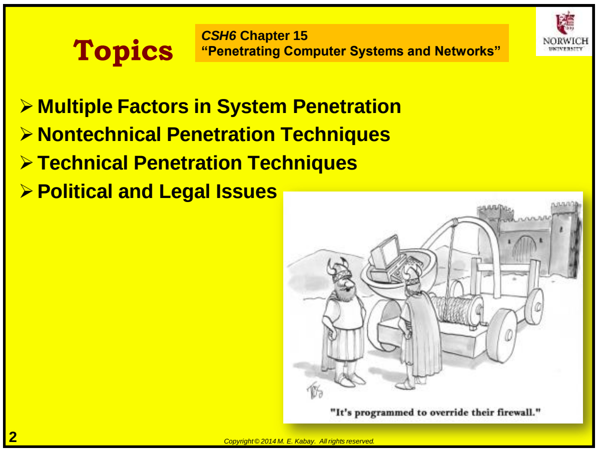
CSH6 Chapter 15

"Penetrating Computer Systems & Networks"

Chey Cobb, Stephen Cobb & M. E. Kabay

1

Copyright © 2014 M. E. Kabay. All rights reserved.



Topics

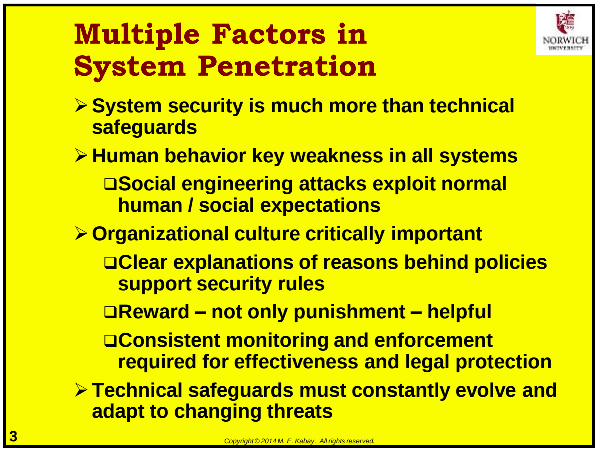
CSH6 Chapter 15
"Penetrating Computer Systems and Networks"

- Multiple Factors in System Penetration
- Nontechnical Penetration Techniques
- Technical Penetration Techniques
- Political and Legal Issues

"It's programmed to override their firewall."

2

Copyright © 2014 M. E. Kabay. All rights reserved.

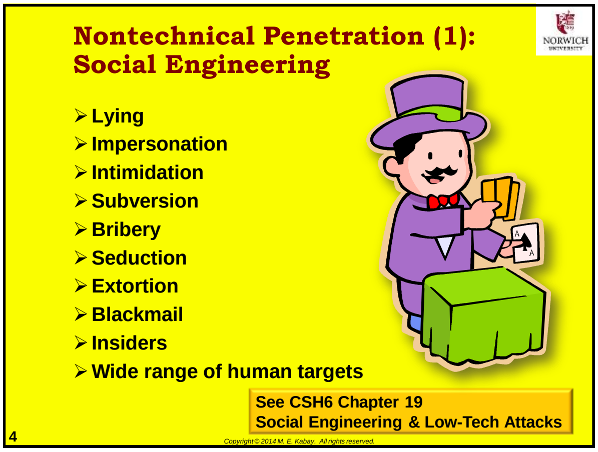


Multiple Factors in System Penetration

- System security is much more than technical safeguards
- Human behavior key weakness in all systems
  - ❑Social engineering attacks exploit normal human / social expectations
- Organizational culture critically important
  - ❑Clear explanations of reasons behind policies support security rules
  - ❑Reward – not only punishment – helpful
  - ❑Consistent monitoring and enforcement required for effectiveness and legal protection
- Technical safeguards must constantly evolve and adapt to changing threats

3

Copyright © 2014 M. E. Kabay. All rights reserved.



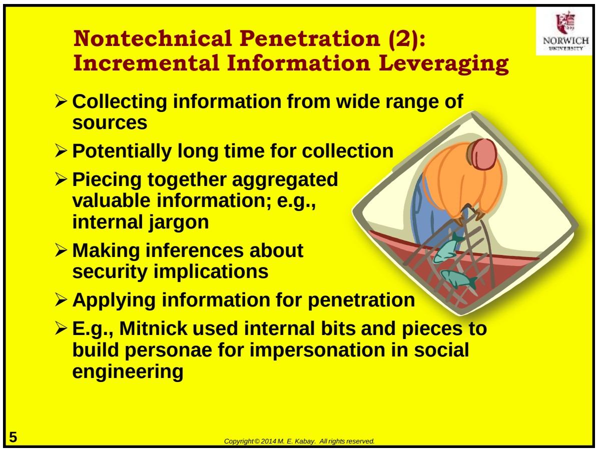
Nontechnical Penetration (1): Social Engineering

- Lying
- Impersonation
- Intimidation
- Subversion
- Bribery
- Seduction
- Extortion
- Blackmail
- Insiders
- Wide range of human targets

See CSH6 Chapter 19
Social Engineering & Low-Tech Attacks

4

Copyright © 2014 M. E. Kabay. All rights reserved.

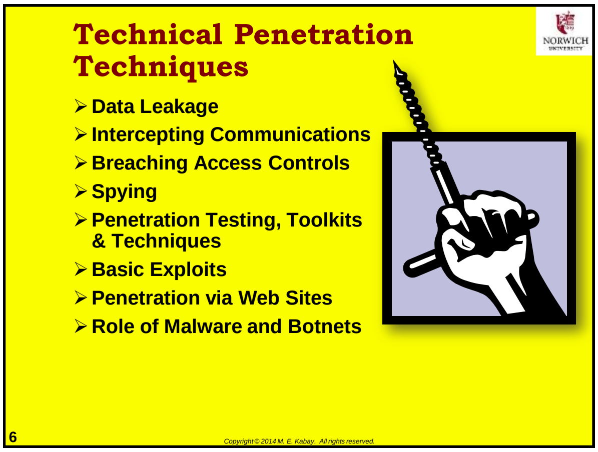


Nontechnical Penetration (2): Incremental Information Leveraging

- Collecting information from wide range of sources
- Potentially long time for collection
- Piecing together aggregated valuable information; e.g., internal jargon
- Making inferences about security implications
- Applying information for penetration
- E.g., Mitnick used internal bits and pieces to build personae for impersonation in social engineering

5

Copyright © 2014 M. E. Kabay. All rights reserved.



Technical Penetration Techniques

- Data Leakage
- Intercepting Communications
- Breaching Access Controls
- Spying
- Penetration Testing, Toolkits & Techniques
- Basic Exploits
- Penetration via Web Sites
- Role of Malware and Botnets

6

Copyright © 2014 M. E. Kabay. All rights reserved.

Data Leakage

- Definition:
  - ❑ Imperceptible transfer of data without authorization
  - ❑ Concealed, hard-to-detect copying or transmission of confidential data using *covert channels*
  - ❑ Alternative channels can be entirely independent of normal system (e.g., photography, human memory)
  - ❑ Impossible to stop transfer of information from secure to non-secure region
  - ❑ E.g., encrypted messaging, steganography
- Data loss from lost / stolen unencrypted portable devices
- Copying to portable devices (laptops, USB flash drives, CDs, DVDs, iPods….)

Copyright © 2014 M. E. Kabay. All rights reserved.

Intercepting Communications

- Transmission Media
- Protocols
- Applications

Copyright © 2014 M. E. Kabay. All rights reserved.

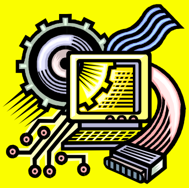
Transmission Media

- Asynchronous links
- Microwave
- Leased lines
- Fiber optics
- Satellites
- Emanations

Copyright © 2014 M. E. Kabay. All rights reserved.

Asynchronous Links

- Easy to tap
  - ❑ Twisted-pair accessible via alligator clips, splices
  - ❑ Most cabling clearly labeled, identifiable
  - ❑ Wiring closets, patch panels unlocked
- Defenses
  - ❑ Shielded cables
  - ❑ Locked cabinets
  - ❑ Encryption of data stream



Copyright © 2014 M. E. Kabay. All rights reserved.

Microwave

- Predominant method for long-distance phone lines
  - ❑ 2/3 phone calls
  - ❑ Line-of-sight: towers spaced every 25 miles
  - ❑ Vulnerable to denial-of-service attacks (topple towers)
- Footprint expands over distance
  - ❑ Can intercept data, decode using standard equipment
  - ❑ But volume of high-bandwidth lines makes specific taps difficult
- Encryption the only protective mechanism

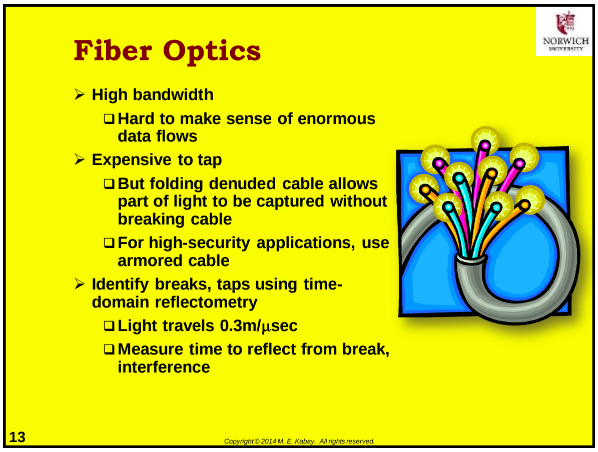
Copyright © 2014 M. E. Kabay. All rights reserved.

Leased Lines

- Phone lines normally switched
- Can fix circuit in place, improve quality
- Used for critical, high-volume data communications
- Increased vulnerability to tapping
- Beware *off-premises extension*
  - ❑ Easy to order extension without authorization
  - ❑ Use phone services of victim without paying
  - ❑ Check your phone bills for unauthorized extensions

Copyright © 2014 M. E. Kabay. All rights reserved.

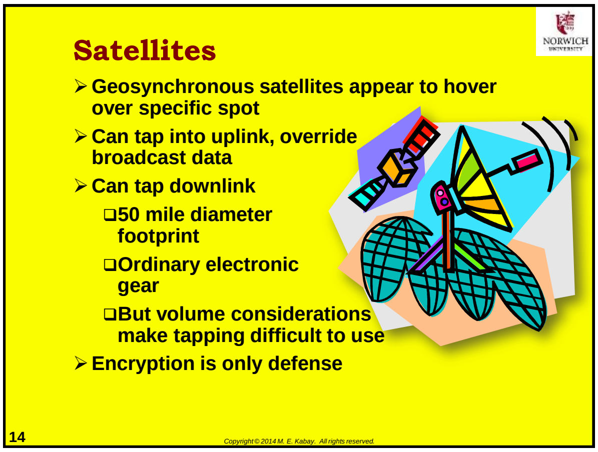
Copyright © 2014 M. E. Kabay *All rights reserved.*



Fiber Optics

- High bandwidth
  - Hard to make sense of enormous data flows
- Expensive to tap
  - But folding denuded cable allows part of light to be captured without breaking cable
  - For high-security applications, use armored cable
- Identify breaks, taps using time-domain reflectometry
  - Light travels 0.3m/µsec
  - Measure time to reflect from break, interference

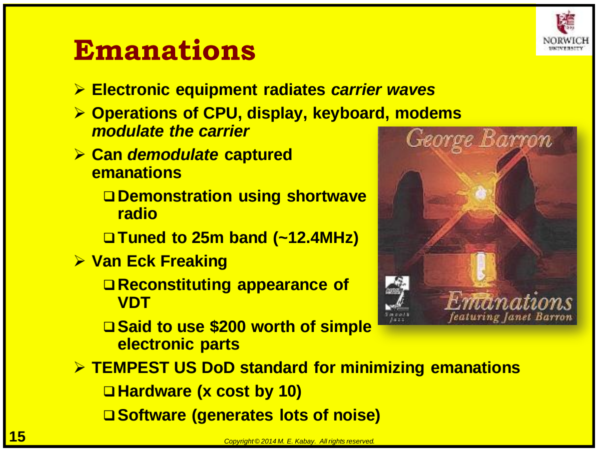
13 Copyright © 2014 M. E. Kabay. All rights reserved.



Satellites

- Geosynchronous satellites appear to hover over specific spot
- Can tap into uplink, override broadcast data
- Can tap downlink
  - 50 mile diameter footprint
  - Ordinary electronic gear
  - But volume considerations make tapping difficult to use
- Encryption is only defense

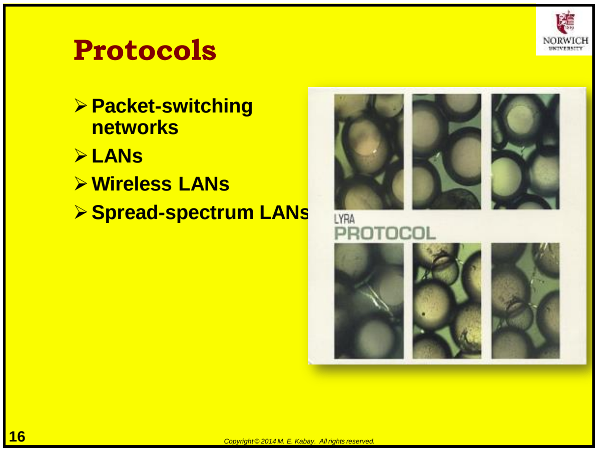
14 Copyright © 2014 M. E. Kabay. All rights reserved.


George Barron
Emanations
featuring Janet Barron

Emanations

- Electronic equipment radiates *carrier waves*
- Operations of CPU, display, keyboard, modems *modulate the carrier*
- Can *demodulate* captured emanations
  - Demonstration using shortwave radio
  - Tuned to 25m band (~12.4MHz)
- Van Eck Freaking
  - Reconstituting appearance of VDT
  - Said to use $200 worth of simple electronic parts
- TEMPEST US DoD standard for minimizing emanations
  - Hardware (x cost by 10)
  - Software (generates lots of noise)

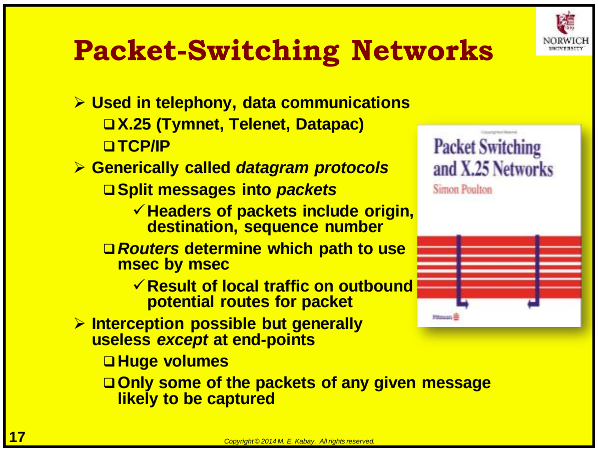
15 Copyright © 2014 M. E. Kabay. All rights reserved.


LYRA
PROTOCOL

Protocols

- Packet-switching networks
- LANs
- Wireless LANs
- Spread-spectrum LANs

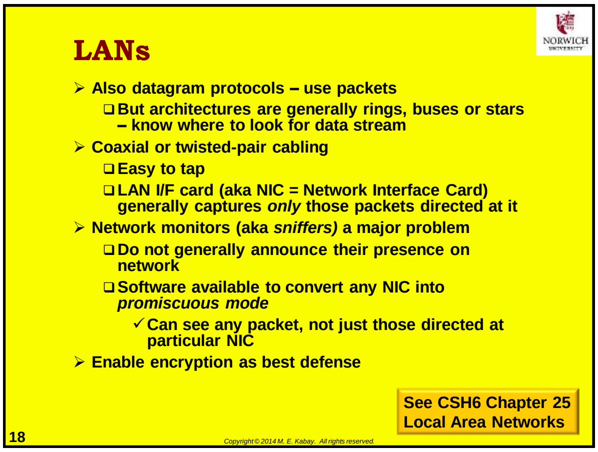
16 Copyright © 2014 M. E. Kabay. All rights reserved.


Packet Switching and X.25 Networks
Simon Poulton
Pitman

Packet-Switching Networks

- Used in telephony, data communications
  - X.25 (Tymnet, Telenet, Datapac)
  - TCP/IP
- Generically called *datagram protocols*
  - Split messages into *packets*
    - ✓ Headers of packets include origin, destination, sequence number
  - *Routers* determine which path to use msec by msec
    - ✓ Result of local traffic on outbound potential routes for packet
- Interception possible but generally useless *except* at end-points
  - Huge volumes
  - Only some of the packets of any given message likely to be captured

17 Copyright © 2014 M. E. Kabay. All rights reserved.

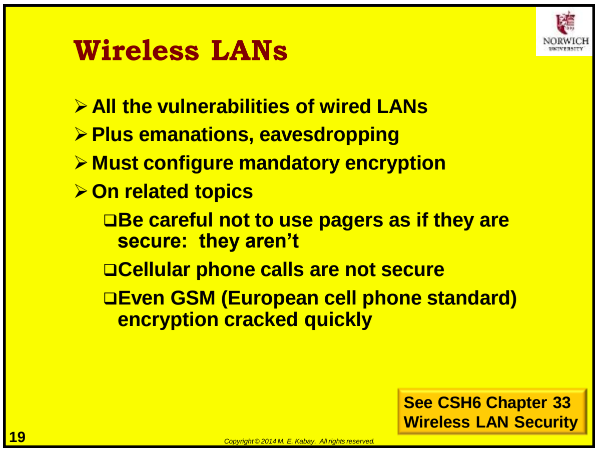


LANs

- Also datagram protocols – use packets
  - But architectures are generally rings, buses or stars – know where to look for data stream
- Coaxial or twisted-pair cabling
  - Easy to tap
  - LAN I/F card (aka NIC = Network Interface Card) generally captures *only* those packets directed at it
- Network monitors (aka *sniffers)* a major problem
  - Do not generally announce their presence on network
  - Software available to convert any NIC into *promiscuous mode*
    - ✓ Can see any packet, not just those directed at particular NIC
- Enable encryption as best defense

See CSH6 Chapter 25
Local Area Networks

18 Copyright © 2014 M. E. Kabay. All rights reserved.



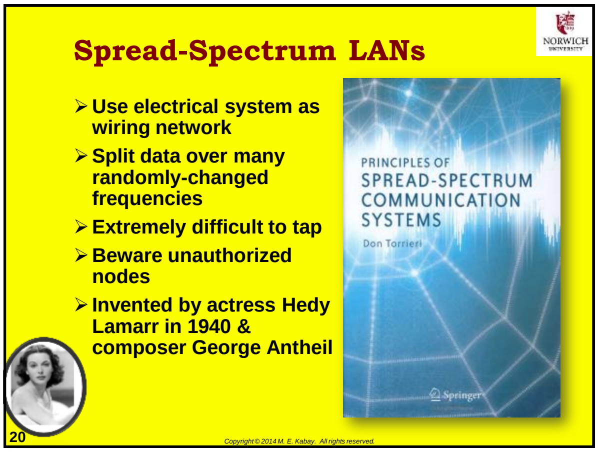
Wireless LANs

- All the vulnerabilities of wired LANs
- Plus emanations, eavesdropping
- Must configure mandatory encryption
- On related topics
  - ❑Be careful not to use pagers as if they are secure: they aren't
  - ❑Cellular phone calls are not secure
  - ❑Even GSM (European cell phone standard) encryption cracked quickly

See CSH6 Chapter 33
Wireless LAN Security

19

Copyright © 2014 M. E. Kabay. All rights reserved.

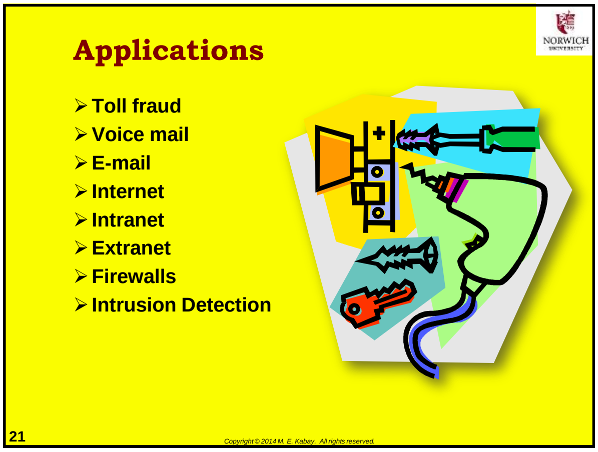

PRINCIPLES OF
SPREAD-SPECTRUM
COMMUNICATION
SYSTEMS
Don Torrieri
Springer

Spread-Spectrum LANs

- Use electrical system as wiring network
- Split data over many randomly-changed frequencies
- Extremely difficult to tap
- Beware unauthorized nodes
- Invented by actress Hedy Lamarr in 1940 & composer George Antheil

20

Copyright © 2014 M. E. Kabay. All rights reserved.

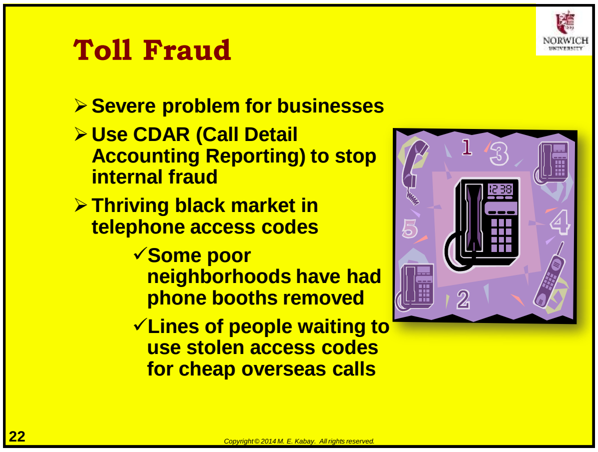


Applications

- Toll fraud
- Voice mail
- E-mail
- Internet
- Intranet
- Extranet
- Firewalls
- Intrusion Detection

21

Copyright © 2014 M. E. Kabay. All rights reserved.

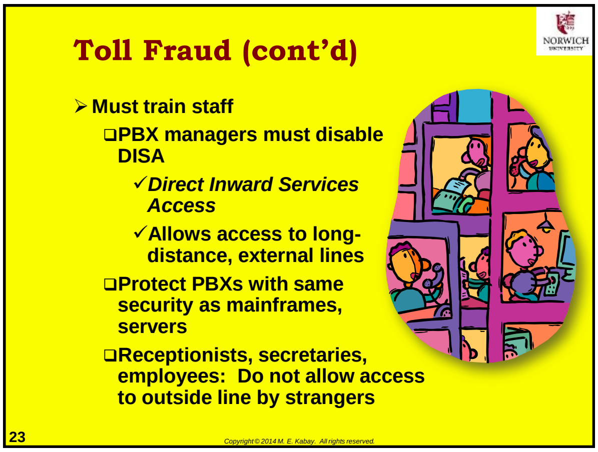


Toll Fraud

- Severe problem for businesses
- Use CDAR (Call Detail Accounting Reporting) to stop internal fraud
- Thriving black market in telephone access codes
  - ✓Some poor neighborhoods have had phone booths removed
  - ✓Lines of people waiting to use stolen access codes for cheap overseas calls

22

Copyright © 2014 M. E. Kabay. All rights reserved.

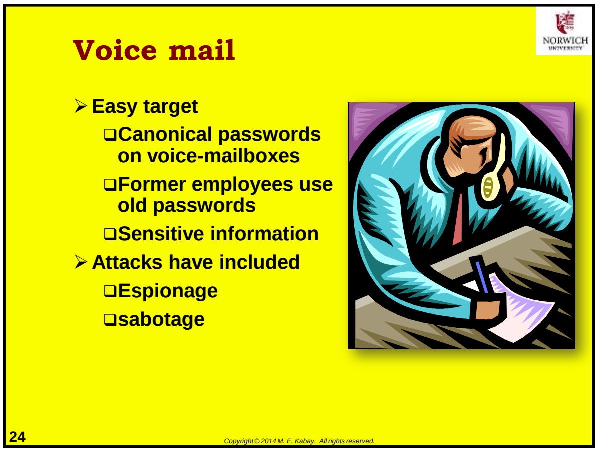


Toll Fraud (cont'd)

- Must train staff
  - ❑PBX managers must disable DISA
    - ✓*Direct Inward Services Access*
    - ✓Allows access to long-distance, external lines
  - ❑Protect PBXs with same security as mainframes, servers
  - ❑Receptionists, secretaries, employees: Do not allow access to outside line by strangers

23

Copyright © 2014 M. E. Kabay. All rights reserved.



Voice mail

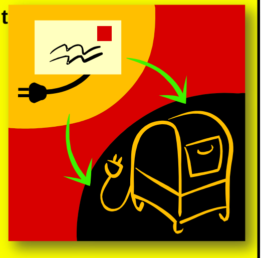
- Easy target
  - ❑Canonical passwords on voice-mailboxes
  - ❑Former employees use old passwords
  - ❑Sensitive information
- Attacks have included
  - ❑Espionage
  - ❑sabotage

24

Copyright © 2014 M. E. Kabay. All rights reserved.

E-mail

- Primary problem is concept of privacy
- Generally e-mail is difficult to intercept in transit
- Loss of control over published information
- Damage to organization's reputation
- Waste of time if uncontrolled

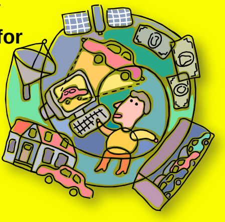


25

Copyright © 2014 M. E. Kabay. All rights reserved.

Internet

- Most important communications component for most organizations today
  - ❑Intranet: TCP/IP network for internal use
  - ❑Extranet: TCP/IP network for clients or partners
- Highly vulnerable
  - ❑IPv4 has no packet authentication – therefore spoofing easy
  - ❑Many weaknesses in software

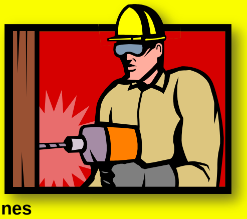


26

Copyright © 2014 M. E. Kabay. All rights reserved.

Penetration Tools

- Almost all successful attacks exploit known vulnerabilities
  - ❑Most vulnerabilities used have been known for years
- Port & vulnerability scanners
- Buffer overflow exploits very common
- *War dialers* used to be important to locate modem lines
- Brute-force *password crackers* useful if system allows access to password file for offline testing
- Rainbow tables store precalculated encrypted values for testing against password files

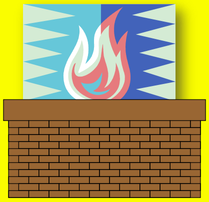


27

Copyright © 2014 M. E. Kabay. All rights reserved.

Firewalls

- Key component of today's security architecture
- Devices that filter inbound and outbound packets
- Apply rules reflecting *policy*
- Useless to install firewall without policy – generally pass-through



See CSH6 Chapter 26
Gateway Security Devices

28

Copyright © 2014 M. E. Kabay. All rights reserved.

Intrusion Detection

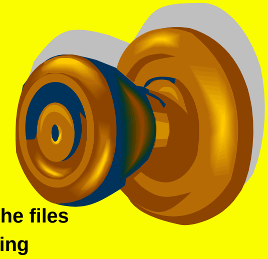
- No security perimeter should be expected to reach perfection
- Must be able to spot intrusions quickly
- Essential component of effective security
- Allows measured, planned response
  - ❑Stop or monitor, collect evidence
  - ❑Valuable in forensic work

29

Copyright © 2014 M. E. Kabay. All rights reserved.

Breaching Access Controls

- Brute-force attacks
- Demon (war) dialing
- Exhaustive search
- Keyspace issues
- Login speed
- Scavenging RAM
- Scavenging swap & cache files
- Dictionary-based guessing
- Stealing
- Scavenging (including discarded media)

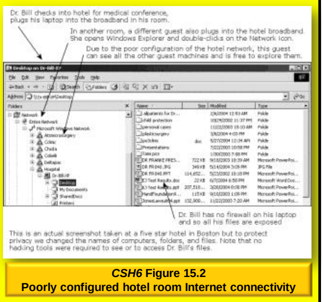


30

Copyright © 2014 M. E. Kabay. All rights reserved.

Spying

- Laser interferometry (bouncing lasers off windows)
- Shoulder surfing
- War-driving
- Keyloggers
- Exploiting insecure public networks (e.g., hotels) – see Fig 15.2



Dr. Bill checks into hotel for medical conference, plugs his laptop into the broadband in his room.

In another room, a different guest also plugs into the hotel broadband. She opens Windows Explorer and double-clicks on the Network icon.

Due to the poor configuration of the hotel network, this guest can see all the other guest machines and is free to explore them.

Dr. Bill has no firewall on his laptop and so all his files are exposed

This is an actual screenshot taken at a five star hotel in Boston but to protect privacy we changed the names of computers, folders, and files. Note that no hacking tools were required to see or to access Dr. Bill's files.

CSH6 Figure 15.2
Poorly configured hotel room Internet connectivity

Penetration Testing, Toolkits & Techniques

- System administrators and security experts commonly use vulnerability analysis and automated penetration tools to test system security
  - ❑So do criminal hackers
- Scanners serve several functions
  - ❑Laying out network architecture
  - ❑Determining which protocols are in use
  - ❑Mapping firewall rule sets
  - ❑Determining which operating systems are in use

Basic Exploits (1)

- Buffer Overflow
  - ❑Most common exploit of poor coding
  - ❑Insert data beyond expected end of input
  - ❑Interpret extra data as instructions
- Password Cracking
  - ❑Steal encrypted password file
  - ❑Run crack program on other computer
  - ❑Or try rainbow tables of predetermined passwords vs one-way encrypted codes

Image from http://bildbevis.se/images/20060112000555_overflow.jpg used with kind permission of author

Basic Exploits (2)

- Rootkits
  - ❑Once system has been cracked, apply *rootkit*
  - ❑Ensures that criminal can re-enter system at will
  - ❑Installs a backdoor
  - ❑Hides itself from discovery (invisible, wipes log records….)
- Trojan Code: often part of rootkits
- Back Doors: beware utilities that have been converted to Trojans with back doors

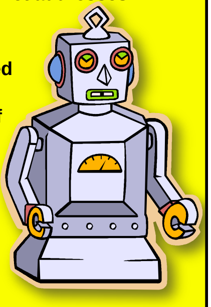
Penetration via Web Sites

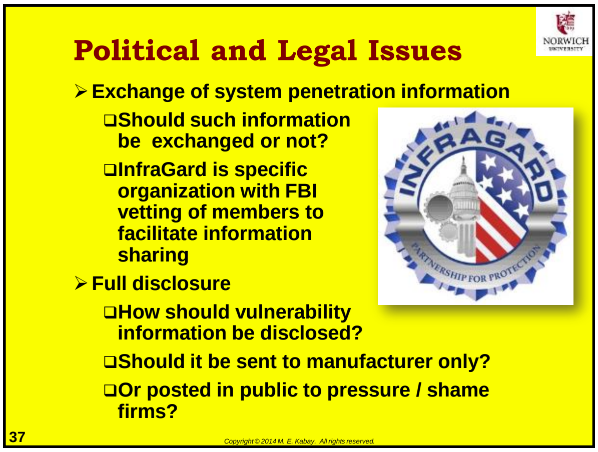
- Many Web sites are interactive: receive user input such as name, e-mail address etc.
- Attackers enter long or random inputs ("fuzzing") to see what happens
- Can cause buffer overflows and improper actions by Web server ("executing arbitrary code")
- Use of special characters in input strings (.., /, \, metacharacters)
- Server-side includes – special commands interpreted by Web server – including *exec* for execution of code

See CSH6 Chapter 21
Web-Based Vulnerabilities

Role of Malware and Botnets

- Viruses and worms may communicate confidential data to external Internet addresses
- Bots are malware that wait for instructions from controllers
- Botnets are collections of infected computers
- Botmasters can tell thousands of infected computers to launch attacks (especially DDoS)
- Google research suggests that 10% of all Web pages are infected with malware that can infect target computer upon viewing



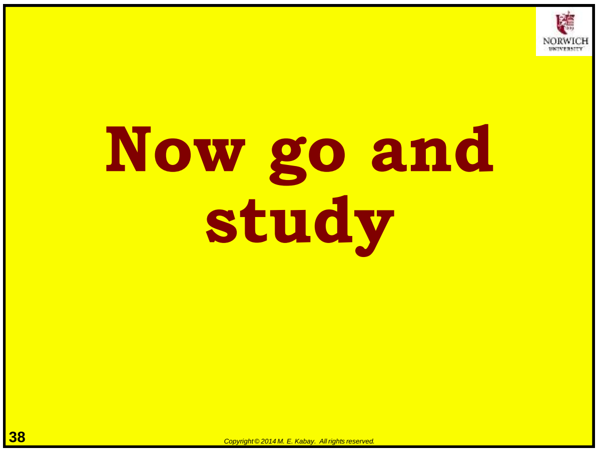

INFRAGARD
PARTNERSHIP FOR PROTECTION

Political and Legal Issues

- Exchange of system penetration information
  - ❑Should such information be exchanged or not?
  - ❑InfraGard is specific organization with FBI vetting of members to facilitate information sharing
- Full disclosure
  - ❑How should vulnerability information be disclosed?
  - ❑Should it be sent to manufacturer only?
  - ❑Or posted in public to pressure / shame firms?

37

Copyright © 2014 M. E. Kabay. All rights reserved.



Now go and study

38

Copyright © 2014 M. E. Kabay. All rights reserved.