Local Area Networks

CSH6 Chapter 25

"Local Area Networks"

Gary C. Kessler & N. Todd Pritsky
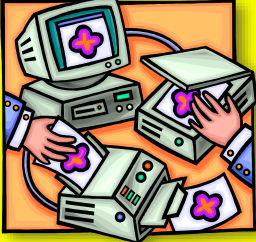
Topics

- **Policy and Procedures**
- **Physical Site Security**
- **Physical Layer**
- **Network Operating System Issues**

Chapter 25 should be read in conjunction with Chapter 24 on Operating System Security. Chapter 25 includes commentary on operating systems commonly used on workstations configured on LANs.

Policy and Procedures

- **Without framework of policy and procedures, technology cannot be selected appropriately**
- **Extensive list of suggestions available in many texts and online**
  - **Many chapters in *CSH6***

  - **RFC 2196:**
    Site Security Handbook
- **http://www.ietf.org/rfc/rfc2196.txt**

Physical Site Security

- **Physical access to LAN equipment is the single most dangerous vector for attack**
- **Protect equipment and transmission media against physical damage**
  - **Accident**
  - **Intentional attack**
  - **Denial of service**

    See *CSH6* Chapters 22 and 23

- **Business continuity planning & disaster recovery planning**
  - **Require consideration of networks**

    See *CSH6* Chapters 58 and 59

Physical Layer Issues

- **ISO OSI Model**
- **Sniffers and Broadcast LANs**
- **Attacks on the Physical Plant**
- **Modems, Dial-Up Servers, Telco**
- **Wireless LANs**
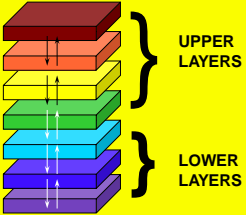
ISO OSI* Model

The 7 layers

- **Application (7)**
- **Presentation (6)**
- **Session (5)**
- **Transport (4)**
- **Network (3)**
- **Data Link (2)**
- **Physical (1)**

UPPER LAYERS

LOWER LAYERS

*International Organization for Standards Open System Interconnect

OSI Data Transfer

OUTPUT   **INPUT**

IBM's TCP/IP Redbook

http://www.redbooks.ibm.com/pubs/pdfs/redbooks/gg243376.pdf
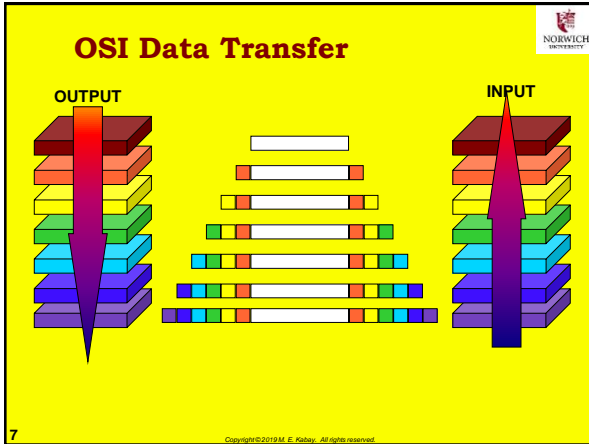
Part I. Core TCP/IP protocols
- Chapter 1. Architecture, history, standards, and trends
- Chapter 2. Network interfaces
- Chapter 3. Internetworking protocols
- Chapter 4. Routing protocols
- Chapter 5. Transport layer protocols
- Chapter 6. IP multicast

Part 2. TCP/IP application protocols
- Chapter 7. Application structure and programming interfaces
- Chapter 8. Directory and naming protocols
- Chapter 9. Remote execution and distributed computing
- Chapter 10. File related protocols

- Chapter 11. Mail applications
- Chapter 12. The World Wide Web
- Chapter 13. Multimedia protocols
- Chapter 14. Wireless Application Protocol (WAP)
- Chapter 15. Network management
- Chapter 16. Utilities

Part 3. Advanced concepts and new technologies
- Chapter 17. IP Version 6
- Chapter 18. Multiprotocol Label Switching (MPLS)
- Chapter 19. Mobile IP
- Chapter 20. Integrating other protocols with TCP/IP
- Chapter 21. TCP/IP security
- Chapter 22. Quality of Service
- Chapter 23. Availability, scalability, and load balancing

Sniffers and Broadcast LANs

- **Most LANs use broadcast packets / frames**
- **Normally nodes read only designated packets / frames by destination address**
- **Nodes in *promiscuous mode* read all frames**
- **Sniffers capture and analyze all packets**
  - **Older models were hardware – obvious**
  - **Software sniffers practically invisible on network**
- **Countermeasures**
  - **Cryptography the most obvious: IPSec, SSH**
  - **Can put servers on switches to avoid broadcasts**
  - **Special software can test timing of networks to detect sniffers**

TCP/IP Sniffers

- ***BUTTsniffer* (Windows NT)**
- ***Ethereal* (Windows, Unix)**
- ***Network Monitor* (free with, and for, Windows NT)**
- ***Sniffit* (Linux, SunOS, Solaris, FreeBSD, Irix)**
- ***snort* (Unix)**
- ***Solsniff* (Solaris)**
- ***tcpdump* (Unix)**
- ***WinDump* (Windows 9x/NT)**

Image used with kind permission of IXXAT, Inc.
http://www.ixxat.com/introduction_tcp_ip_en.html

Sniffer Detectors: AntiSniff®

- **L0pht Heavy Industries – hackers**
- **Released *AntiSniff* in 1999**
  - **Notes below from Nomad review at http://www.nmrc.org/pub/review/antisniff-b2.html**
- **Pro**
  - **Accurate detection of promiscuous mode Ethernet cards**
  - **Alerts sent via email – also includes visual and audio alerts**
  - **AntiSniff sessions can be stored for later use/analysis**

Limitations of AntiSniff®

Comments from Nomad:
- **NT version runs at high priority and is resource-intensive – need dedicated machine**
- **Can only work properly checking Ethernet cards on the same segment as the system running AntiSniff**
  - **Again, this is not a flaw, but due to the nature of networking in general.**
  - **It will work in a switched environment with a smart hub**
- **No SNMP support**

Attacks on the Physical Plant

- ➢ Wiretapping cables (use shielding, testing)
- ➢ Van Eck phreaking (use TEMPEST standard for shielding or obfuscation)
- ➢ Removal of end-of-cable resistors (causes noise and DoS)
- ➢ Twisted-pair LANs (10BaseT Ethernet) susceptible to tapping at punch-down junction boxes
- ➢ Generally protect cabling against tampering
- ➢ Protect servers against unauthorized physical access

13

Modems, Dial-Up Servers, Telco

- ➢ Modems can bypass perimeter protection
  - ❑ May be installed without authorization
  - ❑ Users often have modems on laptops linked into network
  - ❑ Bypass firewalls etc.
  - ❑ Allow easy outbound a ccess
- ➢ Auto-answer modems allow inbound access across firewalls
- ➢ Dial-up servers allow centralized control of modem communications
- ➢ Modems becoming less important today because of high-speed Internet connectivity
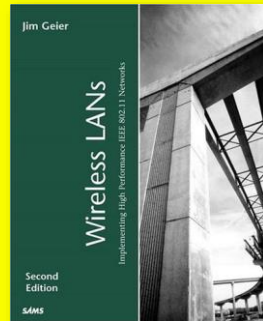
300 baud modem c. 1980

14

Wireless LANs

Jim Geier

Wireless LANs

Implementing High Performance IEEE 802.11 Networks

Second Edition

SAMS

- ➢ **Overview of Wireless LANs**
- ➢ **Wired Equivalent Privacy (WEP)**
- ➢ **Web for Authentication**

15

Overview of Wireless LANs

- ➢ Data carried on radio-frequency radiation more easily intercepted than data on physical wires
  - ❑ Typical range measured in meters or more
  - ❑ Infrared transmission doesn't go through walls
- ➢ IEEE 802.11 Standards for Wireless Networking
  - ❑ Direct-Sequence Spread Spectrum (DSSS)
  - ❑ Frequency-Hopping Spread Spectrum (FHSS)
  - ❑ Without codes/patterns, seems like noise to eavesdropper

See *CSH6* Chapter 5

16

Wired Equivalent Privacy

- ➢ Optional encryption
  - ❑ 40-bit RC4 by default (inadequate today)
  - ❑ 128-bit version available for some products
- ➢ Vendors have defined additional encryption similar to virtual private networks (VPNs)
  - ❑ Use public key cryptography (PKC) & support public key infrastructure (PKI)
  - ❑ E.g., MS Point-to-Point Encryption used in Point-to-Point Tunneling Protocol (PPTP)
- ➢ Some provide authentication
  - ❑ E.g., RADIUS (Remote Access Dial-In User Service)
 - ❑ Not generally interoperable

Cisco Wireless LAN Security

Expert guidance for securing your 802.11 networks

Krishna Sankar
Sri Sundaralingam
Andrew Balinsky
Darrin Miller

17

WEP for Authentication

- ➢ Adds extra layer to userID/password normally used
- ➢ Wireless device must have same encryption key as LAN's access point
- ➢ Wireless access points (WAPs) usually also able to
  - ❑ Define access control lists (ACLs) based on
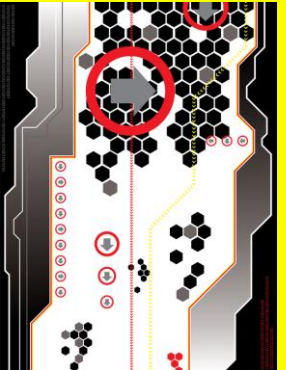 - ❑ Media access control (MAC) addresses

John R. Vacca

Guide to **Wireless Network Security**

Springer
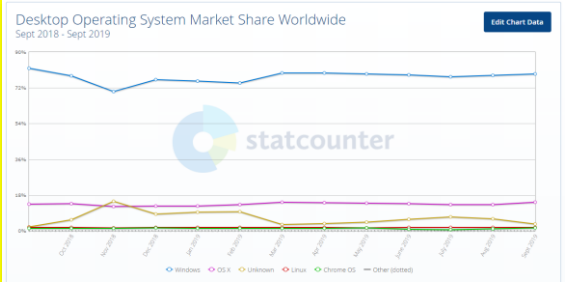
18
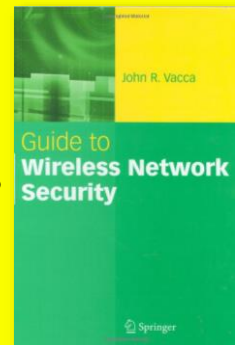
Network Operating System Issues

- Overview of Network OS Topics
- Windows 9x
- NT/2000, XP, Vista, 7
- UNIX
- MacOS

19

OS Desktop Market Shares

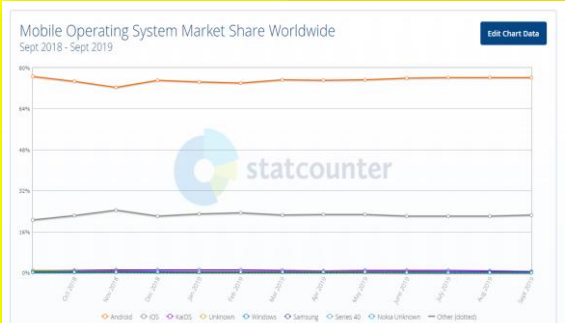Desktop Operating System Market Share Worldwide
Sept 2018 - Sept 2019

statcounter

https://gs.statcounter.com/os-market-share/desktop/worldwide

20

OS Mobile Device Market Shares

https://gs.statcounter.com/os-market-share

Mobile Operating System Market Share Worldwide
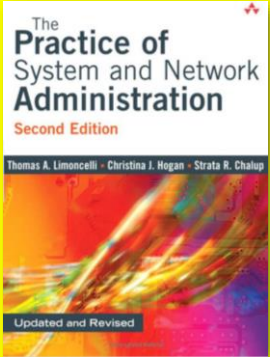Sept 2018 - Sept 2019

statcounter

21

Overview of Network OS Topics

- LAN environment has changed since 1990s
  - At that time, desktops ran applications under Windows
  - Network ran Novell Netware for file sharing
- By late 2000s, networking commonplace for all desktop OSs (Windows, *nix, MacOS…)

The Practice of System and Network Administration
Second Edition
Thomas A. Limoncelli · Christina J. Hogan · Strata R. Chalup
Updated and Revised

22

General Considerations for NW Security (1)

1. Strong passwords & effective password policies
2. Disable/uninstall unused services
3. Keep OS up to date by version & patches
4. Define users, groups, domain trust relations
5. Secure running applications
6. Limit use of root logon to need – and local
7. Limit guest, demo, anonymous accounts
8. Put boot/system files on separate partitions, drives, I/O controllers from application programs and data
9. Audit servers

I
II
III
IV
V
VI
VII
VIII
IX

23

General Considerations for NW Security (2)

10. Monitor log files
11. Remove floppy, CD, DVD drives from servers after use
12. Implement industry best practices for securing OS
13. Use vulnerability assessment tools regularly
14. Use intrusion detection tools
15. When using SNMP, block external access to SNMP
16. Don't make your OS version & processor type public info

X
XI
XII
XIII
XIV
XV
XVI

24

Windows 9x

- Windows OSs susceptible to
  - Exploitation of NETBIOS file & print sharing
  - Abuse of resource sharing through TCP/IP when network has Internet access
- Windows challenge-handshake authentication protocol (CHAP)
  - Used for sending passwords
  - But same challenge used for 15 minutes
  - Thus possible capture/replay by intruder with physical access & sniffer
- BackOrifice & NetBus: remote-control tools
- Password crackers can break .PWL password files
- PW-protected screensaver? Reboot!
- Use 3rd party secure bootlocks

25

NT/2000
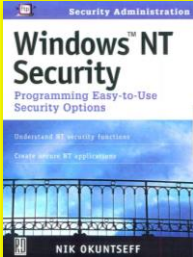
- Windows 2000 Millennium Edition has same weaknesses as 9x
- Stronger:
  - Windows NT Server
  - NT Workstation
  - 2000 Server
- Many hacking tools available for these versions as well
- Vulnerabilities in Internet Explorer (IE) & Office products weaken OS
- Ideally, disable all Active Scripting and ActiveX options in Restricted Sites Zone of IE

26

NT/2000 (2)

- NT/2000: Simple recommendations for basic security
  - Format drives using NTFS, not FAT
  - Use long file names & disable DOS 8.3 naming
  - Disable *Everyone* group
  - Rename administrator account
  - Turn auditing on (off by default)
- W2K: Enable Encrypting File System (EFS)
  - Automatic encryption of disk data
  - Should enable recovery of keys

Security Administration

Windows™ NT Security

Programming Easy-to-Use Security Options

Understand NT security functions

Create secure NT applications

NIK OKUNTSEFF

27

Windows NT Audit Tools (1)

- *netstat* examines open ports
- *Event Viewer* examines application, security, and system logs.
- *net start, net user, net group, net local group* display running services, users, groups, and local groups
- *dumpel* converts Event Viewer logs to ASCII files
- *NetMon* displays network traffic
- *netsvc* displays local and remote running services and drivers
- *addusers* displays users and groups
- *findgrp* displays local and domain groups for a user

28

Windows NT Audit Tools (2)

- *local* and *global* show all members of specific local or global groups
- *dommon* displays trusted domains
- *xcacls* examines the file Access Control Lists (ACL)
- *perms* examines the ACLs associated with a user
- *sysdiff* displays changes in the Registry and file system
- *regdmp* creates an ASCII version of the Registry
- *ralist* lists a domain's Remote Access Servers (RAS)
- *rasusers* lists users authorized for dial-in access

29

Windows XP: Better Security

- EFS, firewall, Data Execution Prevention
- But original release included *raw sockets*
  - Permits program to manipulate TCP/IP communications directly
  - Without use of normal application program interfaces (APIs) that apply security
  - Allowed external control
  - **Steve Gibson**
    http://www.grc.com
  - Steve Gibson warned (2001) of serious risk from script kiddies for denial of service applications
  - See http://www.informit.com/articles/article.aspx?p=27289
- MS removed raw sockets in Service Pack 2 (SP2)

30

Vista: Child of *Trustworthy Computing Initiative*

- Vista released Jan 2007; but by end of July 2009,
  - 22% market share (360M users)
  - 70% market share for Windows XP (1.1B users)
- Major security change is *User Account Control* (UAC)
- Requires user response to allow action requiring *admin* privileges
  - Run as admin
  - Changing files in root and program files folders
  - [Un]Installing apps, drivers, ActiveX
  - Changing settings for Firewall, UAC, Update, user accounts, Parental Controls, Task Scheduler
  - Restoring system files from backups
  - Viewing or changing other user's data

Administering Windows Vista Security
The Big Surprises
Mark Minasi
Byron Hynes

31   *Copyright © 2019 M. E. Kabay. All rights reserved.*
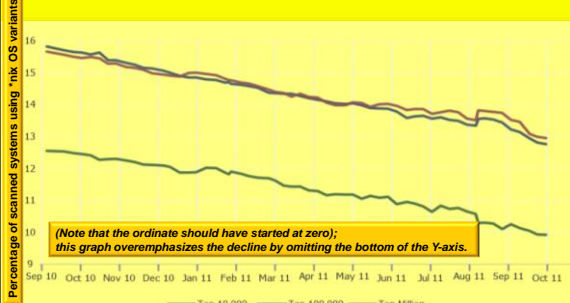
Vista: Stepchild of the NSA?!?

- Alec Klein & Ellen Nakashima
  - *Washington Post* (January 9, 2007)
  - NSA "participated" in creation of Vista security elements
- Unclear extent of involvement
- NSA acknowledged helping to protect OS against "worms, Trojan horses and other insidious computer attackers…."
- Microsoft made NSA involvement public
- Authors Kessler & Pritsky comment, "It is left as an exercise for the reader to decide whether having a spy agency working on a premier OS is a good thing or not."
- What do *you* think?
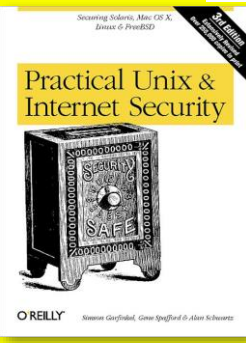
32   *Copyright © 2019 M. E. Kabay. All rights reserved.*

UNIX (1)

- *NIX (UNIX variants) usage falling on servers:

(Note that the ordinate should have started at zero); this graph overemphasizes the decline by omitting the bottom of the Y-axis.

Percentage of scanned systems using *nix OS variants

— Top 10,000   — Top 100,000   — Top Million

33   http://trends.builtwith.com/Server/Unix

UNIX (2)

- UNIX security architecture
  - Developed originally for use in trusted community – security not paramount
  - Usual list of normal security functions
  - Enormous list of services
- Extensive literature on *NIX security
- Apply proper security audits, vulnerability assessment to *NIX systems

Practical Unix & Internet Security
Securing Solaris, Mac OS X, Linux & FreeBSD
3rd Edition
O'REILLY
Simson Garfinkel, Gene Spafford & Alan Schwartz

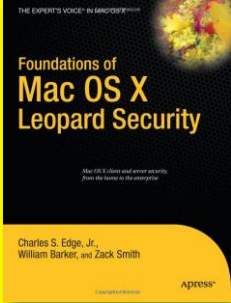34   *Copyright © 2019 M. E. Kabay. All rights reserved.*

MacOS (1)

- Mac OS originally designed with little concern for security
- Every user is admin
- Sharing capabilities more complex than on Windows
  - Therefore more risk of naïve user error
- Little user-level protection
  - No default requirement for password at logon
  - No standard password-equipped screen saver

35   *Copyright © 2019 M. E. Kabay. All rights reserved.*

MacOS (2)

- Malware attacks fewer
  - But MS Office malware works
  - DoS attacks work
  - Use anti-malware package!
- Other tools
  - DiskLocker: password-protection of entire HD
  - FileLock: locks on individual files
  - Empower: applications & files
  - MacPassword, Sesame: multilevel passwords

Foundations of Mac OS X Leopard Security
Mac OS X client and server security, from the home to the enterprise
Charles S. Edge, Jr., William Barker, and Zack Smith
Apress

36   *Copyright © 2019 M. E. Kabay. All rights reserved.*

MacOS (3)

- Mac-oriented security tools for networking include
  - Intermapper: SNMP tool for AppleTalk & IP
  - MacRadius: RADIUS for dial-in servers
  - NetLock: encryption for sessions, passwords, logins
  - Network Security Guard: vulnerability scanner
- Update versions and apply patches promptly
- Criminal hackers still not as frequently attacking Macs
  - Fewer targets, less familiarity

Mac Security Superguide

37 Copyright©2019 M. E. Kabay. All rights reserved.

Now go and study

38 Copyright©2019 M. E. Kabay. All rights reserved.