Lecture 16

System Security

Knowledge is Different in Different States of Consciousness

Wholeness Statement

In this lecture we contrast how a machine used by a developer is configured with how the DMZ web server is configured. Knowledge is different in different states of consciousness. We also review user security.

Main Point

1. The web server is used by untrusted users from the Internet and trusted administrators from the internal network. Maharishi has been very careful with how he gives out the knowledge of transcending. Purity of teaching keeps the teaching strong.

Main Point

2. A given developer machine can be accessed by any developer on the internal network. Developers are trusted. The field of transcendental consciousness can be accessed by any one with a human physiology provided that the correct technique is used.

Main Point

3. Never leave your terminal unlocked and unattended, even when meditating in front of the terminal. Remember that if sleep comes during meditation, give in to it. Trying to stay awake introduces effort into the practice; the practice should be effortless.

Main Point

4. Take security warnings seriously. For example if a browser warns about a certificate, ask for help if you don't understand what the problem is. Similarly, take warning signs from your body seriously and seek help to resolve them before they get worse. Better yet use Ayurveda to detect problems before they become symptomatic.

Overview

- How does administering security affect a system?
- Focus on two systems
  - DMZ web server
  - User system in development subnet
- Assumptions
  - DMZ system: any user of trusted administrative host has authenticated to that system correctly and is a "trusted" user
  - Development system: standard system that can be used by any of the developers

DMZ Web Server: Consequences of Policy

1. Incoming web connections come from outer firewall
2. Users log in from trusted administrative host; web pages are also downloaded through it
3. Log messages go to DMZ log host only
4. Web server may query DMZ DNS system for IP addresses
5. Other than these, no network services provided
6. Restricts access as much as possible
7. Public keys reside on web server

Devnet User System: Policy Components

1. Only authorized users can use devnet systems; can work on any workstation
2. Sysadmins must be able to access workstations at any time
3. Authorized users trusted not to attack systems
4. All network communications except email confidential, integrity checked
5. Base standard configuration cannot be changed
6. Backups allow any system to be restored
7. Periodic, ongoing audits of devnet systems

Consequences for Devnet Infrastructure

- No direct access between Internet and devnet systems
  - Developers who need to do so have separate workstations connected to commercial ISP
  - These are physically disconnected from devnet and cannot be easily reconnected

Procedural Mechanisms

- Some restrictions cannot be enforced by technology
  - Moving files between ISP workstation and devnet workstation using a floppy
  - No technological way to prevent this except by removing floppy drive
    - Infeasible due to nature of ISP workstations
  - Drib has made procedures, consequences for violating procedures, very clear

Comparison DMZ Web Server vs. Devnet

- Differences spring from different roles
  - DMZ web server not a general-use computer
  - Devnet workstation is
- DMZ web server policy: only administrative users have access as users
- Devnet workstation policy: Many different users
  - Used for software creation, testing, maintenance

Comparison

- Location
  - DMZ web server: all systems assumed hostile, so server replicates firewall restrictions
  - Devnet workstation: internal systems trusted, so workstation relies on firewall to block attacks from non-devnet systems
- Use
  - DMZ web server: serves web pages, accepts commercial transactions
  - Devnet workstation: many services provided

Comparison

- Differences also lie in use of systems
  - DMZ web server: in area accessible to untrusted users (from Internet)
    - Limiting number of users limits damage successful attacker can do
    - User info on system, so don't need to worry about network attacks on that info
    - Few points of access (3 user accounts)
  - Devnet workstation: in area accessible to only trusted users (subnet of internal network)
    - General user access system
    - Shares user base with other systems
    - Many points of access

Comparison

- Both use strong authentication
  - All certificates installed by trusted sysadmins
- Both allow reusable passwords
  - DMZ web server uses MD-5, does not age passwords
  - Devnet workstation uses DES-based hash, ages passwords (3-90 days)

Comparison

- DMZ web server: only necessary processes
  - New software developed, compiled elsewhere
  - Processes run in very restrictive environment
  - Processes write to local log and directly to log server
- Devnet workstation: provides environment for developers
  - More processes for more tasks
  - Process environment less restrictive to allow sharing, etc.
  - Processes write to log server, which does all logging

Comparison

- Both use physical means to prevent system software from being compromised
  - Attackers can't alter CD-ROMs
- Reloading systems
  - DMZ web server: saves transaction files, can regenerate system from WWW-clone
  - Devnet workstation: just reboot, reformat hard drive
    - Files on hard drive are transient or replicated (logs)

Comparison

- Devnet workstation: users trusted not to attack it
  - Any developer can use any devnet workstation
  - Developers may *unintentionally* introduce Trojan horses, etc
    - Hence everything critical on read-only media
- DMZ web server: fewer trusted users
  - Self-contained; none of its files mounted remotely
  - CD-ROM has minimal web server system augmented only by additional programs tailored for Drib's purpose

Networks

- Both systems need appropriate network protections
  - Firewalls provide much of this, but separation of privilege says the systems should too
- How do administrators configure these?

DMZ Web Server

- Accepts web requests only from inner firewall
- Inner firewall prevents internal hosts from accessing DMZ web server
- Accepts SSH connections only from trusted administrative host
  - All other connections rejected
- Accepts SSH connections only from authorized users coming in from trusted administrative server
  - SSH provides per host *and* per user authentication
  - Public keys pre-loaded on web server
- Inner firewall prevents other internal hosts from accessing SSH server on this system

DMZ Server Availability

- Need to restart servers if they crash
  - Automated, to make restart quick
- Script

```
#! /bin/sh
echo $$ > /var/servers/webdwrapper.pid
while true
do
    /usr/local/bin/webd
    sleep 30
done
```

- If server terminates, 30 sec later it restarts

DMZ Web Server: Clients

- DNS client gets IP addresses and host names from DMZ DNS
  - Client ignores extraneous data
  - If different responses to query, discard both
- Logging client sends log messages to DMZ log server
  - Logs any attempted connections to any port

Devnet Workstation

- Servers:
  - Mail (SMTP) server
    - Very simple, just forwards mail to central devnet mail server
  - SSH server
  - Line printer spooler
  - Logging server

Checking Security

- Security officers scan network ports on systems
  - Compare to expected list of authorized systems and open ports
    - Discrepencies lead to questions
- Security officers attack devnet systems
  - Goal: see how well they withstand attacks
  - Results used to change software, procedures to improve security

Users

- What accounts are needed to run systems?
  - User accounts (“users”)
  - Administrative accounts (“sysadmins”)
- How should these be configured and maintained?

DMZ Web Server User Accounts

- Web server account: *webbie*
- Commerce server account: *ecommie*
- *webbie* creates file in a transaction directory, both have the following ACL:
  - (*ecommie*, { *read*, *write* })
- *ecommie* then copies file into spooling area (enciphering it appropriately), then deletes original file
  - Note: *webbie* can no longer read, write, delete file

Sysadmin Accounts

- One user account per system administrator
  - Ties actions to individual
- Can never log into sysadmin account remotely
  - Must log into user account, then access sysadmin account (must supply another password)
    - Supports tying events to individual users
- Direct login is allowed from system console (in a restricted, locked room)
  - Useful if major problems
  - Three people in room with console at all times

DMZ User Accounts

- DMZ web server needs only three user accounts: webbie, ecommie, and one sysadmin account (SSH)

Authentication

- Focus here is on techniques used
- All systems require some form

DMZ Web Server

- SSH: cryptographic authentication for hosts
  - Does not use IP addresses
  - Reject connection if authentication fails
- SSH: cryptographic authentication for user; password is required if that fails
  - Must be done from the trusted administrative host
- Passwords: use MD-5 hash to protect passwords
  - Can be as long as desired
  - Proactive password checking to ensure they are hard to guess
  - No password aging

Devnet Workstation

- Requires authentication as unauthorized people have access to physically secure area
  - Janitors, managers, etc.
- Passwords: proactively checked
  - Uses DES-based hash for NIS compatibility
    - Max password length: 8 chars
  - Aging in effect; time bounds (min 3d, max 90d)
- SSH: like DMZ web server, *except*:
  - *root* access blocked
  - Must log in as ordinary user, then change to *root*

Processes

- What each system must run
  - Goal is to minimize the number of these

DMZ Web Server

- Necessary processes:
  - Web server
    - Enough privileges to read pages, etc.
  - Commerce server
    - Enough privileges to copy files from web server's area to spool area; not enough to alter web pages
  - SSH server (privileged)
  - Login server (privileged)
    - A physical terminal or console
  - Any essential OS services (privileged)
    - Page daemon, etc.

Devnet Workstation

- Logging mechanism
  - Records OS calls, parameters, results
  - Saves it locally, sent to central logging server
    - Intrusion detection done; can augment logging as needed
    - Initially, process start, end, audit and effective UIDs recorded
- Disk space
  - If disk utilization over 95%, program scans local systems and deletes all temp files and editor backup files not in use
    - Meaning have not been accessed in last 3 days

Files

- Protections differ due to differences in policies
  - Use physical limits whenever possible, as these cannot be corrupted
  - Use access controls otherwise

DMZ Web Server

- System programs, configuration files, etc. are on CD-ROM
  - If attacker succeeds in breaking in, modifying in-core processes, then sysadmins simply reboot to recover
  - Public key for internal commerce server here, too
- Only web pages change
  - Too often to put them on CD-ROM
  - Small hard drive holds pages, spool areas, temp directories, sysadmin home directory

DMZ Web Server

- Everything statically linked
  - No compilers, dynamic loaders, etc.
- Command interpreter for sysadmin
  - Programs to start, stop servers
  - Programs to edit, create, delete, view files
  - Programs to monitor systems
- No other programs
  - None to read mail or news, no batching, no web browsers, etc.

DMZ Web Server

- Checking integrity of DMZ web server
  - Not done
- If question:
  - Stop web server
  - Transfer all remaining transaction files
  - Reboot system from CD-ROM
  - Reformat hard drive
  - Reload contents of user directories, web pages from WWW-clone
  - Restart servers

Devnet Workstation

- Logs on log server examined using intrusion detection systems
  - Security officers validate by analyzing 30 min worth of log entries and comparing result to reports from IDS
- Scans of writable media looking for files matching known patterns of intrusions
  - If found, reboot and wipe hard drive
  - Then do full check of file server

Summary: DMZ Web Server

- Runs as few services as possible
- Keeps everything on unalterable media
- Checks source of all connections
  - Web: from outer firewall only
  - SSH: from trusted administrative host only
- Web, commerce servers transfer files via shared directory
  - They do not directly communicate

Summary: Devnet Workstation

- Runs as few programs and servers as possible
  - Many more than DMZ web server, though
- Security prominent but not dominant
  - Must not interfere with ability of developer to do job
  - Security mechanisms hinder attackers, help find attackers, and enable rapid recovery from successful attack
- Access from network allowed
  - Firewall(s) assumed to keep out unwanted users, so security mechanisms are second line of defense

Key Points

- Use security policy to derive security mechanisms
- Apply basic principles and concepts of security
  - Least privilege, separation of privilege (defense in depth), economy of mechanism (as few services as possible)
  - Identify who and what you are trusting

User Security

Chapter 25

User Policy

- Assume user is on Drib development network
  - Policy usually highly informal and in the mind of the user
- The users' policy:
  - U1 Only users have access to their accounts
  - U2 No other user can read or change a file without owner's permission
  - U3 Users shall protect integrity, confidentiality, availability of their files
  - U4 Users shall be aware of all commands that they enter or that are entered on their behalf

Passwords

- Theory: writing down passwords is ***BAD***!
- Reality: choosing passwords randomly makes them hard to remember
  - If you need passwords for many systems, assigning random passwords and *not* writing something down won't work
- Problem: Someone can read the written password
- Reality: degree of danger depends on environment, how you record password

Login Procedure

- User obtains a prompt at which to enter name
- Then comes password prompt
- Attacks:
  - Lack of mutual authentication
  - Reading password as it is entered
  - Untrustworthy trusted hosts

Lack of Mutual Authentication

- How does user know whether interacting with legitimate login procedure?
  - Attacker can have Trojan horse emulate login procedure and record name, password, then print error message and spawn real login
- Simple approach: if name, password entered incorrectly, make the prompt for retry different
  - In UNIX V6, it said "Name" rather than "login"

Noticing Previous Logins

- Many systems print time, location (terminal) of last login
  - If either is wrong, probably someone has unauthorized access to account; needs to be investigated
- Requires user to be somewhat alert during login

Reading Password As Entered

- Attacker remembers it, uses it later
  - Sometimes called “shoulder surfing”
  - Can also read chars from kernel tables, passive wiretapping, etc.
- Approach: encipher all network traffic to defeat passive wiretapping

Leaving the System

- People not authorized to use systems have access to rooms where systems are
  - Custodians, maintenance workers, etc.
- Once authenticated, users must control access to their session until it ends
  - What to do when one goes to bathroom?

Practical Points

Protecting access to your account

- Never give your password to anybody!!
- Make it hard to guess
- Don’t write it down
- Use different passwords on different accounts
- Change it regularly

Special Cases

- Sometimes can relax the above requirements
- For example, consider the console room where the trusted administrative host was located.
- Can write password on blackboard because:
  - In locked room; system can only be accessed from within that room
  - No networks, modems, etc.
  - Only authorized users have keys to room
  - Only people who will see it are authorized to see it

Login Procedure

- Be sure to enter password into real dialog box (mutual authentication)
- Make sure no one is looking over your shoulder as you enter password (shoulder surfing)
- Make sure connection is enciphered before entering password (SSL, SSH)
- If last login is displayed, make sure that it is plausible that you did it.

Leaving the System

- If you leave the terminal for even a few seconds, Ctrl+Alt+Del/Lock Computer
- If you shutdown, wait until the system is shutdown, otherwise a dialog asking to save some file may interrupt the shutdown process.
- No modems allowed!! Sometimes a modem doesn't close the connection.
- Do not plug wireless access points into an ethernet jack.

Protecting files

- If you manipulate ACLs be sure that you do it correctly.
  - In the on-campus course, each student has their own directory on the course server; only the student can read/write to their directory.
  - This was tested in the on-campus lab 1.
- Remember in Windows and other systems, that a deleted file goes into recycle bin.
- If you delete a file from the recycle bin, be aware that its blocks may still be on the hard-drive and a knowledgeable attack can reassemble the file.
- How to clean in Windows?
- If you copy a file make sure that the new file has the correct permissions

Protecting files

- Be careful not to overwrite files.
- If files are encrypted, be sure they are encrypted correctly and that the key is secured.
- Minimize the number of files that contain unencrypted passwords. (can encipher web.config)
- Be sure that configuration files used by programs at startup are secure.
- Don't run files from the Internet or open unknown documents in email without proper virus protection.
- If browser warns about a certificate, take it seriously.

Protecting files

- Word documents can retain deleted portions or contain information that is only displayed when the document is printed. Be sure that deleted portions are not in a document you send to somebody.
- One SCI student discovered this the hard way. He copied the final SCI essay of another student and emailed it to his group leader. When the group leader printed out the essay, the name of the other student was printed in the header. This header did not show up when the file was viewed in Microsoft Word.

Protecting files

- If you make hard-copies be sure to dispose of them properly (e.g., shredding to avoid dumpster diving).
- Be careful, forwarding and replying to email because there might be people on the list who shouldn't see it.
- If you leave a company be aware that all of your files may be read by somebody.
- Beware of phishing attacks (http://cups.cs.cmu.edu/antiphishing_phil/)
- In summary, a chain is as strong as its weakest link.

CONNECTING THE PARTS OF KNOWLEDGE WITH THE WHOLENESS OF KNOWLEDGE

1. A developer can log onto any machine in the devnet.
2. Only an administrator can log onto the DMZ web machine using SSH from the physically secured trusted administration host.

3. Transcendental Consciousness is a state of complete knowledge.
4. Wholeness moving within itself: in Unity Consciousness, one has complete knowledge of subject and object, they are both experienced as manifestations of one's own Self.