Internet Services and Security
Fortaleza, May 1996

Casper Dik
Casper.Dik@Holland.Sun.COM

Network Security Group
Sun Microsystems, Inc.

Casper Dik
Casper.Dik@Holland.Sun.COM

- Network Security Group
  - 5-10 people
  - part of Enterprise Network Services
- Sun Wide Area Network (SWAN)
  - 15000 users, plus contractors
  - 40000 systems (mostly Solaris 2.x)

Introduction
Problems faced on a Network

- The world is one big street
  - everybody is your neighbour
  - no neighbourhood watch
- Most hacking requires no skills
  - Script kids run rampant
  - Hacking is almost never innocent

Agenda

- Problems faced on SWAN
- Policies & Procedures
- Securing System Services
- Tools
- Logging & Auditing
- Solutions used on SWAN

Problems faced on SWAN

- **15000** users
- **40000** hosts
- **one** Network Security Group
- Geographically spread
- Many different types of users
  - CEO, Engineers, Sales, Support, Service, Administrators, HR
- Lots of different uses
  - Lots of databases, bugtool, Video, WWW, software distribution & development

Problems faced on SWAN

- A single firewall doesn't suffice
  - No single access control policy fits all users.
  - Can you trust all your users?
  - Can we control all remote access?
  - Should a single breach give access to the entire net?
  - What rules are there for connecting equipment to SWAN?
  - What are the powers of the incident response groups?

Policies and Procedures

People are part of the Problem

Policies and Procedures

- Risk Assessment
- Control over physical network
- Acceptable system configurations
- Remote access
- Software installations
- Disaster recovery

Policies and Procedures
Risk Assessment

- What is valuable
  - replacement value
  - loss of production
- What is vulnerable and how
  - Theft
  - Hacking
  - Fire and natural disasters
- Overall security and safety policy

Policies and Procedures
Software Configuration

- Only recent, or well patched software
  - required patchlist
- Old operating systems treated differently
  - Unnecessary services switched off
  - Protected networks for unsafe machines
- TCP wrappers
- Minimum logging requirements
  - What happened and when?
  - Synchronized clocks to correlate logs

Policies and Procedures Software Configuration

- Different systems require different types of configuration
  - personnel records
  - financial data
  - home directories
- Acceptable network services
  - not all services equally acceptable everywhere
- Additional protection for certain services

Policies and Procedures Acceptable Use

- Importing software from the net
  - Viruses/Trojans
- Implied permissions vs true permissions
- Information protection
- Physical security
- Forwarding E-mail off-site
- Consequences of violation
  - termination
  - suspension

Policies and Procedures
Connection Policies

- Modems connected to desktops
  - PC anywhere from home
  - Uncontrolled dial-ins
  - Internet connections behind the firewall
- Rules needed for modems & connections
  - register all modems
  - dial-out only where possible (PBX)
  - fax-only when possible
  - firewalls for all external network connections

Policies and Procedures System Administration

- Respecting user's rights
  - privacy - monitoring, reading mail/files
  - Account suspension - when?
- Local laws are important here
  - Evidence validity (search warrant needed?)
  - Lawsuits
- Check with legal dept.

Policies and Procedures
Account termination

- Disable login
  - disable password & change shell
- backup & remove files
- remove user from aliases & access list
- Standard part of employee termination process

Securing System Services

Don't trust what you don't control

Securing System Services Problems

- Old Software
- The bottom layer: IP
- Domain Name Service
- R* services
- Password authenticated services
- Guest services
- ONC RPC
- Client software

Securing System Services Solutions

- Run up-to-date software
- Configure your software properly
- One-time passwords
- SSH
- Secure RPC
- Kerberos
- GSS-API
- User Education/Policies

Securing System Services
Problems with old software

- Software no longer updated
- Security problems not fixed/fixable
- *legacy* applications running on *legacy* systems
- Dreaded *End-of-Life*
  - "We can't fix that system, it's EOL"

Securing System Services
Problems at the IP layer

- Address impersonation
  - source routing
  - spoofing
    - Guessable Initial Sequence Numbers (ISNs)
- Session hijacking
  - Needs sequence numbers
- Password Sniffing
- No privacy, no integrity

Securing System Services
Problems with DNS

- Name Server Cache Pollution
- Falsified address -> name mappings
  - hostname based authentication at risk
- Many historical bugs
- Gives out information about your site

Securing System Services
Problems with R* services

- Rlogind & rshd use name based authentication
  - IP address spoofing
  - DNS attacks
  - transitive trust
- Trusts credentials send by remote end
- Requires remote end to be a port < 1024
  - *who controls the other side?*

Securing System Services Problems with passwords

- Reusable passwords can be sniffed
- Examples of reusable passwords:
  - ftpd/telnetd/rexecd: standard Unix passwords
  - NFS filehandles used as access keys
  - X magic cookies

Securing System Services
Problems with Guests

- ftpd
  - file permissions
  - "site-exec" bug
  - warez
- www
  - cgi-bin
    - perl.exe in cgi-bin
    - improper input checking in scripts
  - old web server software

Securing System Services
Problems with ONC RPC

- AUTH_SYS/AUTH_UNIX (default)
  - client sends credentials, server believes them
  - client trusts server's responses
  - no integrity
  - no privacy

Securing System Services
Problems with ONC RPC

- AUTH_KERB/AUTH_DES shortcomings
  - no integrity
  - no privacy

Securing System Services
Problems with ONC RPC

- At risk, lacking access controls:
  - NFS
    - *has nfs_portmon*
  - rexd
  - admind (Solaris 2.x)
  - NIS
    - *has /var/yp/securenets*

Securing System Services
Problems with ONC RPC

- NFS file data can be spoofed
  - even with AUTH_DES & AUTH_KERB!
- NIS can be spoofed by faking responses or entire servers

Securing System Services
Problems with Client Software

- Webbrowser vulnerabilities
  - Buffer overrun
  - JAVA bugs
  - JavaScript
  - Information leakage
- MIME
  - executable attachments
  - MS-Word documents with Macro virus

Securing System Services Solutions: Staying ahead

- Keep informed
  - Read Usenet
  - Read mailing lists
    - firewalls
    - bugtraq (defunct??)
    - OS specific (e.g., sun-managers)

Securing System Services Solutions: Staying ahead

- Run recent releases of OS
  - Not all bugs fixed with patches
    - Random ISNs
  - Older OSes not patched at all
  - Less chance of forgetting important patches
  - New security features

Securing System Services Solutions: Staying ahead

- Remember where you got your freeware
  - Make sure you notice updates
- Sendmail *bug-of-the-month* club
- BIND (named) security problems
- HTTP daemon security problems
- Kerberos implementation weaknesses

Securing System Services
Solutions: Configure Cleanly

- Check /etc/hosts.equiv and ~/.rhosts files
- Check for strong passwords
  - *reusable passwords are a thing of the past*
- Integrity checking
  - tripwire/tiger
  - backups
  - original OS distribution (from CD)

Securing System Services Solutions: One-time passwords

- Reusable passwords are the softest target
  - most attacks use sniffers
  - should only be allowed on local LAN or encrypted links
- S/Key
  - logdaemon
  - OPIE

Securing System Services Solutions: One-time passwords

- Digital Token Cards
  - Challenge/response
  - Sequence number based on current time
- Examples:
  - SecureID
  - Enigma DES Gold
- Card must have PIN!

Securing System Services Solutions: One-time passwords

- Vulnerabilities
  - Some are vulnerable to active attack
  - S/Key vulnerable to dictionary attack
  - Digital Tokens cost are seen as expensive
  - User typed one-time passwords are not convenient

Securing System Services Solutions: SSH

- Public key authentication (RSA)
- RSA encrypted session key exchange
- End-to-end encryption
- Padding with random data
- Checksum (CRC)
- Hourly change of *server* key
- More info from
  - http://www.cs.hut.fi/ssh/

Securing System Services Solutions: SSH

- Advantages
  - No IP addresses or nameservers trusted
  - No password sniffing
  - Integrity & Privacy
  - Tunneling of arbitrary TCP connections
  - Secure remote X connections
  - Captured session cannot be decrypted

Securing System Services Solutions: SSH

- Disadvantages
  - Not legally available/usable everywhere
  - Endpoints vulnerable, as always
  - Stolen secret key allows impersonation
  - Complex system

Securing System Services Solutions: Secure RPC

- Diffie-Hellman Key exchange
- DES session key
- Secure NFS, NIS+, admind, rexd, X server
- Broken in theory, still very effective in practice

Securing System Services Solutions: Secure RPC

- Advantages
  - No replay attacks
  - Authenticates users and systems

Securing System Services Solutions: Secure RPC

- Drawbacks
  - Root on client workstation has access
  - requires synchronized clocks
  - No message integrity or privacy
  - need to re-enter password after network login
  - *don't forget to keylogout*

Securing System Services Solutions: Kerberos

- Requires secure key server
- Stores shared secret
- Requires all services to be kerberized
- Also as AUTH_KERB flavour for Sun RPC

Securing System Services Solutions: Kerberos

- Advantages
  - Authenticates requests and services
  - Not replayable
  - Single sign-on, secure net logins

Securing System Services Solutions: Kerberos

- Drawbacks
  - Essentially requires single user systems
  - Synchronized clocks
  - Centralized, secure, server
  - Usually no inter REALM authentication

Securing System Services Solutions: GSS-API

- GSS-API: the future, RFCs 1508 & 1509
- Supports many security mechanisms, e.g., Kerberos V
- Integrates with ONC RPC as RPCSEC_GSS (Kerberos V)
- RPCSEC_GSS offers three options:
  - Authentication
  - Authentication & Integrity
  - Authentication & Privacy

Securing System Services Solutions: GSS-API

- Advantages
  - Only support for framework required.
  - New mechanisms can be added by 3rd parties
  - Integrity & Privacy & Authentication
  - Replay protection
- Disadvantages
  - Export control?

Securing System Services Solutions: Misc.

- Virtual Private Networks
  - cheaper than leased lines
  - as secure
  - local dial-in access possible everywhere
  - perhaps not as reliable
- Products
  - SKIP

Securing System Services Solutions: User Education

- Run standard copy, not every user his own
  - Swift control of Java/Netscape problems
  - Requires admin to closely track new releases
- Dangers of e-mail/document exchange
  - Click-to-execute attachments
  - MS-Word Macro Viruses
- The *Good Times!* virus is a HOAX!
- Proper password use

Tools

- Resource locations
- Auditing tools
- TCP access & logging

Tools
Where to get them

- PERL
  - http://www.perl.com/perl/index.html
- COAST archives
  - ftp://coast.cs.purdue.edu/pub/tools/
- SATAN, TCP wrappers/logdaemon, rpcbind/portmap
  - ftp://ftp.win.tue.nl/pub/security/
- CERT
  - http://www.cert.org/pub/

Tools
Auditing your network

- COPS
- TIGER
- SATAN
- ISS

Tools
Auditing with COPS

- Old
  - doesn't know about newer systems
- Limited usefulness
- *Should be buried*
  - no maintenance for 6 or more years

Tools
Auditing with TIGER

- Well maintained
- Best supported on SunOS 4.x/Solaris 2.x
- Comes with checksums from standard installs
- Checks system configuration
- Uses break-in detection heuristics
- Well documented

Tools
Auditing with SATAN

- Probes many network services
  - Gives mapping of current services
- Checks for known bugs
  - *known at the time of the last SATAN release*
  - insofar remotely testable
- Test for dangerous configuration
  - NFS exports to world
  - rexd
- re-run often
- new release imminent

Tools
Auditing with ISS

- Old version available in source
  - NFS bugs
  - NIS information/bugs
  - portscanning
- New commercial version
  - Many, many checks; IP spoofing
  - http://www.iss.net/
  - Well maintained

Tools
TCP tools

- TCP wrappers
- logdaemon
- "secure" rpcbind/portmap
- identd
- xinetd

Tools
TCP wrapper

- Access controls based on IP address hostname
- Extra logging
- Disadvantages
  - IP address based

Tools
Logdaemon

- Replacements for rshd, rlogind, rexecd, login, ftpd, telnetd
- S/Key
- Control on .rhosts files (no "+")
- Fine grained access controls
- Better logging

Tools
Secure Rpcbind (portmap)

- hosts.allow/hosts.deny access controls
- per service controls
- no call forwarding
- Standard in some OSes
- Disadvantages
  - IP based authentication (won't help at all for UDP, some for TCP)
  - RPC services still accessible through portscan

Tools
Identd

- RFC 1413
- gives username information to remote servers
- *your* identd can help *you* identify problems
  - *remote values are of no use to you*
- professional courtesy/good neighbourliness

Tools
Xinetd

- inetd & tcp wrapper rolled into one
- Disadvantages
  - complex
  - not a plug-in replacement (inetd does evolve, xinetd doesn't always track closely)
- Similar functionality available as
  - tcpwrappers
  - standard in inetd on some OSes.

Logging

- Syslog configuration hints
- Other logfiles to watch
- What to do with your logs
- SWATCH

Logging
Syslog Configuration

- Secure centralized log server
  - No ordinary users
  - No weak access
- One entry for the client's /etc/syslog.conf
  - *.debug   @loghost
  - *.debug;mail.none   @loghost

Logging
What to do with the logs

- Don't run after all incidents
  - If you recognize what it is, you're protected against it.
  - Don't waste your time chasing newbies.
  - Be alert.
- Concentrate efforts on unexpected entries
  - System failures
  - New ways to hack systems

Logging
SWATCH

- SWATCH can take over your tedious tasks
  - requires centralized logging
  - give alerts for important log messages
  - call program for log messages
    - call pagers
    - send e-mail
  - count and summarize common messages
  - more useful with enhanced daemons (logdaemon, tcpd)

Logging
SWATCH cont'd

- Filter out known innocent messages
- Get notification on known problems
  - login FAILURES
  - rsh connections
  - system reboots/crashes
- Don't discard unexpected messages
  - May indicate new problem or new attack

Solutions on SWAN

- Network Security Group
- Controlling the Users
- Tightly controlled access
- Auditing with Autohack
- Incident Response
- Configuration Guidelines

Solutions on SWAN
Network Security Group

- one group in overall control of security
- 5-10 persons spread all over the world
- How do we manage?
  - Recommendations/auditing only
  - No system administration duties

Solutions on SWAN
Educating the Users

- "Only" internal users to worry about
- Information protection guidelines
- User behavior guidelines
  - no off-site e-mail forwarding
  - no unauthorized SWAN connections
  - software from the Internet must be audited
  - SWAN usage policies
- Automated Termination Procedures
  - computer access revoked
  - digital token disabled

Solutions on SWAN
Helping the Sysadmins

- Check security of newly developed tools
- Answer queries on security issues
  - network connections
  - software configuration
- Register dangerous items
  - Internal network connections
  - Modem lines
  - Fax modems

Solutions on SWAN
Tightly controlled access

- Only Sun employees have access
- Digital Tokens for home/nomadic access
- All modems/modem pools/lines registered
- Fax only modems when possible
- Firewalls between SWAN and other networks
- SWAN access only for hosts with proper configuration
- Labs on isolated subnets

Solutions on SWAN
Incident Response

- Auditing "suspect" systems
- Checking out suspected employees and accounts
- Investigating suspect system events
- Checking conformance to standards of installed systems
- Intrusion detection

Solutions on SWAN Configuration Guidelines

- List of required patches
- System configuration requirements
  - End User Desktops
  - Servers
    - home directory servers
    - ftp servers
    - www servers
    - console servers
    - personal databases

Solutions on SWAN
Configuration Guidelines

- Outside the firewall
  - Minimal "bare-bones" systems
    - no window system
    - no compilers & tools
  - No network services beyond requirements
    - no sendmail
    - no NFS/lockd/statd
    - no reusable passwd access
  - Compartmentalization
    - run services in separate environments

Solutions on SWAN Auditing

- Locally
  - Conformance with system configuration
  - Automated SunSWAT
- Remotely
  - Over the WAN with Autohack and other tools
- Over the internet
  - Firewall complex
  - Systems outside the firewall

Solutions on SWAN Auditing with Autohack

- Batchmode remote vulnerability checking
  - Remotely checking for known vulnerabilities
  - Builds database
    - which system runs which services
    - what version of services systems run
  - Rescan of database allows quick identification of hosts vulnerable to new bugs
  - http://coast.cs.purdue.edu /pub/doc/tools/muffett-wanhack.ps

Solutions on SWAN Summary

- We still have a relatively open network
- Achievements
  - steady decline in incidents involving outside
  - considerably fewer insecure systems
- Problems
  - rules slow down progress
  - administrator and user awareness
  - EOL systems

Summary

- Obsolete but hard to avoid
  - IP addressed based authentication
  - Reusable passwords
- Up and coming
  - Encryption; there's no substitute
  - SSH
  - virtual private networks (SKIP)
- Don't forget User Education
  - They are *most* of the problem

For Further Information

- Practical Unix Security
    - New edition out now
- Dan & Wietse's book/tutorials
    - free tutorials