Computer security

Knut Omang
Ifi/Oracle Apr 30, 2014

(includes content by: Vera Goebel, Matija Pužar, Željko Vrba and Andrew Tannenbaum)

ORACLE

Today: Computer security

- Types of threats
- Prevention of unauthorized access
  - Standard OS measures
- Outside attack categories
- Dangers lurking on the inside
- OS strategies and defenses

ORACLE

What is computer security?

Very broad term:

- File system security
- Network security
- Data integrity
- Data confidentiality
- Data loss
- Physical security
- Social engineering

ORACLE

Threat model

- Understanding the threats:
  - What are we protecting?
  - From whom are we protecting it?
- ideally, the system should be *designed* for security!
- A chain is not stronger than it's weakest link
  - Where is additional resources best spent?
- The simplest is often the best

ORACLE

Security goals and threats

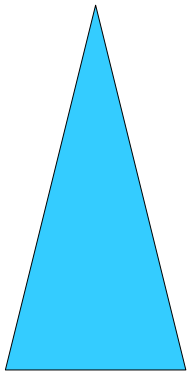
Goal	Threat
Data confidentiality	Exposure of data
Data integrity	Tampering with data
System availability	Denial of service
Resource protection	Misuse of resources

Some resource types:
- Money
- Computer resources
- Network bandwidth
- Call charges
- Credentials/trust/identities
- …

ORACLE

Types of threat

- Casual prying by non-technical users
- Script-kiddies
- Snooping by insiders
- Determined attempt to make money
- Commercial, military or government espionage



level of effort/cost needed to protect the system

ORACLE

Trends…

- Better and easier to use encryption tools
- Increasingly complex systems
- Web applications
  - advanced content
  - mix of script/program - server side/client side
- More and more at stake (?)

ORACLE

Today: Computer security

- Types of threats
- Prevention of unauthorized access
  - Standard OS measures
- Outside attack categories
- Dangers lurking on the inside

ORACLE

Preventing unauthorized access

- Contributes to all goals
  - but don't forget fire/earthquake or a malevolent user
- Initial system access: authentication
- Per user access: differentiation
  - Need-to-know..

ORACLE

OS security models

- None (single-user OS, e.g. DOS)
- Classical UNIX: (owner,group,others) rights
  - each user is a member of at least one group
- VMS -> Windows NT
  - users and groups in a list – Access Control List (ACLs)
  - Domain users/groups

ORACLE

Authentication

- Protecting access to the system
- Identifies user and his/her actions
- Something the user knows
  - username + password, pass-phrase
- Something the user has
  - physical object (magnetic card, smartcard)
- Something the user is
  - physical characteristics (biometrics)

ORACLE

UNIX permissions

```
-rw-r--r--    1 zvrba    ifi-a00     96031 2005-06-12 21:20 workplan.pdf
drwx--x--x    2 zvrba    ifi-a00      1024 2005-11-05 16:34 www_docs/
-rw-------    1 zvrba    ifi-a00      2402 2005-10-12 08:05 xorg.conf
```

owner, group, others; **r**ead, **w**rite, e**x**ecute; sometimes surprising semantics (e.g. delete files you don't own)

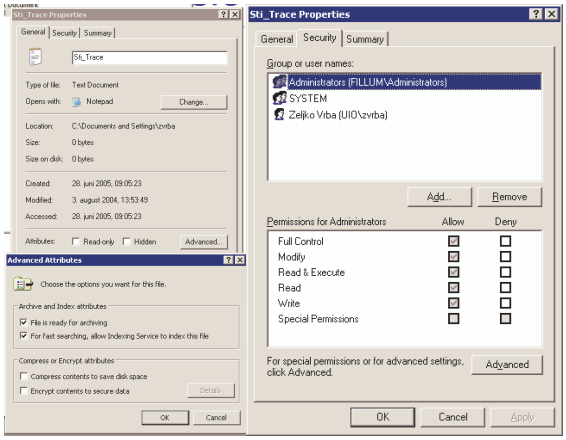
SUID, SGID and sticky bits

Newer:

- ACLs on files (getfacl, setfacl commands)
- Permissions to expose socket (ex.Secure Linux)

ORACLE

Windows permissions



both users and groups in the ACL!

security descriptors for each **object**

ORACLE

Theory: Bell-LaPadula

- Solve the confinement problem (information leakage)
- each object has a classification (label)
- each subject has a clearance and a security level
- two fundamental axioms:
  - the simple security property
    - Level k can only read objs at levels <= k
  - the *-property
    - Level k can only write objs at levels >= k

ORACLE

(Accidental) data loss

Common Causes

1. Acts of God: fires, floods, wars
2. Hardware or software errors: CPU malfunction, bad disk or memory, program bugs
3. Human errors: data entry, wrong tape mounted

Often cause more damage than intruders!
BACKUP! (data and location)

ORACLE

File system encryption

- encryption: data forever lost if key (or passphrase) is lost; **backup!**
- individual file vs. partition encryption
- transparent vs. non-transparent (separate program)
- windows upgrades and reinstallations can destroy the original EFS key!

ORACLE

System integrity

- Integrity of all system components (configuration files, binaries, etc.)
  - Trust that critical parts of system behaves as intended
- Discretionary access controls
  - Users can choose what to allow to who
- Mandatory access controls
  - the administrator can override and set policies for access

ORACLE

Today: Computer security

- Types of threats
- Prevention of unauthorized access
  - Standard OS measures
- Outside attack categories
- Dangers lurking on the inside
- OS strategies and defenses

ORACLE

Outside attacker categories

- Network service scans
  - Scan for vulnerable services
  - Attack vulnerability
- Network interception attacks
  - sniffing
  - man-in-the-middle
- Trojan horses/viruses
  - Email/web pages/CD-roms with embedded malware
  - Mobile code
- Theft/destruction..

ORACLE

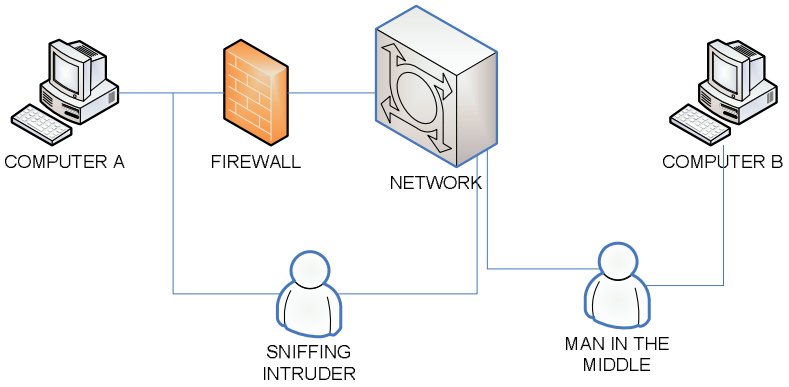
Network service scans+attacks

Look for known program versions with weaknesses, then exploit..

- Basic services:
  - Morris worm: finger daemon, buffer overflow
  - Code Red Worm: Buffer overflow + Microsoft IIS
  - Sendmail, Exchange, Bind, Apache
- Web applications
  - injection flaws
    - print ”select sensitive_data from account where user = ’$user’ ”
    - Steve Jobs & friends: sinus tone generator
  - cross site scripting:
    - Blog entries/im’s/comments that introduces new elements
  - Lots and lots more…
- Strikingly often instances of missing input validation!

ORACLE

Network interception attacks



data sniffing and/or modification; replay and man-in-the-middle attacks

use ssh, gpg/pgp and https: provide both data integrity and confidentiality

a question of **trust!**

ORACLE

Spoofing and phishing

- Spoofing: Masquerading as someone trusted
- Phishing: Using spoofing to trick user/program to give away sensitive information:
  - frequent PayPal spam
  - Fake login GUIs (or ATM frontends ...)
  - DNS spoofing/forging (+ bank application…)

Countermeasures:

- check Received:-mail headers and URLS
- never reveal sensitive data unless the query is expected (and even then be cautious!)
- Be critical to browser plugins and requests for more privileges..
- Run web browser with few privileges...

ORACLE

Increasing use of mobile code

- Postscript
- Document macros/additions
- Applets
- Browser plugins..
- ...

ORACLE

Denial-of-service attacks

- A service is overwhelmed with bogus traffic that effectively inhibits normal operation
- Stateful firewalls properly configured may help somewhat
  - But cannot always distinguish good from bad traffic (ex. http)
    - Example: Russia-Georgia war
- Distributed Denial-of-service and botnets
  - Hard to fully protect against
  - DDos + src address spoofing -> backscatter

ORACLE

Today: Computer security

- Types of threats
- Prevention of unauthorized access
  - Standard OS measures
- Outside attack categories
- Dangers lurking on the inside
- OS strategies and defenses

ORACLE

Insider attacks

- Password guessing
- Login spoofing
- Spyware
  - key logging, identity theft,…
- Opening up the system
  - Root kits
  - Trap doors
  - Logic bombs
- Providing confidential info to 3rd parties
  - Covert channels
    - Steganography: Images, empty disks with 'white noise'

ORACLE

Password guessing

- Alphabet size
- Simple one-way encryption
  - /etc/passwd
- One-way encryption with n-bit random value
  - n-bit "salt" (Unix: n=12)
- Protected passwd + lookup delay
  - /etc/shadow

ORACLE

What is the problem with this .profile?

....

PATH=.:$HOME/bin:/usr/bin:/bin:/usr/local/bin:/sbin:/usr/sbin
export PATH

....

ORACLE

Reasonable defaults

Make it easy(iest) to be secure – examples:

- Mandatory access control policies
  - Not possible to disable password or use 3-letter dictionary word or first name
- Umask/default file protection
- Make use of mount options
  - /usr read-only
  - /var read-write, noexec, nodev
  - nosuid where applicable

ORACLE

Mandatory access controls

- Linux
  - grsecurity (http://www.grsecurity.org)
  - SELinux (http://www.nsa.gov/selinux)
  - can cause compatibility problems with "badly behaved" software
- FreeBSD
  - MAC (http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/mac.html)
  - BIBA and MLS policies
- Proactive: confine damage if break-in occurs

ORACLE

Physical security

- Often neglected, but:
  - physical access is unrestricted access
  - do you trust your system administrator?
- Precautions:
  - data encryption (only cold storage safe!)
  - remove all recording devices
  - Faraday cage

ORACLE

Defenses

- Firewalls
- Service logging/alerting
- Intrusion protection software
  - tripwire
  - antivirus software
- Write-only storage for integrity checks
- Multiple layers (like ancient cities with fortresses..)
- Code signing

ORACLE

Firewall/NAT devices

- Software package on desktop
- Separate box
- Filtering traffic in both directions
- Typical home fw setup
  - network address translation (NAT)
  - everything above port 1024 is ok
  - traffic must be initiated from inside
  - well known insecure services blocked for outgoing as well

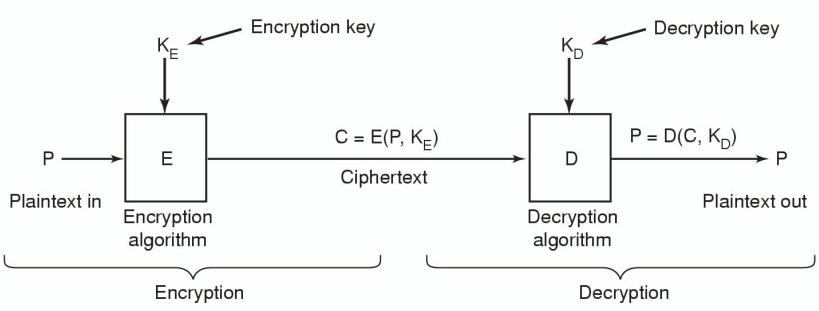
ORACLE

Typical firewall functions

- Masquerade/NAT
  - Make all inside machines appear to come from same IP(s)
- Block services
  - Inside AND outside!
- Interaction with services
  - "Universal Plug and Play" - uPnP support
  - Other schemes for auto-modify..
- Different protocol levels
  - IP layer
  - Layer 4: TCP/UDP/IPsec
  - ALGs (ftp,SIP,IPsec/TCP,IPTV, ...)

ORACLE

Cryptography



an important **foundation**, but far from enough; **secure protocols** are also needed. **NEVER design your own, use proven and tested solutions, e.g. OpenSSL (http://www.openssl.org)**

random numbers often forgotten, but crucial part of secure system (fatal Netscape flaw)

ORACLE

Symmetric cryptography

- One key both for encryption and decryption
- Good algorithm is **publicly reviewed**
  - DES (being phased out, replaced by AES/Rijndael)
  - IDEA, Blowfish, Twofish, Serpent, etc.
- Problem: secure key exchange

ORACLE

Asymmetric cryptography (1)

- All users pick (public, private) *key pair*
  - public key cryptography
- Digital signatures and encryption
  - public key: encryption/verification
  - private key: decryption/signing
- algorithms:
  - DSA, RSA (1024 bits min. secure today)
  - ECC has smaller key size

ORACLE

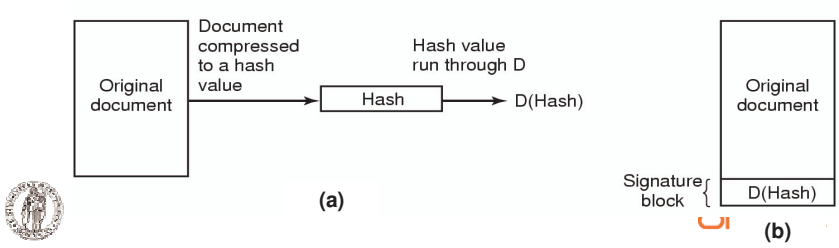
Asymmetric cryptography (2)

- Slow; mixed scheme is used:
  - *random symmetric* key for bulk encryption
  - encrypted by public key of recipient
- Trust problems
  - Is the key owner really he who claims to be?
  - hierarchical: X509 certificate authorities (e.g. Verisign) and why should we trust them?
  - other: ssh (personal verification)
- Key distribution: public servers (e.g. LDAP) and how trustworthy they are?

ORACLE

Digital signatures

- rely on one-way hash functions as cryptographic primitive
  - SHA-0, and MD5 (**both broken!**)
  - SHA-1 (considerabely weakened), SHA256, etc.
  - RIPEMD 160
- ensure **data integrity** and **authenticity**



Hardware support

- "Dongles"
- Trusted Platform Module (TPM)
- Macrovision, CD software copy protection, DVD, Blu-ray?

- Where is the control?
- 'Security' of vendors vs security for the sys.owner...
  - Security of continued operation...

ORACLE

Threat model revisited

- Understanding the threats:
  - What are we protecting?
  - From whom are we protecting it?
- ideally, the system should be *designed* for security!
- A chain is not stronger than it's weakest link
  - Where is additional resources best spent?
- The simplest is often the best
- Trade-offs...

ORACLE

Security vs simple to use

- How many passwords can *you* remember?
- What will happen if network access is forbidden but needed to work efficiently?
  - hospitals/patient data
  - Laptops? Home networks?
- Windows: functionality vs. Security
  - What is the first settings people change after installing windows?
  - What privileges to grant the ordinary user..
  - Ever experienced a slow windows box due to virus protection software?
- What do you do if your favorite game does not work with the firewall?
  - Campus pathways…
  - Tanenbaum: "Features are the enemy of security"

ORACLE

Secure system design

1. System design should be public
   - security by obscurity does not work
2. Reasonable defaults (no/minimum access)
3. Check for current authority, not only at the beginning
4. Give each process/subprocess least privilege possible
5. Protection mechanism should be
   - simple, uniform
   - well supported by system – security is not an add-on feature
6. Scheme should be psychologically acceptable

ORACLE