Lecture Notes on Internet Security

Allen Dutoit

Technische Universität München

Lehrstuhl für Angewandte Softwaretechnik

February 2, 1998

Odds and Ends

- February 6, lecture on Re-engineering by Prof. Bruegge

Outline

- ❖ A worm example
- ❖ What is computer security?
- ❖ Why is internet a security problem?
- ❖ Typical attacks
- ❖ Solutions
- ❖ Summary
- ❖ Security related courses at TUM
- ❖ References

Internet worm 1988

- 3000-4000 computers were infected (about 5% of the internet)
- Many ghost processes were consuming CPU time
- Killing these processes did not seem to help
- Rebooting machines did not cure the problems
- The problem only occurred on sun’s and vax’en

Internet worm overview

- Internet worm propagated by exploiting three different vulnerabilities:
  - **sendmail debug mode**
  - **fingerd buffer overrun**
  - **accounts with no or weak passwords**
- Several features were designed to conceal its identity
  - **command shell was zero'ed out**
  - **all strings in the binary were XORed**
- Once on the machine, the worm would collect information:
  - **/etc/hosts**
  - **.rhost files**

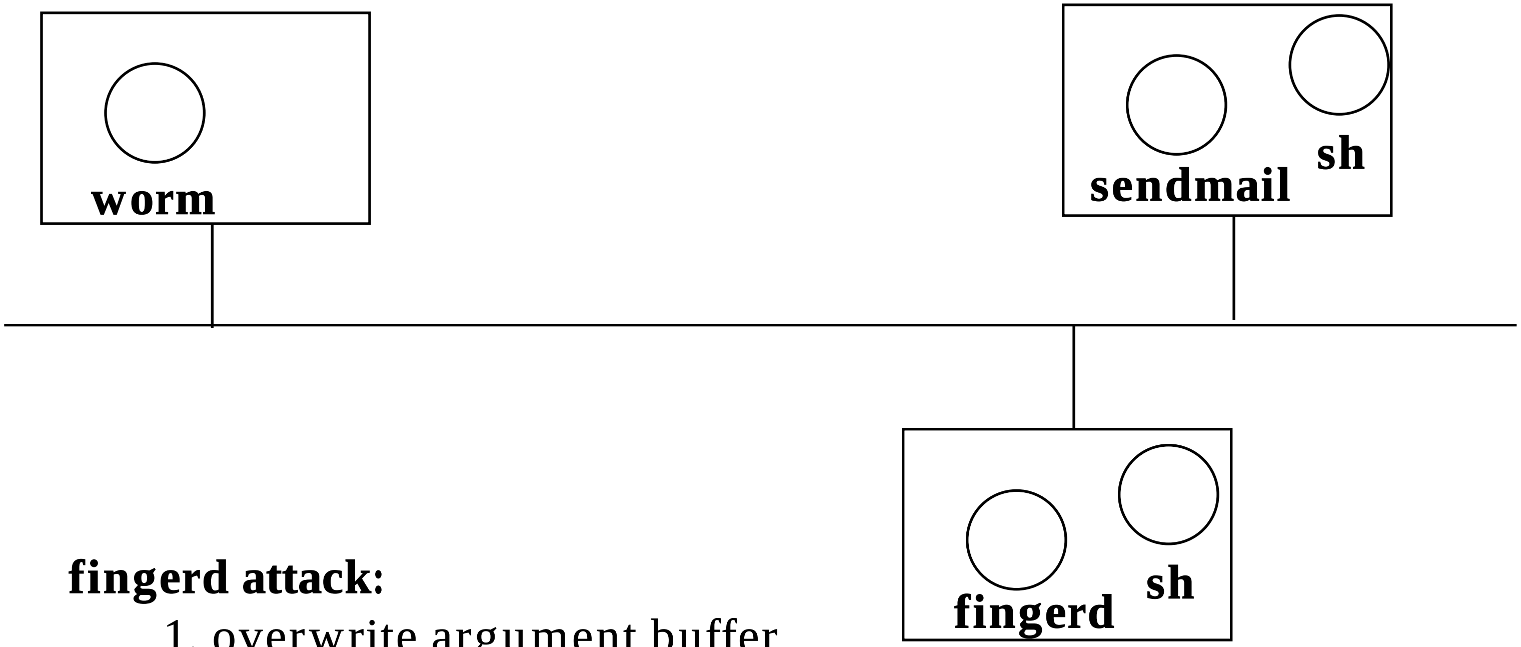
Internet worm: propagation

local attack

1. try passwords from a dictionary
2. use `rsh` to exploit network of trust

sendmail attack:

1. put `sendmail` in debug mode
2. have `sendmail` fork `sh`
3. use the shell to download and compile a new worm



fingerd attack:

1. overwrite argument buffer and replace `finger` with `sh`
2. use the shell to download and compile a new worm

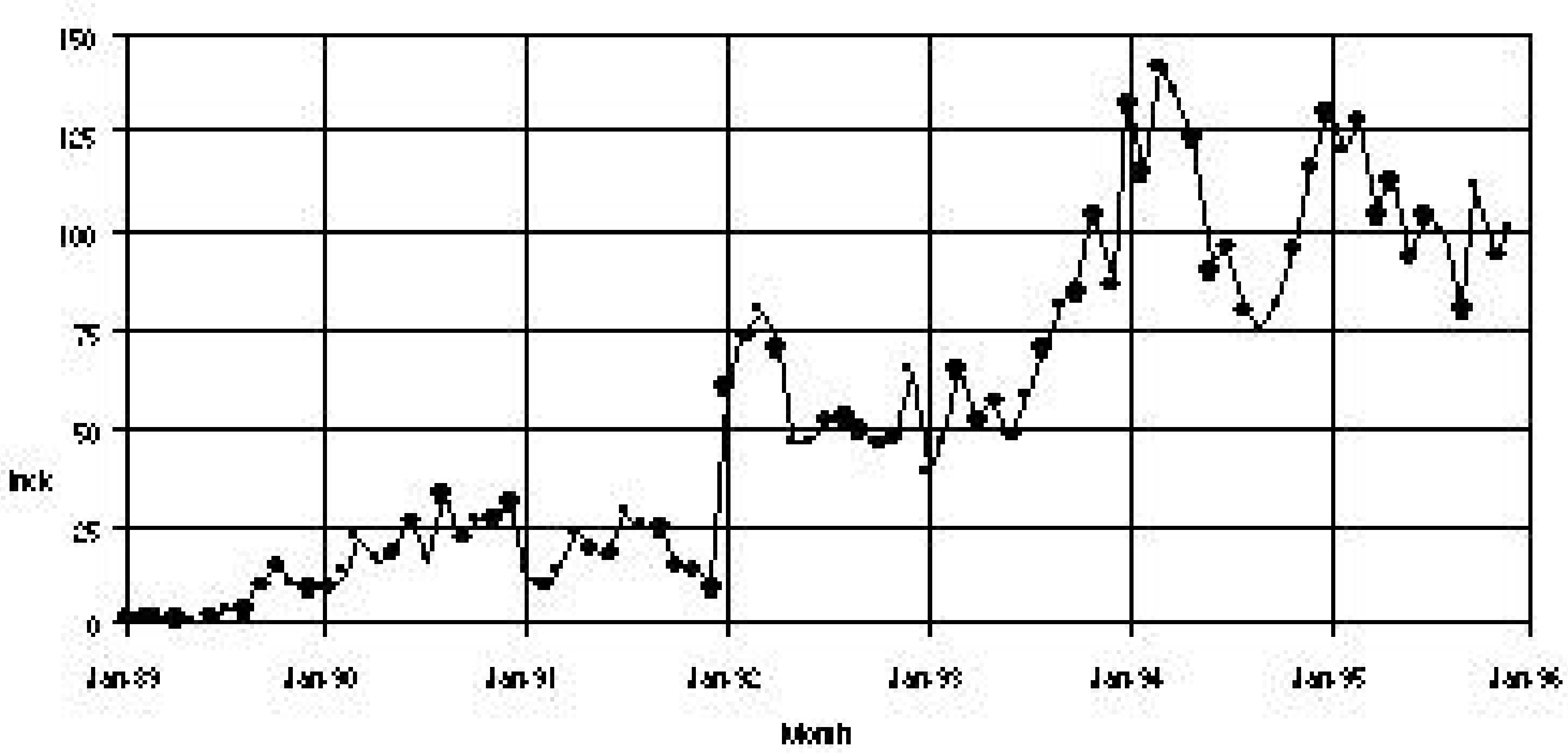
Internet worm: aftermath

- Estimated damage
  - **5% of the internet affected(80’000 nodes)**
  - **Disrupted e-mail, work at many universities and research institutions**
  - **Thousands of sysadmin hours**
  - **Possibly several millions of dollars in total costs.**
  - **The internet took 1 week to recover.**
- Robert T. Morris was
  - **suspended for 1 year from Cornell**
  - **convicted of ‘Federal Computer Tampering’**
  - **$10’000 of fine, 400 hours of community work, and 3 years probation**
- CERT was created …

CERT® (Computer Emergency Response Team)

- Created in 1988 in the aftermath of the Internet Worm
- Funded by DARPA (Defense Advanced Research Projects Agency)
- Provides incident response services to sites that have been the victims of attack
- Publishes security alerts
- Researches security and survivability in wide-area-networked computing
- Develops information to improve security at your site.

CERT: Trends



150
125
100
75
50
25
0
Incid
Jan-89
Jan-90
Jan-91
Jan-92
Jan-93
Jan-94
Jan-95
Jan-96
Month

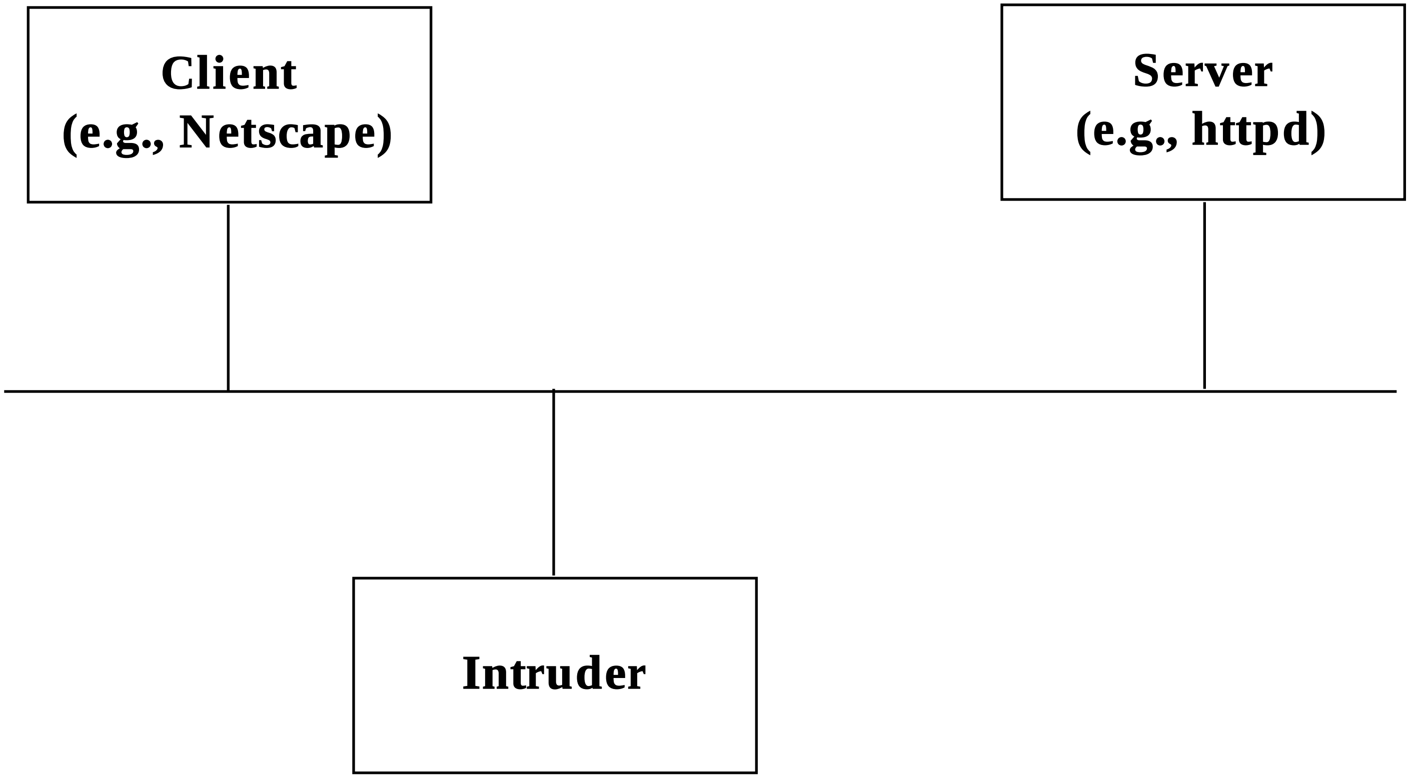
Why is internet security becoming an issue?

- Many more hosts
  - **several millions of nodes,**
  - **doubles every 10-15 months)**
- WWW increased the popularity of the internet
- Internet is not a research network anymore
  - **buy computers, software, stocks, services**
  - **advertisement medium**
  - **news medium**

What is computer security?

- Data confidentiality
  - **passwords**
  - **credit card numbers**
  - **e-mail**
- Data integrity
  - **...**
- Availability of service
  - **spamming**
  - **ping attacks**
- Non repudiation
  - **spoofing**

Terms and concepts



Typical attacks

- Weak passwords
- Bugs
- Misconfiguration
- Protocol weaknesses
- Social engineering
- Physical security

Passwords

- Typical setup
  - **legitimate user / password combinations are stored in an encrypted file**
  - **users authenticate by typing a user / password combination**
  - **password is encrypted and compared to stored copy**
- Important properties
  - **encryption should be a one way function**
  - **encryption should be SLOW**
  - **a seed is appended to the password such that two users with the same password are encrypted differently**

Password issues

- `crypt()`
  - **1 second in 1976**
  - **1ms in 1990**
  - **1 µs using DES hardware**
- A dictionary of 250’000 can be encrypted in less than 5 minutes on a typical desktop machine.
- `/etc/passwd` is world readable
- Password guessing algorithms are easily distributed
- Typical users use short and common passwords (including their name)

Password attacks: crack 5.0

- Fast crypt function
  - **typically 1 encryption < 1ms**
- Large dictionary
- Support for distributed computing
- Rules for generating combinations
  - **hello -> olleh, h3llo, h3ll0, 0Ll3H**

- Given enough CPU time, can typically guess 15-25% of account passwords
- First passwords are guessed within minutes

Bugs

Specific bugs can be taken advantage of to have a server program execute code.

- Example: buffer overrun:
  - **usually causes the program to crash**
  - **by carefully choosing the input, can be used to modify the program and execute commands**

- Example: user input in shell scripts
  - **user input is often included as is in shell scripts**
  - **by including characters such as " ; \n, shell commands can be executed by the server**

Bugs: NCSA httpd 1.5 and Apache 1.0.3

- Attack

```
http://www.victim.com/cgi-bin/phf?Qalias=
  x%0a/bin/cat%20/etc/passwd
```

- Vulnerability
  - **The phf CGI program uses the URL to construct a shell command**
  - **The line return character was NOT filtered out**
  - **Instead of executing:**

    ```
    % phf -m Qalias=“x /bin/cat /etc/passwd”
    ```

  - **It executed:**

    ```
    % phf -m Qalias=x
    % /bin/cat /etc/passwd
    ```

Bugs: phf attack

- Vulnerability discovered in February 1996.
- Many web sites were still successfully attacked using this method in late 1996 and 1997.

- Workarounds:
  - **repair and recompile cgi scripts**
  - **remove phf and other related scripts**

Misconfiguration

- Network services whose access rights are not configured properly

- Examples:
  - **Anonymous ftp**
  - **Log files with world readable or world writable permissions**
  - **Default accounts with well know passwords**

Misconfiguration example: www.x.edu

- ❖ Anonymous ftp could write files in incoming directory
- ❖ www and ftp servers located on same machine
- ❖ Logs were not reviewed on a regular basis

-> ftp was used to store stolen files and used as a pirate distribution site

www.x.edu (continued)

- The incident lasted several months.
- The problem was discovered only when the site became popular.
- Once the problem was repaired, the attackers attempted to use www to retrieve the stolen files.
- That attack failed, triggering other types of attacks.

- The web server held fast, but was unsuable for more than a week due to the load.

Protocol weakness

- Many protocols were not designed with security in mind.
  - **IP spoofing**
  - **TCP ACK**
  - **ping**
- Many programs (including web browsers) allow clear passwords to be transmitted on the network
- X11 allowed anybody to look at an arbitrary display including keystrokes

Social engineering

- Email messages seeming to come from a system administrator asking to change a user’s password to a specific password.
- Phone calls from persons impersonating system administrators or law officials asking for a password.

Physical security

- Unsecured terminals
- Unsecured backup tapes
- ‘Lost’ or recycled backup tapes
- Recycled hard disks

Solutions

- Prevention
- Administration
- Policy

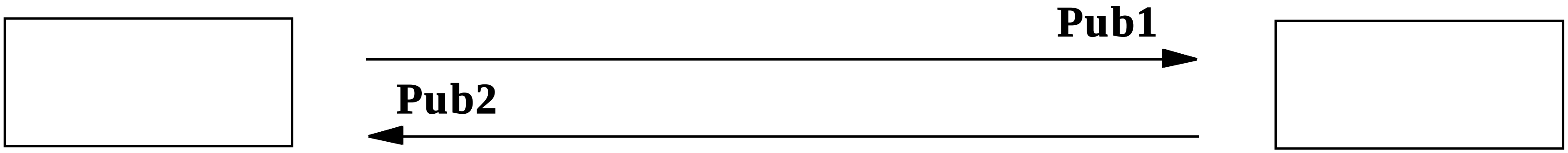
Prevention: encryption

- Secret key encryption
  - **one key is known by both sender and receiver**
  - **selected key allows both encryption and decryption**
  - **drawback: key distribution**
  - **Examples: DES, IDEAL**

- Public key encryption
  - **one key, known to everybody, is used to encrypt**
  - **one key, known only to the receiver, is used to decrypt**
  - **drawback: expensive in CPU time**
  - **Example: RSA**

Encryption: example

1. Exchange of public keys

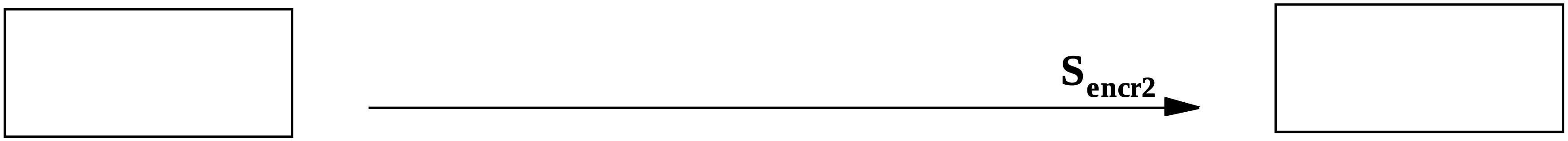


Pub1

Pub2

2. Generation of secret key S

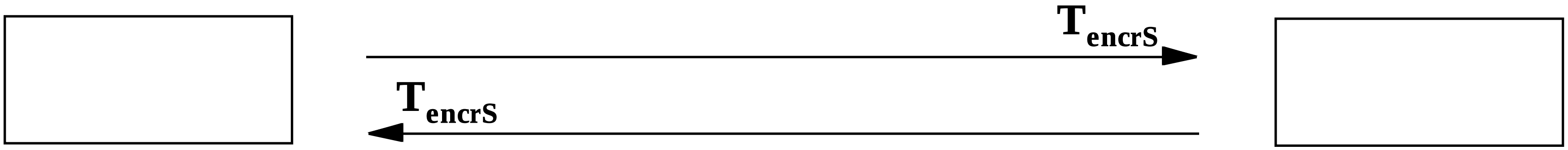
3. S is encrypted using Pub2



S_{encr2}

4. S_{encr2} is decrypted using priv2

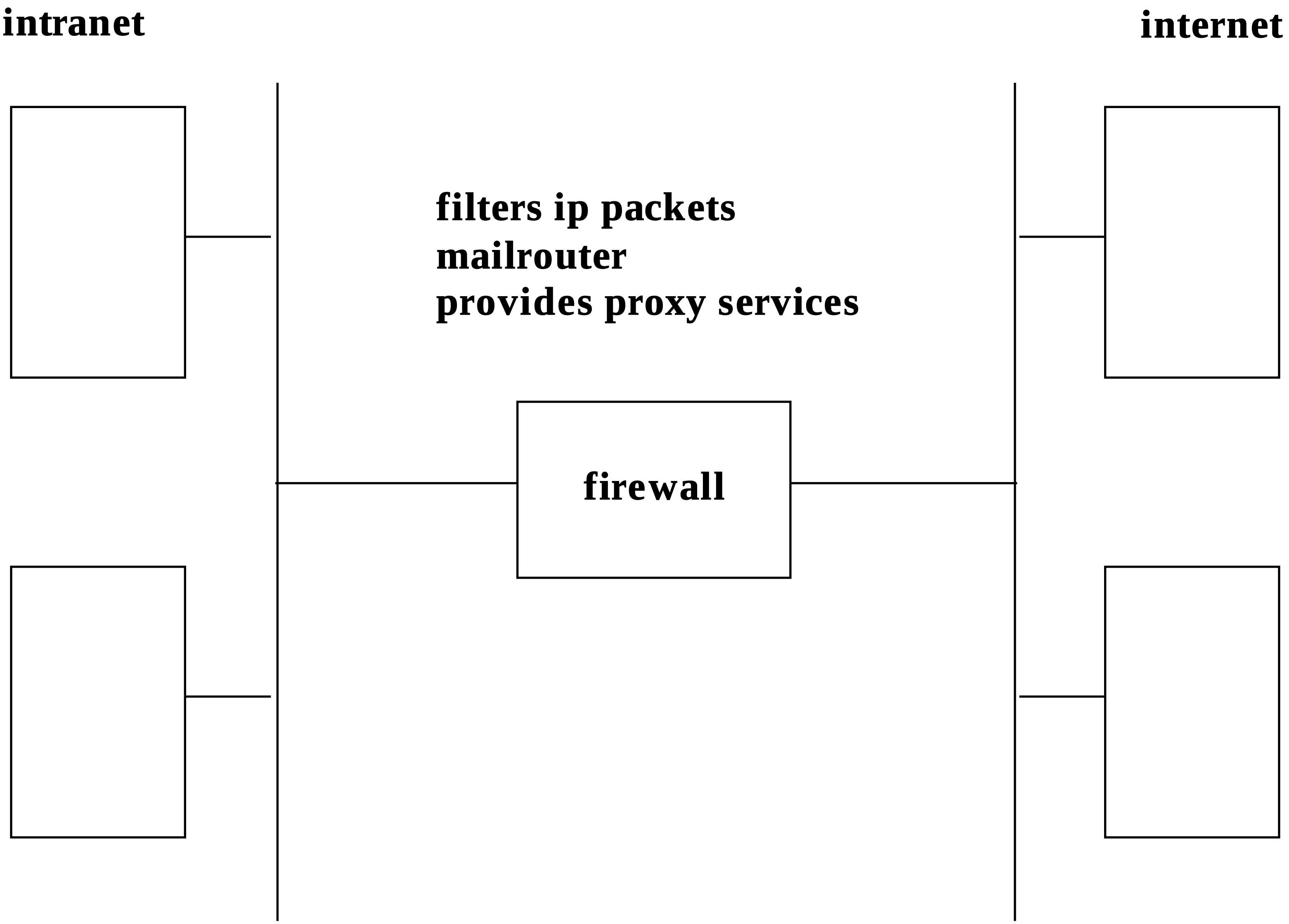
5. Subsequent traffic is encrypted and decrypted with S



T_{encrS}

T_{encrS}

Prevention: firewall



Detection: File integrity checking

- Tripwire (coast.cs.purdue.edu):
  - **computes signatures for a set of files (e.g., everything part of the operating system**
  - **in subsequent runs compares the original signature with the current signatures**

- Can be used to monitor which files change (e.g., new software installations)
- Can be used to detect intrusions (e.g., trapdoors, fake versions of login)

Detection: logs

- Tcp wrappers (written Wietse Venema, win.tue.nl)
  - **Allows logging of any tcp service request**
  - **Enables simple access rights for services that do not provide such functionaltiy**

- syslogd (unix daemon)
  - **Provides a unified logging facility**
  - **Enables remote logging**
  - **Enables logging of multiple machines**

Automated tools

- Tools which scan networks of workstations for known security wholes (bugs or configuration).
  - **SATAN**
  - **ISS**

- Double edge:
  - **Can be used for prevention as well as for attack**

Administration

- Responsibility for the comprehensive security of a service or a site

- Most administration tasks should be centralized
  - **Operating systems upgrades**
  - **Network software upgrades**
  - **Account creation and removal**
  - **Monitoring of advisories**
  - **Monitoring of logs**
  - **Point of contact in case of attack**

Policy

- Define the responsibilities of the organization and the users
  - **Is it ok to share an account?**
  - **Is email going to be read?**
  - **Are .rhosts file going to be read?**
  - **What can of monitoring will be in place?**
  - **What is the password policy?**

Recovery

- Determine what happened from the logs
- Report the incident
- Use backups to get rid of any backdoor, HOWEVER:
  - **patch the holes which were used**
  - **make a new backup**
- Improve infrastructure, procedures, and policy accordingly

Concluding remarks

- Computer security IS an issue
- It will get worse before it gets better
- There exist technical solutions for many security problems
- Computer security is not only a technical issue, but also administrative, social, and legal.

Courses related to security at TUM

- Cryptology by Dr. Gerold (Zenger)
- Secure computer systems
  by Dr. Eckert (Spies)
- Software for high security systems
  by Dr. Saglietti (Jessen)
- Data protection and safety
  by Dr. Dierstein (Bayer)

References

❖ FIRST	www.first.org
❖ CERT	www.cert.org
❖ AUSCERT	www.auscert.org.au
❖ DFN-CERT	www.cert.dfn.de
❖ COAST	coast.cs.purdue.edu