Systemmanagement und Sicherheit

(System Management & Security)

Prof. Dr.–Ing. Damian Weber

Hochschule für Technik und Wirtschaft des Saarlandes

dweber@htw-saarland.de

http://www-crypto.htw-saarland.de

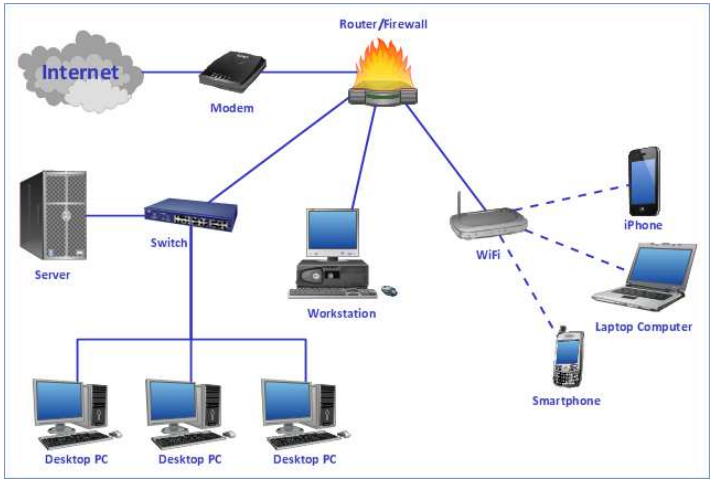
ISL

- 11 FreeBSD machines `isl-c-01 ... isl-c-10 isl-s-01`
- KDE
- your STL-account, STL-home directory
- start terminal
- editor *kate*, *fxite*, *nano*, *joe*, *mp-5*, *leafpad*
- compiling a program with cc (=clang) or gcc (GNU)

  `cc -Wall -c prog.c`
- linking a program with gcc

  `cc -o prog prog.o`
- USB sticks: `usbmount`, `usbumount`

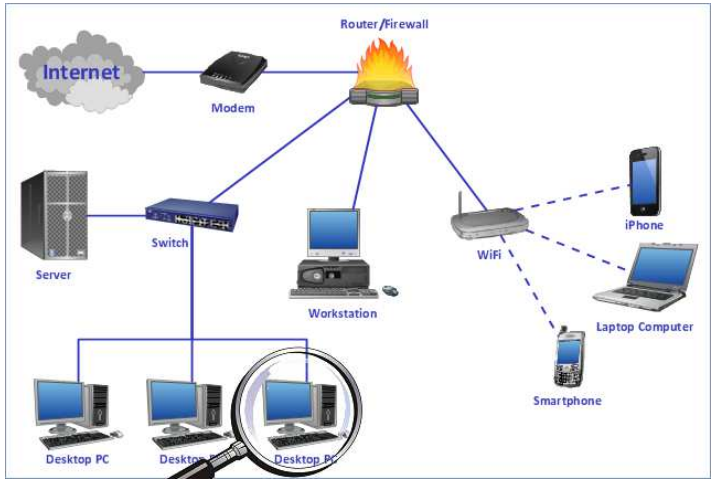
How Secure is Your Network?



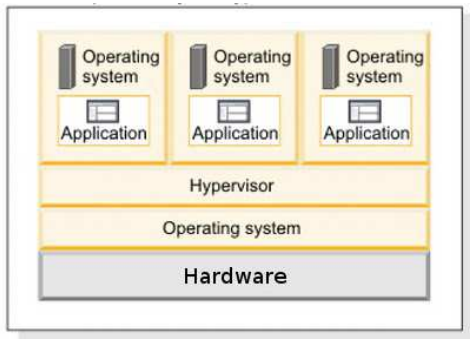
Let's Ask an Expert...

Interview: `https://www.youtube.com/watch?v=XEVlyP4_11M`

How Secure is Your Desktop?



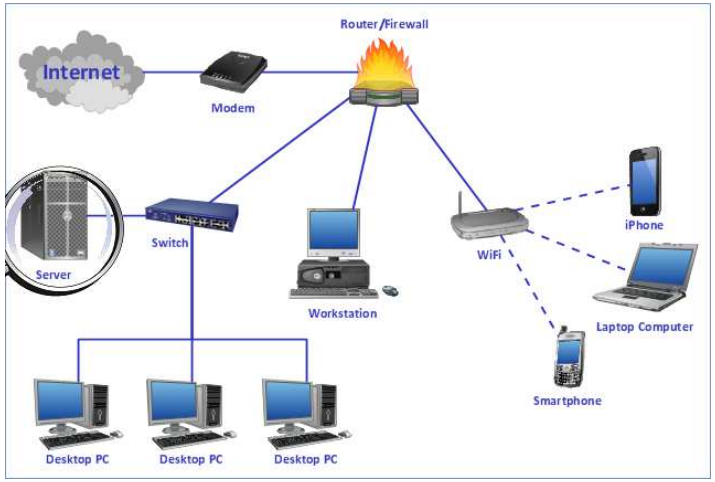
How Secure is Your Desktop?



the lower layer is stronger than the upper layer

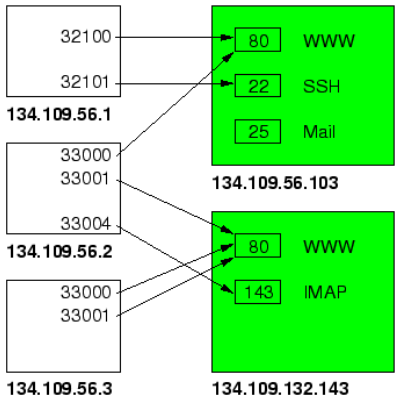
at every layer, malicious actions have been used

How Secure is Your Server?



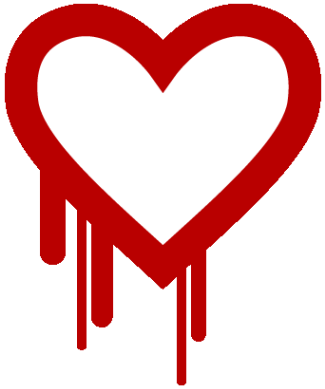
How Secure is Your Server?

server program, uses os with admin privileges. . .



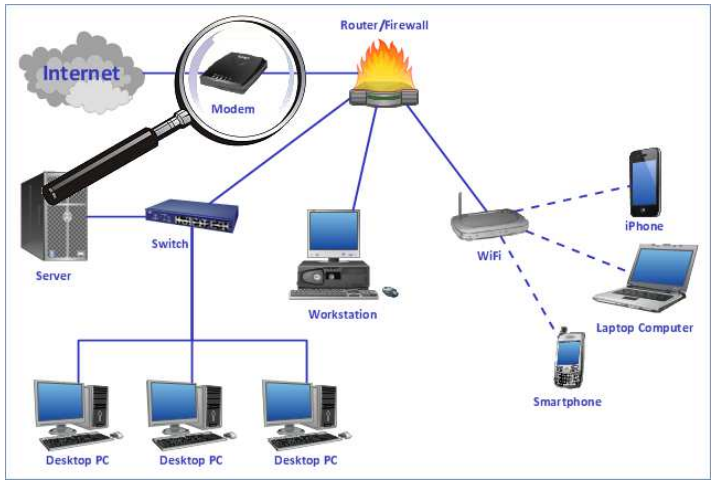
How Secure is Your Server?

server program, programming error on December 31, 2011



`http://heartbleed.com/` April 7, 2014

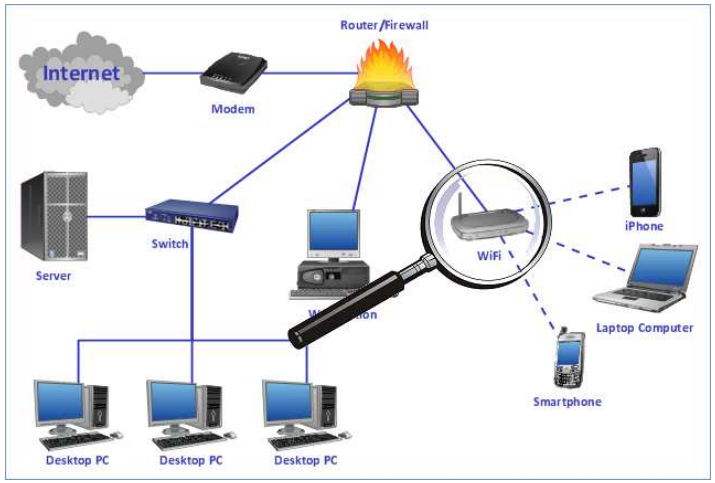
How Secure is Your Modem?



How Secure is Your Modem?

firmware buggy, default admin passwords, vulnerable web servers, ...

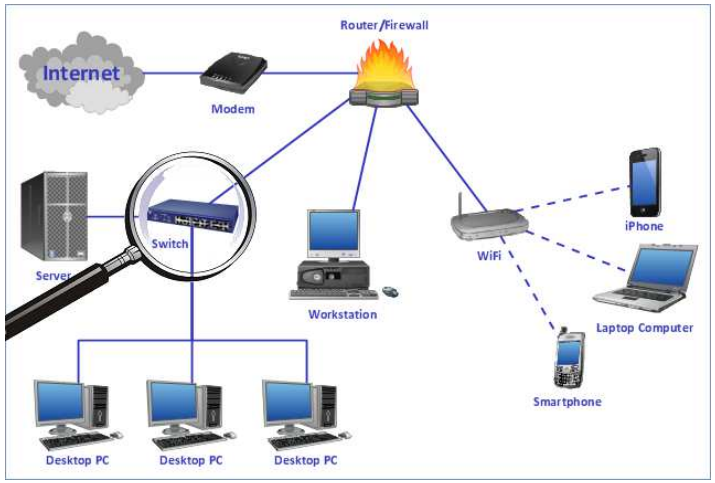
How Secure is Your WiFi?



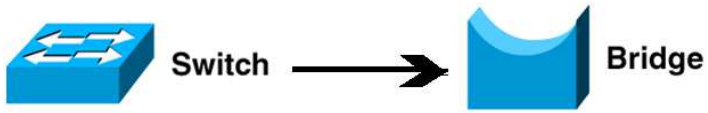
How Secure is Your WiFi?

only WPA2 not broken

How Secure is Your Switch?



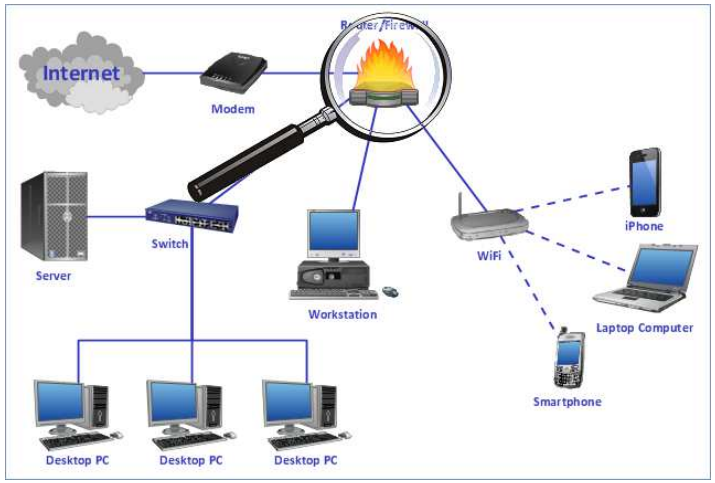
How Secure is Your Switch?



MAC flooding confuses the switch, which then works as hub

attack tool: **ettercap**

How Secure is Your Firewall?



How Secure is Your Firewall?

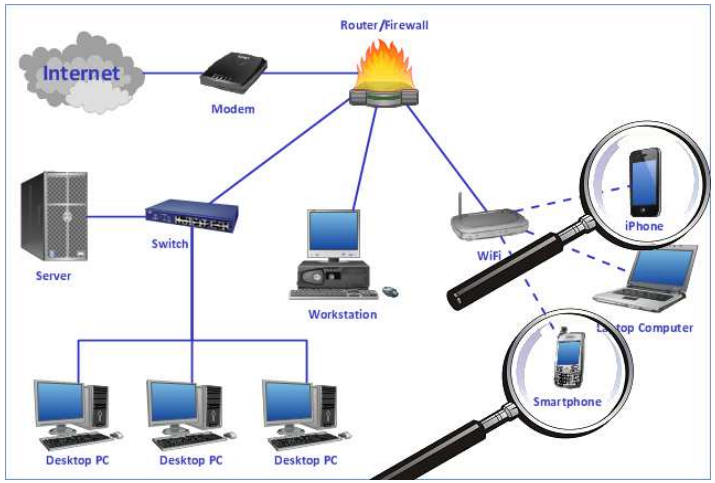
Port List for Firewall Configuration

Purpose	Type	Port Range	Protocol
Secure shell	TCP	22	SSH
Web	TCP	80	HTTP
Secure web	TCP	443	HTTPS
H.323	TCP	1720	H.225
Web conferencing	TCP	1935 (or 80, 443)	RTMP (Macromedia)
H.323	TCP	62000 - 62999	H.245
Network Time Protocol	UDP	123	NTP
SNMP	UDP	161	SNMP
SIP	UDP	5060	SIP
SMTP	TCP	25	E-Mail notification (outbound to a mail server only)
LDAP Integration	TCP	8404 or 389	LDAP
Voice packets	UDP	16384 - 32767	RTP, RTCP (paired)

only as secure as the firewall code

only as secure as your configuration

How Secure is Your Phone?



How Secure is Your Phone?

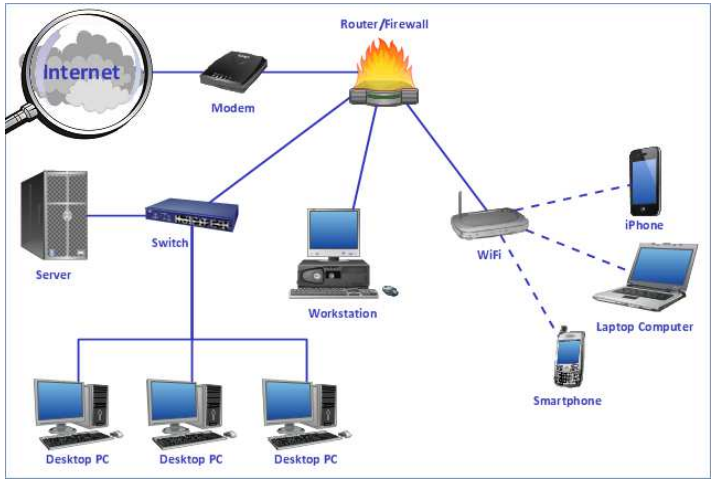
only as secure as

- your operating system (PRISM-Providers: Apple and Google)
- your applications
- your PlayStore / AppStore
- the WLANs you use
- ...

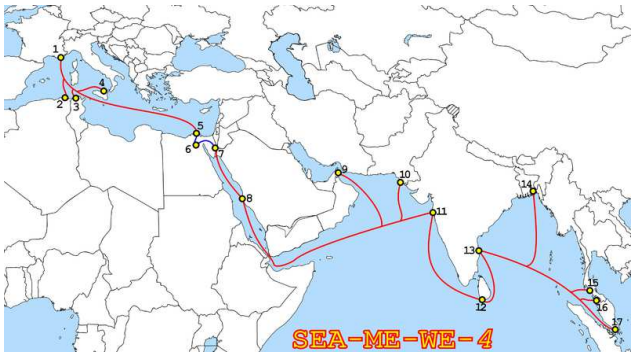
Everything Secure At Your Place?

What if an attacker steals your hard drive?

How Secure is the Internet?



How Secure is the Internet?

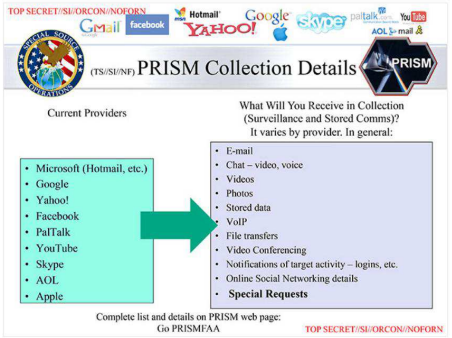


part of the physical layer

How Secure is the Internet?

Providers and data

The PRISM program collects a wide range of data from the nine companies, although the details vary by provider.

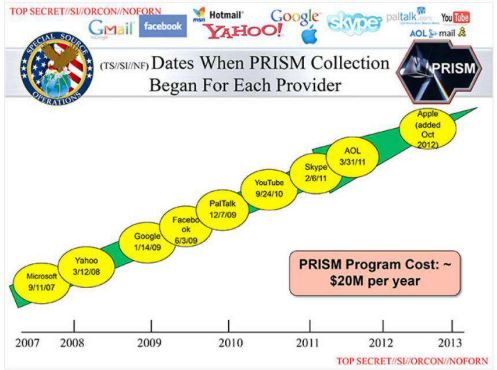


PRISM-Providers for NSA

How Secure is the Internet?

Participating providers

This slide shows when each company joined the program, with Microsoft being the first, on Sept. 11, 2007, and Apple the most recent, in October 2012.



PRISM-Providers for NSA

Good Journalism?

yes, they can

Security is Relative!

Threat Model

- power of an adversary
- time
- capabilities

What is Computer Security?

action	risk	prevention
read e-mail	get malware	software updates
read e-mail	others eavesdrop	encryption
browse the web	get malware	software updates
buy goods	credit card number stolen	trusted service
run applications	bugs, unavailability	software updates
run applications	get malware	open source
run operating system	intruder	system updates
run operating system	intruder	open source
run network	intruder	firewall config

Critical Security Controls

sans.org
20 Critical Security Controls - Version 5

1: Inventory of Devices
2: Inventory of Software
3: Secure Config for Hardware/Software on Workstations
4: Continuous Vulnerability Assessment and Remediation
5: Malware Defenses
6: Application Software Security
7: Wireless Access Control
8: Data Recovery Capability
9: Security Skills Assessment
10: Secure Config for Network Devices
11: Limitation+Control of Network Ports/Protocols/Services
12: Controlled Use of Administrative Privileges
13: Boundary Defense

14: Maintenance/Monitoring/Analysis of Audit Logs
15: Controlled Access Based on the Need to Know
16: Account Monitoring and Control
17: Data Protection
18: Incident Response and Management
19: Secure Network Engineering
20: Penetration Tests and Red Team Exercises

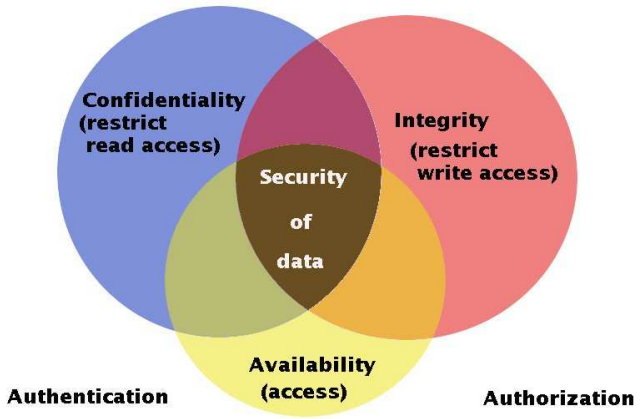
Computer Security? A Personal Opinion.

Use a system where you...

- ...don't have to worry about viruses and trojans:
  ⇝don't use Microsoft Windows
- ...can solve problems by code inspection:
  ⇝use open source software
- ...can verify all cryptographic steps:
  ⇝use open source software
- have trust in control of source code
  ⇝don't use Linux

⇝use one of the BSD operating systems (favourite: FreeBSD)

Generally Accepted Computer Security Goals



Generally Accepted Computer Security Goals

- in terms of data: **CIA**
  - confidentiality (privacy)
  - integrity (non-alteration)
  - availability (reliable timely access)
- in terms of roles
  - authentication (proof of identity)
  - authorization (what are you allowed to do?)
- linking these goals
  - authenticity (proof of source of that data)
  - accountability (who is responsible for that modification?)
  - assurance (why should I trust this system?)

If Data is Non-Alterable and Available but not Confidential

Message (Data)
„The summer time in Europe ends on October 26th, 2014."

Cryptographic hash:

`f2a04587b9c43d28326fcab065b182f748a94455ad1a81d30d325c5a71906077`

The summer time in Europe ends on October 26th, 2014.

If Data is Altered, Hash is Altered

„The summer time in Europe ends

on November 26th, 2014."

`a39c22c3b09c557f24223efb1b1331d9`
`4c575a121eb700bd6bad98440f8e1eb4`

Computing Hashes

You may compute cryptographic hashes by

```
echo -n "(insert some text here)" | sha256
```

Cutting edge: SHA–3 (Keccak), not yet implemented

Other SHA–3 finalists

- BLAKE (very fast, authors Aumasson, Meier et al.)
- Grøstl (Knudsen, Rechberger et al.)
- JH (author Wu)
- Skein (authors Schneier, Callas et al.)

If Data is Confidential and Available but Altered

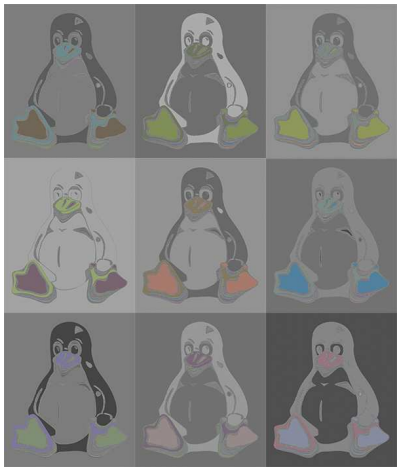
```
$ hexdump -C test.enc.orig
53 61 6c 74 65 64 5f 5f  f2 aa 19 c9 ef 85 af 5e
48 ec 88 a0 28 99 11 41  bd 43 b3 c5 38 84 07 ab
3c de e4 4b 4f c3 b6 11  08 59 1e 0f b5 99 ab dc

$ hexdump -C test.enc
53 61 6c 74 65 64 5f 5f  f2 aa 19 c9 ef 85 af 5e
48 ec 88 a0 28 99 11 41  aa 43 b3 c5 38 84 07 ab
3c de e4 4b 4f c3 b6 11  08 59 1e 0f b5 99 ab dc
```

decryption of altered data usually gives garbage

exception: electronic-codebook-mode (ECB)
(uses independent blocks)

ECB-Mode Encrypted Penguin



encryption is block by block

$\rightsquigarrow$ every block gets another color

Encryption

- do not use ECB–Mode
- use CBC– or CTR–mode (recommendation Schneier/Ferguson)
- use AES or one of the finalists
  - Twofish (Schneier, Ferguson, Kelsey, Whiting, Wagner, Hall)
  - Serpent (Anderson, Biham, Knudsen)
  - MARS (Coppersmith et al., IBM)
  - RC6 (Rivest, patented by RSA)