

Systemmanagement und Sicherheit

(System Management & Security)

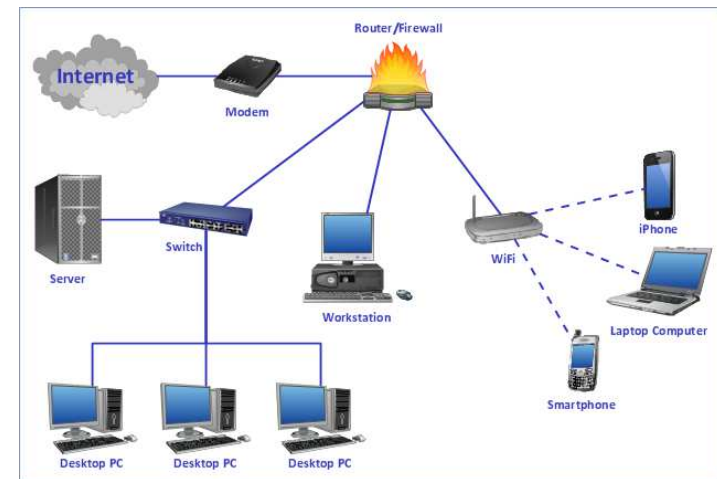
Prof. Dr.-Ing. Damian Weber

Hochschule für Technik und Wirtschaft des Saarlandes

dweber@htw-saarland.de

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

How Secure is Your Network?



ISL

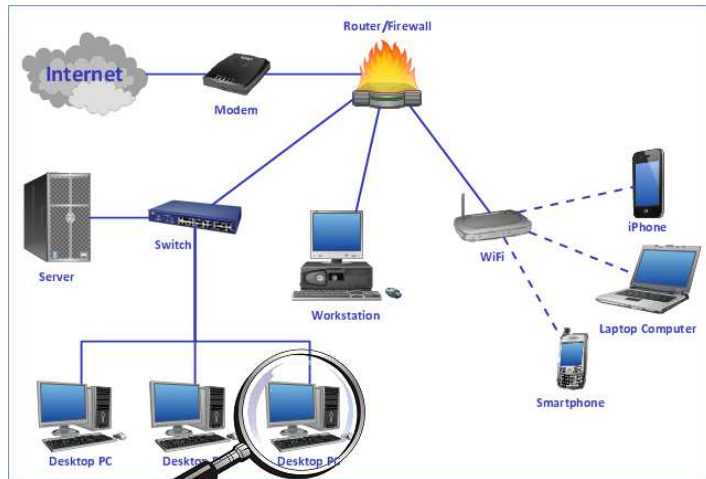
- 11 FreeBSD machines `isl-c-01 ... isl-c-10 isl-s-01`
- KDE
- your STL-account, STL-home directory
- start terminal
- editor *kate*, *fxite*, *nano*, *joe*, *mp-5*, *leafpad*
- compiling a program with `cc (=clang)` or `gcc (GNU)`
`cc -Wall -c prog.c`
- linking a program with `gcc`
`cc -o prog prog.o`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

Let's Ask an Expert...

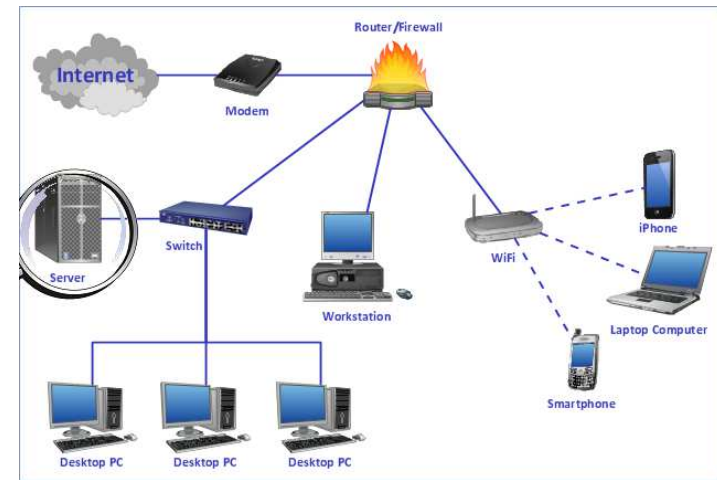


Interview: https://www.youtube.com/watch?v=XEVlyP4_11M

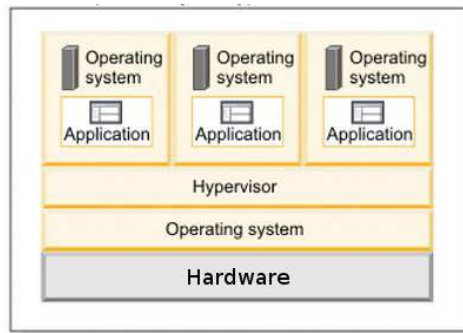
How Secure is Your Desktop?



How Secure is Your Server?



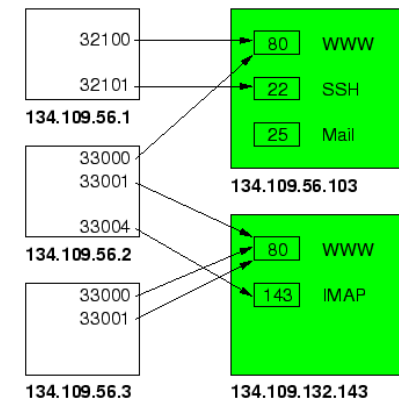
How Secure is Your Desktop?



the lower layer is stronger than the upper layer
at every layer, malicious actions have been used

How Secure is Your Server?

server program, uses os with admin privileges...



How Secure is Your Server?

server program, programming error on December 31, 2011



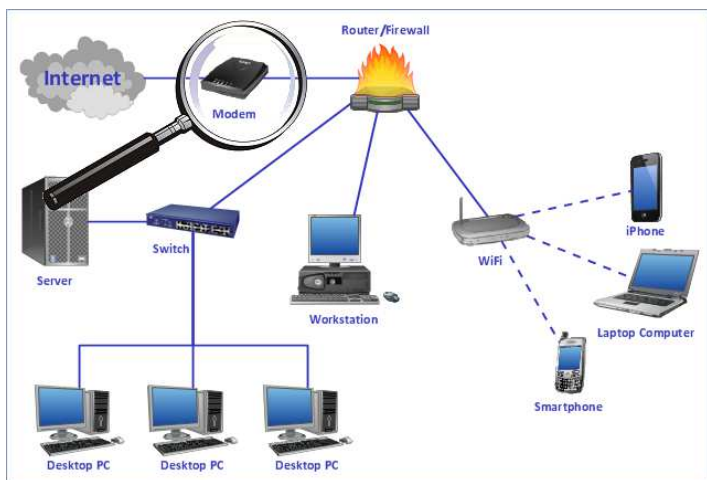
<http://heartbleed.com/> April 7, 2014

How Secure is Your Modem?

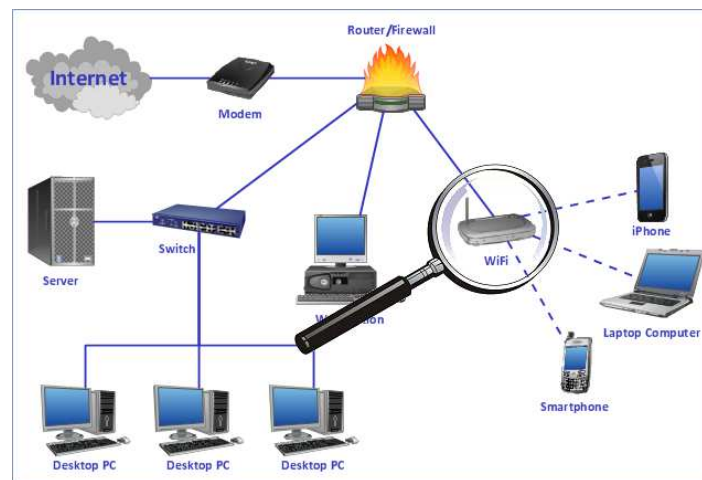


firmware buggy, default admin passwords, vulnerable web servers, ...

How Secure is Your Modem?



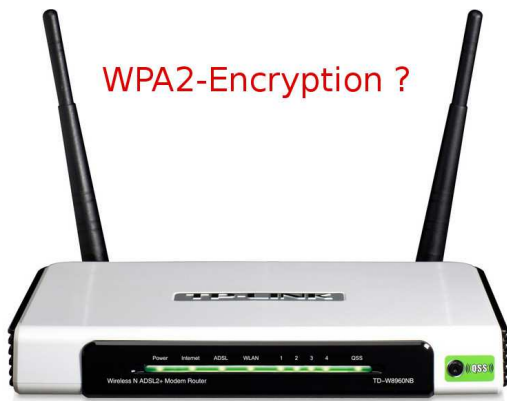
How Secure is Your WiFi?



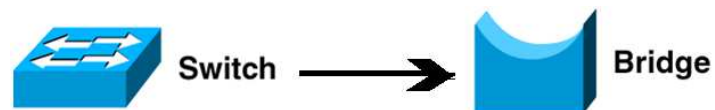
How Secure is Your WiFi?

only WPA2 not broken

WPA2-Encryption ?



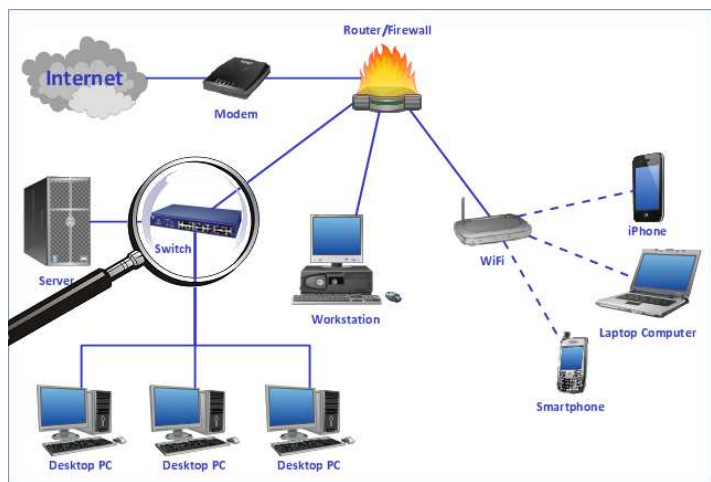
How Secure is Your Switch?



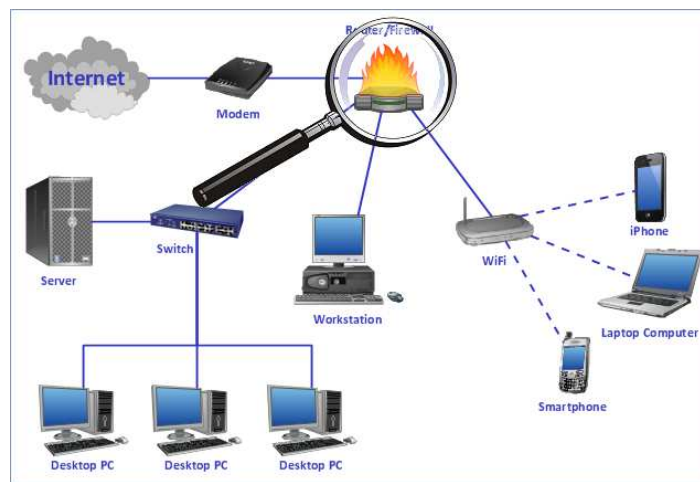
MAC flooding confuses the switch, which then works as hub

attack tool: ettercap

How Secure is Your Switch?



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)

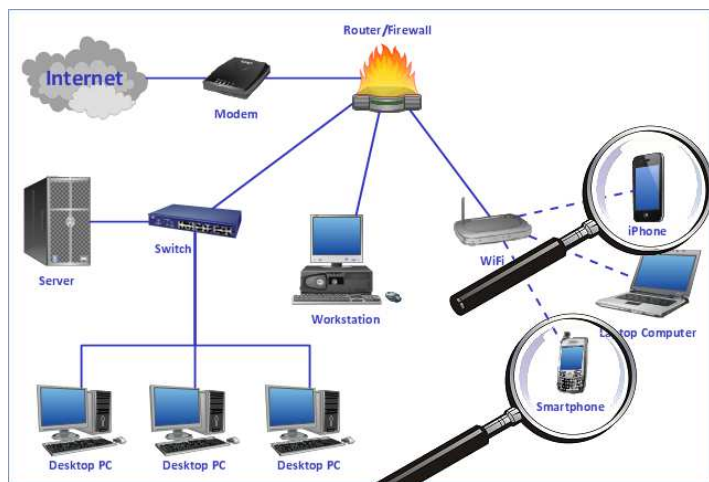
only as secure as the firewall code
only as secure as your configuration

How Secure is Your Phone?

only as secure as

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

How Secure is Your Phone?

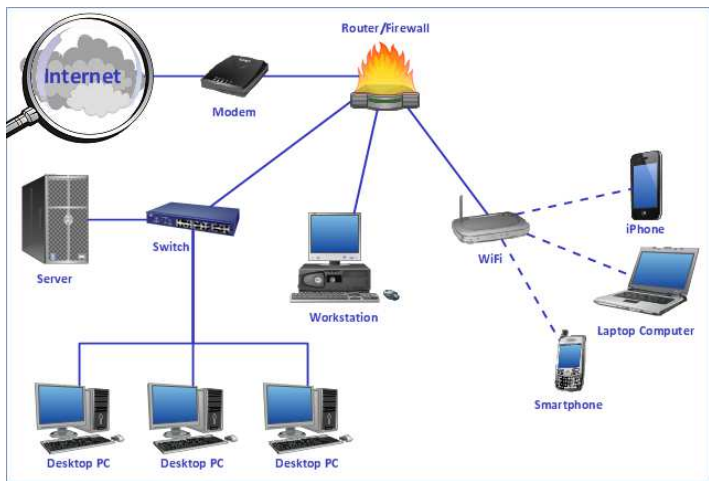


Everything Secure At Your Place?



What if an attacker steals your hard drive?

How Secure is the Internet?



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 Collection Details
(TS//SI//NF)

Current Providers

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PaTTalk
- YouTube
- Skype
- AOL
- Apple

What Will You Receive in Collection (Surveillance and Stored Comms)?
It varies by provider. In general:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- Special Requests**

Complete list and details on PRISM web page: [Go PRISM/FAA](#)

TOP SECRET//SI//ORCON//NOFORN

PRISM-Providers for NSA

How Secure is the Internet?

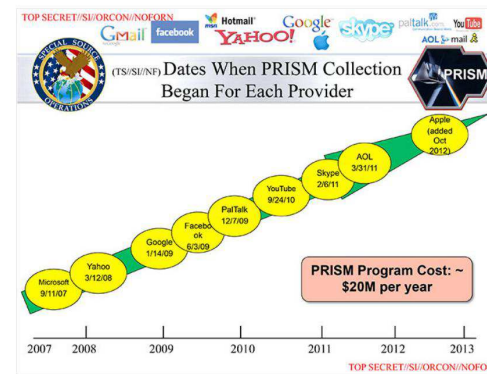


part of the physical layer

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?

Pulitzer-Preis für Snowden-Veröffentlichungen
14.04.2014, 21:59 Uhr, aktualisiert heute, 03:34 Uhr

Die bedeutendste journalistische Auszeichnung der Welt geht an die Medien, die Edward Snowden eine Plattform geboten haben: Der „Guardian“ und die „Washington Post“ werden von der US-Jury für die Enthüllungen prämiert.



Glenn Greenwald und Laura Poitras: Zwei der ausgezeichneten Journalisten.
Quelle: ap

Behörden gelingt Schlag gegen Kreditkartenbetrüger
Finem Medienbericht zulässig haben

yes, they can

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

Security is Relative!

Threat Model

- power of an adversary
- time
- capabilities

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

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)

- 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

Generally Accepted Computer Security Goals

