Leibniz Universität Hannover

Grundlagen der IT-Sicherheit
VL 0: Einführung und Grundlagen

Prof. Dr. Markus Dürmuth, Wintersemester 2024/25

Wer sind wir?

Prof. Dr. Markus Dürmuth
FG Usable Security and Privacy
Lange Laube 6, Raum A103
markus.duermuth@itsec.uni-hannover.de

Arbeitsgebiete: Usable Security, Authentication, Perception of IT Security

Übung: Maike M. Raphael
maike.raphael@itsec.uni-hannover.de

Wer sind Sie?

- Informatik (Bachelor)
- Elektrotechnik und Informationstechnik (Bachelor)
- Elektrotechnik und Informationstechnik (Master)
- Technische Informatik (Master)
- Lehramt
- …

Organisatorisches

Kurs: Grundlagen der IT-Sicherheit

- Vorlesung + Übung (5 ECTS)

Aktuelles Semester (Vorlesungszeitraum 14.10.24 bis 31.01.25)

- Vorlesung: Dienstags, 15:00 – 16:30 (E001, Hauptgebäude)
- Übung: Donnerstags, 14:15 – 15:45 (F102, Hauptgebäude)
- Quiz: ca. jede zweite Woche (siehe nächste Folien)

Organisatorisches - Termine

- Erste Übung: Donnerstag, 17.10.2024, 14:15 bis 15:45 Uhr, Raum F102 im Hauptgebäude

- Keine Übung am 31.10.2024 (Reformationstag)

Notenbonus

- Jedes einzelne Quiz wird „bestanden“ (≥ 70 %) oder „nicht bestanden“
- Mindestens fünf der sechs Quiz bestanden: Notenbonus

Notenbonus:

- Zur Verbesserung der Abschlussnote (Note aus der Klausur)
- Wenn die Klausur bestanden ist (≥ 4,0), dann wird die Note um einen Notenschritt in der Nachkommastelle verbessert
- Beispiel:
  4,0 → 3,7
  2,3 → 2,0

Bearbeitungszeitraum Quiz (vorläufig)

- Quiz 1:
  Donnerstag, 24.10.2024, 16:00 Uhr - Donnerstag, 31.10.2024 14:00
- Quiz 2:
  Donnerstag, 07.11.2024, 16:00 – Donnerstag, 14.11.2024, 14:00
- Quiz 3:
  Donnerstag, 21.11.2024, 16:00 – Donnerstag, 28.11.2024, 14:00
- Quiz 4:
  Donnerstag, 05.12.2024, 16:00 – Donnerstag, 12.12.2024, 14:00
- Quiz 5:
  Donnerstag, 19.12.2024, 16:00 – Donnerstag, 09.01.2025, 14:00
- Quiz 6:
  Dienstag, 16.01.2025, 16:00 – Donnerstag, 23.01.2025, 14:00

Klausur

- Schriftliche Klausur (in Präsenz):
  Voraussichtlicher Termin:
  Do 06.02.2025, 17:30 Uhr
- 90 Minuten
- keine Hilfsmittel erlaubt außer nicht programmierbarer Taschenrechner

- Lehramt (unbenoteter Schein):
  - Schreiben die Klausur mit, unbenotete Bewertung

Organisatorisches

- Feedback ist willkommen!
  - maike.raphael@itsec.uni-hannover.de
  - Weiteres Feedback gerne über das Forum im Stud.IP

- Vorlesung basiert auf der Vorlesung von Prof. Fahl, vielen Dank!

Materialien

- Alles Material wird über Stud.IP zur Verfügung gestellt
- Forum für organisatorische und inhaltliche Fragen
- Übungsmaterial im Ordner der Vorlesung
- Quiz über die ILIAS-Schnittstelle in Stud.IP

Ethik und Legalität

- Sie werden zahlreiche Angriffe kennenlernen
- Verwenden Sie diese nicht ohne die ausdrückliche schriftliche Zustimmung aller Beteiligten!
  - Stellen Sie sicher, dass Sie wissen, wer beteiligt ist.
- Wenn Sie etwas ausprobieren wollen, sagen Sie es uns und wir werden versuchen, eine Testumgebung einzurichten.
- Verletzen Sie nicht: Ethik, LUH-Richtlinien, staatliche, nationale und EU-Gesetze

Themen der Vorlesung

Breiter Überblick über das Thema IT-Sicherheit

- Grundlagen der Kryptographie
  - “Klassische” Chiffren
  - Symmetrische Crypto (AES, Hashfunktionen)
  - Asymmetrische Crypto (RSA)
- Grundlagen Softwaresecurity
  - Buffer Overflows, Integer Overflows, usw.
  - Schutzmechanismen
  - Sichere Software
- Grundlagen Netzwerksicherheit
  - Aufbau Netze, Angriffe
  - Schutzmechanismen (TLS, DNSSEC,...)
- Grundlagen Web Security
  - Grundlagen, SQL injections, Session Hijacking, usw.
- Usable Security
- Ausblick aktuelle Themen

FRAGEN BIS HIERHER?

Unsere heutigen Themen…

- Organisatorisches (geschafft)
- Einführung in das Thema
  - Hacking früher und heute
  - Zahlen, Daten, Fakten
  - Angriffsvektoren
  - Schutzziele
  - Security in der Praxis

HACKING FRÜHER UND HEUTE

Oder auch: Warum sehen wir heute so viele Cyber-Angriffe?

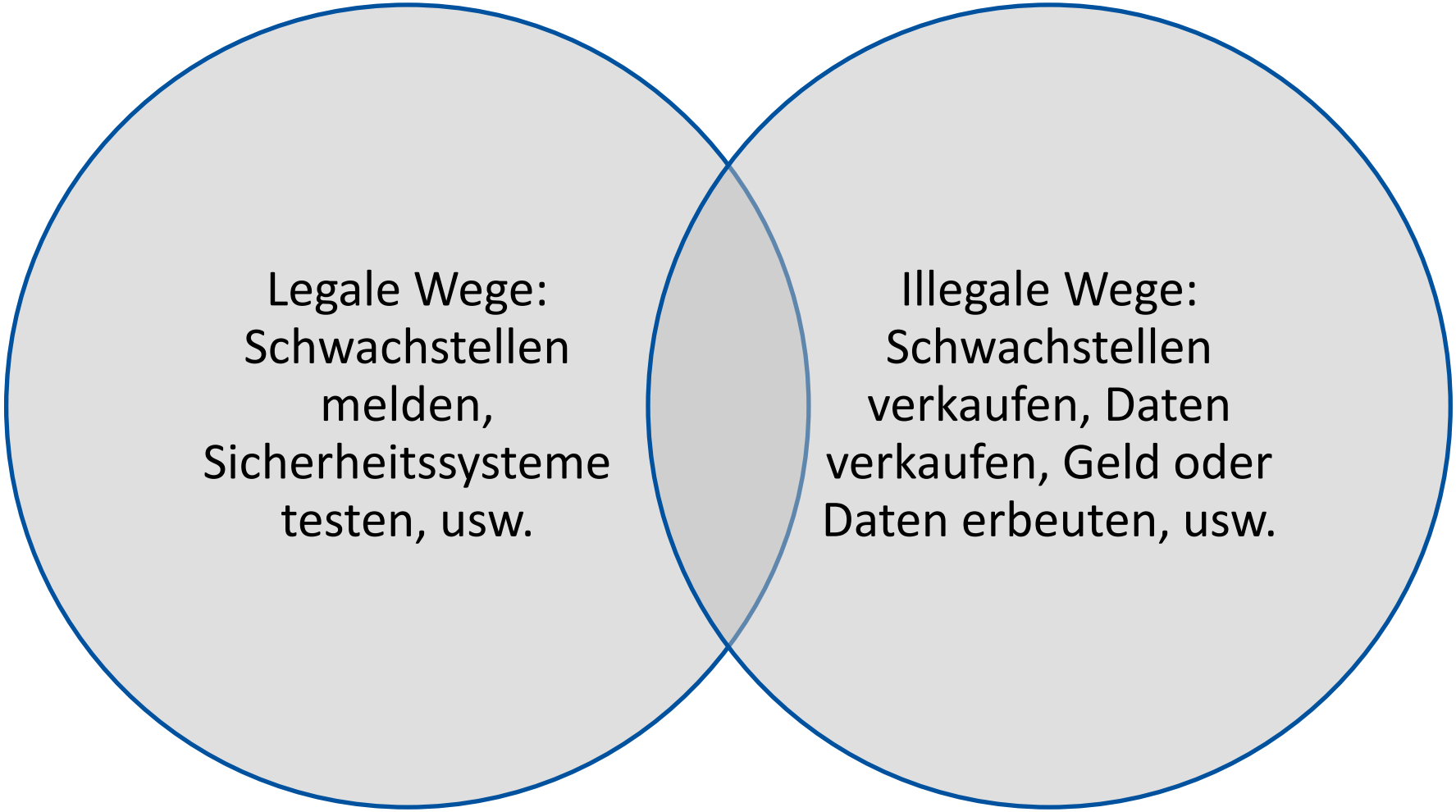
Hacker in den frühen Tagen

Profil:

- Männlich
- Zwischen 14 und 34 Jahren
- Computer-Nerds

Source: Raimund Genes

Die Dinge haben sich geändert – Kommerzialisierung



Die Dinge haben sich geändert – Kommerzialisierung

Bug bounty programs (Bezahle Hacker, Schwachstellen zu finden)

- Google Vulnerability Reward Program: bis zu 20K $
  - Für Chrome-Exploits sogar bis zu 50K $
- Microsoft Bounty Program: bis zu 100K $
  - Für Browser exploits bis zu 100K $ und für neuartige Browser-Schutzmaßnahmen bis zu 50k $
- Mozilla Bug Bounty program: 500$ - 3000$
- Pwn2Own competition: 15K $
- Zero Day Initiative, Verisign iDefense: 2K – 25K $
  - ZDI hat sogar ein “Belohnungsprogramm” ähnlich dem “Vielflieger-Programm”

Die Dinge haben sich geändert – Kommerzialisierung

Schwarzer / Grauer Markt

- Was hat ein Mozilla-Zero-Day-Exploit in den Anfangszeiten gebracht?
  - 500 $: Eine Playstation 4

- Was hat eine Zero-Day-Schwachstelle in Adobe Reader gebracht?
  - 5,000 $ - 30,000 $: Sehr guter Gaming-PC

- Was hat ein iOS-Zero-Day-Exploit später gebracht?
  - 100,000 $ - 250,000 $: 2014 Lamborghini Gallardo

Die Dinge haben sich geändert – Kommerzialisierung

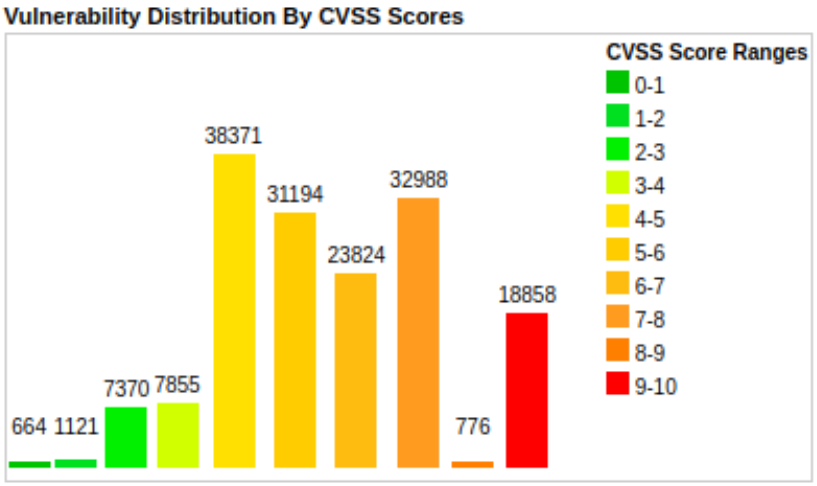
Zero-Day Prices Over Time

Service	Price	Year
"Some exploits"	$200,000–$250,000	2007
"Weaponized exploit"	$20,000–$30,000	2007
A "real good" exploit	$100,000	2007
Microsoft Excel	> $1,200	2007
Mozilla	$500	2007
Vista exploit	$50,000	2007
WMF exploit	$4,000	2007
ZDI, iDefense Purchases	$2,000–$10,000	2007
Adobe Reader	$5,000–$30,000	2012
Android	$30,000–$60,000	2012
Chrome or Internet Explorer	$80,000–$200,000	2012
Firefox or Safari	$60,000–$150,000	2012
Flash or Java Browser Plug-ins	$40,000–$100,000	2012
iOS	$100,000–$250,000	2012
Mac OSX	$20,000–$50,000	2012
Microsoft Word	$50,000–$100,000	2012
Windows	$60,000–$120,000	2012

Source: Rand Corp., National Security Research Division. Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar

ZAHLEN, DATEN, FAKTEN

Offenlegung von Sicherheitslücken



Source: http://www.cvedetails.com/cvss-score-distribution.php

Common Vulnerability Scoring System (CVSS) Base Score setzt sich aus verschiedenen Faktoren zusammen, wie z.B.

- Zugriffsvektor
- Zugriffskomplexität
- Auswirkung auf die Vertraulichkeit
- Auswirkungen auf die Integrität

- Höherer Score – Höhere Folgen für die Security

CVSS-Score-Verteilung für die 30 wichtigsten Produkte

Leibniz Universität Hannover

CVSS Score Distribution For Top 50 Products By Total Number Of "Distinct" Vulnerabilities

	Product Name	Vendor Name	Number of Total Vulnerabilities	# Of Vulnerabilities										Weighted Average	% Of Total									
				0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9+		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9+
1	Debian Linux	Debian	5291		69	275	133	1466	1111	1039	949	16	233	6.20	0	1	5	3	28	21	20	18	0	4
2	Android	Google	3826		36	399	52	1003	367	303	748	34	884	6.80	0	1	10	1	26	10	8	20	1	23
3	Ubuntu Linux	Canonical	2997		43	189	94	890	526	470	551	7	227	6.20	0	1	6	3	30	18	16	18	0	8
4	Mac Os X	Apple	2872	1	24	200	24	535	343	683	510	12	540	6.90	0	1	7	1	19	12	24	18	0	19
5	Linux Kernel	Linux	2711	1	101	440	70	866	153	216	727	9	128	5.80	0	4	16	3	32	6	8	27	0	5
6	Iphone Os	Apple	2454		28	173	19	494	239	859	228	6	408	6.70	0	1	7	1	20	10	35	9	0	17
7	Windows 10	Microsoft	2435		86	340	35	717	95	272	550	7	333	6.20	0	4	14	1	29	4	11	23	0	14
8	Chrome	Google	2253			16		640	224	768	418	1	186	6.70	0	0	1	0	28	10	34	19	0	8
9	Fedora	Fedoraproject	2227		24	121	53	632	515	478	320	7	77	6.10	0	1	5	2	28	23	21	14	0	3
10	Windows Server 2016	Microsoft	2206		82	313	35	673	100	250	468	7	278	6.10	0	4	14	2	31	5	11	21	0	13
11	Windows Server 2008	Microsoft	2075		79	231	16	438	80	224	538	12	457	6.80	0	4	11	1	21	4	11	26	1	22
12	Firefox	Mozilla	1957		8	55	4	423	343	278	336	1	509	7.20	0	0	3	0	22	18	14	17	0	26
13	Windows 7	Microsoft	1943		77	236	13	434	61	208	500	10	404	6.70	0	4	12	1	22	3	11	26	1	21
14	Windows Server 2012	Microsoft	1851		85	255	20	409	91	212	429	8	342	6.50	0	5	14	1	22	5	11	23	0	18
15	Windows 8.1	Microsoft	1746		81	251	18	396	73	203	392	8	324	6.50	0	5	14	1	23	4	12	22	0	19
16	Windows Server 2019	Microsoft	1640		5	222	22	537	84	187	362	4	217	6.30	0	0	14	1	33	5	11	22	0	13
17	Windows Rt 8.1	Microsoft	1615		66	236	18	377	56	187	366	8	301	6.50	0	4	15	1	23	3	12	23	0	19
18	Enterprise Linux Desktop	Redhat	1443		9	82	24	381	231	244	259	1	212	6.60	0	1	6	2	26	16	17	18	0	15
19	Enterprise Linux Server	Redhat	1395		8	67	24	381	220	241	254	2	198	6.60	0	1	5	2	27	16	17	18	0	14
20	Enterprise Linux Workstation	Redhat	1352		8	59	23	367	211	239	246	1	198	6.70	0	1	4	2	27	16	18	18	0	15
21	Opensuse	Opensuse	1276		25	64	51	246	244	222	212	1	211	6.70	0	2	5	4	19	19	17	17	0	17
22	Leap	Opensuse	1236		14	102	38	359	270	258	137	3	55	6.00	0	1	8	3	29	22	21	11	0	4
23	Tvos	Apple	1224		10	38	4	205	92	532	102	4	237	7.10	0	1	3	0	17	8	43	8	0	19
24	Internet Explorer	Microsoft	1177		1	62		132	153	47	203		579	8.10	0	0	5	0	11	13	4	17	0	49
25	Safari	Apple	1118		3	17		218	106	563	65	2	144	6.90	0	0	2	0	19	9	50	6	0	13
26	Mysql	Oracle	1018		24	37	132	578	79	118	40	2	8	5.20	0	2	4	13	57	8	12	4	0	1
27	Enterprise Linux	Redhat	1016		30	92	56	262	188	131	213	5	39	6.00	0	3	9	6	26	19	13	21	0	4
28	Thunderbird	Mozilla	1009		3	19	2	182	126	142	176		359	7.70	0	0	2	0	18	12	14	17	0	36
29	Watchos	Apple	958		2	49	2	186	79	309	108	4	219	7.10	0	0	5	0	19	8	32	11	0	23
30	Windows Vista	Microsoft	793		8	33	2	117	25	56	290	8	264	7.80	0	1	4	0	15	3	7	37	1	32

Source: http://www.cvedetails.com/top-50-product-cvssscore-distribution.php

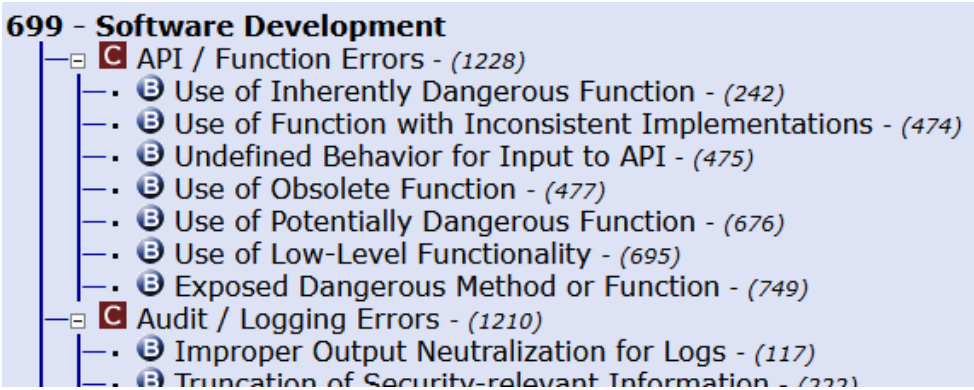
Common Weakness Enumeration - CWE

Umfangreiche und detaillierte Zusammenstellung von Schwachstellen inklusive Lösungsansätzen zum Beheben der Schwachstelle

⇒ Kategorisierung von Hard- und Softwareschwachstellen

⇒ “Einheitliche Sprache” beim Beschreiben und Identifizieren von Sicherheitslücken

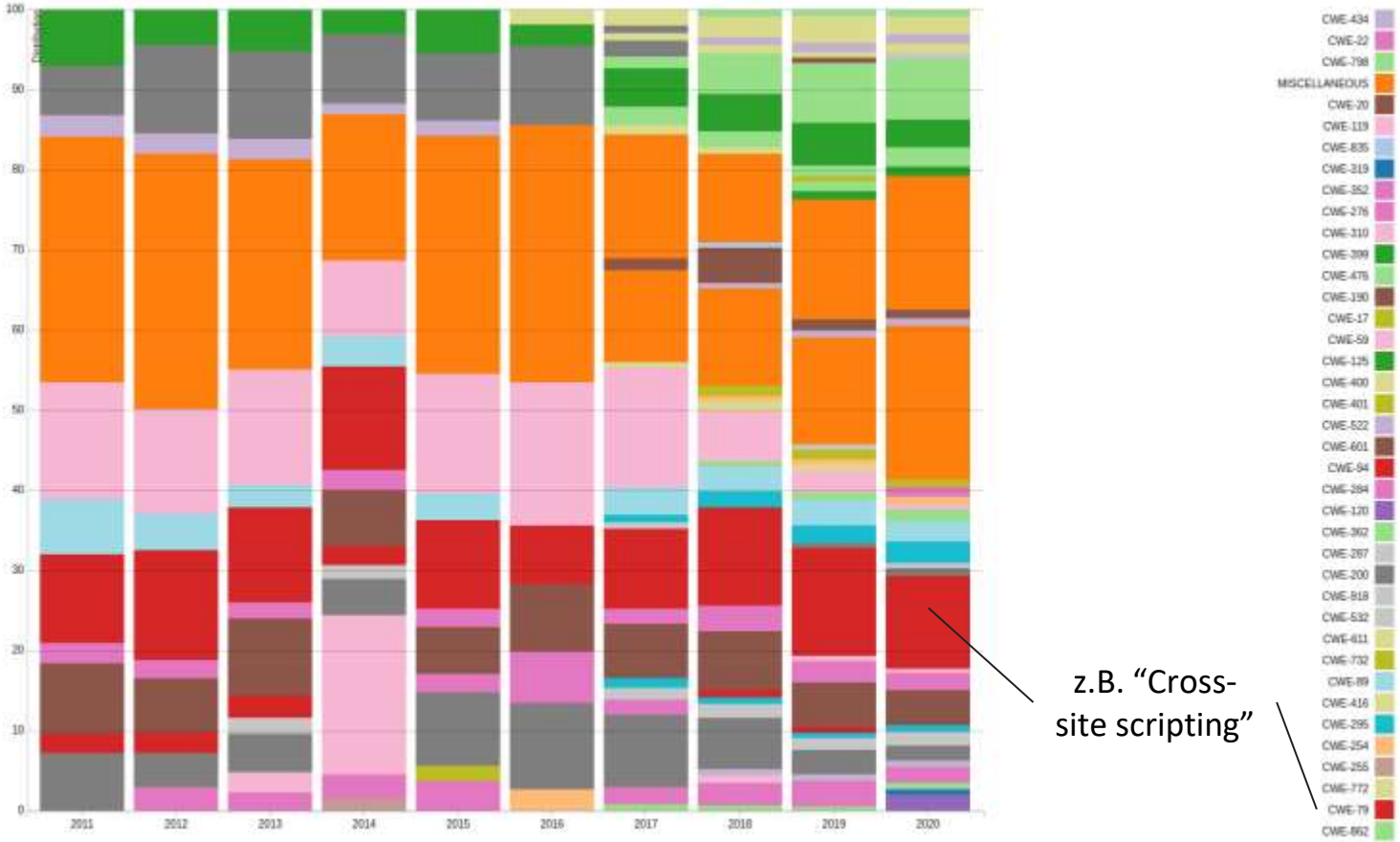
⇒ Unterstützungswerkzeug bei Schwachstellen-Analysen und Prävention



https://cwe.mitre.org/data/definitions/699.html

Offenlegung von Sicherheitslücken

Common Weakness Enumeration - CWE, Types over time:



z.B. “Cross-site scripting”

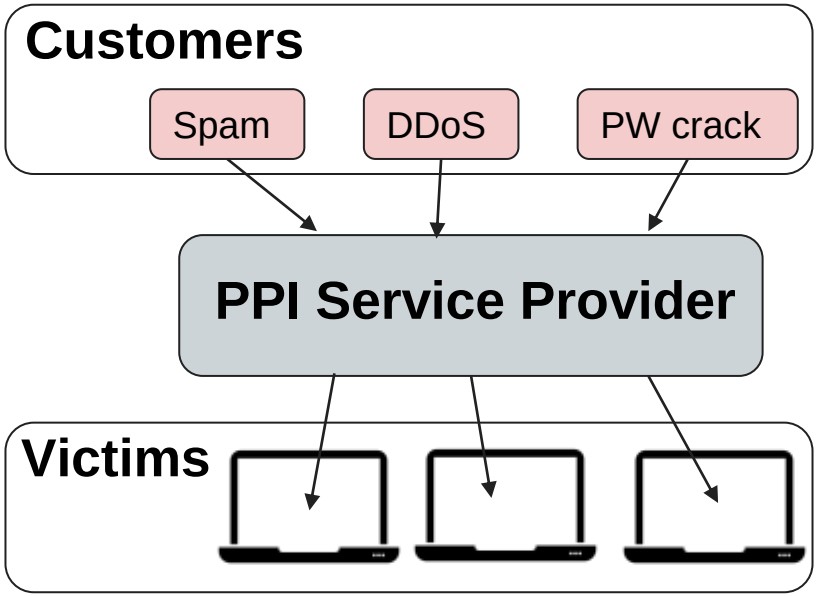
Source: https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cwe-over-time

Schattenwirtschaft für Botnetze

Botnetz: Gruppe von Schadprogrammen, die auf Rechnern ohne Einwilligung der Besitzenden laufen

Pay-per-Install (PPI)-Dienstleister

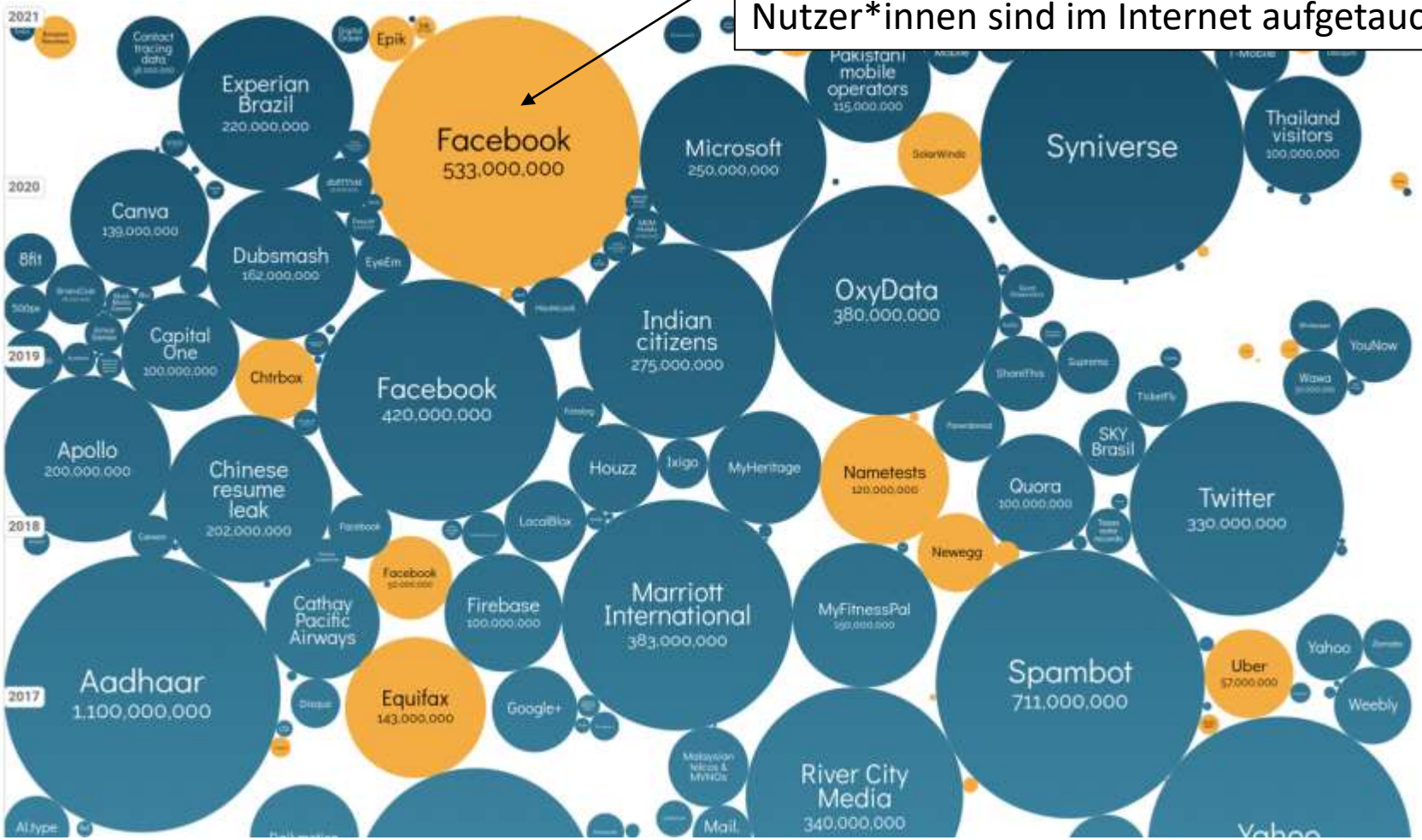
- „Besitzen“ den Rechner des Opfers
- Berechnen Kosten für den "Kunden“
- Führen Code des „Kunden“ auf Victim-Maschinen aus
  - Spam verschicken
  - Passwörter knacken
  - DDoS



Kosten: US: 100 - 180 $ / 1k machines, Asia: 7 - 8 $ / 1k machines

Größte „Datenpannen“

Die Telefonnummern und persönlichen Daten von 533 Millionen Facebook-Nutzer*innen sind im Internet aufgetaucht



Source: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

WAS IST DER SPEKTAKULÄRSTE VORFALL, VON DEM SIE GEHÖRT HABEN?

WAS SIND DIE GRÖßTEN HERAUSFORDERUNGEN?

ANGRIFFSVEKTOREN

Oder auch: Was muss gegen Angriffe abgesichert werden?

Angriffe auf das Betriebssystem

Beispiel: Spielautomaten

- Entwickler des Betriebssystems modifizierte den Code
- Wenn eine Sequenz von 10, 5, 25, 10, 5, … Cent-Münzen eingeworfen wird, gibt die Maschine den Jackpot aus

Der Entwickler wurde aufgrund seiner Gier gefasst!

Was muss abgesichert werden?

OS

Angriffe auf die Software

Beispiel: Pferderennen

- Entwickler der Software modifiziert den Code
- Ermöglicht die Abgabe einer Wette nach dem Ende des Rennens

Der Entwickler wurde aufgrund seiner Gier gefasst!

Was muss abgesichert werden?

Software 

OS 

Angriffe über USB

Malware lässt die Firmware des USB-Sticks eine Tastatur vortäuschen.

Beispiel aus der realen Welt:

Angriff auf Urananreicherungsanlagen im Iran durch Stuxnet

(siehe: https://en.wikipedia.org/wiki/Stuxnet)

Angriffe auf Smartphones

Baseband-Angriffe:

- Infiltrieren des Telefons über die Luft!
- Umgeht Betriebssystem und Antiviren-Software
- Hackt Funkprozessor direkt

https://www.usenix.org/conference/woot12/workshop-program/presentatio

USB-Angriffe:

- Nutzt verstecktes Gerät im Ladegerät eines Mobiltelefons, um persönliche Daten zu stehlen (gespeicherte Passwörter, Bilder, usw.)

http://i1227.photobucket.com/albums/ee430/kalsta1/malicious-usb-charger.jpg

Was muss abgesichert werden?

Software 

OS 

Hardware 

Angriffe auf die Kryptographie

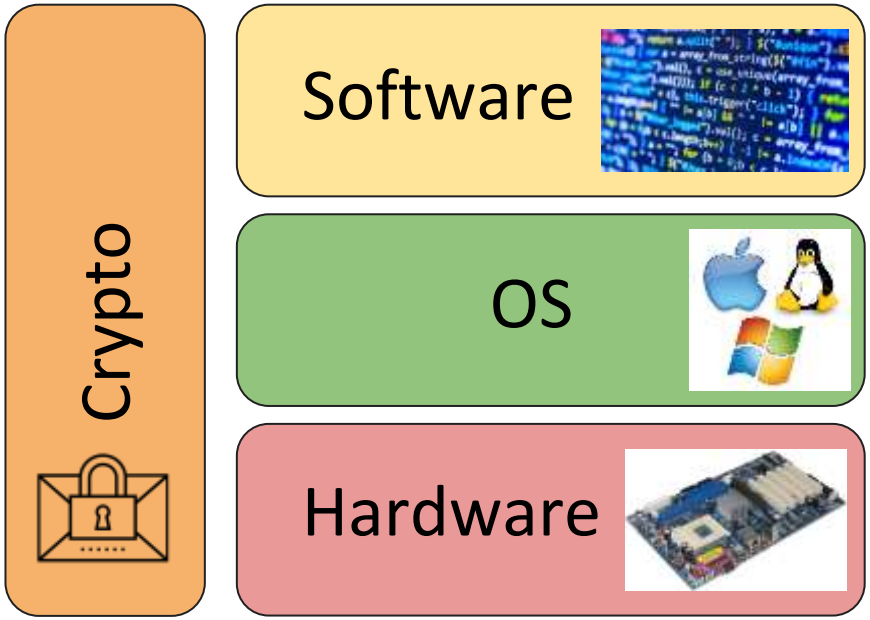
Beispiel: Mifare Classic

- Karten zum Speichern von Geheimnissen
  - Wurden früher (!) in vielen Mensen verwendet
- Verwendete proprietäre Verschlüsselung, nicht öffentlich bekannt

- Mithilfe eines Mikroskops konnten Hardware-Details aus dem Karteninneren analysiert werden
- Daraus wurde der Algorithmus extrahiert
  - -> Linear feedback shift register (LSFR)

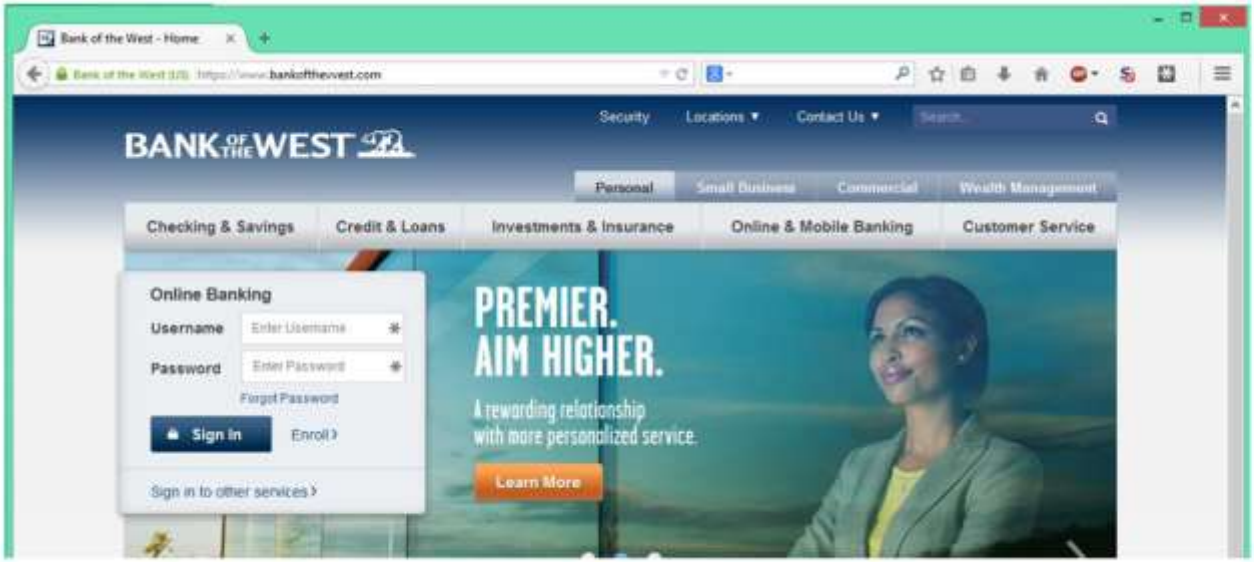
- Sehr schwache Zufallszahlengenerierung
  - Hatte nur 16-Bit-Schlüssel: 65k Möglichkeiten
  - Leicht zu brechen

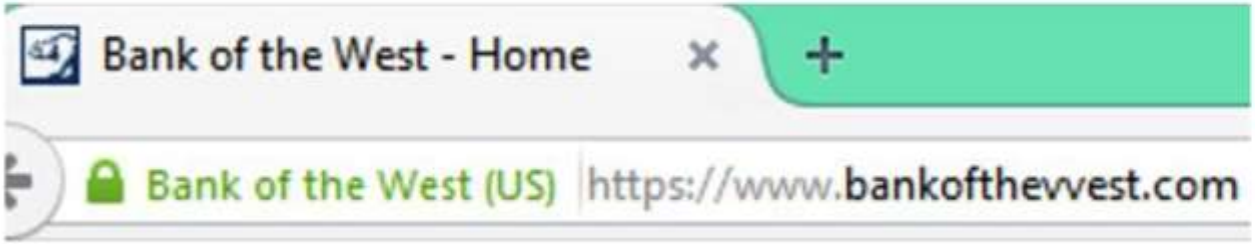
Was muss abgesichert werden?



Angriffe auf den Menschen

- Beispiel: Phishing





...but is not!

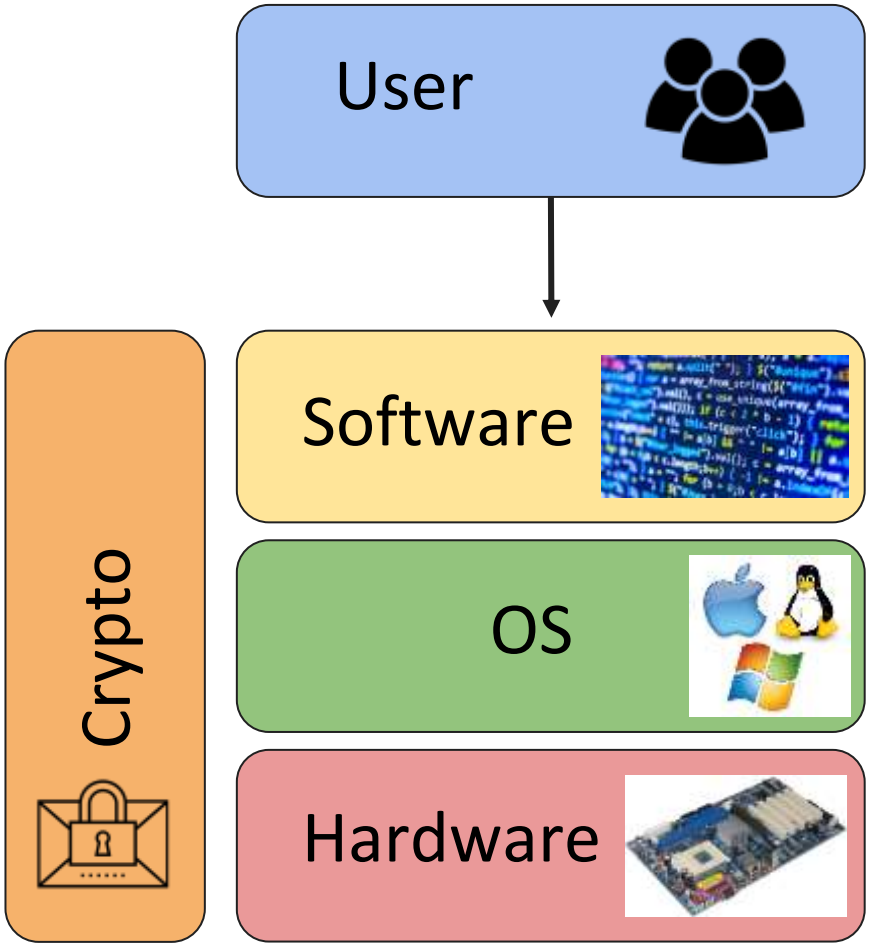
Angriffe auf den Menschen

Beispiel: Social Engineering

Manchmal reicht es aus, nett zu fragen!

http://www.informationsecuritybuzz.com/wp-content/uploads/Social-engineering-attack.png

Was muss abgesichert werden?



Angriffe auf Autos

Angriffs-Kategorien:

- Physischer Zugriff: Verwendung speziell gestalteter Mediendateien, die Malware enthalten, um die Kontrolle über verschiedene Kfz-Systeme zu erlangen
- Fernzugriff: Angriffe auf Schwachstellen in den Basisband-GPRS-Mobilfunk-, FM-RDS- und SMS-Infrastrukturen, die in Fernwartungsdiensten für Fahrzeuge oder in internetfähigen Systemen verwendet werden
- Mehrere Angriffe im Jahr 2015

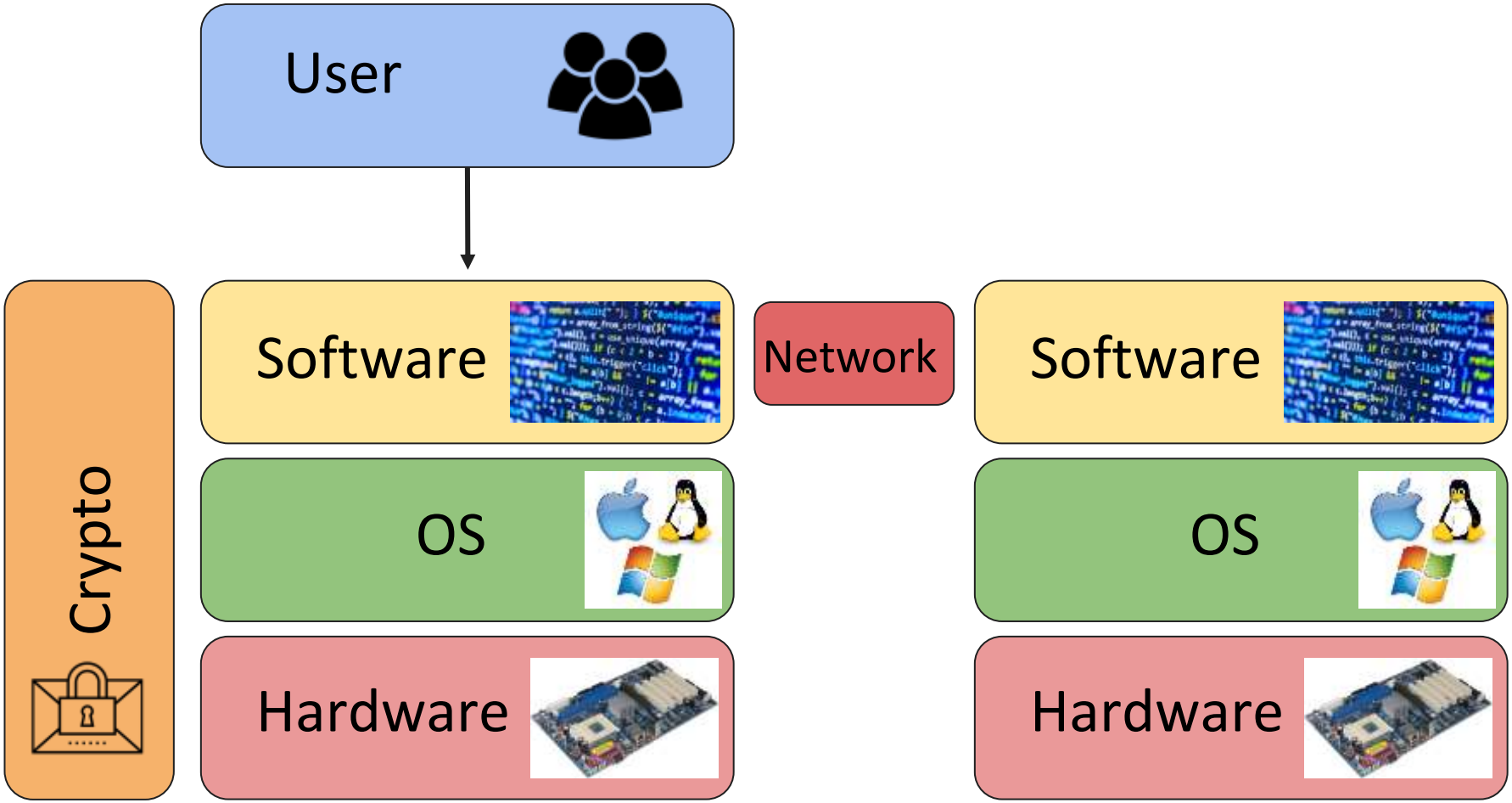
[https://www.youtube.com/watch?v=yTBfImSDQk]

http://upload.wikimedia.org/wikipedia/commons/a/a3/Tesla_Model_S_digital_panels.jpg

Autos mithilfe eines Laptops stehlen

- Sicherheitsmechanismen, die Luxusfahrzeuge schützen sollen, ermöglichen es Angreifern, sie zu kapern.
- Hightech-Kriminelle sorgten international für Schlagzeilen, als sie mit Hilfe eines Laptops und eines Senders die Schlösser eines gepanzerten BMW X5 des Fußballspielers David Beckham öffneten und die Zündung einschalteten - der zweite X5, der ihm innerhalb von sechs Monaten mit dieser Technologie gestohlen wurde.

Was muss abgesichert werden?



Das ist noch nicht alles!

WEITERE ANGRIFFSVEKTOREN

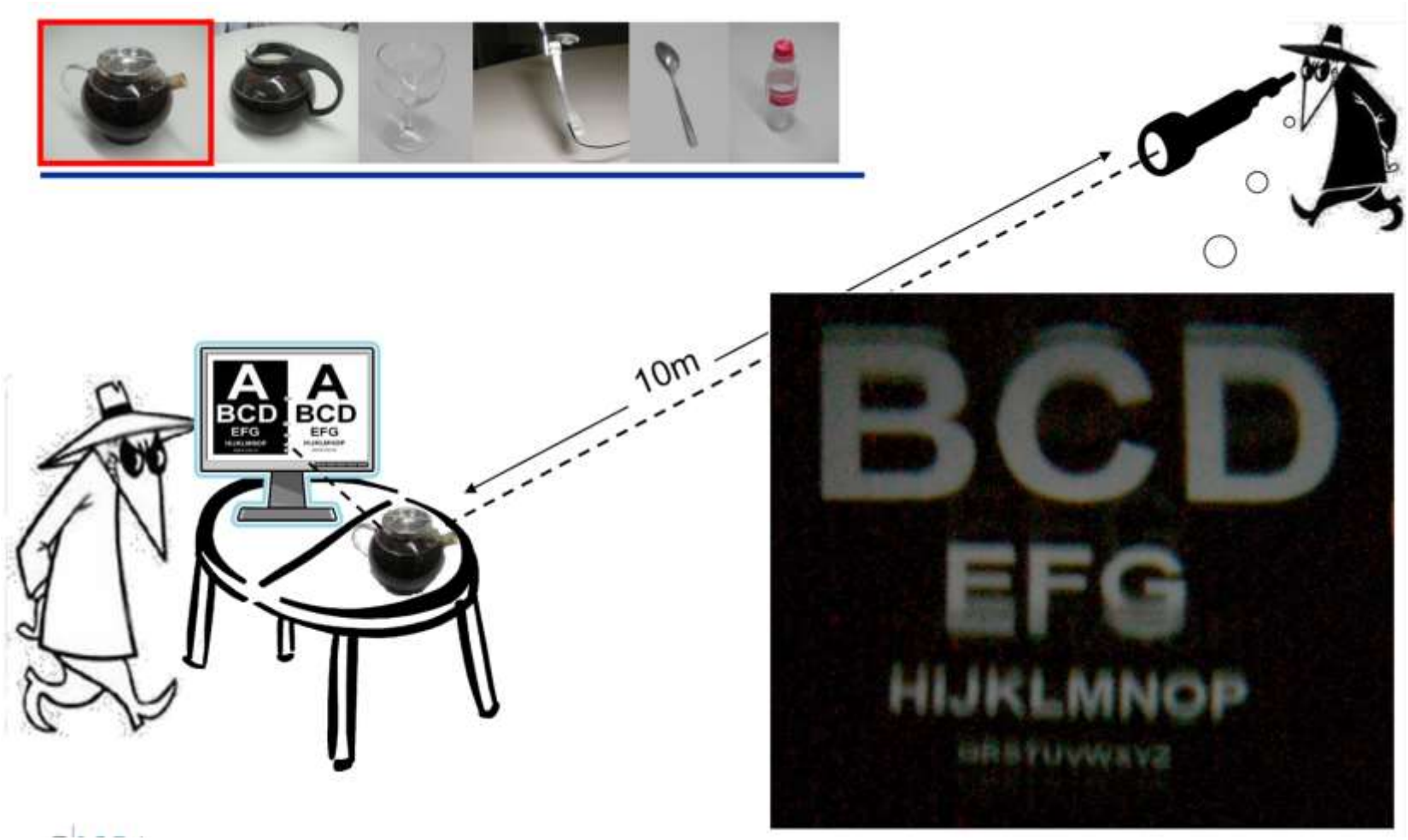
„Smart Home“ über das Internet hacken

Die mangelhafte Sicherheit von HomeMatic wurde von den Hackern Sathya und Malli auf dem 30C3 aufgedeckt. HomeMatic ermöglicht es den Nutzern, Türen zu entriegeln, die Heizung zu steuern oder Alarme von einem Bewegungsmelder zu empfangen. Mit drei Live-Hacks innerhalb einer Stunde zeigten Sathya und Malli, wie sie sich unbefugten Zugang verschaffen und die Kontrolle über jede dieser Funktionen übernehmen konnten. Das Hacken des Stromnetzes bekam auf der DefCon-Hackerkonferenz eine neue Bedeutung, als zwei unabhängige Sicherheitsforscher zwei Tools vorstellten, die sie entwickelt haben, um Automatisierungs- und Sicherheitssysteme für Haushalte und Unternehmen zu hacken, die über Stromleitungen funktionieren.

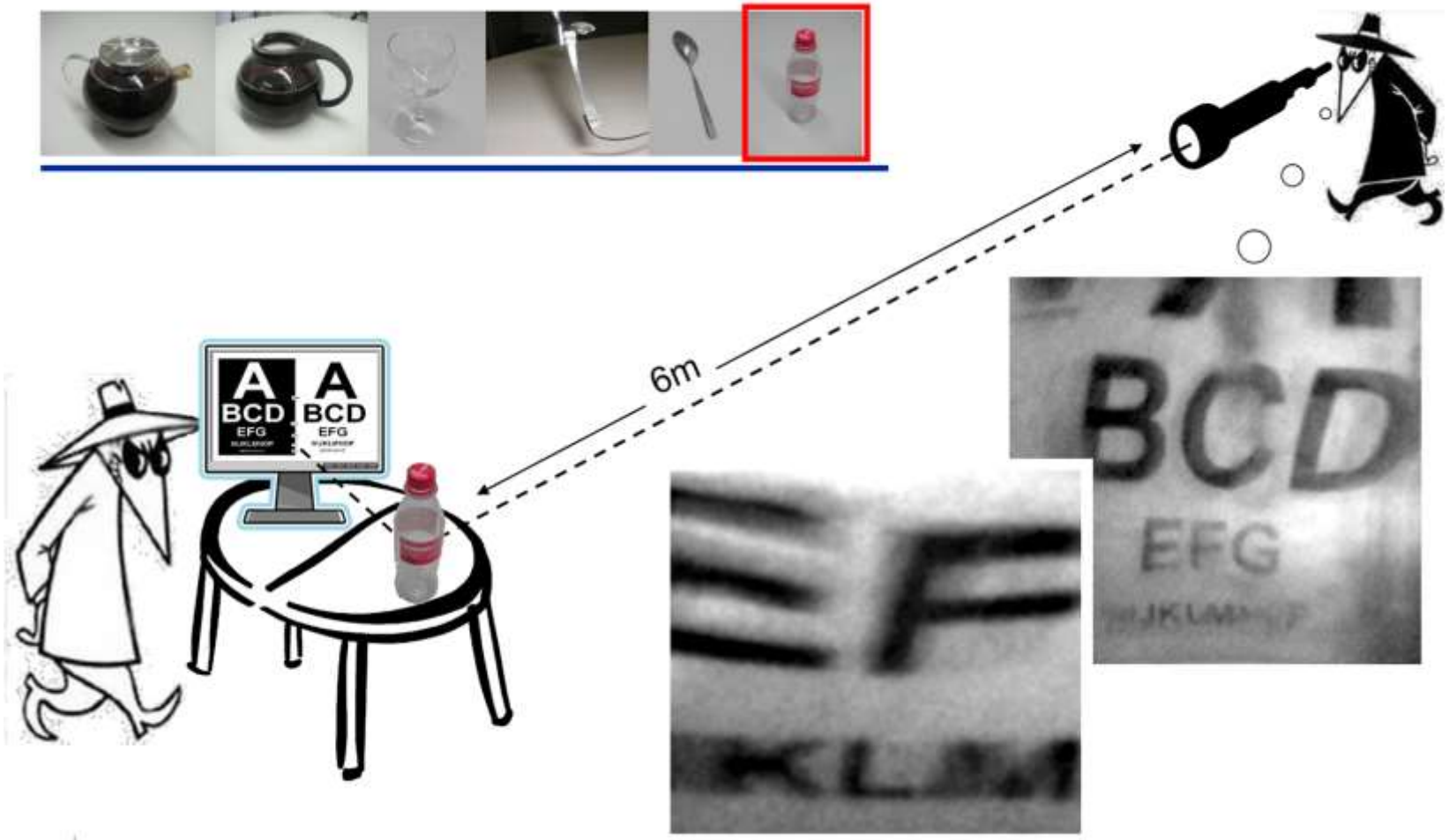
http://electronic-lifestyle.com/wp-content/uploads/2013/09/home-automation.jpg

http://www.wired.com/images_blogs/threatlevel/2011/08/X10-Jammer.png

Reflexionen ausnutzen, um Geheimnisse auszuspionieren

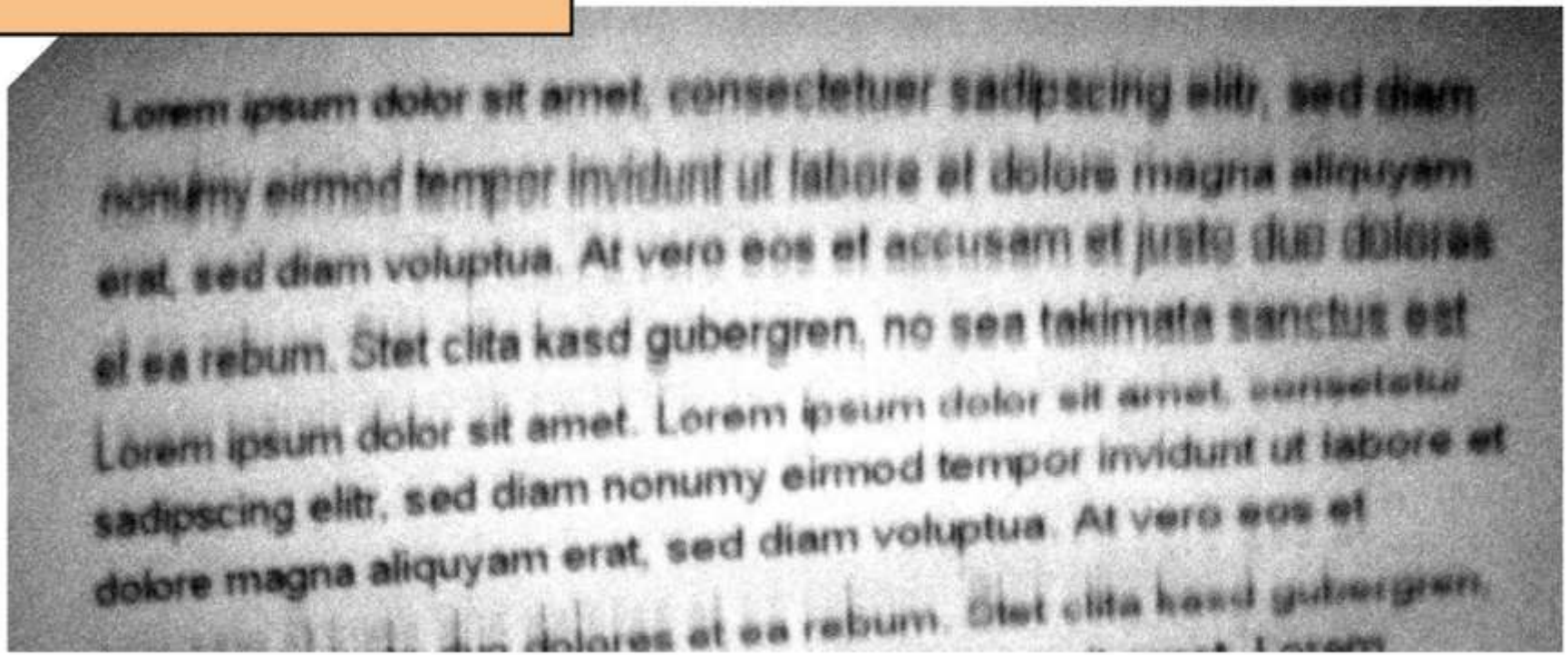


Reflexionen ausnutzen, um Geheimnisse auszuspionieren

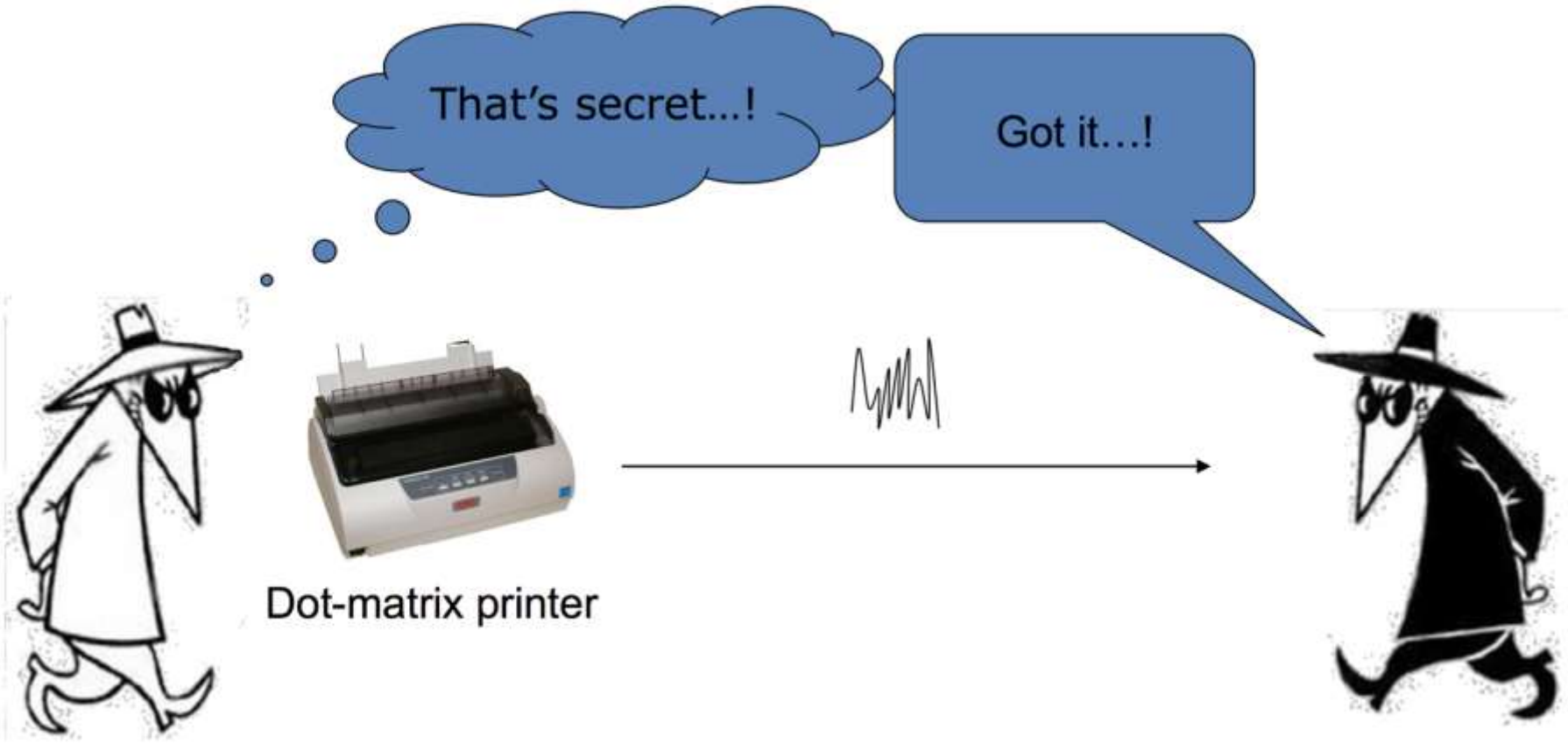


Ausspähen eines Word-Dokuments

- Distance approx. 7 meters
- 12pt font (readable)



Akustische Seitenkanalangriffe



Warum sollte uns das interessieren?

Nadeldrucker werden immer noch verwendet:

- bei Ärzten in Deutschland für sensible Informationen
  - ärztliche Verordnungen
  - Quittungen
  - Patientenüberweisungen
- wird von mehr als 30% der Banken verwendet:
  - Kontoauszüge
  - PIN-Nummern
- Druck von Betäubungsmittelrezepten, die per Gesetz nur auf Nadeldruckern erlaubt sind (Deutschland, Schweiz, Österreich)

Wärmebildkameras leaken Informationen

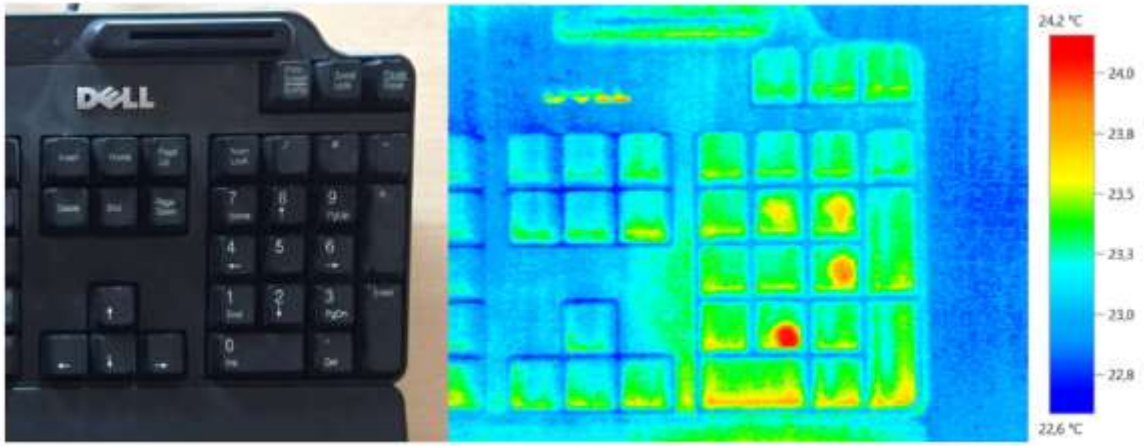


Figure 3: Attack on a computer keyboard, time: 5 seconds, PIN:8962

SCHUTZZIELE

Oder auch: Warum ist es so schwer, die Security zu erhöhen?

Schutzziele

- Viele verschiedene Schutzziele. Hier nur ein kleiner Ausschnitt der möglichen Schutzziele.
- Je nach Kontext nicht immer zu definieren.
- Manche stehen (scheinbar) im Widerspruch
  - z.B. Anonymität vs. Rechenschaftspflicht

Traditionelle Schutzziele der Informationssicherheit („CIA“)

Vertraulichkeit (Confidentiality)
Stelle sicher, dass Informationen nicht von unbefugten Personen eingesehen werden können

Integrität (Integrity)

Daten: Vollständigkeit und Korrektheit der Daten, keine unbefugte Manipulation

System: Korrekte Funktionsweise des Systems, beabsichtigte Leistung wird erbracht, unabhängig von unbefugten Veränderungen

Verfügbarkeit (Availability)
Stelle sicher, dass es einen zuverlässigen Zugang zu Informationen, Programmen, Systemen gibt.

Weitere Schutzziele

Privacy (“Datenschutz”, “Privatsphäre”)

Vertraulichkeit **personenbezogener** Daten.

Anonymität (Anonymity)

Es ist klar, dass eine Ressource genutzt wird, jedoch nicht von wem.

Unbeobachtbarkeit / Verdecktheit (covertness, obscurity)

Es ist nicht nur geheim, wer eine Ressource nutzt, sondern auch, ob sie überhaupt verwendet wird.

Es ist nicht nur geheim, was eine Ressource enthält, sondern dass sie überhaupt existiert.

Weitere Schutzziele

Zurechenbarkeit

Jede Aktion (z.B. Veränderung, Nachricht) ist einer eindeutigen Person zuordbar.

Nicht-Abstreitbarkeit (Nonrepudiation)

Es kann nachgewiesen werden, dass etwas (unabstreitbar) von der angegebenen eindeutigen Person durchgeführt wurde

Weitere Schutzziele

Authentifizierung (Authentication)

Nachweis/Bestätigung einer behaupteten Identität.

Autorisierung (Authorization)

Legt fest, wann/ob eine Entität eine Handlung ausführen darf.

Nachvollziehbarkeit (Auditability)

Speicherung von ausreichend Informationen, um die Umstände und Vorgehensweisen zurückverfolgen zu können.

…und viele weitere, z.B. Zuverlässigkeit (Reliability), Nachweisbarkeit (Detectability), Unleugbarkeit, Unverknüpfbarkeit (Unlinkability),…

IT-SICHERHEIT

Oder auch: Was wollen wir eigentlich erreichen?

„IT Sicherheit“

- **IT Sicherheit** (security): Schutz gegen nicht-authorisierte Manipulation oder Datenzugriff
- (Im Gegensatz dazu **Safety**: Schutz eines Systems gegen „natürliche“ Gefahren)
- Begriffe teilweise verschieden interpretiert, und nicht immer ganz einfach handzuhaben
- Annahmen treffen (Angreifermodell, Angriffsmodell)
  - Mehr in der Übung
- Schutzziele definieren
  - Letztes Kapitel und Übung

Warum ist „Security“ so kompliziert?

- Funktionsweise
  - Wenn der Benutzende <eine erwartete Eingabe> macht, dann macht das System <eine erwartete Aktion>
- Security
  - Wenn ein Benutzer oder eine Außenstehende <etwas Unerwartetes> tut, dann tut das System nicht <etwas wirklich Schlimmes>
- Warum ist Security schwierig?
  - Was sind die möglichen unerwarteten Dinge?
  - Woher wissen wir, dass sie alle geschützt sind?
  - Auf welcher Ebene der Systemabstraktion?
    - Software, Hardware, Krypto, Benutzer, ...?

Allgemein

- Security muss vor allem schützen
- Angreifende müssen nur eine Sicherheitslücke finden

Security in der Praxis

Design kann gut sein …

… doch die Implementierung kann unsicher sein!

- Wenn die Implementierung mehr Aktionen zulässt als der Entwurf, dann kann ein Angriff aufgrund eines Implementierungsfehlers erfolgreich sein.
- Und warum? Implementierungen, die in größere Zusammenhänge eingebettet sind, mit zusätzlichen Fähigkeiten und Beschränkungen.

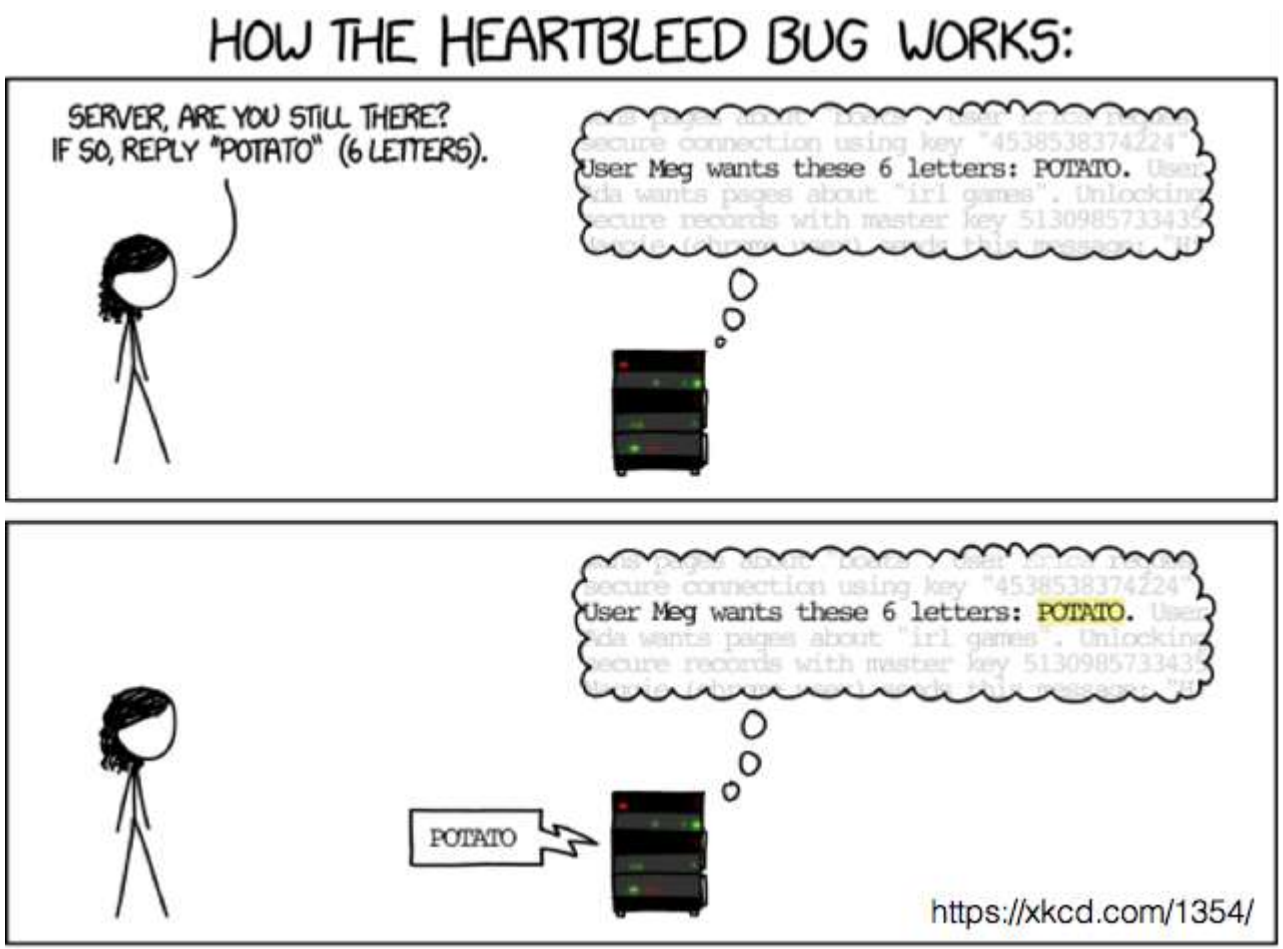
Beispiel: Heart Bleed

TLS ist das wichtigste Netzwerkprotokoll für sichere (verschlüsselte) Kommunikation, wird u.a. von HTTPS verwendet

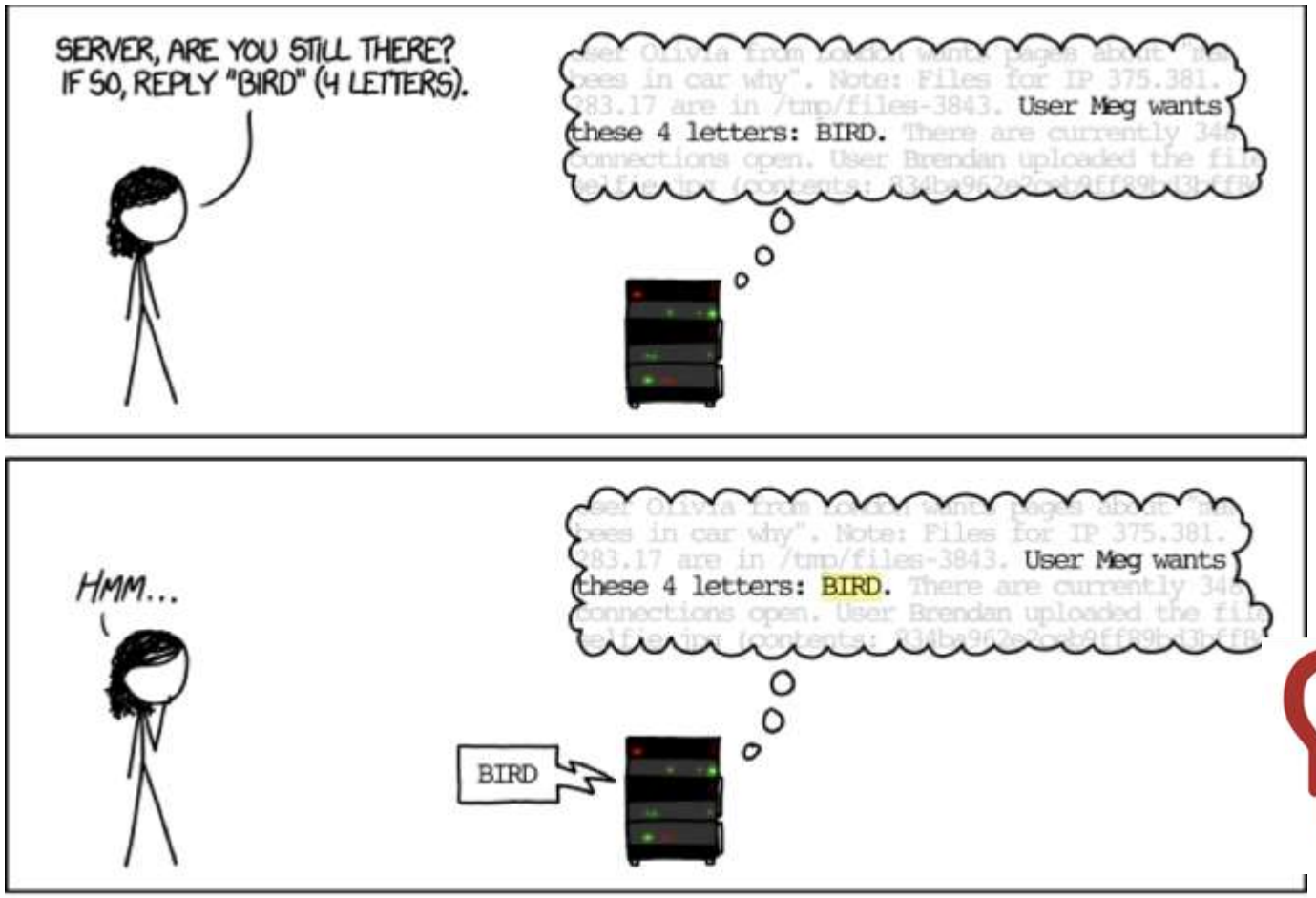
2014 wurde mit Heart Bleed (CVE-2014-0160) eine Schwachstelle in der gängigsten TLS-Implementierung entdeckt.

- Design des Protokolls war in Ordnung
- Implementierung hatte einen Fehler

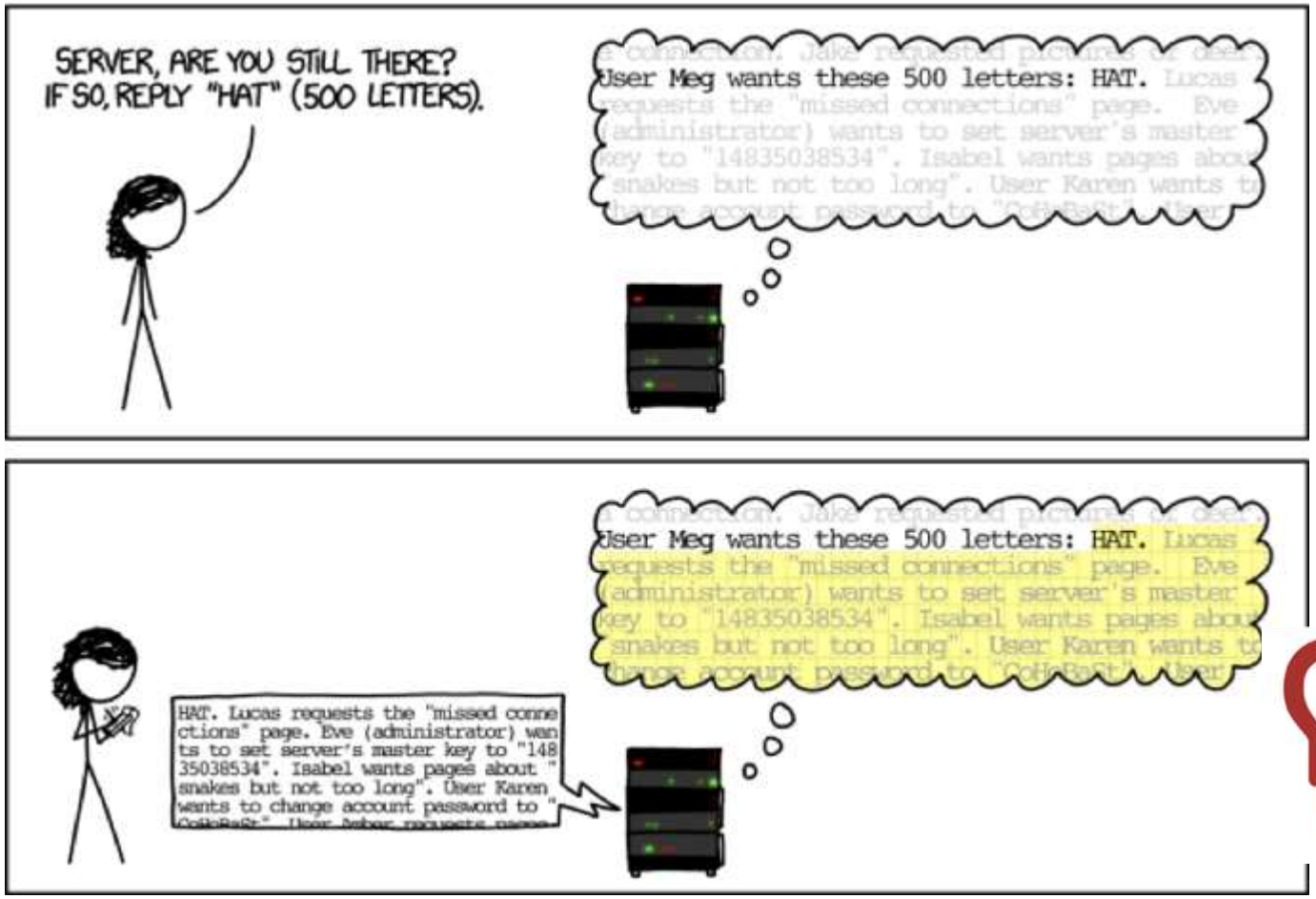
Beispiel: Heart Bleed



Beispiel: Heart Bleed



Beispiel: Heart Bleed



Beispiel: Heart Bleed

- Angreifende könnten bis zu 64kb des Serverspeichers anfordern
  - Ergebnis einer unsachgemäße Eingabevalidierung
  - Passwörter, Kreditkartennummern, private TLS-Schlüssel und mehr könnten in Erfahrung gebracht werden
- 2014 waren die meisten großen Unternehmen betroffen (Google, Yahoo, Facebook, usw.)
- Problem wurde sofort behoben

```
if (1 + 2 + payload + 16 > s->s3->rrec.length) return 0;
```

- Nutzenden wurde empfohlen, ihre Passwörter zu ändern.

Leibniz Universität Hannover

Vielen Dank für Ihre Aufmerksamkeit!

Fragen?