

Identitätsdiebstahl

Prof. Dr. Marc Pouly

`marc.pouly@hslu.ch`

ISF Vorlesung, Frühling 2017

Haltbarkeit einer Hacking Vorlesungen

The average time to patch for Microsoft Windows is 128 days while Linux averages out at 95 days

Probability of Attack based on System Vulnerability Life Cycle, IEEE 2008

*Give a man an exploit and you make him a hacker for a day;
teach a man to exploit bugs and you make him a hacker for a lifetime.*

Felix Lindner, Head of Recurity Labs

Ein Vorlesung kann nicht vor jeder dummen Idee warnen

Cablecom-Lücke: So schützen Sie sich

Cablecom-Kunden sollten ihr WLAN-Passwort ändern. Es lässt sich leicht knacken.

Wer bei Cablecom ein Internetabo abschliesst, erhält kostenlos ein Modem, einen Router oder eine Horizon-Box. Einige dieser Geräte verfügen über WLAN. Um drahtlos ins Internet zu gelangen, müssen Kunden auf ihrem Handy, Tablet oder Computer den entsprechenden WLAN-Namen und das Passwort eingeben. Diese Angaben sind auf der Unterseite des Cablecom-Geräts aufgedruckt.

Das Problem: Das Cablecom-WLAN-Passwort schützt angeschlossene Geräte nicht vor unbefugtem Zugriff. Auf

einer frei zugänglichen Webseite lässt sich anhand des WLAN-Namens das entsprechende Passwort leicht herausfinden. Das hat der K-Tipp nachgeprüft. Folge: Für Übeltäter ist es ganz einfach, private Daten zu lesen.

Cablecom-Sprecher Bernhard Strapp bestätigt die Sicherheitslücke. Alle betroffenen Kunden würden informiert. Und das können Cablecom-Kunden tun: Wer das WLAN-Passwort bereits geändert hat, hat nichts zu befürchten. Alle anderen sollten es unbedingt auch ändern. Infos zum Vorgehen unter cablecom.ch → Support → Suchwörter «WLAN Passwort regelmässig ändern». Im Zweifelsfall die Cablecom-Hotline, Tel. 0800 66 88 66, anrufen.

(cb)



Cablecom-Modem mit WLAN: Passwort sofort ändern



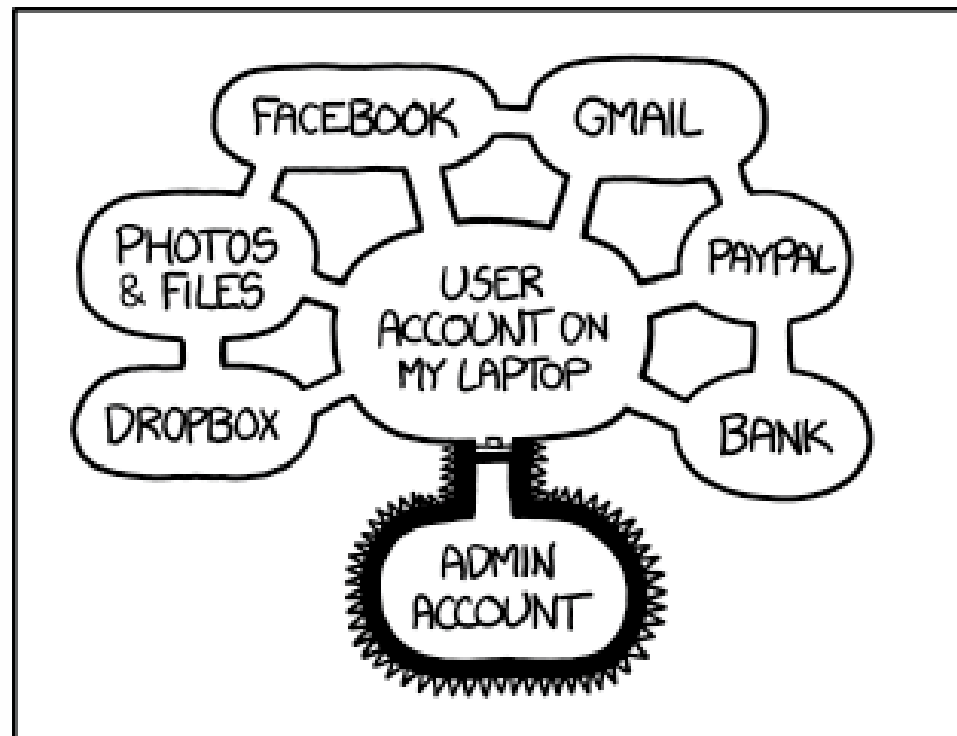
SSID = Passwort ???

Datum: 27.01.2016

Zielsetzung Identitätsdiebstahl

- Wir verstehen Fachbegriffe & Hacker Jargon
 - z.B. was ist Phishing, Pharming, Vishing
- Wir kennen grundsätzliche Angriffstechniken
 - z.B. wie funktionieren Rainbow-Tabellen
- Wir können die Bedrohungslage einschätzen
 - z.B. wie sicher ist E-Banking
- Wir kennen Abwehrmassnahmen und deren Mächtigkeit
 - z.B. wie funktioniert & was bringt Passwörter salzen
- Wir hinterfragen kritisch
 - z.B. Sinn von automatisch generierten Passwörtern / password policies

Wir verlieren manchmal den Blick fürs Wesentliche



IF SOMEONE STEALS MY LAPTOP WHILE I'M
LOGGED IN, THEY CAN READ MY EMAIL, TAKE MY
MONEY, AND IMPERSONATE ME TO MY FRIENDS,
BUT AT LEAST THEY CAN'T INSTALL
DRIVERS WITHOUT MY PERMISSION.

Leitsatz dieser Vorlesung



Put yourself in the attacker's shoes !



Identitätsdiebstahl



1. Ein Hacker stiehlt das E-Mail Passwort seines Vorgesetzten.
1. Ein Hacker stiehlt das Login Passwort zum PC eines Mitarbeiters.
2. Ein Hacker stiehlt ein Facebook Passwort.

Was könnten Sie als Hacker mit diesen Informationen tun ?

Weitere Konsequenzen von Informationsdiebstahl

In den USA ist Identitätsdiebstahl ein grosses Problem, weil es dort – anders als in der Schweiz – mit der Sozialversicherungsnummer ein personenbezogenes Merkmal gibt, das hinreichend ist, um Steuern zurückzufordern und Kreditkartenverträge abzuschliessen. [...] Allein 2011 belief sich der finanzielle Schaden infolge von Identitätsdiebstahl auf \$3.6 Mrd.

NZZ, 20.01.2014

[...] wenn Kriminelle ein E-Mail-Konto hackten und im Namen des Besitzers einen fiktiven Hilferuf an Freunde schickten, indem beispielsweise ein Überfall im Ausland vorgetäuscht werde, [...]. Erfahrungsgemäss würden 3% bis 8% der Empfänger tatsächlich mit Geldüberweisungen reagieren.

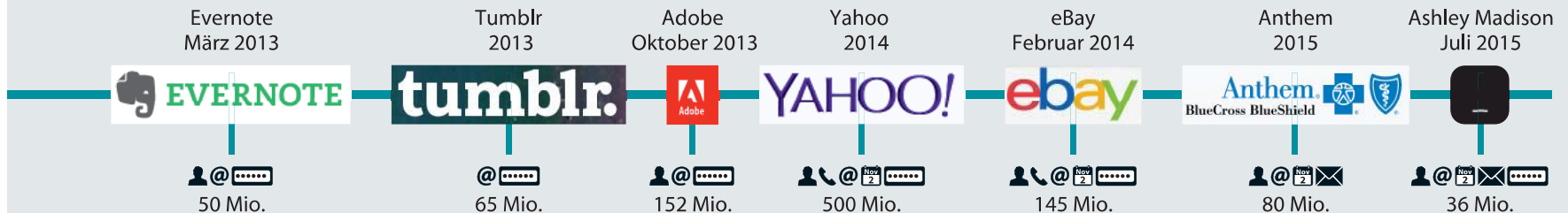
Martin Boess, Direktor der Schweizerischen Kriminalprävention, NZZ, 20.01.2014

Hinweis: Versicherungen sind ein guter Spiegel öffentlicher Wahrnehmung. Groupe Mutuel vertreibt eine weltweit gültige Rechtsschutzversicherung namens [Legisdigit](#), die die Versicherten gegen Risiken im Internet absichert. KPT und die Coop-Rechtsschutzversicherung haben ähnliche Produkte.

Prominente Datendiebstähle

Wenn eine geklaute User-Datenbank öffentlich bekannt wird, liegt der Diebstahl oft Monate oder sogar Jahre zurück. In der Zwischenzeit haben Kriminelle mit den Daten „gearbeitet“.

Nutzername
 Telefonnummer
 E-Mail-Adresse
 Passwort
 Anschrift
 Geburtsdatum



Quelle: c't 2016, Heft 23

<https://haveibeenpwned.com>

<http://www.idtheftcenter.org/2016databreaches.html>

Authentifizierung 1: Telnet & Remote Shell



Hacken Sie dieses System !

Angriffspunkt:

.....

Diese Protokolle stammen aus einer Zeit als Kabelverbindungen als abhörsicher galten

Gegenmassnahme:

.....

Authentifizierung 2: Mailinglist, Wikis & Foren



Hacken Sie dieses System !

Angriffspunkt:

Gegenmassnahme:

Passwörter in Klartext - öfters als man denkt ...

Microsoft Store in Indien gehackt – Passwörter in Klartext gespeichert

Eine Hackergruppe mit dem Namen „Evil Shadow Team“ hat sich nach eigenen Angaben Zugang zum indischen Microsoft Store verschafft. Die Hacker haben angeblich auch auf unverschlüsselte Nutzerdaten zugreifen können.

t3n.de am 13.02.12

January 6th, 2014, 15:47 GMT · By **Eduard Kovacs**

Clear Text Passwords of over 2,000 Users Leaked from the Directors Guild of Canada

July 13th, 2012, 11:20 GMT · By **Eduard Kovacs**

Billabong Hacked, Over 20,000 Clear Text Passwords Leaked



Ein konkretes Beispiel:

Der FTP Client FileZilla speichert Klartext-Passwörter in einer XML Datei

«This is by design. It's the task of the operating system to protect the user's files.»

FileZilla Forum Admin, 2007

Um diese Seite anzuzeigen, müssen Sie sich am Bereich „shield“ auf elk-shield.el.eee.intern: 5601 anmelden.
Ihr Kennwort wird unverschlüsselt übertragen.

Name:

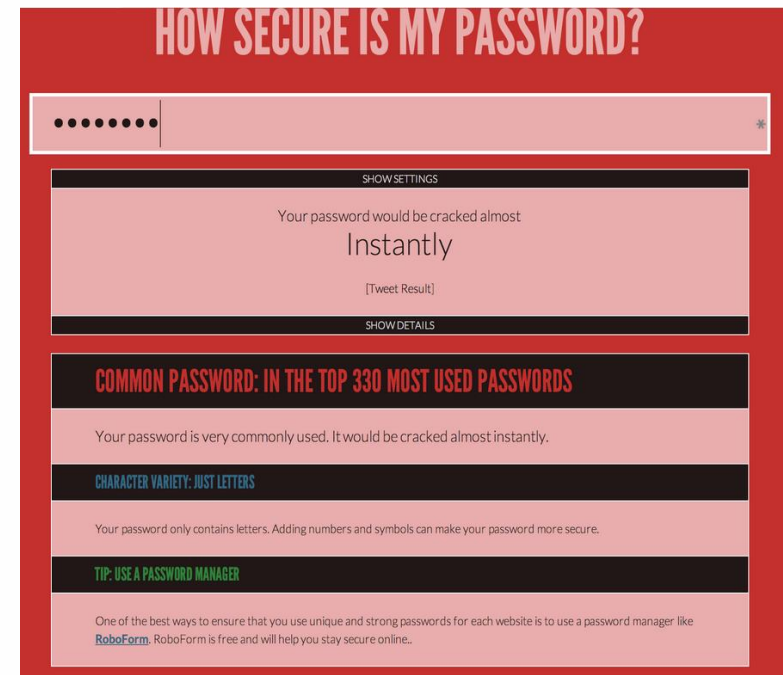
Kennwort:

☐ Kennwort im Schlüsselbund sichern

<http://elk-shield.el.eee.intern> über Safari

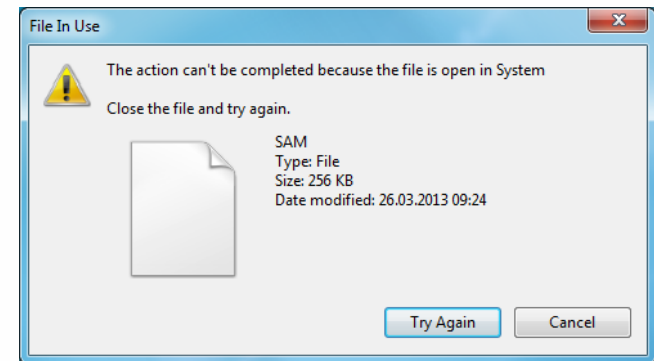
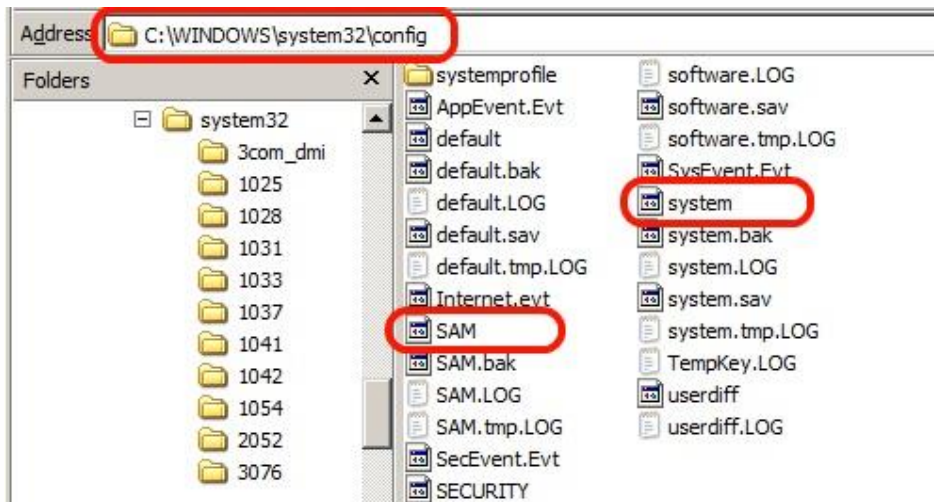
```
2 <Filezilla3>
3   <Servers>
4     <Server>
5       <Host>meineseite.de</Host>
6       <Port>21</Port>
7       <Protocol>1</Protocol>
8       <Type>0</Type>
9       <User>weiss_der_Provider</User>
10      <Pass>sollte_verschlüsselt_sein</Pass>
11      <Logontype>1</Logontype>
```

Wer kennt das nicht ...



Betriebssystemschutz von Passwortdateien: Windows

Windows Betriebssysteme (seit NT) speichern Passwortinformationen in der Registry Datei *Security Account Manager* (SAM). Windows Kernel sichert SAM, so dass Datei **nicht kopiert** werden kann.

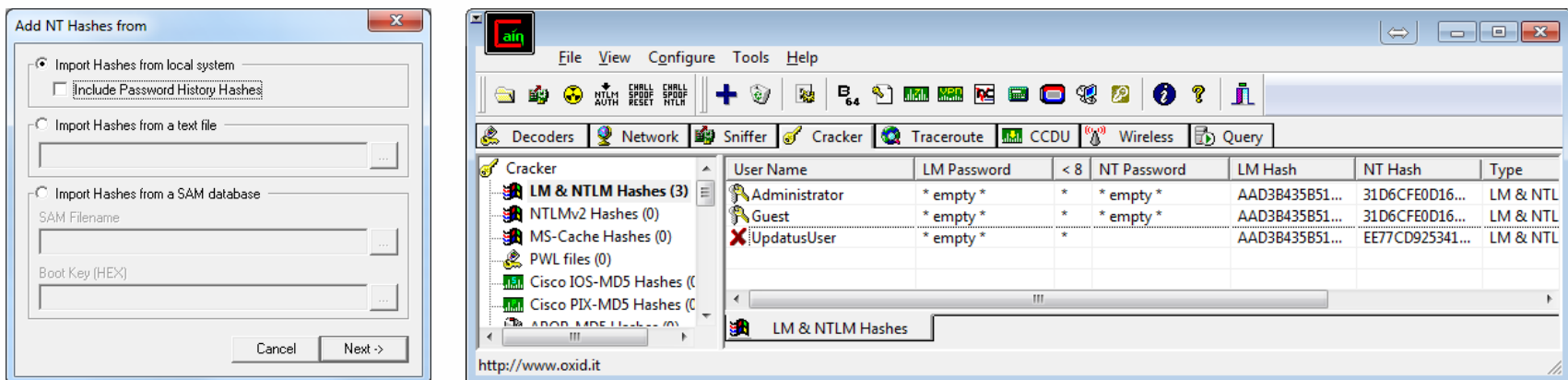


Kopierversuch einer SAM Datei

Wie klauen Sie die Passwortdatei mit Maschinenzugriff ?

So geht es trotzdem ...

Dumping File Sectors directly from Disk using Logical Offsets → [Cain](#)



Wenn SysKey aktiviert ist, verschlüsselt Windows die SAM Datei partiell.

Ändert dies etwas ?

Wenn SysKey aktiviert ist, holt bkhive den Schlüssel aus der Registry.

Betriebssystemsicherheit von Passwortdateien: Linux

Unix Betriebssysteme (seit 1990) speichern Passwortinformationen in Shadow Dateien. Nur Superuser können diese Dateien lesen.

Wie klauen Sie die Passwortdatei mit Maschinenzugriff ?

[John the Ripper](#) beinhaltet `unshadow` Befehl

```
> umask 077  
> unshadow /etc/passwd /etc/shadow > mypasswd
```

Speicherort von Passwortdateien:

Alte Unix Versionen (vor 1990)	→ <code>/etc/passwd</code>
Moderne Unix Versionen	→ <code>/etc/shadow</code>
BSD Unix	→ <code>/etc/master.passwd</code>
Mac OS (10.2 und früher)	→ <code>/private/var/db/netinfo/local.nidb/</code>
Mac OS (10.3 – 10.6)	→ <code>/var/db/shadow/hash/</code>
Mac OS (10.7 und später)	→ <code>/var/db/dslocal/nodes/Default/users/</code>

Passwortdateiklau **mit** Maschinenzugriff → Fazit

- In Klartext gespeicherte (z.B. FileZilla) oder gecachte (z.B. Windows-Domänen Anmeldung) Passwörter können mit Maschinenzugriff leicht geklaut werden.

Der Hacker bekommt die Passwörter direkt !

- Betriebssysteme schützen Passwortdateien, jedoch kann der Schutz leicht umgangen werden.
- Anwendungsprogramme und Betriebssysteme hashen Passwörter bevor sie in einer Passwortdatei abgelegt werden.

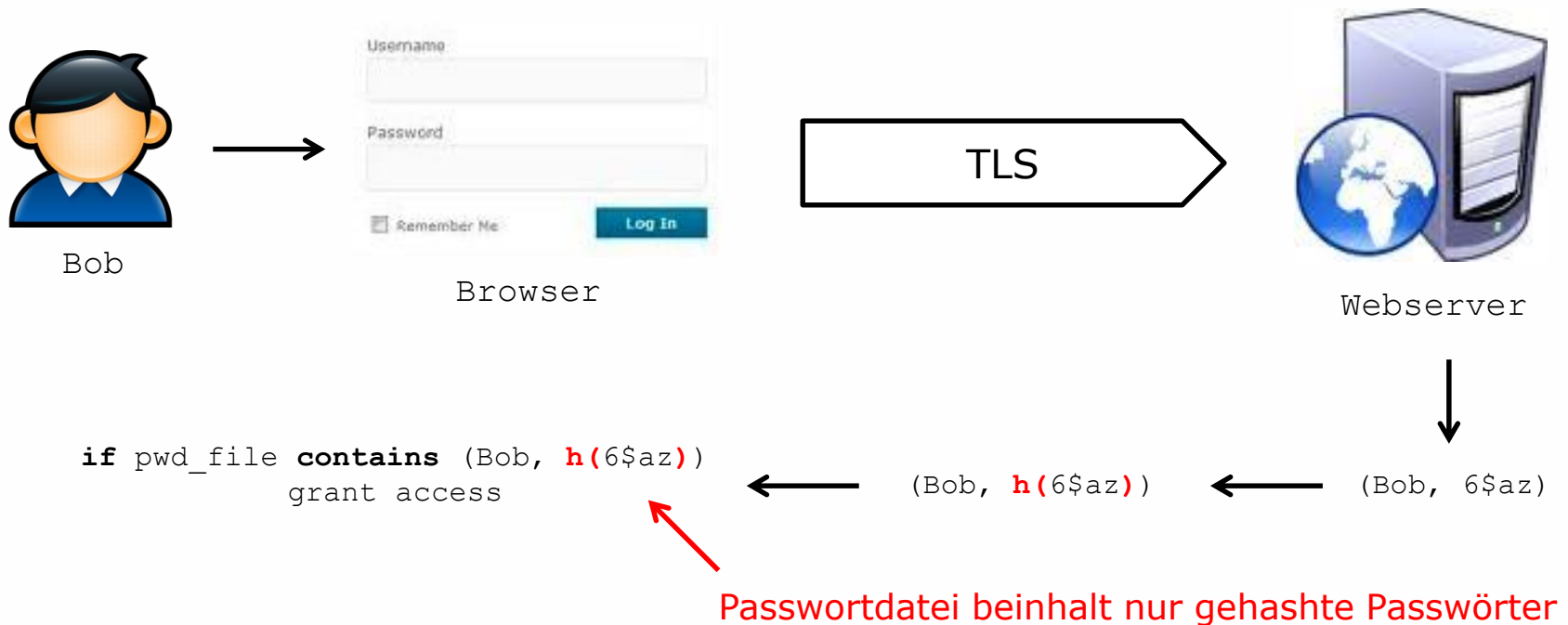
Der Hacker bekommt die Passwortdatei - Passwörter sind aber gehasht !

Passwortdateiklau **ohne** Maschinenzugriff

z.B. mittels SQL Injection oder ...

Authentifizierung 3: Windows Login

Passwörter werden mit einer Einwegfunktion (Hashfunktion) gehasht



Angriffspunkt:

.....

Unsere Webshop Kontodaten

username	email	password	use
christopher.christensen	christoph.christensen@stud.hslu.ch	67a0faf2d32193abf3d062317051708f:	Regis
CyrilleUlmi	cyrille.ulmi@stud.hslu.ch	bd41d90244e96fbc684829a5cb71467a:	Regis
daniel	daniel.foehn@stud.hslu.ch	2145b2cf11f6be38f3d00c582364189a:	Regis
valentin_buergler	valentin.buergler@stud.hslu.ch	164d5fd02634293161afac4cf47299:	Regis
hasselman	thomas.hasselman@stud.hslu.ch	36c749510b2be036136a92a9c1408ac4:	Regis
tavoney	andre.voney@stud.hslu.ch	7def8616a7670a07abb2a1229d9f0b97:	Regis
muhamed.delic	muhamed.delic@stud.hslu.ch	238b5936a3ebce499d7dd5fb72af536d:	Regis
fabmeyer	fabian.meyer@stud.hslu.ch	8cf63880e5d477e850046af7e8daabd0:	Regis
Peter	pascal.stalder@stud.hslu.ch	624d8e6eb27881661fa58d8a1df9156c:	Regis
joel.salzmann@stud.hslu.c	joel.salzmann@stud.hslu.ch	1adbb3178591fd5bb0c248518f39bf6d:	Regis
TheDude	simon.beck@stud.hslu.ch	bfe3ac3ba3db12d9deeb81ce99e3d3a:	Regis
tagabrie	severin.gabriel@stud.hslu.ch	d4e7f8a52dd276a4a25f7873bd5ff23b:	Regis
mzzzz	michael.zurmuehle@stud.hslu.ch	2e8583df29a4c7b6c892e8144bcc75d:	Regis
tabubalo	mario.bubalovic@stud.hslu.ch	16031ce9bd0a73b4a5860e5556dd7b6a:	Regis
lari	larissa.schuler@stud.hslu.ch	df5ea29924d39c3be8785734f13169c6:	Regis
tabay	hamide.bay@stud.hslu.ch	ef12f691c81f56b91e4c0be8a0f89541:	Regis
tckueng	stefan.kueng@stud.hslu.ch	85402764bf469fa48e716a60a46fb42c:	Regis
Morty	eric.brun@stud.hslu.ch	c4ca4238a0b923820dcc509a6f75849b:	Regis
jonas.keiser	jonas.keiser.01@stud.hslu.ch	c8a011db5f24228011fd6956f9858053:	Regis
Sascha	sascha.saegesser@stud.hslu.ch	5f2b910d2eec1102d8cf1756398061a5:	Regis
xKev	kevin.huber@stud.hslu.ch	cb76013bffa977901d250af139744c08:	Regis
markuskaufmann	markus.kaufmann@stud.hslu.ch	6c00b9cb4bd690de2ecc4f677389ccc:	Regis
melvin.werthmueller	melvin.werthmueller@stud.hslu.ch	8042c2ef76e94fb1b546ec621c46c769:	Regis
tajoerim	christoph.joerimann@stud.hslu.ch	16d7a4fca7442dda3ad93c9a726597e4:	Regis
iaarnold	lukas.arnold.01@stud.hslu.ch	afbd0822f9992dc450a42e15339c1b40:	Regis
patrick.bucher	patrick.bucher@stud.hslu.ch	12e561114335b1d5f547a67cf85c4d08:	Regis
PatrickF	patrick.forrer@stud.hslu.ch	39bb37cf36d3b29a9280d8a70a0eed42:	Regis
tobiaskaufmann	tobias.kaufmann@stud.hslu.ch	19118e184f6ea8aebdf000d61521b03b:	Regis
alex	alexander.karlen@stud.hslu.ch	f30aa7a662c728b7407c54ae6bfd27d1:	Regis
StefanieVogel	stefanie.vogel@stud.hslu.ch	827ccb0eea8a706c4c34a16891f84e7b:	Regis

Verwendete Hashfunktionen

Alte Unix Versionen	→ DES
Moderne Unix Versionen	→ MD5
Red Hat Enterprise	→ SHA-512 (SHA2 Familie)
OpenBSD	→ Blowfish
Mac OSX	→ SHA1
Windows Screenshot)	→ LANMAN oder MD4 (genannt NT Hash, vgl. Cain & Abel

Angriffsstrategien

1.Passwort-Hashfunktion knacken

2.Brute-Force Attacken

- Alle möglichen Kombinationen werden systematisch durchprobiert
- Jeder Kandidat wird ghasht und in der Passwortdatei gesucht
- Vorteil: knackt irgendwann jedes Passwort → **vollständige Methode**



Eine kleine Rechenaufgabe

Passwörter bestehen aus den Symbolen (A-Z, a-z, 0-9) und 8 zusätzlichen Sonderzeichen. Das Content Management System Joomla hasht Passwörter mit MD5. Wir verwendet die Software [oclHashcat](#) für einen Brute-Force Angriff mit folgendem PC: 2x AMD HD 6990, 880 MHz GPU, 1250 MHz RAM, Catalyst 12.1, Windows 7 x64. [Benchmark](#) Tests ergaben 23083.9 M/s also rund $23 \cdot 10^9$ Hashs / s.

1. Via Social-Engineering erfahren wir, dass der User ein Passwort der Länge 7 hat. Wie lange beträgt die maximale Wartezeit, bis das Passwort sicher gefunden worden ist?

1. Wie lange müsste man ein Passwort wählen, um ein akzeptables Mass an Sicherheit gegen Brute-Force-Angriffe zu erhalten?

1. Wie bewerten Sie folgende Schlagzeile im 20min?



Nein, «Jesus» ist kein gutes **Passwort**

Leichtes Spiel für Hacker: Noch immer benutzen viele User für ihre Web-Profile unsichere Passwörter - dabei wäre es doch so einfach. Hier die schlechtesten Logins und ein paar Tricks. ...

Publiziert am 24/10/2012 in News

Lösungen

Maximale Wartezeit für Passwörter der Länge 7:

$$((70^7) \text{ s}) / (23 * (10^9)) = 5,96 \text{ Minuten}$$

Maximale Wartezeit für Passwörter der Länge 8:

$$((70^8) \text{ s}) / (23 * (10^9)) = 6,96 \text{ Stunden}$$

Maximale Wartezeit für Passwörter der Länge 9:

$$((70^9) \text{ s}) / (23 * (10^9)) = 20,30 \text{ Tage}$$

Maximale Wartezeit für Passwörter der Länge 10:

$$((70^{10}) \text{ s}) / (23 * (10^9)) = 3,89 \text{ Jahre}$$

Maximale Wartezeit für Passwörter der Länge 11:

$$((70^{11}) \text{ s}) / (23 * (10^9)) = 272,43 \text{ Jahre}$$

Weitere Angriffsstrategien

Brute-Force Angriffe werden bei Passwörtern ab Länge 9 uninteressant.

Vielen Menschen fällt es schwer, sich lange, kryptische Passwörter zu merken und greifen daher auf Merkhilfen zurück.

3. Wörterbuch Attacken

- Nur Wörter aus einem vorgegebenen Wörterbuch werden durchprobiert
- Beruht auf Annahme, dass sinnvolle Wörter als Passwort verwendet wurden oder dass beim Passwort ein Algorithmus hinterlegt ist (z.B. Palindrom)
- Knackt nur Passwörter im Wörterbuch (**unvollständige Methode**)

4. Lookup Tabellen

- Wörterbuch mit 1M Wörter verlangt 1M Hashberechnung
- Effizienter sind Wörterbücher mit (Wort / Hashwert) Einträgen
- Jetzt muss nur noch nach dem Hashwert gesucht werden
- Trade-off: man investiert mehr Memory um Rechenzeit zu sparen.
- Knackt nur Passwörter in der Tabelle (**unvollständige Methode**)

Wörterbücher gibt es zum Beispiel [hier](#)

Wörterbuch-Angriffe durch Regeln ergänzen

- **Variationen mit Gross- / Kleinschreibung**
z.B. *Osterhase* → *OsterHase, oStErHaSe, OSTERhase, ...*
- **Variationen mit Zahlen und Sonderzeichen**
z.B. *Osterhase* → *O1s2t3e4r5h6a7s8e*
- **Buchstaben durch Zahlen ersetzen:**
z.B. *Osterhase* → *15st5rh1se*
- **Kombination mehrere Wörter aus dem Wörterbuch**
z.B. *<Wort><Leerzeichen><Wort>* oder *<Wort><Bindestrich><Wort>*
z.B. *Osterhase* → *OsterhaseesahretsO* oder *Zitate*
- **Kombination mit Brute-Force:**
Für jeden Wörterbucheintrag (z.B. *Adam*) wird ein Brute-Force-Angriff (z.B. mit Längenbeschränkung 4) gestartet. Dies findet *Adam1234, Adam&Eva, Adam%2;e*

Nebst den eingebauten Regeln können eigene Regeln definiert werden, und die Software kann durch Analyse von geknackten Passwörtern eigene Regeln dazulernen. Der BruteForce++ Modus von Hashcat nutzt auch probabilistische Modelle (Markov-Ketten)

Terrible! Top 30 Worst Ashley Madison Passwords

PASSWORD	NUMBER OF USERS
123456	120511
12345	48452
password	39448
DEFAULT	34275
123456789	26620
qwerty	20778
12345678	14172
abc123	10869
pussy	10683
1234567	9468

PASSWORD	NUMBER OF USERS
696969	8801
ashley	8793
fuckme	7893
football	7872
baseball	7710
fuckyou	7458
111111	7048
1234567890	6572
ashleymadison	6213
password1	5959

PASSWORD	NUMBER OF USERS
madison	5219
asshole	5052
superman	5023
mustang	4865
harley	4815
654321	4729
123123	4612
hello	4425
monkey	4296
000000	4240



WORST PASSWORDS OF 2015



SplashData releases its annual list in an effort to encourage the adoption of stronger passwords to improve Internet security. The passwords evaluated are mostly from North American and Western European users. The list shows many **people continue to put themselves at risk for hacking and identity theft** by using weak, easily guessable passwords.



RANK	PASSWORD	CHANGE FROM 2014
1	123456	Unchanged
2	password	Unchanged
3	12345678	1 ↑
4	qwerty	1 ↑
5	12345	2 ↓
6	123456789	Unchanged
7	football	3 ↑
8	1234	1 ↓
9	1234567	2 ↑
10	baseball	2 ↓
11	welcome	NEW
12	1234567890	NEW
13	abc123	1 ↑
14	111111	1 ↑
15	1qaz2wsx	NEW
16	dragon	7 ↓
17	master	2 ↑
18	monkey	6 ↓
19	letmein	6 ↓
20	login	NEW
21	princess	NEW
22	qwertyuiop	NEW
23	solo	NEW
24	password	NEW
25	starwars	NEW



"123456" and "password" once again reign supreme as the most commonly used passwords



Some longer passwords are so simple as to make their extra length virtually worthless



Sports remain a popular password theme. While baseball may be America's pastime, "football" has overtaken it as a popular password. "Football" climbed three spots to number 7 and "baseball" dropped two spots to number 10.



"We have seen an effort by many people to be more secure by adding characters to passwords, but if these longer passwords are based on simple patterns they will put you in just as much risk of having your identity stolen by hackers."

Morgan Slain, CEO of SplashData

SPLASHDATA OFFERS THREE SIMPLE TIPS TO HELP PEOPLE PROTECT



Use passwords or passphrases of twelve characters or more with mixed types of characters



Avoid using the same password over and over again on different websites



Use a password manager such as TeamsID to organize and protect passwords, generate random passwords, and automatically log into websites



TeamsID

www.teamsid.com

Rainbow Tabellen: Motivation

Vorteile / Nachteile von Brute-Force

- Brute-Force knackt (irgendwann) jedes Passwort
- Brute-Force berechnet alle Hashs online
- Erneuter Brute-Force Angriff bedarf der wiederholten Berechnung aller Hashs

Vorteile / Nachteile von Lookup Tabellen

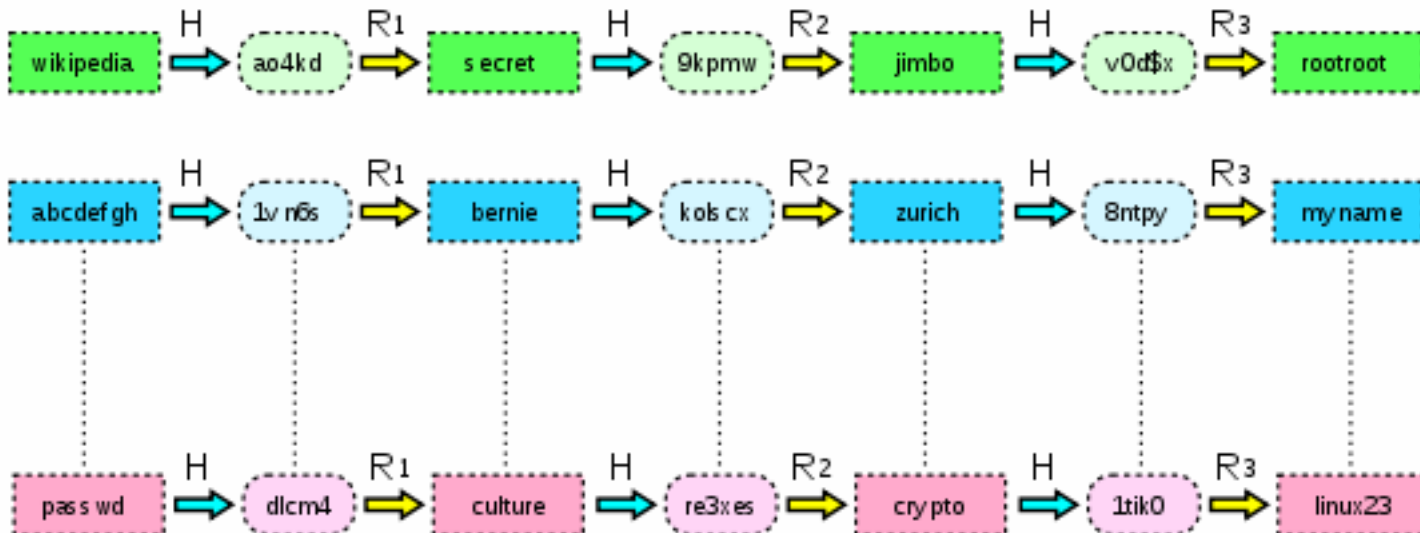
- Lookup Tabellen können offline berechnet und wiederverwendet werden
- Eine vollständige Lookup Tabelle knackt irgendwann jedes Passwort
- So eine Lookup Tabelle wäre zu gross → 1.4 TB für Passwörter mit 6 Stellen

Hashberechnungen vs. Speicherbedarf vs. Vollständigkeit

Rainbow Tabellen bieten einen Mittelweg / Kompromiss

Hashketten

Hashketten alternieren Hashberechnungen und Reduktionen

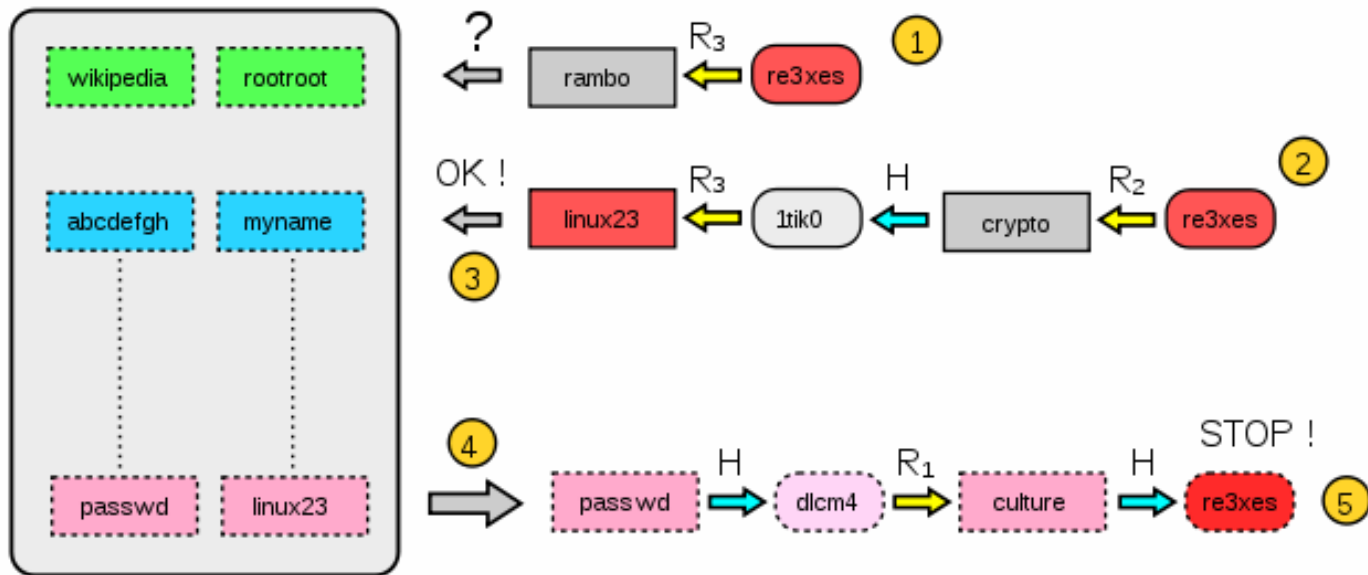


Bildquelle: Wikipedia

Eine Reduktion verwandelt einen Hashwert mittels eines Wörterbuchs wieder in ein mögliches Passwort. Zur Minimierung von Kollisionen sollten bei jedem Schritt eine andere Reduktion verwendet werden.

Rainbow Tabellen

Nur der erste und letzte Eintrag einer Hashkette wird gespeichert.



Quelle: Wikipedia













Beispiel: Knacken des Hashs **re3xes** mit der Rainbow Tabelle

Vorteile / Nachteile von Rainbow Tabellen













- Hybride Version von Lookup und Brute-Force
- Kompromiss bezüglich Hashberechnungen, Speicherplatz, Vollständigkeit
- Verschiedene Tabellen für verschiedene Hash-Algorithmen
- Knackt nur Passwörter im Wörterbuch (**unvollständige Methode**)
- Auf Passwörter einer fixen Länge spezialisiert

Rainbow Tabellen in der Praxis

NTLM Rainbow Tables

Table ID	Charset	Plaintext Length	Key Space	Success Rate	Table Size	Files	Performance
 ntlm_ascii-32-95#1-7	ascii-32-95	1 to 7	70,576,641,626,495	99.9 %	64 GB	Files	
 ntlm_ascii-32-95#1-8	ascii-32-95	1 to 8	6,704,780,954,517,120	96.8 %	576 GB	Files	
 ntlm_mixalpha-numeric#1-8	mixalpha-numeric	1 to 8	221,919,451,578,090	99.9 %	160 GB	Files	
 ntlm_mixalpha-numeric#1-9	mixalpha-numeric	1 to 9	13,759,005,997,841,642	96.8 %	864 GB	Files	
 ntlm_loweralpha-numeric#1-9	loweralpha-numeric	1 to 9	104,461,669,716,084	99.9 %	80 GB	Files	
 ntlm_loweralpha-numeric#1-10	loweralpha-numeric	1 to 10	3,760,620,109,779,060	96.8 %	396 GB	Files	

MD5 Rainbow Tables

Table ID	Charset	Plaintext Length	Key Space	Success Rate	Table Size	Files	Performance
 md5_ascii-32-95#1-7	ascii-32-95	1 to 7	70,576,641,626,495	99.9 %	64 GB	Files	
 md5_ascii-32-95#1-8	ascii-32-95	1 to 8	6,704,780,954,517,120	96.8 %	576 GB	Files	
 md5_mixalpha-numeric#1-8	mixalpha-numeric	1 to 8	221,919,451,578,090	99.9 %	160 GB	Files	
 md5_mixalpha-numeric#1-9	mixalpha-numeric	1 to 9	13,759,005,997,841,642	96.8 %	864 GB	Files	
 md5_loweralpha-numeric#1-9	loweralpha-numeric	1 to 9	104,461,669,716,084	99.9 %	80 GB	Files	
 md5_loweralpha-numeric#1-10	loweralpha-numeric	1 to 10	3,760,620,109,779,060	96.8 %	396 GB	Files	

Durch immer schnellere Computer für Brute-Force-Angriffe verlieren Rainbow Tabellen langsam an Bedeutung. Heute werden Rainbow Tabellen hauptsächlich für Passwörter der Länge 8 und 9 eingesetzt, oder bei nicht-sprechenden Passwörter, weil da Wörterbuch-Attacken nicht funktionieren.

Verteidigungsmassnahmen

- Massnahme gegen Brute-Force: Hashfunktion muss langsam sein
 - Mehrfach-Hash, z.B. `sha1 (sha1 (sha1 (pwd)))`
 - Hashfunktionen kombinieren, z.B. `sha1 (blowfish (pwd))`
- Passwörter salzen:
 - Salt ist eine zufällig generierte Zeichenkette
 - Berechne den Hash von Passwort und Salz $\rightarrow h(\text{pwd} . \text{salt})$
 - Salz und Hashwert werden zusammen in der Passwortdatei gespeichert

Beispiel: Passwortdatei Eintrag in Red Hat Enterprise Linux:

```
joeuser:$6$a1CD9VXvGYo8oScU$0cXhIS3yGke63nr2LmV7eVwLyn97iEzPCSSmwkdytDxBbyLkuZSE8gTtwWIo60l/mI2tiJnCpW5alcDoi
```

```
6 = "Use SHA-512 hashing"
```

```
salt = a1CD9VXvGYo8oScU
```

```
hash = 0cXhIS3yGke63nr2LmV7eVwLyn97iEzPCSSmwkdytDxBbyLkuZSE8gTtwWIo60l/mI2tiJnCpW5alcDoEUI2T/
```

Gegen welche Angriffe hilft Salz ?

Don't eat your Password without Salt !?

Salts used by various operating systems		
Operating system	Salt bits	Number of possible salt values
Windows Mac OS before OS X 10.4	0	1 That is, the one empty salt
Unix (SunOS, Solaris 2.6 through 2.8, HP-UX, OpenBSD, etc)	12	4,096
Mac OS X 10.4 and later	32	4,294,967,296
Unix (Solaris 9 and later, Linux)	48	281,474,976,710,656
Unix with Glibc <code>crypt()</code> supporting 96-bit salts (Linux)	96	79,228,162,514,264,337,593,543,950,336

Sind Password Policies sinnvoll ?

Bei Verwendung von Salz bleiben Wörterbuch und Brute-Force als Angriffe.

- Wörterbuch Attacken erschweren → *strukturloses* Passwort wählen
- Brute-Force Attacken erschweren → *langes* Passwort wählen

1. Was bedeutet strukturlos / lang?

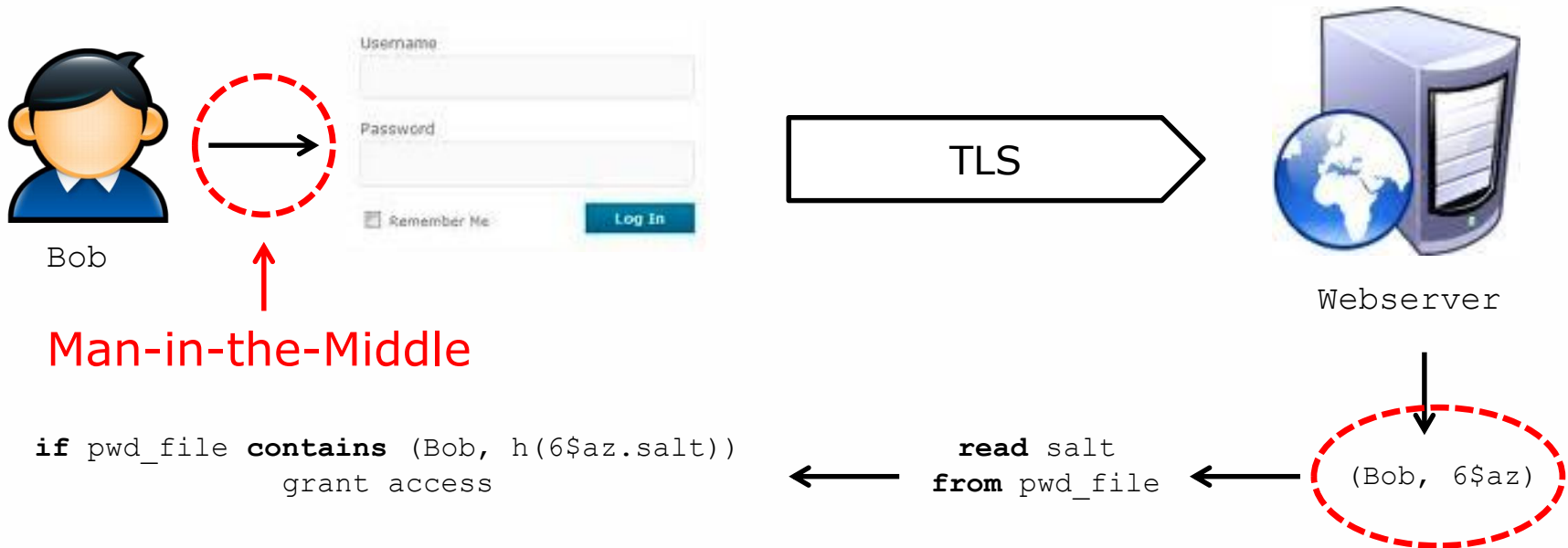
2. Löst also ein langes und kompliziertes Passwort das Problem?

3. Das SAP Tool der HSLU zwingt mich dazu, alle 3 Monate ein neues Passwort mit Mindestlänge 9 zu setzen. Was halten Sie davon?



Authentifizierung 4: UNIX Login

Passwörter gesalzen und gehasht



Angriffspunkt:



Das klappt leider nicht ...

«Das Passwort wird über den verschlüsselten Kanal zum Server geschickt. Das heisst, der Server sieht das Passwort nach dem Entschlüsseln im Klartext. Man könnte doch bereits auf Client-Seite den Hashwert berechnen und diesen zum Server schicken. Dann erfährt ein potentiell mit Spyware infizierter Server das wahre Passwort nicht.»

Warum funktioniert das nicht ?

.....

.

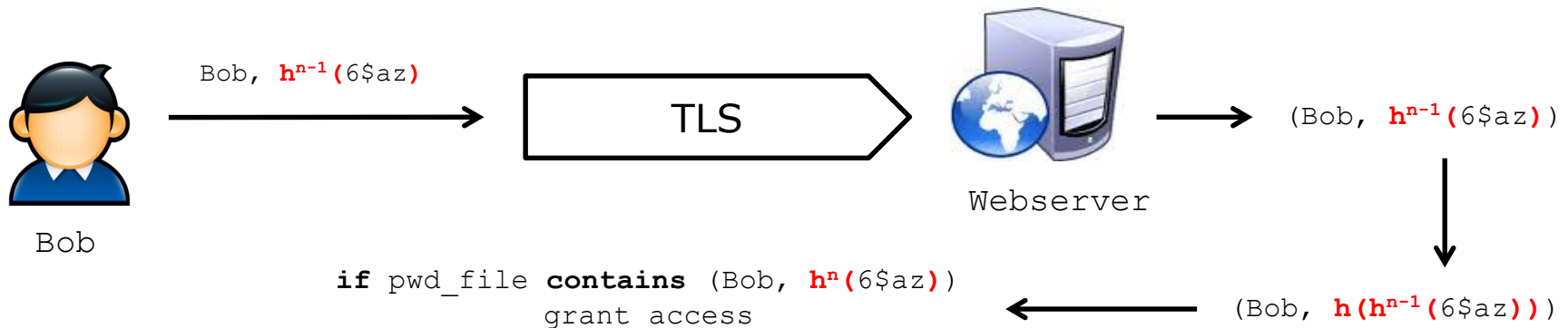
.....

.

Die gleiche Idee haben diese mal durchgedacht

S/KEY Protokoll (vereinfacht)

Annahme: Server und Benutzer kennen ein Geheimnis, z.B. eine Zahl $n > 1$



Danach ersetzt Server $h^n(6\$az)$ durch $h^{n-1}(6\$az)$ in `pwd_file`
 n wird dekrementiert

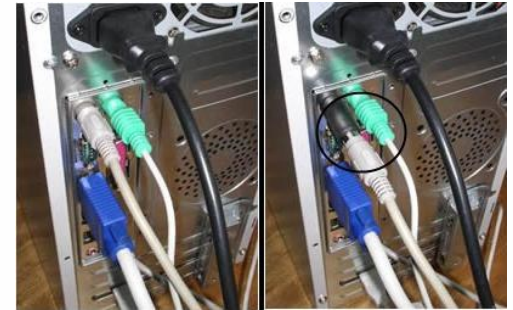
Bei $n = 1$ muss ein neues Passwort gesetzt werden

Welche Vor- und Nachteile sehen Sie ?

.....

Man-in-the-Middle: Keylogger

- Hardware Keylogger
- Skimming (Overlay Tastatur)
- Software Keylogger (Spyware)
- Akustische Keylogger (mit Richtmikrofon)
- Elektromagnetische Keylogger
- Optische Keylogger
- ...



Man-in-the-Middle: Phishing

static-71-97-100-231.dfw.dsl-w.verizon.net/postfinance.ch/index.php

Web static-71-97-100-231.dfw.dsl-w.verizon.net/postfinance.ch/index.php


PostFinance DIE POST **Besser begleitet.** [de](#) [fr](#) [it](#) [en](#) | [Home](#) | [Die Post](#) | [Kontakt](#) | [Sitemap](#)


[Privatkunden](#) [Geschäftskunden](#) [Kundendienst](#) [Wir über uns](#) [Jobs](#)

E-Finance Login

Sie verwenden einen von uns nicht unterstützten Browser. Weitere Informationen erhalten sie [hier](#).


Bitte geben Sie Ihre Sicherheitselemente ein

E-Finance Nummer 


Passwort 


→ [Passwort vergessen](#)

Als Kunde mit einer Benutzeridentifikation geben Sie diese zusätzlich ein

Benutzeridentifikation 

Kundendienst

 [Hilfe zu E-Finance](#)

 [Häufige Fragen zu Login](#)

Sicherheitshinweise

→ [Sicherheit im Internet](#)

→ [e-banking - aber sicher!](#)

Werden Sie Online-Kunde

E-Finance

Hier bieten wir Ihnen die günstigsten Konditionen. Erledigen Sie Ihre Geldgeschäfte sicher via Internet:

→ [Infos zu E-Finance](#)

→ [Demo E-Finance testen](#)

Betreff: Betreff:'Ihr'E+Banking+Zugang'mail.ridicaky+zipet.cz

Datum: Freitag,'11.'März'2016'10:06:55'MiDeleuropäische'Normalzeit

Von: Kantonalbank

An: Kantonalbank



Kantonalbank

Gemeinsam wachsen.

[de](#) | [fr](#) | [it](#) | [en](#)

[Home](#) |

Sehr geehrte Kundin, sehr geehrter Kunde!

Bitte beachten Sie, dass Ihr e-Banking Zugang bald abläuft, da dieser noch nicht unserem neuen e-Banking System angepasst wurde. Dies hätte automatisch erfolgen sollen, wurde aber bei einigen e-Banking Zugängen wegen Überlastung unseres Servers nicht abgeschlossen. Diese e-Banking Zugänge müssen nun manuell aktiviert werden, um einer automatischen Sicherheitssperrung vorzubeugen. Sollte Ihr Zugang aus Sicherheitsgründen gesperrt werden, müssen Sie bis zu 28 Tagen warten, bis Sie Zugangsdaten für das neue e-Banking per Post erhalten und Ihr e-Banking wieder nutzen können. Bitte führen Sie daher die Aktualisierung so schnell wie möglich durch, um Probleme in Ihrem e-Banking zu vermeiden. Um Ihren e-Banking Zugang jetzt zu aktivieren, melden Sie sich zunächst hier bei Ihrem e-Banking an, und füllen Sie das Online-Formular aus.

[> Klicken Sie hier - >](#)

Nach Ausfüllen des Formulars haben Sie den ersten Schritt zur Aktivierung des neuen e-Bankings beendet. Wir danken Ihnen für Ihre Mitarbeit und Ihr Verständnis.

Freundliche Grüße,

Ihr Kantonalbank Team



Aufgabe: Imaginärer Angriff auf die UBS

Diskutieren Sie einen Phishing Angriff auf die UBS.

Stellen Sie den Nachrichtenverkehr zwischen User, Bank und Hacker grafisch dar.

Die UBS Login Prozedur mit TAN Generator ist unten abgebildet.

Eingabe der Vertragsnummer

Zur Prüfung Ihrer Zutrittsberechtigung bitten wir Sie um folgende Angabe:

Vertragsnummer:

Bei Problemen mit dem Login hilft Ihnen die [Online Hilfe](#) weiter.

Hier können Sie die Funktionalitäten des e-bankings mit Demodaten ausprobieren.
Alle Daten in diesem Demo-Vertrag sind öffentlich zugänglich und einsehbar.

Login mit Access Card und Kartenleser

Zur Prüfung Ihrer Zutrittsberechtigung bitten wir Sie um folgende Angabe:

Vertragsnummer:

Eingabe:

Code:

E-Banking Authentifikation

1 R19Y	11 QVI8	21 ZURD	31 35AH	41 19GN	51 B68N	61 1U4F	71 9FB6	81 TSD8	91 J9L5
2 RENT	12 WNJD	22 RD1R	32 731W	42 S2RJ	52 CWI4	62 W3H2	72 KUPB	82 4YWY	92 PR8T
3 3DVI	13 EP7Y	23 NG8T	33 U7N2	43 ZS1J	53 46KK	63 TPLR	73 UF27	83 TENN	93 DBGY
4 7YD1	14 HWZ8	24 SHEJ	34 97MZ	44 WYSD	54 KLM6	64 12Z9	74 NY1E	84 L1QF	94 7K6B
5 DWVN	15 SL4X	25 5GLF	35 PQG8	45 MDV9	55 W6GI	65 GIC5	75 UFMT	85 SRFR	95 RE4Y
6 W1Y8	16 DLJ8	26 IJM5	36 C739	46 JLTD	56 AP2C	66 5HNU	76 LPNS	86 X9RH	96 HT7V
7 6P4Z	17 ARRS	27 3WKB	37 2AF4	47 S7FM	57 K3R3	67 KDVM	77 EWR6	87 EAIK	97 3LFB
8 I4KT	18 VFGL	28 C6IC	38 TIJ9	48 3N4G	58 CMJE	68 29SF	78 GXF5	88 9QLK	98 RJNB
9 J83N	19 QPL4	29 QGNX	39 PM8A	49 DBCQ	59 TXRL	69 3I8B	79 UBP9	89 NB6M	99 94YL
10 L8IN	20 MUY2	30 YY8Q	40 CJ17	50 PT7P	60 16FA	70 LIL2	80 TEYF	90 Y1B5	100 THG5



Empfehlung: Überblick E-Banking Verfahren unserer Kollegen vom IWI



Phishing, Vishing und SMiShing

?#&#>3!"#\$%&'()*+,-./012'34'35#)657#\$8!9:;<=:'25&:9#&5,7#\$
!'&@3;2&,<%)?@AB#C\$5<\$)?@D?EFGHFIJ'3K#=#
A=\$312'34'35#)657#\$8

J#3\$)%##3\$,#)12'34'35#)657#\$8)L2&2-83<C#\$8

1M8!Mf9=,#)%#C#&J#)#\$#)*''25&:N&Q\$'<,-2&#&)<5QP#4#);<=>85\$
C=4)Q&R#\$4=(<'25&4#',-2&S+R#A2"T

U#4)=4,#)-8#)N<'3\$±3,)<54)P#");#44<%#)V#&,#\$)Q\$)V2" "5&±<,-2&)<8)<
5&4#)\$#)12'34'35#)657#\$8)L2&2-83<C#\$A

8-)\$<\$C#=#&)P#\$7#=#&)5&4#)\$#)U<,#&C<&V#);<=>
/V:L2&2)K#\$P#&J#)#&4'3#&)<+&#)5&C#&5,7,#)12'34'35#)657#\$8)*&
" #3\$)Z<5")Q\$)8#5#)54#)\$4(2)R#\$3-8P#\$8>P<44)N&S)L2&2)&±3,)#&#&4'3,)K
<54)5&4#)\$#)U<,#&C<&V#)#42+;#&4±3)N&S#)12'34'35#)657#\$8)C#4,[,-&#&
L2&2)42Q\$A

J#&P#&JN&S#)*''25&:N&Q\$'<,-2&#&)=4,)5&,#\$F
62%&)&6-8V#)A
!;;<=>*P\$#44#F)A
9#&5,7#\$8<"#F)A
\\<44K2\$F)A
L#&8K2\$)C#4,[,-&#&F)A

Von: "CREDIT SUISSE GROUP AG" <aktualisieren@credit-suisse.com>
Betreff: m-Tan Sicherheit und Datenschutz!
Datum: 6. Mai 2013 19:45:46 MESZ
An: Recipients <aktualisieren@credit-suisse.com>



SMS-Sicherheitsverfahren

Sehr geehrter Kunde,

Wir glauben, dass die Sicherheit und die Benutzerfreundlichkeit oberste Priorität sind, wenn wir Ihre Bankgeschäfte ausführen. Das ist, warum wir die neuesten SMS Sicherheitsverfahren für unsere Online- & Mobile-Banking-Transaktionen verwenden. Wir weisen darauf hin, Sie zu Ihrem E-Banking Details zu überprüfen, Sie auf der neuen SMS-Code (mTAN Plus) zu aktualisieren.

Um Ihre Angaben zu überprüfen [Klicken Sie hier](#)

Copyright © 1997 - 2013 CREDIT SUISSE GROUP AG and/or its affiliates. All rights reserved.

Danke für Ihre Aufmerksamkeit

