

Die Snowden-Affäre: Welche Daten kann die NSA
lesen und was kann sie damit machen?
auch ohne Hilfe von Google, Facebook und Supercomputern!

Phillip Alday

25. November 2013

lange Rede, kurzer Sinn

Alles.

lange Rede, kurzer Sinn

Fast Alles.

lange Rede, kurzer Sinn

Leider ist das kein Witz.

Fast Alles.

Post und elektronische Post

Stimmt die Metapher?

Wie sieht Datenschutz bei Email aus?

Post und elektronische Post

Widersprüchlich: Dummheit, Arroganz oder Scheinheiligkeit?

*The information in this email is confidential and is intended solely for the addressee. If you have received it by mistake please notify the sender and delete it immediately. Any disclosure, copying, distribution or use of it is prohibited. Emails are not secure and cannot be guaranteed to be error free as they can be intercepted, amended, lost or destroyed, or contain viruses. Anyone who communicates with ***** by email is taken to accept these risks.*

Quelle: <https://groups.google.com/a/zfsonlinux.org/forum/#!topic/zfs-discuss/at3Cb08d21A>

Post und elektronische Post

Wer hat die Verantwortung die eigenen Daten zu schützen?

Diese Mail könnte vertrauliche und/oder rechtlich geschützte Informationen enthalten. Diese Informationen sind ausschließlich für die bezeichnete/-n Person/-en oder Einrichtung/-en bestimmt. Sollten Sie nicht der für diese E-Mail bestimmte Adressat sein, ist Ihnen jede Veröffentlichung, Vervielfältigung oder Weitergabe untersagt. Haben Sie diese E-Mail irrtümlich erhalten, bitte ich Sie, mich darüber in Kenntnis zu setzen, die E-Mail zurückzusenden und Ihr Exemplar zu vernichten.

Quelle: Verwaltung der Uni-Marburg

Post und elektronische Post

Wissen ist Macht

1. *I am, by definition, the intended recipient.*
2. *All information in the email is mine to do with as I see fit and make such financial profit, political mileage, or good joke as it lends itself to. In particular, I may quote it where I please, provided by copyright law.*
3. *I may take the contents as representing the views of your company if you are using a corporate mail account.*
4. *This disclaimer overrides any disclaimer or statement of confidentiality that may be included in future messages. By sending me email, you agree to these risks.*
5. *For a truly confidential message, please encrypt it.*

Quelle: <https://groups.google.com/a/zfsonlinux.org/forum/#!topic/zfs-discuss/at3Cb08d21A>

Post und elektronische Post

Wissen ist Macht

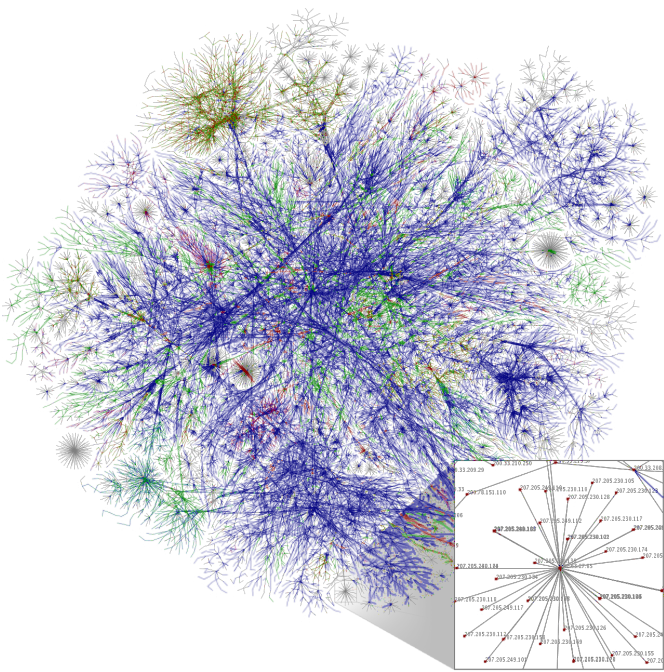
1. *I am, by definition, the intended recipient.*
2. *All information in the email is mine to do with as I see fit and make such financial profit, political mileage, or good joke as it lends itself to. In particular, I may quote it where I please, provided by copyright law.*
3. *I may take the contents as representing the views of your company if you are using a corporate mail account.*
4. *This disclaimer overrides any disclaimer or statement of confidentiality that may be included in future messages. By sending me email, you agree to these risks.*
5. *For a truly confidential message, please encrypt it.*

Quelle: <https://groups.google.com/a/zfsonlinux.org/forum/#!topic/zfs-discuss/at3Cb08d21A>

Trusting Trust and Passing Notes

this is why we can't have nice things

- ▶ Die meisten Internet-Dienste (Webseiten, Dropbox, IMAP, usw.) werden mittels TCP/IP übertragen.
- ▶ Das Routen wird nicht gewährleistet und geht auf einen verteilten Algorithmus zurück.
- ▶ Email wird als Plaintext – meistens als 7-bit ASCII durch MIME-Enkodierung – übertragen.
- ▶ Jeder Rechner auf dem Route kann die Nachricht anschauen!
- ▶ Wenn Email Post ist, dann ist sie eine Postkarte und kein Brief mit Umschlag.



Packet Sniffing

and Promiscuity

- ▶ Meistens achtet ein Rechner nur auf Nachrichten, die an ihn gesendet wurden.
- ▶ In *Promiscuous* Mode liest die Netzwerkkarte jedes Paket aus Medium ein.
- ▶ Bei LAN wird der Verkehr durch Switching reduziert, Zugang zum Kabel auch ein weiteres Hindernis.
- ▶ Bei nicht bzw. schlecht verschlüsseltem WLAN heißt das: jedes Paket von allen anderen Rechnern.

Packet Sniffing

Hört mir endlich jemand zu?

The screenshot shows a Wireshark interface with a filter set to `tcp.port==5190 and !(ip.addr==10.48.29.90)`. The packet list pane shows several packets, with packet 61 highlighted. The packet details pane shows the following structure:

- Ethernet II, Src: Cisco_76:a4:00 (00:07:0d:76:a4:00), Dst: GemtekTe_00:ab:7b (00:14:a5:00:ab:7b)
- Internet Protocol, Src: 64.12.25.104 (64.12.25.104), Dst: 10.48.36.120 (10.48.36.120)
- Transmission Control Protocol, Src Port: aol (5190), Dst Port: 3233 (3233), Seq: 9352, Ack: 500, Len: 154
- ADL Instant Messenger
 - AIM Messaging, Incoming
 - ICBM Cookie: 3535333136323300
 - Message Channel ID: 0x0001

The packet bytes pane shows the raw data of the message. Two yellow circles highlight specific parts of the data:

- The first circle highlights the text `..RISSMIS S609..`, with an arrow pointing to it and the label "Screen name of person sending message".
- The second circle highlights the text `..i know..`, with an arrow pointing to it and the label "Instant message text".

At the bottom of the window, the taskbar shows an open window for "AIMroommate - Wire..." and another for "Microsoft Word - CO...".

Quelle: Pitterle und Alday (2008), „Network Security for College Students: Perception vs. Reality“

HTTPS

sollte HTTP komplett ersetzen!

- ▶ HTTPS
 - ▶ verschlüsselte Erweiterung von HTTP
 - ▶ benötigt Drei-Wege-Handschlag
 - ▶ etwas aufwändiger als normales HTTP
- ▶ Cookies und Sessions
 - ▶ verfolgt Präferenzen und Anmeldungen
 - ▶ oft nicht visuell lesbar und besteht aus einem Hash
 - ▶ leicht zugänglich!

Sidejacking

i haz ur login

- ▶ Viele Webseiten nutzen HTTPS nur fürs Einloggen und danach eine eindeutige Session-ID.
- ▶ Mit Packetsniffing kann man die ganze Sitzung anschauen – herkömmlich MITM-Angriff.
- ▶ Mit Packetsniffing kann man auch die Session-ID fangen und damit die Sitzung für sich übernehmen.
- ▶ Mit WLAN wird das nur schlimmer!

Sidejacking

i haz ur login

- ▶ Viele Webseiten nutzen HTTPS nur fürs Einloggen und danach eine eindeutige Session-ID.
- ▶ Mit Packetsniffing kann man die ganze Sitzung anschauen – herkömmlich MITM-Angriff.
- ▶ Mit Packetsniffing kann man auch die Session-ID fangen und damit die Sitzung für sich übernehmen.
- ▶ Mit WLAN wird das nur schlimmer!

Sidejacking

i haz ur login

- ▶ Viele Webseiten nutzen HTTPS nur fürs Einloggen und danach eine eindeutige Session-ID.
- ▶ Mit Packetsniffing kann man die ganze Sitzung anschauen – herkömmlich MITM-Angriff.
- ▶ Mit Packetsniffing kann man auch die Session-ID fangen und damit die Sitzung für sich übernehmen.
- ▶ Mit WLAN wird das nur schlimmer!

Sidejacking

i haz ur login

- ▶ Viele Webseiten nutzen HTTPS nur fürs Einloggen und danach eine eindeutige Session-ID.
- ▶ Mit Packetsniffing kann man die ganze Sitzung anschauen – herkömmlich MITM-Angriff.
- ▶ Mit Packetsniffing kann man auch die Session-ID fangen und damit die Sitzung für sich übernehmen.
- ▶ Mit WLAN wird das nur schlimmer!

Sidejacking

buckle up!

- ▶ Wie leicht ist es?
 - ▶ auch die Experte betroffen: BlackHat 2007
 - ▶ ferret und hamster
 - ▶ FireSheep
- ▶ Was können wir dagegen?
 - ▶ SSL/HTTPS
 - ▶ Firefox: <https://support.mozilla.org/en-US/kb/how-do-i-tell-if-my-connection-is-secure>
 - ▶ Chrome <http://chrome.blogspot.de/2010/10/understanding-omnibox-for-better.html>
 - ▶ HTTPSEverywhere – für Chrome und Firefox als Extension verfügbar!
 - ▶ Ausloggen!

Das HRZ ist hier echt kompetent – die wichtigsten Uni-Marburg-Dienste laufen über HTTPS und sind für diesen Angriff nicht anfällig!

Sidejacking

buckle up!

- ▶ Wie leicht ist es?
 - ▶ auch die Experte betroffen: BlackHat 2007
 - ▶ ferret und hamster
 - ▶ FireSheep
- ▶ Was können wir dagegen?
 - ▶ SSL/HTTPS
 - ▶ Firefox: <https://support.mozilla.org/en-US/kb/how-do-i-tell-if-my-connection-is-secure>
 - ▶ Chrome <http://chrome.blogspot.de/2010/10/understanding-omnibox-for-better.html>
 - ▶ HTTPSEverywhere – für Chrome und Firefox als Extension verfügbar!
 - ▶ Ausloggen!

Das HRZ ist hier echt kompetent – die wichtigsten Uni-Marburg-Dienste laufen über HTTPS und sind für diesen Angriff nicht anfällig!

Übrigens

Die NSA hat einen eigenen Raum bei AT&T (der amerikanischen Telekom), damit sie direkten Zugang zum Kern der amerikanischen Netzwerkinfrastruktur haben.

Quelle: https://en.wikipedia.org/wiki/Room_641A

Übrigens

Die NSA hat einen eigenen Raum bei AT&T (der amerikanischen Telekom), damit sie direkten Zugang zum Kern der amerikanischen Netzwerkinfrastruktur haben.

Quelle: https://en.wikipedia.org/wiki/Room_641A



**Ceiling Cat is stealing your information
and watching you masturbate.**



Passwörter

Sharing is **not** caring.

- ▶ Social Engineering
- ▶ Kevin Mitnick – der berühmteste „Hacker“¹ aller Zeit – konnte vergleichsweise wenig mit der Technik anfangen.
- ▶ Snowden hat es auch genutzt, um Zugang zu weiteren Daten zu bekommen.
- ▶ moderne Variante: Phishing
- ▶ Preisgegebene Passwörter sind ein großes Problem für die Uni-Marburg.

Quelle: (Snowden): <http://mobile.reuters.com/article/idUSBRE9A703020131108?irpc=932>


¹eigentlich *Cracker!*

Facebook

Social Engineer's Wet Dream

Keep me logged in [Forgot your password?](#)

Targeted Advert Database



Sign Up

It's free and anyone can join

First Name:

Last Name:

Your Email:

New Password:


I am:

Birthday:

Why do I need to provide this?

[English \(US\)](#) [Español](#) [Português \(Brasil\)](#) [Français \(France\)](#) [Deutsch](#) [Italiano](#) [العربية](#) [한국어](#) [中文\(简体\)](#) [日本語](#) [»](#)

Facebook © 2010 English (US) [About](#) [Advertising](#) [Developers](#) [Careers](#) [Terms](#) [Find Friends](#) [Privacy](#) [Mobile](#) [Help](#) [Get](#)



Quelle: <http://cracked.com>

Facebook

nice to be naughty

- ▶ präziseres Phishing (Spear Phishing)
- ▶ blöde Passwörter (Geburtsdatum, Lieblings-x, usw.) direkt ablesbar

Sicherheit und Authentifizierung

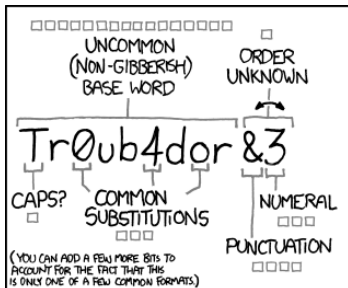
- ▶ something you are
- ▶ something you have
- ▶ something you know

Wie viele davon nutzt Ihre Bank?

Sicherheit und Authentifizierung

- ▶ something you are
- ▶ something you have
- ▶ something you know

Wie viele davon nutzt Ihre Bank?



~28 BITS OF ENTROPY

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

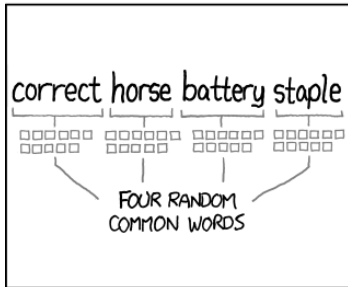
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE: YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: **EASY**

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE O's WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER: **HARD**



~44 BITS OF ENTROPY

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS: **HARD**

THAT'S A BATTERY STAPLE.

CORRECT!

DIFFICULTY TO REMEMBER: **YOU'VE ALREADY MEMORIZED IT**

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Passwortstärke

Everything you know is wrong.

Ein gutes Passwort:

- ▶ ist leicht zu merken.
- ▶ darf Wörter aus dem Wörterbuch enthalten.
- ▶ sollte beliebig lang sein dürfen.
- ▶ sollte beliebige Zeichen (inkl. Leerschlag!) enthalten dürfen.
- ▶ sollte nie im Klartext gespeichert werden.

Überraschung

Überraschung

Die Welt ist voller Idioten.

Überraschung

aber keine große

Die Welt ist voller Idioten.

Passwortwiederverwendung: die größte Gefahr

by far! (lautsagen!)

- ▶ Passwörter sollten mit einer passenden Hashfunktion und Salt gespeichert werden.
- ▶ Sonst ist es ziemlich leicht, durch Brute-Force und Rainbow-Tables, Passwörter zu cracken, wenn die Passwortliste geklaut wird.
- ▶ Wegen Passwortwiederverwendung hat der Cracker Zugang auf alle Konten!
- ▶ Vorschlag: Wichtige Konten (Banken, usw.) bekommen einmalige Passwörter, nur unwichtige teilen ein Passwort.

Siehe auch: <http://bit.ly/17jnyBn> <http://xkcd.com/792/> <http://bit.ly/U0xLC1> <http://wrld.cm/RefPyI>

Banken in Deutschland

das hat mich von Anfang an wahnsinnig gemacht!

Wird ein schlechtes Passwort durch eine TAN-Liste sicher gemacht?

Funktioniert die Anmeldung auf der Webseite gleich wie die „Anmeldung“ beim Geldautomaten?

Banken in Deutschland

das hat mich von Anfang an wahnsinnig gemacht!

Wird ein schlechtes Passwort durch eine TAN-Liste sicher gemacht?

Funktioniert die Anmeldung auf der Webseite gleich wie die
„Anmeldung“ beim Geldautomaten?

Ein erster Versuch

ebg13

Jr purevfur gur Qrpynengvba orpnhfr vg rkcerffrf, va gur gvzryrff
cebfr bs vgf nhgube, Senapvf "Fpbgg" Xrl, gur vqrnyf hc ba juvpu
guvf terng angvba jnf sbhaqrq: 'Jurernf va gur pbhefr bs uhzna
riragf vg orubbirf hf, gur crbcyr, abg gb nfx, Jung pna bhe pbhagel
qb sbe hf, naljnl? ohg engure, jurgure jr unir nalguvat gb srne
rkprcg srne vgfrys, fb gung n tbirezrag bs gur crbcyr, ol gur
crbcyr, naq sbe gur crbcyr, znl or bar angvba, haqre Tbq, jub neg
va urnira, nf jr sbetvir gubfr jub gerfcnff ntnvafg hf naq fbyrzayl
fjrne gb gryy gur gehgu, gur jubyr gehgu, naq abguvat ohg gur
gehgu hagvy qrngu qb hf cneg nf ybat nf jr obgu funyy yvir be
75,000 zvyrf, juvपुरire pbzrf svefg, nzra.

Quelle: *Dave Barry Hits Below the Beltway* (Dave Barry, 2001)

Ersatzverfahren

rot13

We cherish the Declaration because it expresses, in the timeless prose of its author, Francis "Scott" Key, the ideals up on which this great nation was founded: 'Whereas in the course of human events it behooves us, the people, not to ask, What can our country do for us, anyway? but rather, whether we have anything to fear except fear itself, so that a government of the people, by the people, and for the people, may be one nation, under God, who art in heaven, as we forgive those who trespass against us and solemnly swear to tell the truth, the whole truth, and nothing but the truth until death do us part as long as we both shall live or 75,000 miles, whichever comes first, amen.

Quelle: *Dave Barry Hits Below the Beltway* (Dave Barry, 2001)

Kryptographische Verfahren

ein Reading-Week Vortrag an und für sich

- ▶ Output sollte nicht unterscheidbar von Zufälligkeit sein.
- ▶ Big Data und Statistik können auch gegen Verschlüsselung genutzt werden.
- ▶ Gute Trapdoor (Hash) Funktionen und Pseudo-Random-Number-Generatoren sehr wichtig
- ▶ Symmetrisch vs. Assymetrisch

$$? \times ? = 3441$$

$$111 \times 31 = ?$$

Die Macht der Kryptografie

the stars will die before I give up my data.

- ▶ **Public-Key-Verfahren und Signieren**
- ▶ End-to-End Verschlüsselung: Verschlüsselung von Daten bei der Übertragung und beim Speichern (z.B. PGP)
- ▶ Starke Kryptographie wurde als „Waffe“ verstanden und den Export davon verboten!

Die Macht der Kryptografie

the stars will die before I give up my data.

- ▶ Public-Key-Verfahren und Signieren
- ▶ End-to-End Verschlüsselung: Verschlüsselung von Daten bei der Übertragung und beim Speichern (z.B. PGP)
- ▶ Starke Kryptographie wurde als „Waffe“ verstanden und den Export davon verboten!

Die Macht der Kryptografie

the stars will die before I give up my data.

- ▶ Public-Key-Verfahren und Signieren
- ▶ End-to-End Verschlüsselung: Verschlüsselung von Daten bei der Übertragung und beim Speichern (z.B. PGP)
- ▶ Starke Kryptographie wurde als „Waffe“ verstanden und den Export davon verboten!

NSA vs. Kryptografie

Nicht ob, sondern wann.

- ▶ Massive Rechnerleistung
- ▶ Versuche, schwache Verfahren als Standard einzuführen
- ▶ Backdoors in Hardware und Software (Clipper Chip)
- ▶ TLS (Sicherheitsebene in HTTPS) kaputt(er)?
- ▶ Side-Channel Attacks
- ▶ Geheime Zwangsmaßnahme, um Daten, die unverschlüsselt auf einem Cloud-Server liegen zu bekommen

Quelle: <http://blog.cryptographyengineering.com/2013/09/the-many-flaws-of-dualecdrbg.html>

**A CRYPTO NERD'S
IMAGINATION:**

HIS LAPTOP'S ENCRYPTED.
LET'S BUILD A MILLION-DOLLAR
CLUSTER TO CRACK IT.

NO GOOD! IT'S
4096-BIT RSA!

BLAST! OUR
EVIL PLAN
IS FOILED!

**WHAT WOULD
ACTUALLY HAPPEN:**

HIS LAPTOP'S ENCRYPTED.
DRUG HIM AND HIT HIM WITH
THIS \$5 WRENCH UNTIL
HE TELLS US THE PASSWORD.

GOT IT.



If knowledge is power, then
know that this is tyranny!

Quelle: „Hoods on Peregrine“ von Thrice

Ein echtes Beispiel

weshalb ich an Treue-Programmen wie Payback, usw. nicht teilnehme

- ▶ amerikansicher Händler Target entdeckte, dass sie Schwangerschaften durch Einkäufe „finden“ können:
identify about 25 products that, when analyzed together, allowed him to assign each shopper a „pregnancy prediction“ score . . . [and] estimate her due date to within a small window
- ▶ Mit Daten statt Geld bezahlen.
- ▶ Mit genügend Daten geht alles.

Quelle: <http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html>

Ein echtes Beispiel

weshalb ich an Treue-Programmen wie Payback, usw. nicht teilnehme

- ▶ amerikansicher Händler Target entdeckte, dass sie Schwangerschaften durch Einkäufe „finden“ können:
identify about 25 products that, when analyzed together, allowed him to assign each shopper a „pregnancy prediction“ score . . . [and] estimate her due date to within a small window
- ▶ Mit Daten statt Geld bezahlen.
- ▶ Mit genügend Daten geht alles.

Quelle: <http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html>

Facebook

at least he's honest :-)

Zuckerberg: yeah so if you ever need info about anyone at harvard

Zuckerberg: just ask

Zuckerberg: i have over 4000 emails, pictures, addresses, sns

Redacted Friend's Name: what? how'd you manage that one?

Zuckerberg: people just submitted it

Zuckerberg: i don't know why

Zuckerberg: they "trust me"

Zuckerberg: dumb fucks.

Quelle: http://www.newyorker.com/reporting/2010/09/20/100920fa_fact_vargas

Dropbox

Sharing Your Data With the World

- ▶ Zero-Knowledge-Alternative mit Clientside Verschlüsselung:
SpiderOak

Den Nachbarn wecken

bevor er den Tisch vollsabbert

Fragen?