

Grundlagen des Internets und Sicherheit im Web

Das Böse im Netz und was man dagegen tun kann

Georg A. Murzik, Marcus Schilling

Terminal.21

05. November 2016



TERMINAL.21

Grundlagen des Internets

Das wichtigste zuerst

- Das Internet ist keine Wolke!
- Alles wird von Computern gesteuert.
- Jeder Computer gehört jemandem.
- Jeder verfolgt eigene Interessen.
- Es sind stets wesentlich mehr Personen beteiligt, als es scheint.
- Daten, die sichtbar sind, werden gelesen.



TERMINAL.21

Woraus besteht das Web?

- 1 Webdienste
- 2 DNS
- 3 Provider
- 4 Clients / Hosts



Webdienste

- Bekannteste Dienste sind Webseiten
- Cloudspeicher, Handyapps, Navigation, Streaminganbieter sind ebenfalls Webdienste
- Webdienste sind über IP-Adressen zu erreichen
- IP-Adressen kann sich aber keiner merken, deswegen werden normalerweise URLs verwendet.



TERMINAL.21

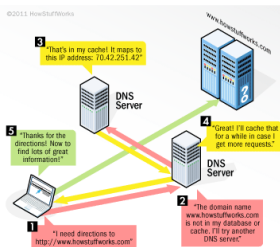
Webclients

- Schnittstelle zwischen Nutzer und Internet
- Bekannteste Clients sind Webbrowser
- Clients stellen Daten von Webservern übersichtlich dar und bieten Interaktionsmöglichkeiten mit dem Server



DNS

- DNS (Domain Name Service) dient als eine Art Telefonbuch des Internets
- Wandelt Domains in URLs in IP-Adressen um
- Jeder Computer, der mit dem Internet kommunizieren möchte, muss mindestens einen DNS kennen.





◀ ◻ ▶ ◀ ◻ ▶ ◀ ≡ ▶ ◀ ≡ ▶ ≡

Gefahren im Netz

Mangelnde Sicherheitsstandards - Infrastruktur

Die Protokolle und die Infrastruktur des Internets sind sehr alt!

- Ursprüngliche Protokolle sahen kaum Bedarf für Internetsicherheit
- Daher keine Authentifizierungs- oder Verschlüsselungsmechanismen
- Heutige Sicherheitstechniken wurden nachträglich implementiert und sitzen eher „oben auf“.

Entwicklung des WWW

Das Web wurde ursprünglich für Forscher entwickelt, die ihre Studienergebnisse untereinander austauschen wollten. Erst durch die allmähliche Verbreitung über den Globus erkannte man, dass gewisse Sicherheitsstandards eingehalten werden mussten.



Mangelnde Sicherheitsstandards - Software

Nicht nur die Infrastruktur weist Lücken auf. Selbst aktuellste Software wird teilweise stümperhaft programmiert.

- Schlechte Programmierung ist kaum mit mangelnden Standards zu erklären.
- Software soll immer schneller mit weniger Aufwand produziert werden.
- Software wird immer komplexer.
- Politik hat sich gewandelt. Software ist nun eher ein Service als ein Produkt.



TERMINAL.21

Übersicht der Gefahren im Netz

Was wollen Angreifer?

Unabhängig von der Art der Schwachstelle ist die Hauptgefahr fast immer dieselbe: Dass Daten in die falschen Hände geraten. Solche Daten könnten z.B. Bank-, Login-, oder Adressdaten sowie allgemeine persönliche Daten sein. Ein anderes Ziel ist die Nutzung der Infrastruktur bspw. für Botnetze.

Es gibt viele Wege, wie man als Angreifer an solche Informationen gelangen kann:

- 1 Phishing
- 2 Ausnutzen von Schwachstellen
- 3 Tracking



TERMINAL.21

Was ist Phishing?

Phishing ist der Versuch, Daten zu stehlen, indem sich ein Angreifer das Vertrauen des Opfers erschleicht, indem er sich für eine vertrauenswürdige Kontaktperson ausgibt.

- gefälschte E-Mails
- gefälschte Webseiten
- gefälschte Nachrichten

Ziele sind die eben genannten Daten der Opfer.



TERMINAL.21

Live-Demo

- Phishing-Angriffe sind recht einfach
- Einfache Angriffe funktionieren vor allem bei Massenangriffen gut
- Gezielte Attacken setzen viel Vorwissen über das Opfer voraus

Beispiel: Studentenfischen

Ich zeige nun, wie wir uns Zugriff auf Studentenlogins verschaffen könnten.



TERMINAL.21

Abwehr von Phishing-Attacken

Entwarnung(?)

Phishing-Seiten unterscheiden sich von realen Seiten!

Vor allem wegen der kurzen Zeit unterscheidet sich die falsche Seite von der realen in folgenden Punkten:

- 1 URL
- 2 Verschlüsselung / Zertifikat
- 3 Verhalten



TERMINAL.21

Abwehr von Phishing-Attacken II

Was man tun kann:

- 1 Misstrauisch sein & Nachdenken!
- 2 Links mit dem Mouse-Hover-Test prüfen, bevor man sie anklickt.
- 3 URL prüfen.
- 4 Im Falle von E-Mails den vermeintlichen Sender selbst noch einmal kontaktieren (nicht über angebotene Links!).



TERMINAL.21

Deutlich schwieriger abzuwehren sind solche Angriffe, die *Schwachstellen* der Internetseite selbst, des Browsers oder sonstige Programme des Computers ausnutzen.



TERMINAL.21

Was sind „Schwachstellen“!?

Schwachstellen sind nichts anderes als Programmierfehler, oder auch Anwendungsfälle, die der oder die Programmierer nicht bedacht haben.

- Programme prüfen Eingaben nicht (Code-Injection, XSS)
- Programme können zum Absturz gebracht werden (Buffer Overflow)
- Programme überprüfen Dateien nicht (Macro-viren)
- Programme vertrauen ihren eigenen Protokollen zu sehr (Code Injection)
- Programme vertrauen einem bestimmten Webserver zu sehr (Code Injection)



TERMINAL 21

Was kann passieren?

- größtenteils Code Injection
- Privilegien des Programmes werden genutzt, um Code auf dem Computer selbst auszuführen
- Schaden abhängig von der Integration des Programmes in das Betriebssystem und seiner Berechtigungen
- Schlimmstenfalls installieren von permanenten Schadprogrammen



TERMINAL

Schwachstellen im Browser

Webbrowser

Browser setzen vorrangig auf Kommunikation mit dem Internet. Sie öffnen Dateien aus dem Internet und können kleine Programme (wie Javascript) aus dem Internet direkt ausführen.

→ **Klingt nach der vollen Drönung!**

Gerade Browser besitzen daher viele Angriffsflächen für Schadcode.



TERMINAL.21

Angriffsflächen von Browsern

AddOns

- Erweiterungen der Funktionsfähigkeit des Browsers
- Individualisierung und Personalisierung des Browsers
- zeigen Emojis, Blockieren Werbung oder leiten den gesamten Datenverkehr über Proxys

!!!

Präparierte Webseiten könnten externen Code in verwundbaren Addons ausführen.

Hinweis: Webseiten können sehen, welche Addons verwendet werden - sogar die, die eigentlich deaktiviert sind.



Angriffsflächen von Browsern II

Plugins

- ähnlich wie Addons
- dienen der Darstellung bestimmter Seiteninhalte
- häufig proprietär, von anderer Software auf dem Computer installiert
- bekanntestes Plugin: FlashPlayer von Adobe

Noch ein Tip:

Webseiten können auch alle Plugins sehen, die verwendet werden und darauf entsprechend reagieren.



TERMINAL.21

- „Privacy protects us from abuses by those in power, even if we're doing nothing wrong at the time of surveillance.“
– *Bruce Schneier*
- Welche Daten werden für welchen Verwendungszweck wo erhoben, wie verarbeitet und an wen weitergegeben?
- Tradeoff: Privatsphäre vs. Useability

Spielregeln

- personenbezogenen Daten
- Verwendung
- notwendigen und freiwilligen Angaben
- Aufklärung über etwaige Nachteile
- Einwilligung



Rechte

- Informationelle Selbstbestimmung
- Recht auf Auskunft
- Recht auf Berichtigung
- Recht auf Löschung



Praxis: Internet

- viele Länder, viele Gesetze
- personenbezogene Daten?
- viele Daten -> Zuordnung



Tracking beim Verbindungsaufbau I

- DNS-Anfragen
- IP-Adressen Routing
- Laden von externen Seiteninhalten
 - Web-beacons
 - Social-media-like-buttons



Tracking beim Verbindungsaufbau II

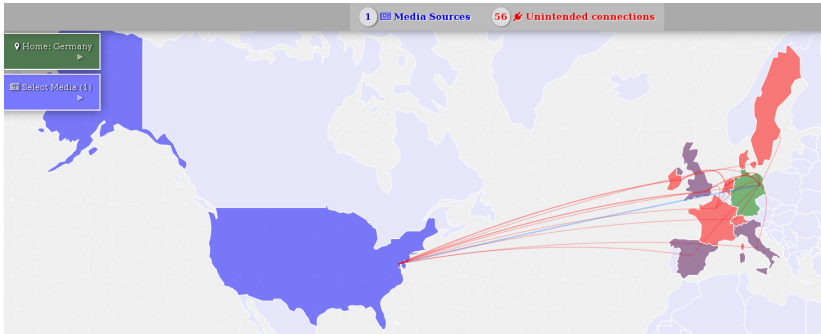


Abbildung: Verbindungen im Allgemeinen



TERMINAL.21

Tracking beim Verbindungsaufbau III

Du bist Terrorist

The image shows a YouTube video player interface. At the top, the video title is "Du bist Terrorist". Below it, the channel name "alexander lehmann channel" is displayed with "36 videos". To the left of the channel name is a small profile picture of a red and white soccer ball. To the right of the channel name is a "Subscribe" button with "14,322" subscribers. On the far right, the video has "3,099,825" views, with "26,699" likes and "1,542" dislikes. Below the video player, there are buttons for "Like", "Dislike", "About", "Share", "Add to", "Watch later", "Queue", and "Flag". At the bottom, there are links for "Share this video", "Embed", and "Email". Below these links is a row of social media sharing icons: Facebook, Twitter, Google+, Reddit, Blogger, Tumblr, VK, Dribbble, DeviantArt, Pinterest, StumbleUpon, LinkedIn, and Print.

Abbildung: Social-media-like-buttons

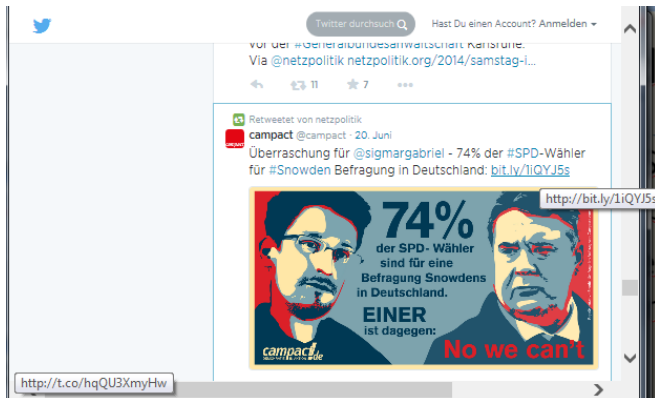
Tracking durch verräterischen Browser I

- Geodaten
- URLs
- Cookies in verschiedenen Geschmacksrichtungen
- Browserfingerprinting: Betriebssystem, Browsersoftware, Auflösung, JavaScript / Flash, Plugins, Addons, installierte Schriften, Sprache, Cookies ...



TERMINAL.21

Tracking durch verräterischen Browser II



TERMINAL 21

Tracking durch verräterischen Browser II

DATA GATHERED SINCE	YOU HAVE VISITED	YOU HAVE CONNECTED WITH
APR 24, 2015	3 SITES	87 THIRD PARTY SITES



Tracking durch verräterischen Browser IV





Panopticlick

How Unique — and Trackable — Is Your Browser?

Within our dataset of several million visitors, only **one in 348 browsers** have the same fingerprint as yours.

Currently, we estimate that your browser has a fingerprint that conveys **8.44 bits of identifying information**.

The measurements we used to obtain this result are listed below. You can read more about our methodology, statistical results, and some defenses against fingerprinting in [this article](#).

Help us increase our sample size:     

Browser Characteristic	bits of identifying information	one in x browsers have this value	value
User Agent	6.31	79.56	Mozilla/5.0 (Windows NT 6.1; rv:31.0) Gecko/20100101 Firefox/31.0
HTTP_ACCEPT Headers	5.01	32.24	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 gzip, deflate en-us,en;q=0.5
Browser Plugin Details	1.82	3.53	no javascript
Time Zone	1.82	3.52	no javascript
Screen Size and Color Depth	1.82	3.52	no javascript
System Fonts	1.82	3.52	no javascript
Are Cookies Enabled?	0.43	1.34	Yes
Limited supercookie test	1.82	3.52	no javascript



TERMINAL.21

Counterstrike

Sicherheitsmaßnahmen

- Software aktuell halten
- URLs vor dem Klicken überprüfen
- JavaScript u. Flash im Ausnahmefall erlauben
- Nachladen von Schriften deaktivieren
- verschiedene Passwörter nutzen
- keine komischen Sachen runterladen und ausführen



TERMINAL.21

Datenschutzmaßnahmen

- Datensparsamkeit
 - weniger ist mehr
 - nicht überall registrieren
 - nicht eingeloggt bleiben
- Kostenlose Dienste hinterfragen
 - Suchmaschinen: <https://duckduckgo.com>
 - Email: <https://mailbox.org>, <https://poesto.de>
 - Cloud: verschlüsselt und oder selbst betreiben
- auf HTTPS achten
- Cookies verbieten, Ausnahmen erlauben
- Verlauf und Cache sitzungsweise löschen lassen
- JavaScript u. Flash deaktivieren
- Plugins deaktivieren



TERMINAL

Addons Firefox I

PrivaConf <https://addons.mozilla.org/de/firefox/addon/privaconf/>

Cookie-Controller <https://addons.mozilla.org/de/firefox/addon/cookie-controller/>

Canvasblocker <https://addons.mozilla.org/de/firefox/addon/canvasblocker/>

no-resource-uri-leak <https://addons.mozilla.org/de/firefox/addon/no-resource-uri-leak/>

No-Script <https://addons.mozilla.org/en-US/firefox/addon/noscript/>



TERMINAL.21

Addons Firefox II

https-everywhere

<https://www.eff.org/https-everywhere>

uBlockOrigin [https://addons.mozilla.org/en-US/
firefox/addon/ublock-origin/](https://addons.mozilla.org/en-US/firefox/addon/ublock-origin/)

UserAgentChanger ... Finger weg!



TERMINAL.21

Datenkraken

- Google: Alles, was du bei Google gemacht hast
- facebook: Was die so für Daten sammeln
- Apple: Datenschutzbestimmungen
- towerdata: Daten von anderen einkaufen



much knowledge – so interactive – wow

- Hasso-Plattner-Institut: **Browser-Sicherheits-Check**
- Ratgeber: **Surfen im öffentlichem WLAN**
- Ratgeber: **Privacy freundliche Software**
- Online-Nachrichten: **Visualisierung von Trackern**
- VDS: **Visualisierung von Metadaten**
- Browserfingerprinting **Browser-Check**
- Nachschlagewerk zum Tracking: **privacy Handbuch**
- <https://download.terminal21.de/workshops/swap2016/>



TERMINAL.21