

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



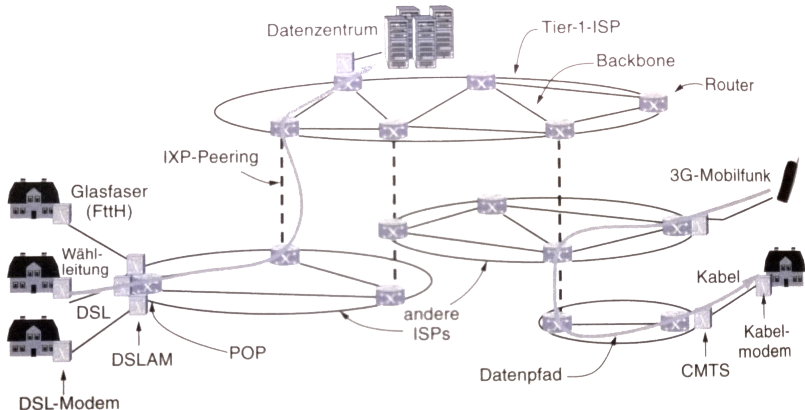
Das wichtigste zuerst

- 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

Wer hängt zwischen mir und der Webseite?



terminal.21

Woraus besteht das Web?

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



Webdienste

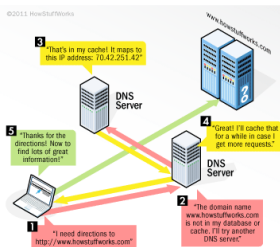
- Bekannteste Dienste sind Webseiten
- Cloudspeicher, Handyapps, Navigation, Streaminganbieter sind ebenfalls Webdienste
- Webdienste sind über IP-Adressen zu erreichen
- IP-Adressen kann sich aber keiner merken, deswegen werden normalerweise URLs verwendet.



TERMINAL.21

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.



Webclients

Webclients sind die Schnittstelle zwischen Nutzer und Internet. Bekannteste Clients sind Webbrowser. Sie fordern Daten von Webservern an und stellen die Antwortdaten für den Nutzer übersichtlich dar und bieten weitere Interaktionsmöglichkeiten mit Webdiensten.



Aufruf einer Webseite

Webseiten werden über die IP-Adresse des hostenden Servers angefordert. Um den Aufruf von Webseiten zu vereinfachen, werden stattdessen URLs verwendet (z.B. `https://www.privacy-handbuch.de/`). Diese können entweder direkt in das Adressenfeld des Browsers eingetragen oder über Links aufgerufen werden, die normalerweise in blauer Schrift und unterstrichen dargestellt werden.



TERMINAL

Aufruf einer Webseite II

Der Browser ruft zunächst einen DNS-Dienst auf. Dieser ist in der Konfiguration der Internetverbindung angegeben. Der Dienst kann die Anfrage an viele weitere DNS-Dienste weiterleiten, bis einer der Dienste die passende IP-Adresse zu dieser URL kennt. DNS-Dienste sind hierarchisch aufgebaut. So gibt es eigene DNS-Dienste für alle Adressen, die auf .de enden. Für die oben angegebene Adresse würde dann der Eintrag „privacy-handbuch.de“ gesucht.



TERMINAL.21

Aufruf einer Webseite III

Für die Adresse, die daraufhin zurückgegeben wird (in unserem Fall die IPv6-Adresse 2a01:238:20a:202:1078:0000:0000), könnte wieder ein DNS-Dienst verfügbar sein, unter dem die Subdomain `www.privacy-handbuch.de` abgefragt wird. Hier wird dann die IPv4-Adresse 81.169.145.78 geliefert. Ob hier Unterseiten eine andere IP-Adresse haben oder sogar verschiedene IP-Adressen für die gleichen Unterseiten existieren, kommt auf die Netzwerkstruktur des Webdienstes an. Für das oben genannte Beispiel gibt es nur die Subdomain `www.privacy-handbuch.de`, die auch unter `privacy-handbuch.de` erreichbar ist.



TERMINAL.21

Aufruf einer Webseite IV

Die Anfrage an einen Webserver enthält die angefragte Datei, z.B. <https://www.privacy-handbuch.de/index.htm> oder https://www.privacy-handbuch.de/handbuch_11.htm sowie die eigene IP-Adresse, zu der die Antwortdaten gesendet werden sollen. Die Antwort enthält Verweise auf alle benötigten Dateien, die zum Darstellen der Webseite erforderlich sind. Diese Dateien werden häufig erst kurz vorher durch den Server generiert, um die Webseite an den Benutzer anzupassen.



TERMINAL

Aufruf einer Webseite V

Der Webclient lädt alle erforderlichen Dateien herunter und bindet sie, wie in der index.htm-Datei beschrieben, auf der Webseite ein. Anschließend wird die handbuch.css-Datei ausgewertet, die erweiterte Informationen zur Darstellung der Webseite bereitstellt. Manchmal werden auch Skripte eingebunden, mit denen die Seite oft auch ohne erneute Anfrage an den Webserver mit dem Nutzer interagieren kann. Wurde alles geladen und ausgewertet, so wird die Webseite angezeigt.



TERMINAL.21

Gefahren im Netz

Das Internet wurde ursprünglich unter der Prämisse gebaut, dass nur wenige Menschen in der Lage sein werden, es zu nutzen. Die ursprüngliche Zielgruppe bestand hauptsächlich aus Forschern, die ihre Studien mit anderen Universitäten oder auch innerhalb einer Universität austauschen wollen. Es wurde daher kaum auf eine sichere Infrastruktur wert gelegt und die Protokolle von heute entsprechen immer noch denen von damals. Sicherheitsstrukturen wurden erst nachträglich eingebaut und erinnern eher an Flicker.



TERMINAL.21

Zusätzlich zu der löchrigen Infrastruktur des Internets werden auch viele Webdienste im Internet stümperhaft programmiert. Diese Kombination führt zu allerlei Gefahren im Internet, denen man sich als normaler Nutzer oftmals nicht bewusst ist. Genau um diese Gefahren soll es nun gehen.



TERMINAL.21

Übersicht der Gefahren im Netz

Unabhängig von der Art der Schwachstelle ist die Hauptgefahr immer die selbe: Dass Daten in die falschen Hände geraten. Solche Daten könnten z.B. Bank-, Login-, oder Adressdaten sowie allgemeine persönliche Daten sein.

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

- 1 Phishing
- 2 Ausnutzen von Schwachstellen
- 3 Tracking



TERMINAL.21

Als Phishing bezeichnet man den Versuch, an persönliche Daten eines Opfers zu gelangen, indem man ihn auf gefälschte Webseiten leitet, ihm falsche E-Mails oder Kurznachrichten sendet. Opfer eines solchen Angriffes ist wahrscheinlich schon jeder einmal gewesen, der im Web unterwegs war. Angriffe reichen von sehr plumpen Versuchen wie „Sie sind der 1.000.000. Benutzer, holen sie sich hier ihren Gewinn ab.“ bis zu aufwändig gestalteten E-Mails, dass man mal eben online bei seiner Bank eine verdächtige Aktivität überprüfen soll, damit kein Geld verloren geht.



TERMINAL.21

Wie einfach es ist, einen solchen Angriff zu starten, möchte ich nun vorführen.

Abwehr von Phishing-Attacken

Die eben erstellte Webseite unterscheidet sich von der originalen Webseite in folgenden Eigenschaften:

URL In der Live-Demo hatte ich keine Zeit, eine richtige Domain für meine Webseite zu registrieren. Hätte ich diese gehabt, so hätte ich eine genommen, die der originalen zum Verwechseln ähnlich sieht, z.B. gooogle.de statt google.de. Die Domain ist teil der URL, die oben im Browser steht. Hier wäre es einfach zu durchschauen, dass die Seite nicht echt ist - schließlich steht hier nur eine einfache IP-Adresse.



TERMINAL.21

Abwehr von Phishing-Attacken II

TLS-Verschlüsselung In der Live-Demo hatte ich ebenfalls keine Zeit, mir ein Zertifikat für meinen Server zu besorgen. Dieses sorgt dafür, dass die Verbindung mittels TLS verschlüsselt und über die Zertifizierungsstelle autorisiert ist. Kurz gesagt, dass sichergestellt ist, dass die Webseite die ist, für die sie sich ausgibt und die Verbindung stets verschlüsselt und nicht durch andere manipulierbar ist. Dies erkennt man an dem Schlosssymbol und der grün hinterlegten URL des Browsers.



TERMINAL.21

Abwehr von Phishing-Attacken III

Möchte man sichergehen, dass das Zertifikat einer Webseite vertrauenswürdig ist, so muss man sich die URL und das Zertifikat selbst genau ansehen. Ein Klick auf das Schlosssymbol sollte dies in jedem Browser ermöglichen. Im Zertifikat muss der korrekte Name der Firma stehen, die die Seite betreibt und die URL muss genau die sein, die man erwartet. Fast jede große und bekannte Webseite stellt ihre Identitätsdaten im Zertifikat zur Verfügung.



TERMINAL.21

Abwehr von Phishing-Attacken IV

Verhalten Die Webseite verhält sich anders, als die normale. Gibt man beispielsweise seine Zugangsdaten ein, so wird man nicht eingeloggt, sondern landet wieder auf der (diesmal originalen) Login-Seite des Anbieters. Wenn man das bemerkt, ist es allerdings schon zu spät.



TERMINAL.21

Zusammenfassung

Grundsätzlich können Phishing-Attacken durch etwas Misstrauen im Netz leicht abgewehrt werden. Erwarte ich eine Mail von diesem Anbieter? Würde mir ein Anwalt so etwas wirklich per Mail schicken? Wäre wirklich jemand so großzügig, mir das neueste iPhone einfach so zu schenken? Ist dieser Test bestanden, so gibt es eine weitere Möglichkeit, Phishing zu verhindern: Bekomme ich eine sehr echt aussehende Mail von meiner Bank, so drücke ich auf gar keinen Fall irgendeinen Link darin. Stattdessen mache ich den Browser selbst auf und logge mich in der mir bekannten Webseite der Bank selbst ein. Idealerweise habe ich für solch wichtige Webseiten sowieso ein Lesezeichen gesetzt.



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, genauer gesagt, Anwendungsfälle, die der oder die Programmierer nicht bedacht haben.

Bekommen Programme andere Eingaben, als erwartet und können sie damit nicht korrekt umgehen, so stürzen sie meist ab oder versuchen, die Daten so einzulesen, wie sie es eigentlich nicht tun sollten. Handelt es sich bei einem erwarteten Nutzernamen auf einer Webseite plötzlich um Programmcode, so sollte der Server der Webseite diesen natürlich nicht ausführen. Viele machen das aber (Stichwort: *SQL Injection*).



TERMINAL.21

Was kann passieren?

Werden solche Lücken ausgenutzt, so bedeutet das, dass spezieller Code bspw. in präparierten Webseiten direkt durch den Browser oder gar das Betriebssystem selbst ausgeführt wird und bspw. einen Trojaner installiert. Gelangt dieser auf den Rechner des Nutzers, entstehen erheblich größere Gefahren (Ausspähen der Nutzeraktivität und Dateien auf dem Computer usw.).



TERMINAL.21

Einschub: Trojaner vs. Viren

Viren sind darauf angewiesen, vom Nutzer selbst heruntergeladen zu werden. Sie sind versteckt in vertrauenserweckenden Dateien verschiedener Tauschbörsen wie Videos, Bilder oder besonders kostengünstiger Spiele alternativer Downloadplattformen.

Sie können aber auch in Anhängen von Mails wie PDF- oder MS Office-Dateien lauern und sich dann beim Öffnen nebenher installieren, wenn sie denn eine Schwachstelle in Office oder dem PDF-Viewer ausnutzen können.



TERMINAL.21

Einschub: Trojaner vs. Viren II

Trojaner sind bösartige Programme, die sich in anderen Programmen verstecken und böses auf dem Computer anrichten. Sie können sich mit dem Internet verbinden, mit ihrem Erschaffer kommunizieren und Befehle ausführen oder einfach fleißig Daten vom Rechner klauen. Sie sind gerne versteckt in diversen Crackprogrammen und Keygeneratoren, nach denen viele sogar gezielt suchen.



TERMINAL.21

Schwachstellen im Browser

Browser setzen vorrangig auf Kommunikation mit dem Internet, das Öffnen von Dateien aus dem Internet und dem Ausführen kleiner Programme (Javascript) aus dem Internet.

Klingt nach der vollen Drönung.

Gerade Browser besitzen daher viele Angriffsflächen für Schadcode.

AddOns Addons sind Erweiterungen des Browsers, die Zugriff auf die Inhalte der Webseite bekommen, bevor der Nutzer sie zu sehen bekommt. Ihre Fähigkeiten reichen von der Integration zusätzlicher Emojis über das Blockieren von Werbung bis hin zum Umleiten der gesamten Kommunikation über Proxies.

Präparierte Webseiten könnten externen Code in



TERMINAL.21

Schwachstellen im Browser II

Potenzielle Angriffsflächen:

Plugins Plugins sind ähnlich wie Browser, werden jedoch häufig von anderer Software auf dem Computer installiert. Sie dienen zur Darstellung bestimmter Inhalte auf der Webseite. Das bekannteste und für seine vielen Schwachstellen berühmteste Plugin ist der Flash-Player 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: Keine Daten anfallen lassen. vs. Dienste bequem in Anspruch nehmen



TERMINAL.21

Spielregeln

- personenbezogenen Daten: Informationen, die mit einer Person verbunden werden
- Verwendung: Sammeln, verarbeiten, weitergeben
- Kenntlichmachung von notwendigen und freiwilligen Angaben
- Aufklärung über etwaige Nachteile, wenn man freiwillige Angaben nicht tätigt
- Einwilligung schriftlich oder digital
- neuer Verwendungszweck = neue Erlaubnis



TERMINAL.21

Rechte

- Informationelle Selbstbestimmung
- Recht auf Auskunft: Was wird gespeichert, wo kommt es her, wo geht es hin?
- Recht auf Berichtigung: Wenn was falsch ist.
- Recht auf Löschung: Wenn die Daten für den vereinbarten Zweck nicht mehr notwendig sind.



TERMINAL.21

Praxis

- viele Länder = viele Gesetze
- Es ist praktisch umstritten, welche Daten personenbezogen sind (z.B. Geräteerkennung vs. natürliche Person)
- wir hinterlassen beim Browsen viele Spuren, die nebenbei verarbeitet werden; durch viele Informationsquellen kann man auf die Person schließen



TERMINAL.21

Tracking beim Verbindungsaufbau I

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



Tracking beim Verbindungsaufbau II

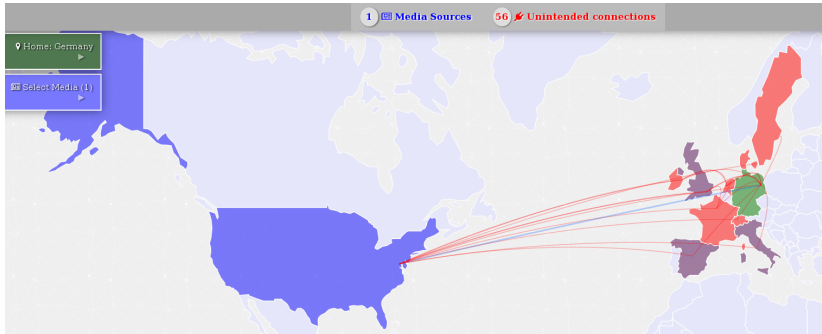


Abbildung: Verbindungen im Allgemeinen



TERMINAL.21

Tracking beim Verbindungsaufbau III

Du bist Terrorist



alexander lehmann channel · 36 videos

Subscribe

14,322

3,099,825

26,699 1,542



Like



About

Share

Add to



Share this video

Embed

Email



Abbildung: Social-media-like-buttons



TERMINAL 21

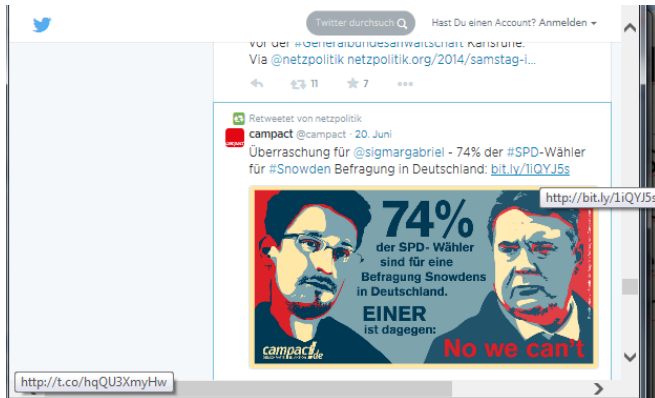
Tracking durch verräterischen Browser I

- 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

Todo-Platzhalter

- sicherheitsrelevante Ratschläge einbauen

Counterstrike

Verhalten im Netz

- Datensparsamkeit
 - Schein vs. Sein
 - Nicht überall registrieren, nicht eingeloggt bleiben
- Kostenlose Dienste hinterfragen
 - Suchmaschinen: Jede Suche ist mit einer Motivation verbunden, die Rückschlüssel zulässt.
<https://duckduckgo.com> ist gut.
 - Email: [web / gmx / aol / google / yahoo / hotmail ...] Sind doof, weil die Nachrichten mit kommerziellen Interessen durchsucht werden. Besser: [mailbox.org / poesto.de]
 - Cloud: Was ich nicht kontrollieren kann ist schon verloren. Würdet ihr wirklich gerne euren privaten Urlaubsfotos auf anderen Computern speichern, auf die mindestens irgendwelche Mitarbeiter zugriff haben? Und außerdem: Irgendwann werden alle gehackt. Wenn, dann die Daten sehr ordentlich verschlüsseln.



TERMINAL.21

Addons

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/>

UserAgentChanger Nicht benutzen!



TERMINAL.21