Sicher Surfen mit Firefox und freier Software

Jali
jali@orca-central.de

Chaos Computer Club Bremen
CCCHB

28. Juli 2009

Übersicht

Übersicht

Übersicht

Übersicht

Definition

- Ein Webserver bietet Informationen im Word Wide Web an

Definition

- Ein Webserver bietet Informationen im Word Wide Web an
- Ein Web-Browser ist ein Programm, dass Informationen (sog. Seiten) herunterlädt und anzeigt.

Definition

- Ein Webserver bietet Informationen im Word Wide Web an
- Ein Web-Browser ist ein Programm, dass Informationen (sog. Seiten) herunterlädt und anzeigt.
- Die „Sprache“ des Web ist das Hypertext Transport Protocol, kurz http

Definition

- Ein Webserver bietet Informationen im Word Wide Web an
- Ein Web-Browser ist ein Programm, dass Informationen (sog. Seiten) herunterlädt und anzeigt.
- Die „Sprache“ des Web ist das Hypertext Transport Protocol, kurz http
- Webserver und Browser erkennen einander an der IP-Adresse

Definition

- Ein Webserver bietet Informationen im Word Wide Web an
- Ein Web-Browser ist ein Programm, dass Informationen (sog. Seiten) herunterlädt und anzeigt.
- Die „Sprache“ des Web ist das Hypertext Transport Protocol, kurz http
- Webserver und Browser erkennen einander an der IP-Adresse
- Eine Webseite beseteht aus Dateien, die Anweisungen für den Browser enthalten. Die Sprache dafür ist die Hypertext Markup Language, oder html

Gefahren, die im Netz lauern

- Malware

Gefahren, die im Netz lauern

- Malware
- Cross-Site-Scripting, z.B auf Facebook, MySpace und Co.

Gefahren, die im Netz lauern

- Malware
- Cross-Site-Scripting, z.B auf Facebook, MySpace und Co.
- Phishing nach Passwörtern und Online Banking Pins

Gefahren, die im Netz lauern

- Malware
- Cross-Site-Scripting, z.B auf Facebook, MySpace und Co.
- Phishing nach Passwörtern und Online Banking Pins
- Datenkraken (Google, Doubleclick.net, etc.)

Bekannte Browser

- Microsoft Internet Explorer
- Mozilla Firefox
- Apple Safari
- Opera
- Konquerer

Warum Mozilla Firefox?

- schnell

Warum Mozilla Firefox?

- schnell
- verbreitet

Warum Mozilla Firefox?

- schnell
- verbreitet
- vielseitig erweiterbar

Warum Mozilla Firefox?

- schnell
- verbreitet
- vielseitig erweiterbar
- plattformunabhängig

Warum Mozilla Firefox?

- schnell
- verbreitet
- vielseitig erweiterbar
- plattformunabhängig
- frei

Warum Mozilla Firefox?

- schnell
- verbreitet
- vielseitig erweiterbar
- plattformunabhängig
- frei
- nicht von Microsoft ;-)

Firefox installieren

Download unter

`http://www.mozilla.com`

Ubuntu User schreiben

`sudo apt-get install firefox`

Aber unter Ubuntu ist Mozilla Firefox schon installiert.

Kommunikation über HTTP

Daten, die zwischen Browser und Server ausgetauscht werden, sind Text

Anfrage an den Webserver

```
GET /path/file.html HTTP/1.0
From: someuser@jmarshall.com
User-Agent: HTTPTool/1.0
```

Kommunikation über HTTP

Daten, die zwischen Browser und Server ausgetauscht werden, sind Text

Antwort vom Webserver

```
HTTP/1.0 200 OK
Date: Fri, 31 Dec 1999 23:59:59 GMT
Content-Type: text/html
Content-Length: 1354

<Inhalt einer Datei>
```

Veschlüsselung mit https

Die Kommunikation zwischen Browser und Server ist identisch mit der ohne Verschlüsselung, nur werden alle Daten vor dem Versenden verschlüsselt.

Verschlüsselung mit https

Dadurch ist sichergestellt, dass kein Fremder, den Datenverkehr mitlesen kann.

Verschlüsselung mit https

Dadurch ist sichergestellt, dass kein Fremder, den Datenverkehr mitlesen kann.

Aber

Woher weiß ich, ob ich mit dem richtigen Partner rede?

Zertifikate

- Zertifikate sind „Beglaubigungen“

Zertifikate

- Zertifikate sind „Beglaubigungen“
- SSL Betreiber erstellt ein Zertifikat für eine bestimmte Seite

Zertifikate

- Zertifikate sind „Beglaubigungen“
- SSL Betreiber erstellt ein Zertifikat für eine bestimmte Seite
- Vertrauenswürdiger Dritter beglaubigt das Zertifikat

Zertifikate

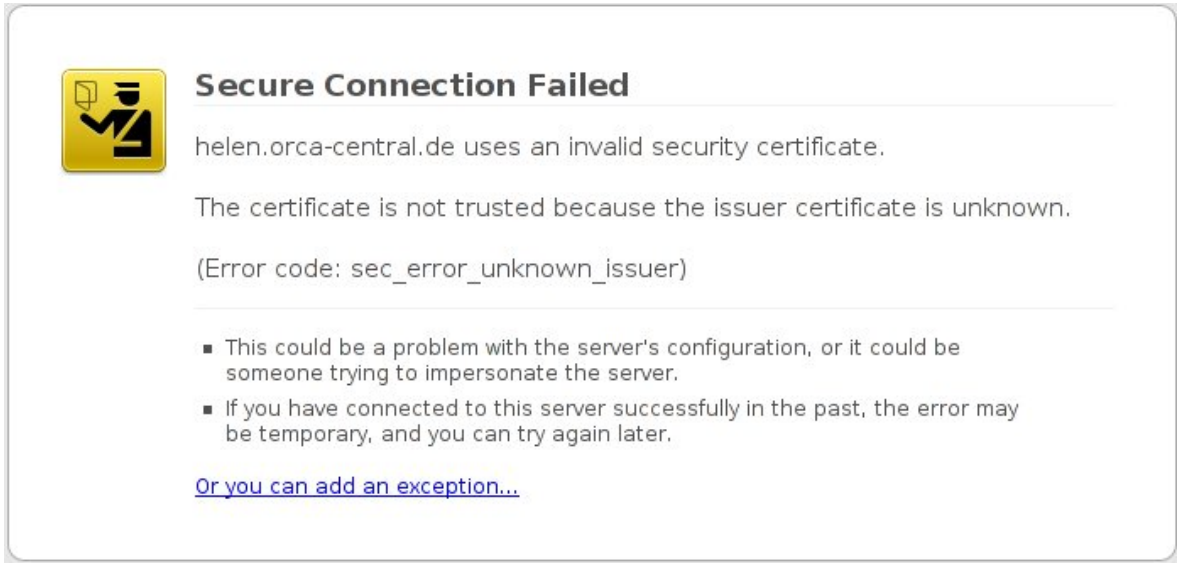
- Zertifikate sind „Beglaubigungen“
- SSL Betreiber erstellt ein Zertifikat für eine bestimmte Seite
- Vertrauenswürdiger Dritter beglaubigt das Zertifikat
- Beglaubiger von Zertifikaten heißen Certificate Authorities (CA)

Zertifikate

- Zertifikate sind „Beglaubigungen“
- SSL Betreiber erstellt ein Zertifikat für eine bestimmte Seite
- Vertrauenswürdiger Dritter beglaubigt das Zertifikat
- Beglaubiger von Zertifikaten heißen Certificate Authorities (CA)
- Jeder Browser kennt die Zertifikate der wichtigsten CAs.

Zertifikatsfehler

Wird ein Zertifikat benutzt, das der Browser nicht kennt, und das von keiner bekannten CA unterschrieben wurde, erhält der User eine Fehlermeldung:

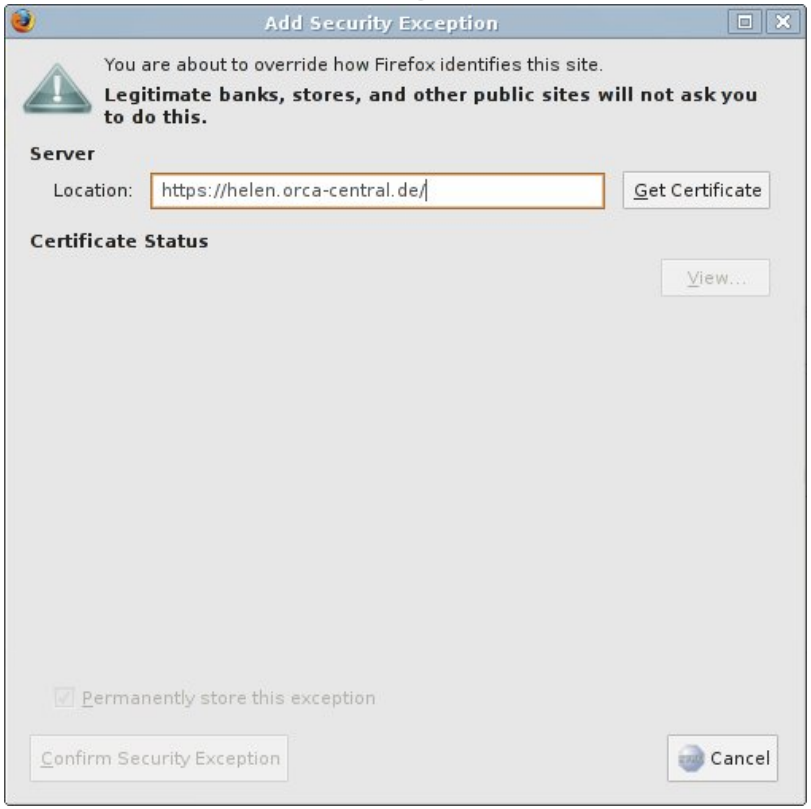


Ein Zertifikat aufnehmen

Ein Zertifikat, dass nicht von einer CA beglaubigt ist, kann man als Ausnahme einfügen.

Ein Zertifikat aufnehmen

Ein Zertifikat, dass nicht von einer CA beglaubigt ist, kann man als Ausnahme einfügen.



Zertifikate immer prüfen

Wichtig

Nicht beglaubigte Zertifikate immer ansehen!

Zertifikate immer prüfen

Wichtig

Nicht beglaubigte Zertifikate immer ansehen!

Wichtig

Wird plötzlich ein Zertifikatsfehler gemeldet, wo vorher keiner war, aufpassen!

CA-Cert

- CA-Cert ist eine CA, die als Verein organisiert ist, und Zertifikate kostenlos unterschreibt.

CA-Cert

- CA-Cert ist eine CA, die als Verein organisiert ist, und Zertifikate kostenlos unterschreibt.
- Jeder kann mitmachen

CA-Cert

- CA-Cert ist eine CA, die als Verein organisiert ist, und Zertifikate kostenlos unterschreibt.
- Jeder kann mitmachen
- Nachteil: CA-Cert ist in keinem Web-Browser standardmäßig vertreten.

CA-Cert Stammzertifkat einfügen

`http://www.cacert.org/index.php?id=3`

Cookies

- Cookies sind kleine Datenpäkchen, die vom Browser gespeichert werden.

Cookies

- Cookies sind kleine Datenpäkchen, die vom Browser gespeichert werden.
- Können z.B. benutzt werden, um Voreinstellungen einer Webseite zu speichern

Cookies

- Cookies sind kleine Datenpäkchen, die vom Browser gespeichert werden.
- Können z.B. benutzt werden, um Voreinstellungen einer Webseite zu speichern
- Werden von Firmen benutzt um Benutzer wiederzuerkennen.

Cookies

- Cookies sind kleine Datenpäkchen, die vom Browser gespeichert werden.
- Können z.B. benutzt werden, um Voreinstellungen einer Webseite zu speichern
- Werden von Firmen benutzt um Benutzer wiederzuerkennen.
- Amazon nutzt sie um zu gucken, welche Produkte der User ansieht.

Cookies

- Cookies sind kleine Datenpäkchen, die vom Browser gespeichert werden.
- Können z.B. benutzt werden, um Voreinstellungen einer Webseite zu speichern
- Werden von Firmen benutzt um Benutzer wiederzuerkennen.
- Amazon nutzt sie um zu gucken, welche Produkte der User ansieht.
- Google erlaubt durch AdWords, Google Ads etc. einen Benutzer auf unterschiedlichen Seiten zu verfolgen.

Cookies

- Cookies sind kleine Datenpäkchen, die vom Browser gespeichert werden.
- Können z.B. benutzt werden, um Voreinstellungen einer Webseite zu speichern
- Werden von Firmen benutzt um Benutzer wiederzuerkennen.
- Amazon nutzt sie um zu gucken, welche Produkte der User ansieht.
- Google erlaubt durch AdWords, Google Ads etc. einen Benutzer auf unterschiedlichen Seiten zu verfolgen.
- Daten werden 18 Monate lang gespeichert.

Cookies

- Cookies sind kleine Datenpäkchen, die vom Browser gespeichert werden.
- Können z.B. benutzt werden, um Voreinstellungen einer Webseite zu speichern
- Werden von Firmen benutzt um Benutzer wiederzuerkennen.
- Amazon nutzt sie um zu gucken, welche Produkte der User ansieht.
- Google erlaubt durch AdWords, Google Ads etc. einen Benutzer auf unterschiedlichen Seiten zu verfolgen.
- Daten werden 18 Monate lang gespeichert.
- So können umfassende Benutzerprofile erstellt werden.

Cookies abschalten

Viele Seiten funktionieren nicht ohne Cookies, weshalb es besser ist, die Cookies beim Verlassen des Browser zu löschen.

Cookiesverwaltung

Ein gutes Tool zur Verwaltung von Cookies ist BetterPrivacy

- Erlaubt die Auswahl, welche Cookies man aktzepieren will.

Cookiesverwaltung

Ein gutes Tool zur Verwaltung von Cookies ist BetterPrivacy

- Erlaubt die Auswahl, welche Cookies man aktzepieren will.
- Unterbindet auch Cookies in Flash-Animationen

Cookiesverwaltung

Ein gutes Tool zur Verwaltung von Cookies ist BetterPrivacy

- Erlaubt die Auswahl, welche Cookies man aktzepieren will.
- Unterbindet auch Cookies in Flash-Animationen
- Als Add-On leicht installiert.

AdBlock Plus

- Filtert Werbeeinblendungen aus Webseiten raus

AdBlock Plus

- Filtert Werbeeinblendungen aus Webseiten raus
- Benutzt eine Blacklist, die vom Anbieter regelmäßig aktualisiert wird.

AdBlock Plus

- Filtert Werbeeinblendungen aus Webseiten raus
- Benutzt eine Blacklist, die vom Anbieter regelmäßig aktualisiert wird.
- Kann man auch benutzen um Spywareserver zu blockieren.

AdBlock installieren

Menü Extras,AddOns in Firefox.

EasyPrivacy hinzufügen

`http://easylist.adblockplus.org/easylist.txt`

Referer

Der Referer (eingentlich http-Referrer) ist ein Feld im http-Protokoll. In ihm steht von welcher Seite aus, eine Webseite aufgerufen wurde.

Referer

Der Referer (eingentlich http-Referrer) ist ein Feld im http-Protokoll. In ihm steht von welcher Seite aus, eine Webseite aufgerufen wurde. Der falsch geschriebene Name (Referer statt Referrer) geht auf einnen Tippfehler im RFC-2616 zurück.

Referer-Misbrauch

Seiten, die Google und Co einbinden, schicken die Referer Information zusammen mit der IP-Adresse an Google. So kann Google feststellen von welchem Link aus ein Angebot erreicht wurde. Das dienst der Abrechnung mit Anzeigenkunden, kann aber auch misbraucht werden um das Surfverhalten der Anwender bis ins Detail nachzuvollziehen.

Referer-Misbrauch

Seiten, die Google und Co einbinden, schicken die Referer Information zusammen mit der IP-Adresse an Google. So kann Google feststellen von welchem Link aus ein Angebot erreicht wurde. Das dienst der Abrechnung mit Anzeigenkunden, kann aber auch misbraucht werden um das Surfverhalten der Anwender bis ins Detail nachzuvollziehen.
Zusammen mit Cookieinformationen lässt sich so quasi die Browserhistoirie nachzeichnen.

RefControl

- AddOn zum entfernen von Referern.

RefControl

- AddOn zum entfernen von Referern.
- Leicht zu installieren

RefControl

- AddOn zum entfernen von Referern.
- Leicht zu installieren
- Erlaubt auch das gezielte „Fälschen“ von Referern, was Probleme mit fehlenden Referern vermeiden hilft.

Anonym surfen mit TOR

- TOR (The Onion Router) ist ein Netz zum verdeckten Surfen

Anonym surfen mit TOR

- TOR (The Onion Router) ist ein Netz zum verdeckten Surfen
- Viele Knoten, die untereinander verschlüsseln, und nur ihren nächsten Nachbarn kennen.

Anonym surfen mit TOR

- TOR (The Onion Router) ist ein Netz zum verdeckten Surfen
- Viele Knoten, die untereinander verschlüsseln, und nur ihren nächsten Nachbarn kennen.
- Verbindungen können nur bis zum TOR Austrittsknoten verfolgt werden.

Anonym surfen mit TOR

- TOR (The Onion Router) ist ein Netz zum verdeckten Surfen
- Viele Knoten, die untereinander verschlüsseln, und nur ihren nächsten Nachbarn kennen.
- Verbindungen können nur bis zum TOR Austrittsknoten verfolgt werden.
- Nächster Workshop am 11.08.09 mit Henning beschäftigt sich damit, wie man TOR benutzt.

Das war's!

Vielen Dank!
Fragen, Ideen, Anregungen?