

Sicheres
Surfen

Randolph
Maaßen

Gefahren

Privacy
Man In The
Middle

Apps

Adblock
(Edge/Plus)
NoScript
Privoxy
Ghostery
RequestPolicy
HTTPS-
Everywhere

HTTPS ist
broken

Funktionsweise
von HTTPS
Fehler von
HTTPS

Sicheres Surfen

Randolph Maaßen

17.01.2014

E-Mail/Jabber: gaireg@gaireg.de

GPG: 1783 B556 Fingerprint: 49A0 1F28 3C65 335C 5331
AD1E 6FF8 2F68 1783 B556

Inhaltsverzeichnis

Sicheres
Surfen

Randolph
Maaßen

Gefahren

Privacy
Man In The
Middle

Apps

Adblock
(Edge/Plus)
NoScript
Privoxy
Ghostery
RequestPolicy
HTTPS-
Everywhere

HTTPS ist
broken

Funktionsweise
von HTTPS
Fehler von
HTTPS

1 Gefahren

- Privacy
- Man In The Middle

2 Apps

- Adblock (Edge/Plus)
- NoScript
- Privoxy
- Ghostery
- RequestPolicy
- HTTPS-Everywhere

3 HTTPS ist broken

- Funktionsweise von HTTPS
- Fehler von HTTPS

Privacy

Sicheres
Surfen

Randolph
Maaßen

Gefahren

Privacy

Man In The
Middle

Apps

Adblock
(Edge/Plus)

NoScript

Privacy

Ghostery

RequestPolicy

HTTPS-
Everywhere

HTTPS ist
broken

Funktionsweise
von HTTPS

Fehler von
HTTPS

- Was wird getracked
 - Wer surft?
 - Woher kommt er/sie?
 - Wohin geht er/sie?
 - Welche Interessen hat er/sie?

Privacy

Sicheres
Surfen

Randolph
Maaßen

Gefahren

Privacy
Man In The
Middle

Apps

Adblock
(Edge/Plus)
NoScript

Privoxy
Ghostery
RequestPolicy
HTTPS-
Everywhere

HTTPS ist
broken

Funktionsweise
von HTTPS
Fehler von
HTTPS

- Was wird getracked
 - Wer surft?
 - Woher kommt er/sie?
 - Wohin geht er/sie?
 - Welche Interessen hat er/sie?

- Versteckte Mittel
 - Tracking Pixel/Grafiken/Cookies
 - Javascript/Flash
 - IP/Browser-Agent

Man In The Middle

Sicheres
Surfen

Randolph
Maaßen

Gefahren

Privacy

Man In The
Middle

Apps

Adblock
(Edge/Plus)

NoScript

Privoxy

Ghostery

RequestPolicy

HTTPS-
Everywhere

HTTPS ist
broken

Funktionsweise
von HTTPS

Fehler von
HTTPS

Mithören der Daten

- Datendiebstahl
- Identität-Diebstahl
- Session-Cookies

Man In The Middle

Sicheres
Surfen

Randolph
Maaßen

Gefahren

Privacy
Man In The
Middle

Apps

Adblock
(Edge/Plus)

NoScript

Privoxy

Ghostery

RequestPolicy

HTTPS-
Everywhere

HTTPS ist
broken

Funktionsweise
von HTTPS

Fehler von
HTTPS

Mithören der Daten

- Datendiebstahl
- Identität-Diebstahl
- Session-Cookies

Verändern der Daten

- Ersetzen von Texten/Grafiken
- Politische/Wirtschaftliche Fehlinformation
- Bankverbindungen

Adblock (Edge/Plus)

Sicheres
Surfen

Randolph
Maaßen

Gefahren

Privacy
Man In The
Middle

Apps

Adblock
(Edge/Plus)

NoScript

Privacy

Ghostery

RequestPolicy

HTTPS-
Everywhere

HTTPS ist
broken

Funktionsweise
von HTTPS
Fehler von
HTTPS

Gegen: Privacy/Tracking

Funktionsweise:

Blockiert Werbe-Elemente etc. von gelisteten Domains, es werden globale Listen geführt

Verfügbar für:

- Firefox
- Chrome
- Opera

Url: <https://www.adblockplus.org/>

NoScript/NotScripts

Sicheres
Surfen

Randolph
Maaßen

Gefahren

Privacy
Man In The
Middle

Apps

Adblock
(Edge/Plus)

NoScript

Privacy

Ghostery

RequestPolicy

HTTPS-
Everywhere

HTTPS ist
broken

Funktionsweise
von HTTPS

Fehler von
HTTPS

Gegen: Privacy/Tracking

Funktionsweise:

Verhindert die Ausführung von JavaScript-, Java-, Flash-, Silverlight-, etc.- Elementen

Verfügbar für:

- Firefox
- Chrome
- Opera

Url: <http://noscript.net/>

Sicheres
Surfen

Randolph
Maaßen

Gefahren

Privacy
Man In The
Middle

Apps

Adblock
(Edge/Plus)

NoScript

Privoxy

Ghostery

RequestPolicy

HTTPS-
Everywhere

HTTPS ist
broken

Funktionsweise
von HTTPS
Fehler von
HTTPS

Gegen: Privacy/Tracking

Funktionsweise:

Ein HTTP/HTTPS Proxy wird Lokal oder im Netz
installiert und blockiert unerwünschte Inhalte

Verfügbar für:

- Linux
- Windows
- Mac

Url: <http://www.privoxy.org/>

Ghostery

Sicheres
Surfen

Randolph
Maaßen

Gefahren

Privacy
Man In The
Middle

Apps

Adblock
(Edge/Plus)
NoScript
Privacy

Ghostery
RequestPolicy
HTTPS-
Everywhere

HTTPS ist
broken

Funktionsweise
von HTTPS
Fehler von
HTTPS

Gegen: Privacy/Tracking

Funktionsweise:

Scannt die Webseite und Blockiert Elemente von
unerwünschten Domains

Verfügbar für:

- Firefox
- Chrome
- Opera
- Safari
- IE

Url: <https://www.ghostery.com/>

RequestPolicy

Sicheres
Surfen

Randolph
Maaßen

Gefahren

Privacy
Man In The
Middle

Apps

Adblock
(Edge/Plus)
NoScript

Privoxy

Ghostery

RequestPolicy

HTTPS-
Everywhere

HTTPS ist
broken

Funktionsweise
von HTTPS
Fehler von
HTTPS

Gegen: Privacy/Tracking

Funktionsweise:

Blockiert anfragen auf fremde Webseiten

Verfügbar für:

- Firefox

Url: <https://www.requestpolicy.com/>

HTTPS-Everywhere

Sicheres
Surfen

Randolph
Maaßen

Gefahren

Privacy
Man In The
Middle

Apps

Adblock
(Edge/Plus)
NoScript
Privacy
Ghostery
RequestPolicy

HTTPS-
Everywhere

HTTPS ist
broken

Funktionsweise
von HTTPS
Fehler von
HTTPS

Gegen: Man In The Middle

Funktionsweise:

Basierend auf Rulesets werden HTTP-Anfragen in
HTTPS-Anfragen geändert

Verfügbar für:

- Firefox
- Chrome
- Opera

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

Funktionsweise von HTTPS

Sicheres
Surfen

Randolph
Maaßen

Gefahren

Privacy
Man In The
Middle

Apps

Adblock
(Edge/Plus)
NoScript
Privacy
Ghostery
RequestPolicy
HTTPS-
Everywhere

HTTPS ist
broken

Funktionsweise
von HTTPS
Fehler von
HTTPS

- Ein Zertifikat wird vom Server geladen und vom Browser überprüft
- Ein Session-Key wird vom Browser generiert
- Der Session-Key wird mit dem Public-Key verschlüsselt, nur der Server kann ihn entschlüsseln
- Die Daten werden mit dem Session-Key verschlüsselt übertragen

Fehler von HTTPS

Sicheres
Surfen

Randolph
Maaßen

Gefahren

Privacy
Man In The
Middle

Apps

Adblock
(Edge/Plus)
NoScript
Privacy
Ghostery
RequestPolicy
HTTPS-
Everywhere

HTTPS ist
broken

Funktionsweise
von HTTPS
Fehler von
HTTPS

- Eigenen Zertifikaten wird generell nicht vertraut
- Die Verschlüsselung ist nur solange sicher, wie der Privat-Key sicher ist
- Die Session-Keys können auch nachträglich mit dem Private-Key entschlüsselt werden, Gegenmaßnahme siehe PFS
<https://www.eff.org/deeplinks/2013/08/pushing-perfect-forward-secrecy-important-web-privacy-protection>

Danke

Sicheres
Surfen

Randolph
Maaßen

Gefahren

Privacy
Man In The
Middle

Apps

Adblock
(Edge/Plus)
NoScript
Privacy
Ghostery
RequestPolicy
HTTPS-
Everywhere

HTTPS ist
broken

Funktionsweise
von HTTPS
Fehler von
HTTPS

Vielen Dank für ihre Aufmerksamkeit

E-Mail/Jabber: gaireg@gaireg.de

GPG: 1783 B556 Fingerprint: 49A0 1F28 3C65 335C 5331
AD1E 6FF8 2F68 1783 B556