Wegen NSA etc. pp. brauchen wir alles in HTTPS!!1!

Dirk Wetter

@drwetter

- Motivation Kurzvortrag
  - Überreaktion in puncto Privacy + SSL
    - IMO stellenweise wenig fundiert
    - Begriffsverwirrung
  - Ins rechte Maß rücken
  - Provokation beabsichtigt!

Scott Adams / Dilbert 1994: http://dilbert.com/strip/1994-02-22

Vorab

- **Was war Sicherheit (Security) nochmal??**
  - C)onfidentiality Vertraulichkeit
  - I)ntegrity Integrität
  - A)vailabilty Verfügbarkeit

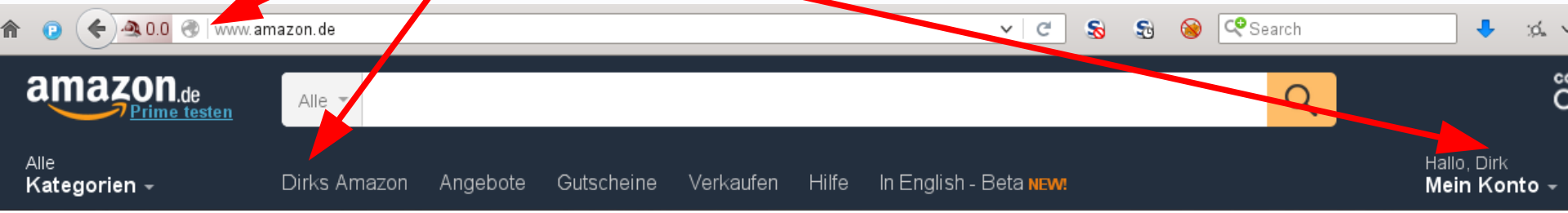
Vortragsthema: Privacy = Datenschutz

- Subset von Vertraulichkeit
- **Kontext hier: Dritten gegenüber**

Kleine Historie

- HTTPS
  - ~2010: HTTPS everywhere (EFF)

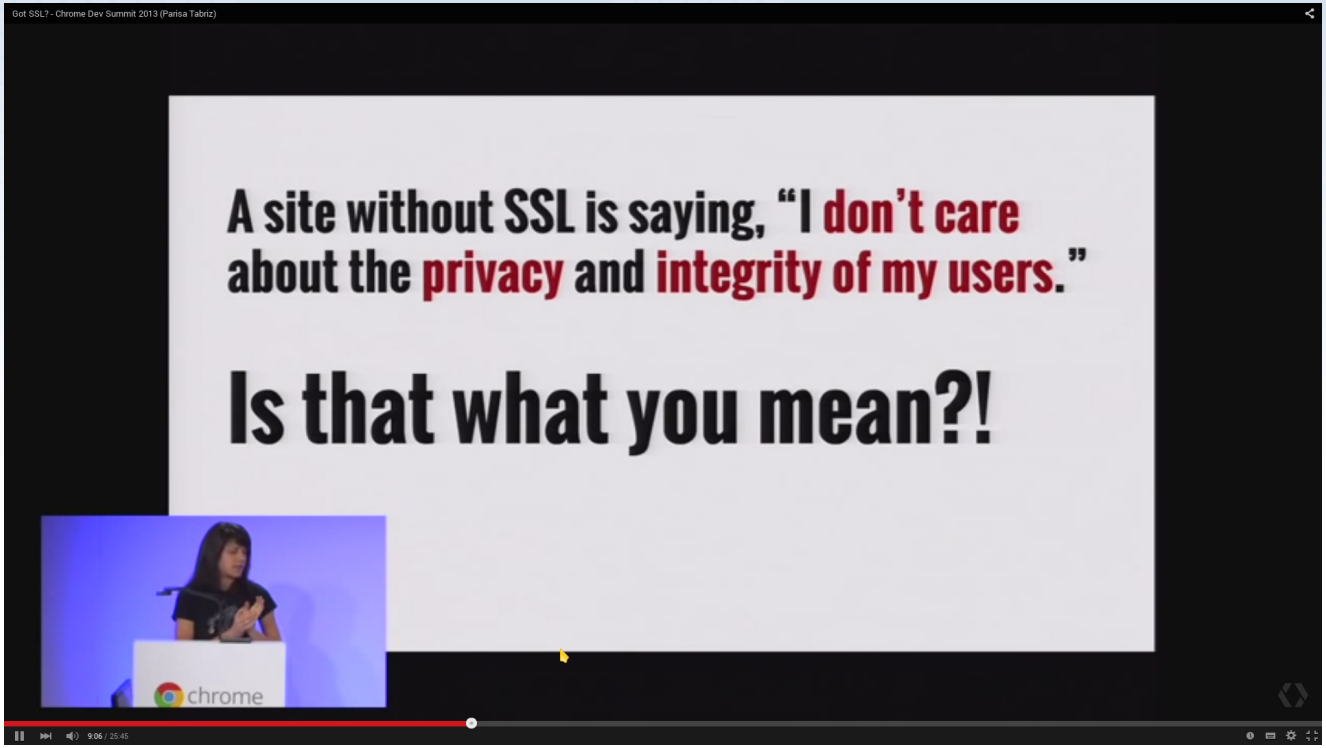
WTF?



Kleine Historie

- HTTPS
  - ~2010: HTTPS everywhere (EFF)
  - 2013: Google @ Chrome Dev Summit

(später relativiert)



Got SSL? - Chrome Dev Summit 2013 (Parisa Tabriz) https://www.youtube.com/watch?v=sJ8EX61fFWQ

Kleine Historie

- HTTPS
  - ~2010: HTTPS everywhere (EFF)
  - 2013: Google @ Chrome Dev Summit
  - 8/2014: Googles Marktmacht

Google | Webmaster Central Blog

HTTPS as a ranking signal

Posted: Wednesday, August 06, 2014

For these reasons, over the past few months we've been running tests taking into account whether sites use secure, encrypted connections as a signal in our search ranking algorithms. We've seen positive results, so we're starting to use HTTPS as a ranking signal. For now it's only a very lightweight signal — affecting fewer than 1% of global queries, and carrying less weight than other signals such as high-quality content — while we give webmasters time to switch to HTTPS. But over time, we may decide to strengthen it, because we'd like to encourage all website owners to switch from HTTP to HTTPS to keep everyone safe on the web. Safe??

http://googlewebmastercentral.blogspot.com.au/2014/08/https-as-ranking-signal.html

Kleine Historie

- HTTPS
  - ~2010: HTTPS everywhere (EFF)
  - 2013: Google @ Chrome Dev Summit
  - 8/2014: Googles Marktmacht
  - 12/2014: Google legte nach

The Chromium Projects

Marking HTTP As Non-Secure

Proposal

We, the Chrome Security Team, propose that user agents (UAs) **gradually change their UX to display non-secure origins as affirmatively non-secure**. We intend to devise and begin deploying a transition plan for Chrome in 2015.

We know that active tampering and surveillance attacks, as well as passive surveillance attacks, are not theoretical but are in fact commonplace on the web.

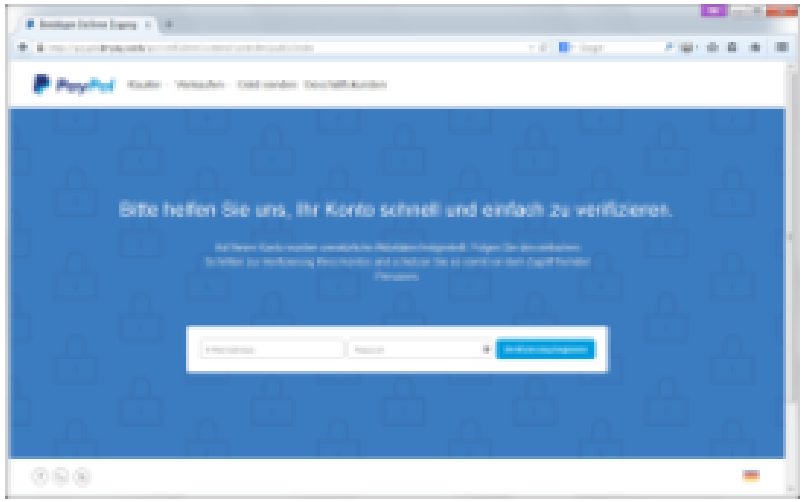
https://www.chromium.org/Home/chromium-security/marking-http-as-non-secure

Kleine Historie

- Leider: HTTPS nicht zwangsweise sicher

Online-Ganoven haben eine täuschend echt gestaltete Phishing-Seite aufgesetzt, die mit einem gültigen SSL-Zertifikat ausgeliefert wird. Sie missbrauchen dabei den CDN-Dienst Cloudflare, der seinen Nutzern seit einigen Monaten kostenlose Zertifikate ausstellt.

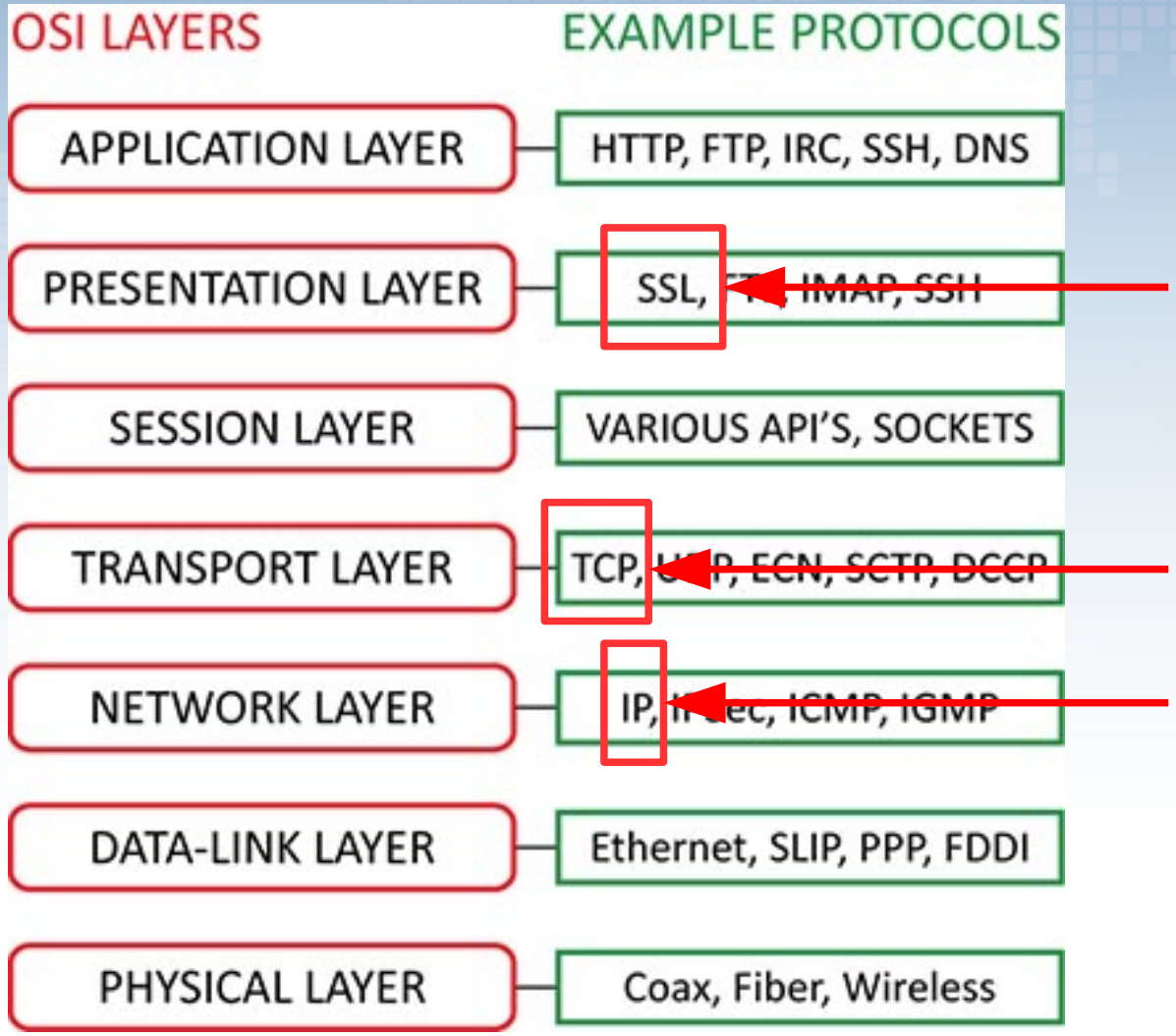
Und das ist denkbar einfach: Die Registrierung bei Cloudflare dauert Sekunden, persönliche Daten fragt der Dienst nicht ab. Anschließend muss man beim Domain-Anbieter nur noch die DNS-Einstellungen anpassen. Innerhalb von 24 Stunden wird die Site mit einem gültigen SSL-Zertifikat ausgeliefert, das von der Zertifizierungsstelle Comodo ausgestellt wurde.



Die Masche ist alt, die Umsetzung aber selten so perfekt: Paypal-Phishing mit knackiger Domain und HTTPS-Zertifikat.

http://www.heise.de/-2514585

OSI-/IP-Nachilfe



```
▶ Internet Protocol Version 4, Src: [redacted], Dst: 81.169.199.25 (81.169.199.25)
▶ Transmission Control Protocol, Src Port: 52314 (52314), Dst Port: https (443), Seq: 1, Ack: 1, Len: 2
▼ Secure Sockets Layer
  ▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 197
    ▼ Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 193
        Version: TLS 1.2 (0x0303)
      ▶ Random
        Session ID Length: 0
        Cipher Suites Length: 26
      ▶ Cipher Suites (13 suites)
        Compression Methods Length: 1
      ▶ Compression Methods (1 method)
        Extensions Length: 126
      ▼ Extension: server_name
          Type: server_name (0x0000)
          Length: 15
        ▼ Server Name Indication extension
            Server Name list length: 13
            Server Name Type: host_name (0)
            Server Name length: 10
            Server Name: testssl.sh
      ▶ Extension: renegotiation_info
      ▶ Extension: elliptic_curves
      ▶ Extension: ec_point_formats
      ▶ Extension: SessionTicket TLS
      ▶ Extension: next_protocol_negotiation
      ▶ Extension: Unknown 16
      ▶ Extension: Unknown 30032
      ▶ Extension: status_request
      ▶ Extension: Unknown 18
      ▶ Extension: signature_algorithms
```

IP

TCP

SSL/TLS

ClientHello

(abgeschnorchelt am Router)

Plus:
CN ServerHello

SSL-Inhalte und Privacy

- Klar!
  - Browser-Fingerprinting auf dem Draht!

ClientHellos
(abgeschnorchelt am Router)

Firefox

```
  Cipher Suites Length: 26
▶ Cipher Suites (13 suites)
  Compression Methods Length: 1
▶ Compression Methods (1 method)
  Extensions Length: 126
▶ Extension: server_name
▶ Extension: renegotiation_info
▶ Extension: elliptic_curves
▶ Extension: ec_point_formats
▶ Extension: SessionTicket TLS
▶ Extension: next_protocol_negotiation
▶ Extension: Unknown 16
▶ Extension: Unknown 30032
▶ Extension: status_request
▶ Extension: Unknown 18
▶ Extension: signature_algorithms
```

Chrome

```
  Cipher Suites Length: 20
▶ Cipher Suites (10 suites)
  Compression Methods Length: 1
▶ Compression Methods (1 method)
  Extensions Length: 112
▶ Extension: server_name
▶ Extension: renegotiation_info
▶ Extension: elliptic_curves
▶ Extension: ec_point_formats
▶ Extension: SessionTicket TLS
▶ Extension: next_protocol_negotiation
▶ Extension: Unknown 16
▶ Extension: status_request
▶ Extension: signature_algorithms
```

SSL-Inhalte und Privacy

✓	Method	File	Domain	Type	Transferred	Size	0 ms / 1.28 s / 2.56 s / 3.84 s
			github.com		14.89 KB		→ 672 ms
			assets-cdn.github.com		44.41 KB		→ 251 ms
			assets-cdn.github.com		58.03 KB		→ 331 ms
			assets-cdn.github.com		73.31 KB		→ 505 ms
			assets-cdn.github.com		115.79 KB		→ 632 ms
			avatars1.githubusercont...		1.55 KB		→ 465 ms
			assets-cdn.github.com		2.26 KB		→ 458 ms
			camo.githubusercontent...		0.65 KB		→ 308 ms
			github.com		0.17 KB		→ 177 ms
			collector-cdn.github.com		2.82 KB		→ 134 ms
			assets-cdn.github.com		3.94 KB		→ 62 ms
			github.com		0.08 KB		→ 315 ms
			live.github.com		—		→ 414 ms
			collector.githubapp.com		0.03 KB		→ 424 ms
			api.github.com		0 0.03 KB		→

SSL-Inhalte und Privacy

- Nur in der Konsole. Im Netz:
  - Längen nicht einsehbar (MTU)
    - 304
    - HTTP/ 1.1 Pipelining
    - Keepalive
  - SSL-Session-ID / TLS Session -Tickets

Wireshark

524	3.010620000	[redacted]	81.169.199.25	TCP	66 443	46376 > https [ACK] Seq=960 Ack=95195 Win=44160 Len=0 TSval=64755558
525	3.010720000	81.169.199.25	[redacted]	TCP	1506 46376	[TCP segment of a reassembled PDU]
526	3.012238000	81.169.199.25	[redacted]	TCP	1506 46376	[TCP segment of a reassembled PDU]
527	3.012253000	[redacted]	81.169.199.25	TCP	66 443	46376 > https [ACK] Seq=960 Ack=98075 Win=44160 Len=0 TSval=64755558
528	3.014286000	81.169.199.25	[redacted]	TLSv1.2	1506 46376	Application Data
529	3.014432000	81.169.199.25	[redacted]	TCP	1506 46376	[TCP segment of a reassembled PDU]
530	3.014444000	[redacted]	81.169.199.25	TCP	66 443	46376 > https [ACK] Seq=960 Ack=100955 Win=44160 Len=0 TSval=6475555
531	3.020430000	81.169.199.25	[redacted]	TCP	1506 46376	[TCP segment of a reassembled PDU]
532	3.020540000	81.169.199.25	[redacted]	TCP	1506 46376	[TCP segment of a reassembled PDU]
533	3.020553000	[redacted]	81.169.199.25	TCP	66 443	46376 > https [ACK] Seq=960 Ack=103835 Win=50944 Len=0 TSval=6475555
534	3.022302000	81.169.199.25	[redacted]	TCP	1506 46376	[TCP segment of a reassembled PDU]
535	3.022446000	81.169.199.25	[redacted]	TCP	1506 46376	[TCP segment of a reassembled PDU]
536	3.022462000	[redacted]	81.169.199.25	TCP	66 443	46376 > https [ACK] Seq=960 Ack=106715 Win=56832 Len=0 TSval=6475555
537	3.024303000	81.169.199.25	[redacted]	TCP	1506 46376	[TCP segment of a reassembled PDU]
538	3.026052000	81.169.199.25	[redacted]	TCP	1506 46376	[TCP segment of a reassembled PDU]
539	3.026067000	[redacted]	81.169.199.25	TCP	66 443	46376 > https [ACK] Seq=960 Ack=109595 Win=62592 Len=0 TSval=6475555
540	3.028089000	81.169.199.25	[redacted]	TLSv1.2	1080 46376	Application Data

SSL-Inhalte und Privacy

- **Content Dritter!**

✓	Method	File	Domain	Type	Transferred	Size	0 ms / 1.28 s / 2.56 s / 3.84 s
200	GET	testssl.sh	github.com	html	14.89 KB	59.21 KB	→ 672 ms
200	GET	github-760a949769f28e3d6febd885...	assets-cdn.github.com	css	44.41 KB	183.18 KB	→ 251 ms
200	GET	github2-622bce26a4704c8a581fe1e...	assets-cdn.github.com	css	58.03 KB	252.20 KB	→ 331 ms
200	GET	frameworks-06e65f5639cc52d1aaa...	assets-cdn.github.com	js	73.31 KB	201.44 KB	→ 505 ms
200	GET	github-ee4ac88329bd04835855a91...	assets-cdn.github.com	js	115.79 KB	357.59 KB	→ 632 ms
200	GET	8036727?v=3&s=40	avatars1.githubusercont...	png	1.55 KB	2.07 KB	→ 465 ms
200	GET	octocat-spinner-32.gif	assets-cdn.github.com	gif	2.26 KB	3.01 KB	→ 458 ms
200	GET	68747470733a2f2f62616467657...	camo.githubusercontent...	svg	0.65 KB	0.65 KB	→ 308 ms
200	GET	show_partial?partial=tree/recently_...	github.com	html	0.17 KB	0.22 KB	→ 177 ms
200	GET	api.js	collector-cdn.github.com	js	2.82 KB	7.80 KB	→ 134 ms
200	GET	ZeroClipboard.v2.1.6.swf	assets-cdn.github.com	x-sho...	3.94 KB	5.26 KB	→ 62 ms
200	GET	counts	github.com	json	0.08 KB	0.10 KB	→ 315 ms
101	GET	ODAzNjcyNzpkNDA2YmMxYzl5O...	live.github.com	plain	—	0 KB	→ 414 ms
200	GET	page_view?dimensions[page]=h...	collector.githubapp.com	gif	0.03 KB	0.05 KB	→ 424 ms
200	POST	stats	api.github.com	json	0 0.03 KB	0.00 KB	→ 5

Inhalte via HTTPS und Privacy

- Tracker
  - Die wahren Privacy Killer!
  - Schlechtes Beispiel (da HTTP):

33 Tracker

www.bild.de/bundesliga/1-liga/home-1-bundesliga-fussball-news-31035072.bild.html

youtube

Bild

1. MONAT 0,99 €

WETTER 13°C HAMBURG

BILD.SHOP COMMUNITY LOGIN

BILDplus NEWS POLITIK GELD UNTERHALTUNG SPORT BUNDESLIGA LIFESTYLE RATGEBER REISE AUTO DIGITAL SPIELE REGIO VIDEO

BREAKING NEWS TURM WIEDER OFFEN - ERSTRAHLT IN BLAU-WEISS-ROT +++ BKA: DEUTSCHLAND IM VISIER ISLAMISTISCHER TERRO

Activate Adobe Flash.

Activate Adobe Flash.

Inhalte via HTTPS und Privacy

- **Mixed-Content**
  - State of the (small) disaster:

Mixed Content Handling

Mixed Content Tests

Images	Passive	Yes
CSS	Active	No
Scripts	Active	No
XMLHttpRequest	Active	No
WebSockets	Active	No
Frames	Active	No

(1) These tests might cause a mixed content warning in your browser. That's expected.

(2) If you see a failed test, try to reload the page. If the error persists, please get in touch.

Fix: `about:config`
`security.mixed_content.block_display_content`

Related Functionality

Upgrade Insecure Requests (more info)	No

Inhalte via HTTPS und Privacy

- **Mixed-Content**
  - State of the (bigger) desasters:

Mixed Content Tests	Webkit @ Android 5.0.1		@ Android 4.0.3 FF < 23
Images	Passive	Yes	Yes
CSS	Active	No	Yes
Scripts	Active	No	Yes
XMLHttpRequest	Active	Yes	Yes
WebSockets	Active	Test failed	N/A
Frames	Active	No	Yes

Zusammenfassung

- **HTTPS != VPN**
  - **IP-Adresse, Port, Hostname!!**
  - **Inhalte** per HTTPS werden geschützt
    - auf dem Draht (Endpunkte)
    - so gut wie CA-System und Verschlüsselung halt
    - Längen + Anzahl: nur mit Ressourcen++ bestimmbar
  - URL: aus network sniffing history / klicken
  - Hostname+ URL: selten 1/1, eher 1/n
    - Inhalte Dritte mehr ableitbar

Vgl. E-Mails:
S/MIME, PGP

Zusammenfassung

- **HTTPS != VPN (cont'd)**
  - Browser: TLS Extension, fingerprinting
  - Alte Browser „lecken (potentiell) schlimmer”
  - Weitere Privacy u.a. -Probleme
    - Tracker
    - Mixed Content

Zusammenfassung

- **Kontext ist wichtig!**
  - *Warum* will ich verschlüsseln?
    - Informationswerte?
    - `testssl.sh` vs. `xing.com`
    - Story: `.ietf.org`

IETF

- „HTTPS everywhere for IETF“
  - Roy Fielding

Browsers don't send singular messages containing anonymous information. They send a complex sequence of messages to multiple parties with an interaction pattern and communication state.
[..]
If the IETF wants to improve privacy, it should work on protocols that provide anonymous access to signed artifacts (authentication of the content, not the connection) [..]

IETF

- HTTPS
  - „HTTPS everywhere for IETF“
  - Roy Fielding
  - Tony Hain

While I don't object to making the IETF content available via https/tls, this proposed statement reads as political knee-jerk BS that is both unnecessary and uncalled for. What the statement MUST focus on is 'data integrity', and SHOULD NOT stop to fear mongering over 'privacy'. "It is public data ..."

HTTPS: Am weitesten vorne

- Sonst das Meiste im Netz unverschlüsselt!
  - SMTP
  - Status IMAP/POP (GER: ~ok)
  - VoIP (POTS in Backbone: nein!)
  - Jabber: so lalla
  - DNS (gehört weiter nach oben)
    - DANE/DNSSEC
  - …

- **Danke!**

mail bei drwetter punkt eu

dirk aet owasp org

@drwetter