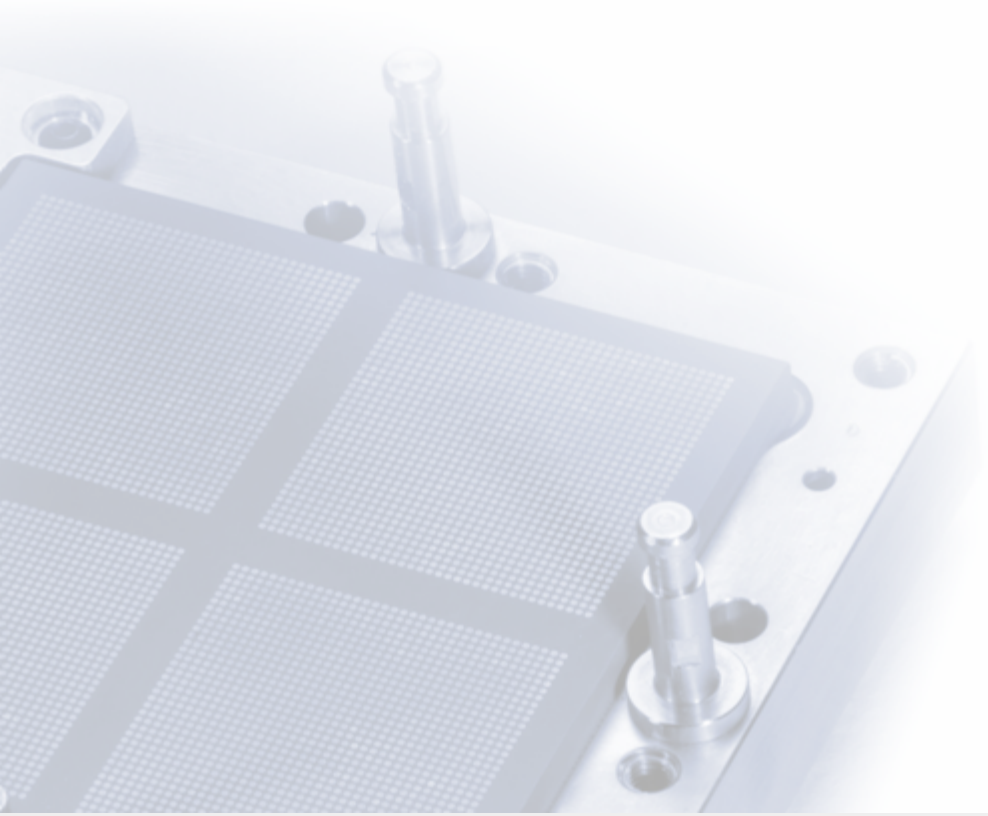
Leibniz Universität Hannover

TLS – Teil 2

Hergen Harnisch
harnisch@luis.uni-hannover.de



TLS für http

TLS für http

DFN-PKI:

- UH-CA
  - Serverzertifikate
  - Nutzerzertifikate
- CCC-CA

Let's encrypt

TLS für http

Was liefert TLS?

- Verschlüsselung (aber nicht des Servernamens)
- Authentifizierung des Servers, Integrität
- mit Client-Zertifikaten auch Client-Authentifizierung (selten)

TLS für http

Was liefert TLS?

- Verschlüsselung (aber nicht des Servernamens)
- Authentifizierung des Servers, Integrität
- mit Client-Zertifikaten auch Client-Authentifizierung (selten)

Warum TLS für Webserver?

- bei Webanwendungen mit Login etc.: offensichtlich
- bei normalen Webseiten:
  - Teil-Privacy (Servername sichtbar, Unterseite nicht)
  - kein falscher Content durch MitM o.ä.
  - und eben auch kein falscher malicious Content

TLS für http

https erzwingen

Problem: http funktioniert auch

- Nutzer muss aktiv https wählen oder darauf achten
- Downgrade-Attacken möglich (https-URLs umschreiben)

Lösung eigentlich nur client-seitig möglich:

Nutzer/Browser muss https wählen

TLS für http

https erzwingen

Problem: http funktioniert auch

- Nutzer muss aktiv https wählen oder darauf achten
- Downgrade-Attacken möglich (https-URLs umschreiben)

Lösung eigentlich nur client-seitig möglich:

Nutzer/Browser muss https wählen

HTTP Strict Transport Security (HSTS)

Webseite kann Header ausliefern, der nachfolgende Besuche über https erzwingt:

```
Strict-Transport-Security: max-age=31536000
```

Beachte: empfehlenswert für TLS-only Webanwendungen

TLS für http

Pinning etc.

Bisher viele Probleme mit Vertrauenswürdigkeit von CAs. Daher einige Vorschläge/Planungen:

- DANE auch für Webserver (Key im DNS mit DNSSEC)
- Certificate-Transparency
- Certificate-Pinning

TLS für http

Pinning etc.

Bisher viele Probleme mit Vertrauenswürdigkeit von CAs. Daher einige Vorschläge/Planungen:

- DANE auch für Webserver (Key im DNS mit DNSSEC)
- Certificate-Transparency
- Certificate-Pinning

HTTP Public Key Pinning (HPKP)

Nachfolgende Besuche erwarten mind. ein Zertifikat mit passendem PIN:

```
Public-Key-Pins: pin-sha256="..."; ...; max-age=604800
```

Empfehlung: derzeit nicht einsetzen oder kurzes max-age

TLS für http

Probleme

TLS-spezifische Header

Kombination aus HSTS und HPKP mit auslaufenden / anderen Zertifikaten:

- kann zu zentral unbehebbarem Denial-of-Server führen
- wg. Fehlkonfiguration oder durch Angriff

daher: HPKP erstmal meiden, Domains ohne www zentral abzusichern

TLS für http

Probleme

TLS-spezifische Header

Kombination aus HSTS und HPKP mit auslaufenden / anderen Zertifikaten:

- kann zu zentral unbehebbarem Denial-of-Server führen
- wg. Fehlkonfiguration oder durch Angriff

daher: HPKP erstmal meiden, Domains ohne www zentral abzusichern

TLS als Sicherheitsmaßnahme

TLS allein macht den Webserver nicht sicher!
Webanwendungen haben leicht Probleme, die nicht vergessen.

DFN-PKI:

TLS für http

DFN-PKI:

- UH-CA
  - Serverzertifikate
  - Nutzerzertifikate
- CCC-CA

Let's encrypt

DFN-PKI: UH-CA

Serverzertifikate

Berechtigung muss nachgewiesen werden:

⟶ Institut muss durch Akkreditierungsschreiben zustimmen

⟶ Ausweis oder Pass & persönliches Erscheinen

- Generierung Schlüssel & CSR offline (ggf. bei uns mit RA)
- Angabe einer Kontakt-Mailadresse: möglichst Funktions-Mail
  - unabhängig von Person wg. Nachfolger & Vertretung
  - dahin Info-Mail wg. ablaufender Zertifikate
- Zertifikat *mit* Zertifikatskette einspielen (sha256 !)

Anforderungen durch uns

- Domain gehört der Universität, mind. Admin-C/Tech-C
- DNS läuft über zentrale LUH-Server (ns1|2.uni-hannover.de)

DFN-PKI: UH-CA

interne Server

Policy-Änderung führt zu anderem Umgang mit Intranet-Servern:

problemlos rein interne Server, die aber einen global auflösenden DNS-Namen haben

nicht mehr interne Serverbezeichnungen oder private IP-Adressen

- geben Sie dem Server einen offiziellen DNS-Namen
  (das reicht, Dienst muss nicht aus dem Internet erreichbar sein)
- sprechen Sie Dienste nicht über die IP an
- zur Not gibt es noch eine LUH-Internal CA …

DFN-PKI: UH-CA

Nutzerzertifikate

zur Client-Authentifizierung

- wird selten eingesetzt, derzeit beim DFN oder SAP-WebGUI
- als zusätzliche oder Admin- Login-Methode geeignet
- leider aufwendig, aber: clientseitiges SSO, 2-Factor

für Mail

Signatur	uneingeschränkt empfehlenswert, insbesondere als Abgrenzung zu Spam/Phishing
Verschlüsselung	abzuraten, Archiv-Problem; Zusenden von PWs okay

(LUH-Webmailer unterstützt das nicht, Schlüssel-Upload wäre nötig)

DFN-PKI: CCC-CA

Smartcards für SAP-GUI-Nutzung

Wir stellen über eine andere CA (CCC-CA) Zertifikate für Smartcards aus:

- dient der Authentifizierung am SAP-System (und Verschlüsselung)
- hat T-Systems-Signaturkarten für SAP-Nutzung ersetzt
- Antragsverfahren ist anders
  - separate Webseite wg. Smartcard-Anforderungen
  - mehrstufiges Genehmigungsverfahren wg. SAP
- normale Nutzerzertifikate in der DFN-PKI-Global

Aus Anwendersicht:

- Nutzer muss Karte selbst beantragen, PIN geheim halten
- bei Software-Installation genau die Webseite dazu beachten

Let's encrypt

Leibniz Universität Hannover

TLS für http

DFN-PKI:

- UH-CA
  - Serverzertifikate
  - Nutzerzertifikate
- CCC-CA

Let's encrypt

Let's encrypt

Kostenlose Webserver-Zertifikate

u.a. von Mozilla unterstützte CA

- automatisierter Zertifikatsbezug
- teilweise automatische Anpassung in Server-Konfig
- kurze Laufzeit von $\leq$ 90 Tagen
  DFN: Jahre
- nur Prüfung des „faktischen Webserver-Besitzes" (Ist)
  DFN: Prüfung organisatorischer Art (Soll; Ist bei Nutzung)
- keine Bestätigung der Organisationszugehörigkeit
  DFN: Ausgestellt durch LUH

Let's encrypt sollte aus Sicherheitssicht in LUH (und insbesondere für Webanwendungen) nicht eingesetzt werden.

Hausaufgaben

TLS für http

DFN-PKI:

- UH-CA
  - Serverzertifikate
  - Nutzerzertifikate
- CCC-CA

Let's encrypt

Hausaufgaben

- Beachten Sie die Hinweise von bettercrypto.org
- Prüfen Sie die Einstellungen mit ssllabs.com
- Setzen Sie HSTS-Header bei TLS-only-Webanwendungen
- Ersetzen Sie sha1-Zertifikate (auch die Kette)
- Sperren Sie nicht mehr benötigte Zertifikate
- Transferieren Sie zusätzliche Domains durch das Rechenzentrum

Hausaufgaben

- Beachten Sie die Hinweise von bettercrypto.org
- Prüfen Sie die Einstellungen mit ssllabs.com
- Setzen Sie HSTS-Header bei TLS-only-Webanwendungen
- Ersetzen Sie sha1-Zertifikate (auch die Kette)
- Sperren Sie nicht mehr benötigte Zertifikate
- Transferieren Sie zusätzliche Domains durch das Rechenzentrum

- Kümmern Sie sich um die vielzähligen Sicherheitsprobleme dynamischer Webseiten:
  SQL-Injection, Code-Injection, XSS, XSRF, Session-Hijacking …