

Securing Security - DANE Introduction

Patrick Koetter und Carsten Strotmann, sys4 AG

CREATED: 2023-10-19 THU 08:43

Why "Securing Security"

Modes of encryption

- opportunistic encryption
- mandatory encryption

Opportunistic encryption

- No expectation (we take what we get)
- Encryption only if available
- No alerting if encryption fails

Mandatory encryption

- Encryption required
- Abort and alarm in case encryption is failing
- Authentication of the communication peer
- Abort and alarm in case the identity of the peer can not be verified

Issues with opportunistic encryption

- Weaknesses of the Certification Authority (CA) model
- Downgrade attacks are possible
- MITM (Men in the Middle) attacks are possible
- When using certificate pinning, fully automatic certificate rollover are not possible

Problems of the PKIX system (Internet CA model)

- Every CA can issue certificates for every domain
- Sloppy security practices by some CA - the CA model is as secure as its weakest link
- Some CAs are operated by non-trustworthy actors
- CAs sometimes issue wrong or unauthorized certificates




Türktrust? Diginotar? StartSSL?
Symantec?

heise online > DigiNotar

DigiNotar

Fatale Panne bei Zertifikatsherausgeber Türktrust

04. Januar 2013, 12:32 Uhr  195 [heise Security](#)

Zwei für Kunden ausgestellte SSL-Zertifikate eigneten sich dazu, Zertifikate für beliebige Domains auszustellen. Mit einem der beiden wurde ein Wildcard-Zertifikat für Google.com erzeugt. Mehr...

29C3: "Das SSL-System ist grundlegend defekt - und jemand muss es reparieren"

28. Dezember 2012, 21:00 Uhr  162 [heise online](#)

Nach den Vorfällen um den Zertifikats-Anbieter Diginotar plant die EU-Kommission durch eine Regulierung das Vertrauen in die Verschlüsselung wieder herzustellen. Doch die Regelung greife viel zu kurz, meint der Forscher Axel Ambak auf dem 29C3. Mehr...

Protokoll eines Verbrechens: DigiNotar-Einbruch weitgehend aufgeklärt

02. November 2012, 07:00 Uhr  80 [heise Security](#)

Auf rund 100 Seiten hat das mit der Untersuchung des SSL-GAUS beauftragte Unternehmen Fox-IT seine Ergebnisse zusammengetragen. Eine spannende Lektüre – nicht nur für Admins. Mehr...

EU-Behörde für IT-Sicherheit kritisiert Zertifizierungsstellen

07. Dezember 2011, 17:55 Uhr  22 [heise Security](#)

Die IT-Sicherheitsbehörde Enisa äußert sich erstmals über die

Anzeige

Top-News

Gesellschaft für Informatik: BSI soll Lücken veröffentlichen

Internetkonzerne wollen NSA-Befugnisse beschneiden lassen

IEEE-Tagung: WLAN soll bis zu 176 GBit/s schaffen

Microsofts SChannel-Fix wird zum Problem-Patch

Es ist ein Androide: Nokia kündigt Tablet N1 an

neue Videos

1 2 3 4 5

nachgehakt: Online-Banking

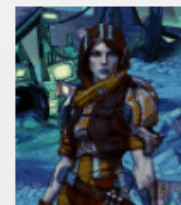
Worauf man beim Online-Banking achten sollte, um nicht über den Tisch gezogen zu werden, erläutert Axel Kossel.



heise open

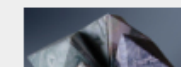
"Borderlands: The Pre-Sequel" für Linux

Mit "Borderlands: The Pre-Sequel" ist ein Top-Spiel bereits zum Starttermin auch für Linux verfügbar. Wir haben uns das Spiel unter Linux angesehen.



Telepolls

Folgen des "größten



Email encryption session downgrade

- STARTTLS works without a policy channel
- STARTTLS support of a peer is unknown before the connection attempt
- Attacker can strip the STARTTLS command from the unencrypted connection and downgrade the session to "Non-TLS"

Email encryption session downgrade

```
220 mail.example.com ESMTP
EHLO client.example.com
250-mail.example.com
250-PIPELINING
250-SIZE 409600000
250-ETRN
```

```
250-STARTTLS
```

```
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
```

Session Downgrade

In recent months, researchers have reported ISPs in the US and Thailand intercepting their customers' data to strip a security flag—called STARTTLS—from email traffic. (...) By stripping out this flag, these ISPs prevent the email servers from successfully encrypting their conversation, and by default the servers will proceed to send email unencrypted.

<https://www.eff.org/deeplinks/2014/11/starttls-downgrade-attacks>

MITM Attacks

- Attacker break TLS secured connections with a matching certificate (matching **Common Name**)
- Most MTA (mail server) accept self-signed certificates (validation of peer identity is not possible)



Missing automation

- Manual validation of certificates for certificate pinning
- Validation of certificates needs knowledge
- Validation of certificates requires work by a human
- Certificate changes at the peer must be monitored
- Manual certificate pinning does not scale

Securing Security

The Plan

- Add a trusted policy channel to TLS
- Build a trust chain
- Signal encryption ability
- Communicate identity

Welcome to DANE

DANE = "DNS-based Authentication of Named Entities" (RFC 6698)

- DANE uses and requires DNSSEC
- DNS is **the** (new) communication channel for policy information
- DNSSEC enables the trust relationship
- DNS records signals the ability for TLS encryption

DANE Use-cases

- **SMTP** - binds service/server to one or more x509 certificates
- **HTTP** - binds service/server to one or more x509 certificates
- **IPSEC** - publishes the IPSec encryption configuration for a host
- **OpenPGP** - connects a public PGP/GPG key to an email address
- **S/MIME** - binds an email address to x509 certificates
- **DoH/DoT** - provides authentication for DNS encryption

Other options to secure TLS connections

DANE is not the only technology that aims to improve the security of the Internet PKI (PKIX):

- **Certificate Transparency** - provides an immutable log of issued certificates - can be used to detect misuse of the CA system (after the fact)
- **CAA-Record** - publishes a policy that binds a domain to one or more certification authorities (CA)

TLS Key Pinning

- Key Pinning
 - **HPKP** - HTTP Public Key Pinning - RFC 7469 (deprecated)
 - **MTA-STS** - SMTP MTA Strict Transport Security - RFC 8461
 - Key Pinning had issues and is not widely deployed
 - Qualsys: HKPK is dead
 - Google Chrome has removed HKPK in Version 78 (Current Version is 118)

Deprecate support for public key pinning (PKP) in Chrome, and then remove it entirely.

DNS as a policy channel

DNS as a policy channel

- DNS has been developed in 1983 as an lightweight, networked hierarchical database for Internet infrastructure information
- DNS has been used mostly for name and address lookups in the early years
- DNS is now becoming the preferred channel to publish security policy information for Internet services

DNS as a policy channel

```
; <<>> DiG 9.16.44-Debian <<>> txt microsoft.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13974
;; flags: qr rd ra; QUERY: 1, ANSWER: 16, AUTHORITY: 0, ADDITIONAL: 1

;; QUESTION SECTION:
;microsoft.com.                IN      TXT

;; ANSWER SECTION:
microsoft.com.      3568    IN      TXT      "google-site-verification=pjPOauSPcrfXOZS9jnPPa5a
microsoft.com.      3568    IN      TXT      "fg2t0gov9424p2tdcuo94goe9j"
microsoft.com.      3568    IN      TXT      "t7sebee51jrj7vm932k531hipa"
microsoft.com.      3568    IN      TXT      "google-site-verification=M--CVfn_YwsV-2FGbCp_HFa
microsoft.com.      3568    IN      TXT      "google-site-verification=GfDnTUdATPsK1230J0mXbfs
microsoft.com.      3568    IN      TXT      "d365mktkey=SxDf1EZxLvMwx6eEZUxzjFFgHoapF8DvtWEUj
microsoft.com.      3568    IN      TXT      "hubspot-developer-verification=OTQ5NGIwYWEtODNmZ

;; Query time: 1097 msec
;; SERVER: 100.115.92.193#53(100.115.92.193)
;; WHEN: Tue Oct 17 09:35:22 CEST 2023
;; MSG SIZE  rcvd: 512
```

Examples of DNS based policy data

- DANE (TLS policy via DNS - the topic of our workshop)
- CAA (Restricting certificate issuing)
- DKIM/DMARC/SPF (Email security)
- Authentication token for internet services (the TXT records at the domain root)
- HTTPS Records (Public key for TLS "encrypted client hello")
- MTA-STS (SMTP-TLS policy via HTTPS)
- SSHFP (SSH fingerprints)
- IPsec (IPsec configurations)

Security of DNS based policy data

- The original DNS system has no build-in security
 - Attacking DNS data is not hard (cache poisoning, DNS spoofing)
 - DNS data might be communicated by untrusted parties (operators for secondary services, insecure DNS resolver caches)
- DNSSEC adds authentication and integrity proof to DNS
 - Recipients of DNS data can validate the origin and the content of the DNS data

The need for DNSSEC

- Policy data in DNS demands DNSSEC
- DANE requires DNSSEC to work
- Operating other DNS based policy methods without DNSSEC severely weakens the security of these policy methods

DNS based policy data without DNSSEC is like having a strong secured iron door inside a paper wall.

End

Questions ? Answers!

