Domain Impersonation is Feasible: A Study of CA Domain Validation Vulnerabilities

Lorenz Schwittmann, **Matthäus Wander**, Torben Weis

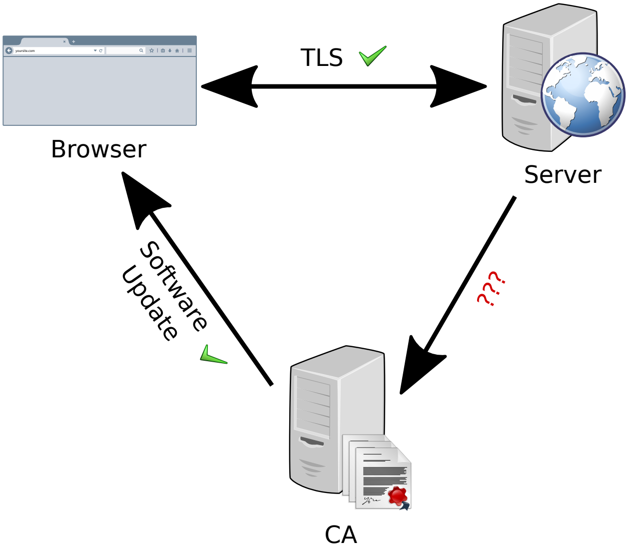
2019-07-24

Distributed Systems Group, University of Duisburg-Essen

UNIVERSITÄT DUISBURG ESSEN

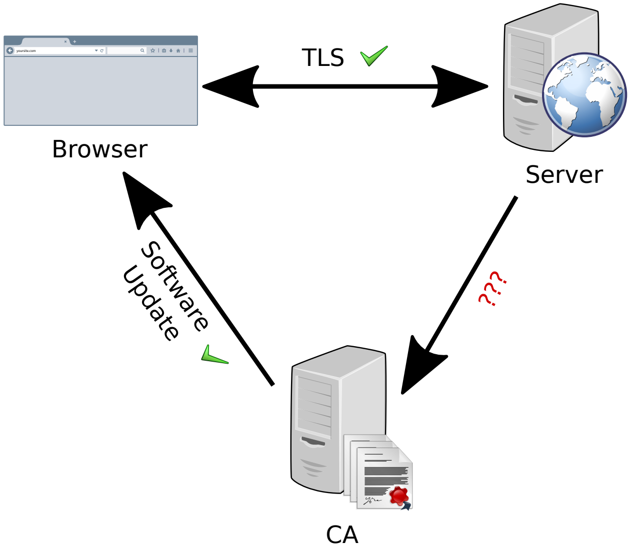
Open-Minded

Trust in the web



Research questions:

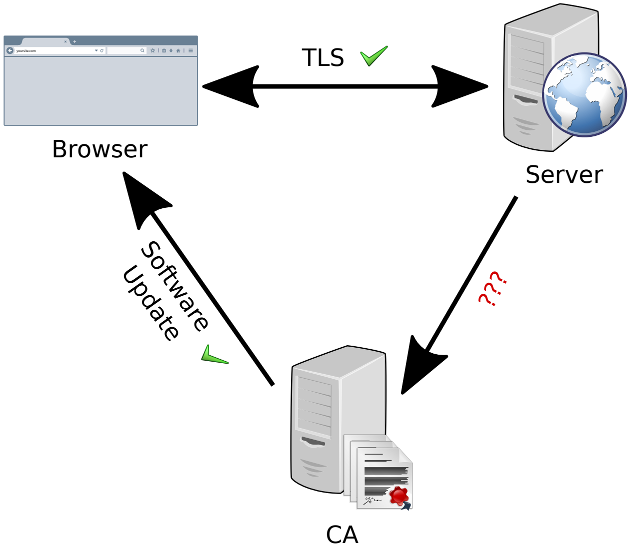
Trust in the web



Research questions:

- What security measures do CAs employ to prevent attacks on domain validation?

Trust in the web

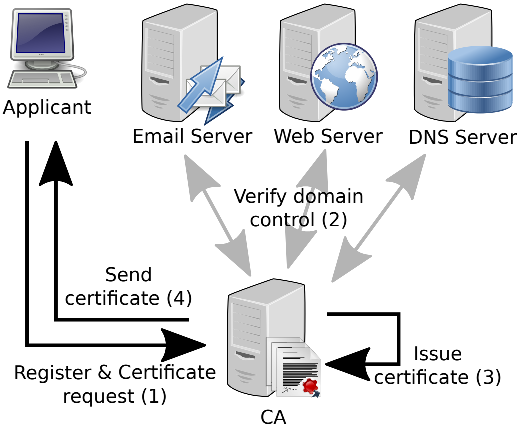


Research questions:

- What security measures do CAs employ to prevent attacks on domain validation?
- How secure is Let's Encrypt compared to traditional CAs?

Table of contents

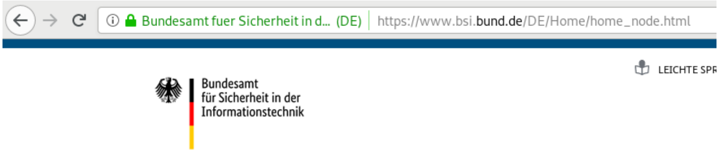
Process of Certificate Issuance



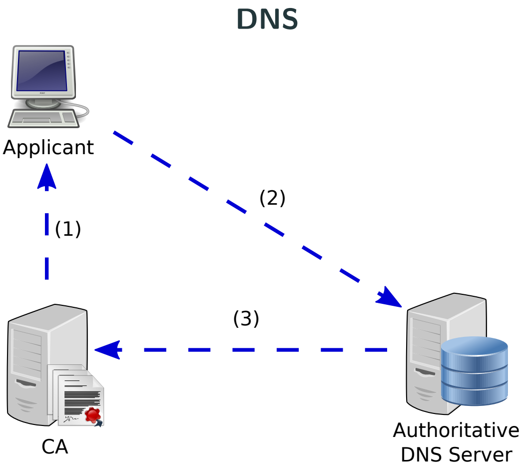
DV/EV Certificates

- Scope of this work: *Domain Validation*
  - Verifies that *applicant* controls domain

- Out of Scope: *Extended Validation*
  - Verifies entity (e.g. company), more expensive

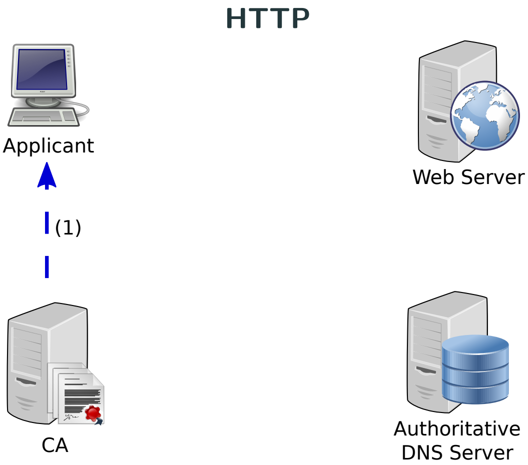


Validation Method: DNS



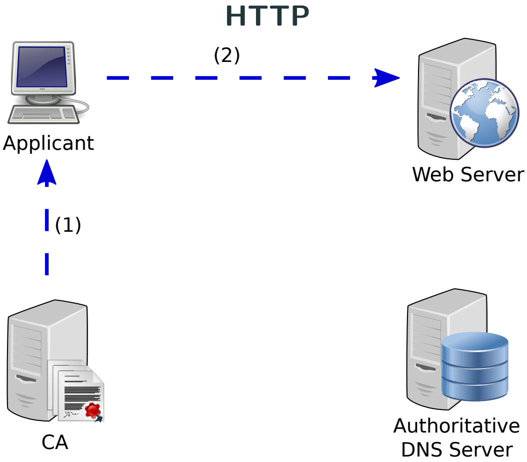
- Show control over domain
- Applicant adds resource record chosen by CA to DNS zone
- Dashed lines: Flow of random token

Validation Method: HTTP



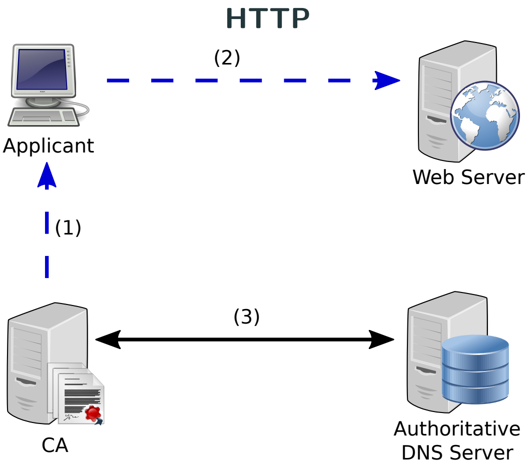
- Show control over domain by placing file on webserver
- Dashed lines: Flow of random token
- Solid line: supporting DNS lookups

Validation Method: HTTP



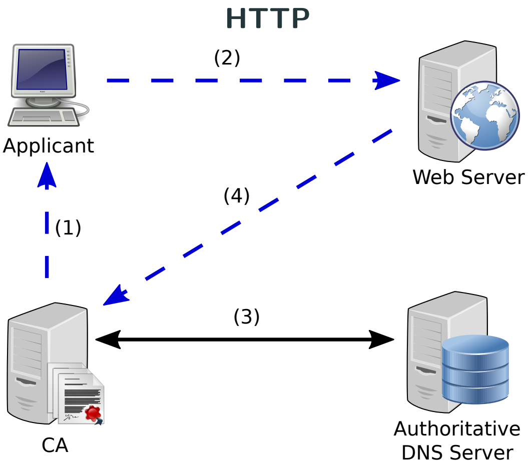
- Show control over domain by placing file on webserver
- Dashed lines: Flow of random token
- Solid line: supporting DNS lookups

Validation Method: HTTP



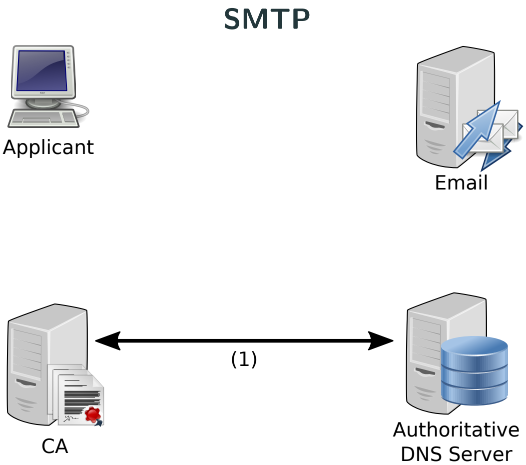
- Show control over domain by placing file on webserver
- Dashed lines: Flow of random token
- Solid line: supporting DNS lookups

Validation Method: HTTP



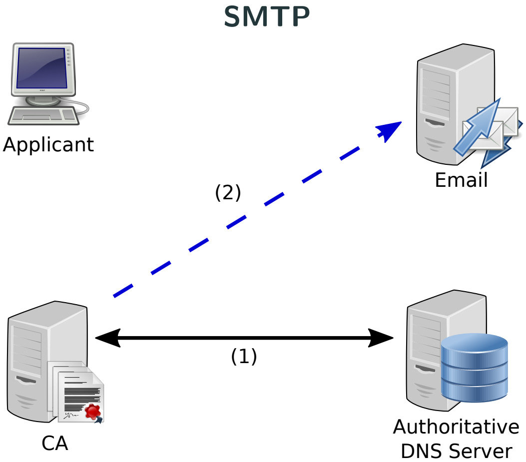
- Show control over domain by placing file on webserver
- Dashed lines: Flow of random token
- Solid line: supporting DNS lookups

Validation Method: SMTP



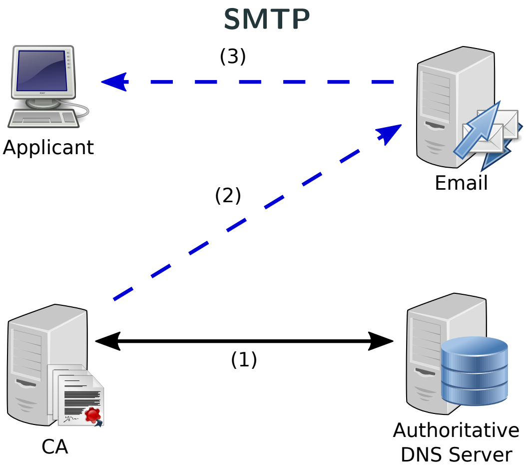
- CA sends email with random token to domain owner
- Applicant has to show knowledge of this token

Validation Method: SMTP



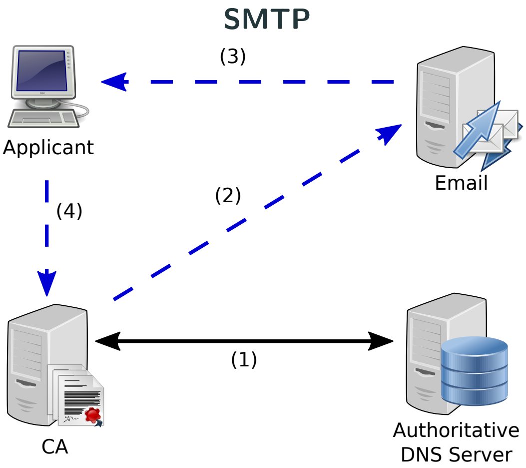
- CA sends email with random token to domain owner
- Applicant has to show knowledge of this token

Validation Method: SMTP



- CA sends email with random token to domain owner
- Applicant has to show knowledge of this token

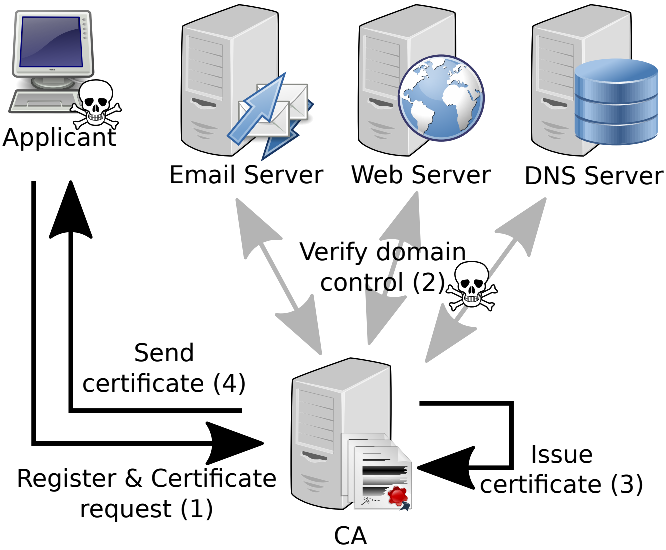
Validation Method: SMTP



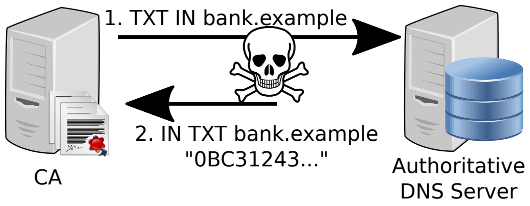
- CA sends email with random token to domain owner
- Applicant has to show knowledge of this token

Attacks on Domain Validation

Attacks in General



On-Path Attacker

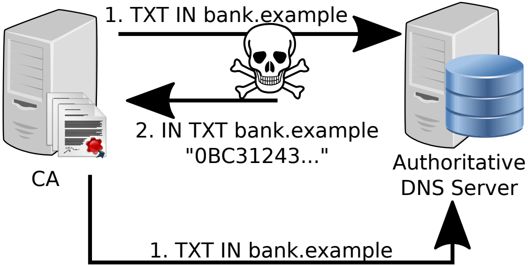


Countermeasures

- Multipath queries

Attacks on DNS-based Validation

On-Path Attacker

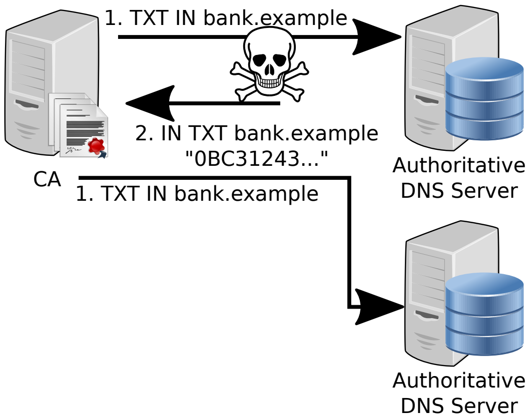


Countermeasures

- Multipath queries
- Relay Node in different autonomous system

Attacks on DNS-based Validation

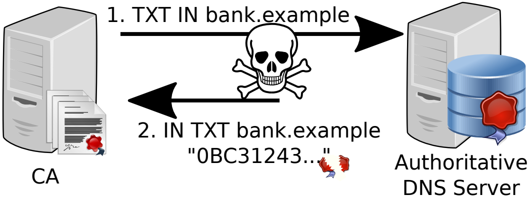
On-Path Attacker



Countermeasures

- Multipath queries
- Relay Node in different autonomous system
- Multiserver queries

On-Path Attacker

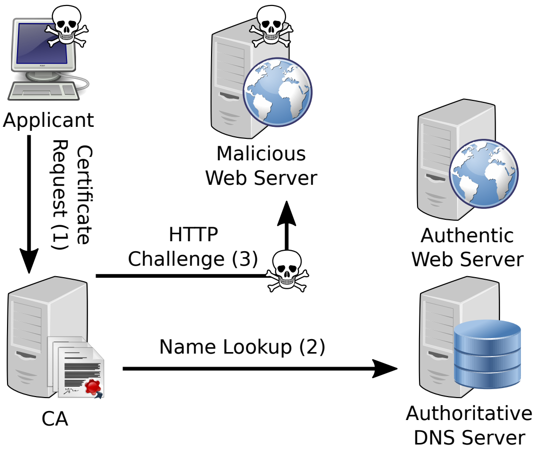


Countermeasures

- Multipath queries
- Relay Node in different autonomous system
- Multiserver queries
- DNSSEC

Attacks on HTTP-based Validation

On-Path Attacker

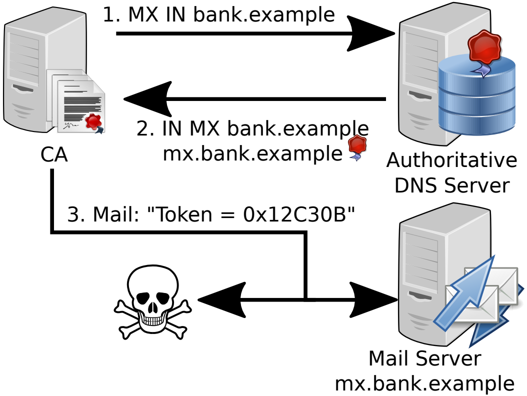


Countermeasures

- HTTP multipath, request from different AS
- HTTPS? Requires trusted certificate, cannot be presumed by CA
- DNS-Based Authentication of Named Entities (DANE)

Attacks on SMTP-based Validation

Passive Attacker



Countermeasures

- Opportunistic STARTTLS

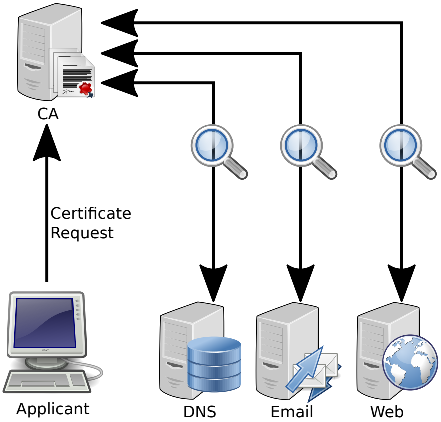
Countermeasure: CAA Record

CAA DNS RR

- Limits which CAs may issue certificates for domain
- Mandatory by CA/Browser Forum Baseline Requirements
- Example: `example.com. CAA 0 issue "letsencrypt.org"`
- When not existing/insecure: attacker can choose weakest CA

Measurement Method

Setup



Detection of Countermeasures

DNS, different categories:

1. Obvious from single query
   - DNS cookies
   - TCP transport
   - 0x20 encoding
   - specific type/name queries (e.g. `TLSA` under _25._*tcp.domain*)
2. Obvious from multiple queries
   - DNSSEC, requires `DO` flag in all queries and additional `DNSKEY` query
   - Multipath queries
   - Multiserver queries
3. Exclude by counterexample
   - Source port randomization
4. Not observable
   - Flood recognition against off-path spoofing

Detection of Countermeasures

HTTP, all observable

- HTTP multipath
- DANE: HTTPS + `TLSA` query with DNSSEC

SMTP, all observable

- STARTTLS, command initiated by sending MTA
- DANE via DNS queries
- End-to-end encryption via DNS queries

Conclusiveness of Method

- Search for countermeasures
- **Absence** of countermeasures means **vulnerability** in our model
- Presence of countermeasures does not allow to conclude absence of vulnerability (i.e. informational status, implementation errors)
- Susceptible to report a false negative vulnerability rating
- But no false positive rating: vulnerabilities are definite

Results

Tested CAs

CA	Tested Validation Methods	Trusted Root CA
AlphaSSL	Email, DNS	GlobalSign
Amazon	Email, DNS	Starfield Technologies
Certum	Email, DNS, HTTP	Certum
Comodo	Email, DNS, HTTP	Comodo
DigiCert	Email[1] with identity validation	DigiCert
GeoTrust	Email	GeoTrust
GlobalSign	HTTP[2]	GlobalSign
GoDaddy	Email, DNS, HTTP	Go Daddy Group
Let's Encrypt	DNS, HTTP, TLS-SNI	IdenTrust
Network Solutions	Email	USERTRUST
RapidSSL	HTTP[3]	DigiCert
SSL.com	Email, DNS, HTTP	USERTRUST
Starfield Technologies	Email, DNS, HTTP	Starfield Technologies
StartCom	Email	–
Thawte	DNS, HTTP	DigiCert
Thawte	Email	Thawte

Further available validation methods: [1]HTTP, DNS; [2]DNS, Email; [3]Email

Covers 96% of publicly trusted certificates in Alexa TOP 10 million as of 2018.

Vulnerabilities found for DNS-based validation

Classification of vulnerable (●), mitigated (◐), found no vulnerability (○).

CA	CAA		DNS	
	On-path	Off-path	On-path	Off-path
AlphaSSL	○	○	●	◐
Amazon	●	◐	◐	◐
Certum	○	○	●	◐
Comodo	○	○	○	○
GoDaddy	◐	◐	●	◐
Let's Encrypt	○	○	○	○
SSL.com	○	○	○	○
Starfield Technologies	◐	◐	●	◐
Thawte	○	○	◐	◐

Vulnerabilities found for HTTP-based validation

Classification of vulnerable (●), mitigated (◐), found no vulnerability (○).

CA	CAA		DNS		HTTP
	On-path	Off-path	On-path	Off-path	Active
Certum	○	○	○	○	●
Comodo	○	○	●	◐	●
GlobalSign*	○	○	◐	◐	●
GoDaddy	●	◐	○	○	●
Let's Encrypt	○	○	○	○	●
RapidSSL	○	○	○	○	●
SSL.com	○	○	○	○	◐
Starfield Technologies	●	◐	○	○	●
Thawte	○	○	○	○	●

* GlobalSign solved the DNS vulnerabilities in August 2018 after we disclosed our results.

Vulnerabilities found for SMTP-based validation

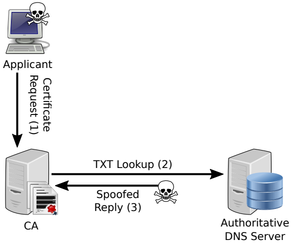
Classification of vulnerable (●), mitigated (◐), found no vulnerability (○).

CA	CAA		DNS		SMTP		
	On-path	Off-path	On-path	Off-path	Passive	Active	TLS version
AlphaSSL	○	○	○	○	○	●	1.2
Amazon	●	◐	◐	◐	○	●	1.0
Certum	●	◐	●	◐	○	●	1.0
Comodo	○	○	○	○	○	○	1.2
DigiCert	○	○	○	○	○	●	1.2
GeoTrust	●	◐	●	◐	○	●	1.0
GoDaddy	●	◐	●	◐	○	●	1.2
Network Solutions	○	○	●	◐	○	●	1.2
SSL.com	○	○	●	◐	○	●	1.2
Starfield Technologies	●	◐	○	○	○	●	1.2
StartCom	●	◐	●	◐	●	●	none
Thawte	●	◐	●	◐	○	●	1.0

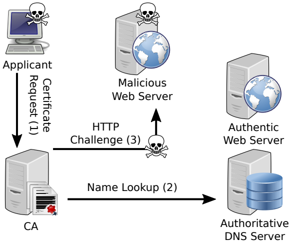
Experimental Validation

Experiment: Perform Actual Attack

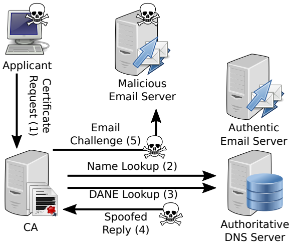
GoDaddy/DNS



Thawte/HTTP



Network Solutions/Email



→ successfully obtained certificates in every case

Disclosure of Results

Disclosed findings to CAs

- Starfield Technologies: DNSSEC not mandatory, therefore not supported
- Thawte: DNSSEC not a priority
- Certum: Acknowledged baseline violation, fixed in July 2018
- GlobalSign: Extensive communication. Acknowledged findings, deployed new infrastructure and provided voucher codes. We verified countermeasure existence in August 2018.
- Let's Encrypt: Acknowledged HTTP vulnerability, favors validation method restrictions in `CAA` records

Recommendations

Domain Owners

- Use CAA records to restrict which CAs which may issue certificates
- Use DNSSEC signing
- Use downgrade resilient signaling mechanisms like DANE or CAA to restrict validation channels when available

CA

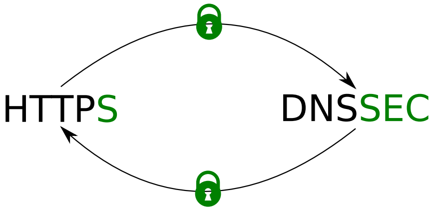
- Perform DNSSEC validation

CA/Browser Forum

- Codify DNSSEC validation in the CA/Browser Forum Baseline Requirements

Conclusion: Certificate Authorities

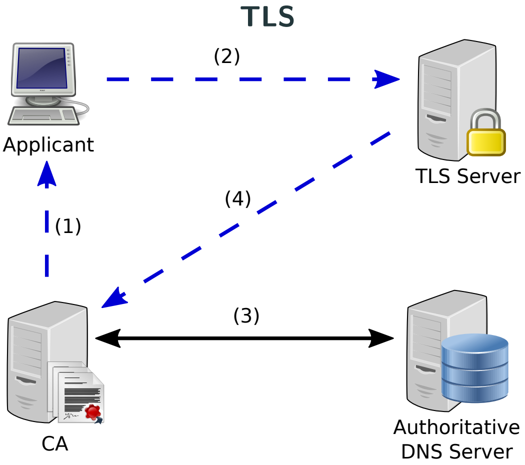
- Domain validation attacks are feasible for network-level attacker
  - **Every** CA was vulnerable via at least one validation method
- Research question: Let's Encrypt is at least as secure as traditional CAs
- Higher price did not correlate with higher security
- Takeaway: Web security relies indirectly on DNSSEC



Backup

Backup

Validation Methods: TLS



- Equivalent to HTTP
- Random token passed in TLS handshake

Vulnerabilities found for TLS-SNI-based validation

Classification of vulnerable (●), mitigated (◐), found no vulnerability (○).

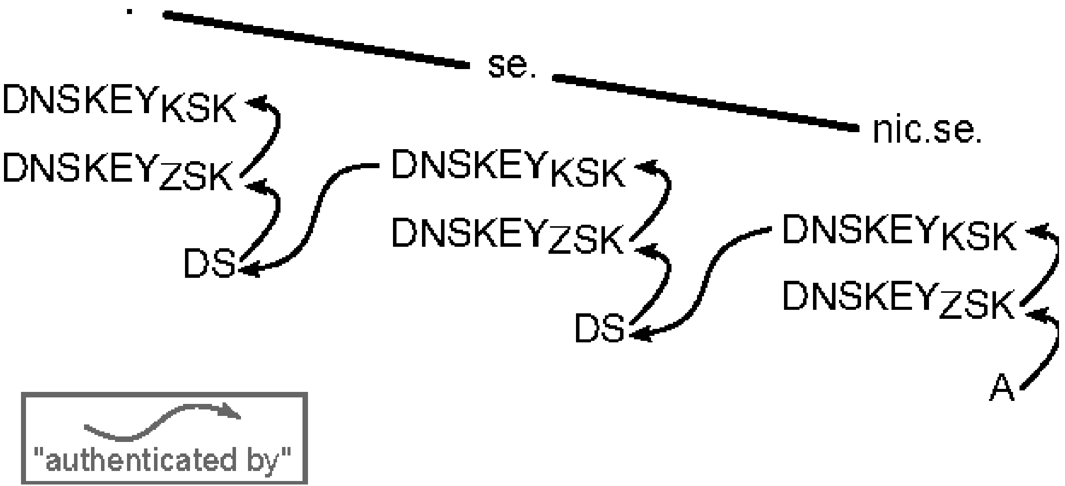
CA	CAA		DNS		TLS
	On-path	Off-path	On-path	Off-path	Active
Let's Encrypt	○	○	○	○	●

Process of validation

Possible procedures (Excerpt CA/Browser Forum Baseline v1.4.1 3.2.2.4):

1. Established relation (CA = Domain registrar)
2. Email, fax, sms, mail to domain contact
3. Constructed email {admin, administrator, webmaster, hostmaster, postmaster}@domain
4. Change to website (/.well-known...)
5. Transmit random number in TLS handshake
6. DNS changes (TXT RR)

DNSSEC



Source: Hahn & Holz 2011

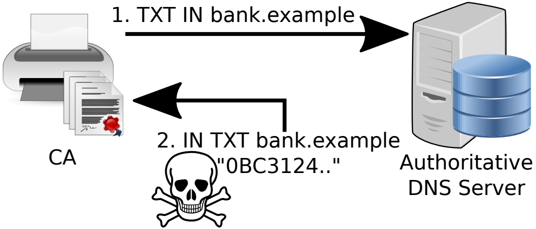
X.509 Certificates

```
Certificate  ::=  SEQUENCE  {
    tbsCertificate       TBSCertificate,
    signatureAlgorithm   AlgorithmIdentifier,
    signatureValue       BIT STRING
}
TBSCertificate  ::=  SEQUENCE  {
    version         [0]  EXPLICIT Version DEFAULT v1,
    serialNumber         CertificateSerialNumber,
    signature            AlgorithmIdentifier,
    issuer               Name,
    validity             Validity,
    subject              Name,
    subjectPublicKeyInfo SubjectPublicKeyInfo,
    issuerUniqueID  [1]  IMPLICIT UniqueIdentifier OPTIONAL,
                         -- If present, version MUST be v2 or v3
    subjectUniqueID [2]  IMPLICIT UniqueIdentifier OPTIONAL,
                         -- If present, version MUST be v2 or v3
    extensions      [3]  EXPLICIT Extensions OPTIONAL
                         -- If present, version MUST be v3
}
```

X.509 v3 certificate structure according to RFC5280.

Attacks on DNS change

Off-Path Attacker

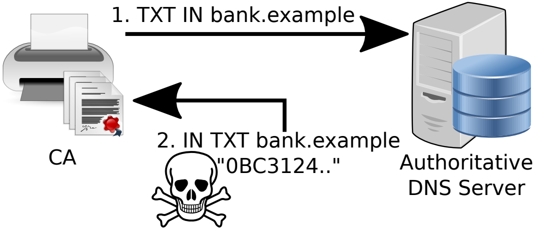


Attempts to spoof DNS response

- Unaware of actual DNS query
- ID field (16 bit) of query and response have to match
- Attacker has to spoof large amounts of packets

Attacks on DNS change

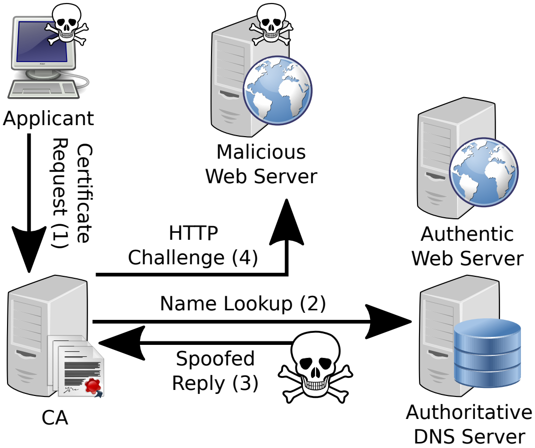
Off-Path Attacker



Countermeasures

- All on-path attacker countermeasures
- Increase entropy
  - Source port randomization
  - 0x20 encoding
  - TCP requests
  - DNS cookies
- Recognize flooding

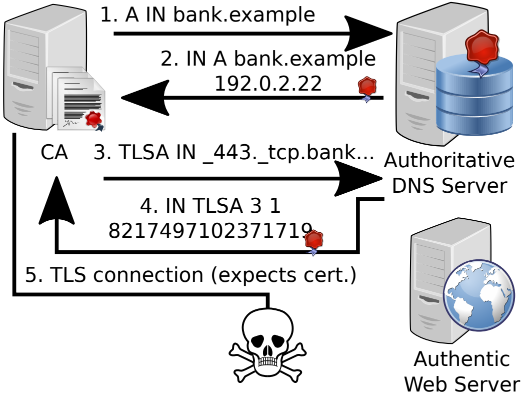
DNS attack on HTTP/TLS-based validation



- Validation depends on DNS
- Successful DNS attack jeopardizes HTTP validation
- Previous attacks and countermeasures apply
- Only on-path attacker considered for HTTP-level attacks

Attacks on HTTP/TLS-based validation

On-Path Attacker

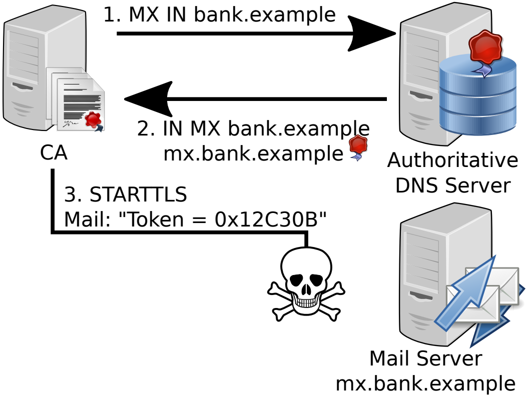


Countermeasures

- HTTP multipath, request from different AS
- DNS-Based Authentication of Named Entities (DANE)
  $\rightarrow$ applies also to TLS-based validation

Attacks on email-based validation

Active Attacker

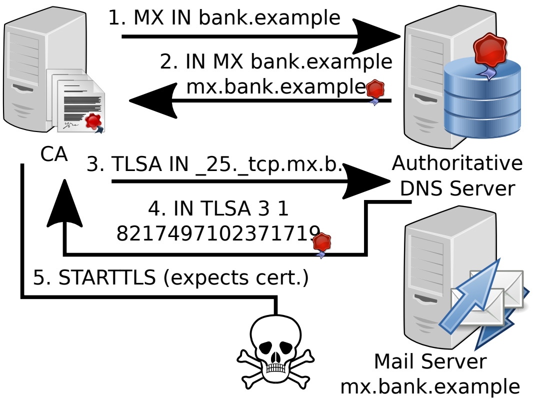


Countermeasures

- STARTTLS with DANE secured certificate
- MTA-STS, requires trusted certificate
- End-to-end email encryption, public keys via DNS

Attacks on email-based validation

Active Attacker



STARTTLS/DANE dependencies

- DNSSEC in all DNS steps
- Redirected MX lookup: TLSA record will not be queried

Time boundary

HTTP and SMTP: DNS queries after connection not relevant for validation request

Example:

```
12:44:40 DNS breaklowerparameters.com IN A -EDC
12:44:40 DNS breaklowerparameters.com IN AAAA -EDC
12:48:37 HTTP GET breaklowerparameters.com/.well-known/pki-valid[...]
12:48:49 DNS breaklowerparameters.com IN CAA -EDC
12:48:49 DNS www.breaklowerparameters.com IN CAA -EDC
12:48:49 DNS breaklowerparameters.com IN DNSKEY -EDC
12:48:49 DNS breaklowerparameters.com IN DNSKEY -EDC
12:48:49 DNS breaklowerparameters.com IN CAA -EDC
12:49:25 DNS breaklowerparameters.com IN A -ED
```

Anomalies - HTTP

Certum via HTTP validation

- Instructed to place random token X at `/.well-known/pki-validation/`X`.html`
- Violates baseline requirement as "the Request Token or Random Value MUST NOT appear in the request"

Starfield Technologies via HTTP validation

- Requests to three different URLs
    1. HTTP `/.well-known/pki-validation/godaddy.html`
    2. HTTPs `/.well-known/pki-validation/godaddy.html`
    3. HTTP `/.well-known/pki-validation/starfield.html`
- Brand-agnostic backend?

Anomalies - SMTP

Validation email to all five constructed addresses

- Performed by Amazon, DigiCert, Godaddy and Starfield Technologies
- Separate SMTP connections, increases chances for attacker
- Also increases likelihood for owner to discover attack

Passive Attacks

- All CAs except StartCom used STARTTLS
- Some CAs negotiated TLS 1.0, not recommended by RFC 7525

Active Attacks

- Only Comodo used STARTTLS + DANE + DNSSEC
- Network Solutions and SSL.com queried `TLSA` record but no `DNSKEY`
- Unusable by specification and vulnerable to on-path attackers

Anomalies - DNSSEC

Certum (DNS and HTTP), GoDaddy (HTTP) and Starfield Technologies (HTTP and email)

- Observed queries via Google Public DNS, a DNSSEC validating public DNS resolving service
- No `DNSKEY` query from resolver in CA's networks
- Relying on Google for validation, no own DNSSEC capabilities?

DNS raw data

Countermeasure	AlphaSSL	Amazon	Certum	Comodo	GoDaddy	Let's Encrypt	SSL.com	Starfield Technologies	Thawte
DnsBit0x20	No	No	No	No	No	Full	No	No	No
DnsBit0x20CAA	No	No	No	No	No	Full	No	No	No
DnsCAADNSSEC	Full	Partial	Full	Full	Partial	Full	Full	Partial	Full
DnsDNSCookie	No	No	No	No	No	No	No	No	No
DnsDNSCookieCAA	No	Full	No	No	No	No	No	No	Partial
DnsDnskey	Full	No	Full	Full	Full	Full	Full	No	Full
DnsMultiServer	Partial	Full	No	Partial	No	No	Full	No	Full
DnsMultiServerCAA	No	No	No	Full	No	No	Full	No	Partial
DnsMultipath	No	Full	No	No	No	No	Full	No	Full
DnsMultipathCAA	No	No	No	Full	Full	No	Full	Full	Partial
DnsRelevantDNSSEC	No	No	No	Full	No	Full	Full	No	No
DnsTcp	No	No	No	No	No	No	No	No	No
DnsTcpCAA	No	Partial	No	No	No	No	No	No	No

HTTP raw data

Countermeasure	Certum	Comodo	GlobalSign	GoDaddy	Let's Encrypt	RapidSSL	SSL.com	Starfield Technologies	Thawte
DaneTls443	No	No	No	No	No	No	No	No	No
DnsBit0x20	No	No	No	No	Full	No	No	No	No
DnsBit0x20CAA	No	No	No	No	Full	No	No	No	No
DnsCAADNSSEC	Full	Full	Full	Partial	Full	Full	Full	Partial	Full
DnsDNSCookie	No	No	No	No	No	Partial	No	No	No
DnsDNSCookieCAA	No	No	No	No	No	Full	No	No	Full
DnsDnskey	Full	Full	Full	Full	Full	Full	Full	Full	Full
DnsMultiServer	Partial	No	Full	Full	Partial	Partial	Partial	Partial	Partial
DnsMultiServerCAA	No	Full	No	No	No	No	Full	No	No
DnsMultipath	Full	No	No	Full	No	Partial	Full	Full	Partial
DnsMultipathCAA	No	Full	No	No	No	No	Full	No	No
DnsRelevantDNSSEC	Full	No	No	Full	Full	Full	Full	Full	Full
DnsTcp	No	No	No	No	No	No	No	No	No
DnsTcpCAA	No	No	No	No	No	Partial	No	No	Partial
HttpMultipath	No	No	No	No	No	No	Full	No	No

TLS-SNI raw data

Countermeasure	Let's Encrypt
DaneTls443	No
DnsBit0x20	Full
DnsBit0x20CAA	Full
DnsCAADNSSEC	Full
DnsDNSCookie	No
DnsDNSCookieCAA	No
DnsDnskey	Full
DnsMultiServer	Partial
DnsMultiServerCAA	No
DnsMultipath	No
DnsMultipathCAA	No
DnsRelevantDNSSEC	Full
DnsTcp	No
DnsTcpCAA	No
TlsMultipath	No

Email raw data

Countermeasure	AlphaSSL	Amazon	Certum	Comodo	DigiCert	GeoTrust	GoDaddy	Network Sol.	SSL.com	Starf.	StartCom	Thawte
DaneTls25	No	No	No	Full	No	No	No	Partial	Partial	No	No	No
DnsBit0x20	No	No	No	No	No	No	No	No	No	No	No	No
DnsBit0x20CAA	No	No	No	No	No	No	No	No	No	No	No	No
DnsCAADNSSEC	Full	Partial	Partial	Full	Full	Partial	Partial	Full	Full	Partial	Partial	Partial
DnsDNSCookie	No	No	No	No	No	No	No	No	No	No	No	No
DnsDNSCookieCAA	No	No	No	No	No	No	No	No	No	No	No	No
DnsDnskey	Full	Full	No	Full	Full	No	No	Full	Full	Full	No	No
DnsMultiServer	Partial	Partial	No	Partial	Partial	No	No	No	No	No	No	No
DnsMultiServerCAA	No	No	No	No	Partial	No	No	Full	No	No	No	No
DnsMultipath	No	Full	No	Full	Full	No	No	No	No	No	No	No
DnsMultipathCAA	No	No	No	No	Partial	No	No	Full	No	No	No	No
DnsRelevantDNSSEC	Full	No	No	Full	Full	No	No	No	No	Full	No	No
DnsTcp	No	No	No	Partial	No	No	No	No	No	No	No	No
DnsTcpCAA	No	No	No	No	No	Partial	No	No	No	No	No	Partial
TlsSmtp	Full	Full	Full	Full	Full	Full	Full	Full	Full	Full	No	Full

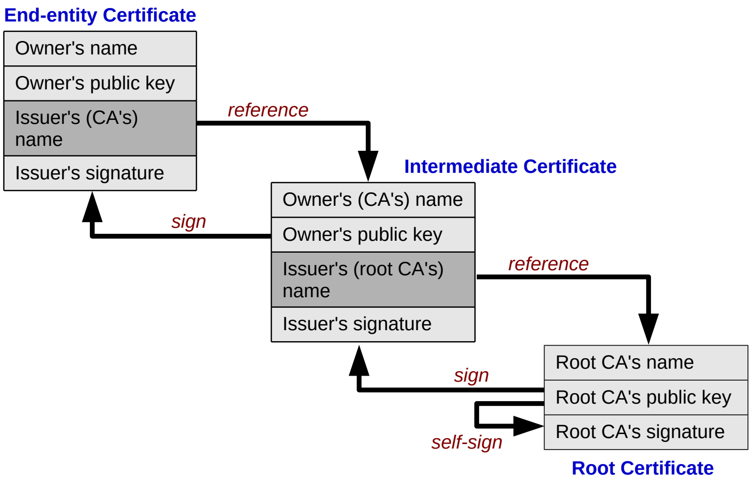
Future work/CA Study

Fehler provozieren, SMTP

- DANE $\rightarrow$ TLSA-Anfragen
  - Zone signieren
  - Invalide Signaturen bei Mailserver 1, spricht kein TLS
  - Valide bei Mailserver 2 mit unbk. Hashalg, Server, spricht kein TLS
  - Mailserver 3 mit validen Signaturen, bek. Hash
  - Sollte nur beim 3. zugestellt werden

Kleinere CAs untersuchen

X.509 Trust



Chain of trust.svg, Wikimedia ©Yanpas 2016