WiP: Untangling Certificate Error Messages

Making X.509 errors usable

Martin Ukrop, Pavol Žáčik

ACSAC 2019, 12. 12. 2019

CROCS
Centre for Research on Cryptography and Security

Martin Ukrop, mukrop@mail.muni.cz
Masaryk University, Czech Republic
Ph.D. research cooperation with Red Hat Czech

Red Hat

Your connection is not private

Attackers might be trying to steal your information from **sha1-intermediate.badssl.com** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_WEAK_SIGNATURE_ALGORITHM

☐ Help improve Chrome security by sending URLs of some pages you visit, limited system information, and some page content to Google. Privacy policy

Advanced

Back to safety

X509_V_ERR_UNSUPPORTED_EXTENSION_FEATURE

Unsupported extension feature.

X509_V_ERR_UNNESTED_RESOURCE

RFC 3779 resource not subset of parent's resources.

X509_V_ERR_PERMITTED_VIOLATION

Permitted subtree violation.

X509_V_ERR_EXCLUDED_VIOLATION

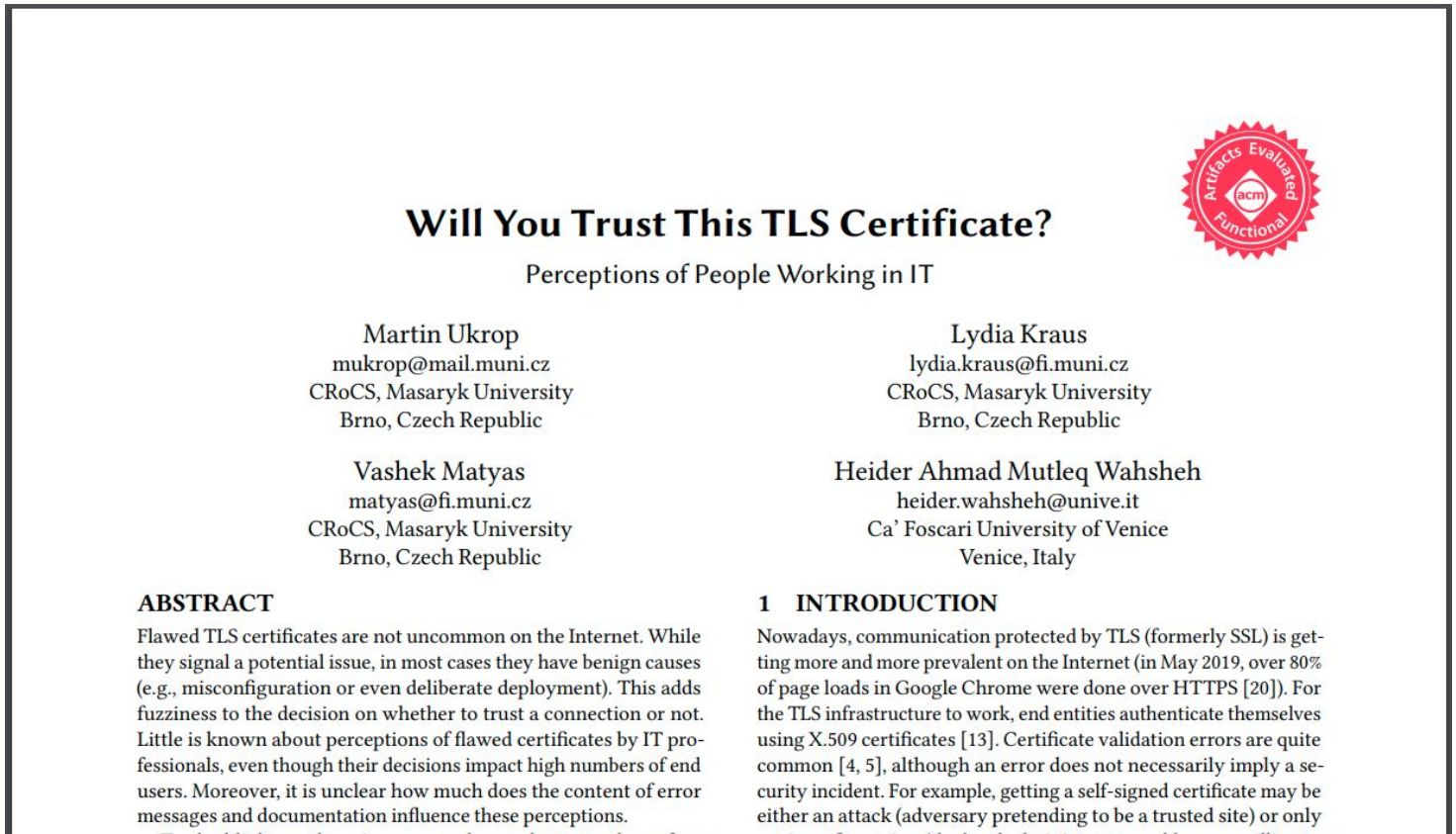
Excluded subtree violation.

Possible X.509 errors...

```
X509_V_OK, X509_V_ERR_UNSPECIFIED, X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT, X509_V_ERR_UNABLE_TO_GET_CRL,
X509_V_ERR_UNABLE_TO_DECRYPT_CERT_SIGNATURE, X509_V_ERR_UNABLE_TO_DECRYPT_CRL_SIGNATURE,
X509_V_ERR_UNABLE_TO_DECODE_ISSUER_PUBLIC_KEY, X509_V_ERR_CERT_SIGNATURE_FAILURE,
X509_V_ERR_CRL_SIGNATURE_FAILURE, X509_V_ERR_CERT_NOT_YET_VALID, X509_V_ERR_CERT_HAS_EXPIRED,
X509_V_ERR_CRL_NOT_YET_VALID, X509_V_ERR_CRL_HAS_EXPIRED, X509_V_ERR_ERROR_IN_CERT_NOT_BEFORE_FIELD,
X509_V_ERR_ERROR_IN_CERT_NOT_AFTER_FIELD, X509_V_ERR_ERROR_IN_CRL_LAST_UPDATE_FIELD,
X509_V_ERR_ERROR_IN_CRL_NEXT_UPDATE_FIELD, X509_V_ERR_OUT_OF_MEM, X509_V_ERR_DEPTH_ZERO_SELF_SIGNED_CERT,
X509_V_ERR_SELF_SIGNED_CERT_IN_CHAIN, X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY,
X509_V_ERR_UNABLE_TO_VERIFY_LEAF_SIGNATURE, X509_V_ERR_CERT_CHAIN_TOO_LONG, X509_V_ERR_CERT_REVOKED,
X509_V_ERR_INVALID_CA, X509_V_ERR_PATH_LENGTH_EXCEEDED, X509_V_ERR_INVALID_PURPOSE,
X509_V_ERR_CERT_UNTRUSTED, X509_V_ERR_CERT_REJECTED, X509_V_ERR_SUBJECT_ISSUER_MISMATCH,
X509_V_ERR_AKID_SKID_MISMATCH, X509_V_ERR_AKID_ISSUER_SERIAL_MISMATCH, X509_V_ERR_KEYUSAGE_NO_CERTSIGN,
X509_V_ERR_UNABLE_TO_GET_CRL_ISSUER, X509_V_ERR_UNHANDLED_CRITICAL_EXTENSION,
X509_V_ERR_KEYUSAGE_NO_CRL_SIGN, X509_V_ERR_UNHANDLED_CRITICAL_CRL_EXTENSION, X509_V_ERR_INVALID_NON_CA,
X509_V_ERR_PROXY_PATH_LENGTH_EXCEEDED, X509_V_ERR_PROXY_SUBJECT_INVALID,
X509_V_ERR_KEYUSAGE_NO_DIGITAL_SIGNATURE, X509_V_ERR_PROXY_CERTIFICATES_NOT_ALLOWED,
X509_V_ERR_INVALID_EXTENSION, X509_V_ERR_INVALID_POLICY_EXTENSION, X509_V_ERR_NO_EXPLICIT_POLICY,
X509_V_ERR_DIFFERENT_CRL_SCOPE, X509_V_ERR_UNSUPPORTED_EXTENSION_FEATURE, X509_V_ERR_UNNESTED_RESOURCE,
X509_V_ERR_PERMITTED_VIOLATION, X509_V_ERR_EXCLUDED_VIOLATION, X509_V_ERR_SUBTREE_MINMAX,
X509_V_ERR_APPLICATION_VERIFICATION, X509_V_ERR_UNSUPPORTED_CONSTRAINT_TYPE,
X509_V_ERR_UNSUPPORTED_CONSTRAINT_SYNTAX, X509_V_ERR_UNSUPPORTED_NAME_SYNTAX,
X509_V_ERR_CRL_PATH_VALIDATION_ERROR, X509_V_ERR_PATH_LOOP, X509_V_ERR_SUITE_B_INVALID_VERSION,
```

And there are other issues…

(Come to my talk tomorrow :-P.)



Will You Trust This TLS Certificate?

Perceptions of People Working in IT

Martin Ukrop
mukrop@mail.muni.cz
CRoCS, Masaryk University
Brno, Czech Republic

Lydia Kraus
lydia.kraus@fi.muni.cz
CRoCS, Masaryk University
Brno, Czech Republic

Vashek Matyas
matyas@fi.muni.cz
CRoCS, Masaryk University
Brno, Czech Republic

Heider Ahmad Mutleq Wahsheh
heider.wahsheh@unive.it
Ca' Foscari University of Venice
Venice, Italy

ABSTRACT

Flawed TLS certificates are not uncommon on the Internet. While they signal a potential issue, in most cases they have benign causes (e.g., misconfiguration or even deliberate deployment). This adds fuzziness to the decision on whether to trust a connection or not. Little is known about perceptions of flawed certificates by IT professionals, even though their decisions impact high numbers of end users. Moreover, it is unclear how much does the content of error messages and documentation influence these perceptions.

1 INTRODUCTION

Nowadays, communication protected by TLS (formerly SSL) is getting more and more prevalent on the Internet (in May 2019, over 80% of page loads in Google Chrome were done over HTTPS [20]). For the TLS infrastructure to work, end entities authenticate themselves using X.509 certificates [13]. Certificate validation errors are quite common [4, 5], although an error does not necessarily imply a security incident. For example, getting a self-signed certificate may be either an attack (adversary pretending to be a trusted site) or only

Let’s improve the situation!

x509errors.org

USABLE X.509 ERRORS

INTRO ERRORS METHODOLOGY ABOUT

Making X.509 errors usable.

Validating X.509 certificates correctly turns out to be pretty complicated (e.g. Georgiev2012). Yet certificate validation is absolutely crucial for secure communication on the Internet (think TLS).

Our goal is to simplify the ecosystem by consolidating the errors and their documentation (similarly to web documentation) and by explaining better what the validation errors mean.

Samples and documentation

For every error, we aim to provide an example certificate ( ), documentation from OpenSSL ( ) and other libraries ( ).

We plan to include the error frequency based on IP-wide scans

Multiple libraries

Our consolidated taxonomy aims for eight most used TLS-enabled libraries. The main structure is based on OpenSSL as it is by far the most used library in the domain of TLS.

Error mapping

Methodology

We extend the existing research on security, TLS and documentation design. Details are described on a

x509errors.org

Trust or chain related errors

These errors occur when the trust chain to the root certificate is not built correctly or fails.
Relevant links: Certificate Paths (RFC 5280), Certificate Revocation Lists (RFC 5280), OCSP (RFC 2560)

- X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT
- X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY
- X509_V_ERR_DEPTH_ZERO_SELF_SIGNED_CERT
- X509_V_ERR_SELF_SIGNED_CERT_IN_CHAIN
- X509_V_ERR_CERT_CHAIN_TOO_LONG
- X509_V_ERR_UNABLE_TO_GET_CRL
- X509_V_ERR_UNABLE_TO_GET_CRL_ISSUER
- X509_V_ERR_CRL_PATH_VALIDATION_ERROR

Trust or chain related errors

These errors occur when the trust chain to the root certificate is not built correctly or fails.
Relevant links: Certificate Paths (RFC 5280), Certificate Revocation Lists (RFC 5280), OCSP (RFC 2560)

- X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT
- X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY
- X509_V_ERR_DEPTH_ZERO_SELF_SIGNED_CERT
- X509_V_ERR_SELF_SIGNED_CERT_IN_CHAIN
- X509_V_ERR_CERT_CHAIN_TOO_LONG
- X509_V_ERR_UNABLE_TO_GET_CRL
- X509_V_ERR_UNABLE_TO_GET_CRL_ISSUER
- X509_V_ERR_CRL_PATH_VALIDATION_ERROR

X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY

Example certificate

Download the certificate archive. If you are interested in generating such certificate yourself, see the generating script for this case on the project GitHub. To get the validation error, run the command as indicated below.

- OpenSSL: `openssl verify endpoint.crt`
- GnuTLS: `certtool --verify --infile endpoint.crt`

OpenSSL: X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY

The issuer certificate could not be found: this occurs if the issuer certificate of an untrusted certificate cannot be found.

GnuTLS: GNUTLS_CERT_SIGNER_NOT_FOUND

The certificate's issuer is not known. This is the case if the issuer is not included in the trusted certificate list.

X509_V_ERR_DEPTH_ZERO_SELF_SIGNED_CERT

X509_V_ERR_SELF_SIGNED_CERT_IN_CHAIN

X509_V_ERR_CERT_CHAIN_TOO_LONG

X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY

Example certificate

Download the certificate archive. If you are interested in generating such certificate yourself, see the generating script for this case on the project GitHub. To get the validation error, run the command as indicated below.

- OpenSSL: `openssl verify endpoint.crt`
- GnuTLS: `certtool --verify --infile endpoint.crt`

OpenSSL: X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY

The issuer certificate could not be found: this occurs if the issuer certificate of an untrusted certificate cannot be found.

GnuTLS: GNUTLS_CERT_SIGNER_NOT_FOUND

The certificate's issuer is not known. This is the case if the issuer is not included in the trusted certificate list.

X509_V_ERR_DEPTH_ZERO_SELF_SIGNED_CERT

X509_V_ERR_SELF_SIGNED_CERT_IN_CHAIN

X509_V_ERR_CERT_CHAIN_TOO_LONG

X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY

Example certificate

Download the certificate archive. If you are interested in generating such certificate yourself, see the generating script for this case on the project GitHub. To get the validation error, run the command as indicated below.

- OpenSSL: `openssl verify endpoint.crt`
- GnuTLS: `certtool --verify --infile endpoint.crt`

OpenSSL: X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY

The issuer certificate could not be found: this occurs if the issuer certificate of an untrusted certificate cannot be found.

GnuTLS: GNUTLS_CERT_SIGNER_NOT_FOUND

The certificate's issuer is not known. This is the case if the issuer is not included in the trusted certificate list.

X509_V_ERR_DEPTH_ZERO_SELF_SIGNED_CERT

X509_V_ERR_SELF_SIGNED_CERT_IN_CHAIN

X509_V_ERR_CERT_CHAIN_TOO_LONG

Search the menus (Alt+/) 100% € % .0 .00 123 Arial 10

fx X509_V_ERR_CERT_REJECTED

	A	B	C	
6	**OpenSSL**	**GnuTLS**	**Botan**	**mbedTLS**
7	X509_V_OK		OK	
8	X509_V_ERR_UNSPECIFIED			
9	X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT			
10	X509_V_ERR_UNABLE_TO_GET_CRL		NO_REVOCATION_DATA	
11	X509_V_ERR_UNABLE_TO_DECRYPT_CERT_SIGNATURE			
12	X509_V_ERR_UNABLE_TO_DECRYPT_CRL_SIGNATURE			
13	X509_V_ERR_UNABLE_TO_DECODE_ISSUER_PUBLIC_KEY			
14	X509_V_ERR_CERT_SIGNATURE_FAILURE	GNUTLS_CERT_SIGNATURE_FAILURE	SIGNATURE_ERROR	MBEDTLS_
15	X509_V_ERR_CRL_SIGNATURE_FAILURE	GNUTLS_CERT_SIGNATURE_FAILURE	CRL_BAD_SIGNATURE	
16	X509_V_ERR_CERT_NOT_YET_VALID	GNUTLS_CERT_NOT_ACTIVATED	CERT_NOT_YET_VALID	MBEDTLS_
17	X509_V_ERR_CERT_HAS_EXPIRED	GNUTLS_CERT_EXPIRED	CERT_HAS_EXPIRED	MBEDTLS_
18	X509_V_ERR_CRL_NOT_YET_VALID	GNUTLS_CERT_REVOCATION_DATA_ISSUED_IN_FUTURE	CRL_NOT_YET_VALID	MBEDTLS_
19	X509_V_ERR_CRL_HAS_EXPIRED	GNUTLS_CERT_REVOCATION_DATA_SUPERSEDED	CRL_HAS_EXPIRED	MBEDTLS_
20	X509_V_ERR_ERROR_IN_CERT_NOT_BEFORE_FIELD			MBEDTLS_
21	X509_V_ERR_ERROR_IN_CERT_NOT_AFTER_FIELD			MBEDTLS_
22	X509_V_ERR_ERROR_IN_CRL_LAST_UPDATE_FIELD			
23	X509_V_ERR_ERROR_IN_CRL_NEXT_UPDATE_FIELD			
24	X509_V_ERR_OUT_OF_MEM			
25	X509_V_ERR_DEPTH_ZERO_SELF_SIGNED_CERT	GNUTLS_CERT_SIGNER_NOT_FOUND	CANNOT_ESTABLISH_TRUST	
26	X509_V_ERR_SELF_SIGNED_CERT_IN_CHAIN	GNUTLS_CERT_SIGNER_NOT_FOUND		
27	X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY	GNUTLS_CERT_SIGNER_NOT_FOUND	CERT_ISSUER_NOT_FOUND	
28	X509_V_ERR_UNABLE_TO_VERIFY_LEAF_SIGNATURE			
29	X509_V_ERR_CERT_CHAIN_TOO_LONG			
30	X509_V_ERR_CERT_REVOKED	GNUTLS_CERT_REVOKED		
31	X509_V_ERR_INVALID_CA	GNUTLS_CERT_SIGNER_NOT_CA		
32	X509_V_ERR_PATH_LENGTH_EXCEEDED	GNUTLS_CERT_SIGNER_CONSTRAINTS_FAILURE		
33	X509_V_ERR_INVALID_PURPOSE	GNUTLS_CERT_PURPOSE_MISMATCH		
34	X509_V_ERR_CERT_UNTRUSTED			
35	X509_V_ERR_CERT_REJECTED			

X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY

Example certificate

Download the certificate archive. If you are interested in generating such certificate yourself, see the generating script for this case on the project GitHub. To get the validation error, run the command as indicated below.

- OpenSSL: `openssl verify endpoint.crt`
- GnuTLS: `certtool --verify --infile endpoint.crt`

OpenSSL: X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY

The issuer certificate could not be found: this occurs if the issuer certificate of an untrusted certificate cannot be found.

GnuTLS: GNUTLS_CERT_SIGNER_NOT_FOUND

The certificate's issuer is not known. This is the case if the issuer is not included in the trusted certificate list.

X509_V_ERR_DEPTH_ZERO_SELF_SIGNED_CERT

X509_V_ERR_SELF_SIGNED_CERT_IN_CHAIN

X509_V_ERR_CERT_CHAIN_TOO_LONG

X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY

Example certificate

Download the certificate archive. If you are interested in generating such certificate yourself, see the generating script for this case on the project GitHub. To get the validation error, run the command as indicated below.

- OpenSSL: `openssl verify endpoint.crt`
- GnuTLS: `certtool --verify --infile endpoint.crt`

OpenSSL: X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY

The issuer certificate could not be found: this occurs if the issuer certificate of an untrusted certificate cannot be found.

GnuTLS: GNUTLS_CERT_SIGNER_NOT_FOUND

The certificate's issuer is not known. This is the case if the issuer is not included in the trusted certificate list.

Botan/NSS/JDK/...: CERT_SIGNER_NOT_FOUND

Some explanation. The certificate's issuer is not known. Or something. This is the case if the issuer is not included in the trusted certificate list.

X509_V_ERR_DEPTH_ZERO_SELF_SIGNED_CERT

X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY

Example certificate

Download the certificate archive. If you are interested in generating such certificate yourself, see the generating script for this case on the project GitHub. To get the validation error, run the command as indicated below.

- OpenSSL: `openssl verify endpoint.crt`
- GnuTLS: `certtool --verify --infile endpoint.crt`

OpenSSL: X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY

The issuer certificate could not be found: this occurs if the issuer certificate of an untrusted certificate cannot be found.

GnuTLS: GNUTLS_CERT_SIGNER_NOT_FOUND

The certificate's issuer is not known. This is the case if the issuer is not included in the trusted certificate list.

The best documenntaion :-) (tested!)

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. In hac habitasse platea dictumst quisque sagittis purus. Mauris a diam maecenas sed enim ut sem
Auctor elit sed vulputate mi sit amet mauris commodo. Odio eu feugiat pretium nibh ipsur
nunc id cursus metus aliquam. Massa eget egestas purus viverra accumsan. A pellentesque

Summary of our goals

1. Provide a useful resource for the IT professionals.
   (examples & documentation)

2. Create better documentation.
   (unify errors, simplify library transition)

3. Save time for the library developers.
   (and yet have good documentation)

Feedback welcome!

Tell me how it can be more useful.

Check out the project at

https://x509errors.org

CROCS

Centre for Research on Cryptography and Security

Martin Ukrop, mukrop@mail.muni.cz

Masaryk University, Czech Republic

Ph.D. research cooperation with Red Hat Czech

Red Hat