Will you trust this TLS certificate?

Perceptions of people working in IT

Martin Ukrop, Lydia Kraus, Vashek Matyas, Heider Wahsheh

ACSAC 2019, 13. 12. 2019

Martin Ukrop, mukrop@mail.muni.cz
Masaryk University, Czech Republic
Ph.D. research cooperation with Red Hat Czech
8:03
The phone beeps.
A text comes.
38 minutes pass...
MISSILE ALERT IN ERROR
THERE IS NO THREAT
Cause? Bad warning system UI!

1. State EOC

- PACOM (CDW) - STATE ONLY
- BMD False Alarm
- Amber Alert (CAE) - Kauai County Only
- Amber Alert (CAE) Statewide
- 1. TEST Message
- PACOM (CDW) - STATE ONLY
- Tsunami Warning (CEM) - STATE ONLY
- DRILL-PACOM (DEMO) STATE ONLY
- Landslide - Hana Road Closure
- Amber Alert DEMO TEST
- High Surf Warning North Shores
Oh, yes.
Bad user interface.

Nothing to do with security...
Ever heard of encrypted email? (being usable and secure)

15 reasons not to start using PGP

Because of popular demand, here’s the collection of reasons to prefer more advanced cryptographic communications tools and stop investing in the old PGP over e-mail architecture, the problem mostly being e-mail rather than PGP.

Pretty Good Privacy is better than nothing, and it is also better than relying on encryption services between the mail servers while it is up and running. So it is still a good choice for professional mail and business mail, but it is not a secure communication medium.

The text concludes mentioning some key differences between PGP and e-mail, but it is not about not using encryption, but about the intellectual trap of giving back to date.

1. Downgrade Attack: The

It’s Time To Drop PGP

"Email is no longer a secure communication medium."

Schinzel

Schneier on Security

Giving Up on PGP

Filippo Valsorda wrote an excellent essay on why he’s giving up on PGP. I have long believed PGP to be more trouble than it is worth. It’s hard to use correctly, and easy to get wrong. More generally, e-mail is inherently difficult to secure because of all the different things we ask of it and use it for.

Valsorda has a different complaint, that its long-term secrets are an unnecessary source of risk.
Ever heard of encrypted email? (being usable and secure)

Why Johnny Can’t Encrypt

A Usability Evaluation of PGP 5.0

ALMA WHITTEN AND J. D. TYGAR

Why Johnny Still Can’t Encrypt: Evaluating the Usability of Email Encryption Software

Steve Sheng
Engineering and Public Policy
Carnegie Mellon University
shengx@cmu.edu

Levi Broderick
Electrical and Computer Engineering
Carnegie Mellon University
lpb@ece.cmu.edu

Colleen Alison Koranda
HCI Institute
Carnegie Mellon University
ckoranda@andrew.cmu.edu

Why Johnny Still, Still Can’t Encrypt: Evaluating the Usability of a Modern PGP Client

Scott Ruoti, Jeff Andersen, Daniel Zappala, Kent Seamons
Brigham Young University
{ruoti, andersen} @ isl.byu.edu, {zappala, seamons} @ cs.byu.edu
Oh, yes.
Those careless end users.

IT professionals know their way...
Eduroam certificate checking
(also far from ideal)

A Practical Investigation of Identity Theft Vulnerabilities in Eduroam

Sebastian Brenza
Horst-Görtz Institute for IT-Security
Ruhr-University Bochum
Bochum, Germany
sebastian.benza@rub.de

Andre Pawlowski
Horst-Görtz Institute for IT-Security
Ruhr-University Bochum
Bochum, Germany
andre.pawlowski@rub.de

Eduroam configuration changes 2019

The widespread service eduroam uses for the protection of user data an encryption based on digital certificates.

These certificates have a limited duration.

The certificate of the highest issuing institution, the so-called root certificate, expired on 09 July 2019 at 23:59 GMT. Therefore, no longer valid certificates are possible in this infrastructure and a conversion is mandatory for all until then so that eduroam can continue to be used.

Affected users

All eduroam users of the DKFZ, but also eduroam users of other German institutions, must urgently adapt their eduroam configuration. This is a general problem that affects the entire German eduroam infrastructure. In parallel to the existing authentication infrastructure, the ITCF has developed a new one, that can be used via a different configuration of the mobile devices.
I need to validate this certificate...

[user@santacrypt ~]$ openssl verify cert-chain.pem
I need to validate this certificate...

[user@santacrypt ~]$ openssl verify cert-chain.pem

CN = secret.devconf.cz, O = TNS Inc., C = CZ
error 47 at 0 depth lookup:
   permitted subtree violation
error cert-chain.pem: verification failed
Solution 1:

“The user should know!”

Not My Problem
Solution 2:

“Let’s investigate, understand it and decide!”

Verify certificates using OpenSSL

I created 2 intermediate certificates called cert1.crt and cert2.crt signed by a common cert0 root and i need to verify them using verify command.

I type:

```
verify -CAfile cert1.crt cert2.crt
```

What I get is:

Hostname validation

OpenSSL 1.1.0 provides built-in functionality for hostname validation since January, 2015. Its been available in Master since then.

One common mistake made by users of OpenSSL Versions prior to 1.0.2 did not perform hostname validation. This require the user to call a few functions to set it up.

A man page on hostname validation has been available.

Example Usage
But there are MANY possible errors...

[user@santacrypt ~]$ man openssl verify | grep ...

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_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_CERTIFICATE_TYPE,
X509_V_ERR_UNSUPPORTED_NAME_SYNTAX, X509_V_ERR_UNSUPPORTED_EXTENSION_SYNTAX,
Problem statement

• How do people in IT perceive certificate flaws?
  – Do they understand the cause?
  – Do they see the (security) consequences?
  – Further complication: Sometimes deliberate deployment of invalid TLS certificates...
Problem statement

• How do people in IT perceive certificate flaws?
  – Do they understand the cause?
  – Do they see the (security) consequences?
  – Further complication: Sometimes deliberate deployment of invalid TLS certificates...

• How do error messages help comprehension?
  – Do they matter much? Can they be better?
So we asked 75 developers at DEVCONF 2018.
Task procedure (simplified)

1. When implementing the TLS connection, you get a certificate validation error.
Task procedure (simplified)

1. When implementing the TLS connection, you get a certificate validation error.
2. Investigate. (Do whatever you would do.)
Task procedure (simplified)

1. When implementing the TLS connection, you get a certificate validation error.

2. Investigate. (Do whatever you would do.)

3. How much do you trust the this certificate?
Task procedure (simplified)

1. When implementing the TLS connection, you get a certificate validation error.
2. Investigate. (Do whatever you would do.)
3. How much do you trust the this certificate?
4. Describe (in your own words) what was the problem with the certificate.
Experiment overview

- 75 participants (67 recorded interviews)
  - 95% employed in IT (median 8 years)
  - 67% have formal education in IT
Experiment overview

- 75 participants (67 recorded interviews)
  - 95% employed in IT (median 8 years)
  - 67% have formal education in IT

- 5 different certificate cases
  - Hostname mismatch, self-signed, expired, name-constrained, OK (control)
Selected conclusions

So, what perceptions do people in IT have? (w.r.t. certificate flaws)
Trust decisions

**Ideal security viewpoint:** Binary trust.

- Validation OK → trusted
- Validation NOK → not trusted
Trust decisions

Ideal security viewpoint: Binary trust.
- Validation OK → trusted
- Validation NOK → not trusted

Real world viewpoint: It’s complicated...
- Expired yesterday → “Looks OK.”
- Expired 14 days ago → “Looks suspicious.”
- Small company → “Self-signed probably OK.”
- Other trust factors...
Over-trusted cases I.

Self-signed certificate

- Certificate correctly signed “by itself”
- Practically no assurances provided
Over-trusted cases I.

Self-signed certificate
• Certificate correctly signed “by itself”
• Practically no assurances provided

Participant opinions
• 21% say “looks OK” or better!
• Confused by the (technically) correct signature
• Trust comparable to expired certificate
Over-trusted cases II.

Name-constrained certificate

- The issuing authority was prohibited to do this
- Problem (attack!?) on the authority level!
Over-trusted cases II.

Name-constrained certificate
• The issuing authority was prohibited to do this
• Problem (attack!?) on the authority level!

Participant opinions
• 20% say “looks OK” or better!
• Error message particularly unhelpful
• Little resources available
Idea: Documentation redesign

A: “Original errors”

- 44 participants
- Real errors from OpenSSL 1.1.0g-fips (currently most used)

error 47 at 1 depth lookup: permitted subtree violation
Idea: Documentation redesign

B: “Redesigned errors”
- 31 participants
- Re-worded errors
- Link to documentation
- Improved documentation

The subject name violates constraints set by CA.

(X509_ERR_NAME_CONSTRAINTS_VIOLATION, see https://x509errors.cz)
Documentation redesign

• Generally comparable
  – Comprehension, less googling, slightly lower times

• Self-signed
  – Sig. lower perceived trust (mean 2.32→1.35 of 1–5)

• Name-constrained
  – Lower perceived trust
  – Better comprehension (14%→33% participants)
  – Less Internet browsing (72%→45% participants)
Link in the error message

...see https://x509errors.cz)
Link in the error message

...see https://x509errors.cz

- Clicked often!
  - 71% of the participants
  - Clicked for multiple cases (mean 4, median 5)

- Nice opportunity to point users to a useful place
Applications & future work

• Embrace the complexity
  – Don’t pretend the world is binary
Applications & future work

• Embrace the complexity
  – Don’t pretend the world is binary

• Look into the situation in other libraries
  – Compare errors and documentation
Applications & future work

- Embrace the complexity
  - Don’t pretend the world is binary

- Look into the situation in other libraries
  - Compare errors and documentation

- Create better documentation
  - Get it to the libraries
Investigating the perception of cert. flaws

- Empirical experiment
  - 5 certificate errors (OpenSSL vs. redesigned)
  - 75 IT professionals at DevConf 2018
Investigating the perception of cert. flaws

• Empirical experiment
  – 5 certificate errors (OpenSSL vs. redesigned)
  – 75 IT professionals at DevConf 2018

• Trust perceptions
  – Non-binary, some misunderstood, some over-trusted
Investigating the perception of cert. flaws

• Empirical experiment
  – 5 certificate errors (OpenSSL vs. redesigned)
  – 75 IT professionals at DevConf 2018

• Trust perceptions
  – Non-binary, some misunderstood, some over-trusted

• Redesigned documentation
  – Reformulating errors (& docs) matters
  – Links in errors are clicked
Usable security may still be unusual...

We use TLS certificate validation as a real-world example to spark conversation on usable security and developer experience. This research is a part of the academic cooperation of Red Hat and Masaryk University.
Usable security may still be unusual...

We use TLS certificate validation as a real-world example to spark conversation on usable security and developer experience. This research is a part of the academic cooperation of Red Hat and Masaryk University.

It seems that the noun security might combine better with an adjective other than usable. Consider rewriting this word pair or choosing a synonym for usable.
May your software always be usable!
(and secure!)

Paper details and artifacts at
crocs.fi.muni.cz/papers/acsac2019

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