PA193 Secure coding principles and practices

Seminar 10: Usable security APIs

23. 10. 2017

redhat

Martin Ukrop, mukrop@mail.muni.cz

Ph.D. research cooperation

CRoCS, Faculty of Informatics, Masaryk University

CRoCS

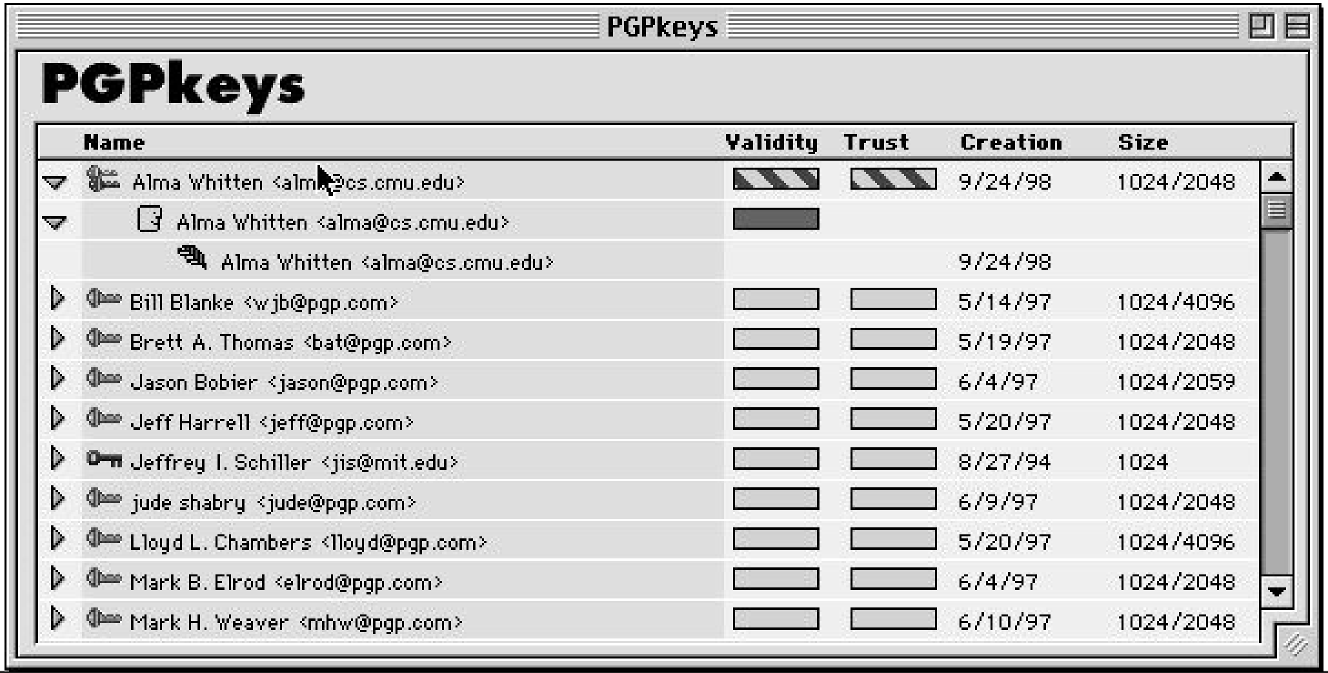
Centre for Research on
Cryptography and Security

Seminar overview

- What is usable security?
- Usable security for developers
- Seminar task
- Research background
- Homework overview
- Homework work

Usable security: How it all began

- "Why Johny can't encrypt" (A. Whitten and J. D. Tygar, 1999)
  - A usability study of PGP 5.0
  - 33% success, 25% exposed private



PGPkeys

PGPkeys

Name	Validity	Trust	Creation	Size
Alma Whitten <alma@cs.cmu.edu>	▨	▨	9/24/98	1024/2048
Alma Whitten <alma@cs.cmu.edu>	■			
Alma Whitten <alma@cs.cmu.edu>			9/24/98	
Bill Blanke <wjb@pgp.com>	□	□	5/14/97	1024/4096
Brett A. Thomas <bat@pgp.com>	□	□	5/19/97	1024/2048
Jason Bobier <jason@pgp.com>	□	□	6/4/97	1024/2059
Jeff Harrell <jeff@pgp.com>	□	□	5/20/97	1024/2048
Jeffrey I. Schiller <jis@mit.edu>	□	□	8/27/94	1024
jude shabry <jude@pgp.com>	□	□	6/9/97	1024/2048
Lloyd L. Chambers <lloyd@pgp.com>	□	□	5/20/97	1024/4096
Mark B. Elrod <elrod@pgp.com>	□	□	6/4/97	1024/2048
Mark H. Weaver <mhw@pgp.com>	□	□	6/10/97	1024/2048

Users are not the enemy

- M. A. Sasse and A. Adams, 1999
  - Study of password authentication
- Consensus at the time:
  - Users are careless and unmotivated (security-wise)
  - Users lack security knowledge
- Promoting “user-centered approach”
  - Work practices? Multiple accounts? Reasons?

Usability matters: SSL validation

- Libcurl
  - the multiprotocol file transfer library

- Two main directives for SSL validation
  - `CURL_SSL_VERIFYPEER` (checking certificate)
  - `CURL_SSL_VERIFYHOST` (checking hostname)

Usability matters: SSL validation

- PayPal SDK:

```
curl_setopt($ch, CURLL_SSL_VERIFYPEER, FALSE)

curl_setopt($ch, CURL_SSL_VERIFYHOST, FALSE)
```

Usability matters: SSL validation

- PayPal SDK: version from 27th April 2012

```
curl_setopt($ch, CURL_SSL_VERIFYPEER, TRUE)

curl_setopt($ch, CURL_SSL_VERIFYHOST, TRUE)
```

- **`Bool`** `CURL_SSL_VERIFYPEER`
- **`Int`** `CURL_SSL_VERIFYHOST`
  - 0: no host verification
  - 1: debug (nearly no verification)
  - 2: verify hostname

Encrypt-then-MAC / MAC-and-encrypt?

- In what order to perform encryption/MAC?
  - 4 possibilities
  - 1 always right, 1 depends, 2 always wrong
- NaCl/libsodium approach (crypto_box API)
  - c = crypto_box(m, n, pk, sk);
  - m = crypto_box_open(c, n, pk, sk);
- Similar issues elsewhere
  - Primitives selection, defaults, padding, randomness, ...

Usability for developers

- *“It is very easy to accidentally combine secure encryption schemes with secure MACs and still get insecure authenticated encryption schemes.”* Tadayoshi Kohno, John Viega & Doug Whiting (2003)

- Crypto that is usable for developers, admins, ...
  - Also end-users in a way

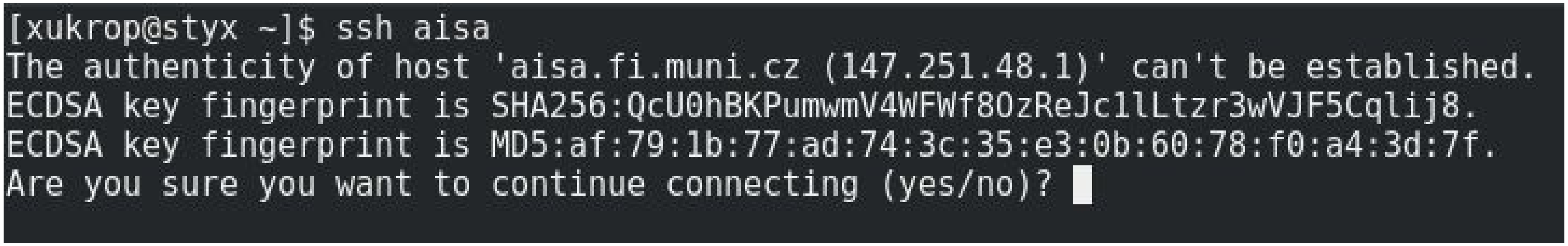
"Developer-resistant cryptography!"

K. Cairns and G. Steel, 2014

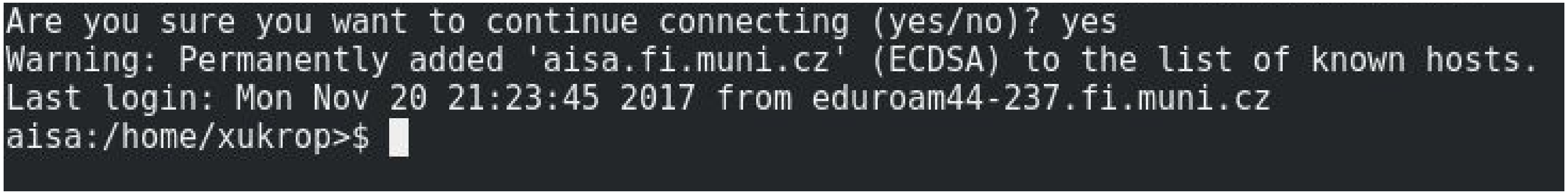
Documentation

- Good/bad documentation can do a lot!
- Research shows even “usable” cryptolibs may have bad results
- What should be in a good documentation?

SSH: Authenticity can’t be established

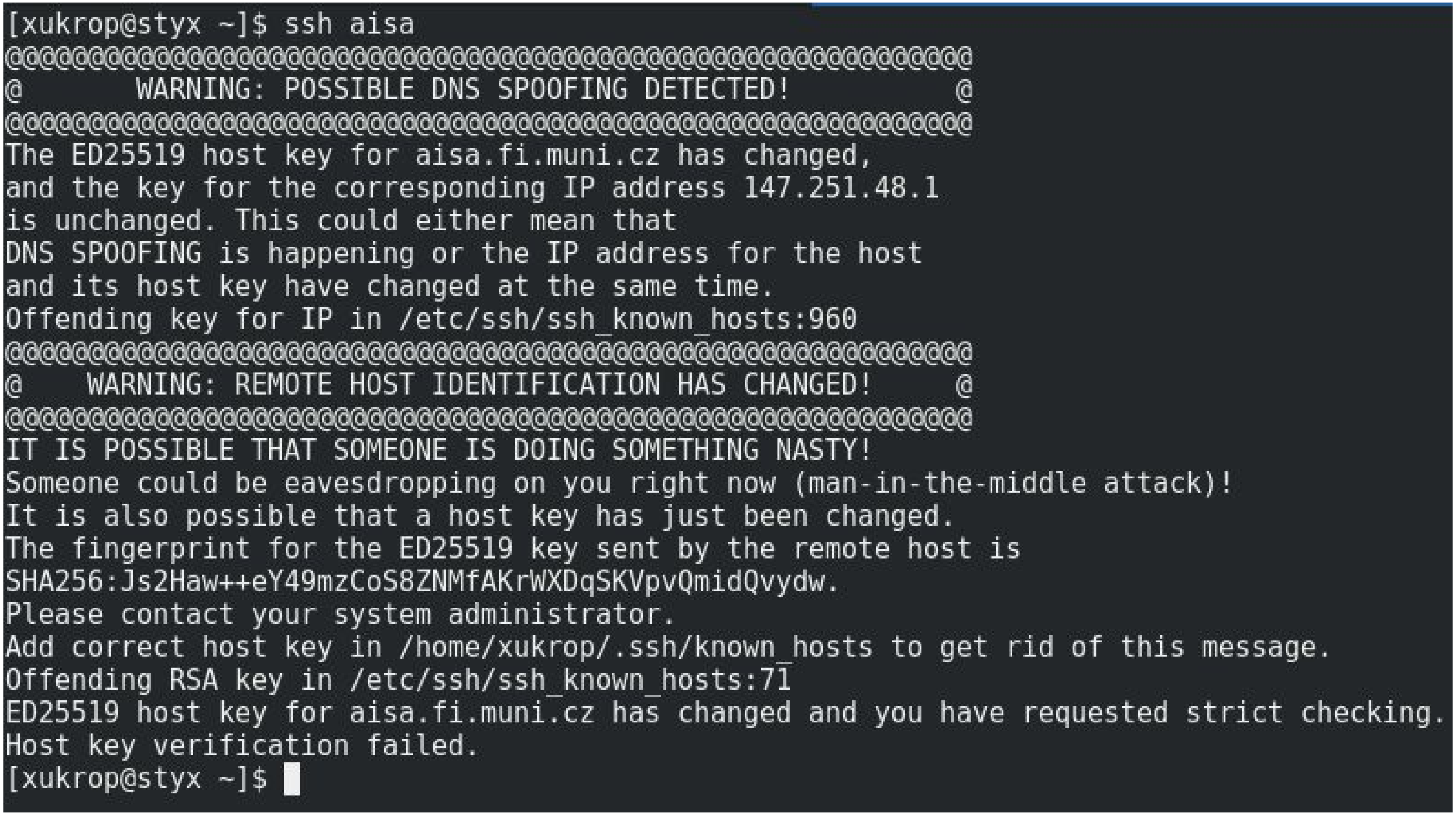


```
[xukrop@styx ~]$ ssh aisa
The authenticity of host 'aisa.fi.muni.cz (147.251.48.1)' can't be established.
ECDSA key fingerprint is SHA256:QcU0hBKPumwmV4WFWf8OzReJc1lLtzr3wVJF5Cqlij8.
ECDSA key fingerprint is MD5:af:79:1b:77:ad:74:3c:35:e3:0b:60:78:f0:a4:3d:7f.
Are you sure you want to continue connecting (yes/no)?
```



```
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'aisa.fi.muni.cz' (ECDSA) to the list of known hosts.
Last login: Mon Nov 20 21:23:45 2017 from eduroam44-237.fi.muni.cz
aisa:/home/xukrop>$
```

SSH: Key changed



```
[xukrop@styx ~]$ ssh aisa
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@       WARNING: POSSIBLE DNS SPOOFING DETECTED!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
The ED25519 host key for aisa.fi.muni.cz has changed,
and the key for the corresponding IP address 147.251.48.1
is unchanged. This could either mean that
DNS SPOOFING is happening or the IP address for the host
and its host key have changed at the same time.
Offending key for IP in /etc/ssh/ssh_known_hosts:960
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the ED25519 key sent by the remote host is
SHA256:Js2Haw++eY49mzCoS8ZNMfAKrWXDqSKVpvQmidQvydw.
Please contact your system administrator.
Add correct host key in /home/xukrop/.ssh/known_hosts to get rid of this message.
Offending RSA key in /etc/ssh/ssh_known_hosts:71
ED25519 host key for aisa.fi.muni.cz has changed and you have requested strict checking.
Host key verification failed.
[xukrop@styx ~]$ █
```

Research: Security implications

“What are security implications of bad usability?”

- OpenSSL:
  - Widely used cryptographic library
  - Anecdotally tragic usability

OpenSSL

Cryptography and SSL/TLS Toolkit

Sminar task (~15 minutes)

- X.509 errors interpretation
  - What do you think?
  - Debriefing after you make an opinion
- Fill in the “Initial questionnaire” in IS
  - 15–20 minutes, work alone
- Data for research!
  - Anonymous (identities stripped after HW evaluation)

Preliminary research results

- Homework on VUT KRY, MU PV079
- 100 certificates, trust assessment
- Interesting points (trust scale 1–4):

– Valid:	1.05	(1–2)
– SHA-1:	2.52	(2–4)
– 512bit RSA:	2.56	(2–4)
– Name ‘*’:	3.17	(2–4)
– Domain mismatch:	3.27	(2–4)
– Expired:	3.36	(2–4)
– Name empty:	3.38	(3–4)
– Revoked:	4.00	(4)

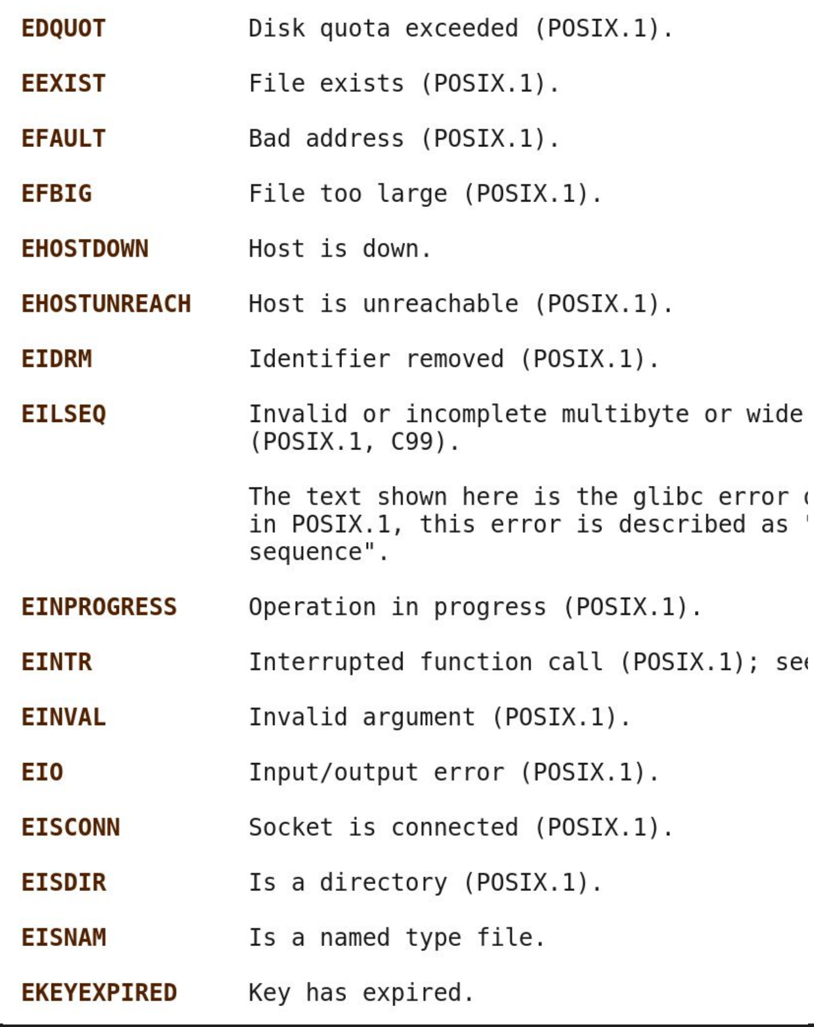
Error messages: The problem

- *“People do not understand the security implications from error messages.”*
  - Often confusing, misleading
  - (Think of the performed experiments.)
- Developer perspective:
  - Formulating error details is left on developers.
  - No standard exists.

Error messages: What can be done?

- Standardization!
  - Understandable (testing)
  - Ease for developers

- Existing case: ERRNO (POSIX)



EDQUOT	Disk quota exceeded (POSIX.1).
EEXIST	File exists (POSIX.1).
EFAULT	Bad address (POSIX.1).
EFBIG	File too large (POSIX.1).
EHOSTDOWN	Host is down.
EHOSTUNREACH	Host is unreachable (POSIX.1).
EIDRM	Identifier removed (POSIX.1).
EILSEQ	Invalid or incomplete multibyte or wide (POSIX.1, C99). The text shown here is the glibc error in POSIX.1, this error is described as sequence".
EINPROGRESS	Operation in progress (POSIX.1).
EINTR	Interrupted function call (POSIX.1); se
EINVAL	Invalid argument (POSIX.1).
EIO	Input/output error (POSIX.1).
EISCONN	Socket is connected (POSIX.1).
EISDIR	Is a directory (POSIX.1).
EISNAM	Is a named type file.
EKEYEXPIRED	Key has expired.

Homework assignment

Writing documentation that conveys security consequences

Homework phase I.

- Study 2 given validation errors in detail
  - Problem? Cause? Consequences? Elimination?
  - Track resources you used
- Write usable documentation for these cases
  - Intended for developers that are not security experts
  - Fill into the prepared structure in gDoc
- (Seminar: Give overview of the gDoc structure)

Homework phase II.

- Read the documentation for 2 other variants
  - Written by other students
- Give and get feedback
  - What is good? Why? What should be better?
- Compare and choose the best

Homework summary

- Initial questionnaire in IS
  - During the seminar
- Phase 1 (create usable documentation)
  - Fill in provided gDocs (links in IS notepad)
  - Deadline: Thu 30. 11. 2017 23:59
- Phase 2 (evaluation & voting)
  - Comments in gDocs, questionnaire in IS
  - Deadline: Thu 7. 12. 2017 23:59
- 5 points (+1 bonus for best solutions)

Look briefly into your HW cases now.

So as not to spent 5 hours finding out what the problem is.

The point is elsewhere :-}.