PA193 - Secure coding principles and practices

Designing good and secure API

Martin Ukrop, mukrop@mail.muni.cz
Lenka Horáková, 396249@mail.muni.cz

CROCS
Centre for Research on Cryptography and Security

Usability

- Usability
  - The ease of use and learnability of a human-made object such as a tool or device.
- Usability (software engineering)
  - The degree to which a software can be used by specified consumers to achieve quantified objectives with effectiveness, efficiency, and satisfaction in a quantified context of use.

Usability research in IT

- Why Johny can't encrypt
  - A usability study of PGP 5.0
  - A. Whitten and J. D. Tygar, 1999
- Users Are Not the Enemy
  - A. Adams and M. A. Sasse, 1999
- Why Johny Still, Still Can't Encrypt
  - Evaluating the Usability of a Modern PGP Client
  - S. Ruoti et allii, 2015

SSL certificates validation

- cURL (libcurl)
  - PayPal SKD version prior to 2012

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

  - PayPal SDK version from 27th April 2012 (“fixed”)

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

  - Amazon Flexible Payment Service, ZenCart, Apache, ...

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, ...

“Developer-resistant cryptography”

- *“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, administrators, …*
  - *Also end-users in a way*

Seminar work

- Compare CLI tools of GnuTLS and NSS
- Navigate to lenkahorakova.sk
  - Use your UCO, password “testing2016”
  - Follow instructions on the website
  - Shut down the virtual machine at the end

Homework (part 1)

- Perform the tasks from the seminar using OpenSSL
  - The accompanying Google Form: goo.gl/w92RL1
  - Upload the created certificate to homework vault

Homework (part 2)

- Write a report comparing the interface of GnuTLS, NSS and OpenSSL's command line utilities
  - Your overall impression of the interfaces of these tools.
  - Concrete examples of good/bad things about each library (anything from API to the documentation). Try to cover all 3 libraries and highlight both positive and negative aspects.
  - Discuss possible security implications of the interface/documentation design.
  - Give at least 3 concrete suggestions on how to improve the interface of the mentioned tools.

Homework (general notes)

- Deadline: 1. 12. 2016 23:59 (full number of 7 points)
  - Every additional 24h started means 2 points penalization
  - It is strongly advised to do it sooner, you'll benefit from remembering the seminar work.
- Upload your solution to IS homework vault
  - Created certificate + report
- Collaboration is not allowed
  - Think and formulate the comparison and improvements independently.