PB173 - Tématický vývoj aplikací v C/C++ (podzim 2014)
Domain specific development in C/C++

Skupina: Aplikovaná kryptografie a bezpečné programování

https://is.muni.cz/auth/predmety/uplny_vypis.pl?fakulta=1433;obdobi=6184;predmet=788705

Petr Švenda svenda@fi.muni.cz

Konzultace: A406, Pondělí 15-15:50

CROCS
Centre for Research on Cryptography and Security

Some t me..

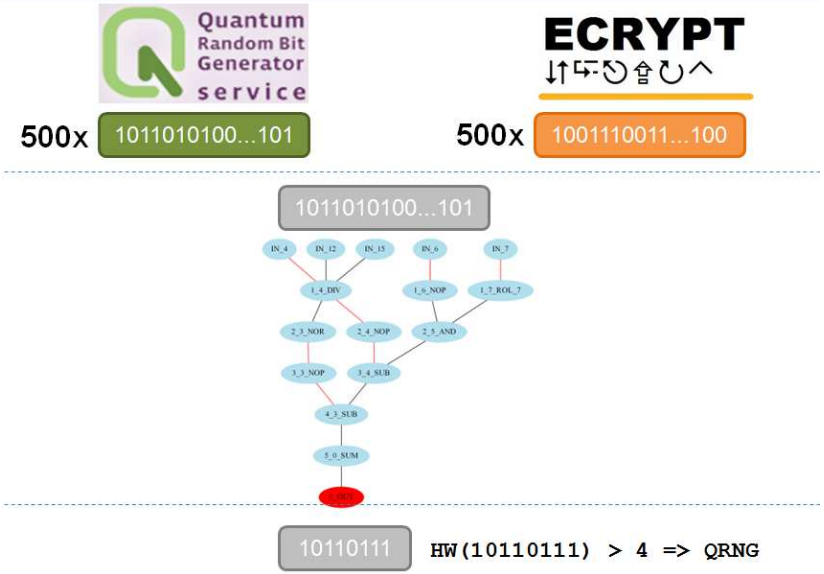
Genetic programming

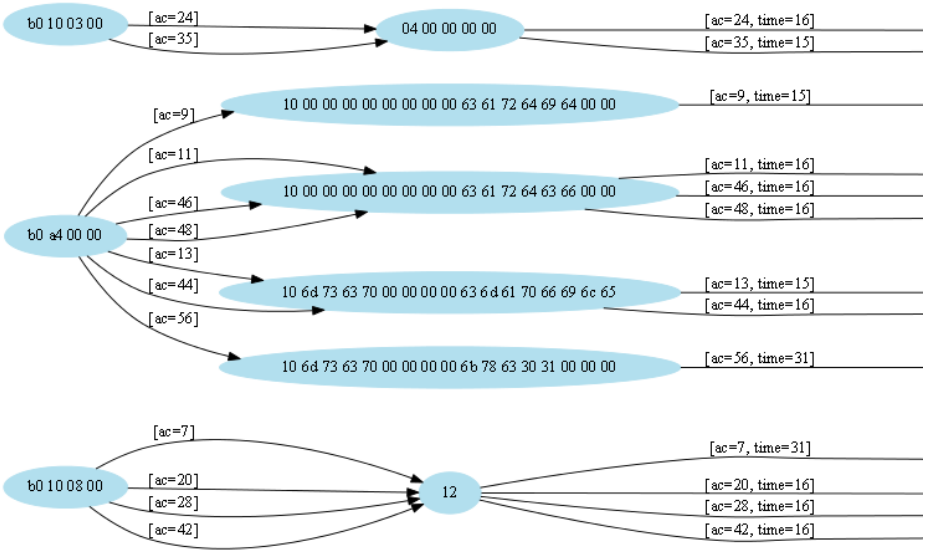
+

Distributed computing

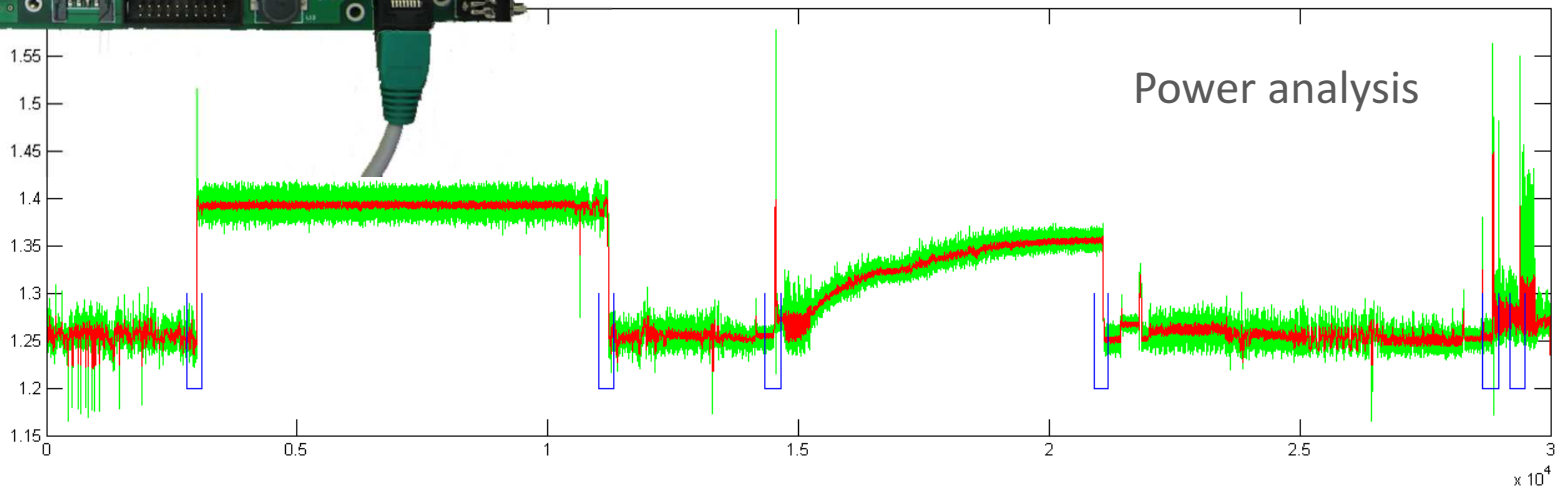
Secrecy amplification protocols for WSN

Random distinguisher for crypto fncs

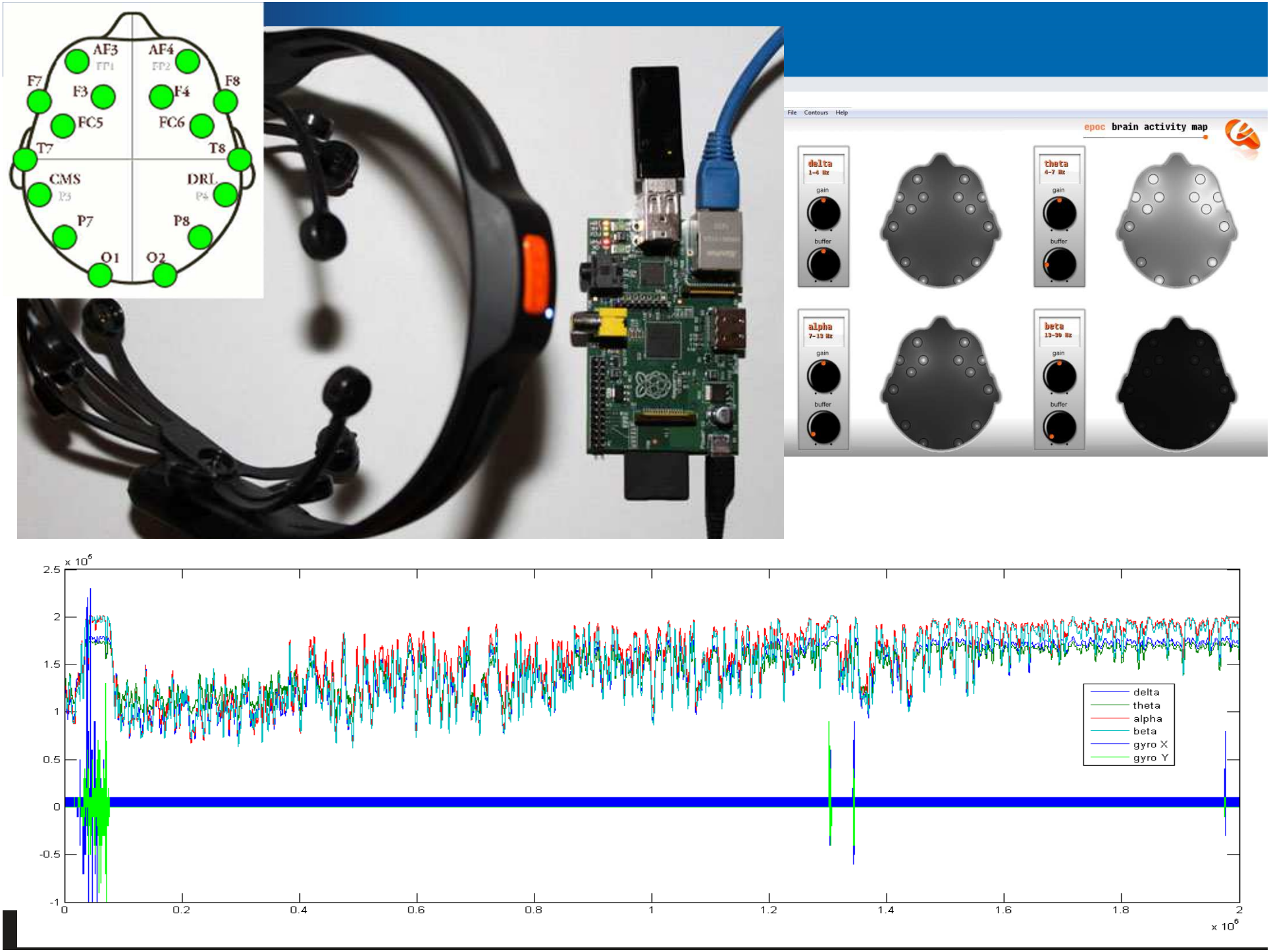




Security programming



Power analysis


AF3
AF4
F7
F3
F4
F8
FC5
FC6
T7
T8
CMS
DRL
P7
P8
O1
O2
File Contours Help
epoc brain activity map
delta
1-4 Hz
theta
4-7 Hz
alpha
7-13 Hz
beta
13-30 Hz
gain
buffer
x 10^6
2.5
2
1.5
1
0.5
0
-0.5
-1
0
0.2
0.4
0.6
0.8
1
1.2
1.4
1.6
1.8
2
x 10^6
delta
theta
alpha
beta
gyro X
gyro Y

http://astrolight.cz

M45 Pleiades star cluster and reflection nebula

Petr Švenda, http://www.
Equinox 80EDP 500m
Canon 400D IRmod @

NGC7000 in Cygnus

Saturn 30.6.2012

Petr Švenda, http://astrolight.cz
SW Orion 120/1000mm, stack 900 frames

The Sun 11.12.2011 (H-Alpha)

Petr Švenda, http://astrolight.cz, 11.12.2011
Solarscope Solarview 50mm 0,7Å, Canon 500D, 105 stack

ORGANIZAČNÍ INFORMACE

Co je cílem předmětu

- Získat zkušenosti s implementací většího programu
- Používat vývojové nástroje
- Naučit se dobré programátorské postupy
  - programování obecně
  - ale speciálně v oblasti bezpečnostních aplikací
- Získat praktické postřehy z implementací kryptografických aplikací
  - co nakonec ve firmě vyžadují

Co není cílem předmětu

- Detailní ovládnutí konkrétní technologie
  - zabrousíme do různých oblastí
- Pokročilé zvládnutí celého vývojového procesu
  - to jednoduše nestihneme
- Vysvětlovat základy kryptografie nebo srovnávat všechny možné varianty řešení problému
  - hlavně se budeme snažit prakticky programovat

Organizační

- Formality výuky
  - každotýdenní dvojhodinovka
  - evidovaná účast, 2 neúčasti bez omluvení OK
- Způsob výuky
  - max. cca 30 min./týdně úvod do problematiky
  - zbytek programování přímo na hodině
  - z mé strany průběžná konzultace nad vznikajícími problémy
  - default Windows (ale můžete pracovat i na jiné platformě)
- Samostatná práce
  - v týmech, průběžná tvorba většího projektu
  - dodělávání práce z hodiny
  - pravidelné bodované předvádění stavu projektu (každé cvičení)

Organizační (2)

- Používané nástroje
  - IDE, verzovací nástroje, Doxygen, debugger, analýza a kontrola kódu
  - konkrétní není striktně dané – použijte svoje oblíbené
  - default Visual Studio
- Hodnocení
  - účast
  - průběžná práce (10 bodů týdně)
  - prezentace celého projektu (30 bodů)
  - možné bonusy
  - max. 150 bodů, zisk alespoň 100 bodů na kolokvium

Rozdělení do týmů

- 2-3 osoby
- Společná práce, ale každý prezentuje svůj přínos
  - Iniciální prezentace domácího úkolu na dalším cvičení
  - zapracování připomínek, prezentace a hodnocení na dalším cvičení
- Využití sdíleného repozitáře (GitHub) + CI (Travis)
- Rozdělení provedeme až po 14 dnech
  - ustálení zapsaných studentů

Celkový přehled

- Základní podklady v ISu (interaktivní materiály)
  - PB173→Interaktivní osnovy → **Aplikovaná kryptografie a bezpečné programování (vyučující Petr Švenda)**
- Může se ale částečně měnit
  - uvidíme dle reálné obtížnosti, rychlosti postupu a zájmu
- Můžete otevřít vlastní řešený problém!

Twitter

- Twitter
  - https://twitter.com/rngsec
  - zveřejnění přípravy a slidů, občasné info
  - hash tag **#pb173_2014**
  - (opravdu důležité věci budou rozesílány hromadně na IS mail)
- Scribd
  - slidy zveřejňovány v IS materiálech i na Scribd.com
  - navíc možnost vkládání poznámek, připomínek, nejasností...

How good YOU are in English?

Apology all my mistakes, please.

Organization

- Seminars + assignments + project
- Assignments
  - Assigned regularly (nearly) every week
  - Initial assigments individual work
  - Most of assignments team work
  - expected workload: 4+ hours/week/participant
  - Network lab available to students
- Project: secure videoconferencing architecture

Attendance

- Seminars
  - Attendance obligatory
  - Absences must be excused at the department of study affairs
  - 2 absences are ok
- Assignments and projects
  - Partially done at seminar
  - Completed during students free time (e.g. at the dormitory)
  - Access to network lab and CRoCS lab is possible
  - Cooperation between team members necessary

Course resources

- Slides (PDF) available in IS
  - IS = Information System of the Masaryk University
- PB173→Interactive syllabi→ **Aplikovaná kryptografie a bezpečné programování (vyučující Petr Švenda)**
- Assignments (what to do) available in IS
  - Submissions done also via IS
- Additional tutorials/papers/materials from time to time will also be provided in IS
  - To better understand the issues discussed
- Recommended literatures

Plagiarism

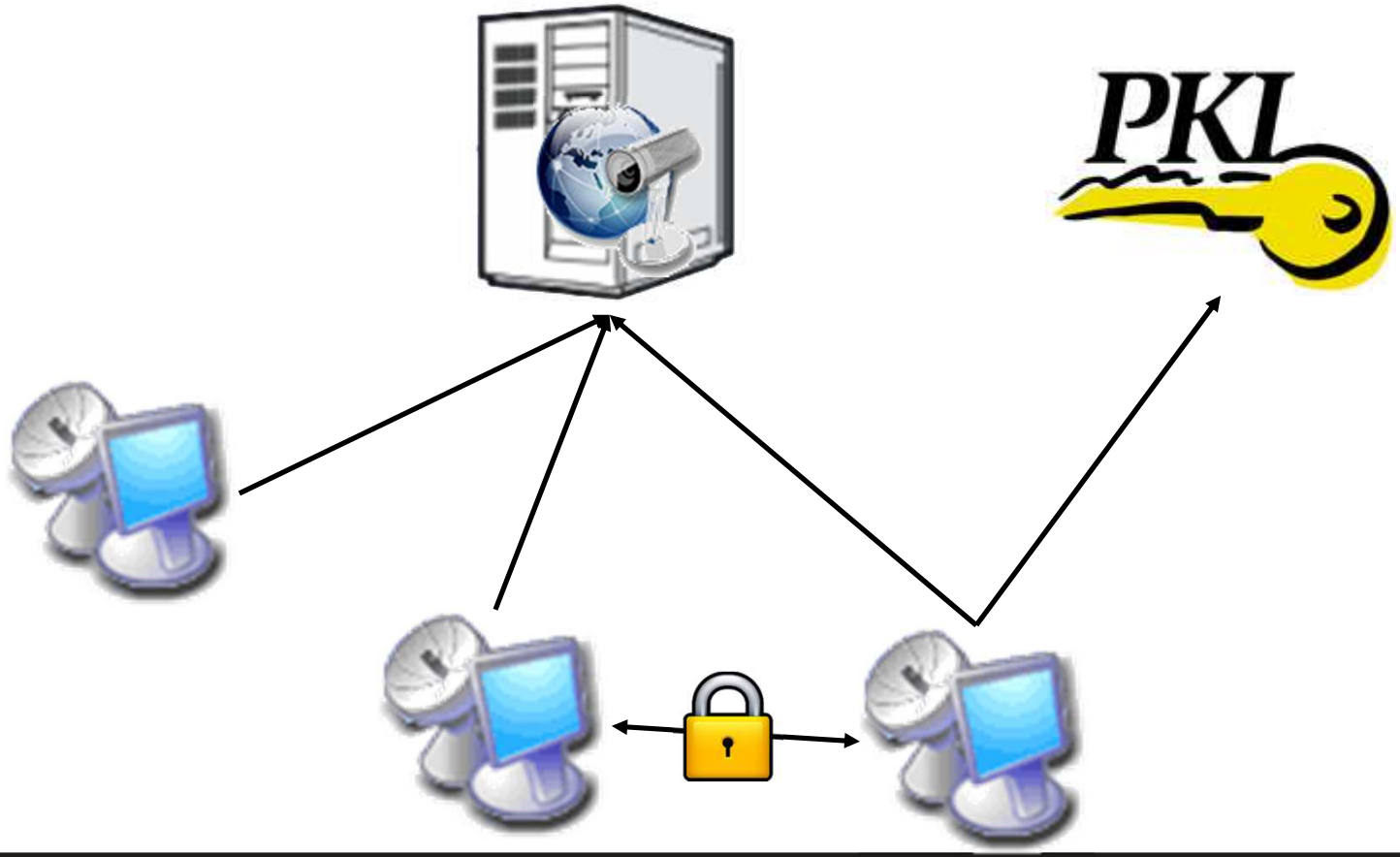
- Projects
  - Must be worked out by a team of 3 students
  - Every team member must show his/her contribution
- Plagiarism, cut&paste, etc. is not tolerated
  - Plagiarism is use of somebody else words/programs or ideas without proper citation
  - IS helps to recognize plagiarism
  - If plagiarism is detected student is assigned -5 points
  - In more serious cases the Disciplinary committee of the faculty will decide

Short questionnaire

- Do you know difference between symmetric and asymmetric cryptography?
- Do you known difference between block and stream cipher?
- Do you know DES and AES algorithm?
- Do you know ECB and CBC encryption mode?
- Do you know principle of hash functions?
- Do you know MD5 and SHA-1 algorithm?
- Do you known concept of digital signature?

"Theme" project

- Secure videoconferencing architecture



"Theme" project

- Certification authority
  - validates and issue user certificates
- Videoconferencing server
  - register and faciliate connection between users
- Client
  - provides operations related to end user usage

- Main focus on solving parts of the architecture

"Theme" project – some details

- Users obtains certificate of identity from Certification authority
- Users register with Videoconferencing server
- Videoconferencing server provides list of connected users, help to establish video connection and charge fee based on call length
- Client maintains user identity, related keys and provides high speed encryption of audio/video stream

Cryptographic libraries

Do not implement your own algorithms

- Time consuming (someone probably already did that before)
- Functional problems
- Low performance
- Security problems due to bugs
- Security problems due to missing defense against implementation attacks

Use well-known implementations

- Use well-known libraries
  - OpenSSL, PolarSSL, GnuPG, BouncyCastle (Java)
- Or implementation of algorithms from well-established authors
  - Brian Gladman, Eric A. Young …

Complexity matters

- Complexity of library implementation should match your needs
  - usually, you need only one or two algorithms
- Multiprocessor or CPU-independent implementation can be overkill
  - and just increase risk of error
- Do you really need library with object-oriented design?

Complexity matters (2)

- Large libraries are not always the most suitable ones
- OpenSSL is complex and interconnected
  - e.g., AES is extractable much easier from PolarSSL then from OpenSSL

Code authenticity

- Source code signature
  - Do you really have original source codes?
  - MD5/SHA1 hash (where to get “correct” hash value?)
  - GPG/PGP
- Generate your own GPG/PGP signature keys
  - use them for inter-team communication
  - sign your code releases

Resilience against bugs

- Do not design algorithms/protocols by yourself
- Try to find existing standards
  - NIST, RSA PKCS, RFC, ISO/ANSI
- Try not to deviate from standards
  - compatibility and compliance
  - no need for (time consuming) specification of detailed your scheme
  - small change can have big security impacts

Libraries used often - OpenSSL

- Pros:
  - Very rich library
    - lots of algorithms, protocols, paddings
    - not “just” SSL
  - well tested functionally & security over time!
  - significant amount of existing examples on web
- Cons:
  - API is complex and sometimes harder to understand
  - (started as Eric Young’s personal attempt to learn BigInts ☺)
  - relatively low-level functions (can be pros!)
  - code is significantly interconnected
    - not suitable for extraction of single algorithm
  - poor official documentation

OpenSSL - problems

- Heart bleed
- Apple goto bug

Webová služba: opakovač paketů

```
network_receive(in_packet, &in_packet_len); // TLV packet
in = in_packet + 3;
```

unsigned char* in


```
out_packet = malloc(1 + 2 + length);
out = out_packet + 3;

memcpy(out, in, length);
```

unsigned char* out


```
network_transmit(out_packet);
```

Problém?

```
network_receive(in_packet, &in_packet_len); // TLV packet
in = in_packet + 3;
```

unsigned char* in


```
out_packet = malloc(1 + 2 + length);
out = out_packet + 3;

memcpy(out, in, length);
```

in_packet_len != length + 3

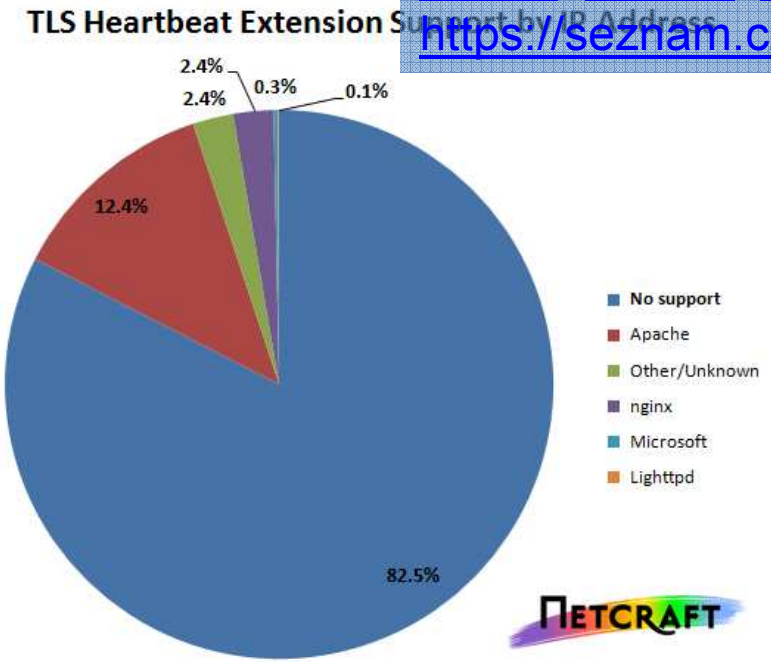
unsigned char* out


```
network_transmit(out_packet);
```

Problém!

O jak závažnou chybu se jedná?

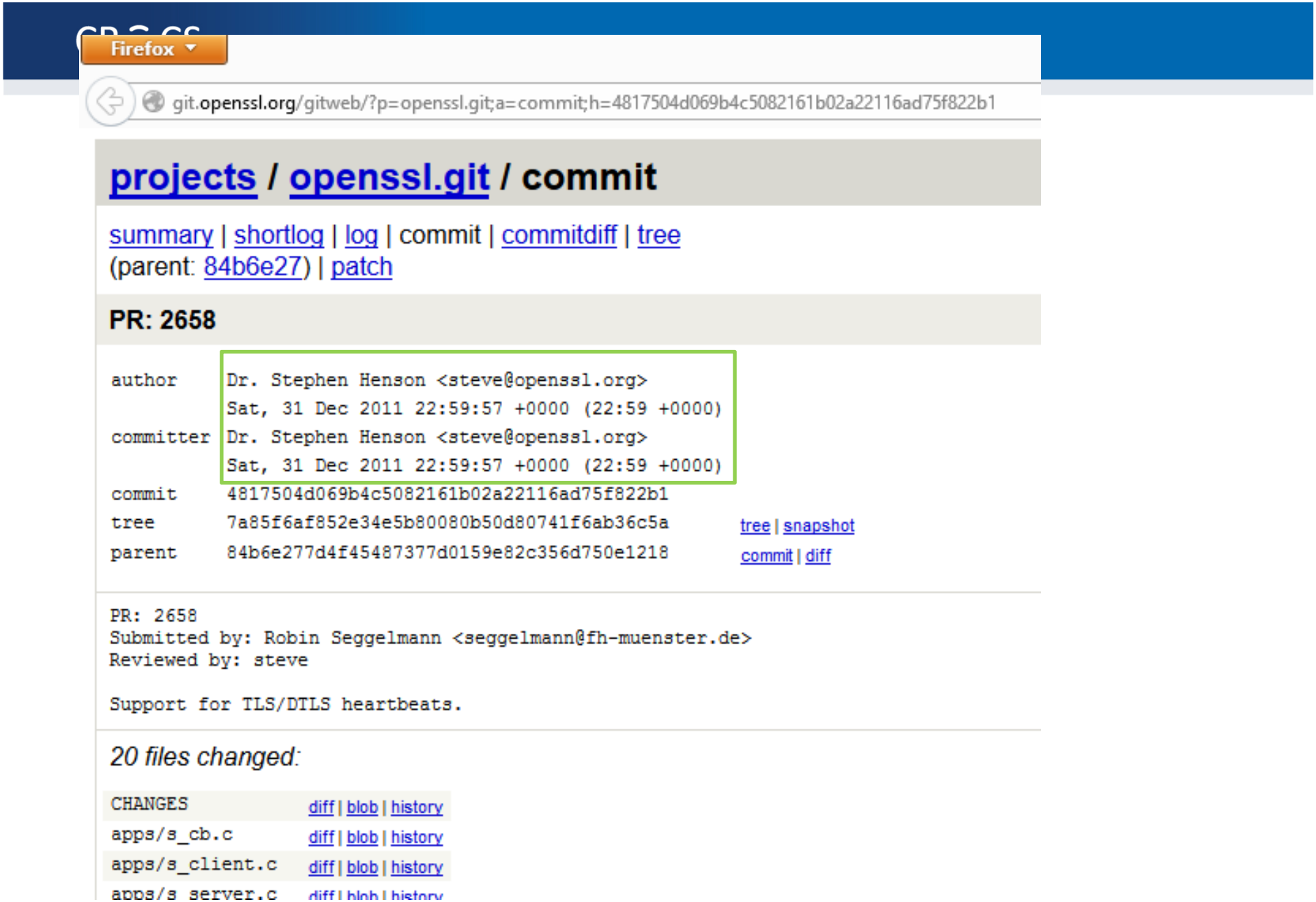
17% SSL web serverů (OpenSSL 1.0.1)
Twitter, GitHub, Yahoo, Tumblr, Steam, DropBox, DuckDuckGo…
https://seznam.cz, https://fi.muni.cz …



- http://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html

Ponaučení

- Vždy VELMI rigidně kontrolujte vstupní argumenty
- Nebezpečný není jen zápis za konec pole, ale i čtení
- Nedůvěřujte informacím od klienta
  - Ani když jste vy sami jeho tvůrci (změna na síťové vrstvě)
- Pro síťové aplikace preferujte jiné jazyky než C
  - Např. automatická kontrola mezí polí (Java, C#)
  - Nenahrazuje kontrolu argumentů!
- Open-source sám o sobě nezajišťuje kód bez chyb
  - "given enough eyeballs, all bugs are shallow" L. Torvalds
- (Nedělejte commity ve spěchu před oslavou)

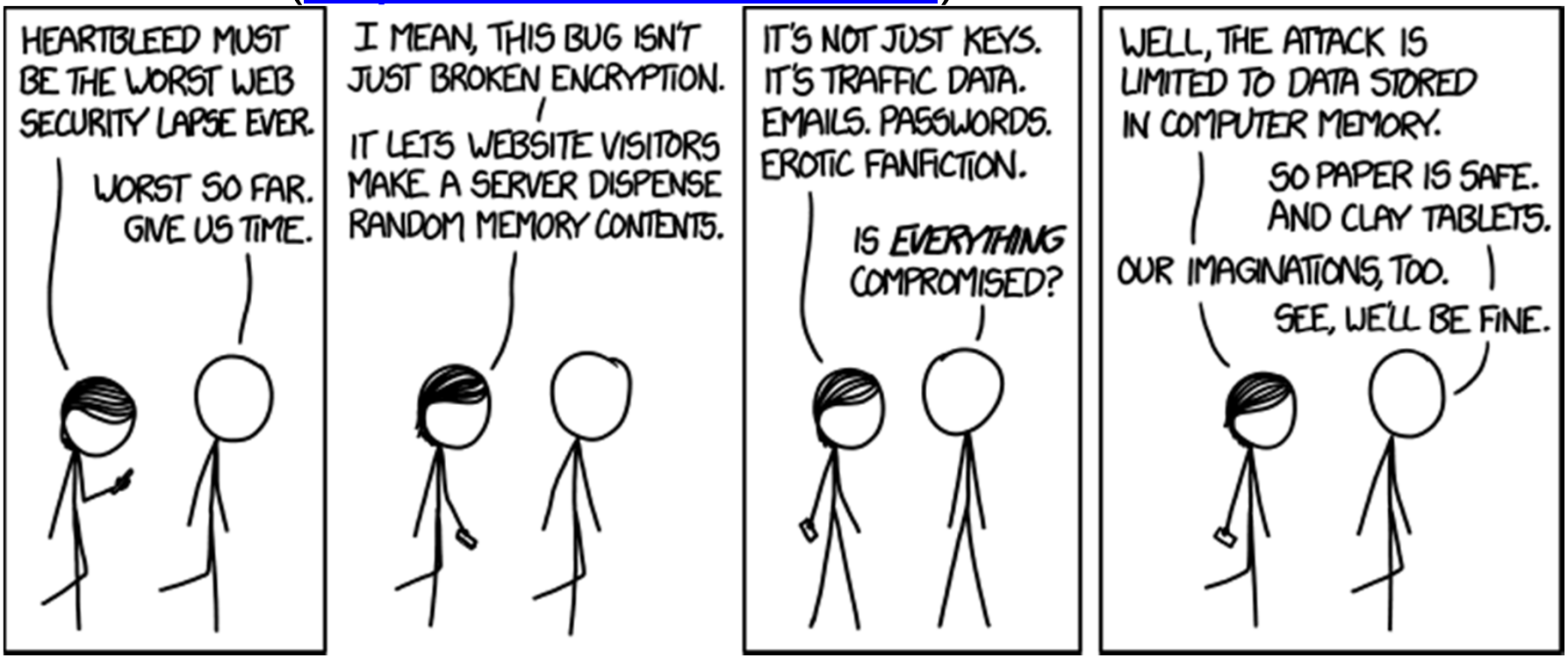

Firefox
git.openssl.org/gitweb/?p=openssl.git;a=commit;h=4817504d069b4c5082161b02a22116ad75f822b1
projects / openssl.git / commit
summary | shortlog | log | commit | commitdiff | tree
(parent: 84b6e27) | patch
PR: 2658
author Dr. Stephen Henson <steve@openssl.org>
Sat, 31 Dec 2011 22:59:57 +0000 (22:59 +0000)
committer Dr. Stephen Henson <steve@openssl.org>
Sat, 31 Dec 2011 22:59:57 +0000 (22:59 +0000)
commit 4817504d069b4c5082161b02a22116ad75f822b1
tree 7a85f6af852e34e5b80080b50d80741f6ab36c5a
tree | snapshot
parent 84b6e277d4f45487377d0159e82c356d750e1218
commit | diff
PR: 2658
Submitted by: Robin Seggelmann <seggelmann@fh-muenster.de>
Reviewed by: steve
Support for TLS/DTLS heartbeats.
20 files changed:
CHANGES diff | blob | history
apps/s_cb.c diff | blob | history
apps/s_client.c diff | blob | history
apps/s_server.c diff | blob | history

Reference

- Všeobecné informace
  - http://heartbleed.com/
- Testování zranitelnosti konkrétní stránky
  - https://filippo.io/Heartbleed/
- Analýza problému na úrovni zdrojáku
  - http://nakedsecurity.sophos.com/2014/04/08/anatomy-of-a-data-leak-bug-openssl-heartbleed
  - http://blog.existentialize.com/diagnosis-of-the-openssl-heartbleed-bug.html

O jak závažnou chybu se jedná? ☺

- XKDC (https://xkcd.com/1353/)



Libraries used often - PolarSSL

- Pros:
  - API is simple and clear
  - easy to extract single algorithm
- Cons:
  - fewer supported algorithms and standards
  - dual licensing, but not BSD-like license

How to use library

- Extract code and compile alone
  - some work with extraction
  - small, clean and self-containing result
- Compile against whole library
  - usually easy to do
  - but dependence on possibly unused code
- Link statically against dynamic library
  - dll must be always present to run program

How to use library (2)

- Link dynamically against dynamic library
  - try to open dll file and obtain function handle
- Link against service provider functions
  - Cryptography Service Providers in particular
  - API for listing of available service providers (CryptEnumProviders)
  - standardized functions provided by providers http://msdn.microsoft.com/en-us/library/aa380252%28v=VS.85%29.aspx#service_provider_functions

Security implications of dynamic libraries

- Library can be forged and exchanged
- Library-in-the-middle attack easy
  - data flow logging
  - input/output manipulation
- Library outputs can be less checked then user inputs
  - feeling that library is my “internal” stuff and should play by „my“ rules
- Library function call can be behind logical access controls

Practical assignment

Practical assignment

- Download OpenSSL and PolarSSL library
  - and check signature (gpg --verify)
- Write small project (PolarSSL based)
  - read, encrypt and hash supplied file, write into out file
  - read, verify hash and decrypt file
  - use AES-128 in CBC mode and SHA2-512
  - use PKCS#7 padding method for encryption (RFC 3852)
- Start with New Project+PolarSSL+AES

Questions ?

Submissions, deadlines

- Upload application source codes as single zip file into IS Homework vault (Crypto - 1. homework (AES+SHA2))
- DEADLINE: 22.9. 23:59 (first part)
  - application capable to read, encrypt, decrypt, hash
  - Text file containing description how you did PGP signature verification (whole process including import of public keys etc.)
  - selected solutions will be discussed during next lecture (23.9.)
  - 0-5 points assigned
- DEADLINE 29.9. 23:59 (second part)
  - finalization of codes based on the discussions during lecture
  - addition of unit tests
  - 0-5 points assigned