

MUNI
FI

Etický hacking

Mgr. Jan Kvapil
408788@mail.muni.cz



O mně

- 2012–2016: Bc. Obecná matematika, PřF MUNI
- Nabírání zkušeností
 - 2016: QA a strojové učení v Honeywellu
 - 2017–2018: Zakázkový vývoj softwaru ve Ytec (NL)
- 2018–2020: Mgr. Bezpečnost informačních technologií, FI MUNI
 - Stáž v Invasys, spolupráce s CRoCS, forenzní analýza,...
- 2020–nyní
 - Dobrovolnická pomoc během pandemie Covidu
 - Information security and cryptography (PV080 @ FI), cvičící a člen core group
 - Etický hacker, bug bounty hunter
- 2022–nyní PhD @ CRoCS pod doc. Petrem Švendou

Disclaimer

Přednáška má pouze vzdělávací charakter a přednášející nenese odpovědnost za případné následné činy posluchačů. Zejména za to, zda budou **etické**.

Osnova přednášky

- Myšlení hackera
- Fyzický a digitální svět
- Platformy a programy
- Reportování chyb
- Příklady zranitelností:
 - GitLab demo
 - (Omylem) uniklé přístupové tokeny
 - [EUDCC: Duplikátní certifikáty v produkčním a testovacím prostředí](#)
 - ROCA

Diskuze a otázky > přednáška

Myšlení hackera

- Způsob **myšlení a přistupování** k systému
 - Testování tvrzení o systému
 - ~~Důvěřuj, ale prověřuj~~
 - Využití systému v plném rozsahu
- Hackers: Heroes of the Computer Revolution (Steven Levy)
 - Počátky hackerství nejen na MIT, 1960+
 - Hackovat neznamenal vždy *rozbít* ([Spacewar](#))
 - Doba mainframe počítačů a děrných štítků
- [L0pht Heavy Industries](#), [Guild of the Grumpy Old Hackers](#)
- Pohled hackera vs. vývojáře vs. uživatele webové stránky



PDP-1 - <https://en.wikipedia.org/wiki/PDP-1>

MUNI
FI

Hacking & bug bounty hunting

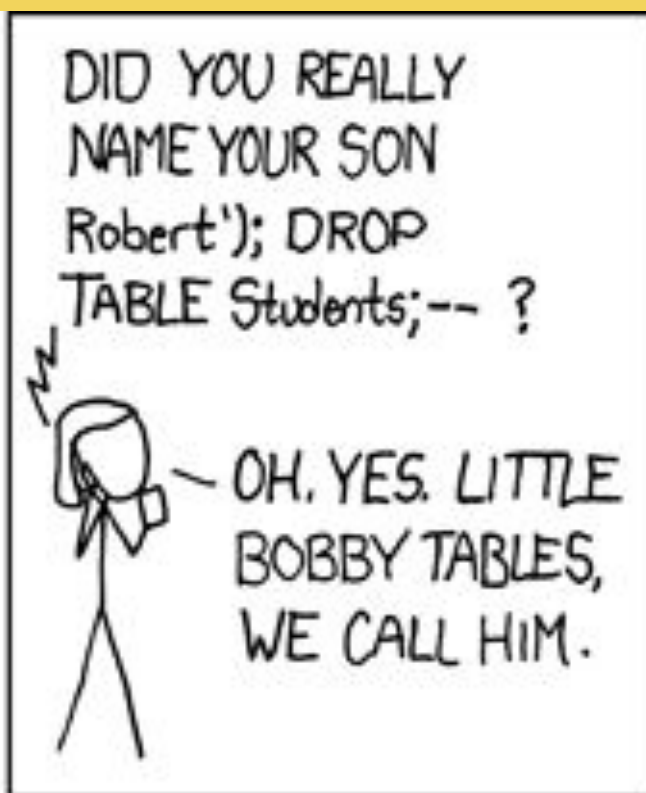
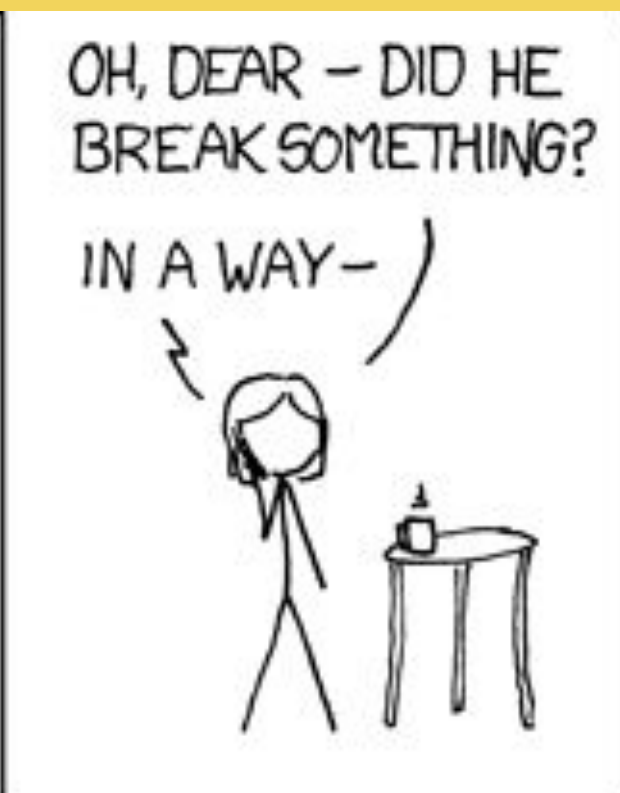
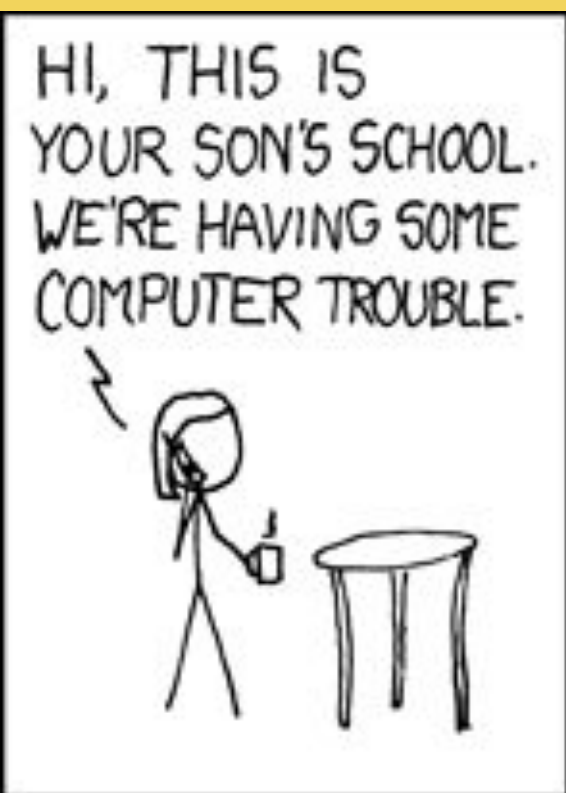
- **Neustálé** učení se nových věcí, technologií, jazyků
- Umění jít do šířky nebo se ponořit do hloubky
- Cit pro **detail**, vzorce a anomálie
- Kreativní myšlení a domýšlení
- Schopnost **komunikace**
- Volnost na úkor režimu *shora*
- Neutuchající zvědavost a fascinace možnostmi
- **Morální a etické** otázky

M U N I
F I

Fyzický a digitální svět

Fyzický a digitální svět

- “Chyba” ve fyzickém vs. digitálním světě
- Rychlost šíření této chyby
- Rozsah jejího dopadu
 - Zamýšlený i nezamýšlený
- Jednoduchost zneužití (a zopakování) této chyby
- Reprezentace informace (v bitech)



Příklady

Fyzický svět

- Nalezené klíče
- (Lesní) požár
- Pandemie
- *Dlouhodobé dopady?*
 - Životní prostředí, [olovnatý benzín](#)
- ...

Digitální svět

- Digitální podpisy/Auth token
- SQL injekce
- Ransomware/viry
- Remote Code Execution
 - [0-click iMessage](#), [more 0-click](#)
- Cross-Site Scripting (XSS)
- ...

M U N I
F I

Platformy a programy

Europe's #1 ethical hacking and bug bounty platform



RESEARCH
floerer

Want to launch a bug bounty program?

Request demo



Want to hunt for vulnerabilities?

Sign up



ACTIVE PROGRAMS

+300

RESEARCHERS

+40,000

BOUNTIES PAID

+3 mio

OUR CLIENTS INCLUDE



Platformy

- Umožňují registraci hackerům i firmám
- Příklady: [HackerOne](#), [Bugcrowd](#), [Intigrity](#), [Synack](#),...
- Moderátor mezi hackerem a konkrétním programem
 - Firmy na nich vytváří programy
 - Hackeři zde reportují zranitelnosti
 - Zprostředkovávají vyplacení bug bounties
- Chrání soukromí hackerů, programů
- Gamifikují hledání chyb
 - Signal, impact, reputace, ranking

Hacktivity

See the latest hacker activity on HackerOne

Sort

Popular ▾



Type

All

Bug Bounty

Published

Disclosed

Filter

Collaborations ⓘ

▲
39



[Reflected xss in https://sh.reddit.com](#)

By [abhiramsita](#) to [Reddit](#)

● Resolved

■ High

\$5,000.00

disclosed 2 days ago

▲
66



[Able to bypass email verification and change email to any other user email](#)

By [bisesh](#) to [Reddit](#)

● Resolved

■ High

\$5,000.00

disclosed 4 days ago

▲
4



[Misconfigured Rate Limit in Sending Notifications to the Victims Phone Via the Endpoint "/inbox "](#)

By [shamim_12__](#) to [Alohi](#)

● Resolved

■ Medium

disclosed 8 hrs ago

▲
36



[Multiple IDORs in family pairing api](#)

By [s3c](#) to [TikTok](#)

● Resolved

■ High

disclosed 4 days ago

▲
5



[Global default settings page is accessible to non-administrators](#)

By [dyls](#) to [Phabricator](#)

● Resolved

\$300.00


disclosed 18 hrs ago

All 307

sort:promoted-desc

307 results matching search • Find charity programs using `charity:true`


Recent



Contrast Security
Contrast automatically detects and fixes vulnerabilities and ...

Points – \$2,000 per vulnerability

Recent




Gearset: Managed Bug Bounty
Industry-leading DevOps solutions for every Salesforce team

\$200 – \$6,000 per vulnerability

Safe harbor


Recent



Latitude Financial Services Vulnerability Disclosure...
Latitude believes in helping people from all walks of life pr...

Safe harbor

Recent



SEEK
SEEK is a diverse group of companies that have a unified purp...

\$50 – \$10,000 per vulnerability

Partial safe harbor

Europe's #1 ethical hacking and bug bounty platform

Want to launch a bug bounty program?

Request demo →

Want to hunt for vulnerabilities?

Sign up →

ACTIVE PROGRAMS

+300

RESEARCHERS

+40,000

BOUNTIES PAID

+3 mio

RESEARCHER
floerer



REFRESH



COUNTRY
Netherlands

Programy

- Veřejné a skryté
- Skryté programy jsou nabízené na základě
 - Možností programu
 - Schopností hackerů
- Definují vlastní politiku = pravidla hackování
- Politiky mezi programy se liší
 - Použití automatizovaných nástrojů/skenů
 - Finanční ohodnocení (bounties)
- Assets (např. IP adresy, domény, Android/iOS aplikace,...)
 - **In scope**: hackování těchto produktů je **povoleno**
 - **Out of scope**: hackování těchto produktů je **zakázáno**



Search or jump to...



[Pull requests](#) [Issues](#) [Marketplace](#) [Explore](#)



CRoCS

Centre for Research on Cryptography and Security

📍 Faculty of Informatics, Masaryk Univ...

🔗 <https://crocs.fi.muni.cz>

Verified

[Overview](#)

[Repositories](#) 77

[Projects](#)

[Packages](#)

[People](#) 6

Pinned

[roca](#) Public

ROCA: Infineon RSA key vulnerability

Python 466 94

[JCAIlgTest](#) Public

Automated testing tool for algorithms from JavaCard API supported by particular smart card. Performance testing of almost all available methods. The results for more than 100+ cards.

Java 81 36

People



Top languages

Python Java

Aplikace na sdílení kódu a spolupráce (Git “web frontend”)

<https://github.com/crocs-muni/>

MUNI
FI



GitHub

How people build software

<https://bounty.github.com>

[m](#) · [@githubsecurity](#)

[Submit report](#)

Reports
resolved

980

Assets
in
scope

25


Average
bounty


\$617

Rewards

 Low

 Medium

 High

 Critical

\$2,000

\$10,000

\$20,000

\$30,000

\$617

\$4,000

\$10,000

\$20,000

See <https://bounty.github.com/index.html#severity-guidelines> for more information about the above.

Last updated on July 1, 2021.

Proč je hackování GitHubu legální?

Legal safe harbor

- We consider security research and vulnerability disclosure activities conducted consistent with this policy as “**authorized**” conduct under the **Computer Fraud and Abuse Act**, the DMCA, and other applicable computer use laws such as Cal. Penal Code 502(c). We waive any potential DMCA claim against you for circumventing the technological measures we have used to protect the applications in this bug bounty program's scope.

[...]

- If your security research as part of the bug bounty program **violates certain restrictions** in our site policies, the safe harbor terms **permit a limited exemption**.

Výtažek z <https://hackerone.com/github>, zvýraznění přidáno.

DMCA = Digital Millennium Copyright Act

Z politiky Paypalu

Ownership of Submissions

*As a condition of participation in the PayPal Bug Bounty Program, you **hereby grant** PayPal, its **subsidiaries, affiliates and customers** a perpetual, **irrevocable**, worldwide, royalty-free, transferrable, sublicensable (through multiple tiers) and **non-exclusive** license to use, reproduce, adapt, modify, **publish, distribute**, publicly perform, create derivative work from, make, use, **sell, offer for sale** and import the Submission, as well as any materials submitted to PayPal in connection therewith, for any purpose. **You should not send us any Submission that you do not wish to license to us. [...]***

Výtažek z <https://hackerone.com/paypal>, zvýraznění přidáno.

In Scope

GitHub.com

GitHub.com is our main web site. It is our most intricate application with a number of user inputs and access methods. GitHub.com is built on Ruby on Rails and leverages a number of Open Source technologies.

Domain

Rewards range from \$555 up to \$20,000 and are determined at our discretion based on a number of factors. For example, if you find a reflected XSS that is only possible in Opera, and Opera is <2% of our traffic, then the severity and reward will be lower. But a persistent XSS that works in Chrome, at >60% of our traffic, will earn a much larger reward.

You can find the app at <https://github.com>.

 Critical

 Eligible

Existující programy

- Internet Bug Bounty Program

- OpenSSL, Curl, Ruby (i Rails), Python, Rust
- Bounties spozorované od různých firem

- Google's Bug Hunting community

- Patch rewards (odměny), Open-source Security Subsidies (dotace)

- European Commission's Open Source Programme

- LibreOffice, Mastodon, Odoo, Cryptpad, LEOS
- BBP Evropské unie na Integrity

MUNI
FI

Reportování chyb

 bitquark

Participants



State ● Resolved ()

Reported to [GitHub](#)

Disclosed April 13, 2022 9:16pm +0200

Severity  High (7 ~ 8.9)

Weakness *None*

Bounty \$10,000

CVE ID *None*

Obsah reportu (submission)

- Asset: <https://api.github.com>
- Zranitelnost: Cross Site Scripting (XSS)
- Závažnost zranitelnosti: Low–Critical, [CVSS 3.1 kalkulačka](#)
- Proof of Concept
 - Shrnutí zranitelnosti a **dopadu** na program
 - Nezbytné kroky k reprodukování zranitelnosti
 - Rozsah (odhadovaných) škod
 - Konkrétní kroky provedené hackerem

Attack Vector (AV)

Network (N) Adjacent (A) Local (L)
Physical (P)

Attack Complexity (AC)

Low (L) High (H)

Privileges Required (PR)

None (N) Low (L) High (H)

User Interaction (UI)

None (N) Required (R)

Scope (S)

Unchanged (U) Changed (C)

Confidentiality (C)

None (N) Low (L) **High (H)**

Integrity (I)

None (N) Low (L) High (H)

Availability (A)

None (N) Low (L) High (H)

Po odeslání reportu...

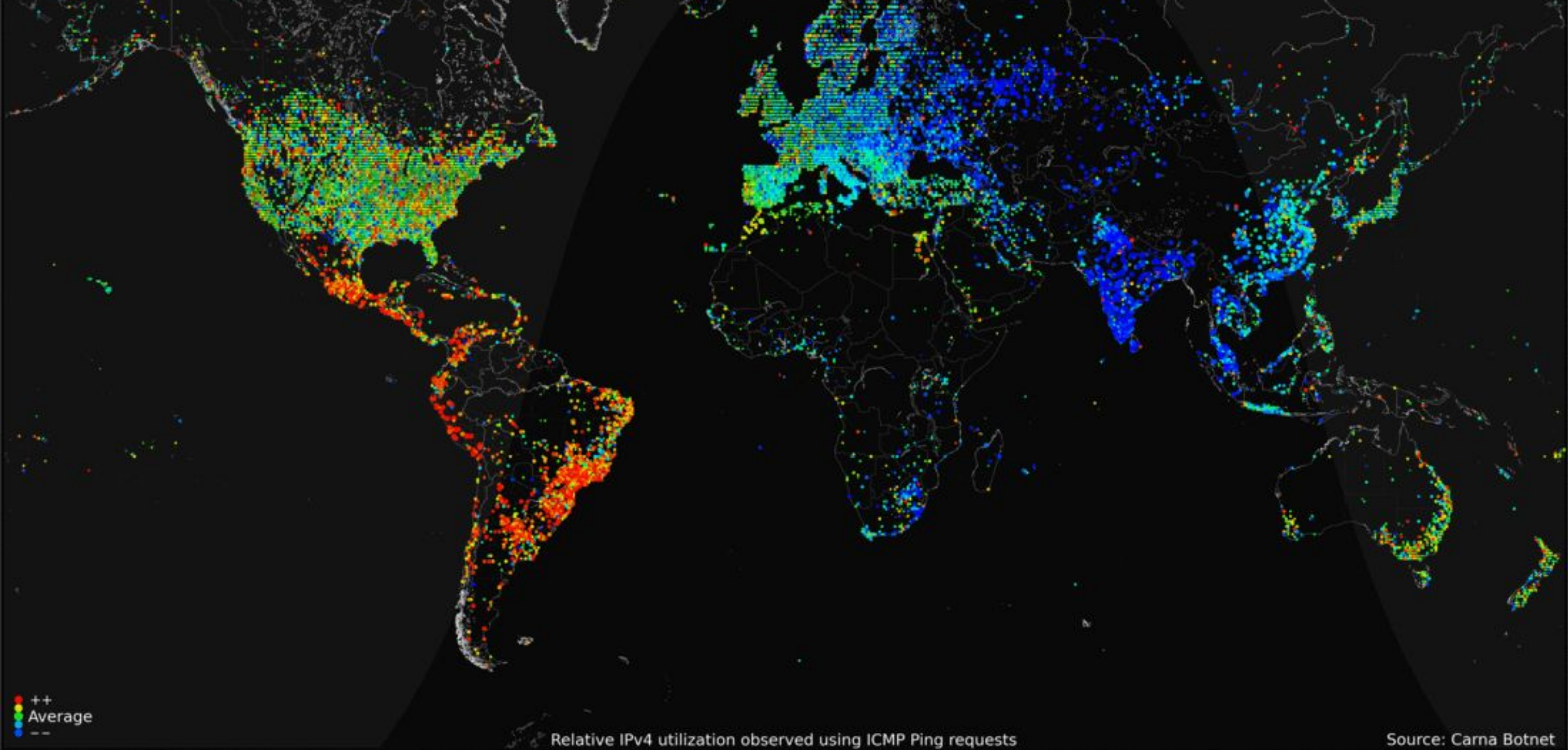
- **Čekání** na triage ze strany platformy nebo programu
 - V řádu dnů až týdnů
 - Non-applicable ~ hackování mimo scope, ztráta *signálu*
 - Informative ~ chyba existuje, ale není závažná
 - Duplicate ~ chyba existuje a je závažná, ale byli jste druzí...
- **Triage**
 - Doplnění dalších informací (např. jaké osobní údaje hacker získal)
 - (Společné) řešení chyby
 - Občas částečné vyplacení odměny (GitLab)
 - Další **čekání**
 - Někdy tzv. re-testing
- Uzavření reportu a další **čekání** na vyplacení odměny

Hacking a další souvislosti

- **Beg bounties**
- Možná pravidla zveřejňování
 - *This bug is subject to a **90 day disclosure deadline**. If a fix for this issue is made available to users before the end of the 90-day deadline, this bug report will become public 30 days after the fix was made available. Otherwise, this bug report will become public **at the deadline**.* ([Google Project Zero](#), zvýraznění přidáno) (až na [výjimky](#))
 - Po vzájemné domluvě
 - Nikdy
- Komu reportovat složitější případy?
 - Chyba se týká více programů, balíčků třetích stran
- Etický hacking a BBH není nic speciálního
 - Omezené množství času, schopností,...

Hacking a další souvislosti

- Argumentování/přesvědčování o závažnosti chyby
- Důvody k hackování
 - Kreativní, vzrušující a seberozvojový koníček
 - Přivýdělek
 - Pomoc ostatním lidem
 - ...



Carna botnet, [Darknet Diaries episode](https://darknetdiaries.com/imgs/carna.gif), <https://darknetdiaries.com/imgs/carna.gif>

M U N I
F I

MUNI FI

GitLab

The image shows a screenshot of the GitLab Community Edition Issue Boards interface. The top navigation bar includes 'GitLab', 'Projects', 'Groups', 'Activity', 'Milestones', and 'Snippets'. The main header displays 'GitLab Community Edition' and 'Issue Boards' for the 'Development' project. A search bar and 'Add list'/'Add issues' buttons are present. The interface is divided into three columns of issue boards:

- Open (4636 issues, 224 comments):**
 - Trigger Token Exposed to Maintainer/Owner of Project/Group #52260 (CI/CD, HackerOne, P3, S3, security)
 - Group Ex-Maintainer Could maintain Access to Project's Source Code/Jobs/Pipelines/Artifacts if it had Shared Group Runner Configured #52184 (CI/CD, HackerOne, Manage, P3, S3, devops:verify, feature-proposal, groups, security)
 - Stored XSS on Pipeline License Tab #51999 (CI/CD, HackerOne, P3, S3, security)
 - JUnit XML MR Widget: Link From Widget To Failed Testfile #46564 (CI/CD, Stretch, customer, devops:verify, feature-proposal, merge-requests)
 - Clean up `ArchiveLegacyTraces` background migrations with `BackgroundMigration.steal` #46906 (CI/CD, Stretch, backstage, blocked)
- backend (1351 issues, 520 comments):**
 - Wiki Page History appears to direct to wrong link and 404s #29528 (P4, Platform, S3, backend, bug, default-priority, default-severity, wiki)
 - What does "xxxx restored source branch xxxx 4 minutes ago" mean? #28918 (Accepting merge requests, Create, P4, S3, backend, bug, default-priority, default-severity, merge-requests)
 - Add mechanism that will discard artifacts metadata if file is too large #8080 (CI/CD, P3, S3, backend, devops:verify, security, technical-debt)
 - Change CI/CD endpoints returning HTML to JSON #42378 (CI/CD, P3, S3, backend, devops:verify, frontend, security)
 - Stored XSS for Environments #53037 (CI/CD, HackerOne, P2, S2, backend, devops:release, security)
- frontend (2418 issues, 476 comments):**
 - Change CI/CD endpoints returning HTML to JSON #42378 (CI/CD, P3, S3, backend, devops:verify, frontend, security)
 - Display a message that GitLab Pages are not supported for nested groups #34589 (CI/CD, P4, S3, Stretch, UX, bug, default-priority, default-severity, devops:release, frontend, pages, subgroups)
 - Exposure of Private Project's Confidential Issues' title and Namespace in Commit Message #52444 (Create, Deliverable, HackerOne, P2, S2, frontend, markdown, security)
 - Hide trigger variables in UI by default #20422 (CI/CD, PM Ready, UX, Verify, backend, devops:verify, direction, feature-proposal, frontend, security)
 - Show enhanced information on running deploys in MR Widget #25140

At the bottom of the page is a large, dense grid of user avatars, representing the GitLab community.

GitLab Demo

- Podobný produkt jako GitHub
- OpenSource
- <https://gitlab.com/gitlab-org/>
- [FI](#) a [MUNI](#) má vlastní instance
- BBP na HackerOne; včetně publikovaných reportů
- [Arbitrary file read via the UploadsRewriter when moving and issue](#)

MUNI FI

(Omylem) uniklé přístupové tokeny

c588e4f9edab64b59a46b8380062e13904cc2ef38c8c58ce2f0f3f277761b669
4457ae87006c310ca8ac5bad162de51b7ce58cc808c6de862e2d7329124386f1
6e5b3013882f40f9d32405d873c3f8479bf7b08117f303225ecfa10702e762ff
c588c1dd5d7a8d15dd615c23ebd1311f55acf0b4e3071c9f7a98dd49f46eaa26
4b117e9702e64cc5e6f664f04a7b7dea48b5fdd811672ac8b484160cca984d3f
d2522ecccd13eb0685bba20496e9d9810f0801f4bcf2a889402d86f4f293f9c5
df4d6b49b3dd16d8f6ed523fc7b4f3854c16bea6d5fdf218a326dfad787470c3
ef191f5c954d1a1a743d3db1a7781f7d979c7db3646743e0de3d60843e2a6e98
fbaf2d5f5ae946e152f18ce6faa282d21dbdaa0697095c274e1708a7589d3a27
1f5330bbf2022fe9355a52bcf29ad7589ccc4f75ef18848cd49e930ec8a082b9
5c5ce94c1fc9defd1da8d6a0133c0150b02d452850ea0b5665bb511402c08d00
0aeeb28ba66a518f9d78addc88e2b96f5dae1f821230e0f41b815bc68837e1a3
fd1fe1eefc87858abf8e7f23c8bc2842d9cd6e718035e8459aef3d1ffac09b68
66234bf4b8aa7088e2db6c8c46137e8594c95e06c9bb3a52e7623a18a46f043b
8627644c0cc0f3bd5d08c558501a6bbbed30de8aff7546b6c2bfff256c40e40780
0edbbff2d2b960d406e494461fe72c52d73d68f565c890f509a59a4bc3b079b8
fc14c4375c4bf2f4e4e6c6953631e6696aa287749c84976d809bbb0d5506ddeb
7350c7df9481fb939081318310edafb2370b45f4e59eebffa92487a056094ad
26e413f6918f0c6f3ff42844341df92f7f5f1cb7233ba1aa2cd81197ce5e1cab
8c6e19dfde2b50e7adb68936d5d2245ccac32c9f3c241e7d2c246e0231982e68
3b49b103f4ceb8800ac9dcfa02c6504eecc5e29570affa0beb9225dcc00b99cb
709d3742aa0bb644d8d7ad3ed45b23f900c903c02a8f3c3dfcf68d373adf6513
374176c9cf9afb257a03d7c505edc66fdc20bf3ffc5f747150bb3f6ac218a617
e1473c578d9c6fd45e34e927ce1996d96d3a586d8104b4bc48bb49f2806434c0
64f28fe7f7832f9dd02ee34c76267cd5b66fcc0398aafb9b1b753fd29b2a4153
acc6519844d1f00235ddd8c521b3e8498f2d4190cf84b8342bcda844242b529d
1470306a47dc3ddeea948b7ffe3225d8a4cd06f28ba4dcf7691464ab032990c4
01107698775ab70c733c584a72cb5b270285a4c8716a351a025c18388282c48b
b5fb706aa0cc5355f48b4ce5212b77812e91c1c406cf178b701c90bef17724bf
fea1c347e9c8b795f0ec09c7ab6b58cd859c21ca97c20a49c5ac6d00e43e8e66
3f5ade56fb9023e36cab622636361bd18b87b3dd592deb11957e51d2e6bf188d
f8957fc14b10c3191bc225fd6ee44518a09e730d38e3ed011ea2f43ac53a3797
688353bf7006f798e1c54c25681b6a19abc930f39ce45560630b9b35fe019c23
bf8d174ac01e888d21d7243a9dbdbf50734c1f757f21c2dfa0abd8be9a8db96e
ab53e593ea80fb3614dbb6da776672652a4228f633ac98c53dbb72723313fc78
90f09c2f4cdbe5feb91e51aa9c3b75571e2932beac1af29b8f94c7ed309ad1a8
68877c64868817b16887c1848c87c651188c1811045668771c1c1451

(Omylem) uniklé přístupové tokeny

- Token je náhodný řetězec
 - Umožňuje přístup ke službě
 - 8537add5d4834edf48e02fe25c3960370629aee4a2711c2c9e85afc933e5540
 - Nesmí být zveřejněn (podobně jako hesla)
- Typické využití pro Application Programming Interface (API)
 - Strukturovaná komunikace mezi dvěma a více počítači
- Vlastnictví tokenu umožní autorizaci požadavku
 - Rozsah autorizace lze někdy omezit (pouze čtení, čtení a zápis, časově omezená platnost)
- Jak může přístupový token uniknout?

(Omylem) uniklé přístupové tokeny

- Reportování tokenů
- Potřeba najít původního majitele tokenu
 - A nereportovat omylem např. zloději tokenu
- Je využití tokenu pro přístup k API opodstatněné?
 - Access tokens that don't belong to GitLab projects/groups/team members (please **contact the owner** of the token, you can find their email address **by querying the /api/v4/user API**) (výňatek z Out of scope HackerOne politiky GitLabu)
- [Shopify a uniklý token](#)

EUDCC: Duplicitní certifikáty

EU Digital COVID Certificates System: Duplicate DSCs in Production and Testing Environments

Low mcoric-dtc published GHSA-xcvc-p4fw-qmcj on Jan 17

Package	Affected versions	Patched versions
Technical Specifications for Digital COVID Certificates, Volume 5: Public Key Certificate Governance ()	1.0	1.1

Description

Affected version:

- Technical Specifications for Digital COVID Certificates, Volume 5: Public Key Certificate Governance, v1.0
Fixed version:
- Technical Specifications for Digital COVID Certificates, Volume 5: Public Key Certificate Governance, v1.1

Description

A potential vulnerability has been discovered in the Governance of the public key certificates of DSC (Digital Signing Certificates) in the EU Digital Covid Certificates (EU DCC) system, insofar the public key certificates of DSCs are re-used between production and testing environments. This vulnerability was due to the then applicable “Guidelines for the Governance of the Public Key Certificates”, adopted in May 2021 by the eHealth Network, whose members are experts representing Member States.

Solution

Immediately after receiving the report (July 20th, 2021), a discussion with the experts of Member States started on how to implement appropriate mitigation measures and eliminate the vulnerability (DCC Community Newsletter of August 11th, 2021). To this end, the first step was to update the “Guidelines for the Governance of the Public Key Certificates” that are managed and adopted by the eHealth Network (Nov 17th, 2021).

As of today, the situation is as follows:

1. The updated guidelines have been adopted by the eHealth Network and now prevent the re-use of DSCs’ public keys, as well as of other public keys, between the Production and non-Production environments.
https://ec.europa.eu/health/sites/default/files/ehealth/docs/digital-green-certificates_v5_en.pdf
2. The onboarding process has been modified accordingly, so no country connected to the EU DCC Gateway would ever be able to use public key certificates already used in TEST or ACC in the Production environment.
3. All the re-used public keys are changed and there are no duplicates between the production and non-production environments.
4. Periodical checks for re-used public keys between the environments are established and the Operations Team is notified.
Improvements in the codebase for preventing the uploading of duplicate public keys are scheduled. In addition, we are introducing additional automatic checks and monitoring processes to reduce risks of errors.
5. All countries connected to the EU DCC Gateway do now comply with the new guidelines. No duplicates exist.

Lastly, it is worth highlighting that the only authoritative list of EU DCC public keys in Production is the one securely distributed through

EUDCC: Duplicitní certifikáty

- European Union Digital Covid Certificate (EUDCC)
- Pas/certifikát, který prokáže o majiteli:
 - Prodělané Covid19 onemocnění
 - Výsledek antigenního nebo PCR testu
 - Prodělané očkování
- Každý stát má vlastní infrastrukturu
 - Vydávání a podepisování DCCs
 - Aplikace pro ověřování certifikátů (čTečka) a uschovávání (Tečka)
- DCC je digitálně podepsaný národní certifikátem
 - CSCA, UPLOAD, AUTHENTICATION, DSC
- [Digital Green Certificates: Security analysis not included](#)

EUDCC: Duplicitní certifikáty

- Produkční a testovací prostředí
- Duplikování produkčních a testovacích klíčů/certifikátů
- Speciální [repozitář](#) na testování funkčnosti pro jiné státy
- Vývoj v čase:
 - Červen 2021: objevení problému a reportování na veřejném Slacku
 - Červenec 2021: stále velké množství duplikátů
 - Září 2021: první oficiálnější reakce ze strany EU
 - Listopad 2021: člověk, který s námi komunikoval oznámil, že už na projektu nepracuje
 - Leden 2022: vydání [GitHub Security Advisory](#)
 - Únor 2022: update GHSA s hlavními datумы

EUDCC: Duplicitní certifikáty

- Výňatky z komunikace
 - Nepřipravenost na hlášení z *neoficiální strany* (tedy ne od členského státu)
 - Z počátku volný deadline
 - Kvůli vážnoucí komunikaci pochopení případného zveřejnění

M U N I
F I

OpenAI: ChatGPT



SQL translate

Code

Transformation

Translate natural language to SQL queries.

Prompt

```
### Postgres SQL tables, with their properties:  
#  
# Employee(id, name, department_id)  
# Department(id, name, address)  
# Salary_Payments(id, employee_id, amount, date)  
#  
### A query to list the names of the departments which employed more  
than 10 employees in the last 3 months  
SELECT
```

Sample response









```
SELECT d.name  
FROM Department d  
INNER JOIN Employee e ON d.id = e.department_id  
INNER JOIN Salary_Payments sp ON e.id = sp.employee_id  
WHERE sp.date > NOW() - INTERVAL '3 months'  
GROUP BY d.name
```

OpenAI – ChatGPT

- Populární model umělé inteligence
- Několik odhalených chyb
 - [Web Cache Deception](#)
 - Vyžaduje interakci uživatele (kliknutí na link)
 - Umožní útočníkovi číst metadata o uživateli
- <https://bugcrowd.com/openai>

Hall of Fame

Thanks to the following researchers for reporting important security issues:

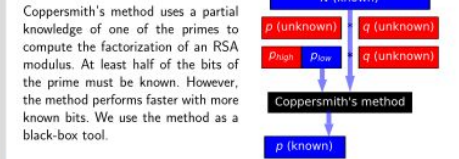
Rank	Researcher	Points
1	 Nagli	75
2	 tess	60
3	 d0xing	20
4	 Asm0d3us	20
5	 c4ng4c3ir0	10
6	 wrathfulDiety	10
7	 rez0	5
8	 cryptographer	5

Abstract

We discovered an algorithmic flaw in the construction of primes for RSA key generation in a widely-used library of a major manufacturer of cryptographic hardware. The primes suffer from a significant loss of entropy. We proposed a practical factorization method that only requires the value of the public modulus and does not depend on a weak or a faulty random number generator. We devised an extension of Coppersmith's factorization attack utilizing an alternative form

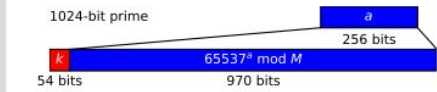
of the primes in question. The library is found in NIST FIPS 140-2 and CC EAL 5+ certified devices used for a wide range of real-world applications, including identity cards, Trusted Platform Modules, GPG, and tokens for authentication or software signing. The impacted devices are widespread. We responsibly disclosed our findings to the manufacturer of the flawed library. Our work was published at ACM CCS 2017 [1] and received the Real-World Impact Award.

Coppersmith's factorization method

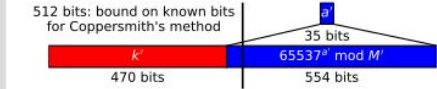


Making the attack practical

To attempt a factorization of a vulnerable RSA key, we guess the value of a and compute the much larger "known" part of the prime as $65537^k \bmod M$. We then try to compute k using Coppersmith's method, what succeeds only if the guess was correct. In the worst case, the attack will require trying half of all the possible values of a .

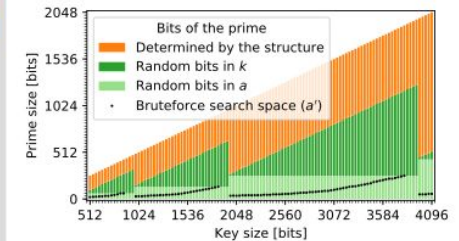


For the majority of RSA key sizes, the bit length of M (and $65537^k \bmod M$) is much larger than the required bound for the attack (one half of the prime's bit length). We find a smaller M' (a divisor of M), such that its size is still sufficient, yet the size of a' is significantly reduced when compared to a .



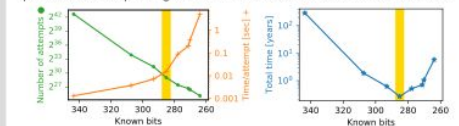
Entropy in primes

The figure shows the number and origin of random bits in relation to the size of the prime (vertical axis) for keys of given length (horizontal axis). A large portion of prime's bits is determined by the structure (orange) and can be computed from the knowledge of random bits (green). Coppersmith's attack further reduces the required number of known bits even lower (black dots).



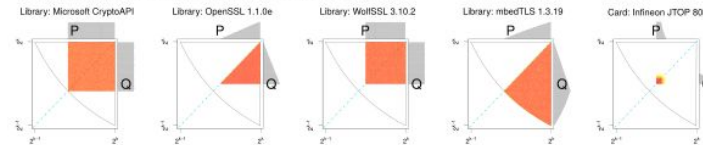
The attack optimization process

Smaller values of M' (fewer known bits) require fewer guesses on the value of a' . However, the evaluation of each guess takes more time. We select the parameters corresponding to the minimal overall time of the factorization.



Background – surprising biases in RSA public keys

Švenda et al. [2] described how cryptographic libraries generate RSA primes in various ways, introducing subtle biases in the public keys, sufficient to classify the keys based on their origin. Infineon smartcards produced especially biased keys.

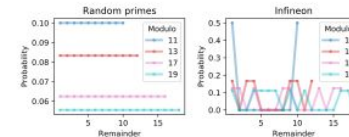


The distribution of the most significant bytes of a pair of RSA primes varies for different cryptographic libraries.

The properties of vulnerable keys

The distribution of the Infineon RSA primes and keys modulo small primes is irregular, unlike randomly chosen primes and keys that are distributed uniformly modulo small primes (left). In fact, the primes belong to a small subgroup modulo

a product M of small consecutive primes, what lead us to the discovery of the structure of the primes (right). The primes and RSA moduli suffer from a significant loss of entropy and can be uniquely fingerprinted using a fast discrete logarithm.



The distribution of RSA keys modulo small primes

$$N = p \cdot q$$

$$p_{ideal} = \text{random prime}$$

$$p_{Infineon} = (k \cdot M + 65537^a \bmod M); \quad a, k \in \mathbb{Z}$$

$$M = 2 \cdot 3 \cdot 5 \cdot 7 \cdot \dots \cdot P_n$$

Entropy in a prime

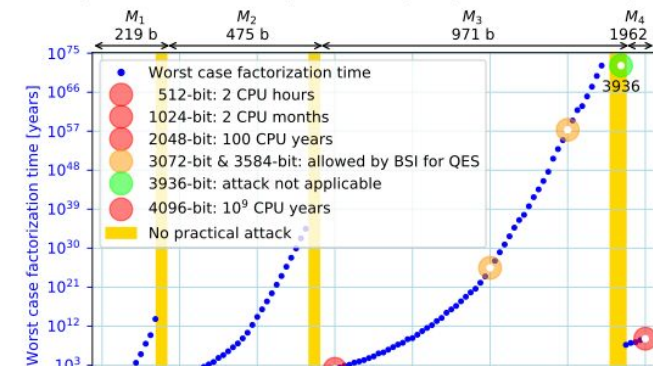
Random: random bits

Infineon: a k determined by the structure

Factorization attack complexity

The complexity of the factorization depends on the size of the keys (horizontal axis). However, due to the different parameters used in their generation (different values of M at the top of the figure), the time required to break a key (vertical

axis, blue dots) does not strictly increase. Therefore, some key lengths are more affected, including the common sizes of 1024 bits and 2048 bits. The attack can be easily parallelized with independent processors to achieve a linear speedup.



ROCA

- Rok 2017, CVE-2017-15361
 - Matúš Němec, Marek Sýs, Petr Švenda, Dušan Klinec, Vašek Matyáš z CROCSu
 - https://crocs.fi.muni.cz/public/papers/rsa_ccs17
- Generování slabých RSA klíčů
- Čipy od Infineon Technologies
- Rozsah na úrovni několika zemí (Slovensko, Estonsko, Španělsko)

Shrnutí

- Způsob myšlení hackera
- Jednání (tedy i hackování) s sebou nese důsledky
 - Potenciálně s velkými následky
- Buďte všímaví a zůstávejte *in scope*
- Používejte 2FA a Password manager

Otázky?

Další odkazy a zajímavé materiály

- [Steven Levy](#)
- [Lyle Bickley explains the PDP-1](#)
- [Cybercompass](#)
- [Darknet Diaries podcast](#)
- [Google Project Zero](#)
- [Hackers Testifying at the United States Senate](#)
- [Hacker news](#)

Zdroje

- Obrázek [Hacker: Heroes of the Computer Revolution](#)
- Poster [ROCA](#)
- <https://about.gitlab.com/press/press-kit/>
- Screenshoty z <https://hackerone.com/>

M U N I

F I