MUNI
FI

Etický hacking

Mgr. Jan Kvapil
408788@mail.muni.cz

Jan Kvapil – CV

- 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
- Běžec, lezec, křesťan

MUNI FI

Disclaimer

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

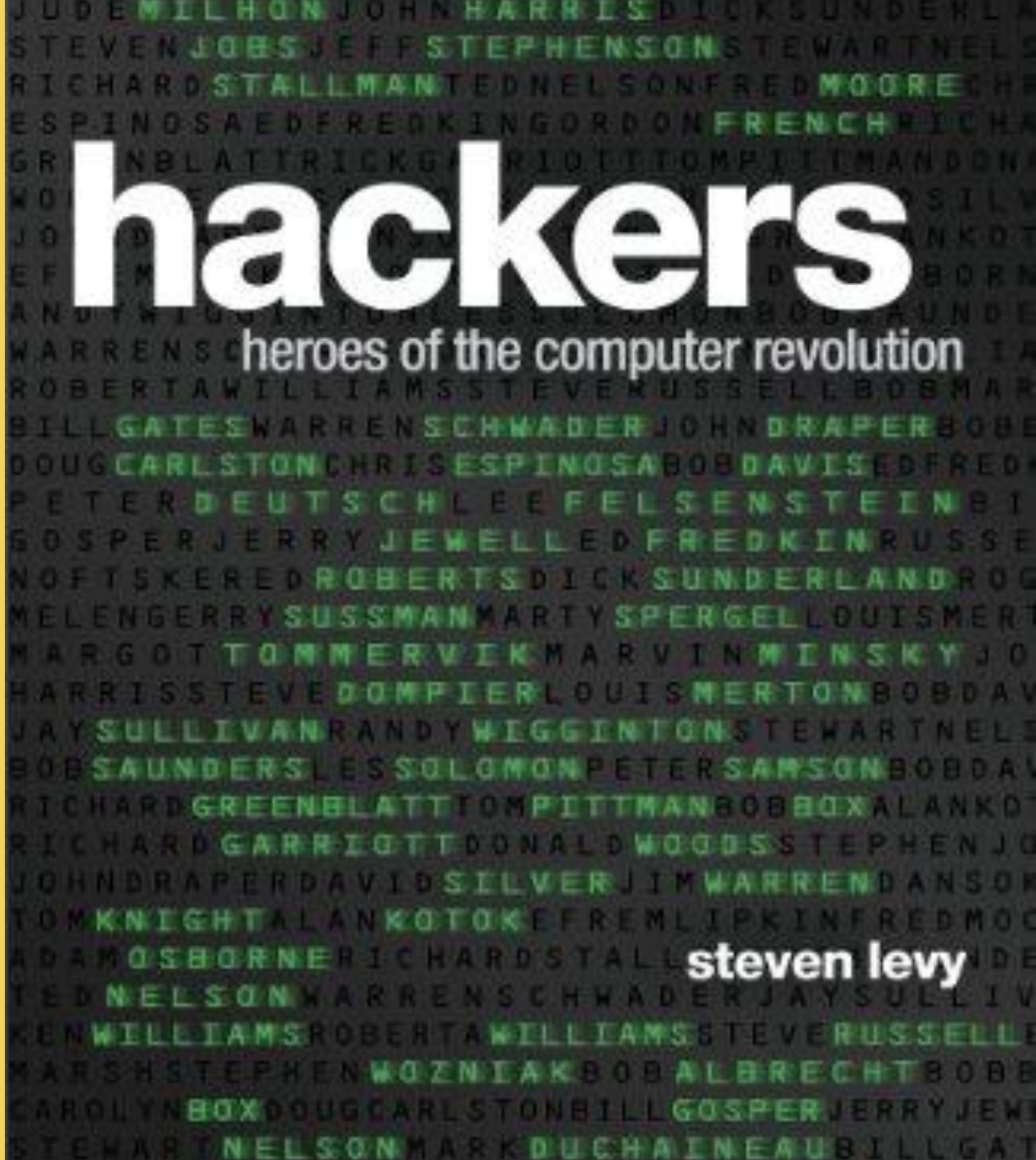
Osnova přednášky

- Myšlení hackera
- Fyzický a digitální svět
- Platformy a programy
- Reportování chyb
- Příklady zranitelností:
  - (Omylem) uniklé přístupové tokeny
  - EUDCC: Duplikátní certifikáty v produkčním a testovacím prostředí
  - ROCA Vulnerability disclosure (doc. RNDr. Petr Švenda, Ph.D.)
  - …

Diskuze a otázky > přednáška

MUNI
FI

Myšlení hackera



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
  - Hackovat neznamenalo vždy *rozbíjet* (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

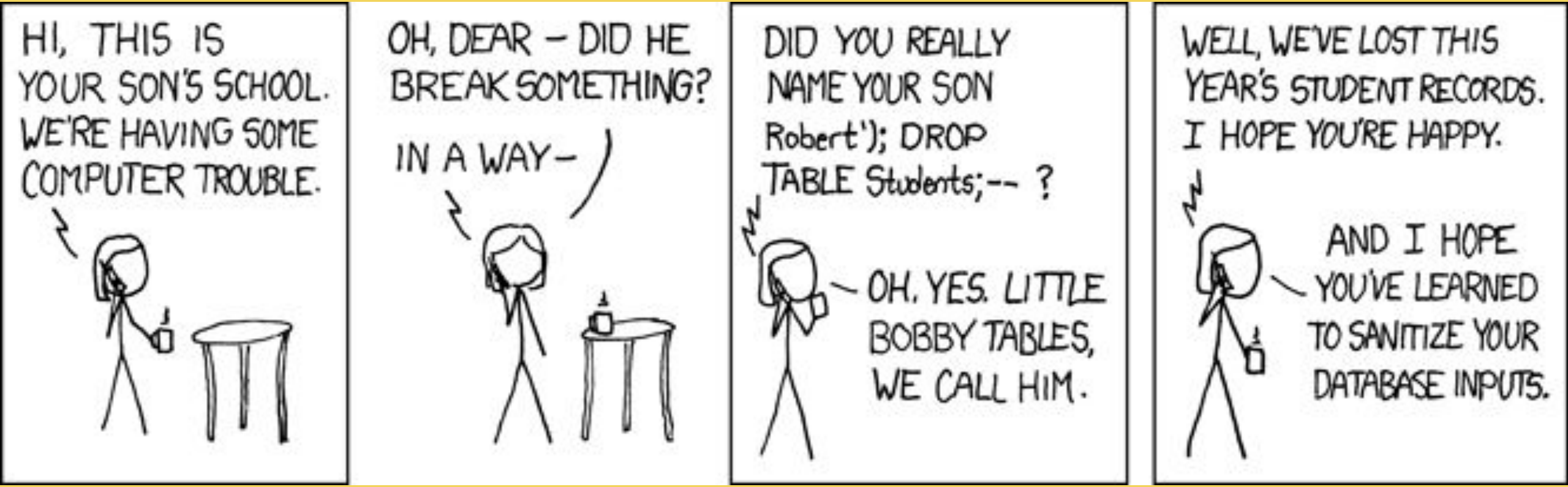
- **Neustálé** učení se nových věcí, technologií, jazyků
- Umění jít do šířky nebo se ponořit do hloubky
- Cit pro **detail**, vzorce a anomálie
- Kreativní myšlení a domýšlení
- Schopnost **komunikace**
- Volnost na úkor režimu *shora*
- Neutuchající zvědavost a fascinace možnostmi
- **Morální a etické**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

MUNI
FI

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 informací



Exploits of a Mom - https://xkcd.com/327/

MUNI FI

Příklady

Fyzický svět

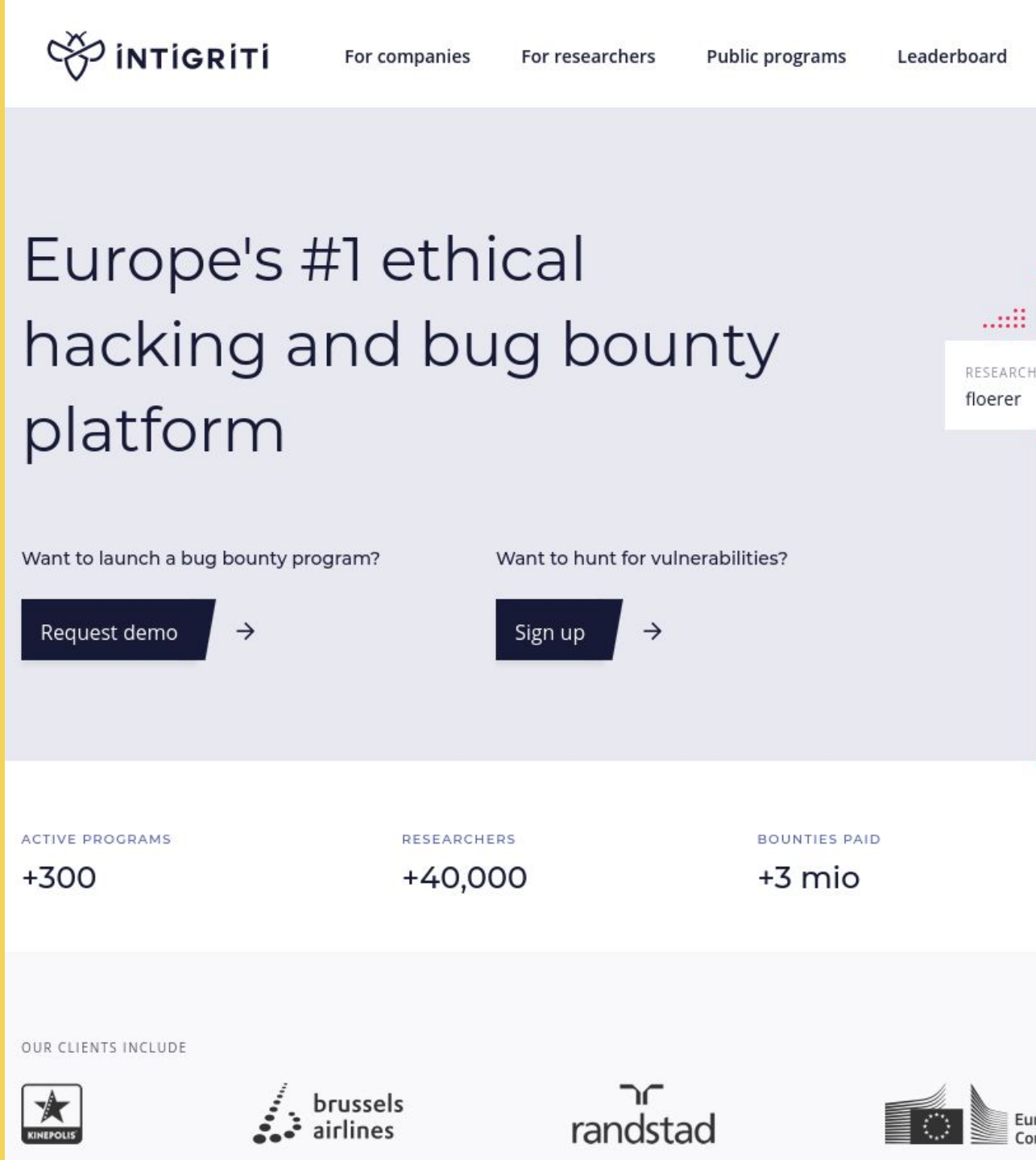
- Nalezené klíče
- (Lesní) požár
- Pandemie
- *Dlouhodobé dopady?*
  - Životní prostředí, olovnatý benzín
- …

Digitální svět

- Digitální podpisy/Auth token
- SQL injekce
- Ransomware/viry
- Remote Code Execution
  - 0-click iMessage
- Cross Site Scripting
-
- …

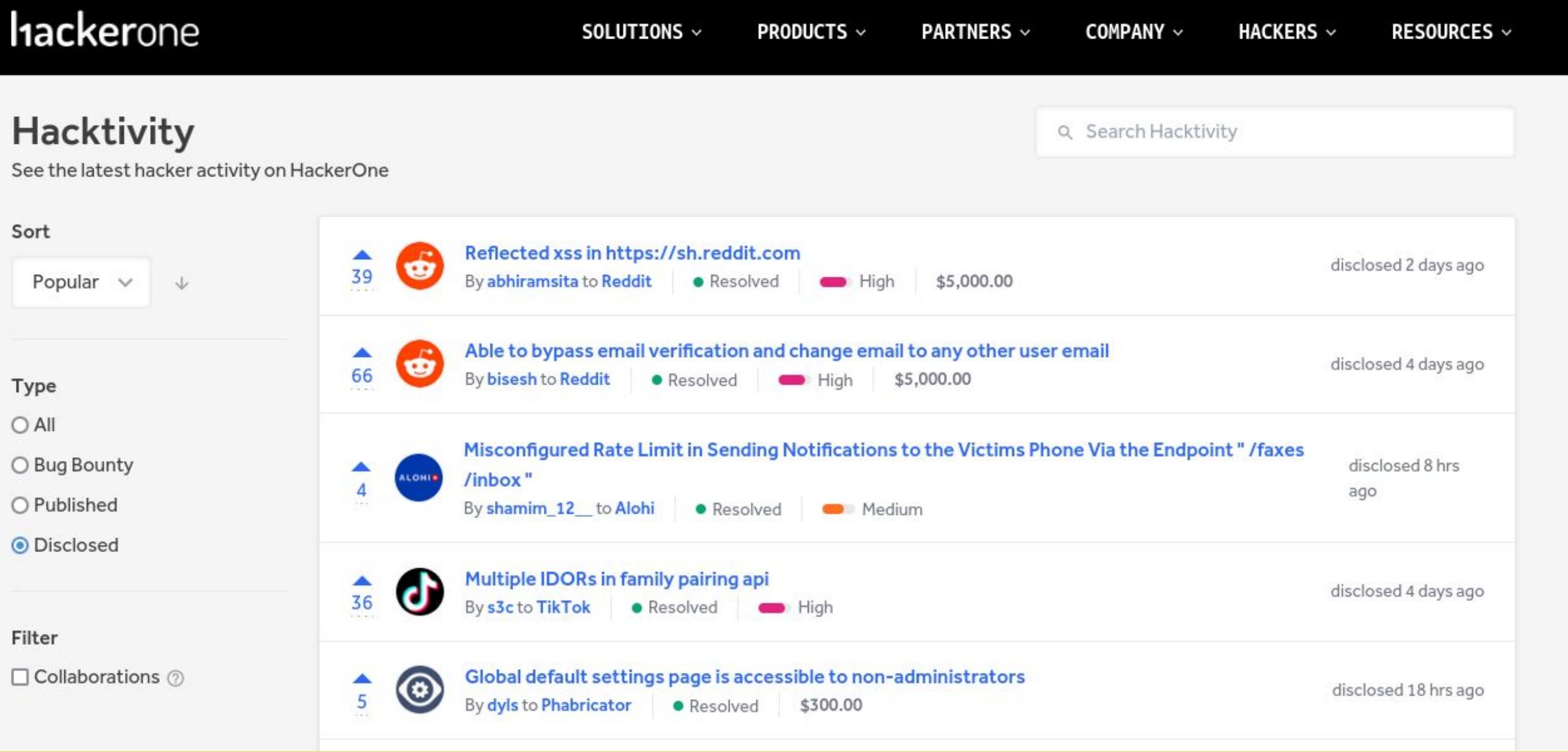
MUNI
FI

Platformy a programy



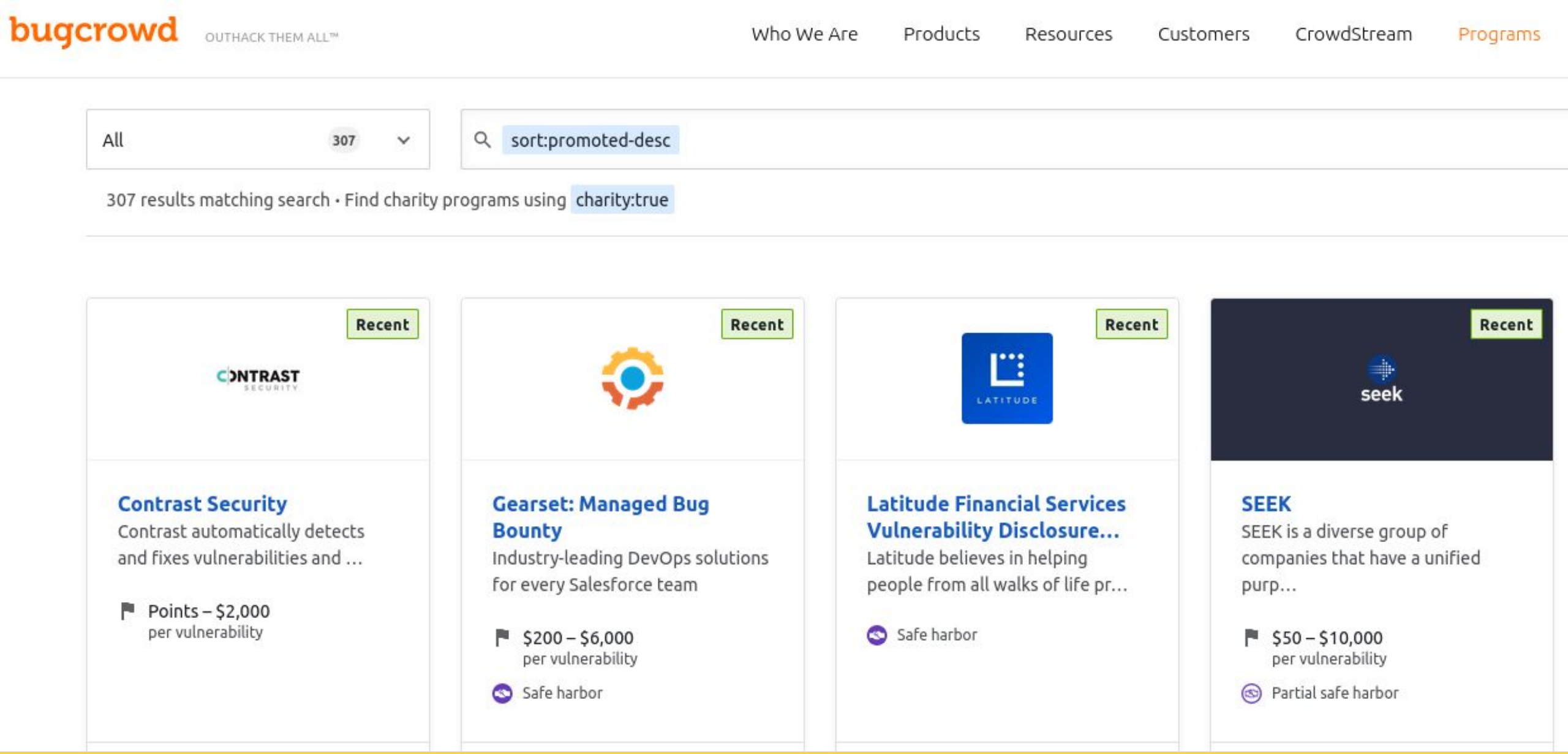
Platformy

- Umožňují registraci hackerům i firmám
- Příklady: HackerOne, Bugcrowd, Intigrity, Synack,...
- Vystupují jako moderátor mezi hackerem a konkrétním programem
  - Firmy na nich vytváří programy
  - Hackeři zde reportují zranitelnosti
  - Zprostředkovávají vyplácení bug bounties
- Chrání soukromí hackerů, programů
- Gamifikují hledání chyb
  - Signal, reputace, ranking



HackerOne - https://hackerone.com/hacktivity

MUNI FI



Bugcrowd - https://bugcrowd.com/programs

MUNI FI

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

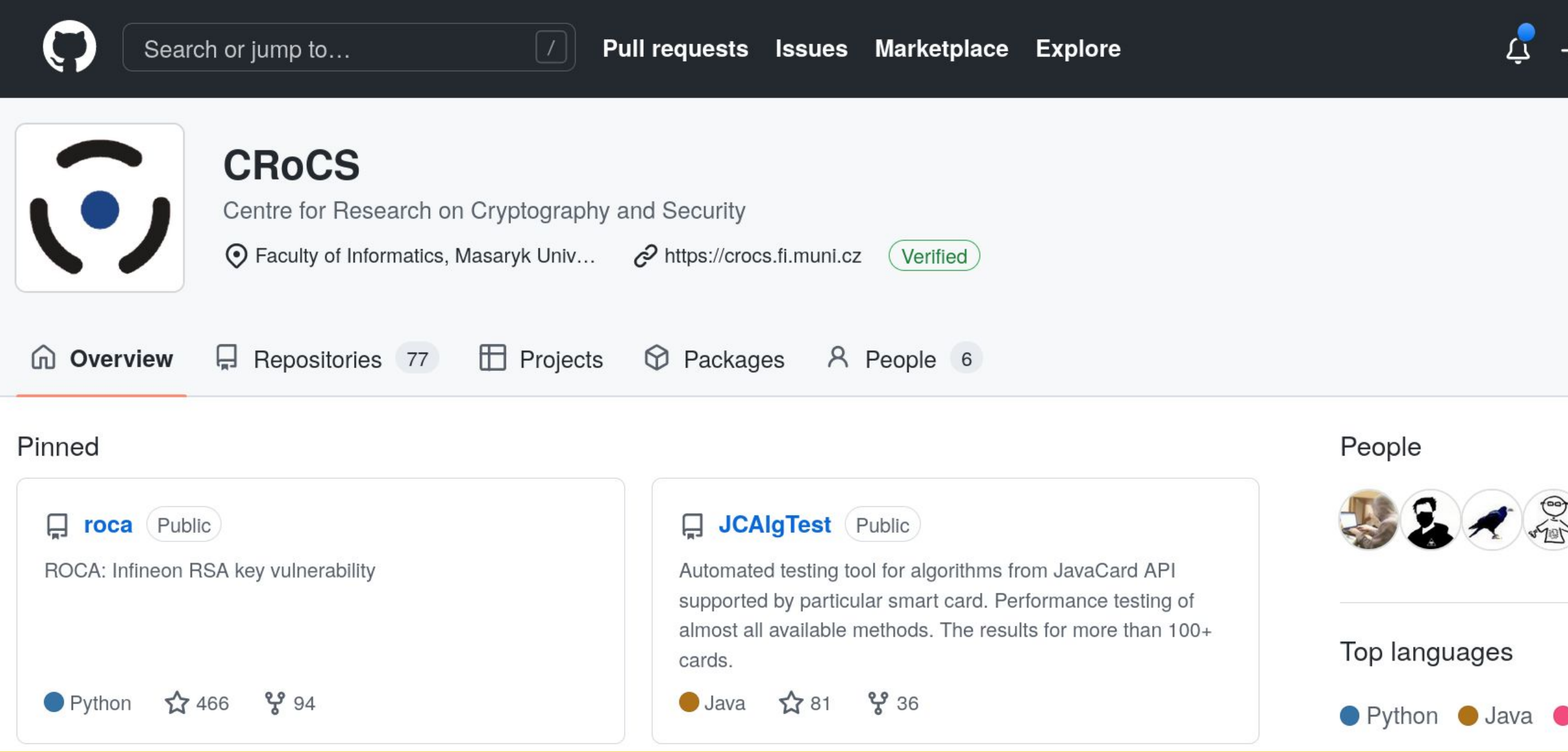
BOUNTIES PAID
+3 mio

Intigrity - https://www.intigriti.com/

MUNI FI

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**



Aplikace na sdílení kódu a spolupráce (Git “web frontend”)
https://github.com/crocs-muni/

MUNI FI

GitHub

How people build software

Submit report

https://bounty.github.com · @githubsecurity

Reports resolved	Assets in scope	Average bounty
980	25	$617

Přehled BBP GitHub - https://hackerone.com/github

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.

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.

Scopes

In Scope

Domain	**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. 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

Příklad assetu in scope z BBP GitHubu

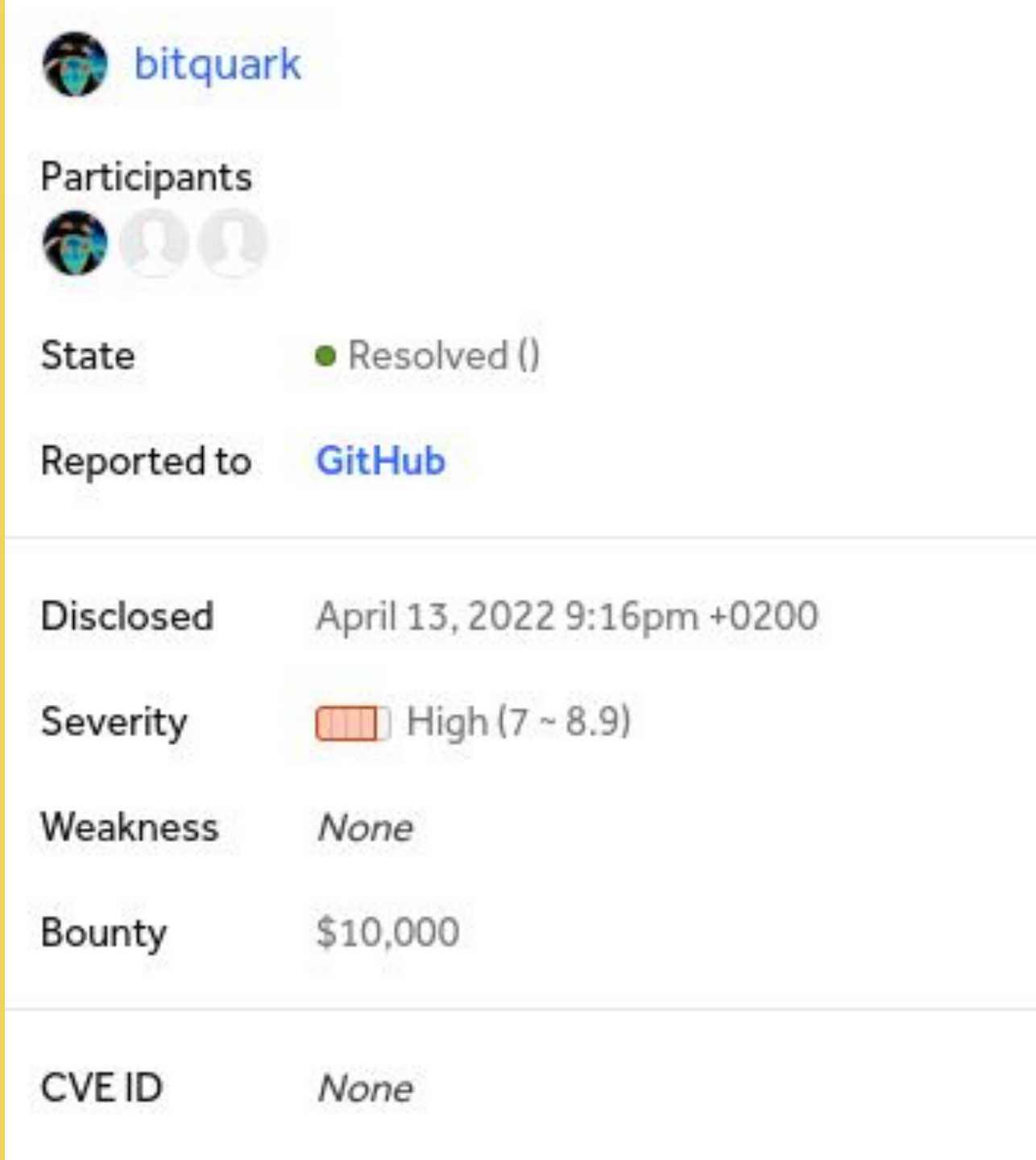
MUNI FI

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 Intigrity

MUNI
FI

Reportování chyb



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

Base Score

7.5
(High)

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)

CVSS 3.1 -
https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

MUNI FI

Po odeslání reportu…

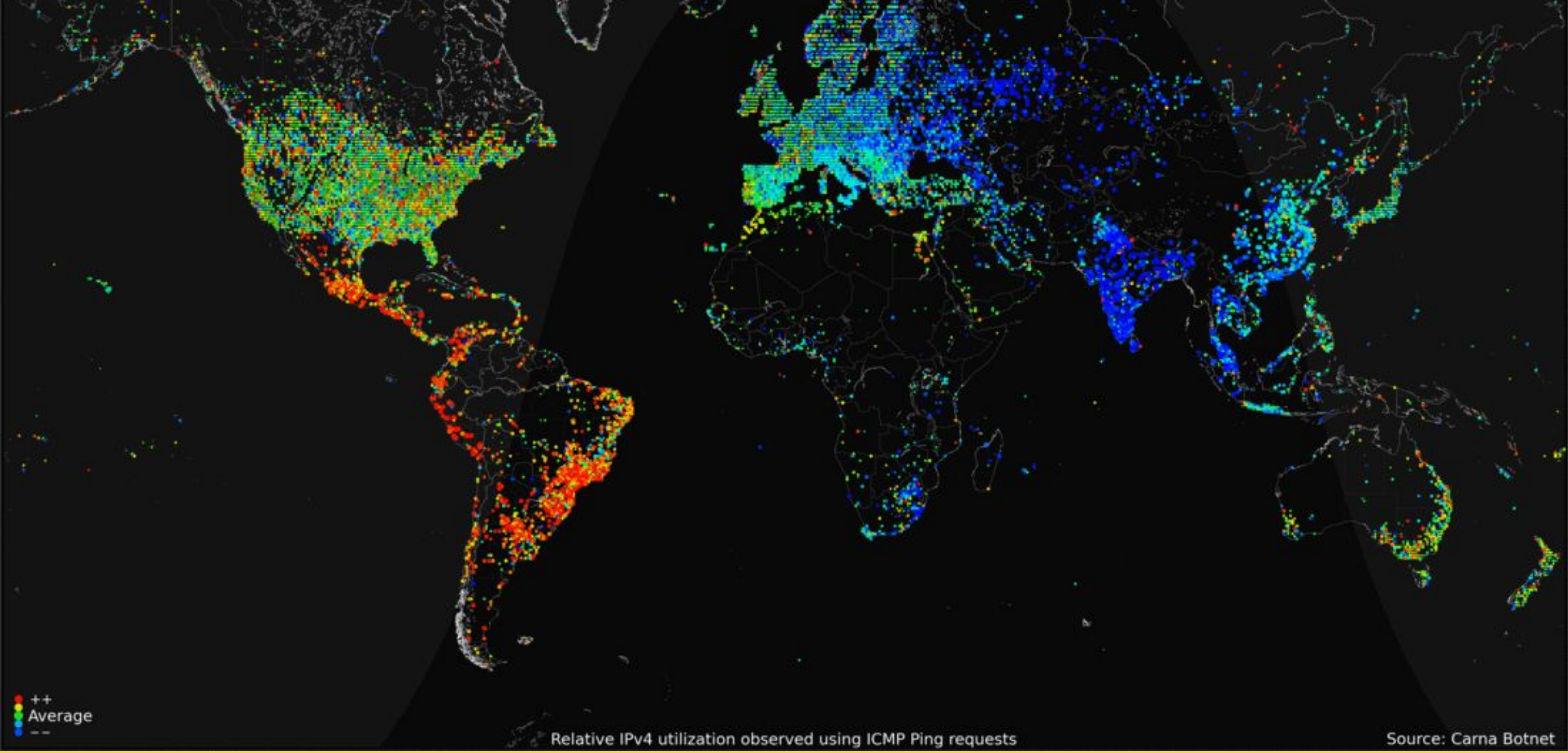
- **Čekání** na triage ze strany platformy nebo programu
  - V řádu dnů až týdnů
  - Non-applicable ~ hackování mimo scope, ztráta signálu
  - Informative ~ chyba existuje, ale není závažná
  - Duplicate ~ chyba existuje a je závažná, ale byli jste druzí…
- **Triage**
  - Doplnění dalších informací (např. 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)
  - Po společné 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]

MUNI FI

MUNI
FI

(Omylem) uniklé přístupové tokeny

Přístupové tokeny

(Omylem) uniklé přístupové tokeny

- Token je náhodný řetězec
  - Umožňuje přístup ke službě
  - `8537addd5d4834edf48e02fe25c3960370629aee4a2711c2c9e85afc933e5540`
  - 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

MUNI
FI

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 datumy

EUDCC: Duplicitní certifikáty

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

MUNI
FI

ROCA

doc. RNDr. Petr Švenda, Ph.D.

The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli

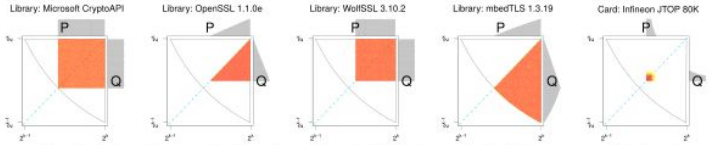
Matúš Nemec, Marek Sýs, Petr Švenda, Dušan Klinec, Vashek Matyáš
Centre for Research on Cryptography and Security, Masaryk University
Ca' Foscari University of Venice

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, PGP, 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.

Background – surprising biases in RSA public keys

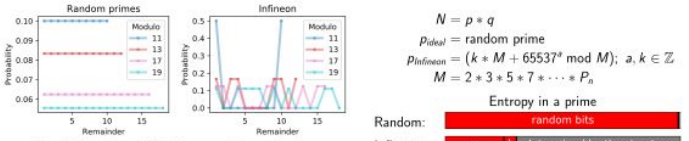
Švenda et al. [2] described how cryptographic libraries generate RSA primes in various ways, introducing subtle biases in the public keys, sufficient to classify the keys based on their origin. Infineon smartcards produced especially biased keys.



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.

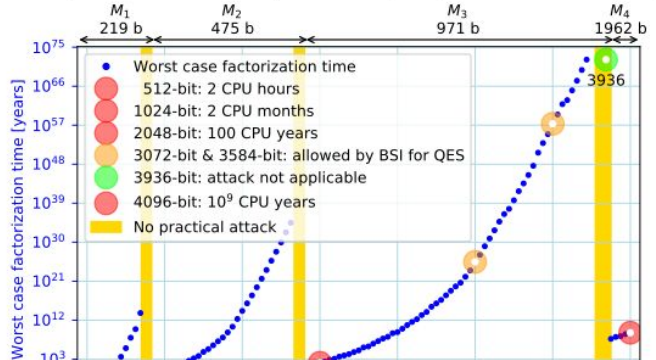


The distribution of RSA keys modulo small primes

$$N = p * q$$
$$p_{ideal} = \text{random prime}$$
$$p_{Infineon} = (k * M + 65537^a \bmod M);\ a, k \in \mathbb{Z}$$
$$M = 2 * 3 * 5 * 7 * \cdots * P_n$$

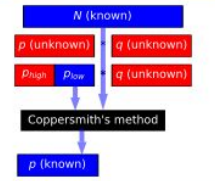
Factorization attack complexity

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.



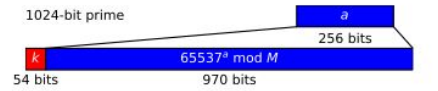
Coppersmith's factorization method

Coppersmith's method uses a partial knowledge of one of the primes to compute the factorization of an RSA modulus. At least half of the bits of the prime must be known. However, the method performs faster with more known bits. We use the method as a black-box tool.

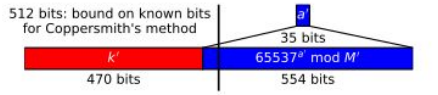


Making the attack practical

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 $65537^a \bmod M$. 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.

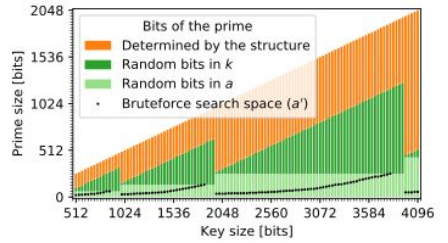


For the majority of RSA key sizes, the bit length of M (and $65537^a \bmod M$) is much larger than the required bound for the attack (one half of the prime's bit length). We find a smaller M' (a divisor of M), such that its size is still sufficient, yet the size of a' is significantly reduced when compared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



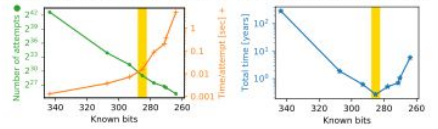
Entropy in primes

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.



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

Děkuje(me) za pozornost

MUNI
FI

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

MUNI

FI