
MŰEGYETEM 1782
JELEK A JELENBEN
A KIBERJÖVŐBŐL
VIK JÖVŐTERVEZŐ ELŐADÁS
Q ÉPÜLET, SIMONYI KÁROLY ELŐADÓTEREM
2025–03–05 17–00
BME VILLAMOSMÉRNÖKI ÉS INFORMATIKAI KAR
JÖVŐTERVEZŐ.BME
Sorozat a közösségi tudományról a Műegyetemen

Budapesti Műszaki és Gazdaságtudományi Egyetem
Villamosmérnöki és Informatikai Kar

A kiberbiztonság kihívásai

Internet-of-Things, mesterséges intelligencia, kvantumszámítógépek

Buttyán Levente
CrySyS Lab, BME
buttyan@crysys.hu

MŰEGYETEM 1782

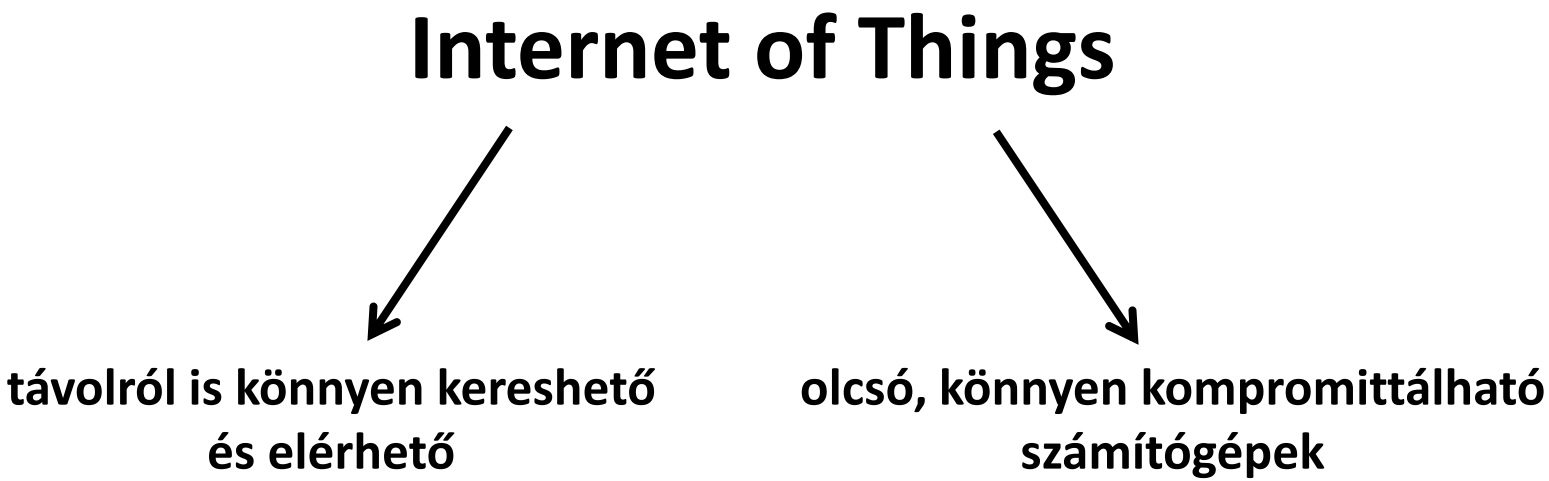
Adi Shamir makes 15 predictions for the next 15 years!

Keynote speech at Financial Crypto, February 2016.

IoT


Okos otthonok és épületek
Intelligens közlekedési rendszerek
Modern járművek
Felhő
Internet
Okos gyárak
Precíziós mezőgazdaság
Orvosi alkalmazások

A hacker perspektívája



Hacking a smart TV is easier than you think

Cybersecurity | Smart TVs | Wifi

New Evil PLC Attack Weaponizes PLCs to Breach OT and Enterprise Networks

Aug 16, 2022 Ravie Lakshmanan

Car Hacking, the Next Frontier of Cybersecurity

Security researchers hijack cars all the time. Here's v
automotive systems at a DEF CON hacking challeng

Perspective

Some Medtronic Insulin Pumps Can Be Hacked, FDA Warns

Hackers hit San Francisco transport systems

28 November 2016

You Can Hijack Nearly Any Drone Mid-flight Using This Tiny Gadget

Oct 27, 2016 Wang Wei

Lehetséges következmények

WIRED SECURITY POLITICS GEAR BACKCHANNEL BUSINESS MORE SIGN IN SUBSCRIBE

ANDY GREENBERG SECURITY JUL 21, 2015 6:00 AM

Hackers Remotely Kill a Jeep on the Highway—With Me in It

I was driving 70 mph on the edge of downtown St. Louis when the exploit be

Lehetséges következmények

WIRED

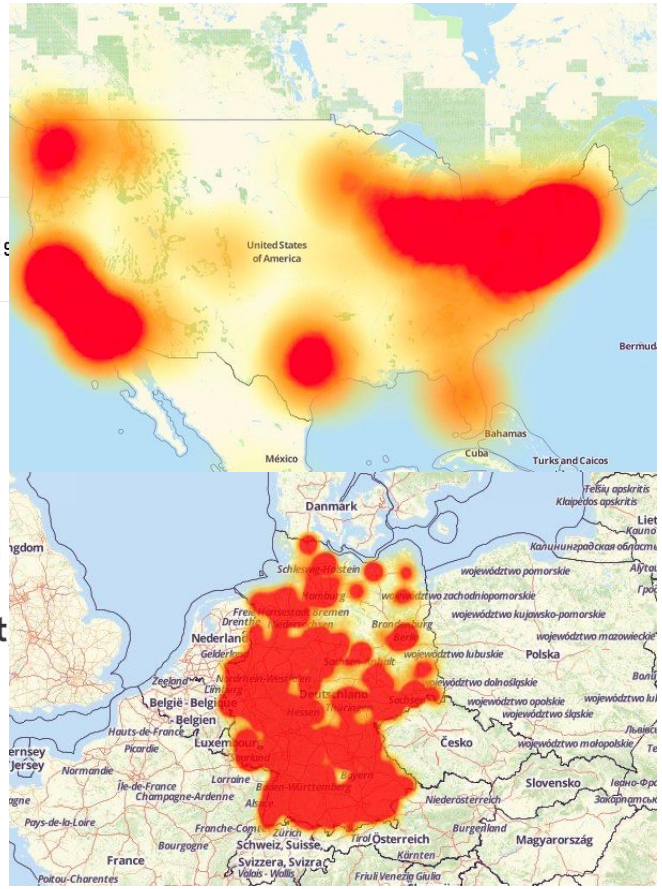
SIGN IN | SUBSCRIBE

FEATURED SWITCH TO A PRIVACY BROWSER WORK-FROM-HOME GEAR MAKE BETTER COFFEE WIRED-TES

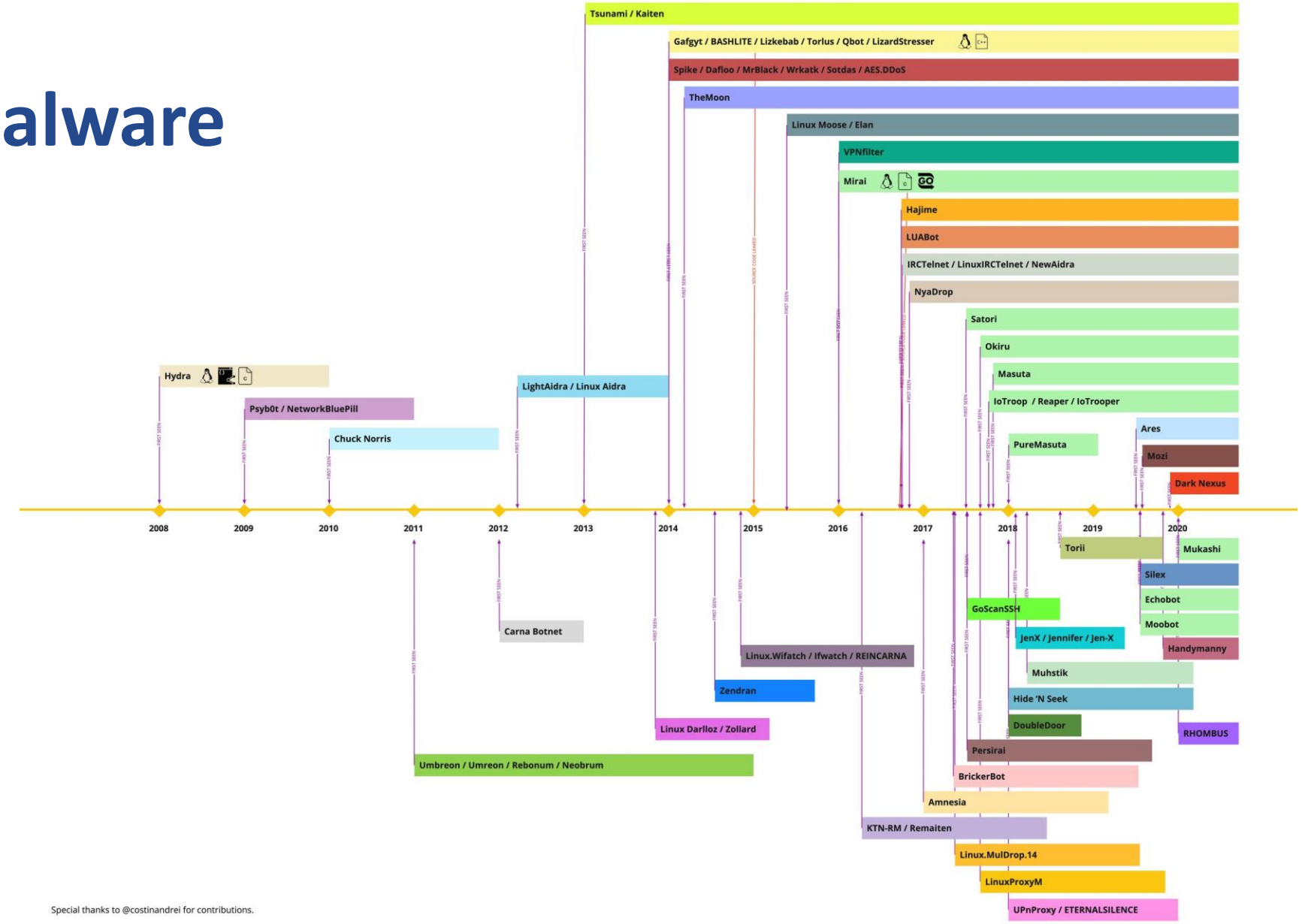
LAUREN GOODE MICHAEL CALORE BOONE ASHWORTH GEAR NOV 16, 2023 8:00 AM

Inside Mirai, the Hack that Broke the Internet

This week, we talk about the Mirai cyberattack that caused a massive internet blackout, the three young friends who wrote the calamitous code, and the FBI manhunt that followed.



IoT malware


Tsunami / Kaiten
Gafgyt / BASHLITE / Lizkebab / Torlus / Qbot / LizardStresser
Spike / Dafloo / MrBlack / Wrkatk / Sotdas / AES.DDoS
TheMoon
Linux Moose / Elan
VPNfilter
Mirai
Hajime
LUABot
IRCTelnet / LinuxIRCTelnet / NewAidra
NyaDrop
Satori
Okiru
Masuta
IoTroop / Reaper / IoTrooper
PureMasuta
Ares
Mozi
Dark Nexus
Hydra
Psyb0t / NetworkBluePill
Chuck Norris
LightAidra / Linux Aidra
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
Torii
Mukashi
Silex
Echobot
Moobot
Handymanny
RHOMBUS
GoScanSSH
JenX / Jennifer / Jen-X
Muhstik
Hide 'N Seek
DoubleDoor
Persirai
BrickerBot
Amnesia
KTN-RM / Remaiten
Linux.MulDrop.14
LinuxProxyM
UPnProxy / ETERNALSILENCE
Carna Botnet
Linux.Wifatch / Ifwatch / REINCARNA
Zendran
Linux Darlloz / Zollard
Umbreon / Umreon / Rebonum / Neobrum
Special thanks to @costinandrei for contributions.

SIMBIoTA: egy hatékony és hatásos megoldás

Hatékony

- Kis memória igény
- Gyors működés

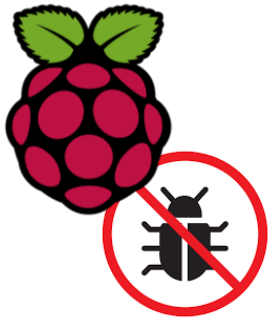
Hatásos

- Magas (90-98%) true positive detekciós ráta (korábban nem látott mintákra is!)
- Nagyon alacsony (0-1%) false positive ráta

Cs. Tamás, D. Papp, L. Buttyán, **SIMBIoTA: Similarity-Based Malware Detection on IoT Devices**, 6th International Conference on Internet of Things, Big Data and Security (IoTBDS), 2021.

D. Papp, G. Ács, R. Nagy, L. Buttyán, **SIMBIoTA-ML: Light-weight, Machine Learning-based Malware Detection for Embedded IoT Devices**, 7th International Conference on Internet of Things, Big Data and Security (IoTBDS), 2022. (Best Paper Award)

Simbiota.io – Az első antivírus Rpi-re



Simbiota
open-source IoT nano agent

FEATURES RESOURCES COMMUNITY ABOUT DOWNLOAD

SUMMARY

This nano agent detects and blocks malware on IoT devices. This is possible because it has a radically small memory footprint - under 10MB - and minimal computational overhead. Simbiota runs as a background process and finds 98% of known malware, therefore it immunizes your IoT platform against potential threats.

Raspberry malware protection is now available for everyone with Simbiota. Our mission is to make it available on all IoT and OT platforms.

DOWNLOAD FOR FREE EXPLORE ALL FEATURES

Cyber Resilience Act

Rendelet a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről

Célok:

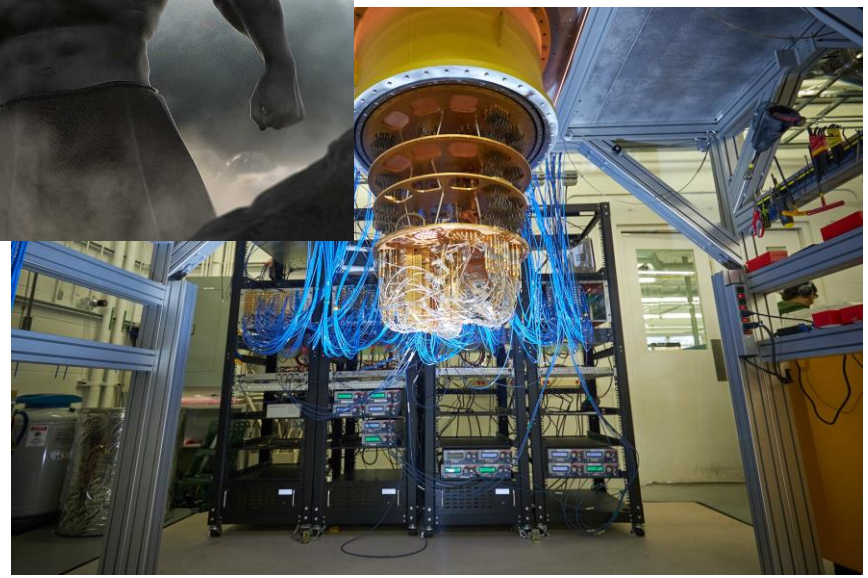
- A hardver- és szoftvertermékek kevesebb sebezhetőséggel kerüljenek forgalomba, és biztosítva legyen, hogy a gyártók a termék teljes életciklusa során komolyan vegyék a biztonságot.
- Megteremteni annak feltételeit, hogy a felhasználók a digitális elemeket tartalmazó termékek kiválasztásakor és használatakor figyelembe tudják venni a kiberbiztonságot.

Dávid és Góliát

Kriptográfia

- Adatok védelme algoritmikus módszerekkel
- Szimmetrikus kulcsú (konvencionális) és aszimmetrikus kulcsú (nyilvános kulcsú) sémák
- Gyakorlati biztonság
  - Óriási kulcstér
  - Nehéz matematikai problémák (pl. faktorizáció, diszkrét logaritmus)
- Példák: AES és RSA

A kvantum veszély

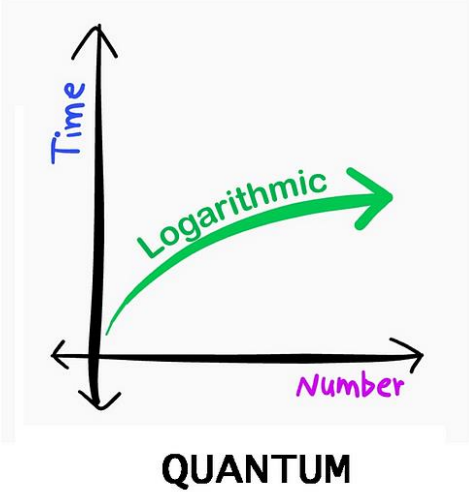


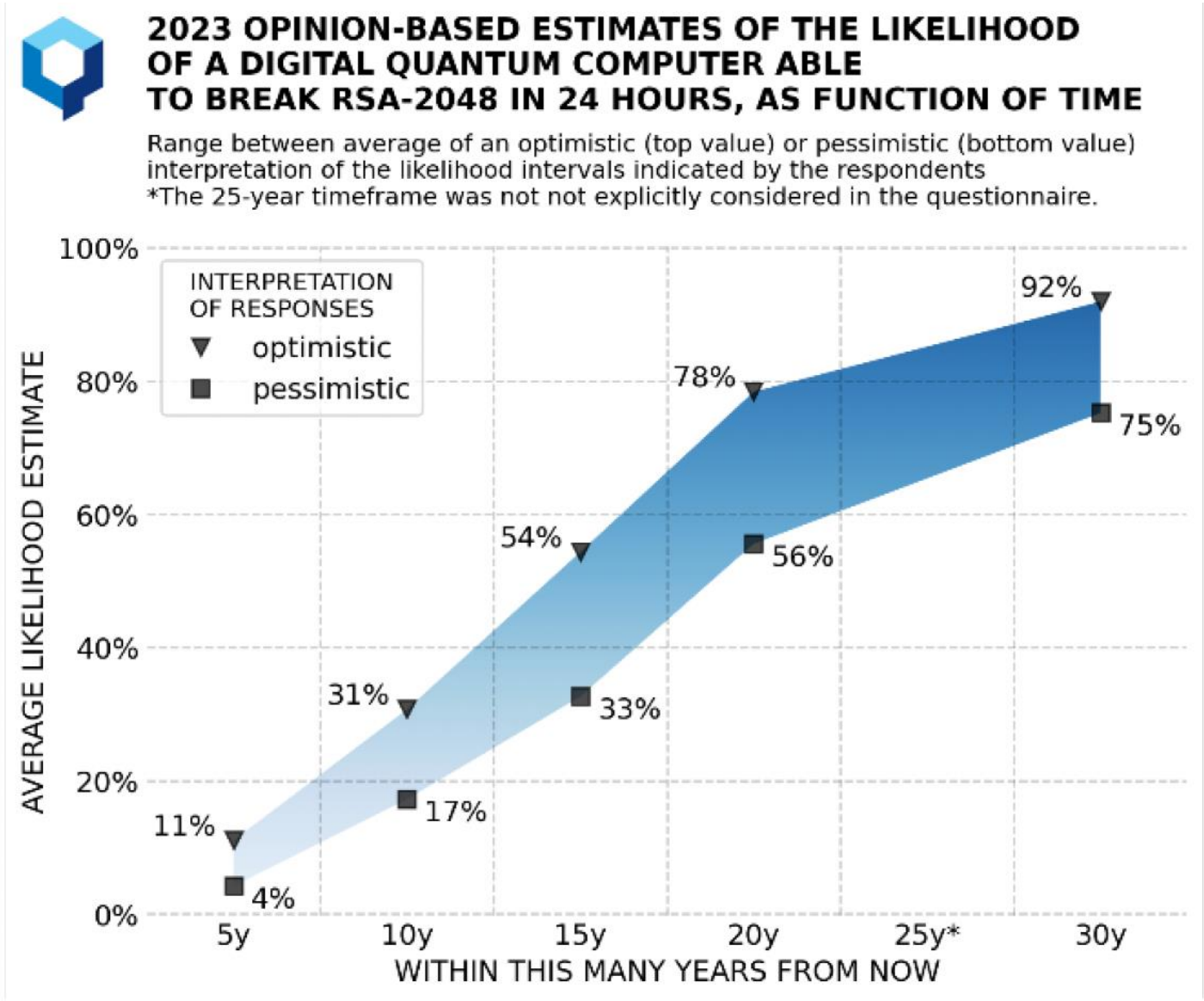
Grover algoritmus (1996):

- Lineáris keresés négyzetes gyorsítása
- **Hatékonyabbá teszi a kimerítő kulcskeresést**
- **Ellensúlyozható a kulcsok méretének növelésével**

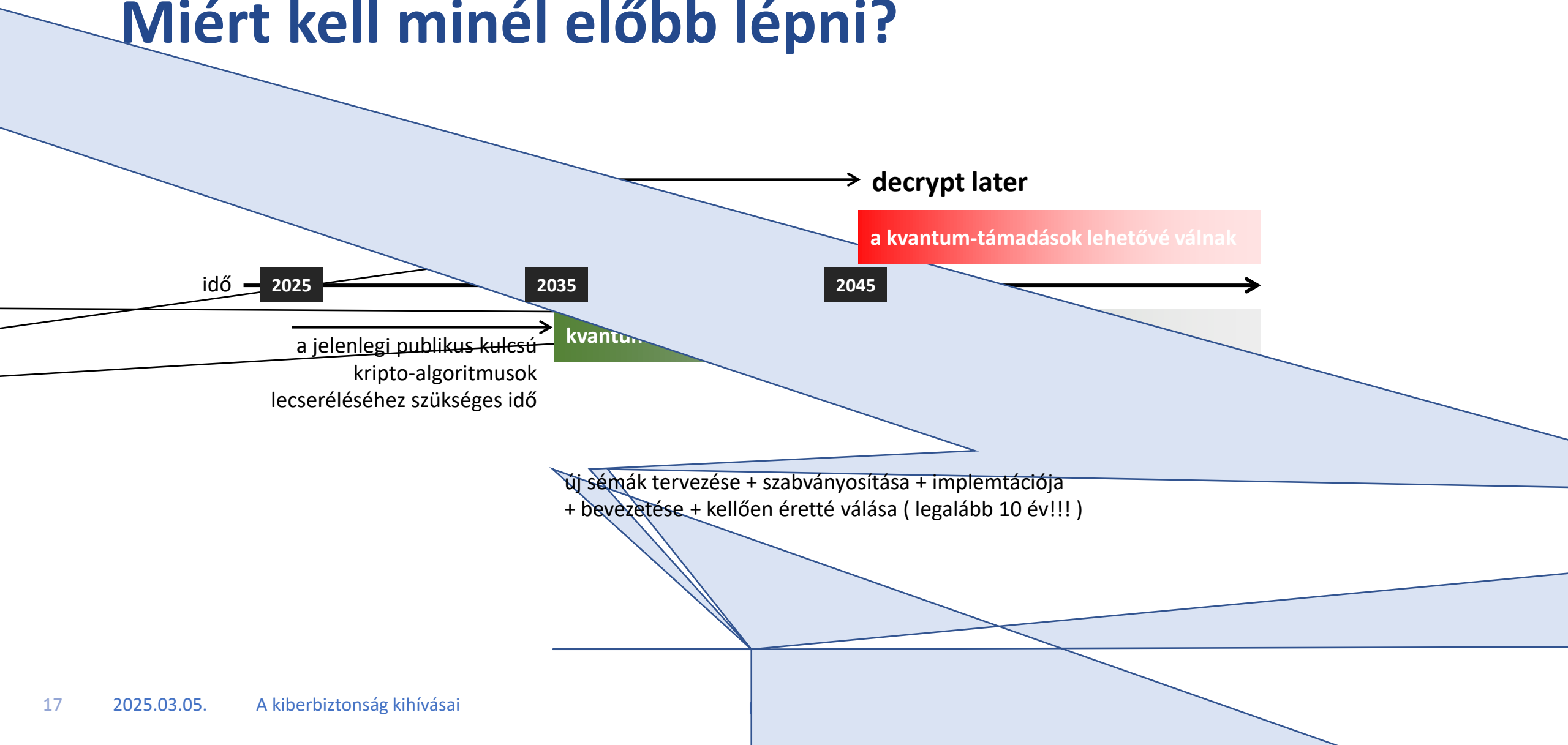
Shor algoritmus (1994):

- A faktorizáció (és a diszkrét log művelet) exponenciális gyorsítása
- **Lehetővé teszi a gyakorlatban használt nyilvános kulcsú kripto rendszerek hatékony feltörését**
- **A kulcsok méretének növelése nem oldja meg a problémát**



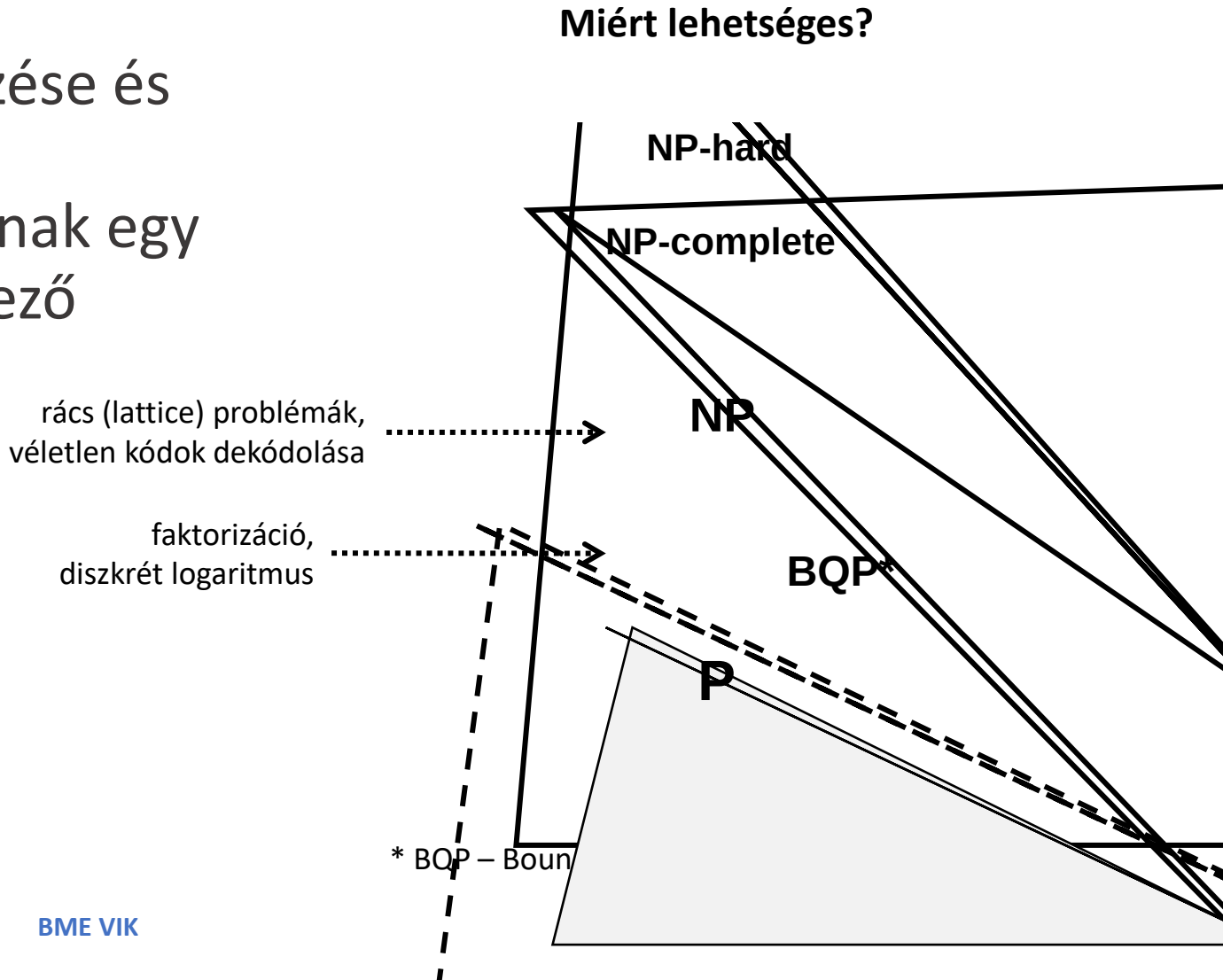

2023 OPINION-BASED ESTIMATES OF THE LIKELIHOOD OF A DIGITAL QUANTUM COMPUTER ABLE TO BREAK RSA-2048 IN 24 HOURS, AS FUNCTION OF TIME
Range between average of an optimistic (top value) or pessimistic (bottom value) interpretation of the likelihood intervals indicated by the respondents
*The 25-year timeframe was not not explicitly considered in the questionnaire.
INTERPRETATION OF RESPONSES
optimistic
pessimistic
AVERAGE LIKELIHOOD ESTIMATE
100%
80%
60%
40%
20%
0%
11%
4%
31%
17%
54%
33%
78%
56%
92%
75%
5y
10y
15y
20y
25y*
30y
WITHIN THIS MANY YEARS FROM NOW

Miért kell minél előbb lépni?



Posztkvantum kriptográfia (PQC)

Olyan kripto-algoritmusok tervezése és elemzése, melyek hagyományos számítógépen futnak, de ellenállnak egy kvantum-számítógéppel rendelkező támadónak is



NIST

https://csrc.nist.gov/projects/post-quantum-cryptography

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

PROJECTS | POST-QUANTUM CRYPTOGRAPHY

Goal: PQC transition by 2035

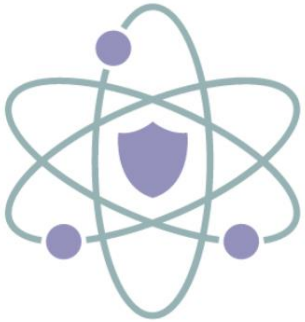
Post-Quantum Cryptography PQC

Post-Quantum Cryptography Standardization

Short URL: https://csrc.nist.gov/pqc-standardization

FIPS 203, FIPS 204 and FIPS 205, which specify algorithms derived from CRYSTALS-Dilithium, CRYSTALS-KYBER and SPHINCS+, were published August 13, 2024.

Additional Digital Signature Schemes - Round 1 Submissions



Post-Quantum Cryptography Alliance

Alliance seeks to address the security challenges posed by quantum computing through the development and adoption of post-quantum cryptography

---

SAN FRANCISCO, CA – FEBRUARY 6, 2024 – The Linux Foundation is excited to announce the launch of the Post-Quantum Cryptography Alliance (PQCA), an open and collaborative initiative to drive the advancement and adoption of post-quantum cryptography. The PQCA brings together industry leaders, researchers and developers to address cryptographic security challenges posed by quantum computing, through the production of high-assurance software implementations of standardized algorithms, while supporting the continued development and standardization of new post-quantum algorithms.

MI – Barát vagy ellenség?

Generative AI is the new strategic battleground

Weaponization of AI

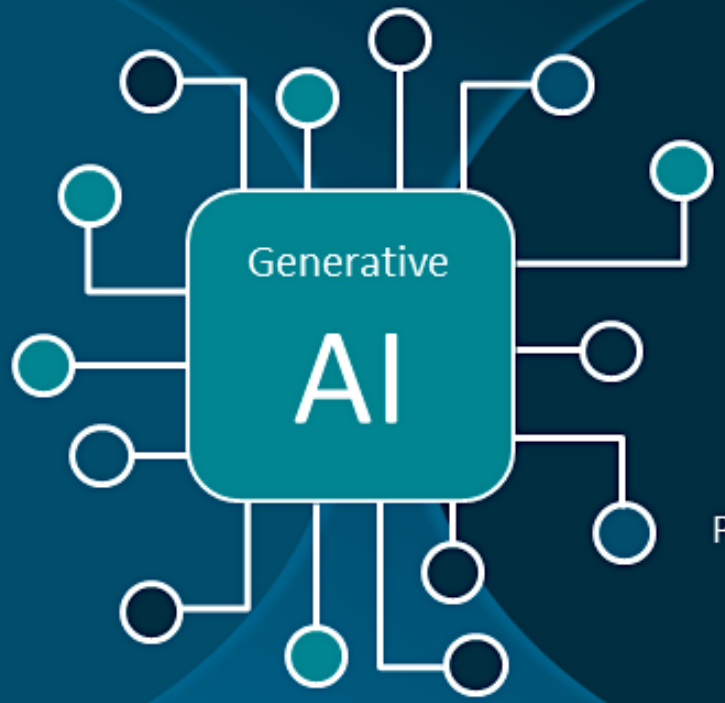
More threat actors to launch attacks

More convincing phishing campaigns

New deep fake social engineering schemes

Malware mutation

Exploit software vulnerabilities



AI to augment cybersecurity

Boost cybersecurity SOC analysts

Breach risk predictions

Enhance cybersecurity posture

Asset inventory management

Prioritize vulnerability remediations

Accelerate resolution time

A gépi tanulás számos biztonsági problémája ismert (pl. evasion, poisoning, model stealing, ...)

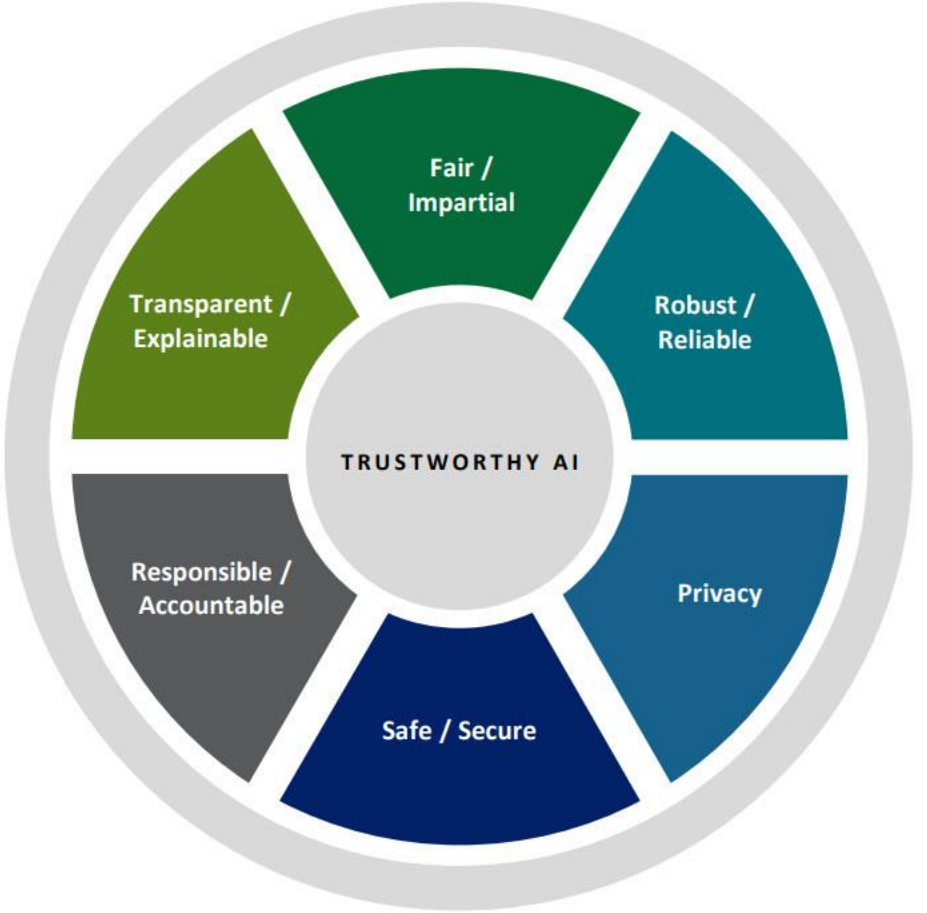
Az MI kritikus rendszerekben történő alkalmazásának biztonsági kockázatai vannak

Szabályozási követelmények (pl. EU AI Act)

Hogyan becsüljük és kezeljük a kockázatokat? Mitől lesz az AI biztonságosan alkalmazható?

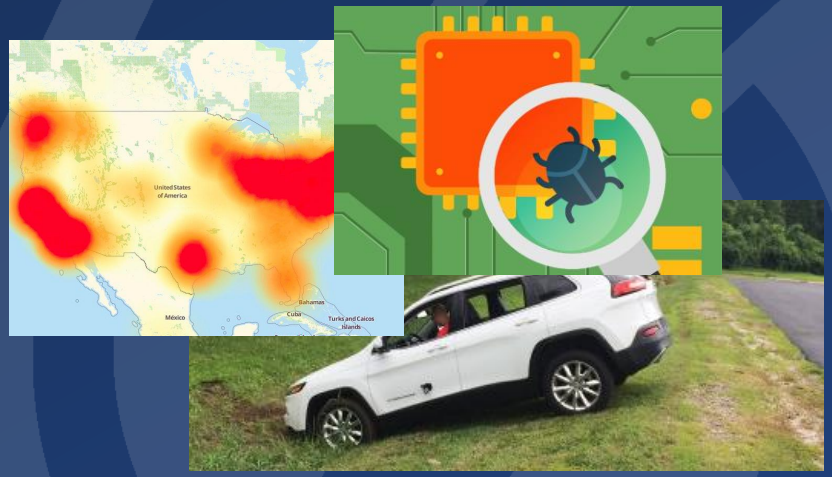
THE CHALLENGES OF USING AI IN CRITICAL SYSTEMS

Megbízható MI

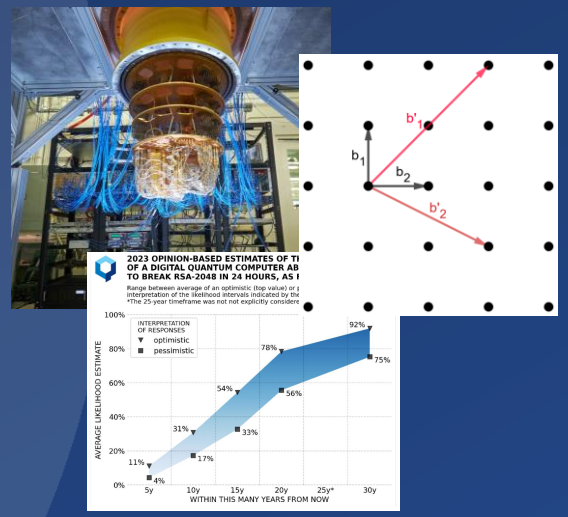


Budapesti Műszaki és Gazdaságtudományi Egyetem
Villamosmérnöki és Informatikai Kar

A kiberbiztonság kihívásai



IoT eszközök védelme kártevők ellen



Posztkvantum kriptográfia

Megbízható MI

MŰEGYETEM 1782