Panorama e Tendências da Cibersegurança no Brasil

Prof. Avelino Francisco Zorzo
Escola Politécnica – PUCRS
avelino.zorzo@pucrs.br

UNB - 2026

Contexto

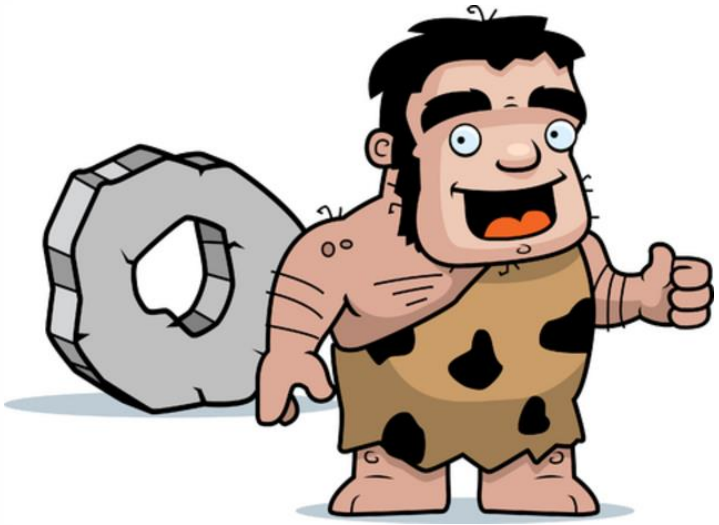
Onde estamos

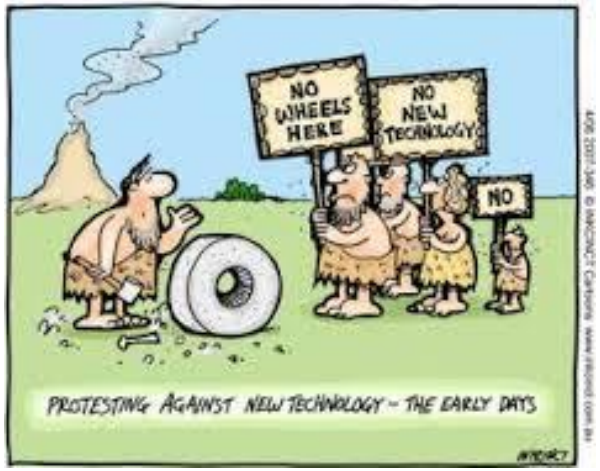
Para onde vamos

Contexto

Evolução na sociedade

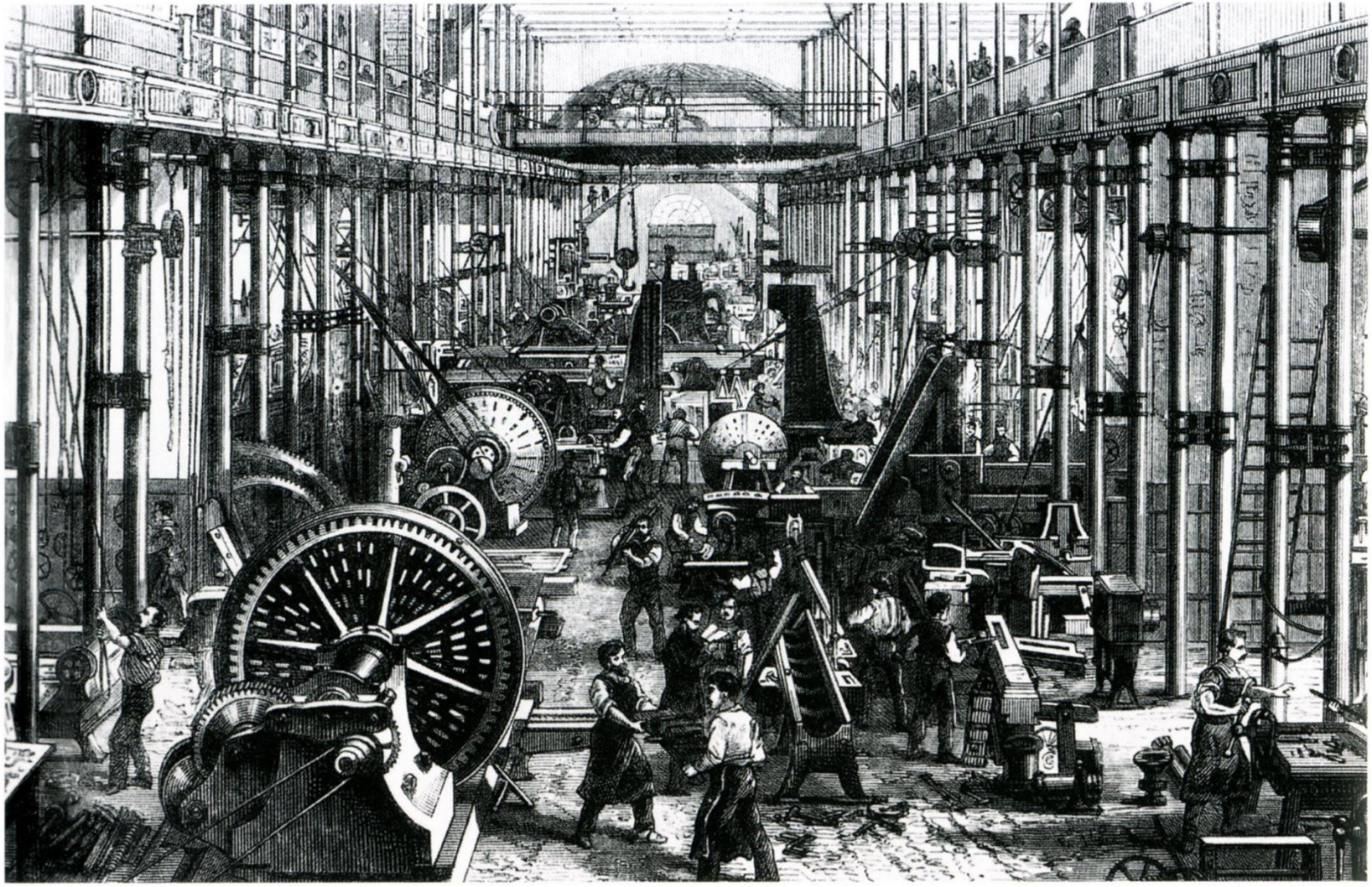
Há muito tempo atrás …





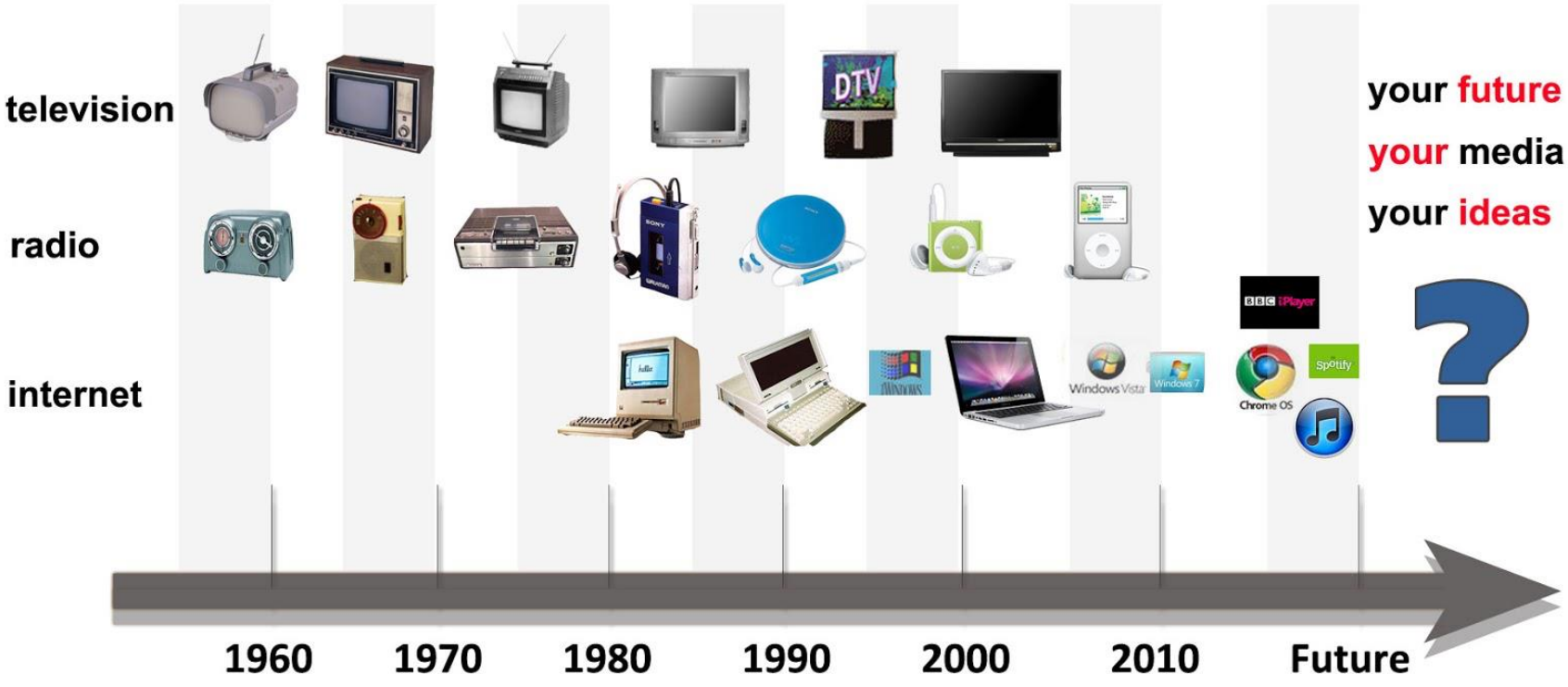
Há muito tempo atrás …

Revolução industrial



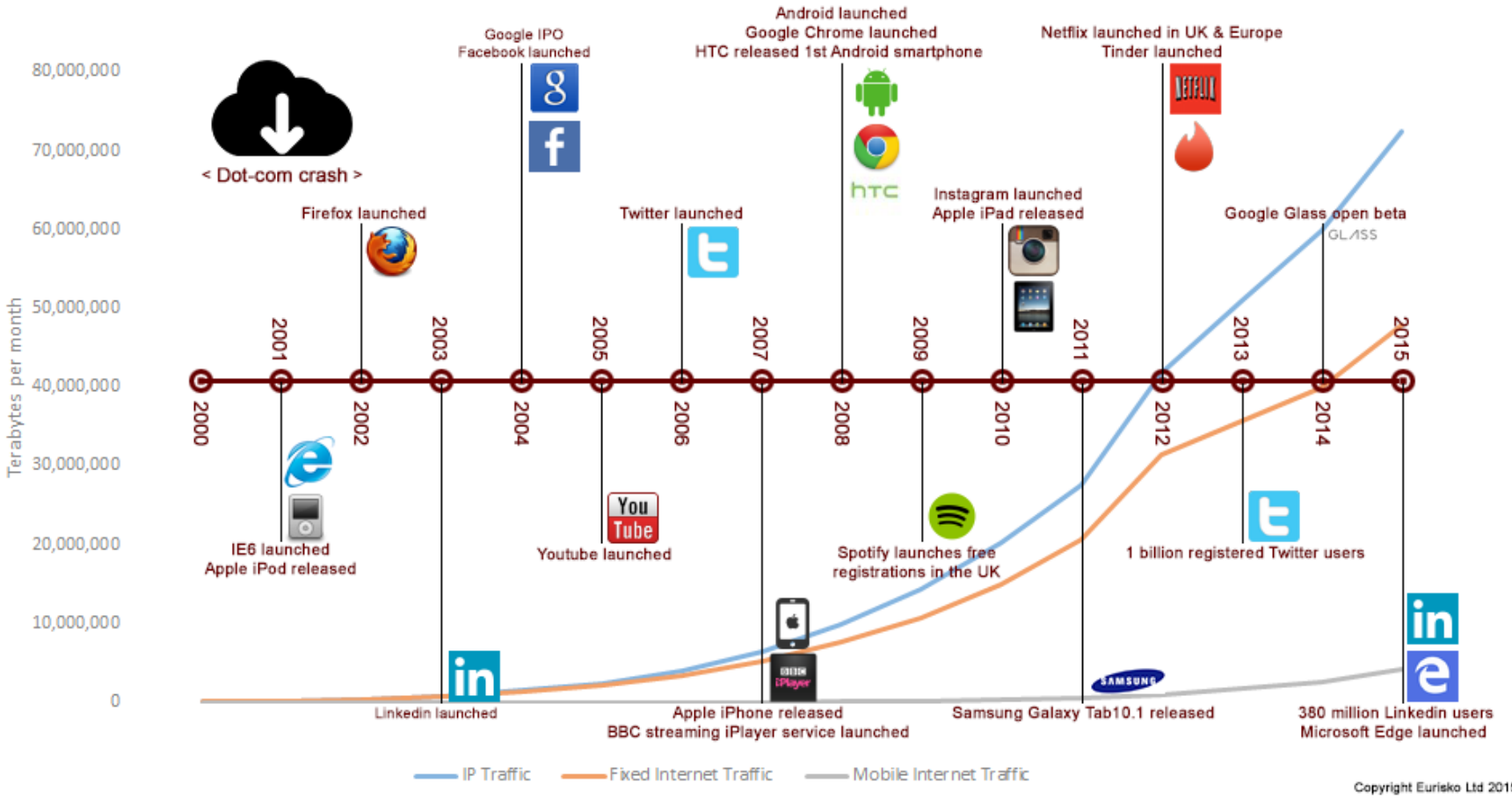
Evolução dos celulares

Mídia


television
radio
internet
DTV
your future
your media
your ideas
BBC iPlayer
Spotify
Chrome OS
Windows Vista
Windows 7
1960
1970
1980
1990
2000
2010
Future

Internet

Internet technology / Internet and IP traffic



Físico vs Digital

Física
- Eletricidade
- Aeronáutica
- ....

Biologia
- Alimentos
- Corpo humano
- ....

Mundo Físico
(conhecido (?))

Mundo Digital
(novo!!)

Internet

Algoritmo

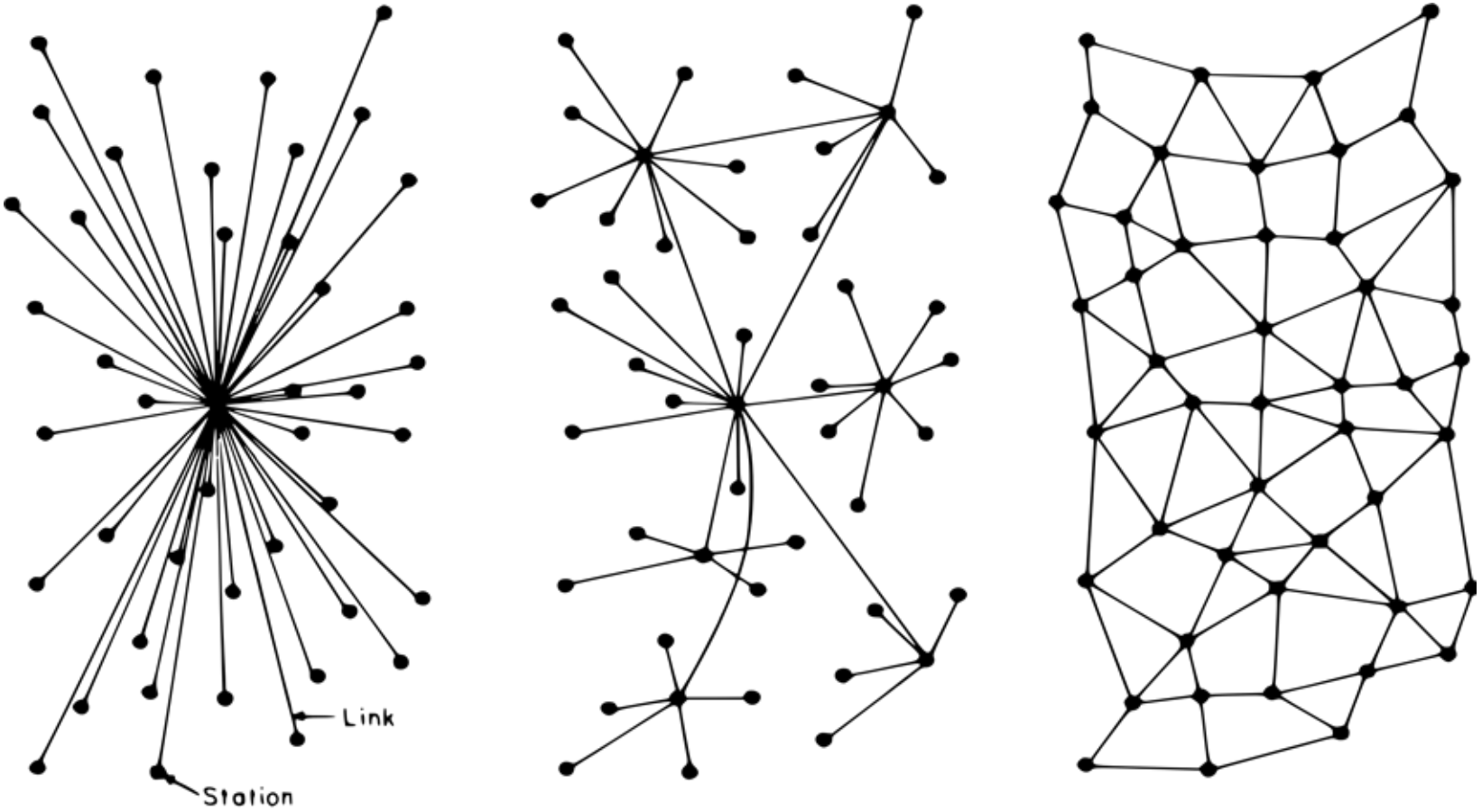
Robôs

Inteligência Artificial

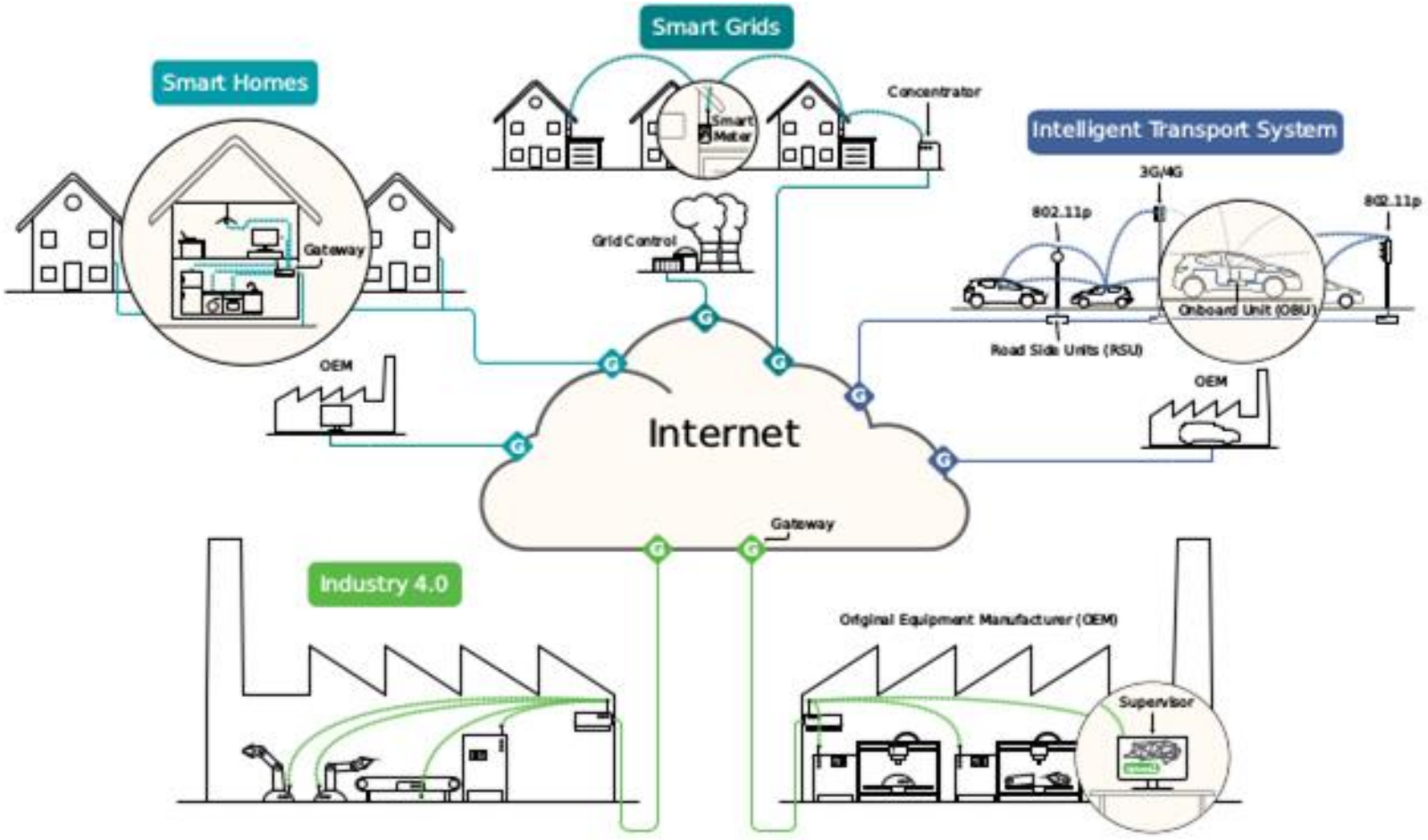
Criptografia

Mundo Digital

- Centralizado → Distribuído

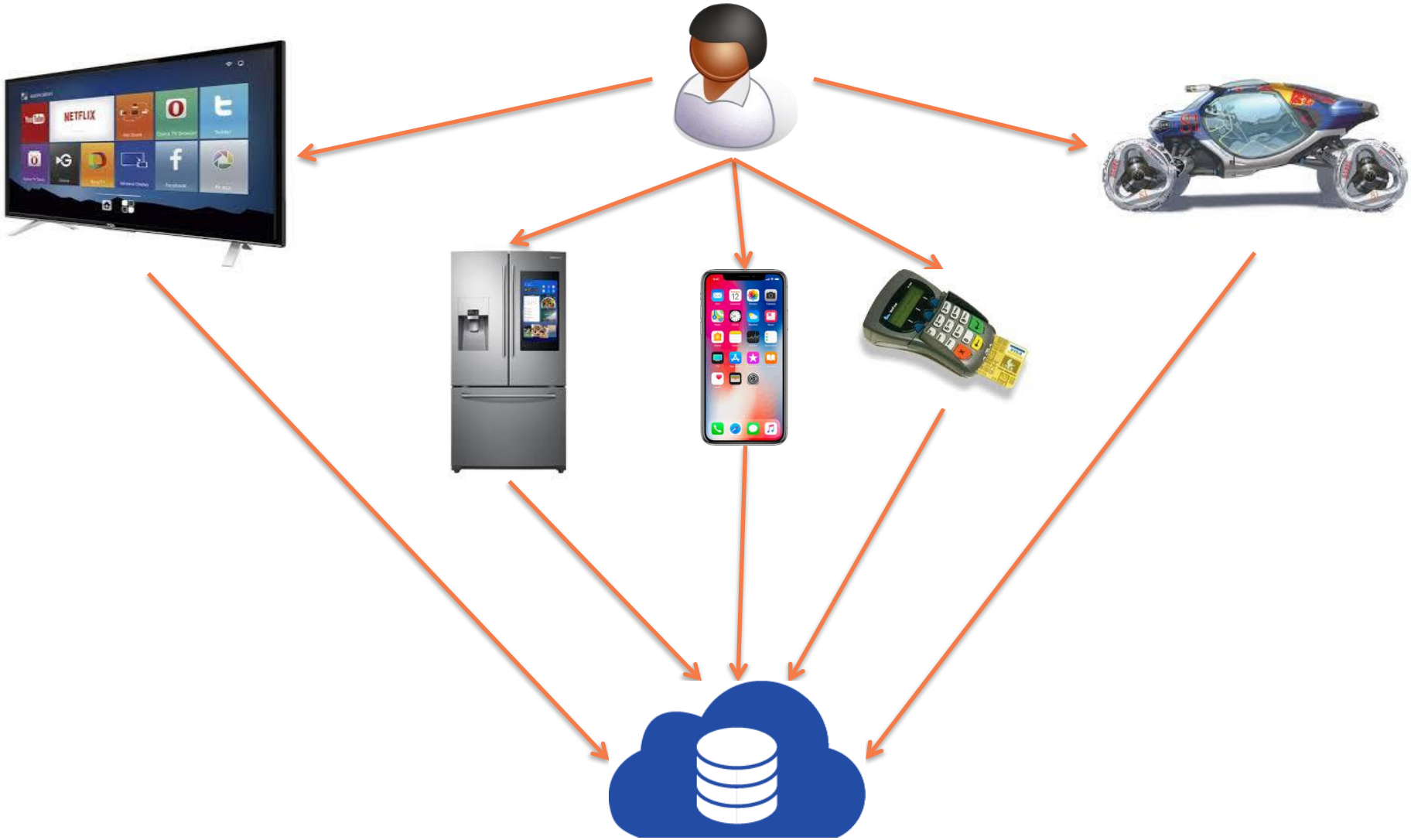


Mundo Digital - Smart *

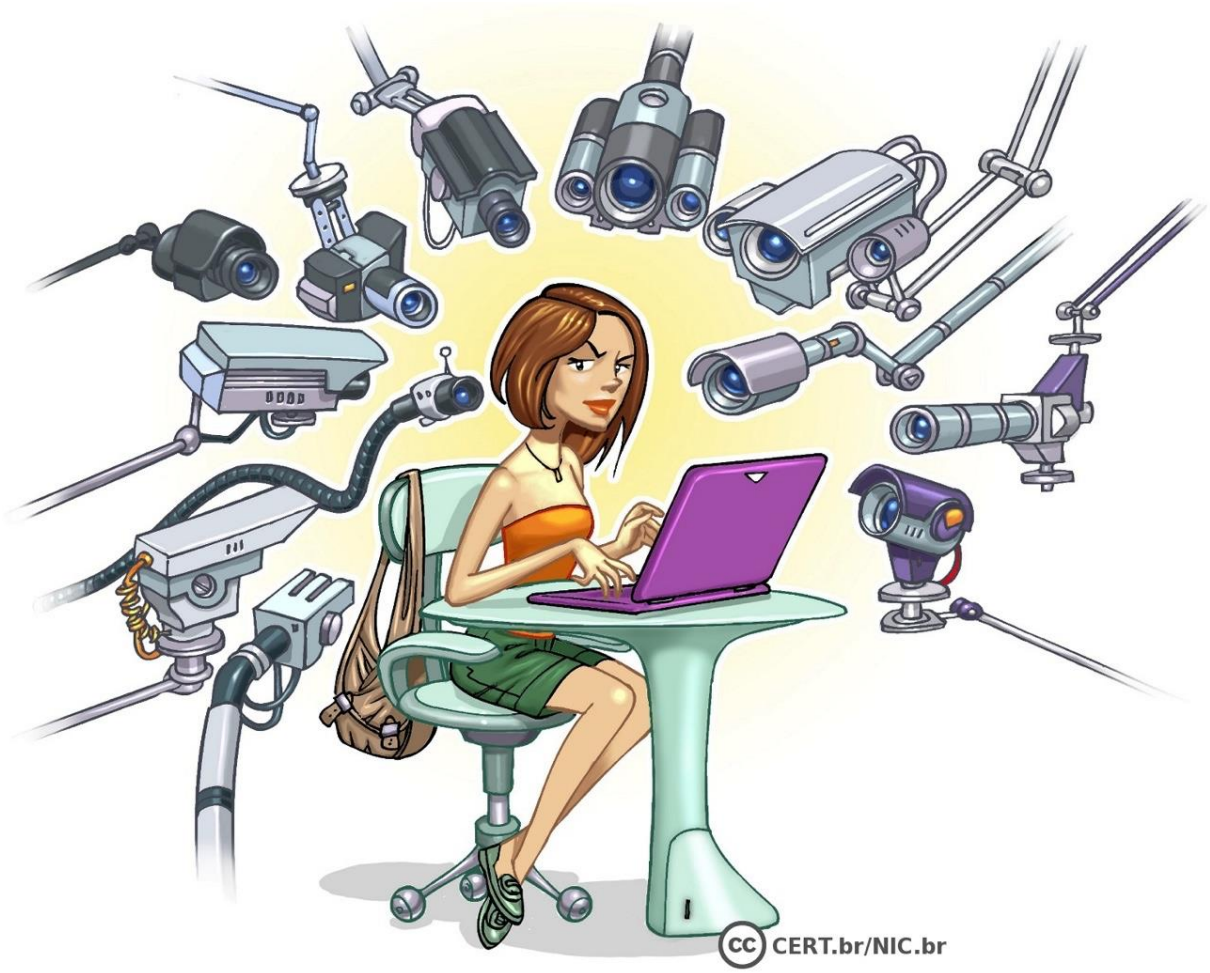


Fonte: Boudguiga, et al., "Towards better availability and accountability for iot updates by means of a blockchain,"

Mundo Digital - Dados

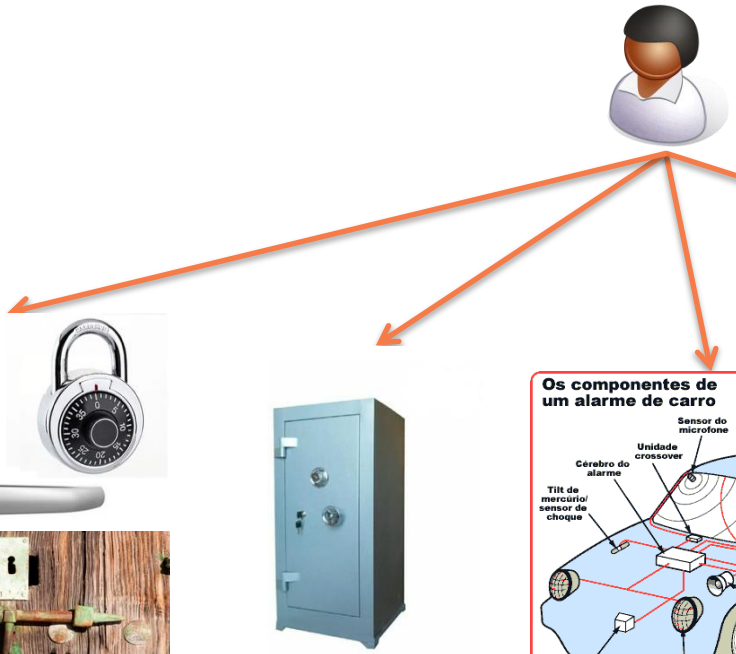


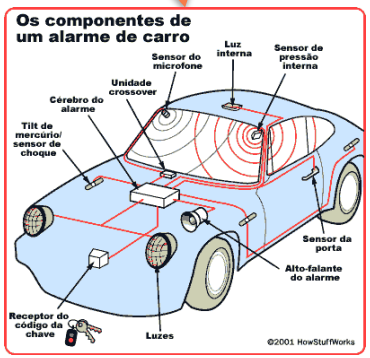
Mundo Digital – Redes sociais



Onde estamos cibersegurança

Segurança no Mundo Físico





Objetivos em segurança

Teoria

Defesa

Primitivas de segurança

Algoritmos para quebra de primitivas

Ataque

Implementação

Como sistemas falham na prática

Prática

Algoritmos, protocolos, ferramentas

Soluções

- Algoritmos de criptografia
  - AES, RSA, ECC, SHA-2, SHA-3, …
- Protocolos
  - TLS/SSL, IPSec, RSADSA, ECDSA, DH, ECDH, …
- Post-quantum cryptography
  - ML-KEM (Kyber), ML-DSA (Dilithium), …
- Ferramentas/soluções
  - ....

Ferramentas/soluções

- Antivirus e antimalware
  - Norton, TotalAV, Surfshark, BitDefender, Guardio,…
- Autenticação com diversos fatores (MFA)
  - Google and Microsoft authenticators, Authy, ..
- Cifragem de disco
  - BitLocker, FileVault, VeraCrypt, Trend Micro, …
- Firewalls
  - Fortinet FortiGate, Check Point …, Cisco …, pfSense
- IDS/IPS
  - Snort, Suricata, Cisco Security, Trelix, Trend Micro, …

Ferramentas/soluções

- Prevenção de perda de dados (DLP)
  - Forcepoint, Symantec, Trellix, …
- Varredura de vulnerabilidade
  - Nessus, QualysGuard, OpenVAS, …
- Pentesting
  - vPenTest, NodeZero, Metasploit, Burp, Nmap, …
- Gestão de identidades
  - Okta, Ping Identity, OneLogin, CiberArk, …
- Outras: DevSecOps, OWASP, …

Panorama nos programas de pós-graduação

Número de programas

Total de Programas de pós-graduação							Totais de Cursos de pós-graduação				
Total	ME	DO	MP	DP	ME/DO	MP/DP	**Total**	ME	DO	MP	DP
94	29	2	16	0	44	3	**141**	73	46	19	3

– 19ª área em número de programas
– 6ª no Colégio da Exatas, Tecnológicas e Multidisciplinar
– maior área: Interdisciplinar com 417 programas
– menor área: Ciências e Humanidades para Educação Básica com 15 programas

94 programas em 74 instituições (diferentes *campi*)

Produções reportadas 21-24

- **Total de produções:** 58.223
- **Relacionadas à Segurança*:** ~2.800 (4,8%)
- **Tipo de Produção:**
  - Bibliográfica: 1.926
    - » 1.193 em eventos; 624 em periódicos; livros/capítulos
  - Técnica: 871 (diversos)
- **Produções nas 74 instituições**

***Palavras-chave:**
segurança, *security*, criptografia, *cryptography*, *crypto*, privacidade, *privacy*, ciber, *cyber*, autenticação, *authentication*, forense, *forensic*, *malware*, *ransomware*, *botnet*, *phishing*, intrusão, *intrusion*, vulnerabilidade, *vulnerability*, lgpd, gdpr, *blockchain*, anonimização, *anonymization*, esteganografia, *steganography*

Principais tópicos

- **Tecnologias Emergentes**
  - Combinação de **Criptografia e Blockchain:** maior volume de trabalhos → descentralização.
- **Segurança Prática**
  - **Malware e Ameaças** → defesa ativa e resposta a incidentes.
- **Impacto Regulatório**
  - **Privacidade e Proteção de Dados** → LGPD
- **Outros**
  - Infraestrutura e redes seguras (zero-trust, cloud e 5G); IA aplicada à segurança; PQC; ZKP; criptografia homomórfica

Principais tópicos

Tópico	#	Assuntos
Criptografia e *blockchain*	489	Algoritmos criptográficos, livros-razão distribuídos (*ledgers*) e *smart contracts*.
Malware e ameaças	470	Deteção de vírus, ataques de *phishing*, detecção de intrusão e análise de *botnets*.
Privacidade e proteção de dados	395	LGPD/GDPR, técnicas de anonimização e modelagem de ameaças à privacidade.
Segurança em IoT e SCF	129	Segurança aplicada à Internet das Coisas e Sistemas Ciber-Físicos (Redes MQTT, Indústria 4.0).
Forense e vulnerabilidades	112	Investigação forense digital, análise de vulnerabilidades em código e busca de *exploits*.
Gestão e governança	68	Políticas de segurança, conformidade, gestão de riscos e governança de TI.

Para onde vamos em cibersegurança?

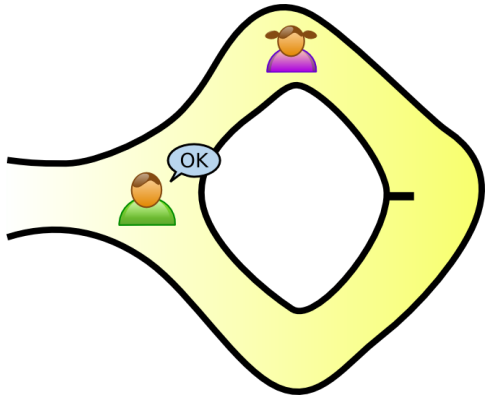
Desafios: Segurança e privacidade

- Aumento de ataques mais sofisticados
- Impacto de ferramentas/técnicas de IA
- Cumprir legislação vigente: GDPR, LGPD, …
- Desenvolver soluções pós-quântica
- Garantir segurança em aplicações em nuvem ou computação de borda
- Conhecimento geral

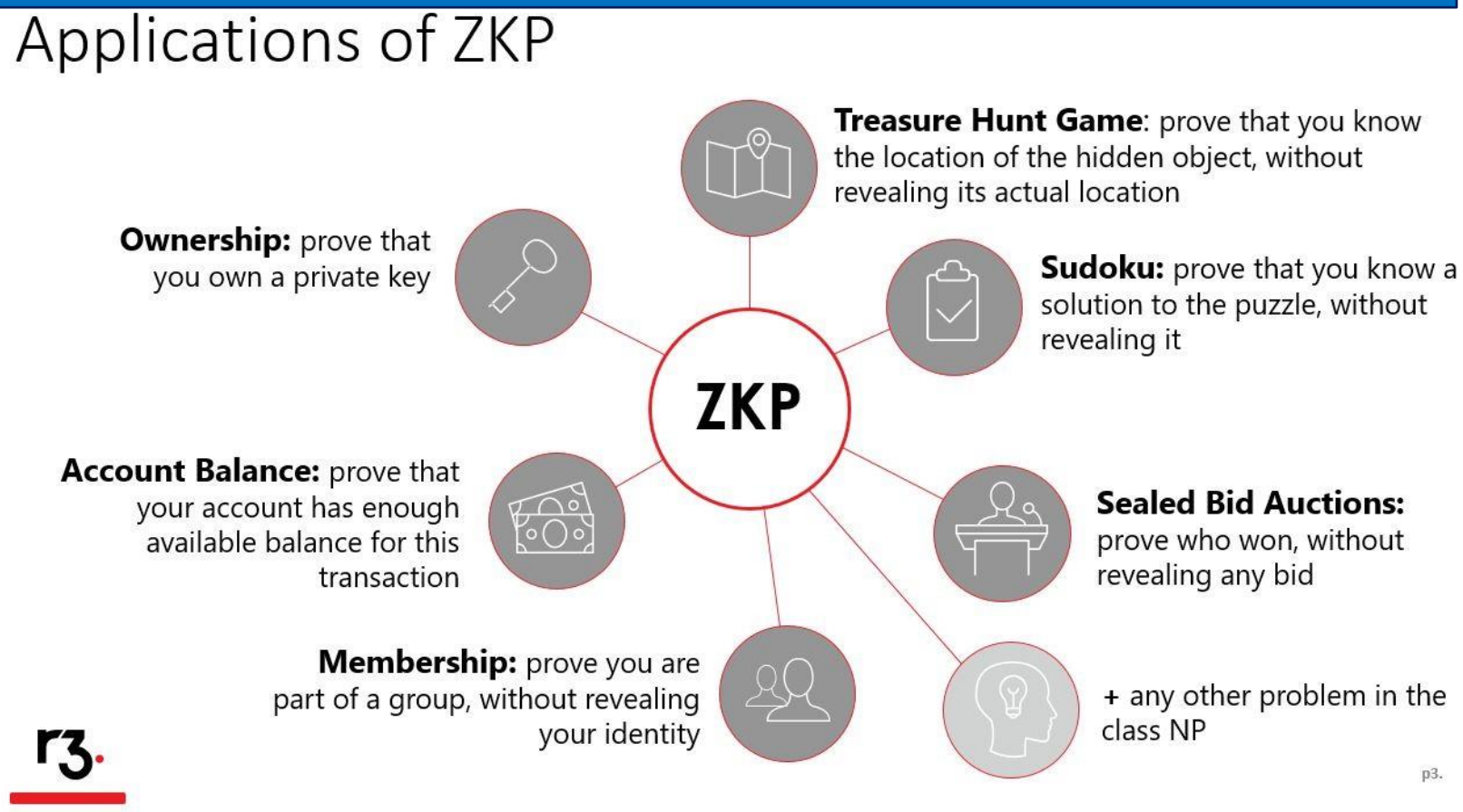
Prova de conhecimento zero - ZKP

- Uma forma criptográfica para uma parte (*prover*) provar para outra parte (*verifier*) que um determinado enunciado é verdadeiro sem revelar qualquer outra informação.

- Exemplo: provar sua idade sem revelar a idade.



Aplicações de ZKP



Source: https://www.linkedin.com/pulse/demonstrate-how-zero-knowledge-proofs-work-without-using-chalkias

Criptografia homomórfica

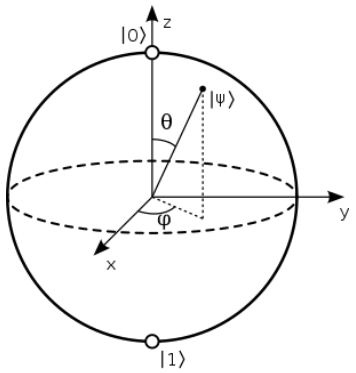
- Uma forma de realizar operações diretamente em dados cifrados sem precisar decifra-los nem compartilhar a chave.
- O resultado permanece cifrado e é decifrado somente por quem detem a chave.
- O resultado é o mesmo se as operações fossem feitas sobre dados decifrados.

Criptografia homomórfica

- Sendo:
  - m_i a mensagem original (texto claro)
  - c_i a mensagem cifrada
  - $enc(m_i) = c_i$ → a função de cifragem
  - $dec(c_i) = m_i$ → a função de decifragem
- Uma operação ϕ é homomórfica se:
  - $dec(\phi(c_1,c_2)) = \phi(m_1,m_2)$

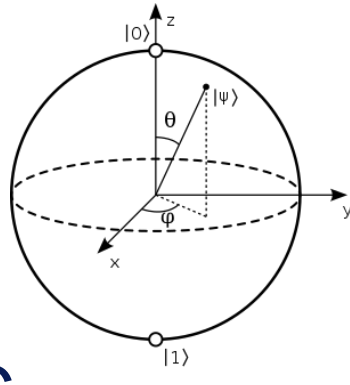
Post-quantum cryptography

- Soluções resistentes a computação quântica.
- Fundamental pois os algoritmos atuais de troca de chave (RSADH ou ECCDH) e assinatura digital (RSADSA ou ECDSA) são vulneráveis a algoritmos, exemplo, Shor.
- Aritmética modular → reticulados



Post-quantum cryptography

- Criptografia baseada em reticulados
- Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) (CRYSTALS- Kyber)
  - Troca de chaves - FIPS 203[1]
- Module-Lattice-Based Digital Signature Algorithm (ML-DSA)
  - Assinatura digital – FIPS 204[2]
- Outros: FN-DSA, SLH-DSA (hash), HQC, …



1. https://csrc.nist.gov/pubs/fips/203/final

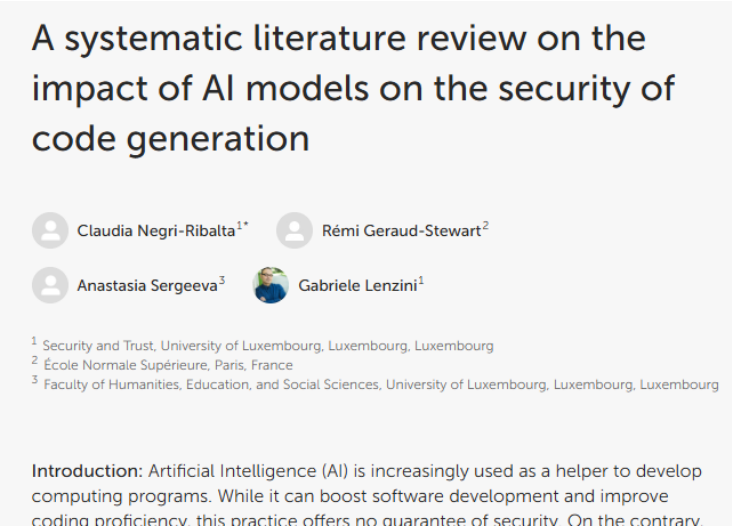
2. https://csrc.nist.gov/pubs/fips/204/final

Qual o impacto de IA na segurança? Alguns estudos iniciais…

Pesquisadores da Universidade de Luxemburgo realizaram uma revisão sistemática da literatura para analisar o **impacto dos modelos de inteligência artificial na segurança da geração de código**.

- Consenso científico de que modelos de IA **não produzem código seguro** e **introduzem vulnerabilidades**, mesmo quando mecanismos de mitigação são aplicados.

- Linguagens como C são particularmente problemáticas para geração automática de código, devido às exigências complexas de gerenciamento de memória.



A systematic literature review on the impact of AI models on the security of code generation

Claudia Negri-Ribalta[1*] Rémi Geraud-Stewart[2]
Anastasia Sergeeva[3] Gabriele Lenzini[1]

[1] Security and Trust, University of Luxembourg, Luxembourg, Luxembourg
[2] École Normale Supérieure, Paris, France
[3] Faculty of Humanities, Education, and Social Sciences, University of Luxembourg, Luxembourg, Luxembourg

Introduction: Artificial Intelligence (AI) is increasingly used as a helper to develop computing programs. While it can boost software development and improve coding proficiency, this practice offers no guarantee of security. On the contrary,

https://www.frontiersin.org/articles/10.3389/fdata.2024.1386720/full

Vulnerabilidades por linguagem

50% do código gerado por IA em C é vulnerável — falhas graves como *buffer overflow (CWE-787)*. Linguagem mais crítica: **problemas de memória e ponteiros** amplificam riscos.

Mesmo sendo mais segura, **38% dos programas gerados têm vulnerabilidades** (*SQL Injection, credenciais expostas*). Pequenas mudanças no *prompt* podem gerar código **seguro ou totalmente inseguro**.

Modelos de IA **corrigem só 20% das falhas conhecidas** — especialmente em código criptográfico. Tendência a **omitir etapas essenciais de segurança**, criando riscos invisíveis.

Código em PHP gerado por IA pode conter **instruções perigosas** e falhas de sanitização. Experimentos mostraram geração de **código adversarial** explorável por atacantes.

https://www.frontiersin.org/articles/10.3389/fdata.2024.1386720/full

Paradoxo do *feedback loop*

- Tentar **corrigir** o código → **piorar** a segurança.
- Ferramenta de IA **corrigisse falhas de segurança** → modelo **introduz** novos *bugs* em partes que antes estavam corretas.
- Código regerado apresentou maior complexidade por linha → tornando-se mais difícil de manter e revisar.
- Quando solicitado a reduzir o tamanho das linhas, o GPT-4o diminuiu a complexidade em 11,3% e corrigiu 17,9% das falhas detectadas.
- Porém, ao pedir menos linhas de código, o modelo gerou código com 18,4% mais complexidade mesmo tendo corrigido 43,2% das vulnerabilidades.

Fonte: *CHONG, C. J. et al. Artificial-Intelligence Generated Code Considered Harmful: A Road Map for Secure and High-Quality Code Generation.* New Jersey Institute of Technology, 2024. Disponível em: arxiv.org/abs/2409.19182

Vantagens e desvantagens do uso de IA

Vantagens

- **Aumento da produtividade**
  - I.A. automatiza a escrita de códigos repetitivos, simples,
  - Conversão entre linguagens é facilitada.
  - Foco em problemas mais complexos, projeto de arquitetura e lógica de negócio.
- **Velocidade no desenvolvimento**
  - Reduz o tempo para criar funcionalidades básicas
- **Assistência ao desenvolvedor**
  - Bom para explicar código existente ou alguns conceitos
  - Bom para iniciantes entender bibliotecas e *frameworks*
  - Refatoração e análise
  - Análise de código existente ….

Desvantagens

- **Geração de código incorreto ou inseguro**
  - O código é gerado com base em dados de treinamento que podem conter vulnerabilidades
  - Pode inserir problemas como SQL injection, …
- **Vazamento de dados**
  - Se não internalizar na empresa
  - Senhas ou dados sensíveis → violar políticas internas
- **“Alucinações” (ERROS)**
  - LLMs podem “inventar” bibliotecas, …
- **Outros**
  - Falta do contexto do negócio → regras de negócio, compliance, …
  - Problemas de propriedade intelectual – de onde vem o código?

Muito mais …

- Problemas técnicos → *heartbleed*, configuração errada, não atualização, *zero-day*, OWASP, IoT, MiTM, ...
- Fatores humanos → falta de conhecimento, falta de treinamento, ataques internos, *phishing*, ...
- *Zero trust architectures* – nunca confie, sempre verifique
- ....

Conclusão

Conclusão

- O mundo mudou significativamente nas últimas décadas – muito rápido.
- Não tem volta!
- Segurança é fundamental.
- Dinâmico e muitas novidades.
- Precisamos expandir as pesquisas nesta área.

Panorama e Tendências da Cibersegurança no Brasil

Prof. Avelino Francisco Zorzo
Escola Politécnica – PUCRS
avelino.zorzo@pucrs.br

UNB - 2026