Security Challenges for IoT and Smart City Systems and Applications

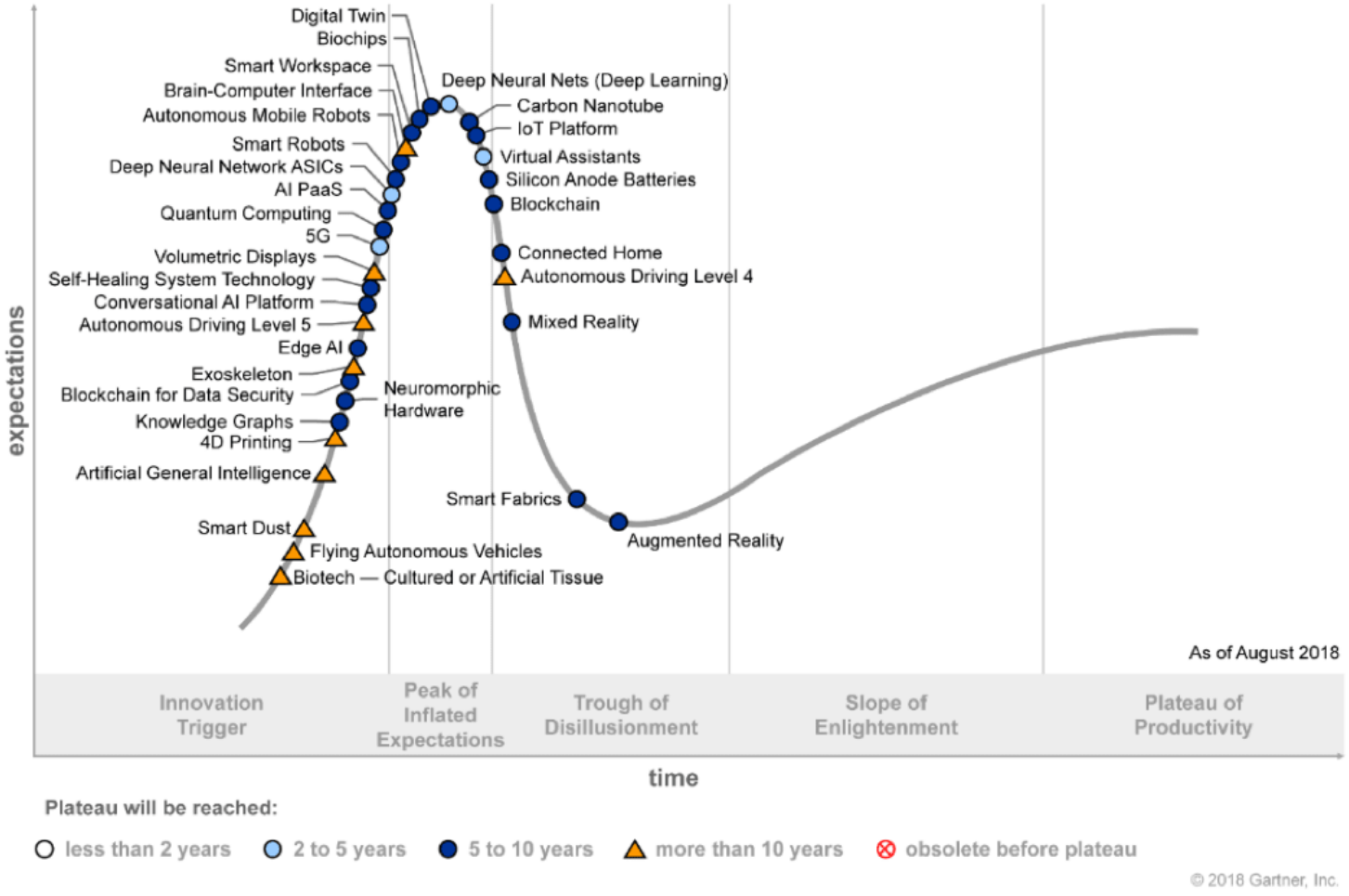
Fabiano Hessel

Smart City Innovation Center

fabiano.hessel@pucrs.br

PUCRS TECNOPUC PARQUE CIENTÍFICO E TECNOLÓGICO DA PUCRS Smart City Innovation Center

Hype Cycle for Emerging Technologies



Points to consider in IoT Solution Planning

✓ Privacy: monitoring, processing, storage and access personal data

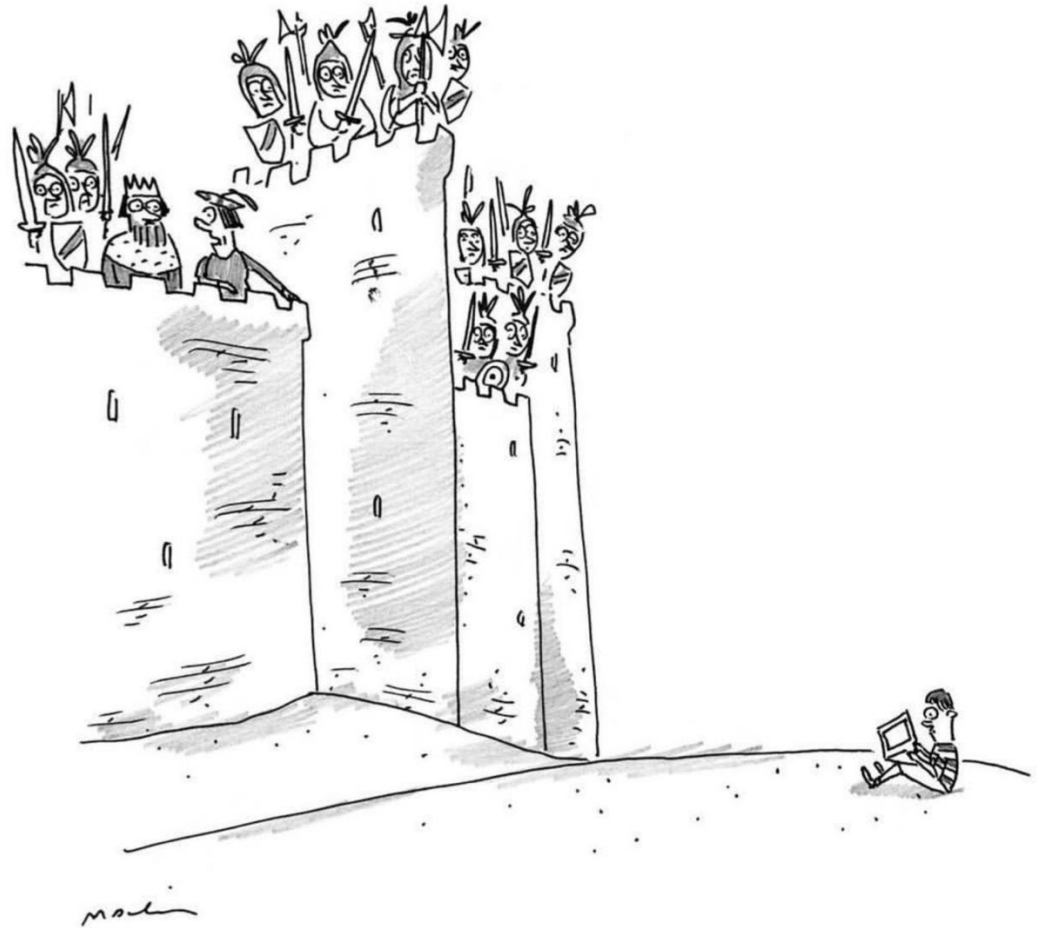
✓ Security: in 2024 companies will spend USD 134B on security (Fonte: Kaspersky, 2018)

✓ Interoperability: IoT silos challenge

✓ Data Analytics: Big Data e Little/Small Data

✓ IoT Market Solutions: lack of adequate technical knowledge to formulate Terms of Reference

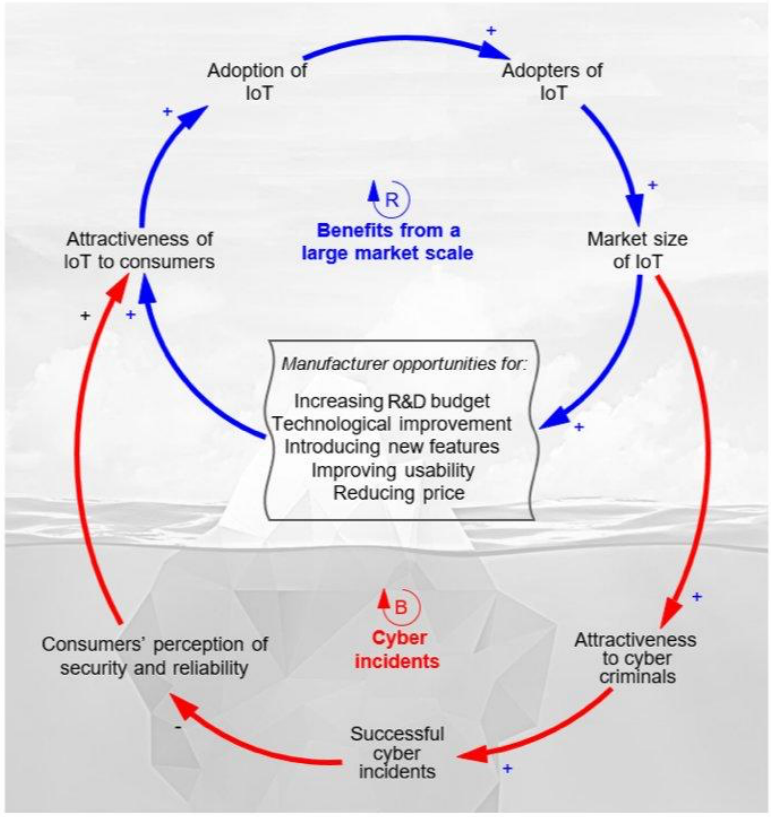
✓ The ecosystem of hardware / software around IoT framework is under construction as now we are sure that the old operating systems and hardware may not be sufficient for Smart Cities and IoT's abilities.



"Bad news, Your Majesty—it's a cyberattack."

Iceberg Model for IoT Products

Cyber risk exposure is part of a customer's perception of security and reliability, and this affects the relative advantage of IoT products.



Source: "The Internet of (Wonderful and Scary) Things,"
By Mohammad Jalali, *MIT Sloan Management Review*, January 2019
sloanreview.mit.edu/article/the-internet-of-wonderful-and-scary-things/

Internet of Things - Security

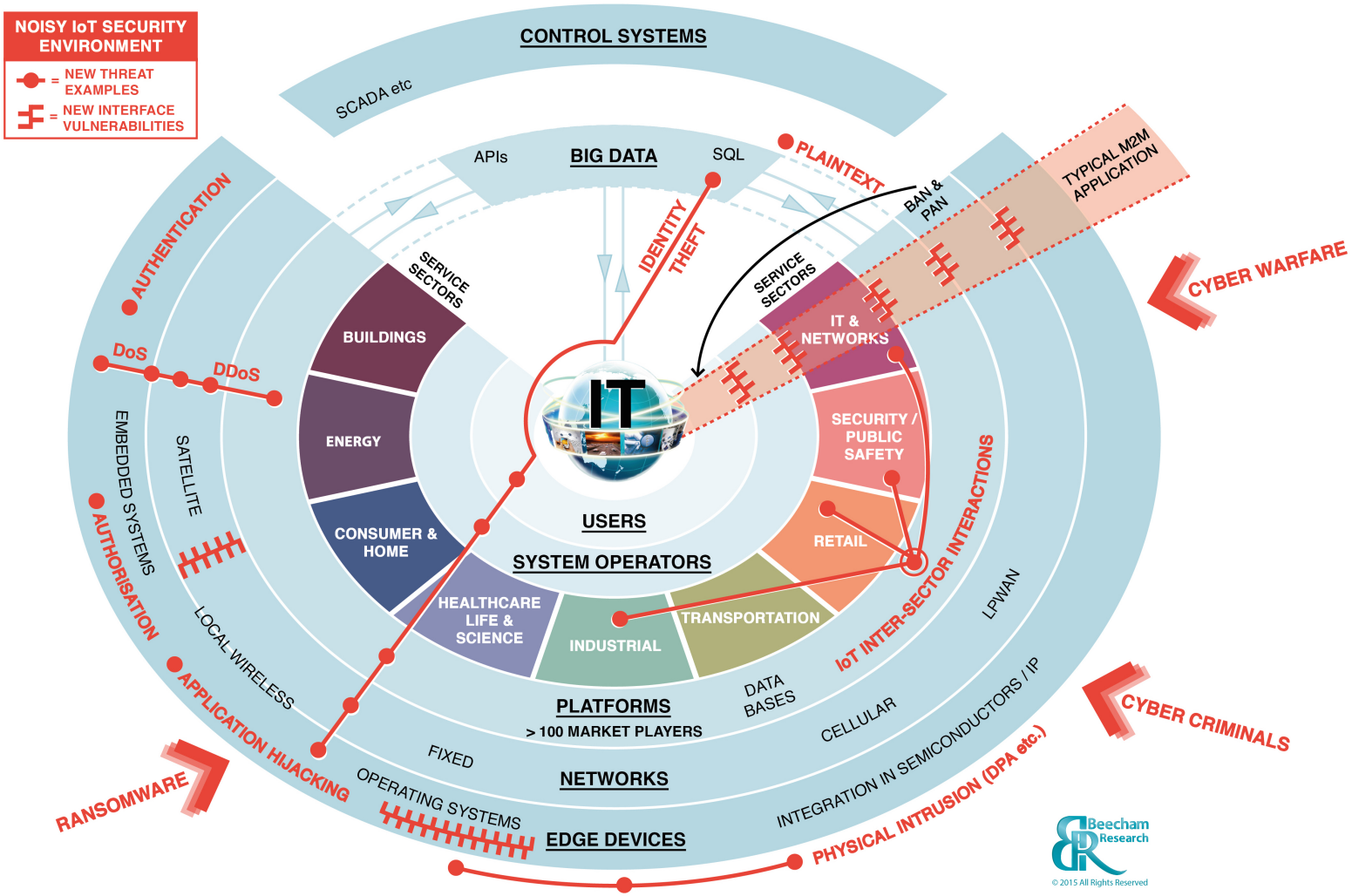
✓Why should you care about the security of your Internet-connected thermostat or home lighting system? (For example, Hotel Casino in Vegas - 2018)

✓The explosive growth of IoT devices has resulted in an increasing concern for the security of these interconnected devices and the privacy of the information they contain.

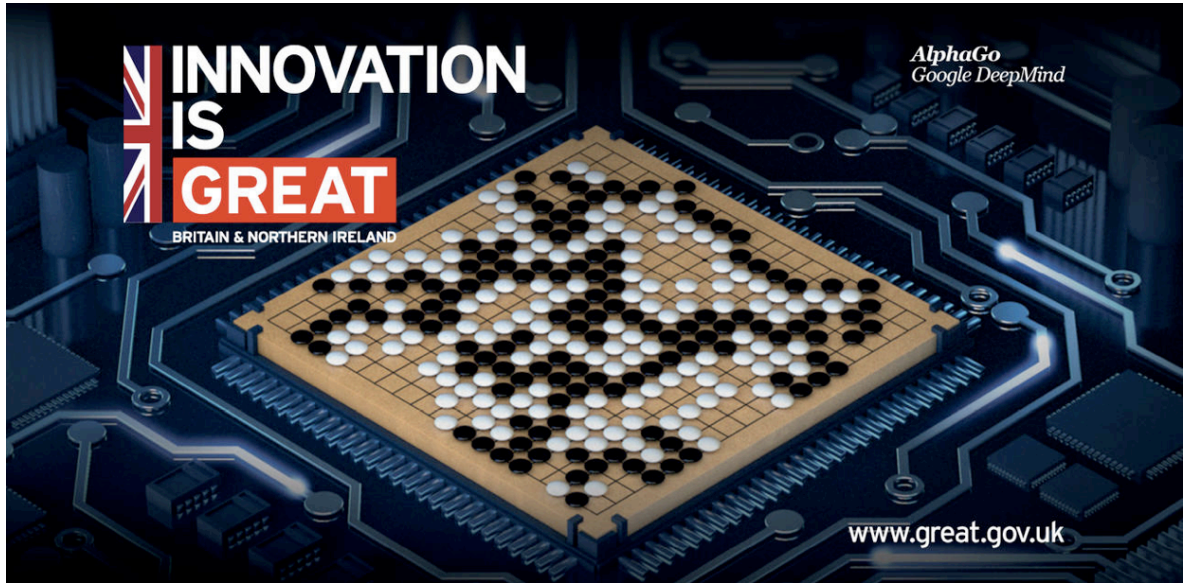
✓The Gartner Research Report: "Predicts 2016: Unexpected Implications Arising From the Internet of Things" says: "IoT becomes an increasingly attractive early link in [the] kill chain, as IoT vendors are most likely to repeat the security mistakes of the past and to not embrace modern security, vulnerability management and disclosure practices."

✓The HP Report – Internet of Things Security: State of the Union – "…a total of 250 security holes have been found in the tested IoT devices — on average, 25 per device. The issues are related to privacy, insufficient authorization, lack of transport encryption, inadequate software protection, and insecure Web interfaces."

IoT Security Threat Map



IoT Security



Global cybersecurity spending is expected to reach almost USD 1.3 trillion by 2021. The UK is investing around USD 1.9 billion to deal with threats and increase its capabilities

Taxonomy of Security Threats Affecting Blockchain Abstract Layers

Security Threats	Attack Vectors	Affected Abstract Layers
Double-Spending Threats	Race Attack	Consensus
	Finney Attack	Consensus
	Vector76 Attack	Consensus
	Alternative History Attack	Consensus
	51% Attack	Network, Consensus, Data Model
Mining/Pool Threats	Selfish Mining/Block-discard Attack	Network, Consensus
	Block-Withholding Attack (BWH)	Network, Consensus
	Fork-After-withhold Attack (FAW)	Network, Consensus
	Bribery Attack	Network, Consensus
	Pool Hopping Attack	Network, Consensus
Wallet Threats	Vulnerable signature	Data Model
	Lack of control in address creation	Data Model
	Collison & Pre-Image Attack	Data Model
	Flawed key generation	Data Model
	Bugs & Malware	Data Model
Network Threats	DDoS Attack	Network, Consensus, *External resource*
	Transaction Malleability Attack	Consensus, Data Model
	Timejacking Attack	Network, Consensus, Data Model
	Partition Routing Attack	Network, Consensus, Data Model
	Delay Routing Attack	Network, Consensus, Data Model
	Sybil Attack	Network
	Eclipse Attack	Network
	Refund Attack	Application - Bitcoin
	Balance Attack	Network, Consensus
	Punitive and Feather forking Attack	Network, Consensus, Data Model
Smart Contracts Threats	Vulnerabilities in contracts source code	Execution
	Vulnerabilities in EVM Bytecode	Execution
	Vulnerabilities in Blockchain	Network, Consensus
	Eclipse Attack on contract blockchain	Network, Consensus
	Low-level attacks	Consensus, Data Model

Security Challenges

✓ Security by design (**IoT device is the challenge**, cloud is not in the IoT/Smart City game)

✓Security will be complicated by the fact that many "things" use simple processors and operating systems that may not support sophisticated security approaches (Edge device, Root of Trust)

✓Do you want your Internet-enabled mattress to pass data about your private behavior to third parties?

✓Many IoT Systems are poorly designed and implemented, using diverse protocols and technologies that create complex and sometimes conflicting configurations

Security Challenges

✓ Limited guidance for life cycle maintenance and management of IoT devices

✓ IoT privacy concerns are complex and not always readily evident

✓ There is a lack of standards for authentication and authorization of IoT edge devices

✓ Security standards, for platform configurations, involving virtualized IoT platforms supporting multi-tenancy is immature

✓ The uses for Internet of Things technology are expanding and changing—often in uncharted waters

Security Challenges

✓ New security technologies will be required to protect IoT devices and platforms from both information attacks and physical tampering, to encrypt their communications, and to address new challenges such as impersonating "things" or denial-of-sleep attacks that drain batteries, to denial-of-service attacks (DoS)

✓ But IoT security will be complicated by the fact that many "things" use simple processors and operating systems that may not support sophisticated security approaches.

✓ The problem: Current IoT ecosystems rely on centralized, brokered communication models, otherwise known as the server/client paradigm

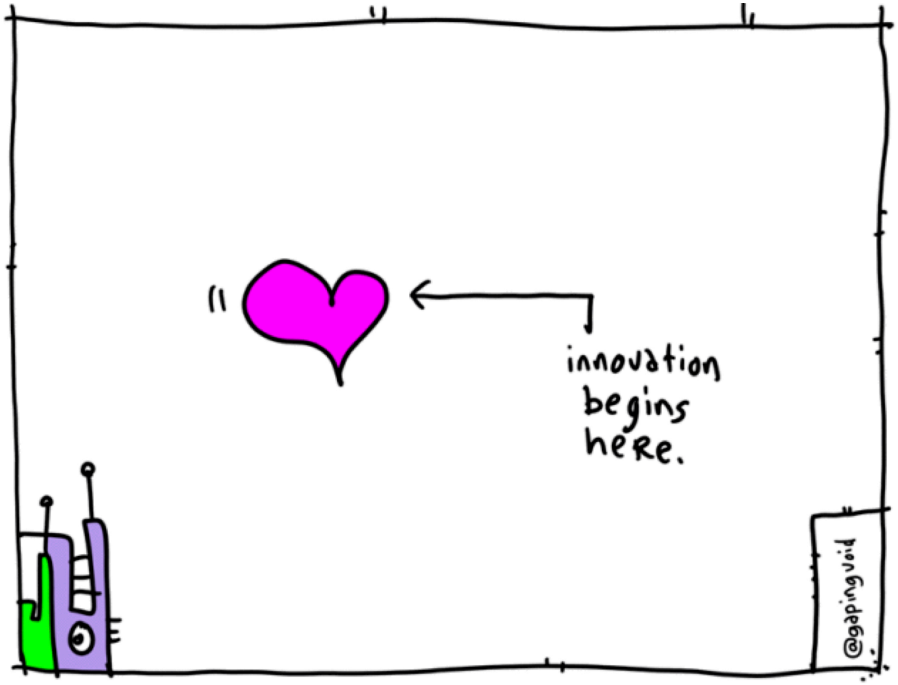
✓ While this model has connected generic computing devices for decades and will continue to support small-scale IoT networks as we see them today, it will not be able to respond to the growing needs of the huge IoT ecosystems of tomorrow

Security Challenges

✓ Existing IoT solutions are expensive because of the high infrastructure and maintenance cost associated with centralized clouds, large server farms, and networking equipment

✓ The sheer amount of communications that will have to be handled when there are tens of billions of IoT devices will increase those costs substantially

✓ Even if the unprecedented economic and engineering challenges are overcome, cloud servers will remain a bottleneck and point of failure that can disrupt the entire network



Thank You

Prof. Dr. Fabiano Hessel
fabiano.hessel@pucrs.br