16.00-17.30 Panel: Will information security be a reality for everyone?

Chair: Wayne Burleson, U.Mass Amherst

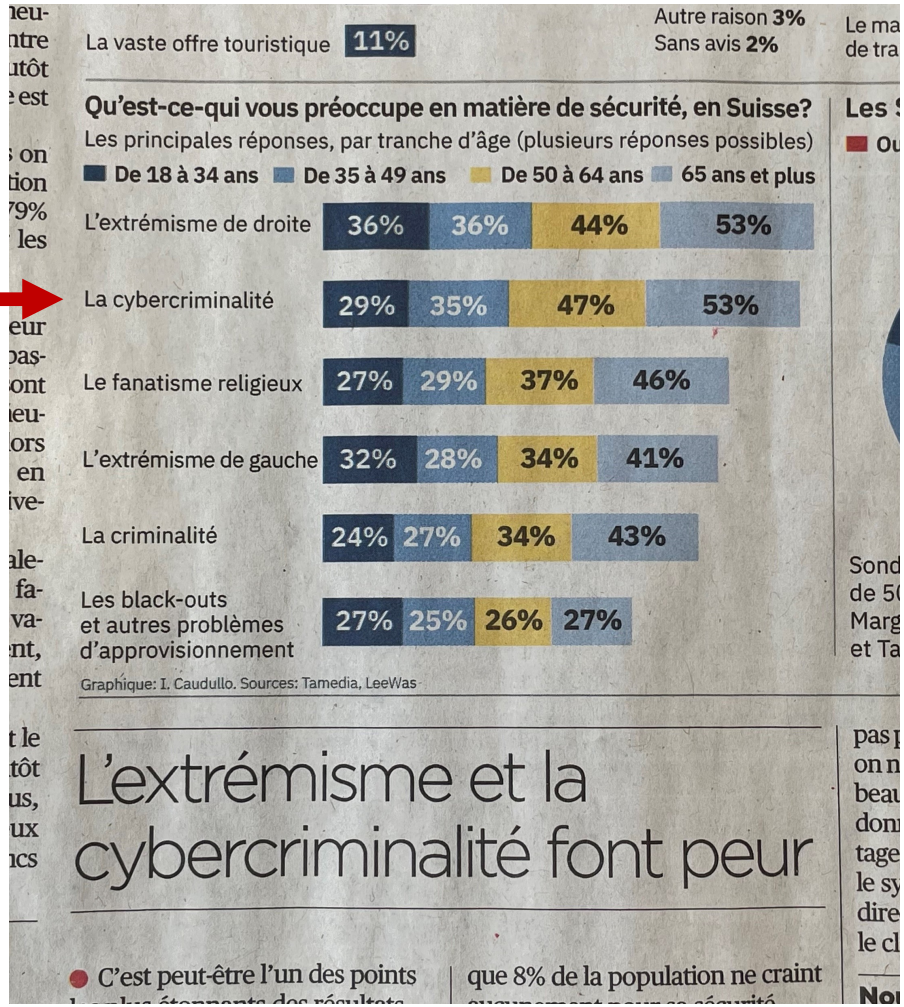
Panelists:
Marilyn Wolf, U.Nebraska. Lincoln
Farinaz Koushanfar, U.C. San Diego
Lejla Batina, Radboud University
Alena Simalatsar, HES-SO, Sion
Rajesh Gupta, U.C. San Diego
Yankin Tanurhan, Synopsys

Summary: Security, safety and privacy are increasingly critical issues as technology permeates society and our lives. They are also difficult to define for different populations, especially in the Metaverse. Security, safety and privacy are also considered fundamental rights that should extend to all citizens of the world, however they are not equally available to all, especially the elderly, the under-educated and other disadvantaged groups. Hardware, software and AI technologies provide numerous security capabilities, but many vulnerabilities remain due to human and political factors. How should security, safety and privacy be balanced and designed into systems while still remaining affordable and accessible? Applications in medical, health, transportation, governance, education and finance present different scenarios, but share common challenges as well.

Questions for Panel

1. What is being done in order to improve security, 360°, hardware-, and software-,
2. Will security be reachable only at high cost (eg. defense) or also accessible to the common user?
3. Will use of security protocols be discriminatory for the under-educated and elderly populations?
4. Will people reject security as complex and intrusive on personal communication devices?
5. What about privacy and safety?
6. Questions from Audience?

Security in the news



April 17, 24 Heures, Switzerland

Why is security difficult?

- Security is heterogeneous and multi-faceted
  - Technical
  - Social
- Security is hard to measure
  - Compared to performance, power, reliability
- Attacks are always evolving. But defenses are as well!

Marilyn Wolf
University of Nebraska

What is security?

- Information security:
  - Avoid unauthorized access.
  - Allow authorized access.
  - Clearly identify what is authorized and what is not.
- Different types of information have different security attributes.

What is safety?

- My definition is physical.
  - Others refer safety as protection of non-physical attributes.
- Safety requires avoiding certain actions, taking some actions.

What is privacy?

- Privacy-protected information is:
  - Not visible to those who should not see it.
  - Visible to those who do.
- Some data may be inferred from data that is not considered private.

Why do definitions matter?

- Security may be defined by law.
  - Different laws cover security and privacy of medical data, legal data, etc.
- Safety depends on physics, ethical principles.
- Protection of a person may affect their data privacy.

Will information security be a reality for everyone?

Farinaz Koushanfar, Ph.D.
Henry Booker Scholar Professor of Electrical and Computer Engineering (ECE)
Founding Co-Director, Center for Machine Intelligence, Computing and Security (MICS)
University of California San Diego

Panel at the Emerging technologies and applications Symposium
Montreux, Switzerland April 19 2023

1. What is being done in order to improve security, 360°, hardware-,and software-,

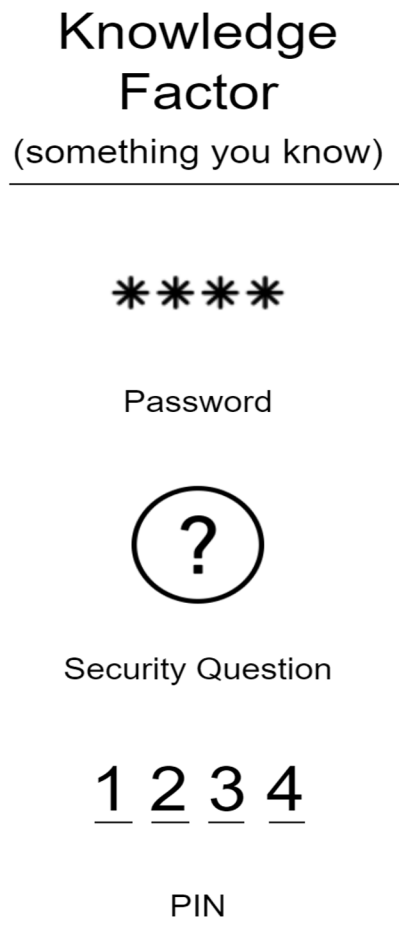
- It’s a rather complex and broad landscape
- Hardware, software, or 360 system
  - Several static/dynamic patches
  - Correct by construction
- Generative AI revolution
  - Amazing new automated tools
  - Mostly centralized (non federated)
  - Simultaneously introduce several new vulnerabilitie
- Complex vulnerabilities and adversaries
  - Centralized (nation-state) adversaries
  - Asymmetric power between users and adversaries

2. Will security be reachable only at high cost (eg. defense) or also accessible to the common user?

- The initial cost would be very high, secure systems would be a service for the privileged
  - E.g., as long as foundation models are centralized, there will be asymmetry between users, and high profile providers / adversaries
- The cost could be amortized gradually – most niche technologies become a commodity
- Major providers or nation-state adversaries
  - May have incentives (e.g., financial or political) that intercept accessibility for common users

3. Will use of security protocols be discriminatory for the under-educated and elderly populations?

- Indeed there is a growing gap
- Technology and education shall both evolve
- E.g., single-factor to multi-factor authentication
- Usable security



4. Will people reject security as complex and intrusive on personal communication devices?

- Security or privacy?
- Due to providers financial (or other interests), several privacy knobs are set to be intrusive and complex → I.e., the default is set to make it complex
- Increasingly important to consider usable security
- Interplay of security, privacy, and user education

5. What about privacy and safety?

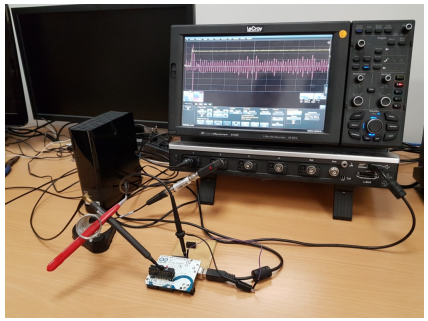
- Even bigger problems…
- Re privacy, it would be an interplay of provider's financial/political incentives
- Privacy preserving protocols and systems will be of increasing importance
- Safety would be an interplay of computing, sensing and actuation in the physical world
  - Not very good models for the physical world, making this super hard
  - Critical due to the potential for physical damages

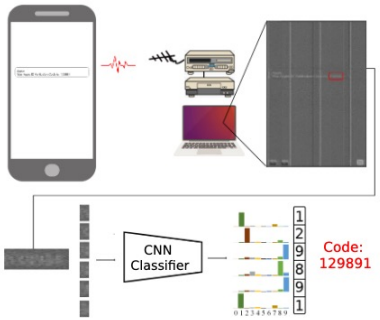
Lejla Batina,
Radboud University
The Netherlands

- 3 years with SafeNet as a cryptographer
- 2005: PhD from KU Leuven, Secure hardware for crypto
- 2006-2009: PostDoc at KU Leuven
- Since 2009- : Digital Security group at Radboud University, full prof. since 2017
- Leading CESCA lab: 10+ PostDocs/PhD students

- Physical attacks on embedded systems
- Secure cryptographic implementations
  - Lightweight cryptography
  - Post-quantum cryptography
- FPGA security
- AI and security

Research topic 1: AI-assisted physical attacks on embedded devices





Research in keywords

- Embedded systems security
- Side-channel analysis and Fault attacks
- Deep learning

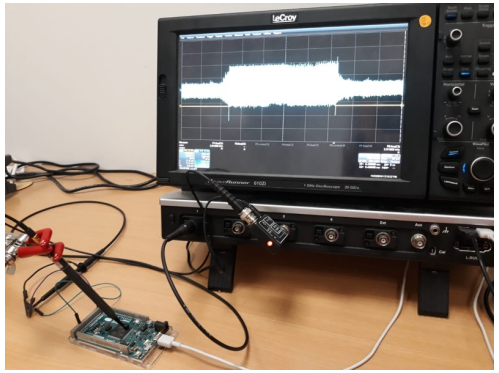
Innovative aspects

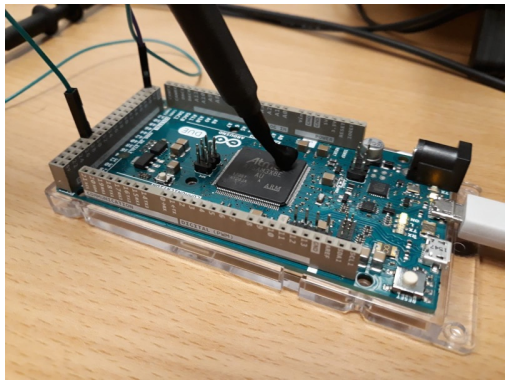
- Application of AI methods to security evaluation
- Using DL to read information from screens

Applications

- Security evaluation / Tools production and evaluation
- Chip manufacturers
- Organizations using secure chips, e.g., governments
- Cyber physical systems

Research topic 2: Reverse engineering AI through side-channel analysis





Research in keywords

- Reverse engineering neural nets (NN)
- Side-channel and Fault analysis
- Trade secrets and input recovery
- Backdoor attacks, poisoning attacks, federated learning

Innovative aspects

- SCA to clone existing NN products
- SCA to learn proprietary information
- New attacks on neural networks
- Applicable to various platforms, such as GPUs, FPGAs

Applications

- Automotive, Semiconductors / IP and content protection
- IoT/ Medical, health, HD cameras

Some points for discussion

- Overall:
  - Improving security by e.g. upgrading to post-quantum and more complex protocols an sw/hw is not helping ALL users
  - We don’t need more or better crypto
  - Security should be available to all -> focus on usable security and privacy
  - Big tech companies do not score high on user privacy & security
- AI and security/privacy:
  - Security risks when implementing AI
  - Can AI break crypto we rely on?
  - Explainability of AI

Alena Simalatsar
HES-SO, Sion, Switzerland

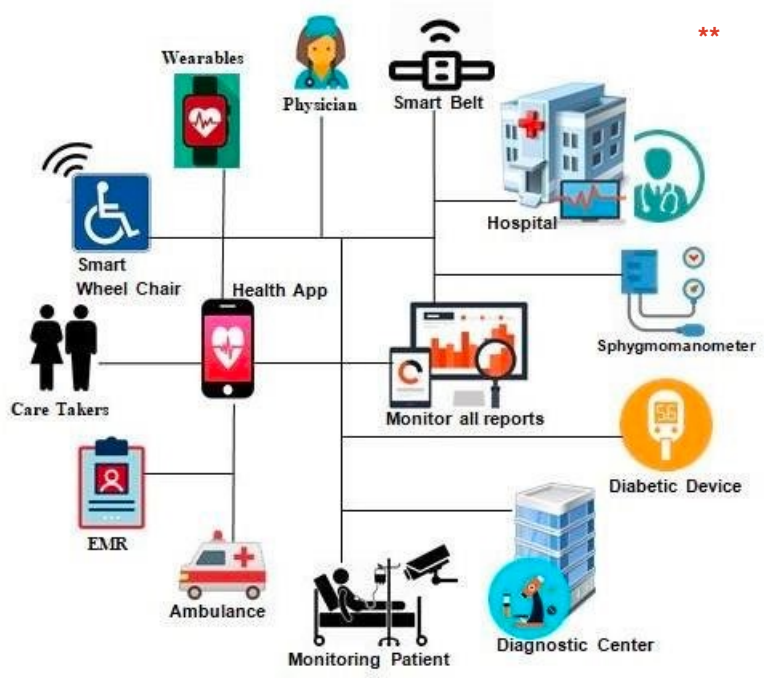
Computer-aided design and technologies for Bio-medical systems

EMAC

École des Médecines Alternatives et Complémentaires

Computer-aided design and technologies for Bio-medical systems + Human Anatomy & Physiology

“Phones and laptops don’t kill a lot of people, cars and medical devices do” *



**

(1) Security will be more about safety than privacy *

(2) We will have to reorganise government functions such as safety regulators, standards bodies, testing labs and law enforcement *

(3) Sustainability: *

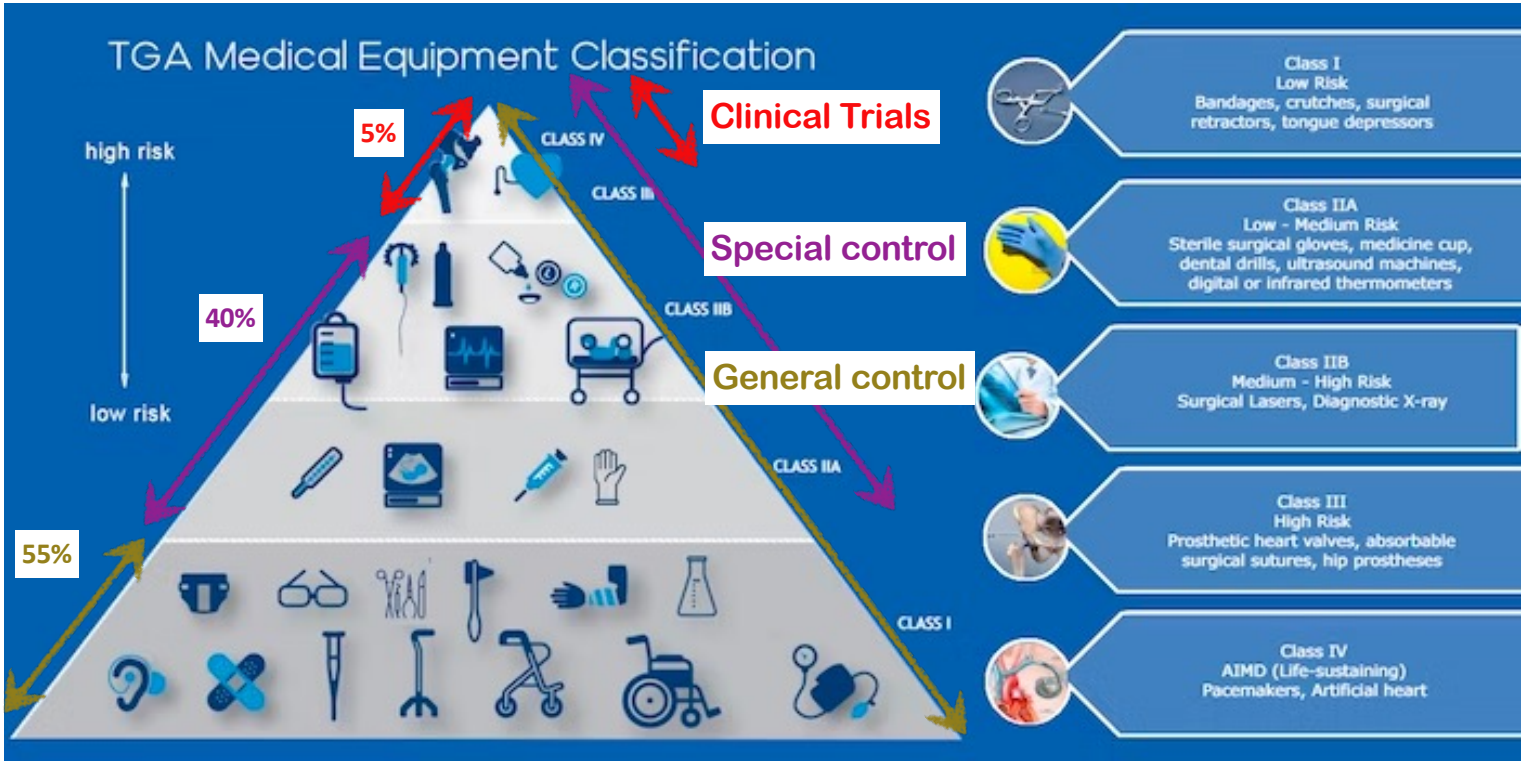
- Phone security upgrades for 2-3 years,
- Cars and medical devices security upgrades for 20-30 years

* Ross Anderson, **"Making Security Sustainable**”, Communications of the ACM, Vol. 61 No. 3, Pages 24-26, March 2018

** N. Dilawar, M. Rizwan, S. Akram, F. Ahamd, “**Blockchain: Securing Internet of Medical Things (IoMT)**”. International Journal of Advanced Computer Science and Applications, 2019

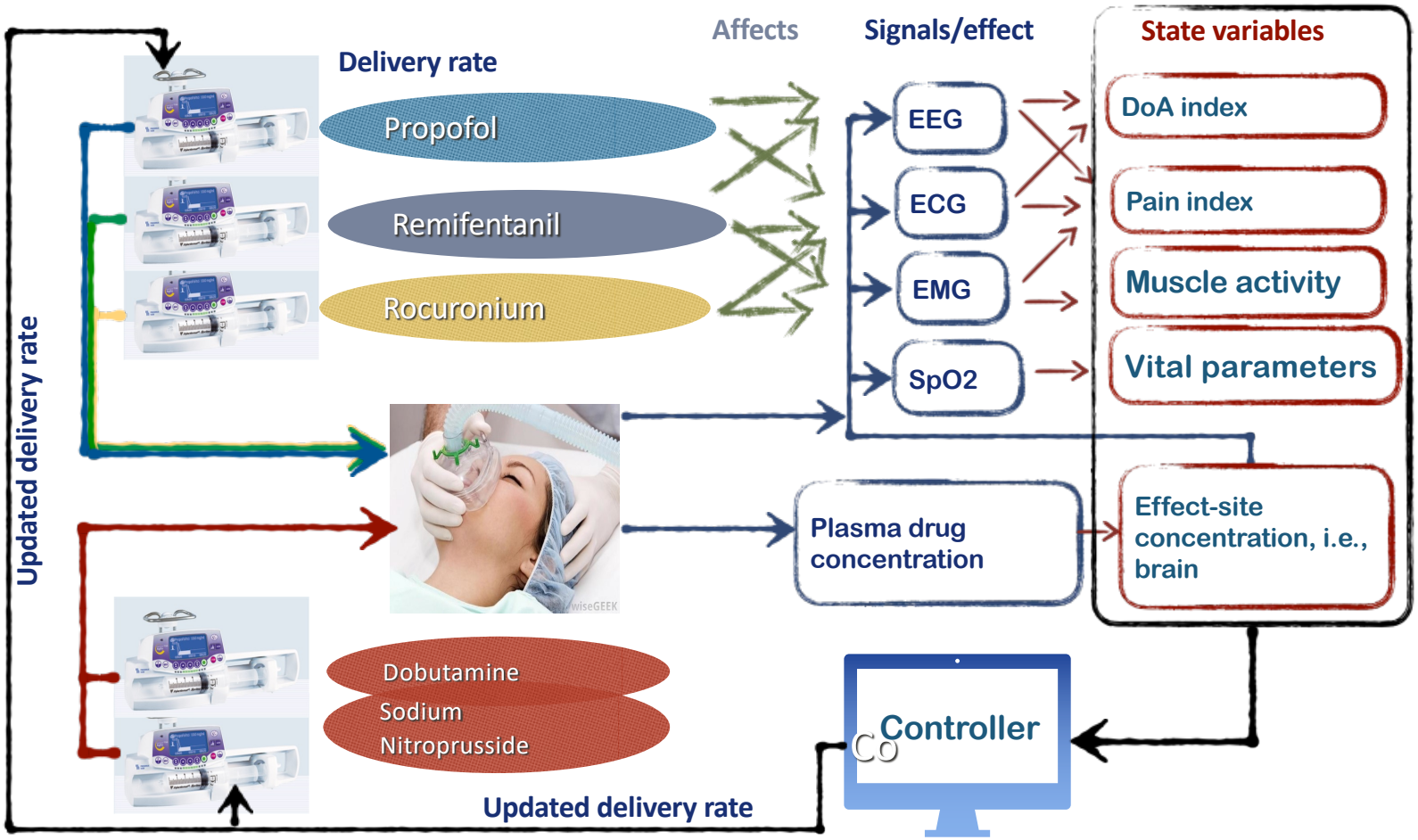
Medical devices (MDs)

https://www.medcart.com.au/blog/how-to-dispose-used-medical-equipment

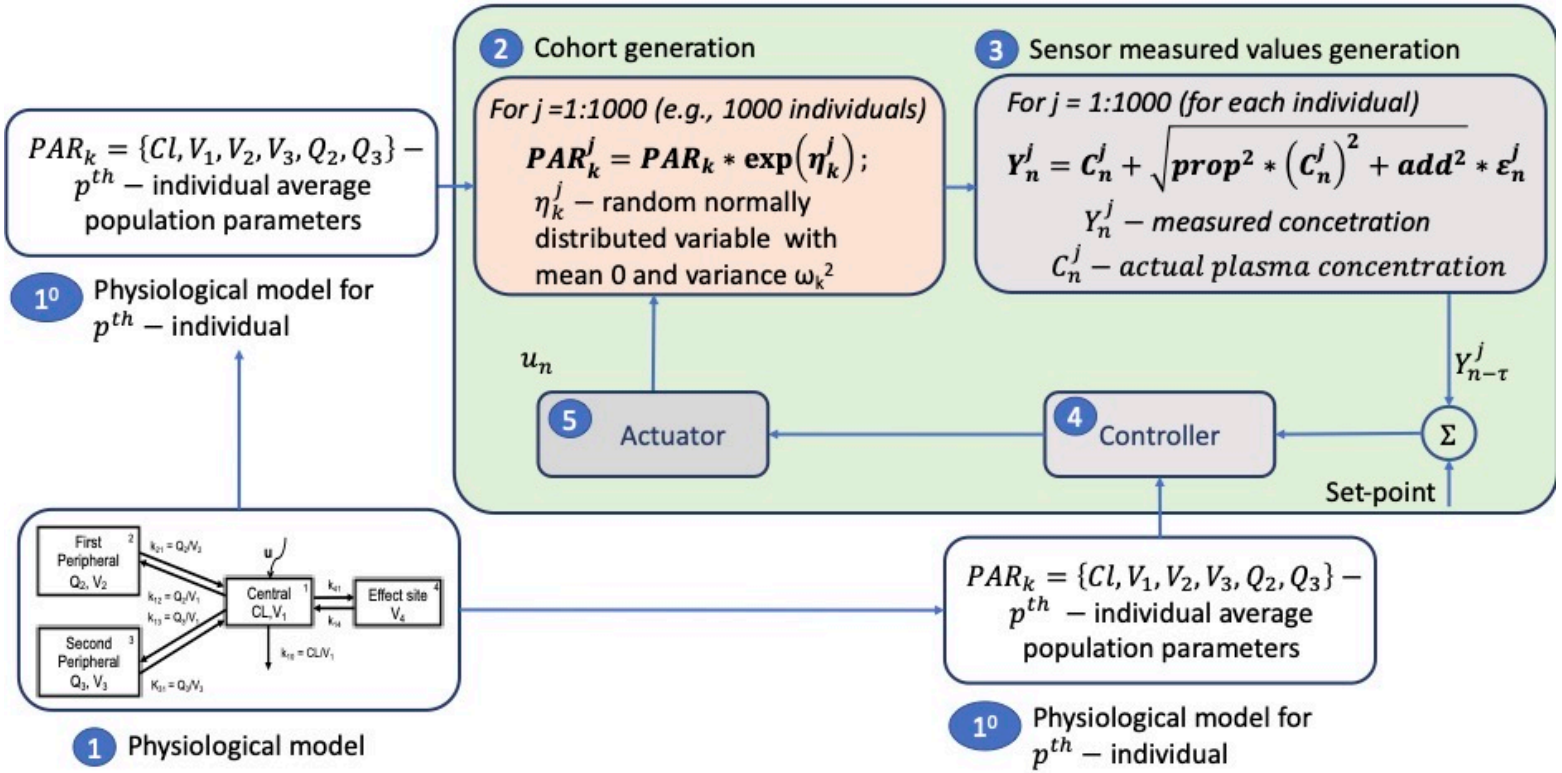


Risk = (1 - Safety) = Probability of Malfunction * Severity of effect

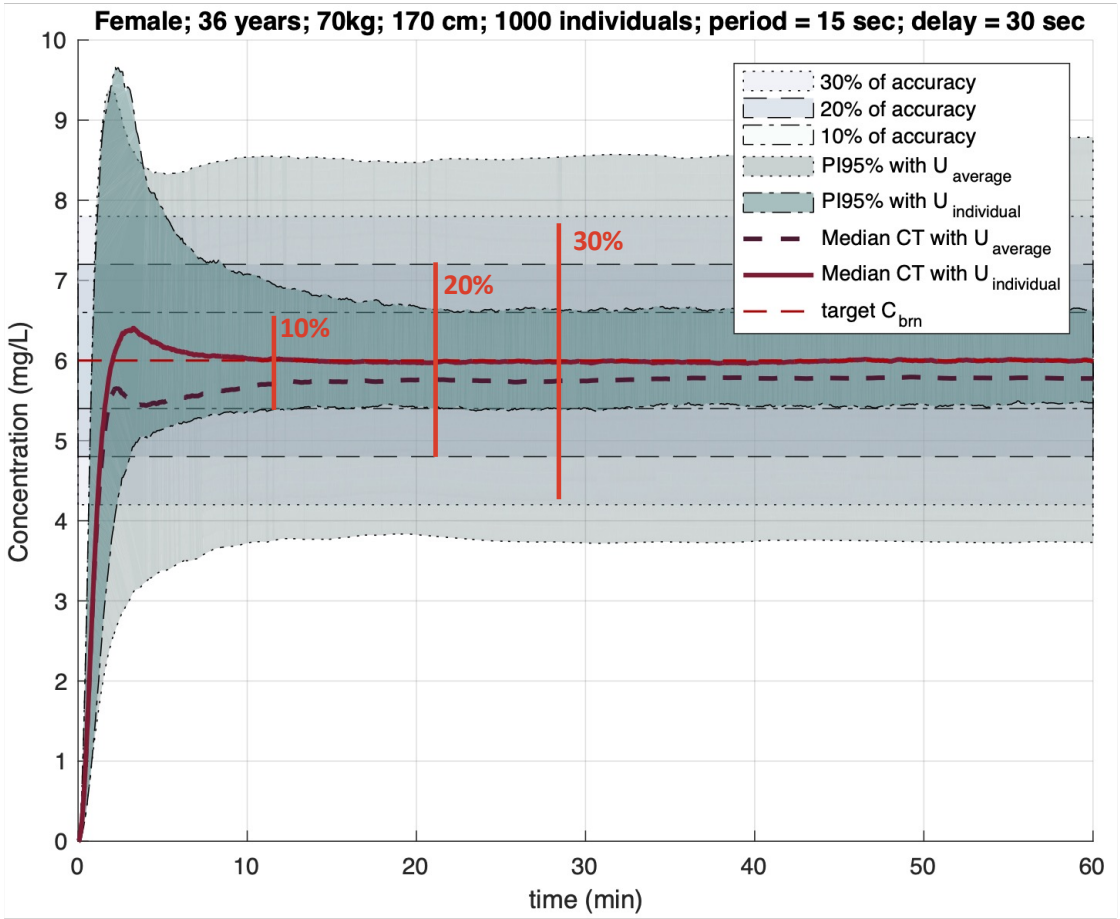
Closed-loop IV anaesthesia



In Silico Clinical Trials



Probability of malfunction VS Severity of effect



Will Information Security be a reality for everyone?

Montreux Panel on Emerging Technologies & Applications

Rajesh K. Gupta
Founding Director

HALICIOĞLU DATA SCIENCE INSTITUTE

UC San Diego

Panel Questions

1. What is being done in order to improve security, 360°, hardware-, and software-,
2. Will security be reachable only at high cost (eg. defense) or also accessible to the common user?
3. Will use of security protocols be discriminatory for the under-educated and elderly populations?
4. Will people reject security as complex and intrusive on personal communication devices?
5. What about privacy? Shouldn't privacy be considered part of security, meaning the protection of confidential information from unwanted intrusions?

My Take

- As an institution builder in AI/ML (data science). Not as a researcher in the area. The obvious two questions are: Will info security be **real**? Will it be for **everyone** (accessible)?

Reality: A New World Emerging…

- We now live in two worlds: physical and cyber.
  - They together form our reality: one is no more real than the other.

- Our challenge is to make sure that they are **causally-connected**

- Causal connection is becoming possible because of
  - Fine and finer grain sensing and situational awareness: over time, over distances
  - Pervasive information leakage via **side channels.** Making radio talk, narrow bandwidth of useful information.

- Even with causal connection (direct, indirect, confounding, etc), causal inference is now facing once esoteric challenges on a daily basis:
  - Base-rate fallacy, Biases of one kind or the other, spurious correlations, our misplaced trust in data, print…
  - COVID-19 taught us many many lessons in this regard

Poverty of Privacy

- Privacy is now the new tradeoff valve against so many things
  - Reproducibility
  - Safety and Security
  - Vulnerability and Power (!)
  - $$

- Privacy mechanisms must straddle the razors edge between noise and bias

- New “Bill of Rights” emerging
  - Right to X by Y over Z
  - Resulting in a race condition between policy and technology means…

New Capabilities Emerging

- A lot of hope is pinned on new AI/ML (and fears too). In general, 3 kind of things AI/ML does:

1. Detecting patterns, generative/discriminative: image, speech, text, data
2. Making decisions: recommendations, spam, copyright, grading, hate speech, driving, diagnosis (apnea, adhd, autism, medical)
3. Predicting social outcomes: recidivism, job performance, policing, terrorist risk.

- (Raw) data and model mechanisms evolving rapidly to create new tradeoff points
- Yet these models need data that is protected, sensitive, self-reported or costly to acquire
- Sociologically, new notions of informed consent emerging
  - Family of ML models that let users opt into reporting personal data at prediction time after seeing the gains of disclosure
    - Berk Ustun: “Participatory Systems for Personalized Prediction”, 2022.

What is being done in order to improve security, 360°, hardware-, and software-,

- Destructive and constructive means: Security improvements through vulnerability detections. Dynamic delegation of authority and authentication.

Will security be reachable only at high cost (eg. defense) or also accessible to the common user?

- Yes and Not Now. High initial costs that drop rapidly (e.g., Homomorphic encryption)

Will use of security protocols be discriminatory for the under-educated and elderly populations?

- Security and Privacy are a side of the Power/Vulnerability/Prosperity coin. Technological and regulatory means to improve affordability.

Will people reject security as complex and intrusive on personal communication devices?

- "Opt-In" paradigms to emerge against demonstrated benefits.

What about privacy? Shouldn't privacy be considered part of security, meaning the protection of confidential information from unwanted intrusions?

- Privacy methods advancing rapidly from enclaves to federated, obscuitrity, noisiness, multi-party computations.

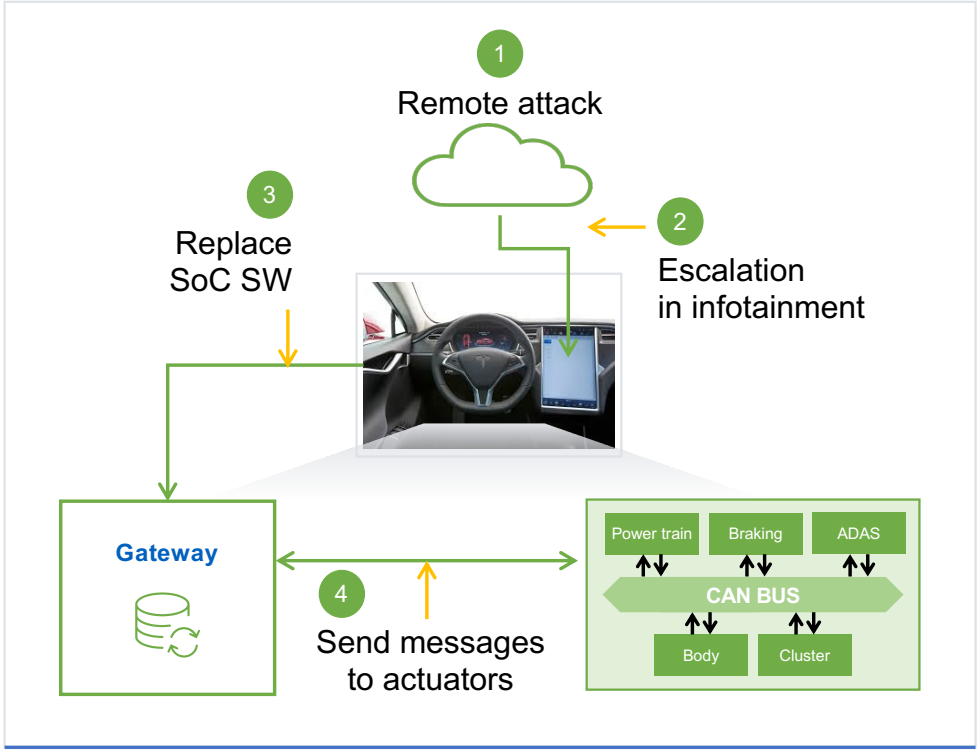
SYNOPSYS®

Security at the Root: Designing for Secure Systems

Dr Yankin Tanurhan, SVP of Engineering
Synopsys Solutions Group

Connected Devices Attacks on the Rise & Evolving

Secure Systems Require SoCs with Integrated Security Features



Everyone is affected - consumers & enterprises, to service providers and manufacturers

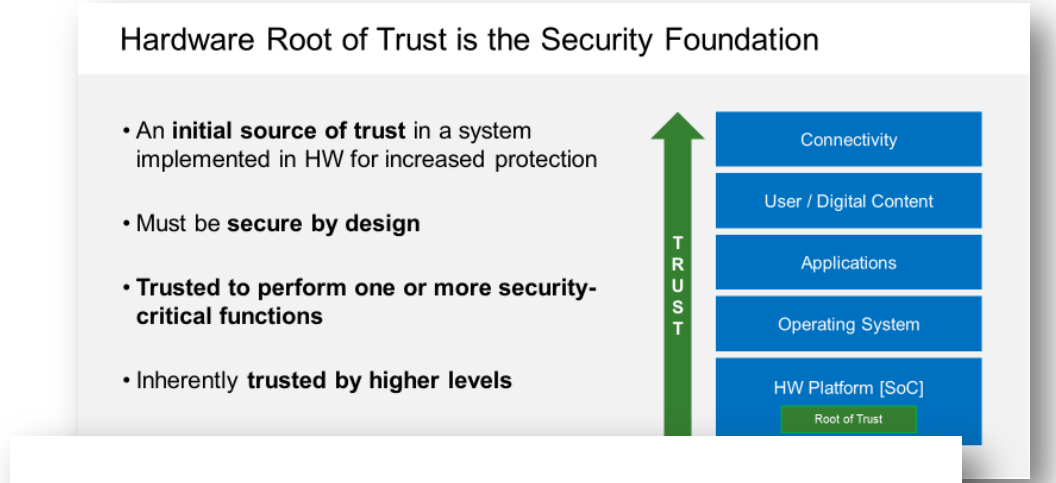
Security is crucial - needs to be addressed at all levels, starting with the SoC

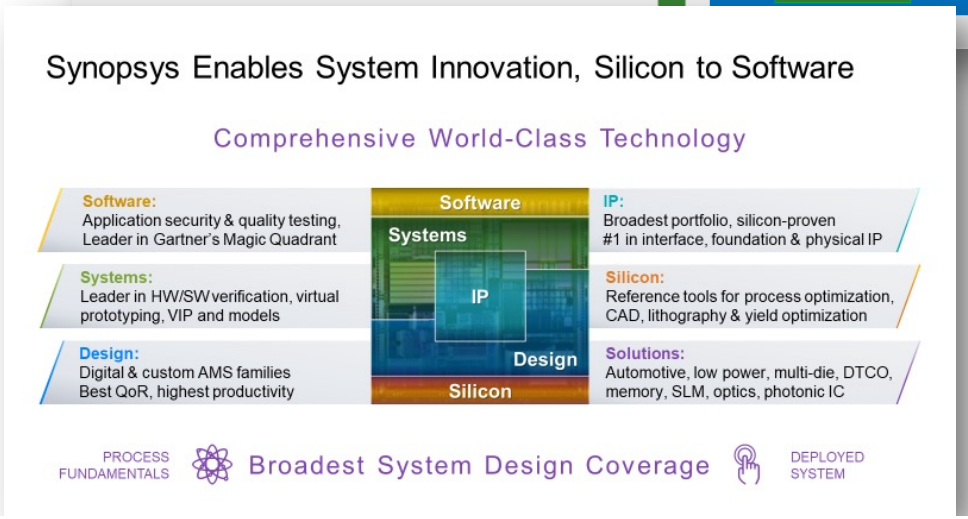
- Latest hacks result in investigation & lawsuits
- Companies need to assess the security of their products
- New regulations for user data privacy impose large fines for non-compliant solutions
- New standards are emerging

EMBEDDED SECURITY is ESSENTIAL.

What is being done in order to improve security, 360°, hardware, and software?

- Though most security issues are due to software vulnerabilities, security starts at the hardware
- We are actively working on many fronts
  - Silicon: sensors, silicon lifecycle management
  - IP: Crypto HW/SW, interface security, secure processors, tRoot HSM
  - Design: EDA tools are not only good for designing SoCs, they are used for security evaluation as well: PrimeTime PX for Side-Channel Power analysis, Z01X for fault injection
  - System: fast processor and system simulation enable secure SW development and testing
  - Software: leading portfolio of Software security analysis tools: Coverity, Black Duck SCA, Defensics fuzzing tools, etc. + security consultancy

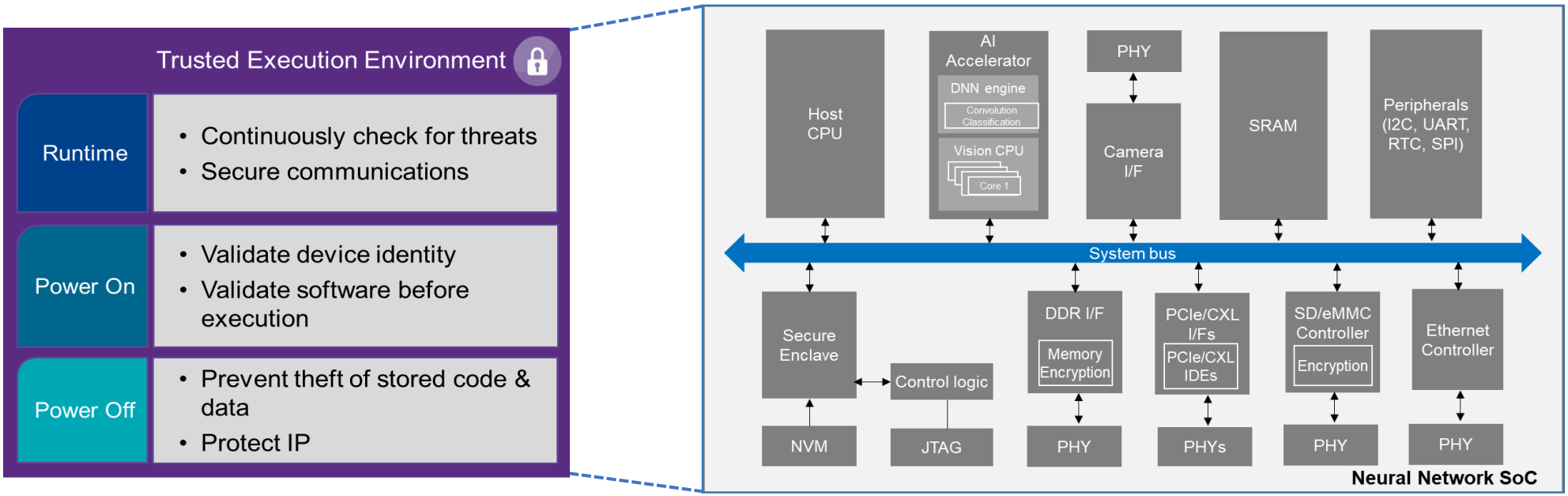




Will security be reachable only at high cost (eg. defense) or also accessible to the common user?

- “Security” is not binary; every system can be hacked when putting enough resources and time in it. If not today, then tomorrow new attacks will be invented that could compromise security. E.g. quantum computers enable great new applications for healthcare and other domains, but also threaten the secure foundation behind the Internet. Secure browsing with sites and servers that can be trusted through certificates use the RSA and ECC public key algorithms. The hard math problems these are based on, are no longer hard for quantum computers. So, new crypto is required: PQC.
- How much security a product needs, depends on the tradeoffs between risks and rewards. Tradeoff between cost of security and reward of an attack. Certain applications require more security and thus higher costs than others.
- Attacks evolve and costs of attacks typically go down. E.g. physical attacks used to be only for highly skilled and experienced people and required expensive equipment. Nowadays, simple side-channel and fault injection attacks can be done by hobbyists and script kiddies. That means defenses for lower-cost, “common user” products also need to improve.
- Cost of more sophisticated (hardware) countermeasures can be brought down using the IP business model. Instead of every company requiring to be a security expert, proven secure IP can be re-used. And costs are lowered as IP product development costs are amortized over many users.

Security-Aware Silicon IP: Key Foundation for System Security



Security Needs

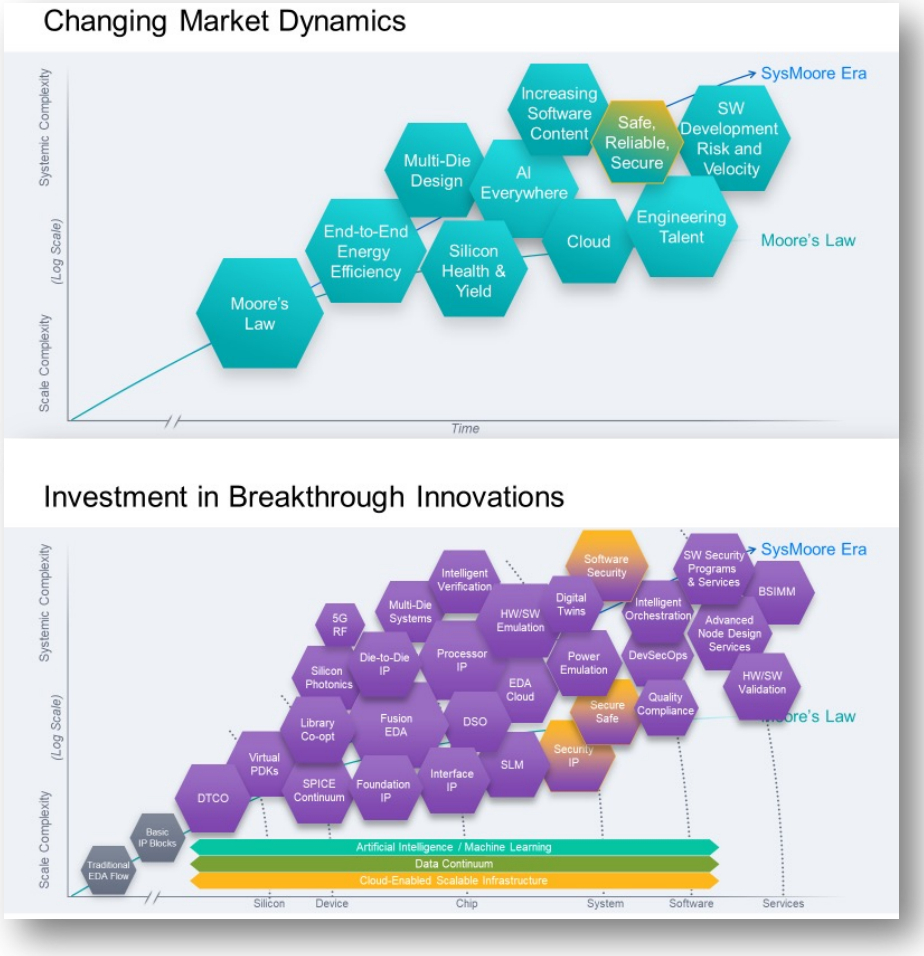
- Overall SoC protection functions (secure bootstrap, key management, secure updates, secure debug/JTAG access…)
- Secure data in motion
- Secure data-at-rest
- Encryption and authentication for model updates, secure communication and inputs from peripherals

Will use of security protocols be discriminatory for the under-educated and elderly populations?

- Though this used to be the case, the situation is improving. The use of security protocols is getting more user friendly, complexities are hidden from the user and you don't need to have a PhD or be an IT professional. More importantly, products more and more come with security enabled by default. E.g. routers don't come with security features disabled by default, or all products configured with the same default username and password.
- This is partly due to market forces – secure products, but especially user friendly, easy to use products may sell for a premium. But it's also due to legislation and security standards. Security standards for IoT devices define a good base security that work out-of-the-box without complex installation and management (e.g. using QR codes instead of manual typing).
- Legislation – maybe more in EU than in US, e.g. Europe's Cybersecurity act (CRA) and Cyber Resilience Act (CRA) – is underway that makes device manufacturers liable for security vulnerabilities and the damage these may cause. That may help to force product manufacturers to make security simple. The obligation for securing devices and protocols is not with the end user, but with the manufacturer and service provider.

Will people reject security as complex and intrusive on personal communication devices?

- Not just on personal communication devices, but on all devices.
- Because of market and legislations, security becomes mandatory and device manufacturers have incentives to reduce complexity and intrusiveness
- Certain services simply cannot be used without proper security in place, e.g. a banking app doesn't work on a phone without PIN or biometric authentication
- To make security simple and non-intrusive for the users, many innovations and new technologies are required. And these again require more and more hardware features and compute power. That's where we can help, if not explicit with novel security features like IDE security for PCIe and IME for memory encryption, then implicit by enabling the compute power required for efficient PQC algorithm implementations and low-power biometric solutions.
- AI may come to the rescue as well, to reduce end-user complexity … but has its own issues as well.



What about privacy and safety?

- Different countries in the world have different views on privacy. Complex geopolitical situation requires different security solutions for different markets and countries. Crypto Agility can help here to deal with the resulting design, manufacturing and logistics complexities.
- Not just US – China differences, also US – EU. See example on the right, enhancements of the EU-US Privacy Shield laws are progressing slowly. Certain EU groups consider US solutions not adequate:
  - No prior authorization for bulk data collection
  - Accountability issue for the Data Protection Review Court (DPRC)
  - Lawsuit-proof regime needed for legal certainty

EUROSMART
The Voice of the Digital Security Industry

EU-US personal data transfers View online

Enhanced EU-US Privacy Shield

LIBE Committee Report opposes new data-flows deal with the US

On 13 April, LIBE Committee adopted Rapporteur Juan Fernando López Aguilar's (S&D, Spain) draft Motion for Resolution on the **EU-U.S. Data Privacy Framework, as well as the amendments tabled to it.** The consolidated text is expected to be made available in the coming weeks. (Draft version available)

According to the European Parliament's press release, the Report acknowledges that the proposed EU-US Data Privacy Framework is an improvement from previous frameworks, but stresses that it does not provide for sufficient safeguards.

The text urges the Commission not to adopt the draft Adequacy Decision that it presented in December 2022, as the Committee considers that the United States' level of personal data protection is not essentially equivalent to that of the EU.