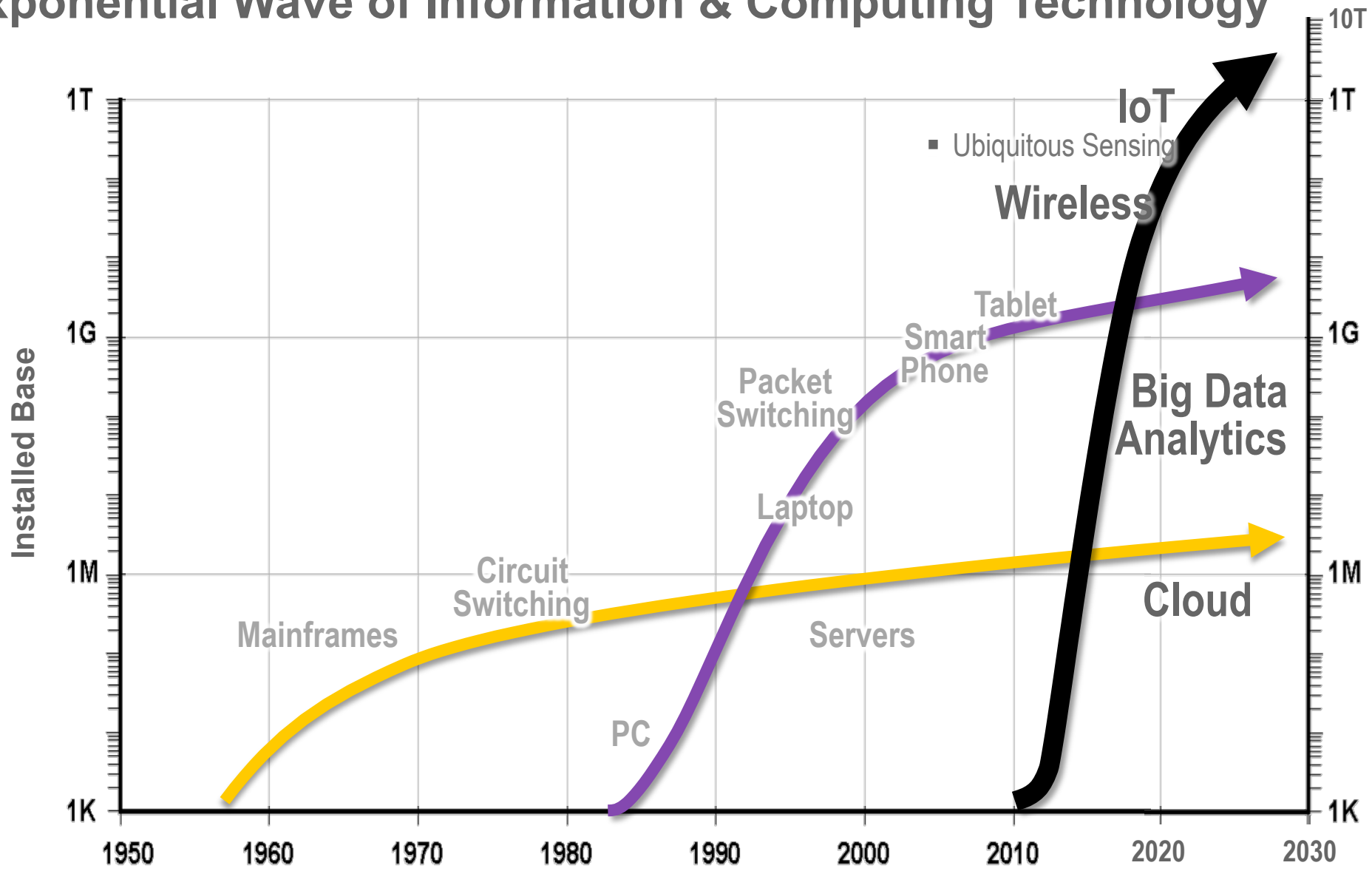
Security at the Edge For Emerging Distributed Sensor Networks

Leadership in Embedded Security Workshop
Computing Community Consortium
August 13, 2018

Samuel H. Fuller
CTO Emeritus and Distinguished Scientist
Analog Devices Inc.
Visiting Scientist, MIT

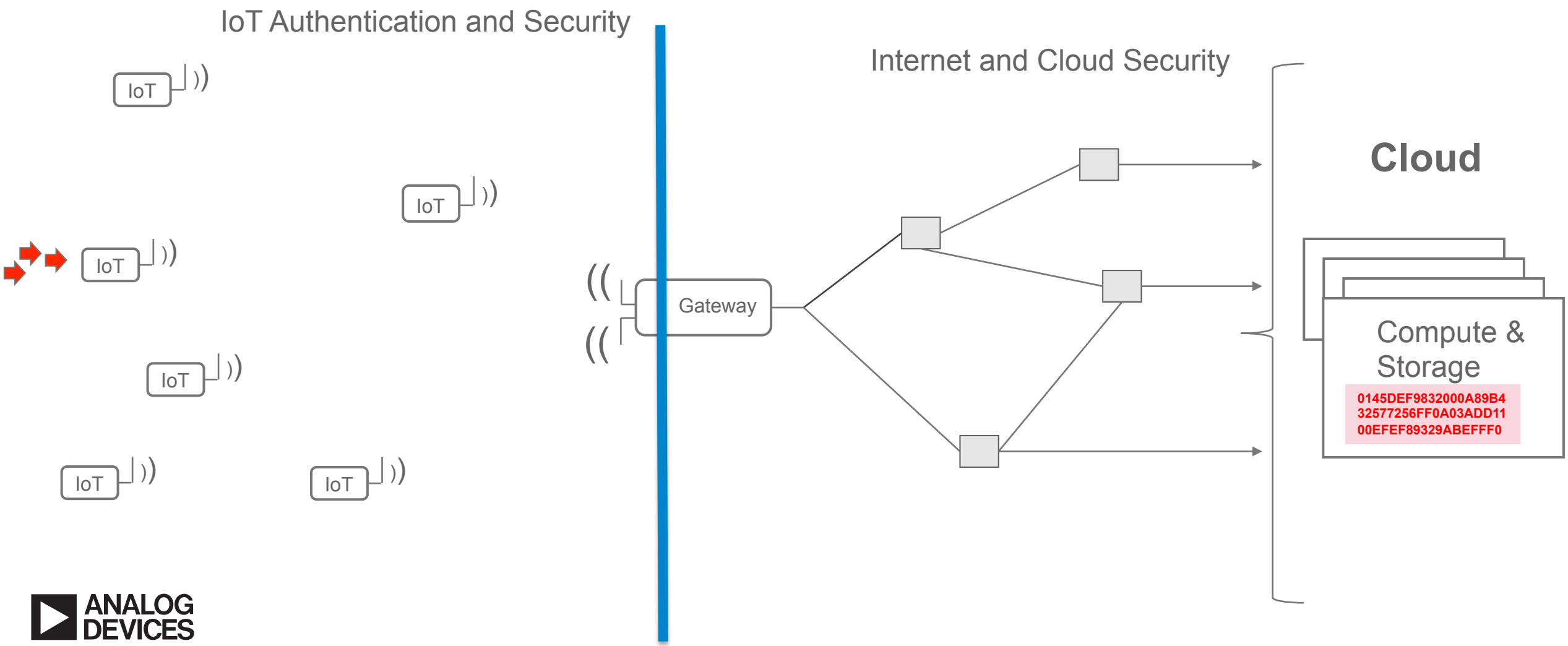
ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

3rd Exponential Wave of Information & Computing Technology



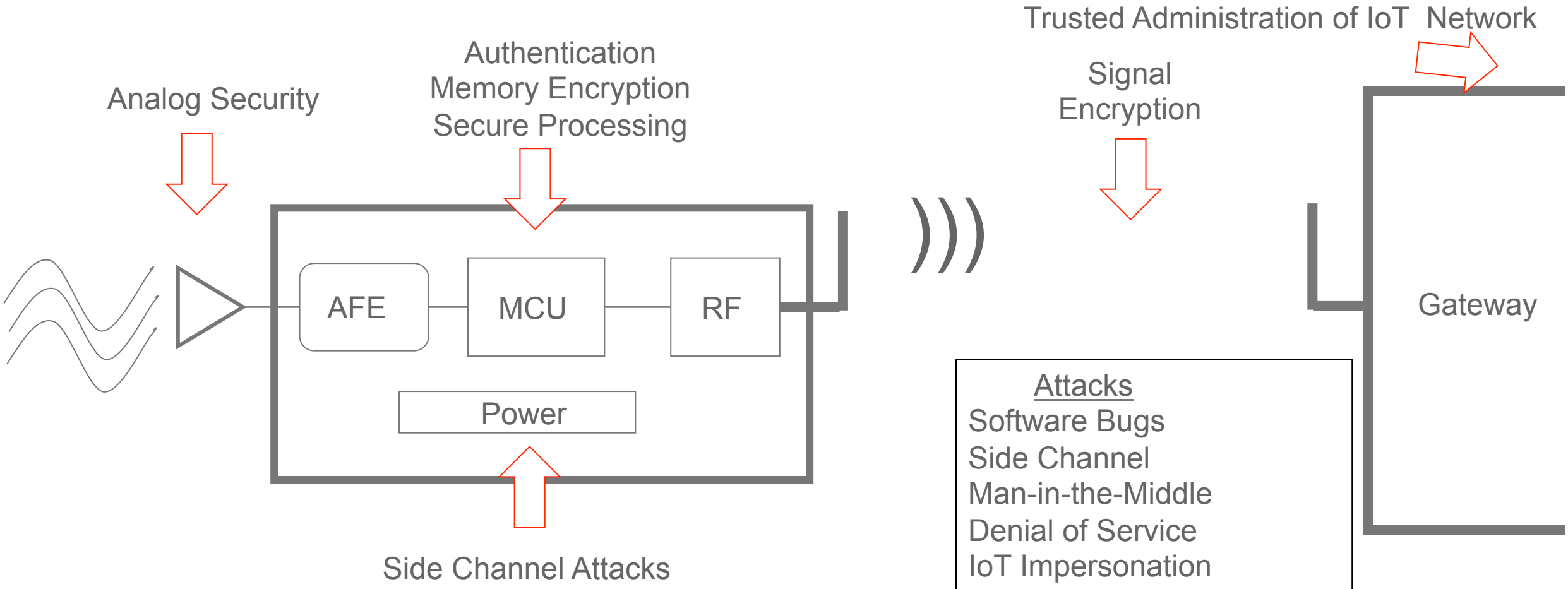
ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

Analog **Physical Signal to** *Digital* **Information**



ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

Security Threats & Defenses

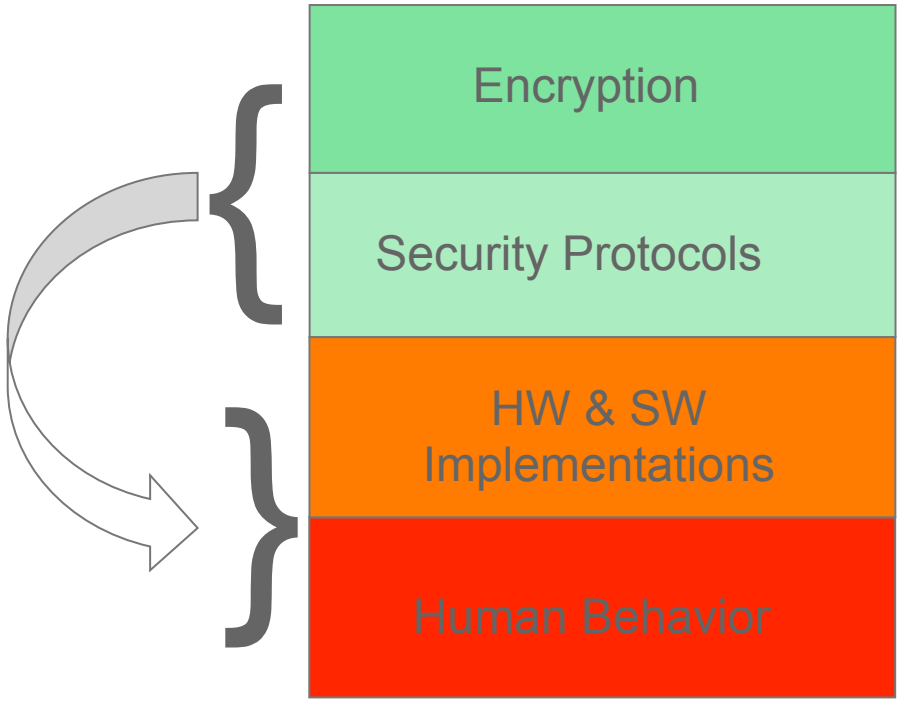


Attacks
Software Bugs
Side Channel
Man-in-the-Middle
Denial of Service
IoT Impersonation
Hardware bugs
Social engineering
Tampering with HW or SW

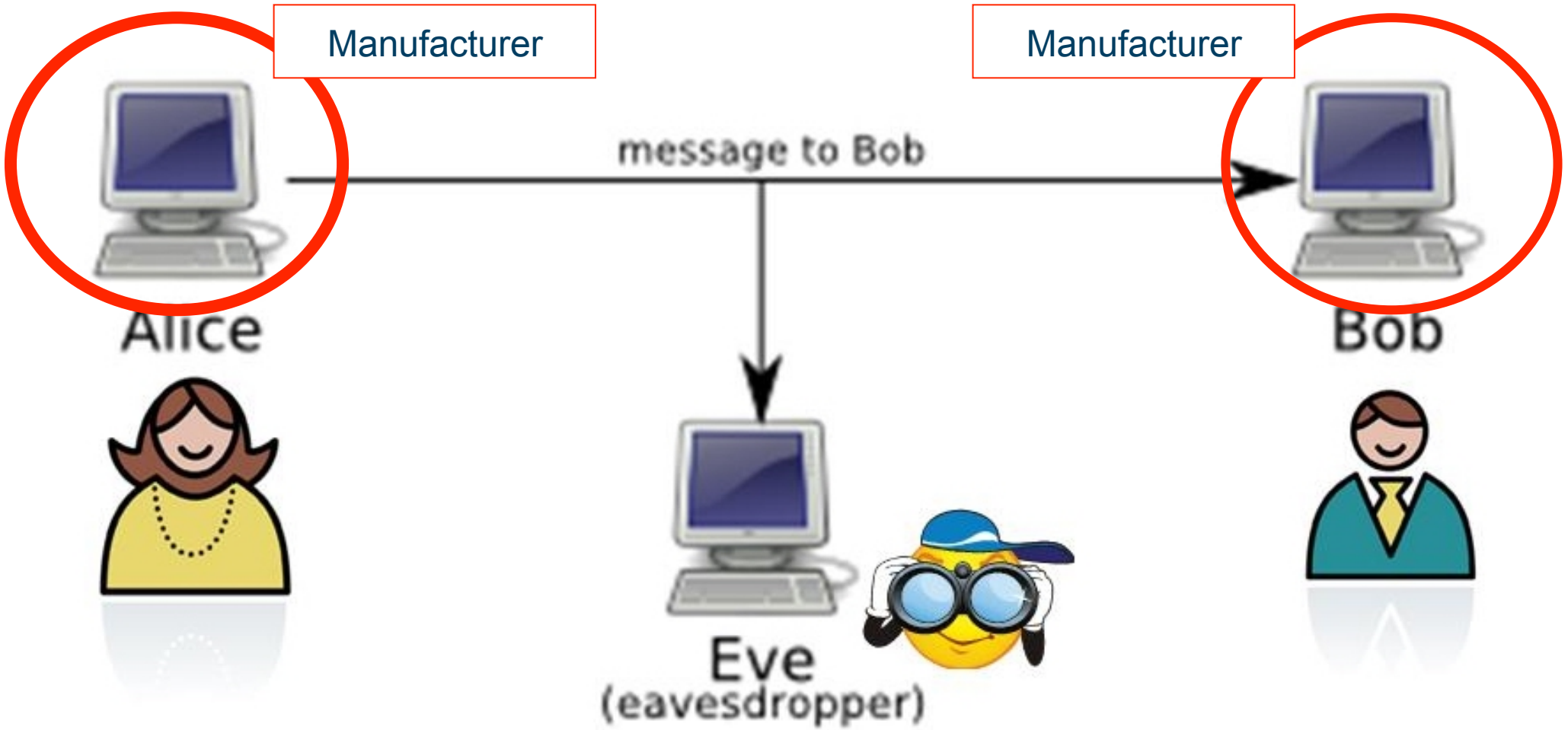
ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

High(est) Level View of Security Risks

- Encryption
  - Two types: Symmetric key encryption & Public Key encryption
  - Deep mathematical foundation
  - Critical toolset for security
  - Research opportunity: quantum secure PKI
- Security Protocols
  - Enable secure communication between parties
  - Not deep mathematics
  - Complicated but robust logic.
- Implementation in Hardware and Software
  - Dozens of bugs/weaknesses per 1000 lines of code
  - Basis for many successful attacks. Big Problem
- Human Behavior
  - Social engineering: fraud, trickery and impatience. **Very Big Problem**



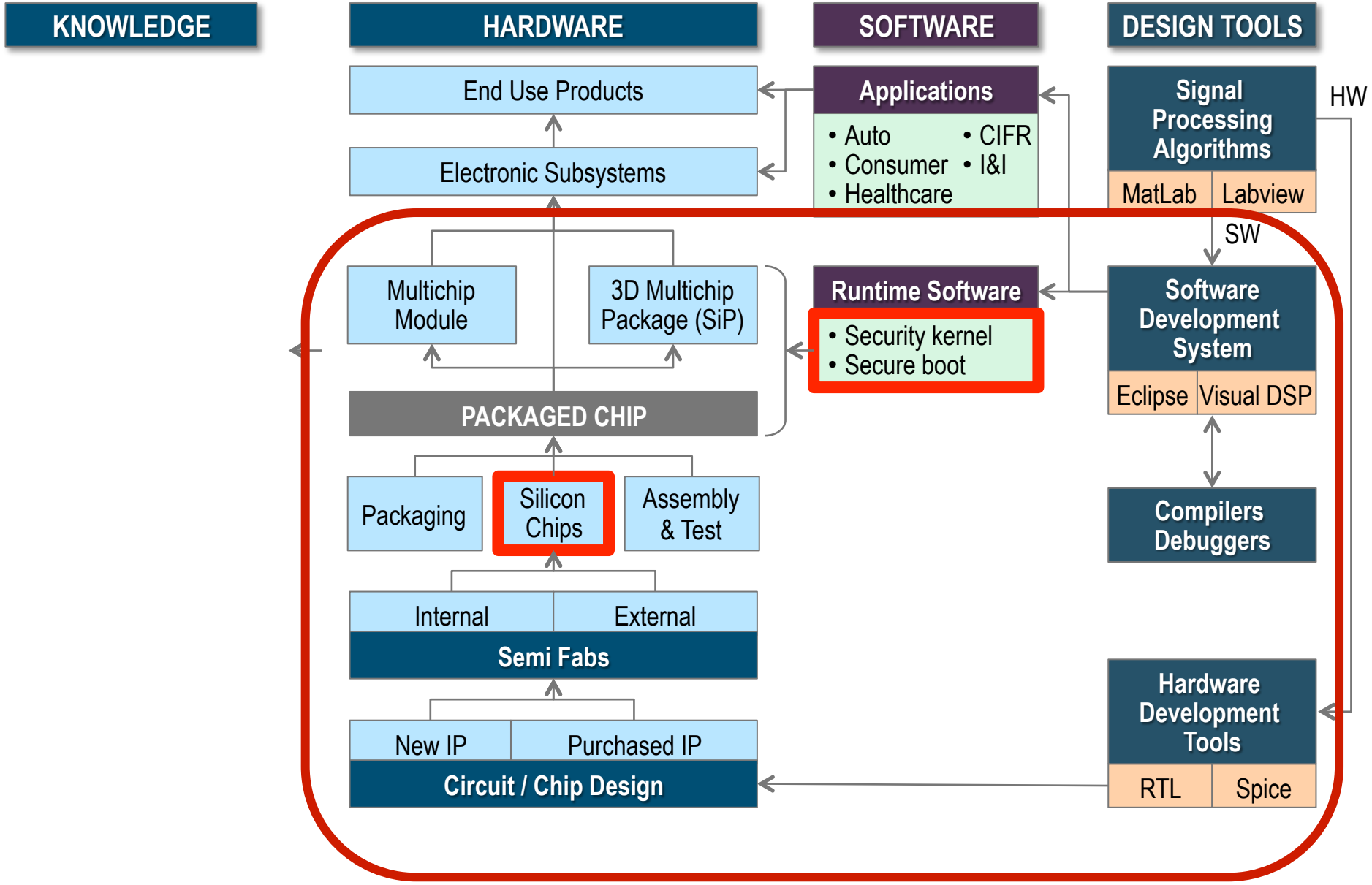
ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™



The “Silent Third Party”: Manufacturer’s HW/SW Platform

ANALOG DEVICES
AHEAD OF WHAT’S POSSIBLE™

Embedded Node Ecosystem



ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

Complexity is the Enemy of Security

Challenges faced by the Silent Third Partner in Security

	Complexity	Maximum Complexity of Trustworthy "Kernel"
▶ Software	10^{12} bits	less than 10K lines of code
▶ Hardware	10^{10} transistors	less than 10K logic gates
▶ People	10^{3} people	1 team of less than 10 people.

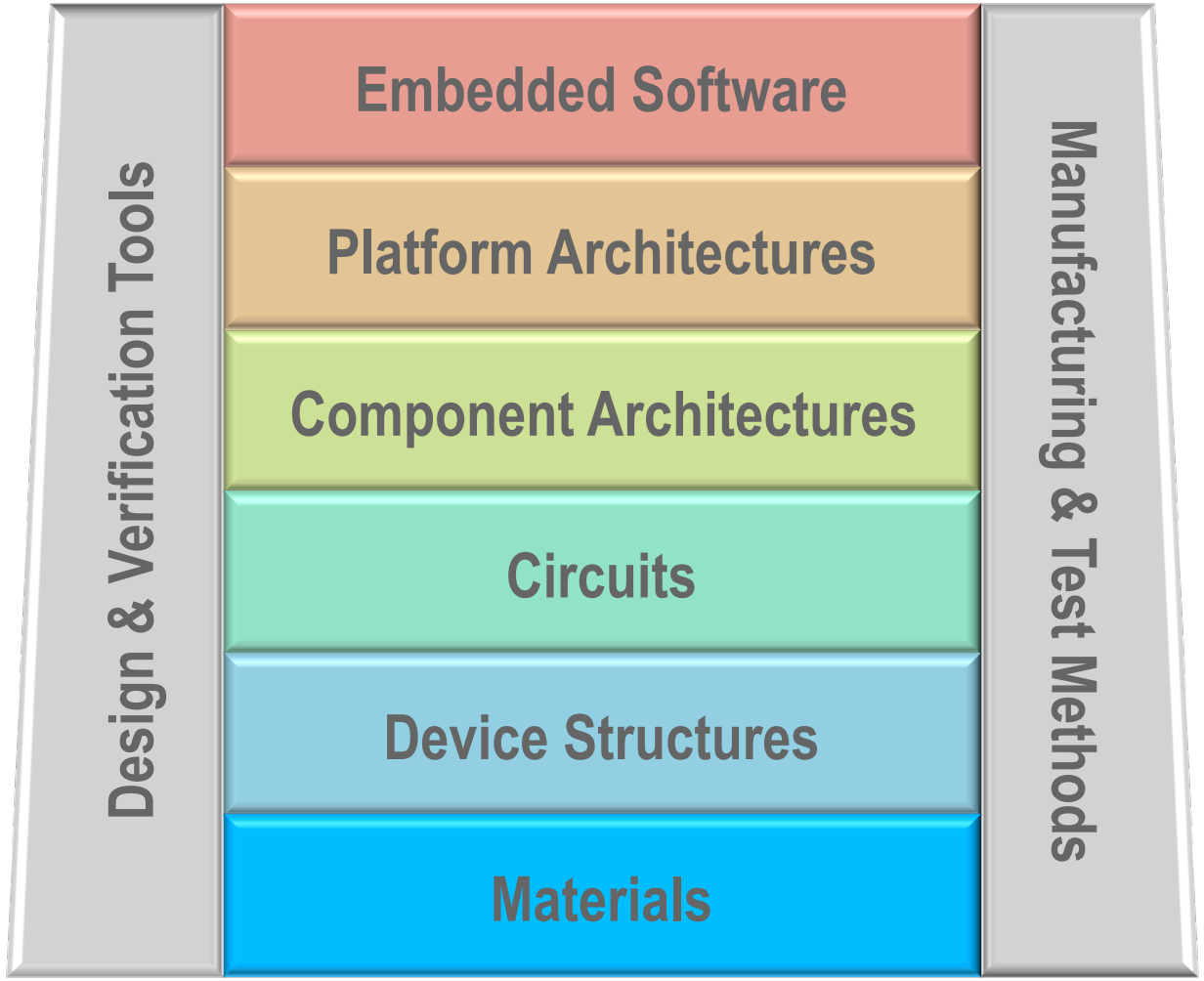
ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

Authentication is particularly critical in Distributed Edge Nodes

- **Experience from Authentication in traditional Distributed Systems**
  - Public Key Encryption proven essential for remote authentication
    - Example: Kerberos from N-S TTP protocol to PKI protocol.
  - Two factor authentication often used for intermittent sensitive interactions

- **What is different about Authentication for Distributed Edge Nodes?**
  - Two Factor authentication difficult when no trusted agent present at Edge Node. More reliance on continuous connectivity or repeated authentication
  - Often Edge Node is severely power constrained. E.g. battery powered or energy harvested from environment
- **Energy efficient strong authentication protocols required.**

Embedded System Technology Stack



Embedded application secure update mechanism

Secure boot/kernel (<< 10K instructions)

Trusted HW Zone. (<< 10K gates)

Encryption IP

Root of Trust

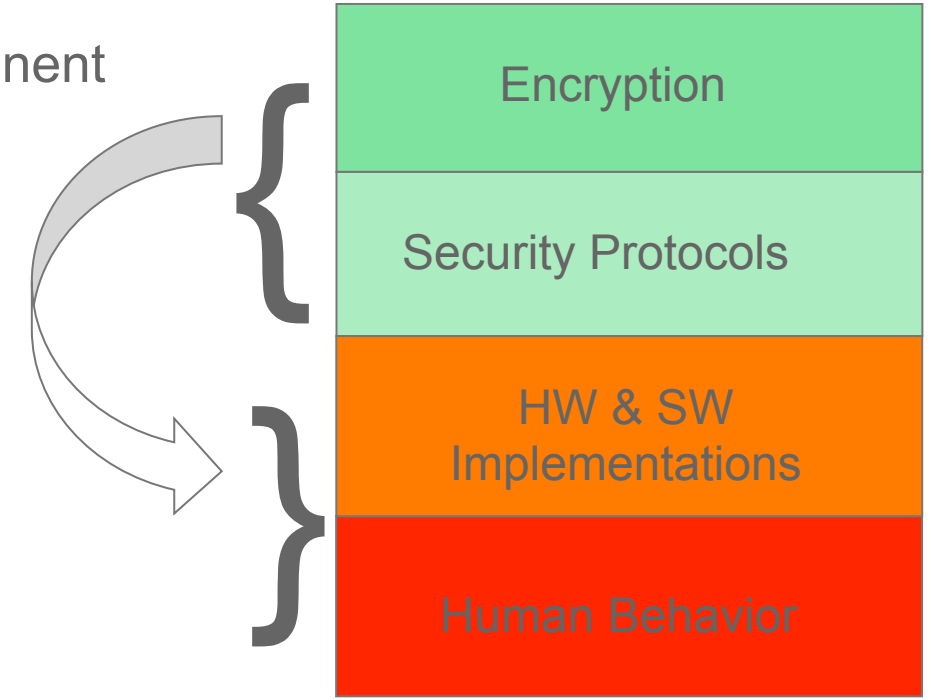
Security from side channel attacks

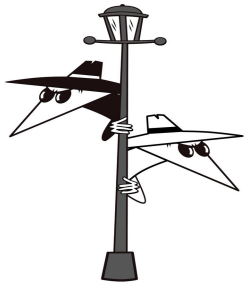
Tamper proof package

ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

If You Remember Nothing else today:

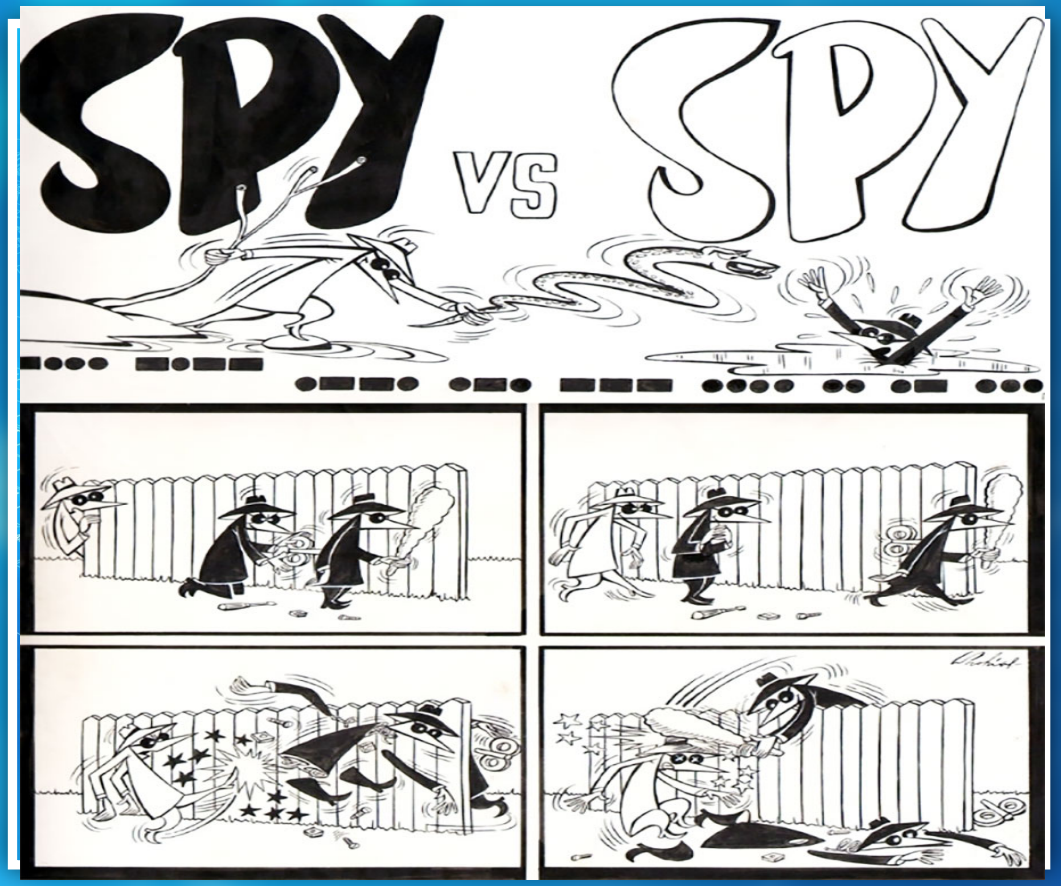
- **Security is a capability of the system** not a component
  - System is only as secure as it's weakest link
  - Encryption is just one of the necessary links
- **Complexity is the enemy of Security**
  - What (1)hardware, (2)software and (3)humans must be trusted?
- **There is no silver bullet**
  - Continual Arms Race of attack/defend/attack/ ….
- **Authentication of IoT nodes is critical**
  - It begins with a secure Root of Trust





ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

Security at the Edge for Emerging Distributed Sensor Networks



Samuel H. Fuller
CTO Emeritus and Distinguished Scientist
Analog Devices Inc.
Visiting Research Scientist, MIT
August 13 , 2018

ANALOG DEVICES