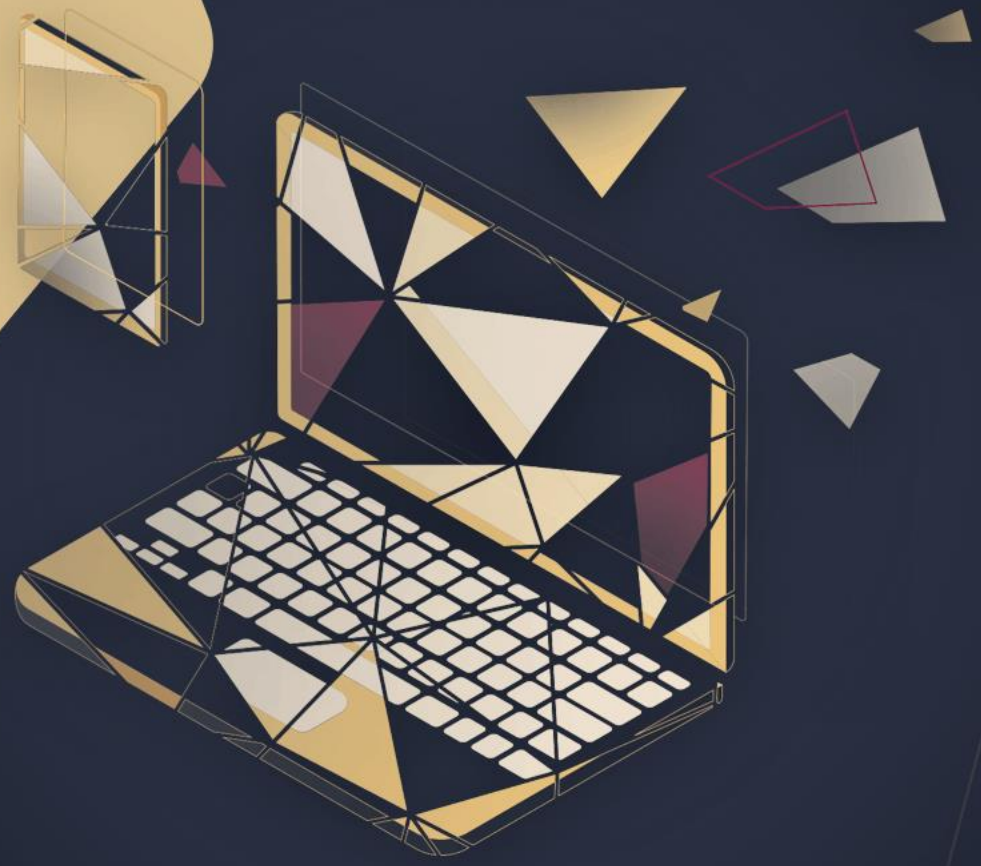
UNBOUND

Securing a Blockchain IoT Ecosystem with MPC



Rebecca Aspler
Director, Product Management

UNBOUND

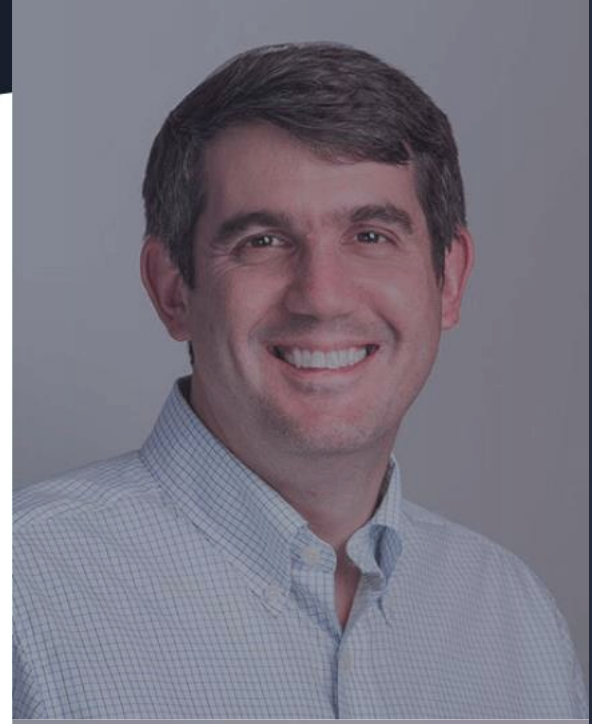
Unbound Tech

WHO WE ARE

Unbound delivers secure, scalable and agile **cryptography designed for the digital business**.

Developed by **world-renowned scientists** in the field of Multiparty Computation.

Built on **100 person-years** of cryptographic research and development experience.



Prof. Yehuda Lindell
CEO, Co-founder

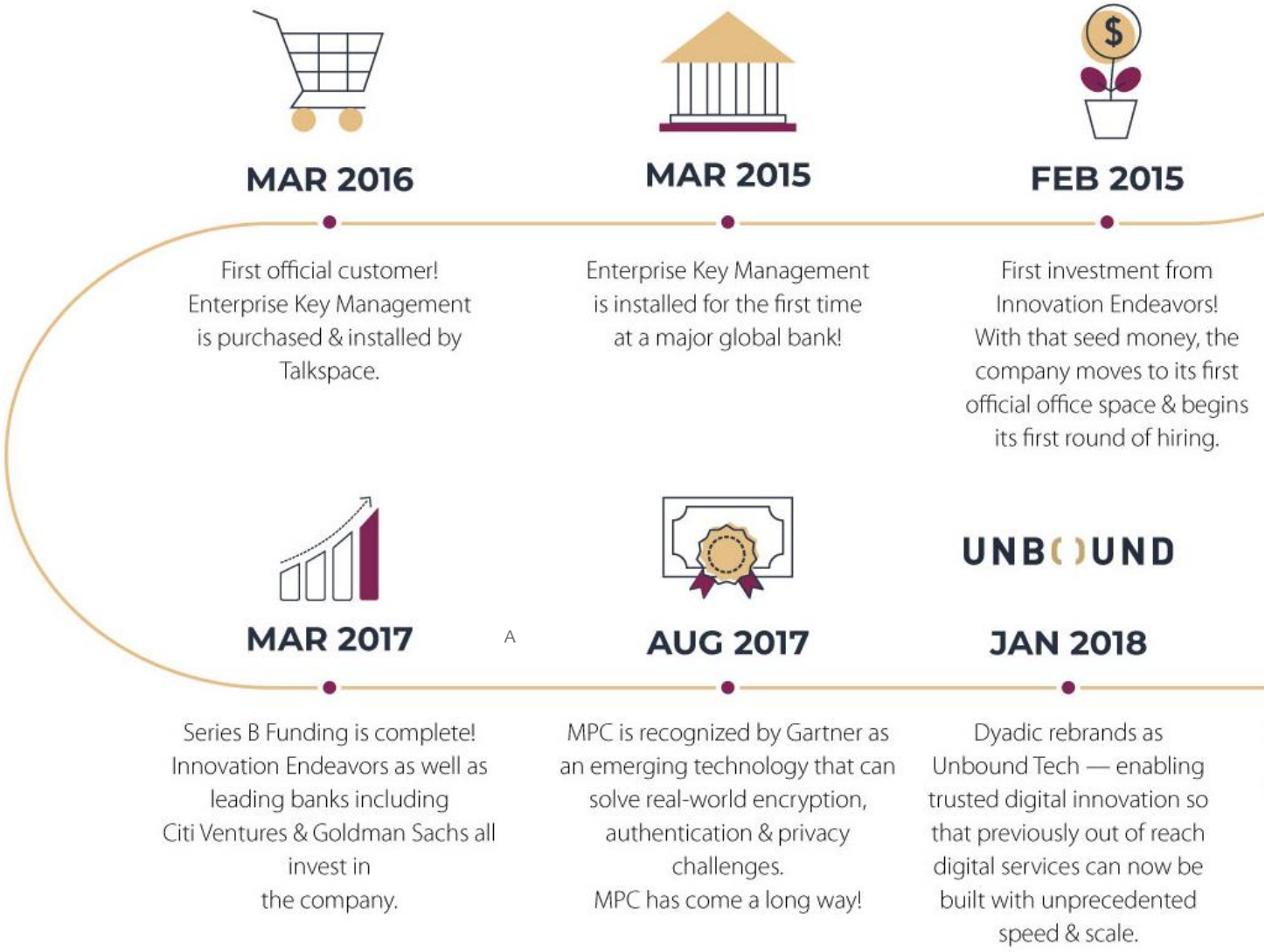
Wikipedia

Prof. Nigel Smart
Co-founder

Wikipedia

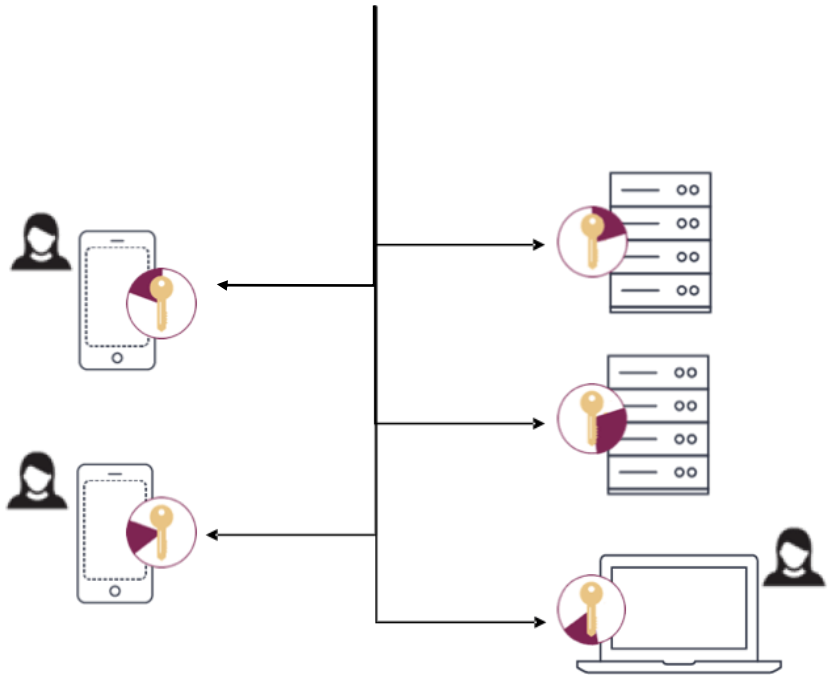
Unbound Tech

- Established in 2015
- Safeguarding Digital secrets – we are eliminating risks (vs. mitigating risk approach)
- Solutions are based on revolutionary breakthroughs in cryptography – Multi-Party Computing (MPC)
- Working with Fortune 1000 enterprises



UNBOUND

MPC Based Authentication and Signing



Pure software approach

- Split the key into different random shares
- Place the random shares in different, highly segregated places (any hardware)
- Perform all cryptographic operations using key shares without ever bringing them together
- Shares are refreshed continuously

How does it work?

- MPC – sub-field of cryptography since 1980s
- Allows multiple machines to jointly compute a function while keeping their inputs private
- Security guarantee – mathematically proven
- Recent protocol optimizations enable commercial use

UNBOUND

Security Challenges with IoT

What is the Need?

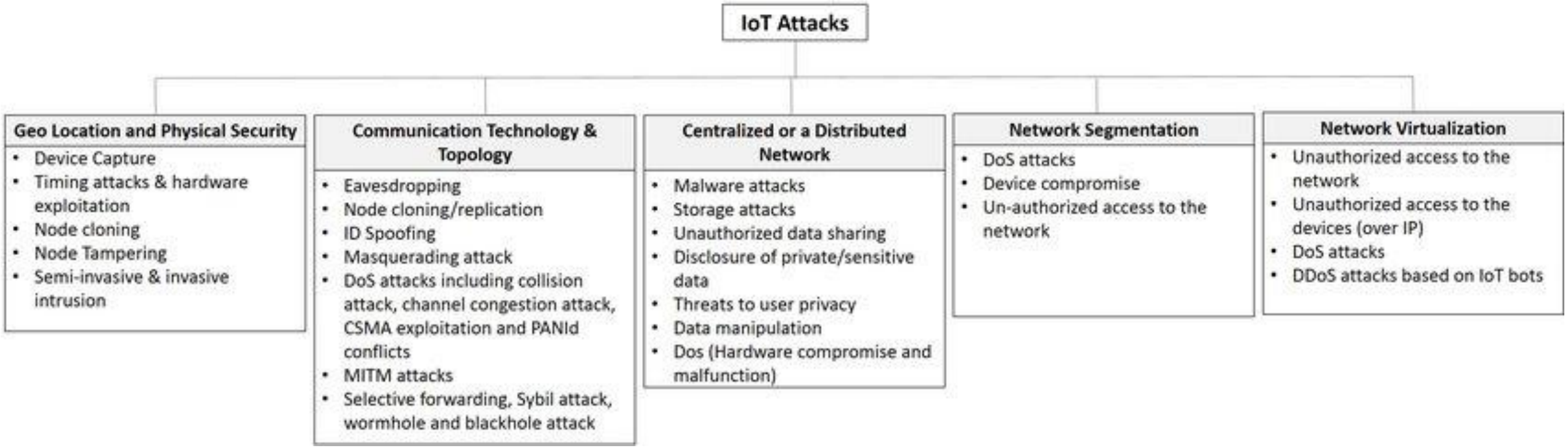
UNBOUND

- From wearables to wind turbines, the application of sensors on the ‘things’ around is everywhere.
- With a projected 10 billion more devices coming online in the next 4 years and some 44ZB of data flowing from them, such an ecosystem and its data requires a secure and efficient way to approve and track the identities, interactions and transactions of every “thing” in the network.

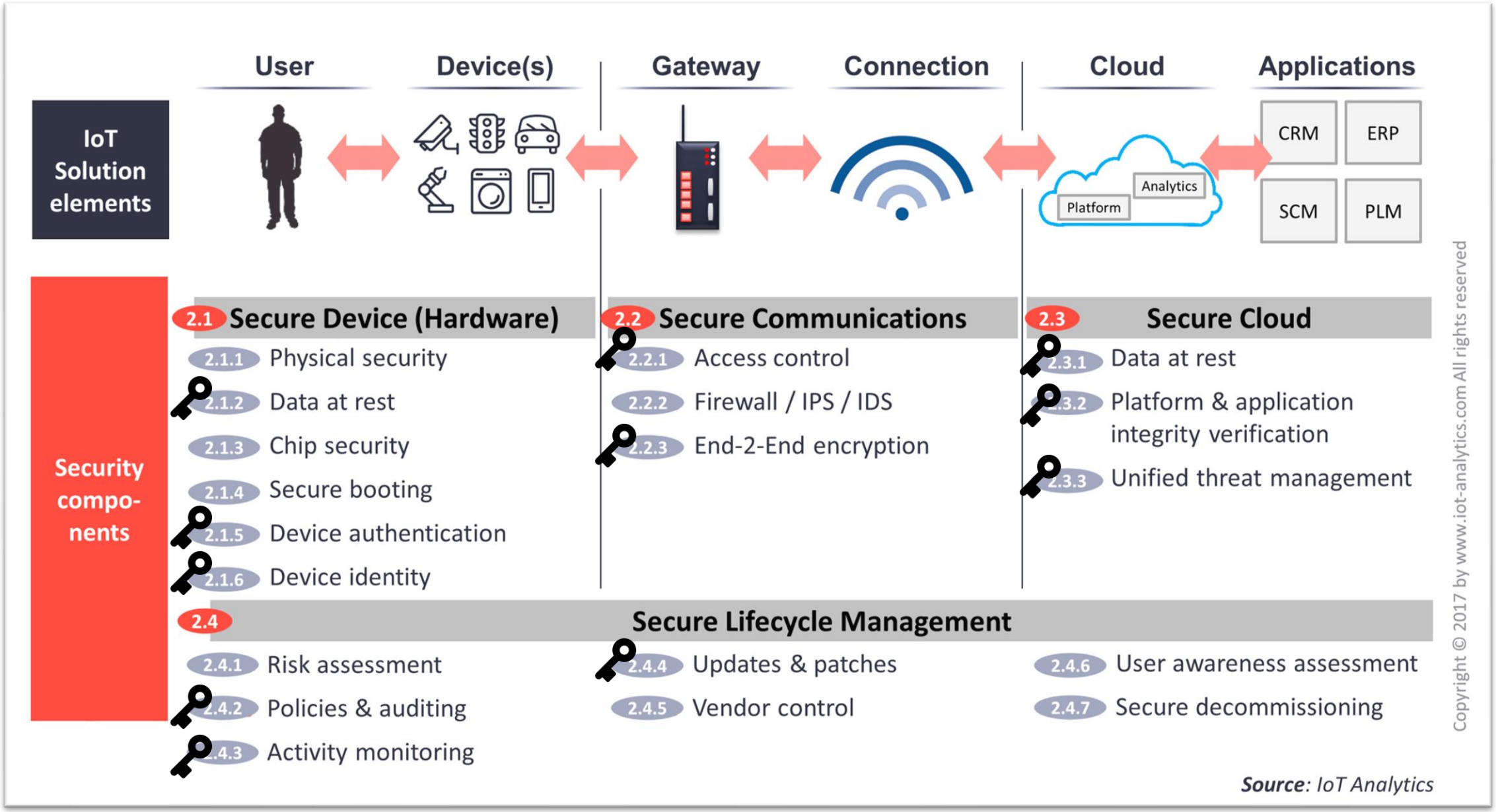
http://www.kaleidoinsights.com/wp-content/uploads/2018/01/KI_Report_IoTBlockchain_FINAL.pdf

IoT Attacks

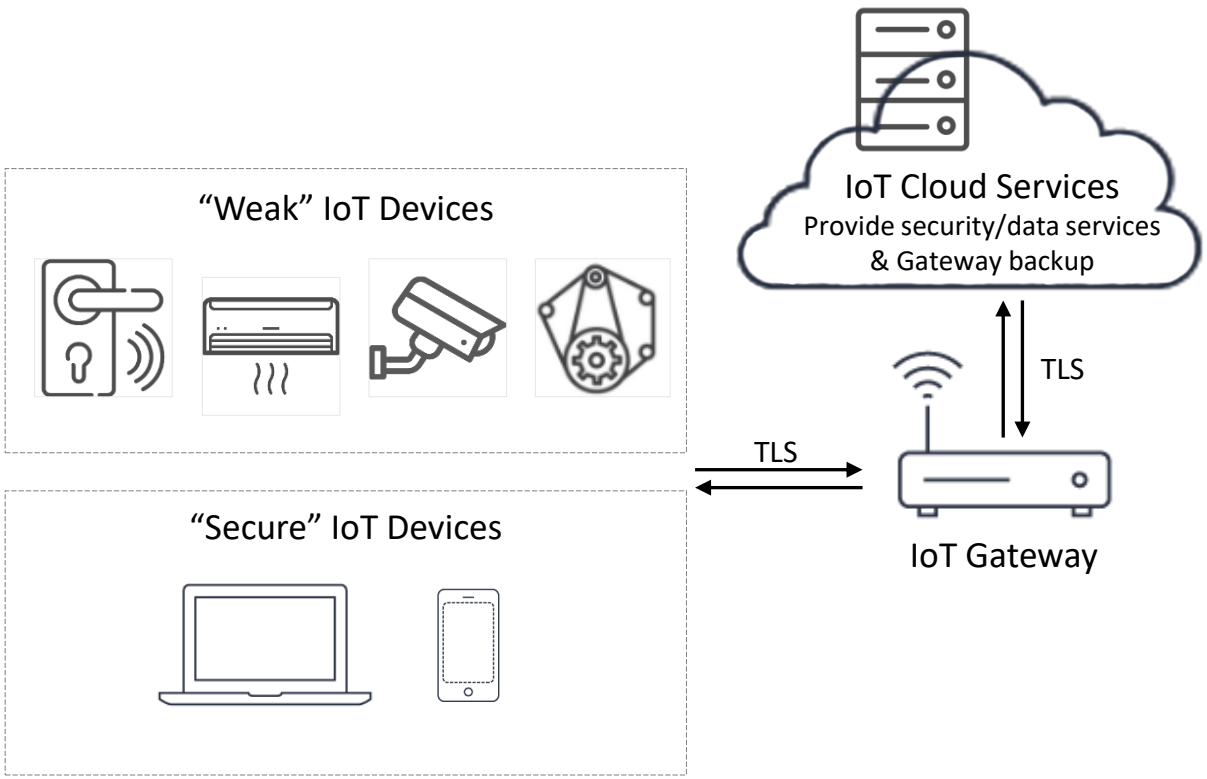
UNBOUND



Four Levels of Required Protection



Assumptions → Required Cryptography



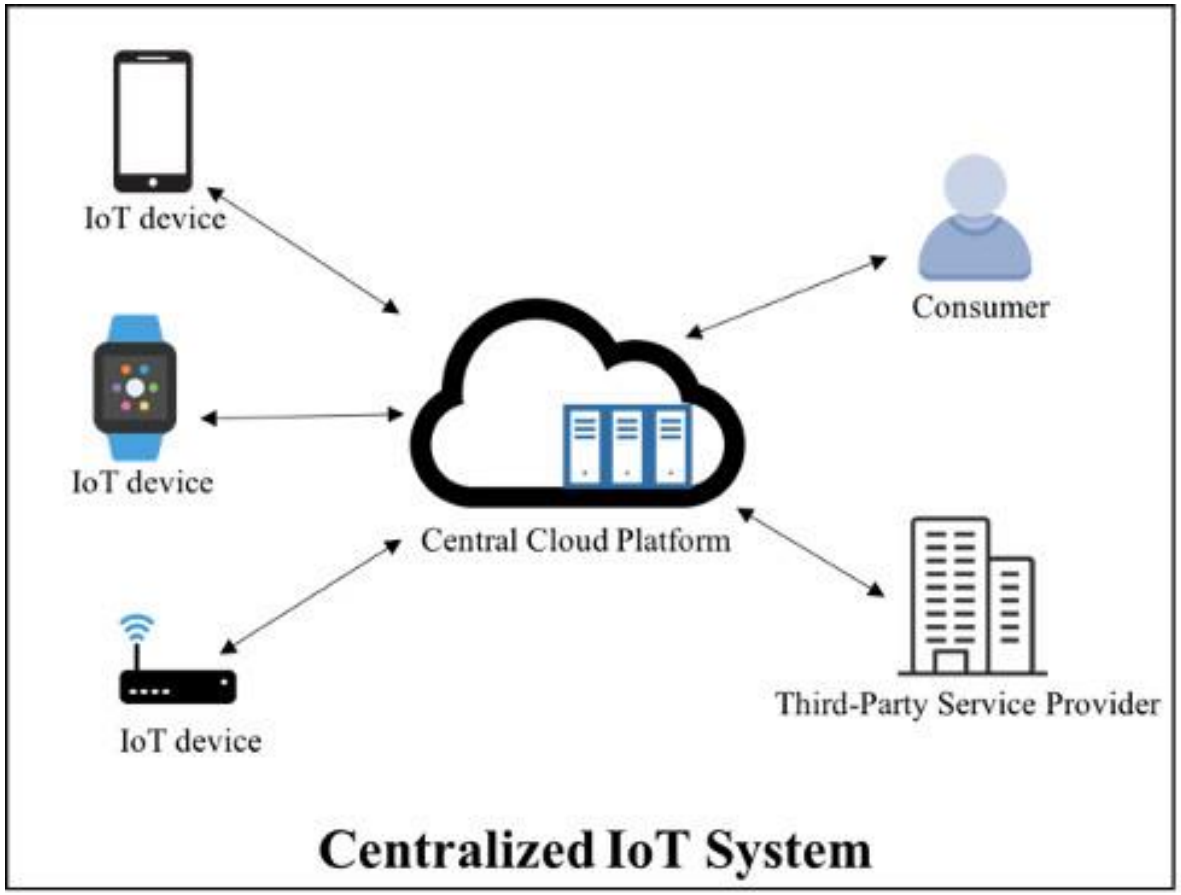
- Most IoT devices don't have secure elements.
- Many IoT devices work on battery and/or have modest processing power.
- Standalone battery is expected to last for at 2+ years.

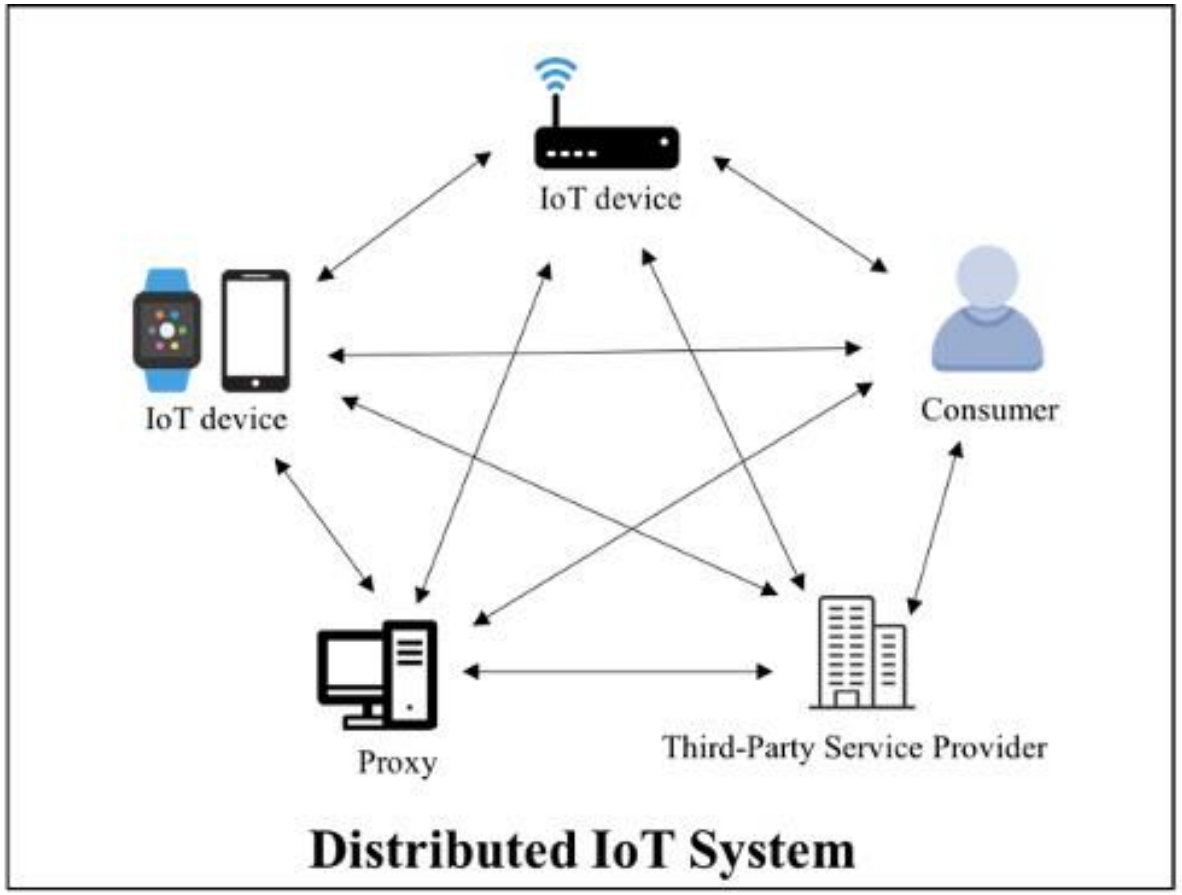
- Cryptography based security is expected to support "weak" IoT devices as well "secure" devices.
  - Obfuscation techniques are considered relatively weak.
  - Hence requiring strong algorithms ED25519/ ECIES (based on ECDH and AES) and AES.
- Operations should include message signing and data decryption.

UNBOUND

IoT Blockchain Use Cases

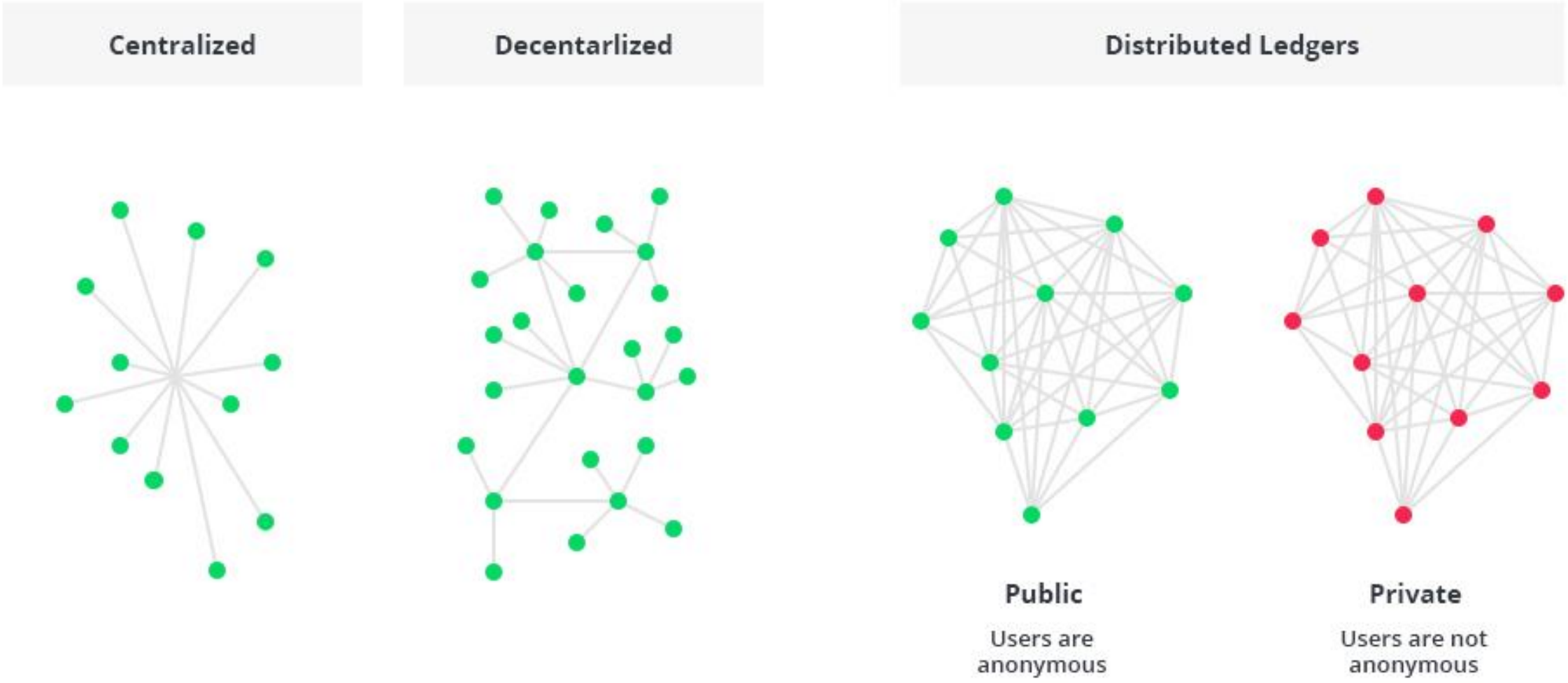
Public vs. Private IoT Ecosystems





Public vs. Private IoT Ecosystems

UNBOUND



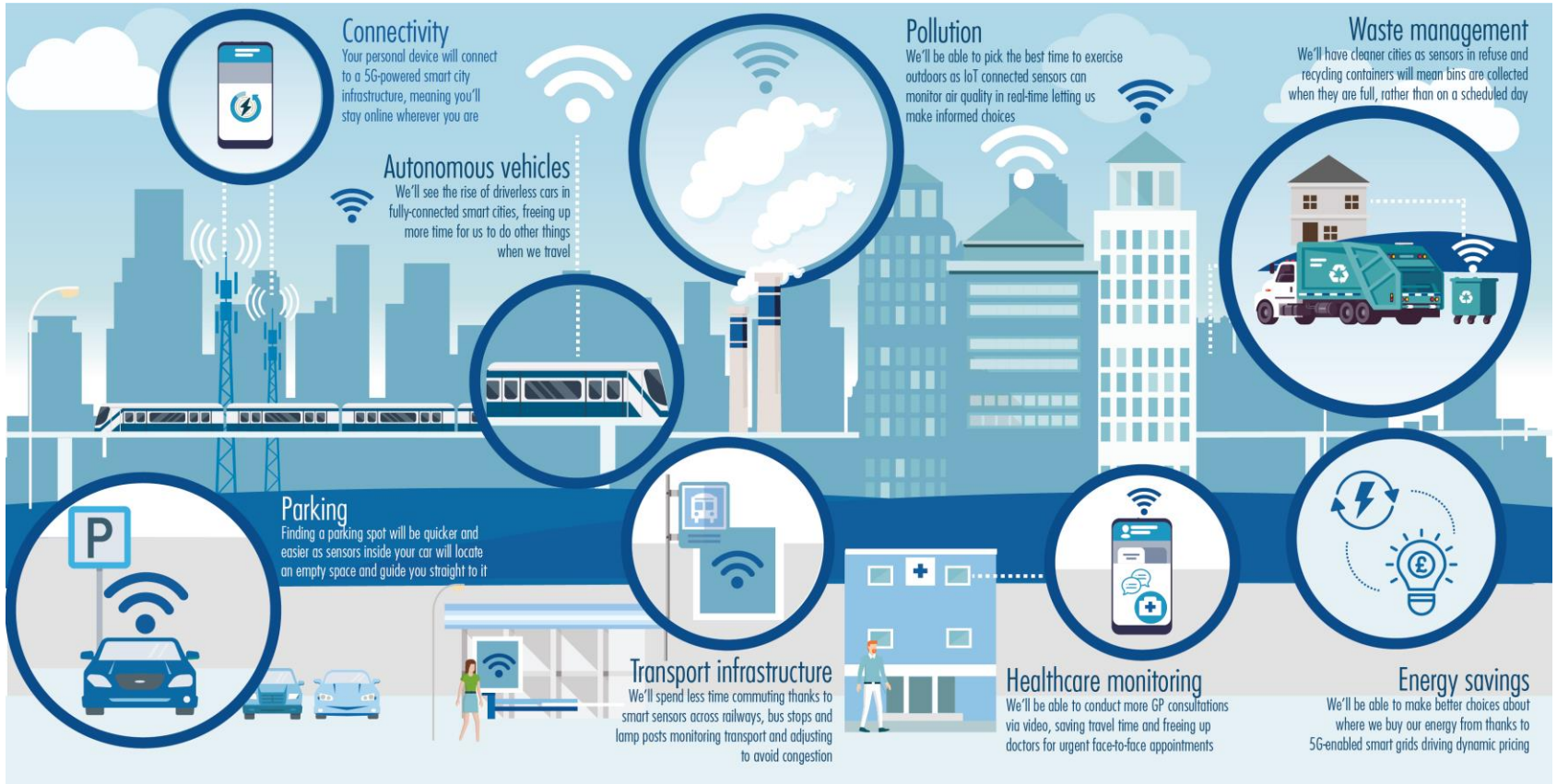
B2B Solutions
Enterprise grade Security Solutions

Usually B2C Solutions
The consumer owns and holds the key

Smart Home Example

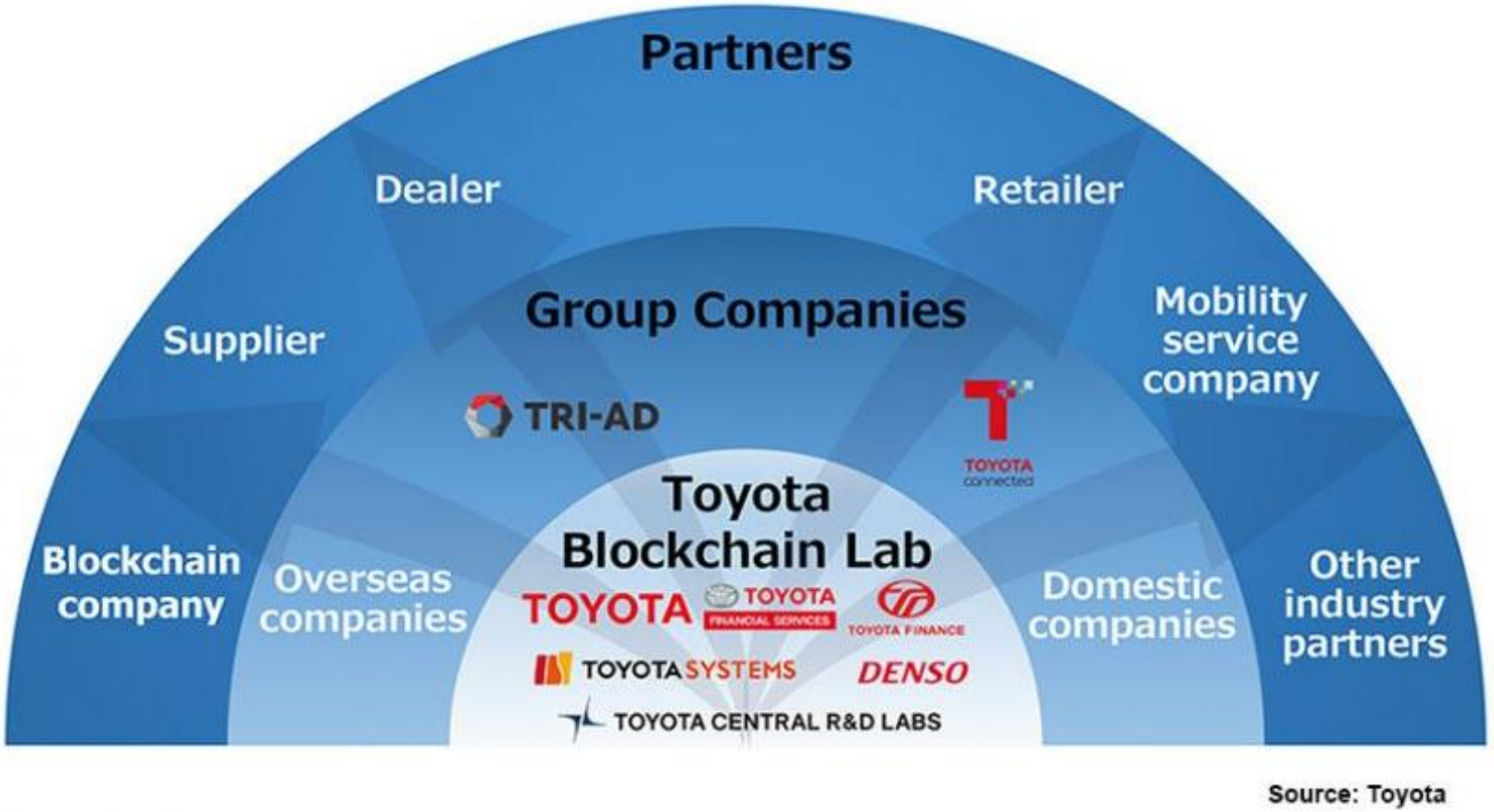
- Types of ecosystems:
  - In-house
  - In building
  - In complex
  - By manufacturer
  - By consumers
- Security Challenges:
  - Provisioning
  - Authentication
  - Data at rest
  - Data at transit
  - Transactions
- Examples of what could go wrong:
  - Safety (open door)
  - Privacy (data)
  - Energy (turn on and off)

Smart City Example



- Types of ecosystems:
  - In neighborhood
  - In area
  - In City
  - By function (traffic light # bus)
  - By manufacturer
  - By consumers
- Security Challenges:
  - Provisioning
  - Authentication
  - Data at rest
  - Data at transit
  - Transactions
- Examples of what could go wrong:
  - Safety (water pollution)
  - DoS (trains, buses, traffic lights)
  - Energy (turn on and off)
  - Privacy (residents' data)

Toyota - Distributed Ecosystem Example



Source: Toyota

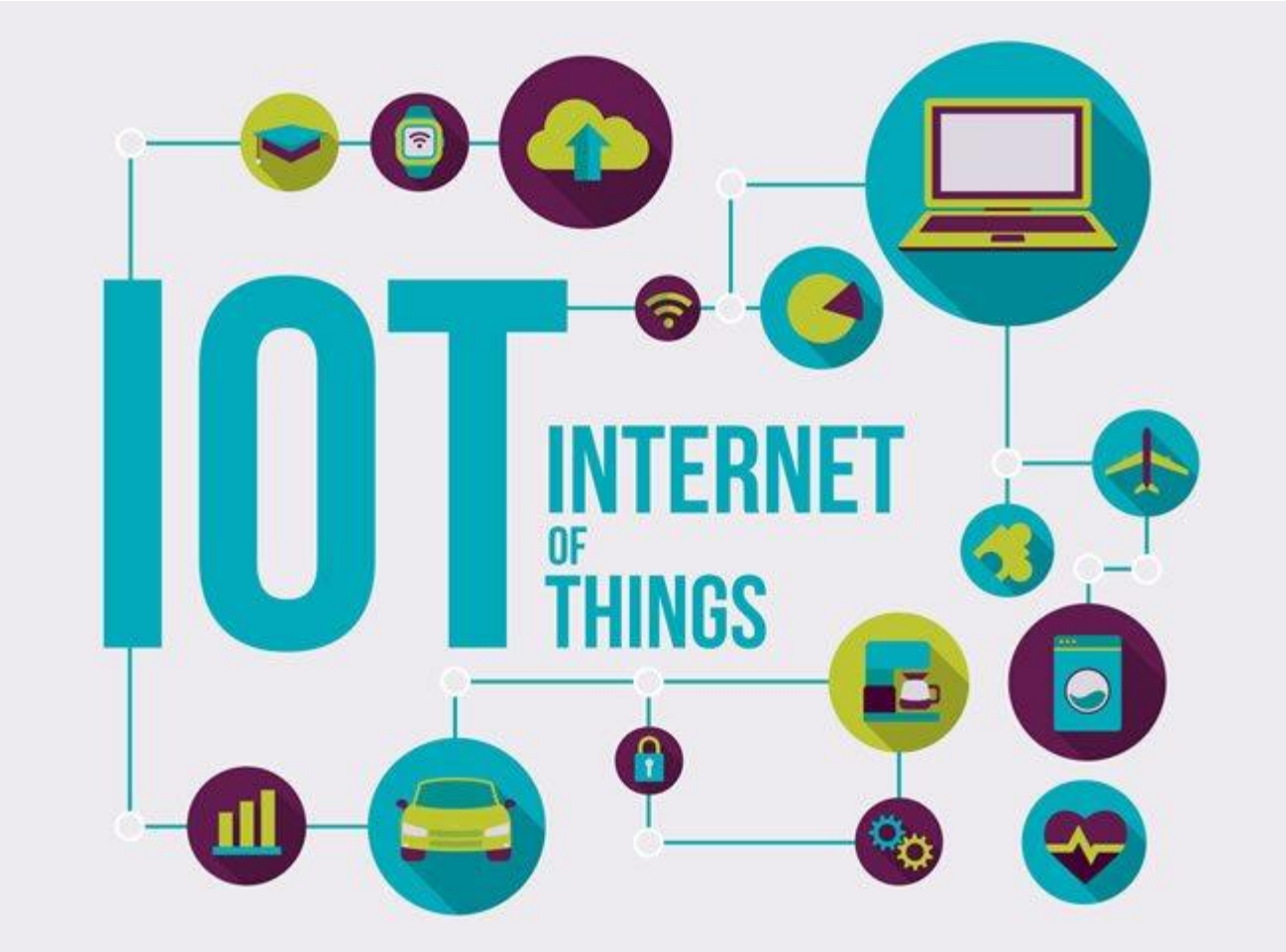
- Types of ecosystems:
  - Manufacturers
  - Service Suppliers
  - Dealers
  - Retailers
  - Consumers
- Security Challenges:
  - Provisioning
  - Authentication
  - Data at rest
  - Data at transit
  - Multi-Party Transactions
- Examples of what could go wrong:
  - Safety (taking control over a car / truck)
  - DoS (car/device isn't working)
  - Privacy (consumers' data)

UNBOUND

IoT Blockchain Security
Current Status Quo

Authenticating IoT Devices – Current ‘Tools’

UNBOUND



- User and PWD
- One-Time Password (OTP)
- Access Token
- Certificate-Based Authentication
- Hardware Token

Challenges with Current Authentication 'Tools'

UNBOUND

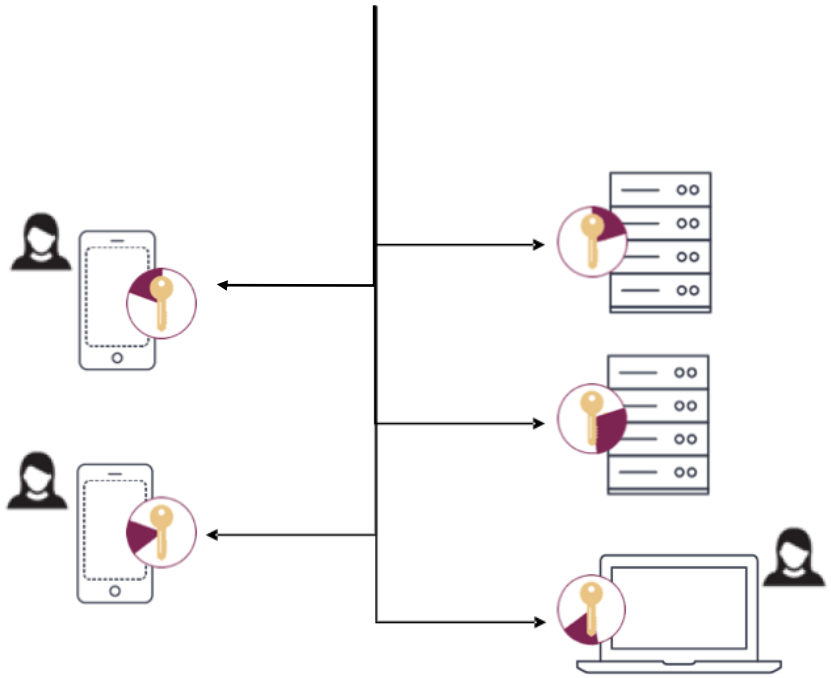
Platform Dependent	• Variety of IoT devices • Manufactured by huge array of vendors
High TCO	• Dedicated teams, HW and SW tools to integrate keys into TPMs. • This is costly, slow, and cumbersome (cars as an example)
Resource Constrained Devices	• Often, these are resource-constrained devices • Or even brownfield equipment, that allow little, if any, hardware modification.
Not Secure	• Old fashioned authentication tools and application security rules are easy to hack.

UNBOUND

MPC
Next Gen Security

UNBOUND

MPC Based Authentication and Signing



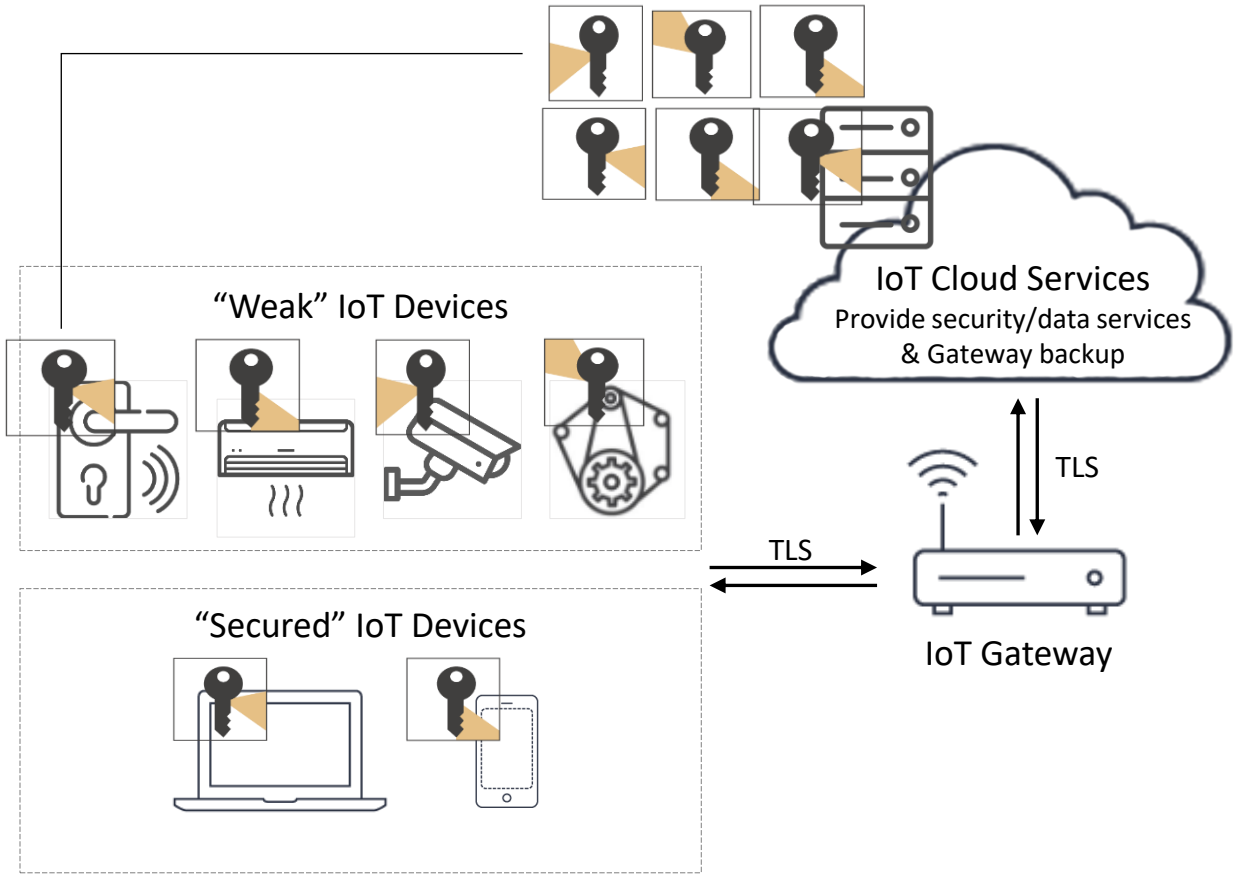
Pure software approach

- Split the key into different random shares
- Place the random shares in different, highly segregated places (any hardware)
- Perform all cryptographic operations using key shares without ever bringing them together
- Shares are refreshed continuously

How does it work?

- MPC – sub-field of cryptography since 1980s
- Allows multiple machines to jointly compute a function while keeping their inputs private
- Security guarantee – mathematically proven
- Recent protocol optimizations enable commercial use

Smart Home Example



- Cryptographic keys are split to shares.
- Each pair requires two keys shares: one is stored on the end point and the other on a server / another client.
- Key Shares are continuously refreshed
- Key shares on end points are cryptographically bound to the specific device.

Mobile App Hack Gives Thieves Full Access to Tesla Model S

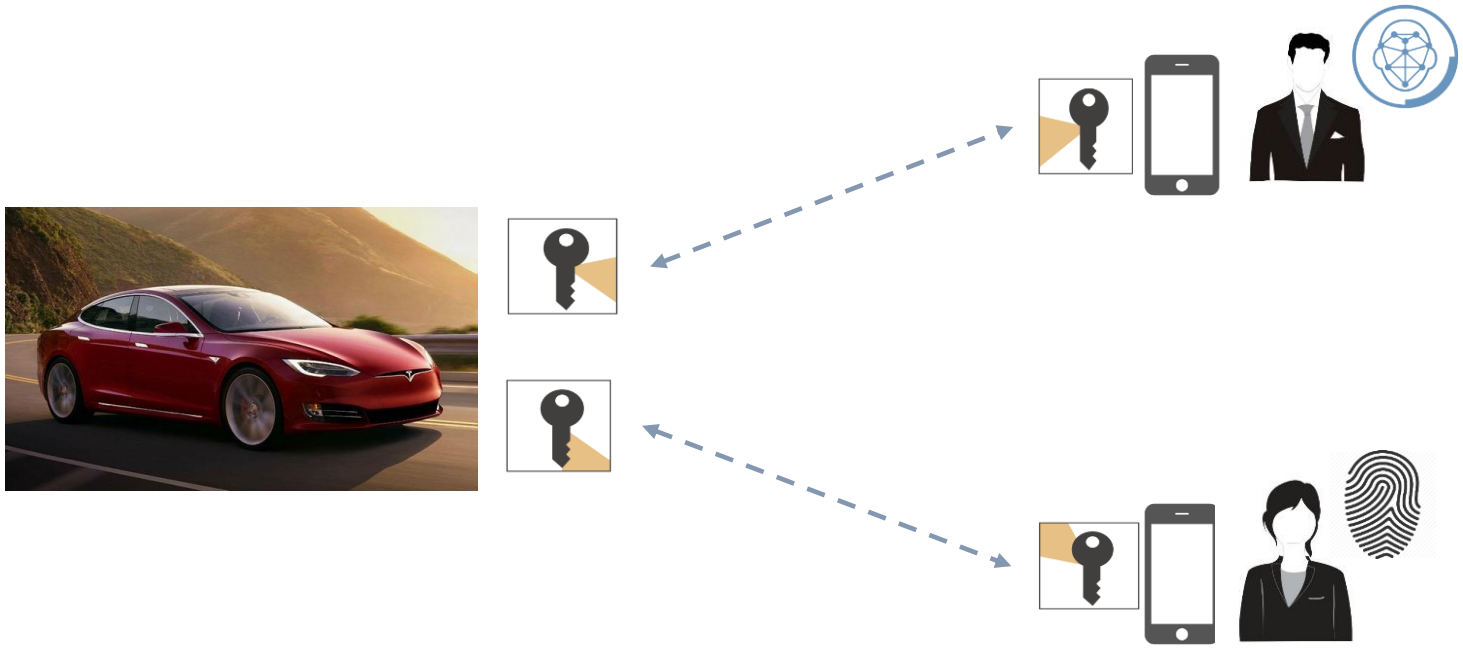
UNBOUND

Security vulnerability

- The Tesla mobile app authenticates used a secret key that had been stored locally by the phone's app.
- The authentication token had been stored in the app's sandbox folder → vulnerable to malware.

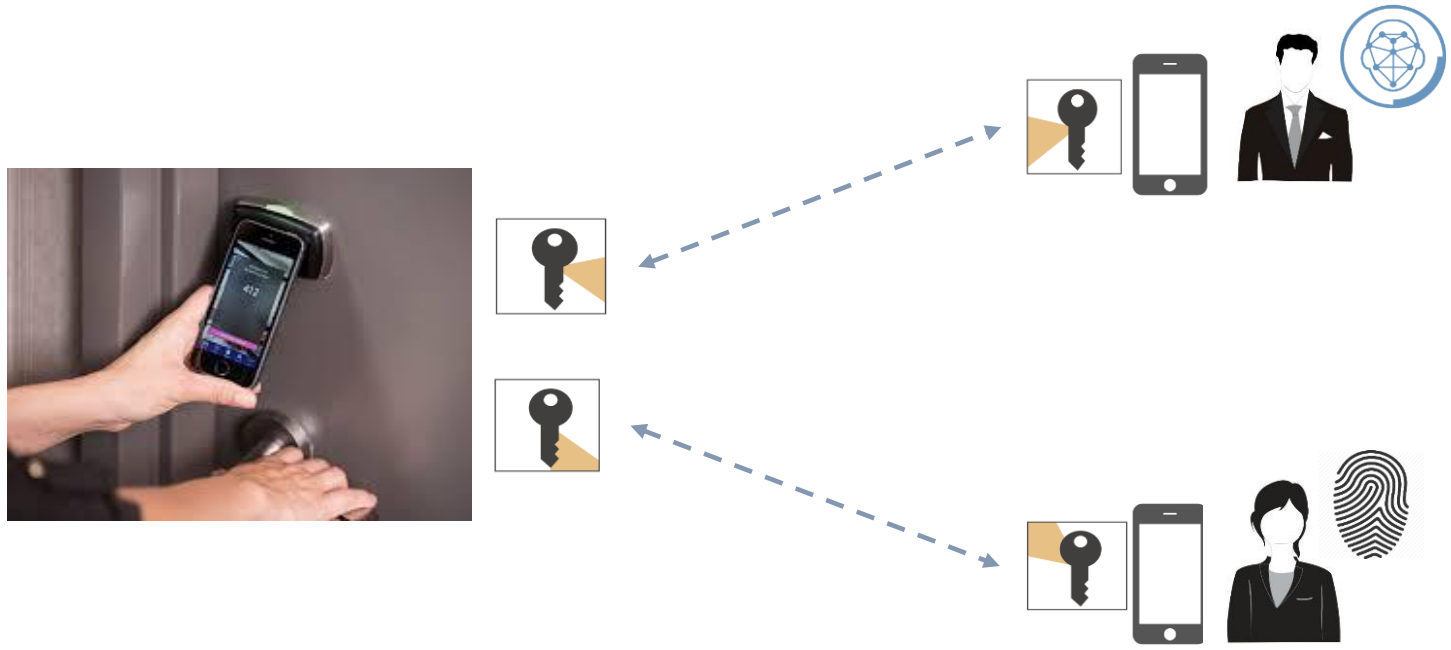
Mobile app hack gives thieves full access to Tesla Model S

Smart Home Example – The MPC Way



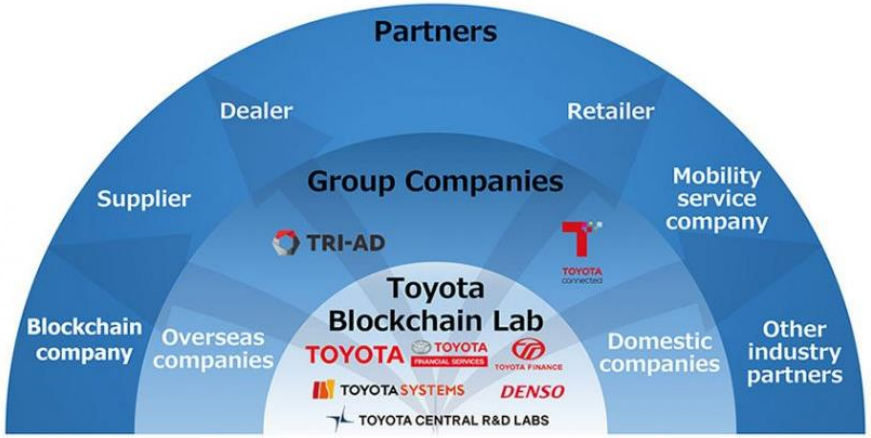
- Keys are split between the car owner app and the vehicle
- Key shares as part of MFA: biometrics, PIN, OTP, password
- Prevent relay crime
- Full authentication of the deriver's identity

Home Door Example – The MPC Way

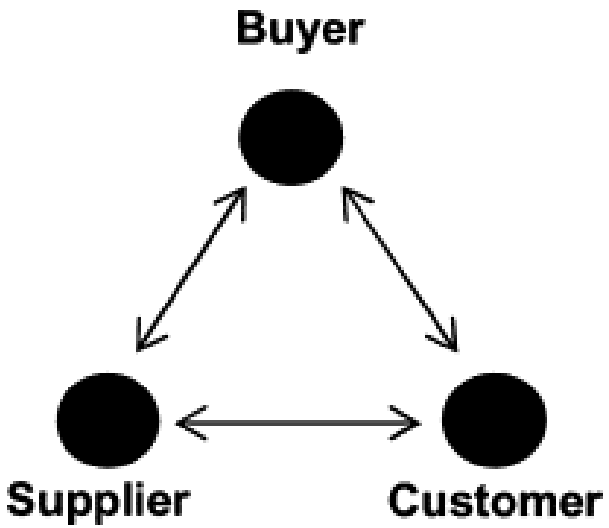


- Keys are split between the home's/ hotel's app and a server
- Key shares as part of MFA: biometrics (FR, fingerprint), PIN, password
- Full authentication of the owners' / guests' identity
- The blockchain could be of the hotel's rooms, the hotel's chain (Hilton for example), the apartments' complex etc.

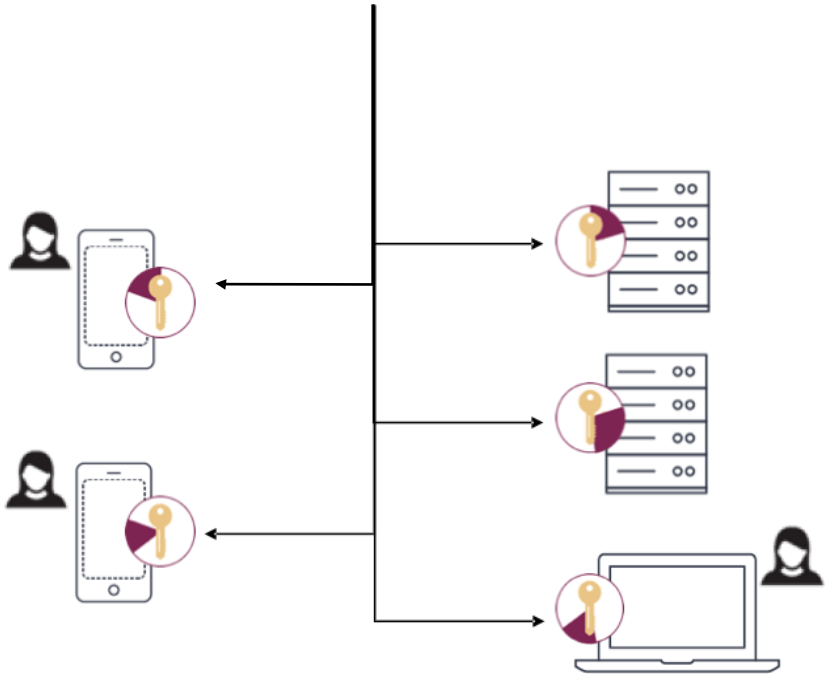
Toyota Use Case – The MPC Way



Source: Toyota



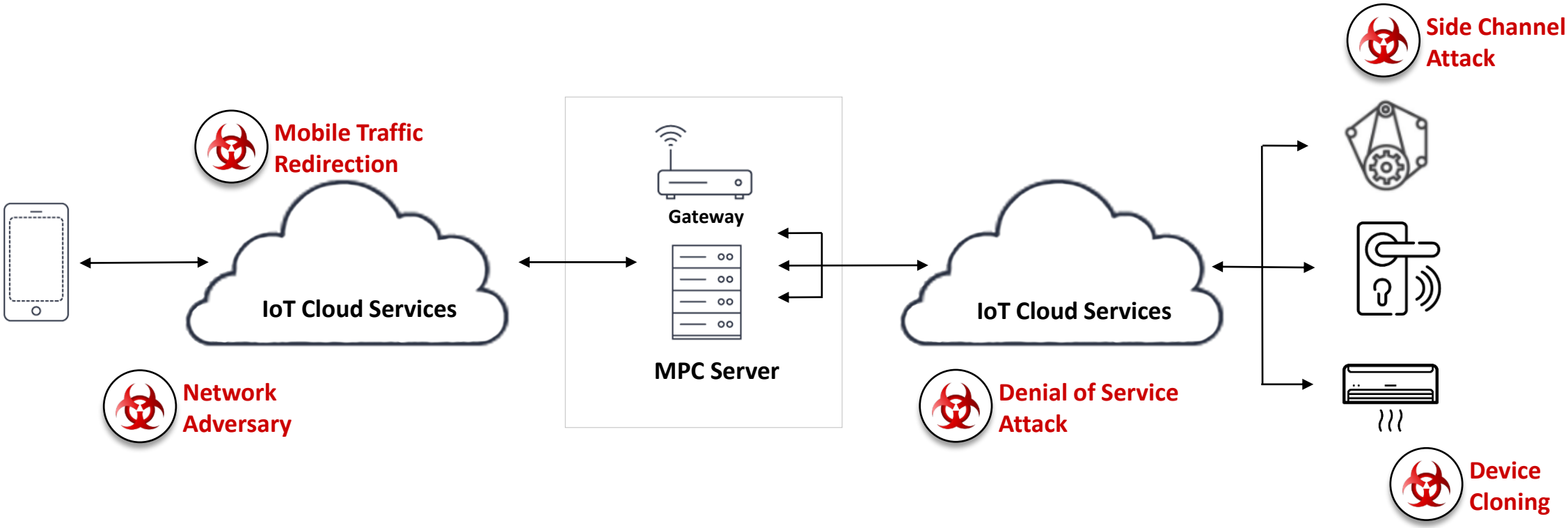
MPC Based Authentication and Signing



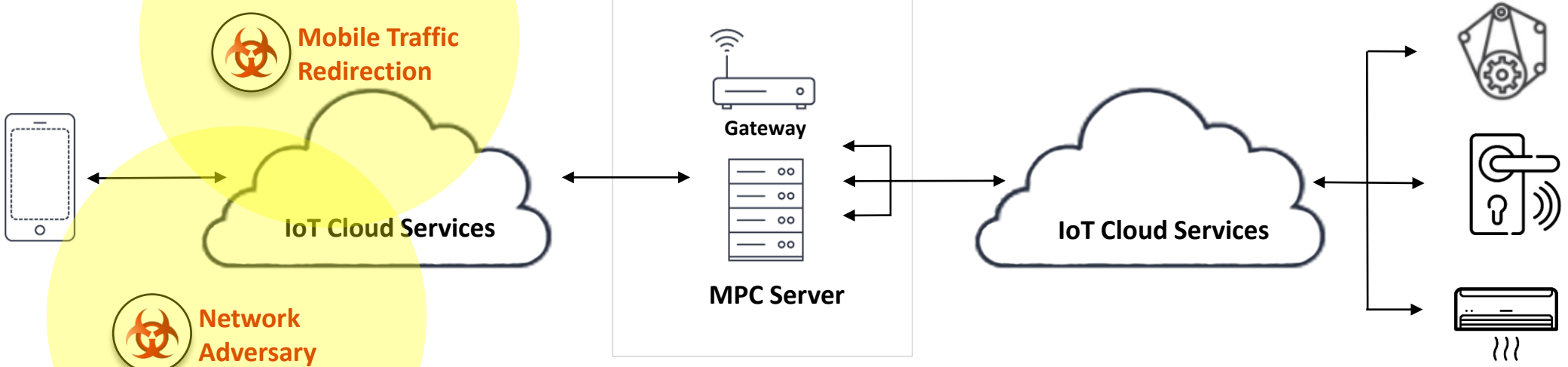
UNBOUND

Threat Model

Threat Model

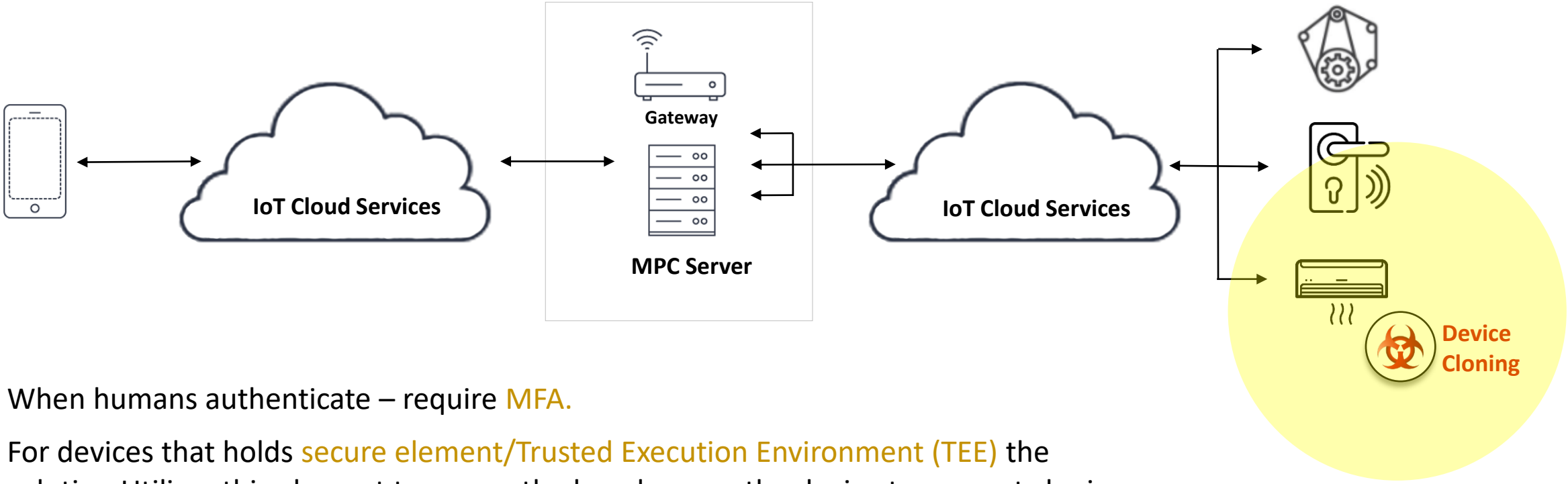


Threat Model
Network Adversary/Traffic Redirection



- All protocol messages are encrypted using AES-GCM with a shared key and a unique counter to prevent replay.
- An attacker can neither learn any information about the message from the mobile phone or the device, nor tamper with any message sent.
- All shared encryption keys are different for every device, so even in the unlikely event that one device is compromised nothing can be learned on other devices.

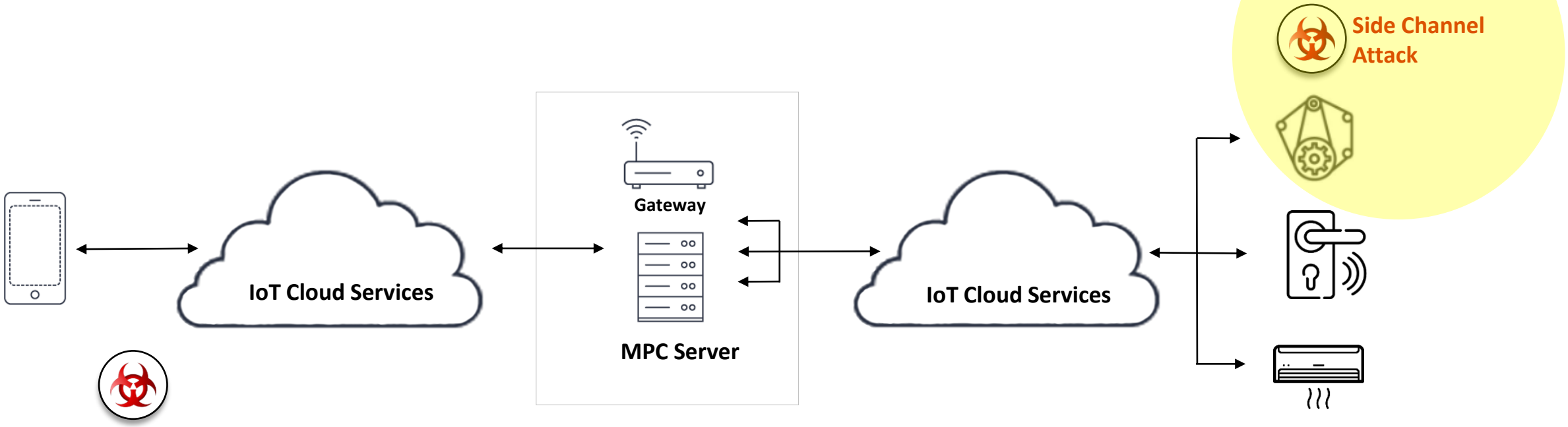
Threat Model
Device Cloning



- When humans authenticate – require MFA.
- For devices that holds secure element/Trusted Execution Environment (TEE) the solution Utilizes this element to secure the key share on the device to prevent cloning.
- Refresh the all shares continuously (configurable per need). A cloned device will need to execute an operation before the legitimate device is authenticating and shares are refreshed.
- If the cloned device carries out an authentication before the legitimate device, the MPC solution-protocols will detect the clone attack and raise a flag.

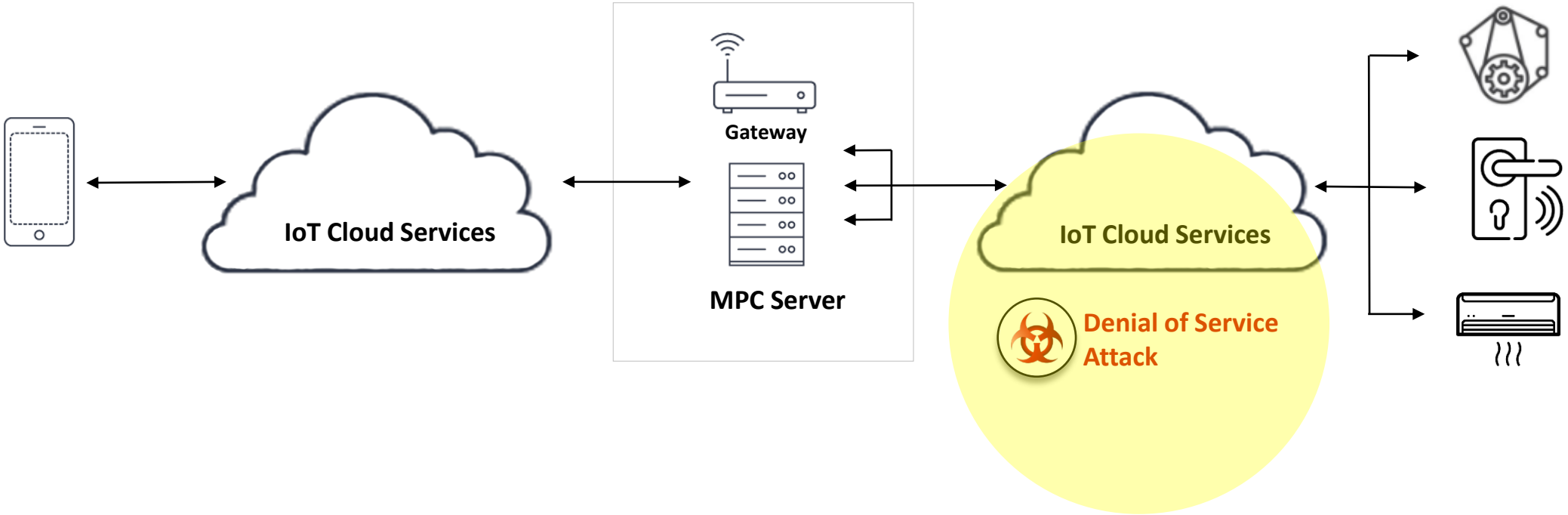
Threat Model
Side-Channel Attack

UNBOUND



- Side-channel Attacks work by obtaining measurements from multiple operations using the same key (timing information, power consumption, electromagnetic leaks or even sound).
- The device holds a random share of the key and not the entire key.
- A sharing refresh takes place at every operation.

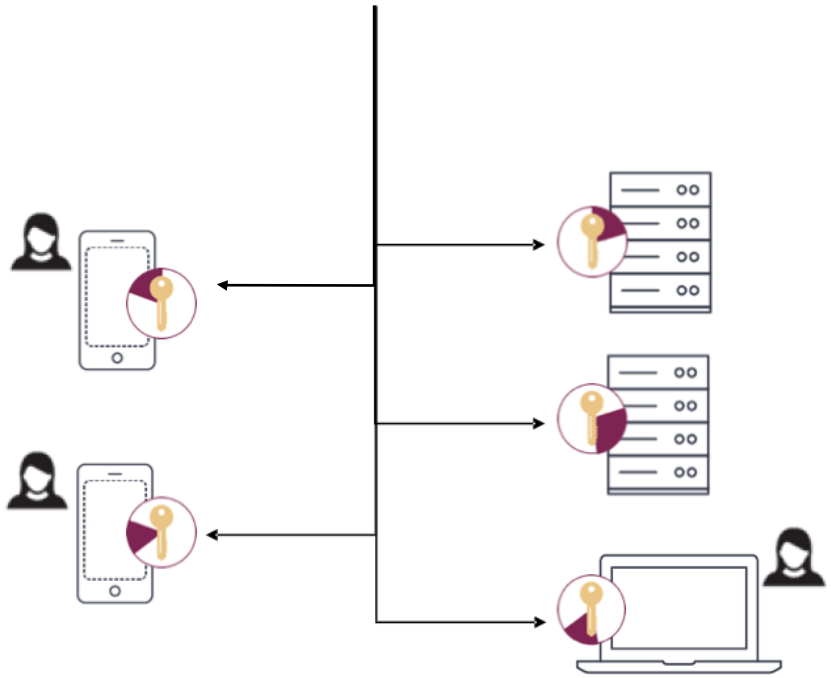
Threat Model
Denial of Service Attack



- The MPC solution requires a proof of work by any IoT device upon enrollment.
- The proof of work is slow, compared to the MPC verification that is very fast.

UNBOUND

MPC Based Authentication and Signing



Pure software approach

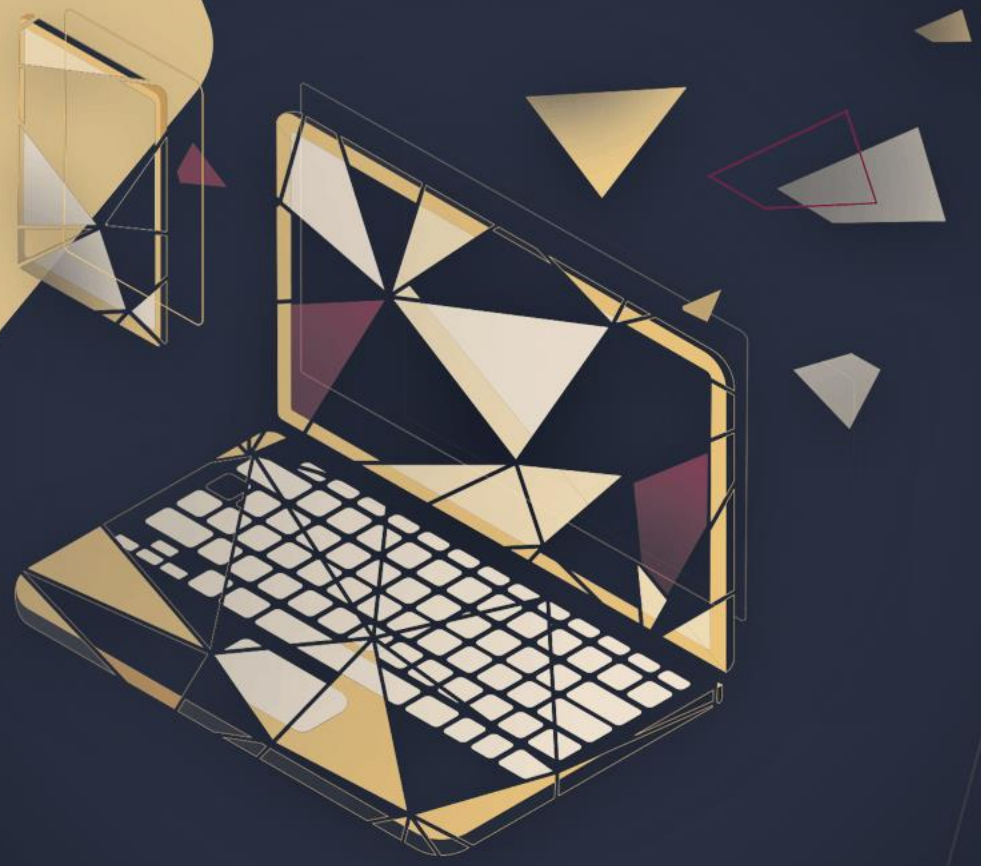
- Split the key into different random shares
- Place the random shares in different, highly segregated places (any hardware)
- Perform all cryptographic operations using key shares without ever bringing them together
- Shares are refreshed continuously

How does it work?

- MPC – sub-field of cryptography since 1980s
- Allows multiple machines to jointly compute a function while keeping their inputs private
- Security guarantee – mathematically proven
- Recent protocol optimizations enable commercial use

UNBOUND

Securing a Blockchain IoT Ecosystem with MPC



Rebecca Aspler
Director, Product Management