Cybersecurity Trends

Arnaud Taddei (WP3/17 Chair)

An “Outside-In” Cybersecurity story

- How is standardization impacted by outside world dynamics in cybersecurity?

- What are the trends in Cybersecurity?
- What is the cold reality?
- What can we do?
- Impact to the ITU?

+

- How to move from framework/requirements/architecture to implementable technical solutions?

Attackers don't stop … but we have a bigger problem

$45B Cost of Attacks in 2018
https://www.securitymagazine.com/articles/90493-cyber-attacks-cost-45-billion-in-2018
$100B Size of the Security market (Gartner)

Innovation don’t stop … but we have a bigger problem

Area of Security Innovation	Consideration
AI/ML vs Security and Privacy	It helps but it creates its own Attack Surface
Quantum (Quantum Computing, Q-Day, QKD, etc.)	An opportunity but will it be really secure?
Cyber Insurance vs Security	Selling security is hard, selling insurances is easier
Privacy, De-anonimisation and Security	A new cat of Schrödinger
Encryption and Security	No, Encryption != Security
Security by Design and Security	No, Security by Design doesn’t mean you are Secure

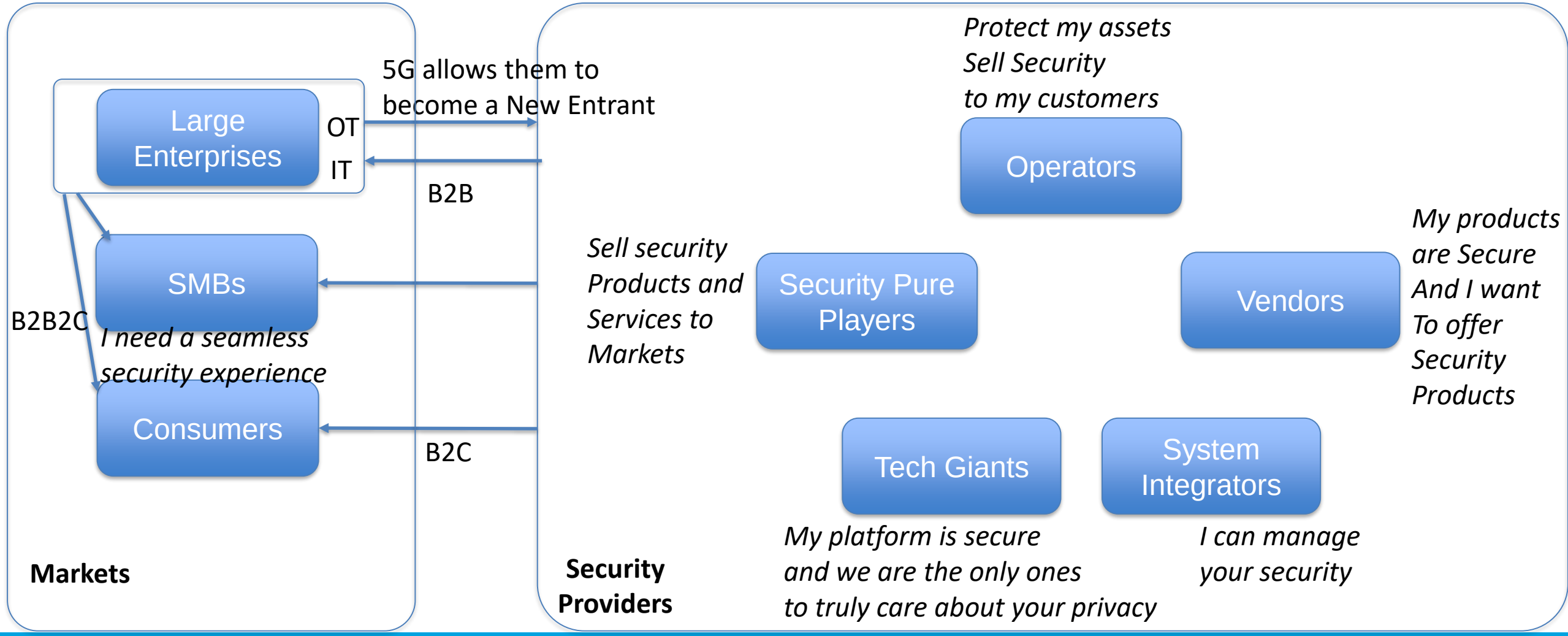
Note: we are not developing on those aspects in this presentation

Cybersecurity state of the union is a Babel Tower

Key industry players at cross

- Not the same understanding
- Very different models
- Some are in a deadly war

Cybersecurity Industry High Level View



People do not speak the same language either (e.g. Privacy)

Member States

Policy Setting
Regulation
Market Dominancy

Privacy means e.g. GDPR, etc.
Very sensitive
BUT: They don't like we discuss about it technically

Private Sector

Products
Services

Privacy means implement GDPR
Propose Products and Services
BUT: Private Sector abused Privacy
private Sector doesn't know how to restrict itself to 'PII' only
privacy is a much bigger pb and standards need to address it technically

Academia

Research
Innovation

Privacy is very young and requires a lot of work

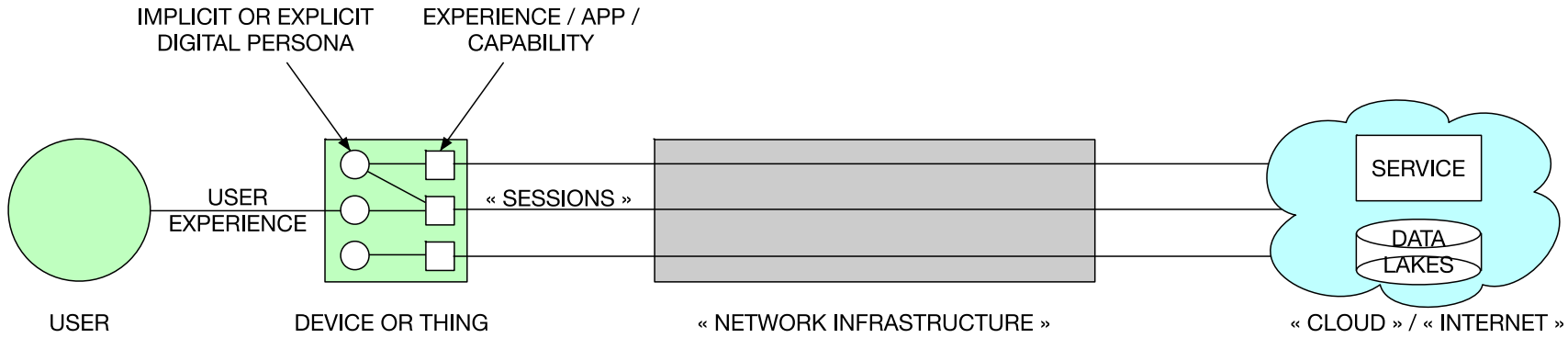
BUT: Theoretical foundation needs a lot of maturity

Civil Society

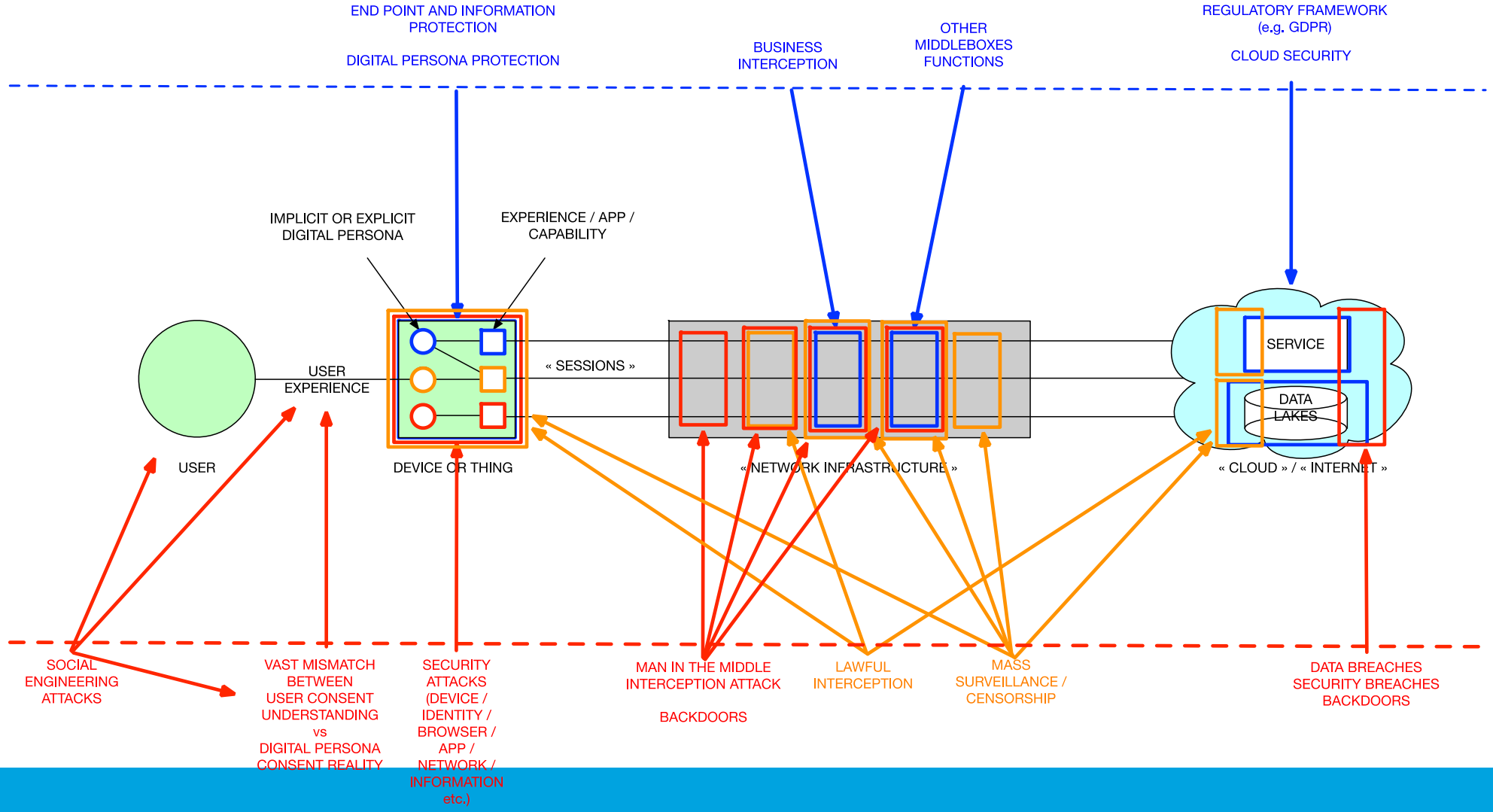
Human Rights
Societal issues

Privacy means rights
Very sensitive
BUT: Did they explain us their theory of Privacy?

A new « cat of Schrödinger »
Privacy hates security but needs it at the same time



Inspection and Interception landscape



The big disagreement: Where to put security?

A 2 WAY PROTOCOL MODEL

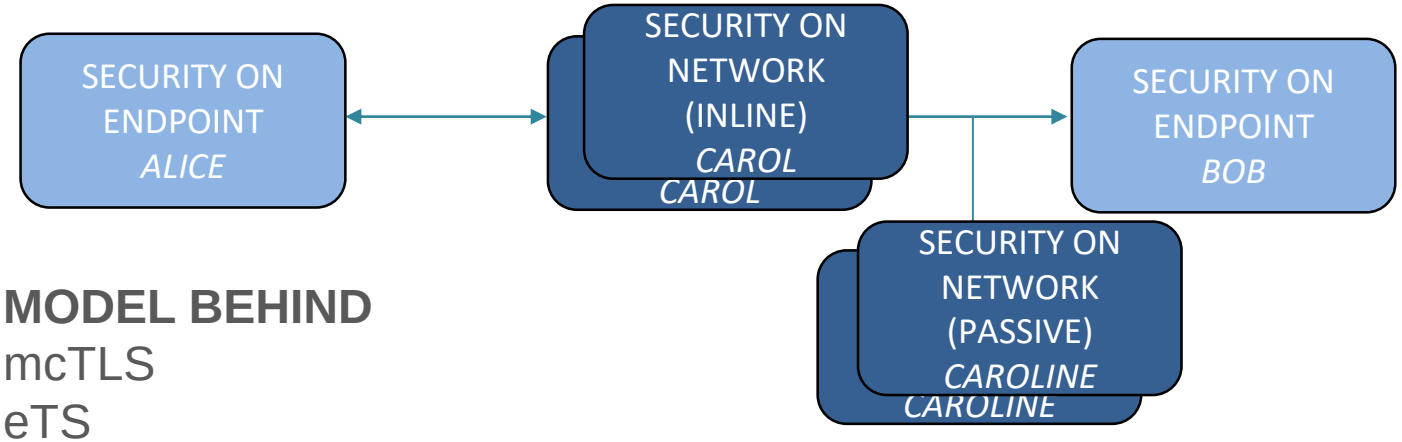
MODEL BEHIND

TLS 1.3
QUIC
DoH
DoT
ESNI
…

Leads to a MAJOR issue leading to

- Hyper Centralization
- Fragmentation of internet

A N WAY PROTOCOL MODEL



MODEL BEHIND

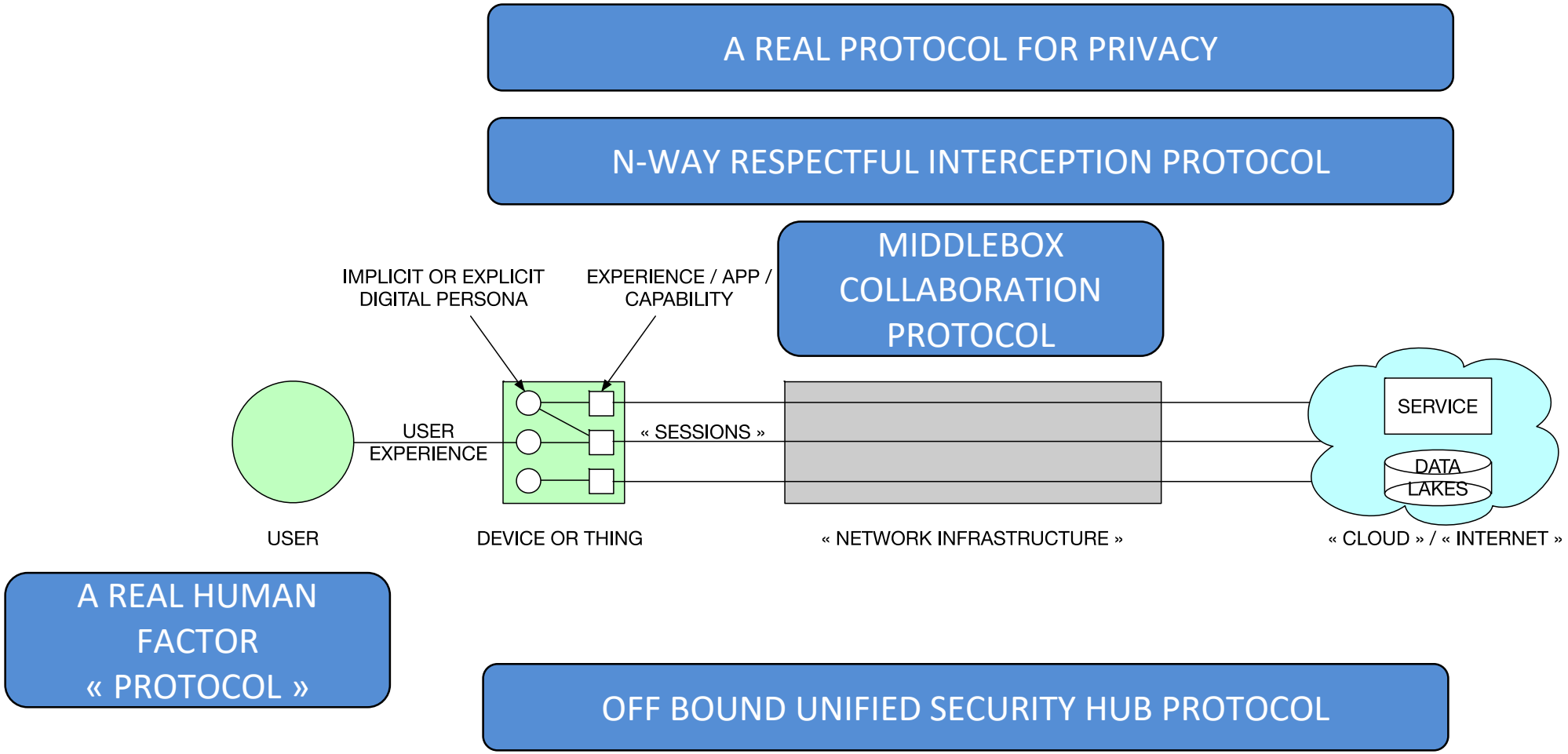
mcTLS
eTS
…

Leads to

- Capabilities and Limitations of Endpoint Security Solutions
- Middleboxes are not going away

!!!! I PUT NO COMMENTS ON PURPOSE !!!!

« Protocols » we miss and under which guarantees



The Frankenstein effect

With a fragmented industry

- We need to assemble a disparate set of unaligned constituencies
- With a choke point on resources and skills

Note: Our human immune system was not ‘patched’, constant long evolution

What is on our critical path

	HIGH LEVEL VIEW ON HOW THE SECURITY WORKS	WHAT IS THE NATURE OF EACH LAYER	WHAT IS THE KEY PROBLEM OF EACH LAYER
1	Security Management and Services	People delivering the service	Lack of people requires …
2	Playbooks to be applied on the overall architecture	Codified knowledge to remediate	… automated playbooks (gap) which relies on …
3	Security products and solutions	Security technology	… an overly complicated security stack which requires integration (gap) and simplification (gap) and …
4	Architecture (5G, IoT, Network, Cloud, etc.)	Assets	… has to work with an exploding attack surface which we need to reduce

The Service level problem

- We are missing 1.9m cyber security specialists
  - We will never fill that gap fast enough
- We are missing professionalization
  - How many vocational, licensed, certified jobs
- We are only at defining Cyber Defence Centers (SoC, CERT, etc.)
  - And we do it at ITU (X.framcdc)!
- Health sector has years of advances on us and it took them 50 years to get there!
- We need AI/ML (but it has its own problems) to automate more
- We need to simplify the stack ‘they’ need to manage
- We need to codify their knowledge

We need a way to better integrate this “Frankenstein”

- Integrated Cyber Defence
- Key features
  - A ‘Security Integration Bus’
  - Cyber Threat Intelligence sharing (OASIS STIX and TAXII)
  - Offer orchestration (OASIS OpenC2)
  - Standardized Security Data Schemas
- Huge benefits when ICD + Playbooks act together

ICD Framework

PRODUCTS products easily communicate with each other, with partners and 3rd parties, and with customers' own SOC tools.

SOC FRONT-ENDS  elastic servicenow splunk> IBM Radar MSS **API**

SOC CAPABILITIES

- DATA LAKES, SIEMS
- ORCHESTRATION
- THREAT INTELLIGENCE & ANALYTICS

EVENTS ACTIONS INTELLIGENCE

AMQP Advanced Message Queuing Protocol

STIX

TAXII

OpenC2

(ICDx) AT CUSTOMER OR HOSTED 

NORMALIZATION FILTERING ROUTING

MESSAGE PUBLISH/SUBSCRIBE

CONNECTORS PARSERS OPENC2 ADAPTORS

DATA HISTORY

WSS CASB EDR SWG SA MA EMAIL DLP DCS SEP 3rd Party Products

Scale demultiplies the attack surface

- How many virtual machines and containers to support 5G big use cases?
  - Mobile broadband, IoT, Low latency/High Reliability
  - 100 of millions? Billions?
  - How many of these will be security capabilities? 10%? 30%?
- Firstly, Zero Touch is not an option
  - Automation, AI/ML will be a key
  - But they increase the attack surface especially adversarial attacks on AI
    - Dataset poisoning, etc.
- Cloud platforms exhibit new attack surface patterns
  - Vast, gigantic east-west traffic
  - Reversal of flow from South-North (Controllers to Service) to North-South
    - Payloads will need to send status, logs, info for controlers, big data, lawful interecept
  - Attack surfaces ‘follow the path”: Gateway → Payloads → Controllers → Game Over

A key opportunity for security standardization and ITU

Standardization can help fill gaps:

- Give a much better foundation for industry growth
- Fix End to End approach
- Architecture refoundation
- Trust in a massive onboarding problem
- Simplify the technical stack
- Participate to the capacity building pb
- Coordinate better
- Incubate and nurture innovation

Potential considerations by ITU-T

- A fundamental revisit on how we ‘architect’ the interactions between SGs and FGs regarding security
  - and change the current “Security by Design” doctrine approach into a real integrated end to end approach
- SG17 with a new “Story” for End to End approach
- A lot of innovative approaches will put pressure on incubation mechanisms
- IF agreement on the above we need a real Architecture Advisory Board

Move away from ‘Security by Design’ only!

- Current Story obtained
  - After external consultation at a Tier 1 operator executive level
  - Developed by consensus of Correspondence Group CG-XSS

- **“SG17 should produce** coherent and high quality technical standards that are making sure that **end customers have trust in the Digital Service Providers (DSP) services that they receive and can be offered security value if they require** in a constantly evolving arms race with cyber adversaries. SG17 should create these standards in an efficient, effective process focused on the needs of the participants without gaps or overlaps between the work items”

Critical areas for SG17

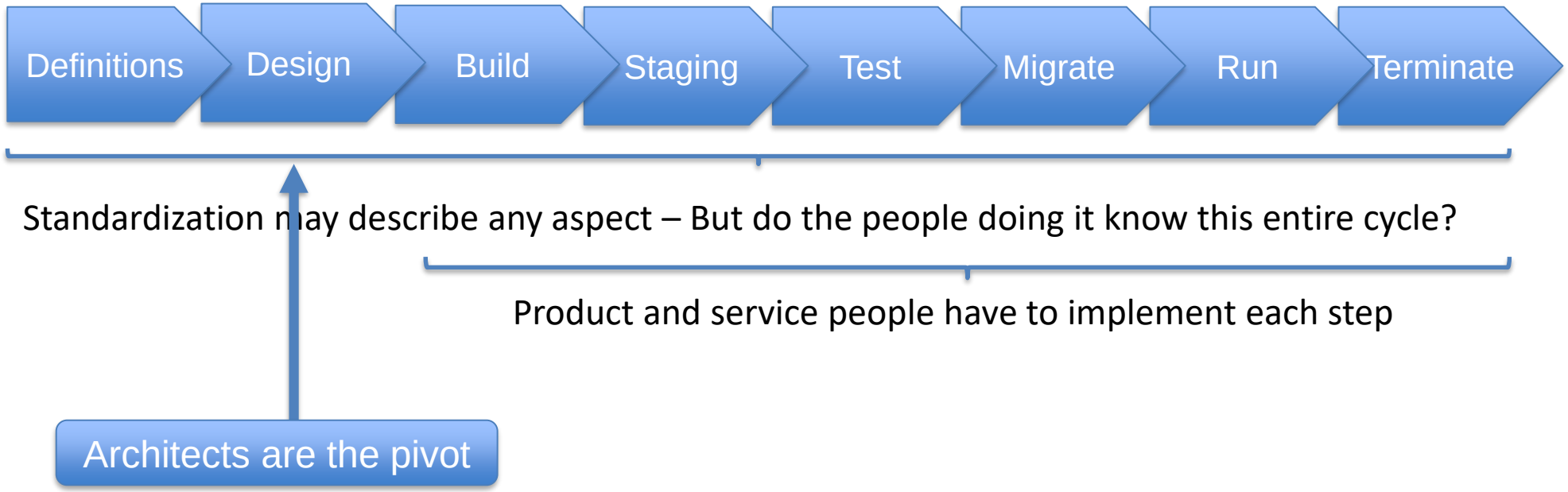
Change Focus

- Digital Service Providers → Customers
- Security by design → End to End view
- TRUST is an existential requirement
- Balance standards for everyone vs standards for premium organizations
- Face the massive onboarding problem
- Keep up with innovation
- …

How to move from Frameworks, Requirements, Architectures to implementable technical solutions?

- We have a method issue
- Too many researchers
- Not enough product architects
- No Shared Vision at architecture level
- Lack harmonization and composability
- Need to improve quality

Some reminders



Domain Knowledge
- Architecture patterns
- Standards (Frameworks, etc.)

Consciously or unconsciously
- Anthropology
- Ethics
- Law
- Technology

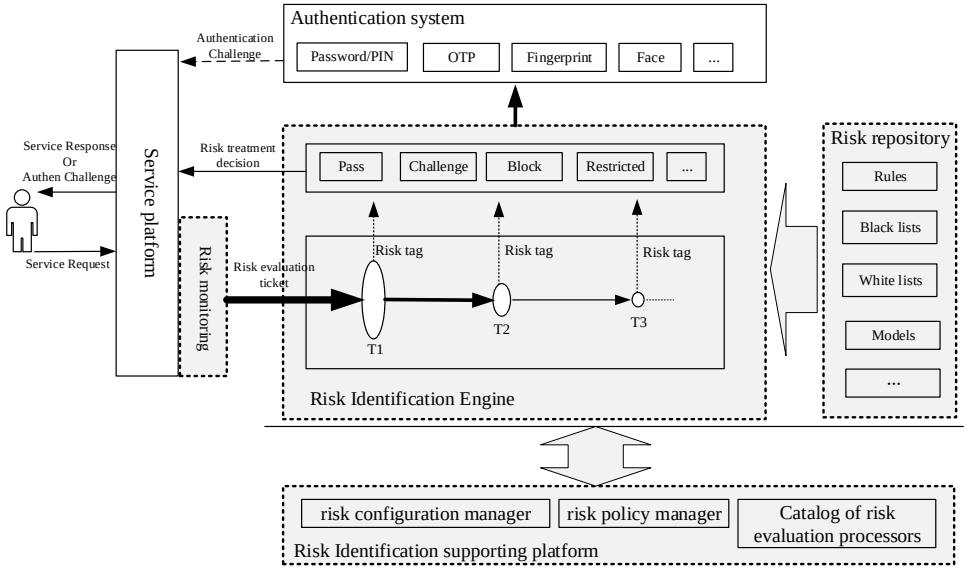
Knowledge on the downstream side
- Design criteria (stability, security, flexibility, manageability, integratability, migratability,sustainability (long term skills, energy saving, etc.))
- Development, System, Operational knowledge

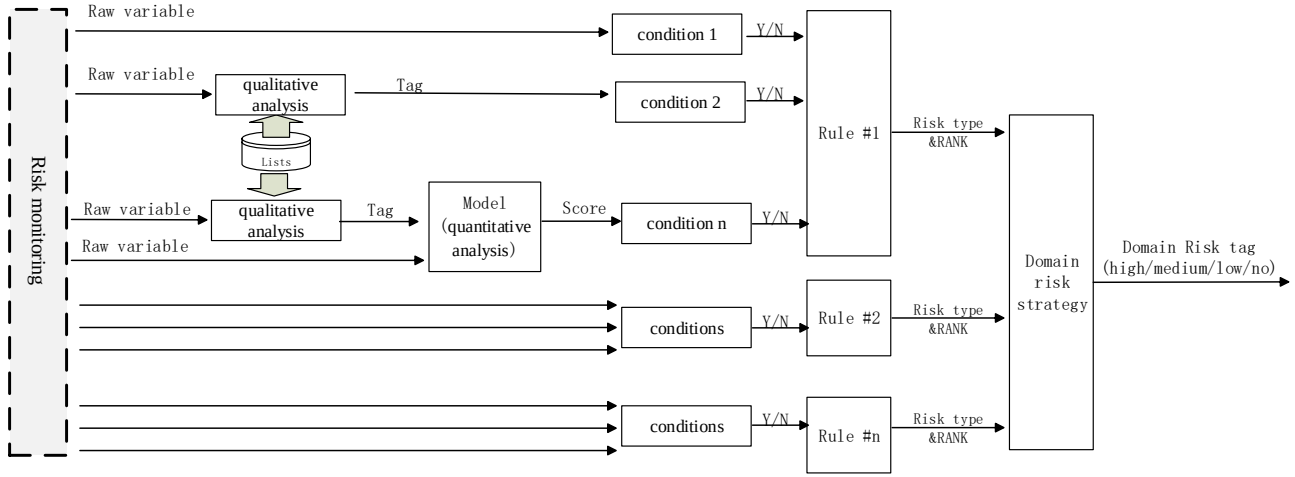
The composition problem

- In mathematics
  - Consider 2 functions g and f
  - If you consider their composites f1 and f2, f1 = g o h and f2 = f o g
  - Then in the general case f1 != f2
- Composition in Architecture is essential and a problem in itself
  - How do I compose AI/ML with Orchestration
  - How do I compose Security with DLT: Security for DLT and DLT for Security
  - How do I compose Cloud with 5G, and 5G with Cloud and with Security and Privacy?
- How do we make ITU recommendations more composable?

What does implementable standards look like?

- Learn from SG15!
- Architects and Service people start to come back in SG17
  - NTT: X.framcdc: Framework for Cyber Defence Center
  - Alibaba Architects: X.tfrca: Technical framework of risk identification to enhance authentication
  - Tencent Architects: X.rfcstap: Reference framework for continuous protection of service access process
  - Symantec: X.icsschemas: Data Schemas for Integrated Cyber Defence Solutions





Some conditions needed

- We need a foundation
  - Symantec: TP.secarch: Implications and further considerations of security architecture patterns
  - Symantec: TP.archdesign: Design Principles and Best Practices for Security. Architectures
- We need a real expertise center model
  - Proposition for an Architecture Advisory Board at TSAG RG-SS
  - Goal to harmonise, compose, identify gaps and generate suggestions for contributions
- We need a good PR!
- We need to check with the users of the recommendations in detail

Questions for GSLA

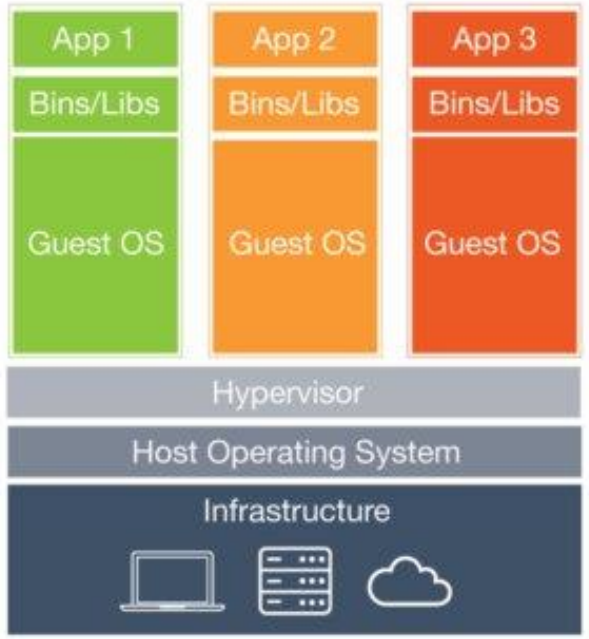
- What is the right ‘story’ (shared vision) for security in ITU-T?
  - Do we accept change and transformation?
  - With a good new ‘story’ can we attract more architects in existing and new sector members?
- Do we recognize our deepest architecture issues?
  - And a chance to fundamentally recreate a foundation for the future?
- What is the right structure for security in ITU-T?

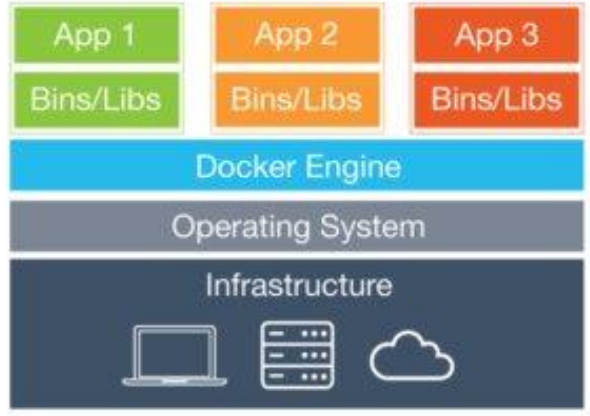
Thank You

- Any Questions or Feedback?

Example: Moving to serverless architectures with containers

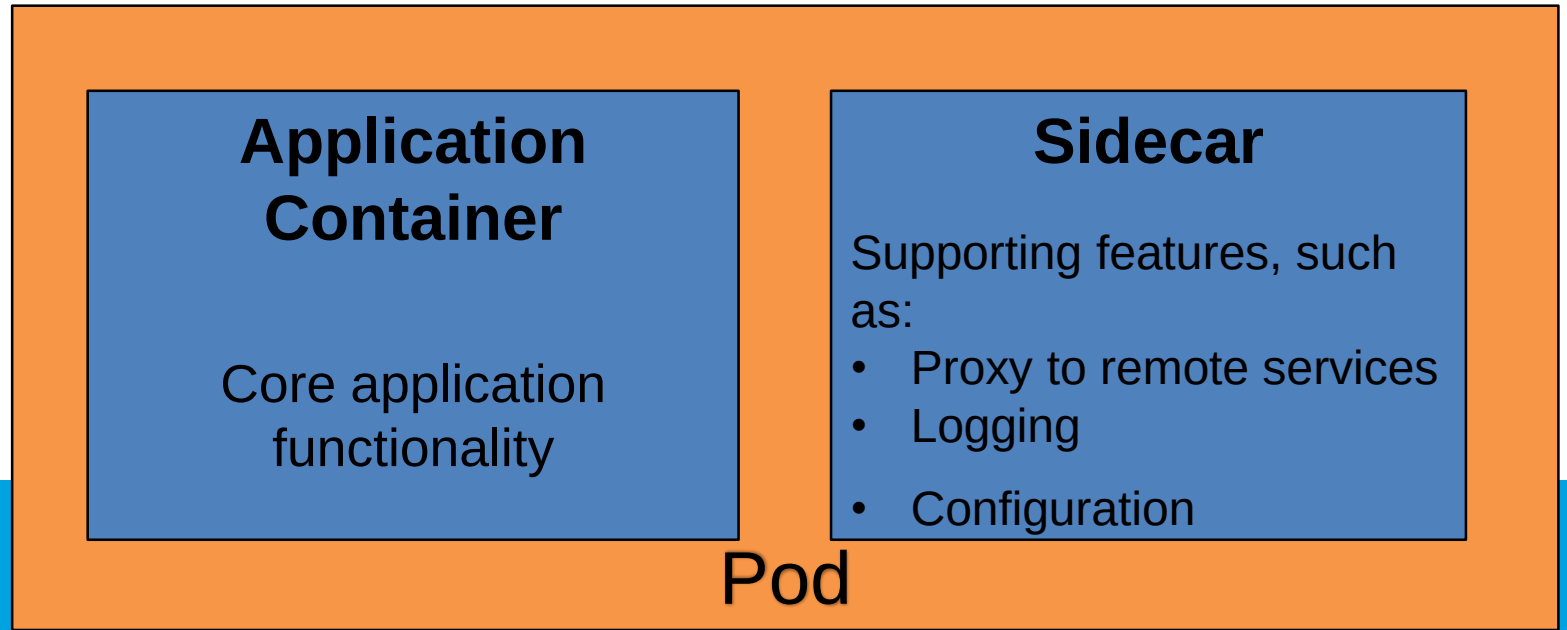
- Unix world
  - BSD Jails (2000)
  - Solaris Zones (2004)
  - IBM AIX Workload Partitions (2007)
- Linux Containers / LXC (2008)
  - Cgroups – CPU/mem limits
  - Namespaces
    User ID, Process ID, Network, IPC, Mount, UTC (hostname)
  - Chroots
  - Linux Security Modules (LSM)
- Docker (2013)
  - API & CLI tools
  - Container Images





If containers win: how can you bring security?

- Sidecar is a utility container in the Pod supporting the main container
- Same lifecycle as parent application
- Independent runtime environment and programming language
- Co-located on the same host
  - Access to same resources
  - Low latency
- Reusable



How to leverage the capabilities of THE ARCHITECTURE to link the Security by Design to Security Orchestration?

- External process that acts as a proxy between your application and external services
- Offloading common client connectivity tasks such as monitoring, logging, routing, security, and resiliency patterns in a language agnostic way