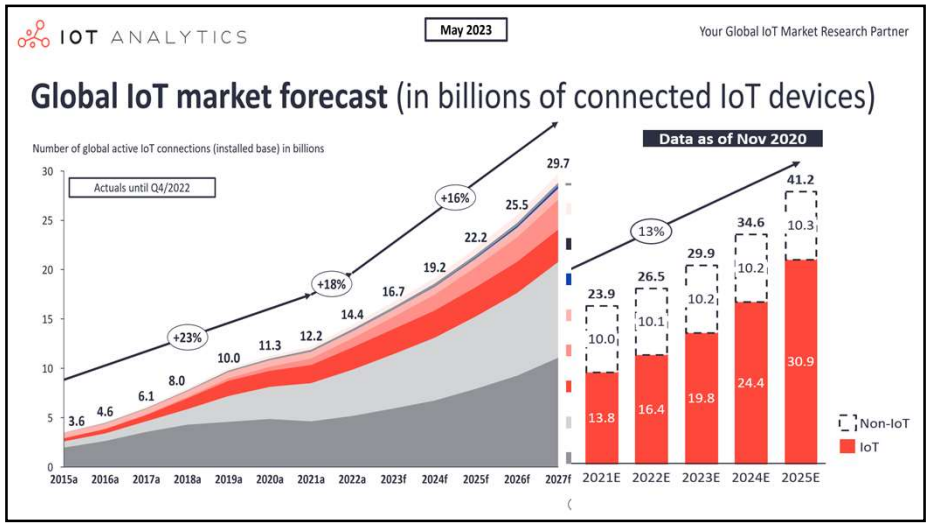

1

## Outline

- Zero Trust (Architecture)
- Trust in computers
- Trust in supply chains



2




3

"The cloud is someone else's computer"

Safe Harbor (2015)

Privacy Shield (2020)

EU-U.S. Data Privacy Framework (2025??)

4

## Paradigm shift (2000s)

Prevent → Detect → Respond → Recover

Prevent → Detect → Respond → Recover

5

## Continuous monitoring and analysis of all humans and devices


6

## IT environment

Walled fortress

- closed doors, physical isolation
- security as protection
- defend data, networks and systems

Open metropolis

- open, unbounded, interconnected
- trust as an enabler
- share content and resources
- protect data

Zero trust access/architecture
[Stephen Paul March, 1994]
[US DOD, Black Core, 200x]
[Jericho Forum, 2003]
[BeyondCorp, 2009]
[Kindervag, 2010]

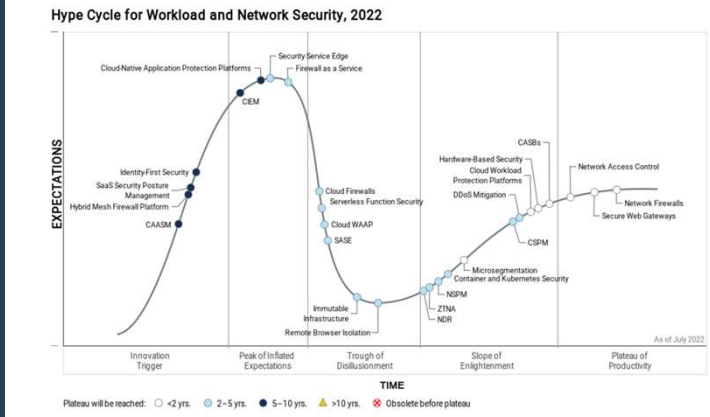
Explicit granting of trust
Continuous evaluation
Least privilege

Feudal system

- impose central rules
- data for protection
- loss of control

7

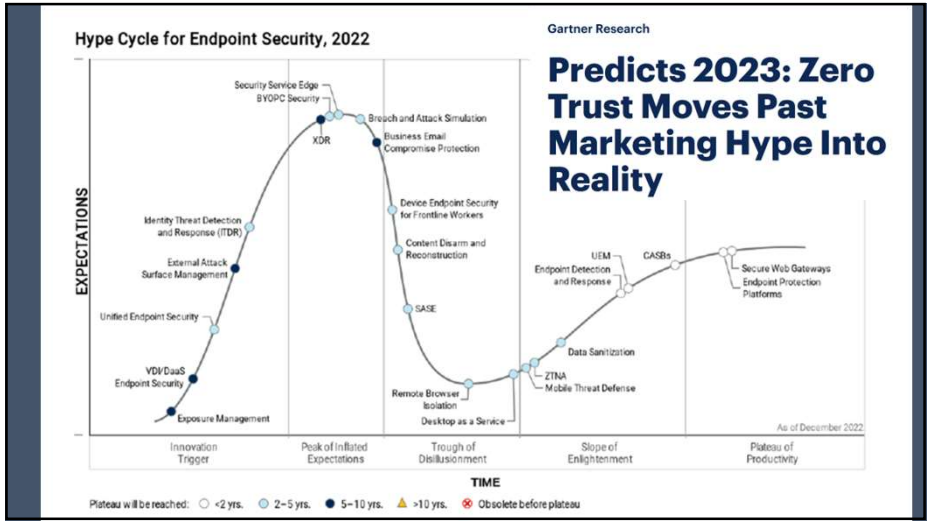
7




Source: Gartner (July 2022)

8

8




9

## What does the industry say?

- Google: application authentication, cloud security model [BeyondCorp]
- Cisco: zero trust networking
- Crowdstrike: identity threat protection
- Banks: Fraud detection based on contextual information

Rather vague concept around mediated access
network -> application -> VM -> data

Credit: Patrick Duvanel

10

10

## Some principles

- Continuous verification: never trust, always verify access, all the time, for all resources
- Limit the blast radius: minimize the impact if an internal or external breach occurs
  - Identity based segmentation
  - Least privilege
- Automate context collection and response: incorporate behavioral data and get context from the entire IT stack
  - User credentials, workloads, endpoints, ….

11

11

## Zero trust: Architectural concept across all layers

Recommended reading:

https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=930420

NIST Special Publication 800-207

**Zero Trust Architecture**

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

12

12

## Zero Trust: not a single architecture but a set of guiding principles for workflow, system design and operations

primarily focused on **data and service protection**

**enterprise assets** (devices, infrastructure components, applications, virtual and cloud components)

**subjects** (end users, applications and other non-human entities that request information from resources)

13

13

## NIST: Zero Trust Definition

cybersecurity paradigm focused on resource protection and the premise that trust is never granted implicitly but must be continually evaluated

- collection of concepts and ideas
- enforcing accurate, least privilege per-request access decisions in information systems and services
- network viewed as compromised

14

14

## NIST: Zero Trust Architecture Definition

end-to-end approach to enterprise resource and data security that encompasses identity (person and non-person entities), credentials, access management, operations, endpoints, hosting environments, and the interconnecting infrastructure

- enterprise's cybersecurity plan encompassing component relationships, workflow planning, and access policies
- includes network infrastructure (physical and virtual) and operational policies

15

15

## Zero Trust Principles

1. All data sources and computing services are considered resources
2. All communication is secured regardless of network location
3. Access to individual resources granted on a per-session basis
4. Access to resources is determined by dynamic policy including
   - the observable state of client identity, application/service, and the requesting asset
   - other behavioral and environmental attributes
5. Monitor and measure the integrity and security posture of all assets (owned and associated)
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed
7. Collect as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture

16

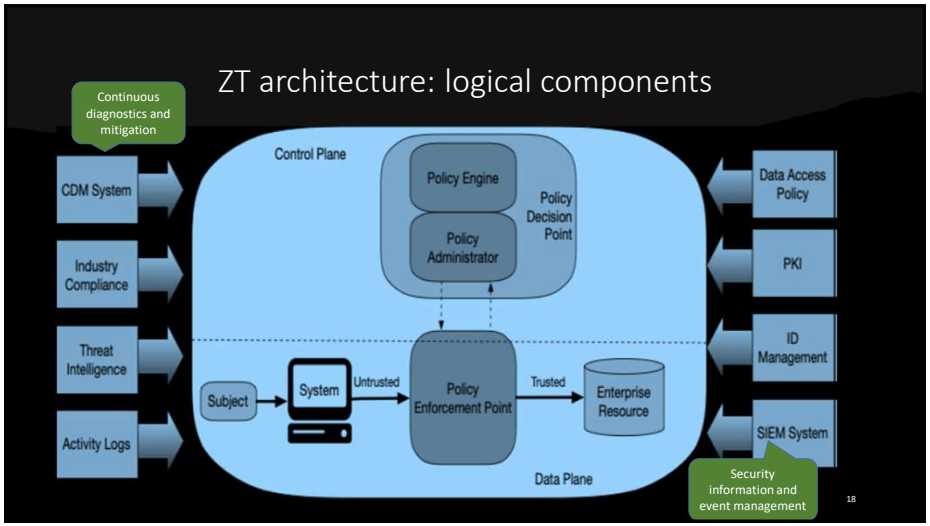
16

## ZT networks

1. The entire enterprise private network is not considered an implicit trust zone
2. Devices on the network may not be owned or configurable by the enterprise
3. No resource is inherently trusted
4. Not all enterprise resources are on enterprise-owned infrastructure
5. Remote enterprise subjects and assets cannot fully trust their local network connection
6. Assets and workflows moving between enterprise and non-enterprise infrastructure should have a consistent security policy and posture

17

17




18

## ZTA Approaches

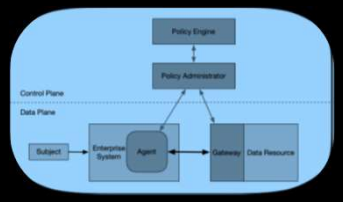
- Enhanced Identity Governance: resource portal model or cloud-based applications/services
  - Open network: risk of DDOS
- Micro-segmentation: gateway component act as PEP
  - Next generation firewall or host-based
- Network Infrastructure and Software Defined Perimeters:
  - overlay network
  - Software Defined Networking (SDN)
  - intent-based networking (IBN)

19

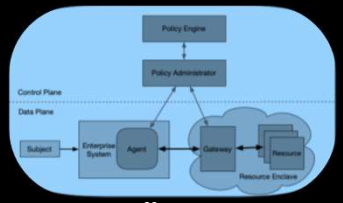
19

## ZTA Deployments (1+2/4)

- Device Agent/Gateway-Based
  - client-server implementation of the Cloud Security Alliance (CSA) Software Defined Perimeter (SDP)



- Enclave-based
  - legacy applications or on-premises data centers without individual gateways
  - cloud-based micro-services for a single business process

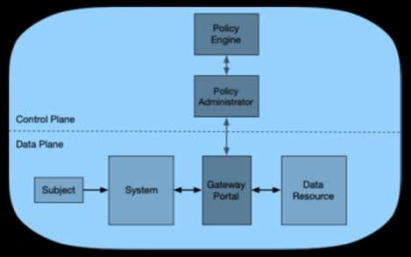


20

20

## ZTA Deployments (3/4): Resource portal model

- PEP is a single component that acts as a gateway for subject requests
  - No need to deploy agent on device
  - Less control over device
  - Less visibility
  - Risk for DOS

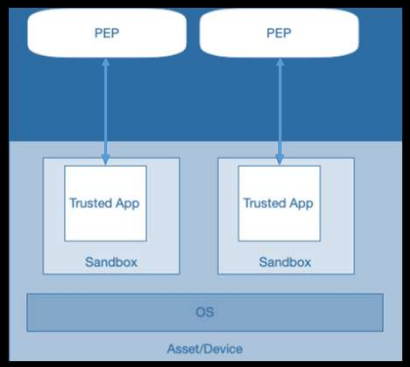



21

21

## ZTA Deployments (4/4): Device Application Sandboxing

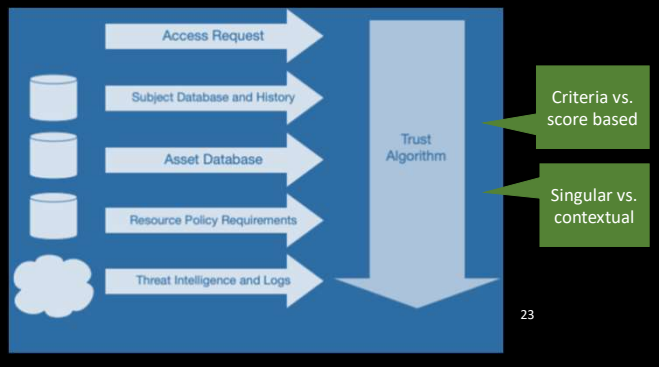
- Individual applications are segmented from the rest of the asset
- Less visibility into client assets
- Application needs to be secure




22

22

## Trust Algorithm: process used by the policy engine to ultimately grant or deny access to a resource




23

23

## ZT network requirements

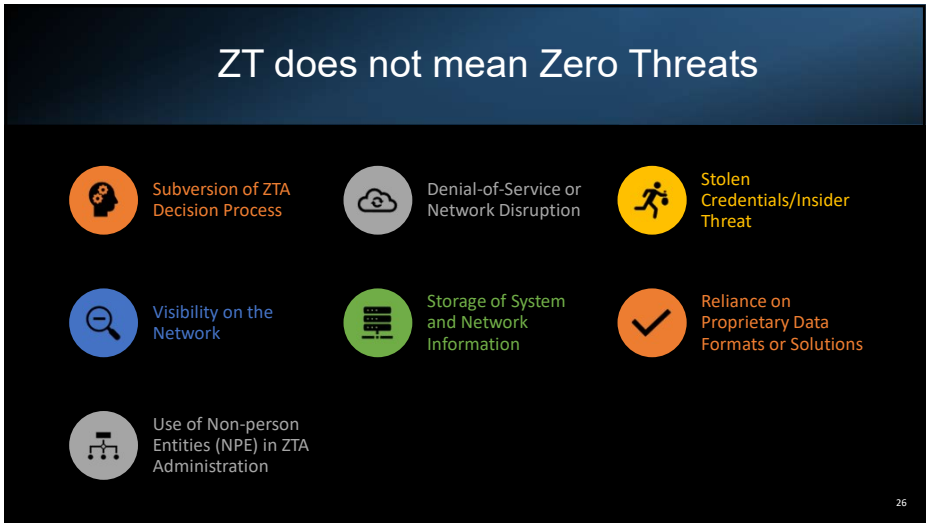
| | | | |
|---|---|---|---|
| Enterprise assets have basic network connectivity | Must be able to distinguish between what assets are owned or managed by the enterprise and the devices' current security posture | All network traffic can be observed | Enterprise resources should not be reachable without accessing a PEP (except e.g. DNS) |
| Data plane and control plane are logically separate | Enterprise assets can reach the PEP component | PEP is the only component that accesses the policy administrator as part of a business flow | Remote enterprise assets should be able to access enterprise resources without needing to traverse enterprise network infrastructure first |
| | The infrastructure used to support the ZTA access decision process should be made scalable | Enterprise assets may not be able to reach certain PEPs due to policy or observable factors | |

24

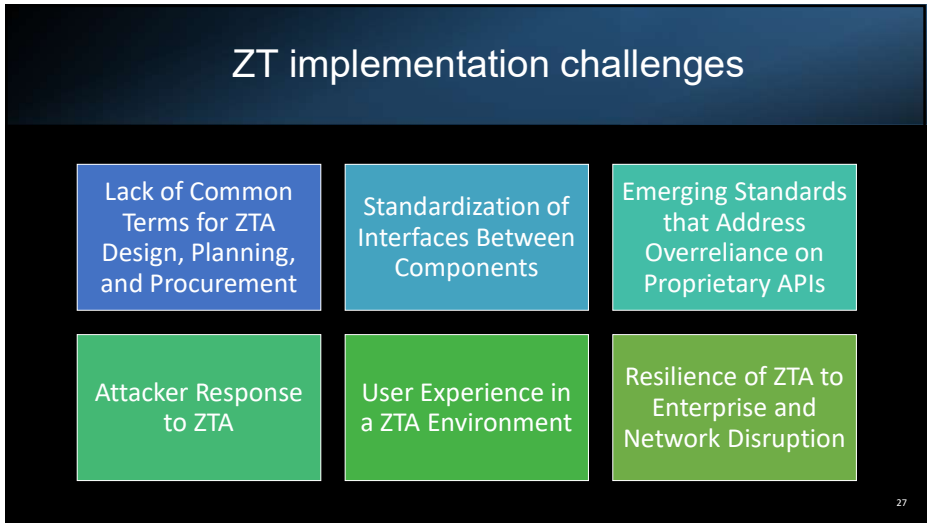
24


ZT deployment scenarios
Enterprise with Satellite Facilities
Multi-cloud/Cloud-to-Cloud Enterprise
Enterprise with Contracted Services and/or Nonemployee Access
Collaboration Across Enterprise Boundaries
Enterprise with Public- or Customer-Facing Services
25

25


ZT does not mean Zero Threats
Subversion of ZTA Decision Process
Denial-of-Service or Network Disruption
Stolen Credentials/Insider Threat
Visibility on the Network
Storage of System and Network Information
Reliance on Proprietary Data Formats or Solutions
Use of Non-person Entities (NPE) in ZTA Administration
26

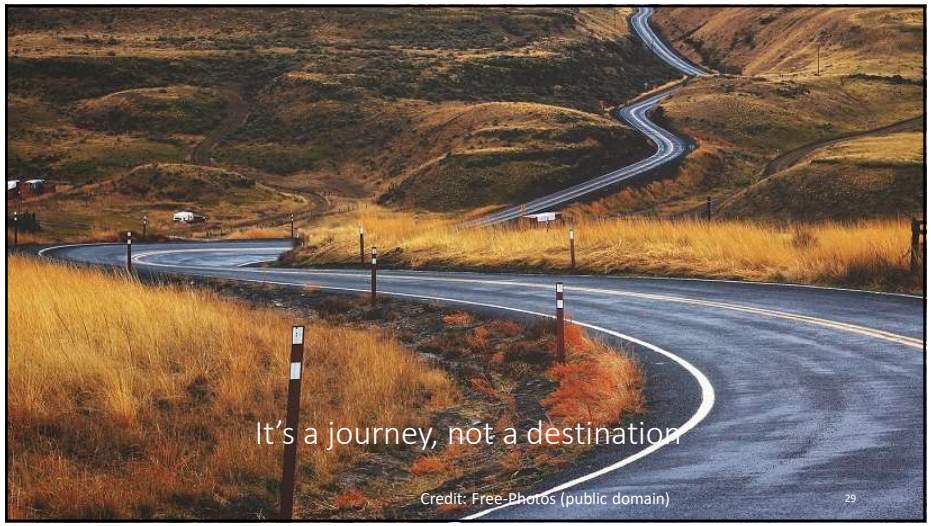
26


ZT implementation challenges
Lack of Common Terms for ZTA Design, Planning, and Procurement
Standardization of Interfaces Between Components
Emerging Standards that Address Overreliance on Proprietary APIs
Attacker Response to ZTA
User Experience in a ZTA Environment
Resilience of ZTA to Enterprise and Network Disruption
27

27


Gartner
Zero trust is top of mind for most organizations as a critical strategy to reduce risk in their environments, but very few organizations have completed the scope of their zero-trust implementations.
Zero trust addresses specific risks in the environment, such as restricting lateral movement on networks and limiting third party and insider threat damages, but not all risks are addressed by a zero-trust posture.
Moving from theory to practice with zero trust is challenging. It is easy to fall into the trap of deploying point zero-trust solutions without developing a strategy, resulting in failed zero-trust project attempts.
28

28




29

## Zero trust does not mean zero trust

**Need to trust**

| hardware | supplier | trust broker |
|---|---|---|
| software | CISO | CA |
| | sysadmin | SSO server |
| | | access proxy |

30

30

## What is a secure computer? (one you can fully trust)

- a computer placed in a basement with no windows and a well–protected door
- with no network connections
- locked up in a vault
- …and switched off

computer security: "the protection resulting from all measures to deny unauthorized access and exploitation of friendly computer systems"

L. M. Molho: Hardware Aspects of Secure Computing, International Workshop on Managing Requirements Knowledge, Atlantic City, NJ, USA, 1970, p. 135

31

31

## Software security

"it's turtles all the way down"

preacher Joseph Frederick Berg (1854):

My opponent's reasoning reminds me of the heathen, who, being asked on what the world stood, replied, "On a tortoise."

But on what does the tortoise stand? "On another tortoise."

With Mr. Barker, too, there are tortoises all the way down.

32

32

## Encrypted hard disk

33

33

## Smart cards

slow
inflexible
inexpensive


34

## Hardware Security Modules (HSMs)

high performance
programmable
expensive

HSM8-S 8000 Series Host Security Module: 25K$

35

## Trust: RFC 4949 (Internet Security Glossary)

- **Trust**: A feeling of certainty (sometimes based on inconclusive evidence) either (a) that the system will not fail or (b) that the system meets its specifications (i.e., that system does what it claims to do and does not perform unwanted functions).
- **Trusted system**: A system that operates as expected according to design and policy, doing what is required – despite environmental disruption, human user and operator errors, and attacks by hostile parties – and not doing other things.
- **Trustworthy system**: A system that not only is trusted, but also warrants that trust because the system's behavior can be validated in some convincing way, such as through formal analysis or code review.

36

## Trust definitions - revisited

- Trusted Computing Group (TCG) definition
  - "an entity can be **trusted** if it always behaves in the expected manner for the intended purpose."
- some people now regret the name ***Trusted Computing***
  - *Trustworthy Computing* or maybe *Trustable Computing* could be a better name, but it is too late to change

37

## Early History of Trusted Computing

| | |
|---|---|
| 1999 | Trusted Computing Platform Alliance (TCPA) founded by IBM, Intel, Compaq, Microsoft, HP |
| Feb. 2002 | Trusted Platform Module (TPM) 1.1b specification published |
| April 2003 | Trusted Computing Group (TCG) formed as successor for TCPA |
| Oct. 2003 | TPM 1.2 specification published |
| 2006 | 20+ million TPMs sold |
| Jan. 2007 | TPM supported by BitLocker drive encryption in Windows Vista |
| June 2007 | Mobile Trusted Module (MTM) 1.0 specification published |
| May 2009 | TPM 1.2 specification adopted as ISO/IEC 11889 standard |
| 2011 | 500+ million TPMs sold |
| Oct. 2012 | Improved TPM support in Windows 8 |
| March 2013 | TPM 2.0 library specification published |

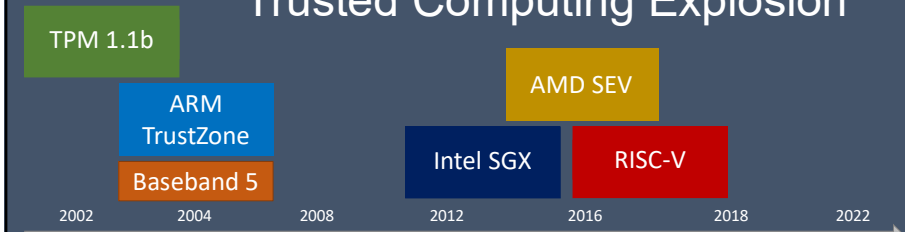
38


## Cryptographic Instructions

- 2009-2011: Intel/AMD add instructions for
  - AES
  - PCLMULQD – multiplication over finite field
- Authenticated encryption:
  - 2010: GCM mode at < 10 cycles/byte
  - 2022: AES OCB: 0.6 cycles/byte
  - 2022: AEGIS: 0.25 cycles/byte

39

## Trusted Computing Explosion



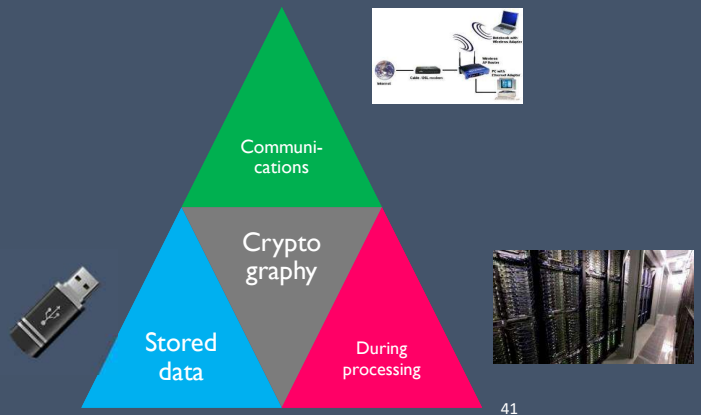

Aegis
Bastion
Sancus
Iso-X
SecureBlue++
TrustLite
SMART
TyTAN
Komodo
Sanctum
Sanctuary
TIMBER-V
OP-TEE
Keystone
MultiZone

Maene et al. 2018
Lee et al. 2020

40

40

## Changing role of cryptography




41

## Computing on Encrypted Data (COED)

Trusted Execution Environments

COED

Fully Homomorphic Encryption (FHE)

Multi-Party Computation (MPC)

Zero-Knowledge Proofs (ZK)

Statistics

Differential Privacy

Synthetic Data Generation

Federated Machine Learning

42


43

## Supply chain interception

(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A "load station" implants a beacon

44


45

## Solar Winds: SUNBURST (2020)

https://en.wikipedia.org/wiki/2020_United_States_federal_government_data_breach

- Pre March – December 2020
- 18000+ organizations worldwide
- Supply chain of Microsoft and SolarWinds + weaknesses in VMWare
- Likely Russia's Foreign Intelligence Services (SVR)

Defense, Labor, Energy, State, National Institutes of Health, Commerce, Homeland Security, Treasury, Agriculture, Justice

NATO, the U.K. government, the European Parliament, Microsoft, Cisco,…

46

46

How to achieve a trustworthy supply chain for software and hardware?

Very hard problem

More than technology

47

47

## Axiomatic Basis of Trust

**Accept without evidence**

Reputation of source
ISO cert.
People cert.

**Based on accountability**

Institutions
Processes

**Supply chain source selection**

Secret purchase
Random selection

48

48

## Analytic Basis of Trust

**Observation**

Testing (never exhaustive)

**Deductive**

Verification

Model checking

49

49

## Synthesized Basis of Trust: based on components and the way the are put together

**Smaller trusted computing base**

e.g. hypervisor

**Split device fabrication**

**Fault tolerant systems**

blockchains

secure MPC

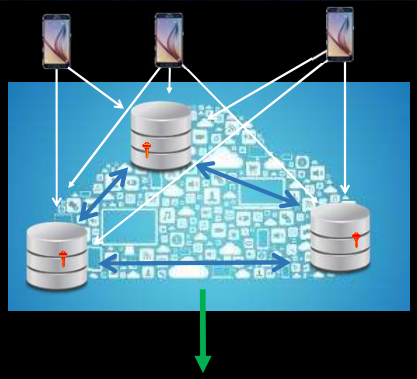
Secure composition

External monitor for catastrophic failures

50

50

## MPC (Multi-Party Computation)



+ secrets shared over multiple servers
+ moderate computation
- high communication overhead

Trust cryptographers
Trust implementers
Trust integrators
Trust your device to operate correctly
Trust your device to protect its data/keys

51

## Analytic Trust: Technical depends on complexity, application, access by vendor post deployment

| 01 | 02 | 03 | 04 | 05 |
|---|---|---|---|---|
| Testing | Isolation | Attestation | Distribution | Encryption |
| • Testing never exhaustive, e.g. VW | | | • Blockchain<br>• Secure MPC | • FHE |

Technical cost

Competition Issues

Transparency (to whom)

52

52

## Fully Homomorphic Encryption

+ single server
+ low communication
- high computation cost
- simple functions: basis statistics, neural networks

Trust cryptographers
Trust implementers
Trust integrators
Trust your device to operate correctly
Trust device that stores the decryption key

53

## Axiomatic Trust: Corporate Governance

implementation of technology requires people and processes

- Exists for accounting: GAAP (Generally Accepted Accounting Principles)
- ISO 27000, NIST cybersecurity framework: partial

| Design | Operations | Effective |
|---|---|---|
| • Based on business<br>• Takes into account industry practice + legal framework<br>• comprehensive<br>• …. | • Integrated with operational activity<br>• Auditable<br>• C-level commitment<br>• Workable<br>• …. | • Continuous improvement<br>• Internal and external audit<br>• Historical record<br>• …. |

54

54

## Axiomatic Trust: Nation-State Policy and Law

| Informal influence | Formal law |
|---|---|
| • Everything between compelled to and might please | • Interference with national influence: narrowly drawn and independent arbiter |

Transparency | Right to contest (in advance?) | Selective enforcement | Independent decision maker

55

55

## Towards a Framework to Evaluate Trust

Transparency | Accountability

Independent evaluation | Provable analytic verification rather than axiomatic non-verifiable approach

56

## Key questions

How does one build an artifact that is trustworthy?

How does one assess the trustworthiness of the artifact?

How does one decide to treat an artifact as trustworthy?

57

57

Avoid a single point of trust that is a single point of failure

Architecture is politics [Mitch Kapor'93]

58

58

## Open (source) solutions

Effective governance

Transparency for service providers

EU-FOSSA **EU Free and Open Source Software Auditing**

59

59

Conclusions

Zero trust does not mean zero trust

Trustworthy computing has non-technical dimension

Rethink architectures: distributed

Open technologies and review by open communities

60

60

## Bart Preneel

ADDRESS: Kasteelpark Arenberg 10, 3000 Leuven
WEBSITE: homes.esat.kuleuven.be/~preneel/
EMAIL: Bart.Preneel@esat.kuleuven.be
MASTODON: bpreneel@infosec.exchange
TWITTER: @bpreneel1
TELEPHONE: +32 16 321148

KU LEUVEN COSIC nextAuth

61

61

## Read more?


https://s3.documentcloud.org/documents/21831749/creating-a-framework-for-supply-chain-trust-in-hardware-and-software.pdf

62

62