NOKIA Bell Labs

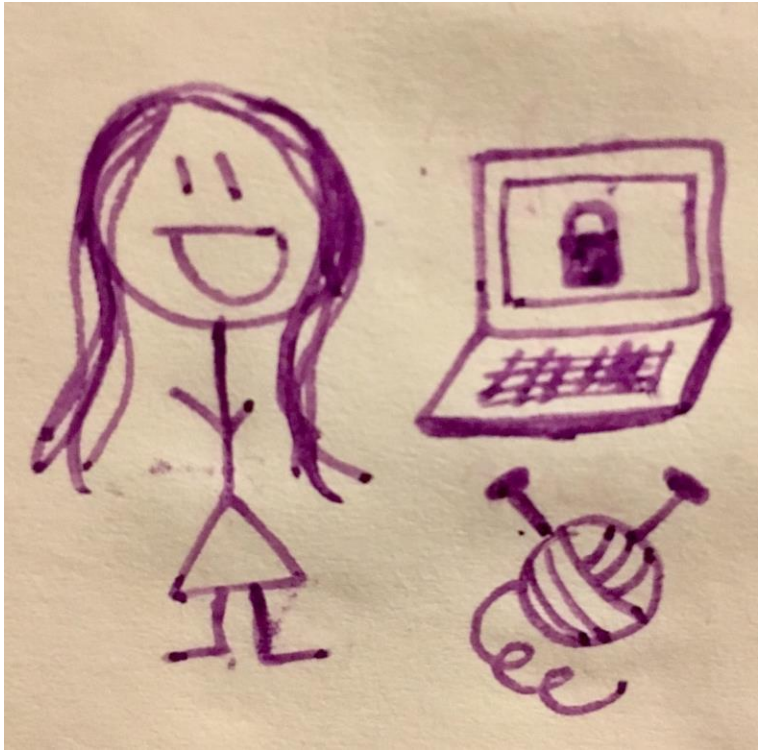
If you like it then you shoulda put a TPM on it

Gabriela Limonta

OWASP Meeting

03.09.2019

Me



Computer/Communications Engineer

~3 years working at Nokia

Researcher in the Cybersecurity Research Team at Nokia Bell Labs

Trusted Computing and Root Cause Analysis in Trusted Systems

I like knitting, running and calligraphy

(pretty bad at portraits, though ☹)

The Cloud

The Cloud
(for real this time)

The Cloud
(for real this time)

Hardware

The Cloud
(for real this time)

Firmware: BIOS/UEFI

Hardware

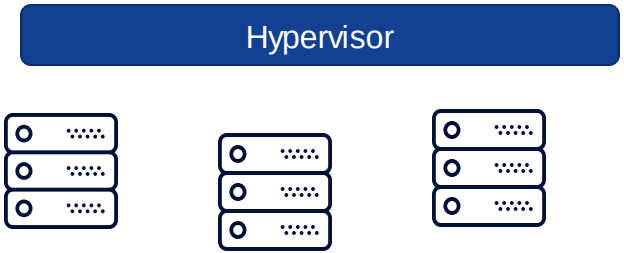
The Cloud
(for real this time)

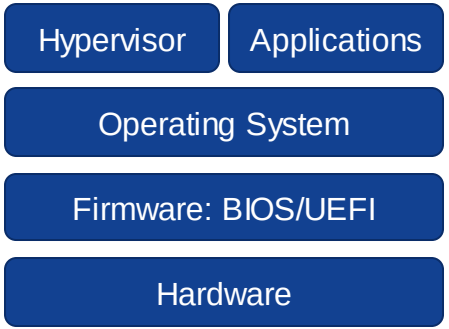
Operating System

Firmware: BIOS/UEFI

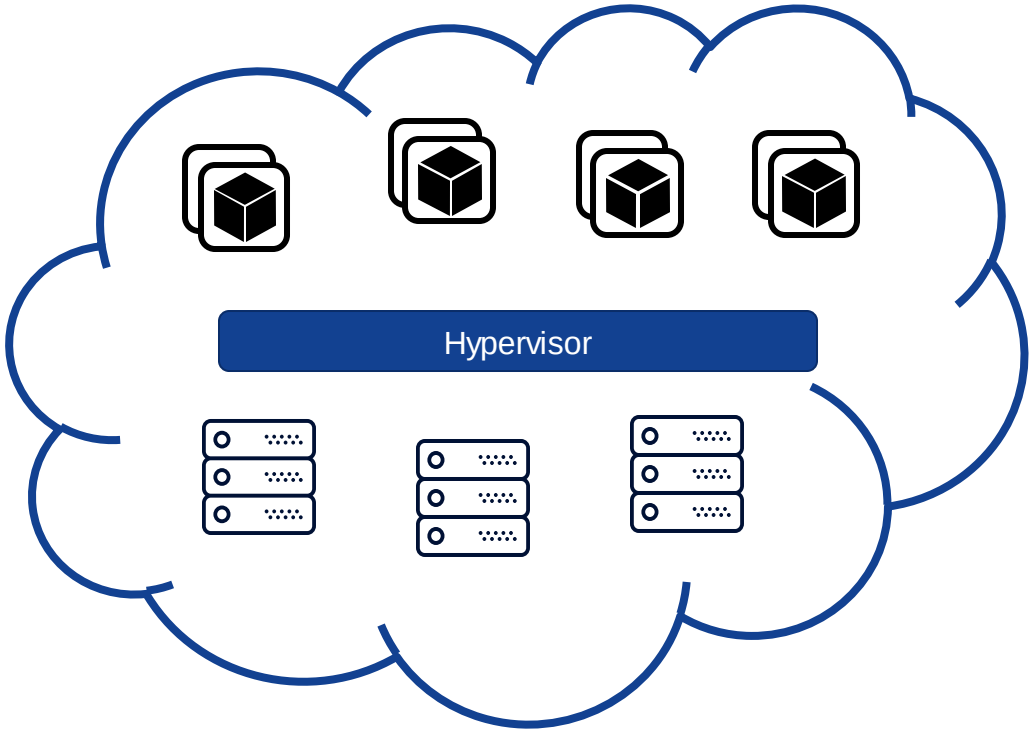
Hardware

The Cloud
(for real this time)





The Cloud
(for real this time)



Virtual Workload

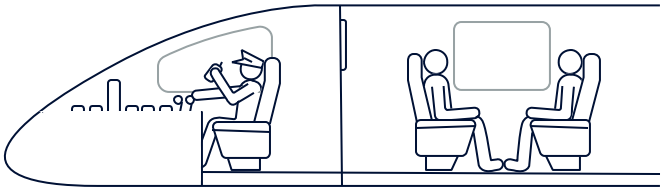
Hypervisor | Applications

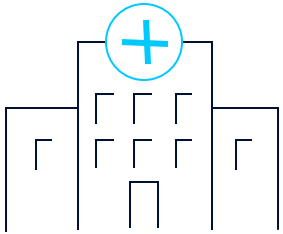
Operating System

Firmware: BIOS/UEFI

Hardware

Industries moving to the cloud





A problem:

A problem:

Do you trust your datacenter?

A problem:
Do you trust your datacenter?

TECH'S BOTTOM LINE

By Bill Snyder, InfoWorld | MAY 15, 2014

Snowden: The NSA planted backdoors in Cisco products

'No Place to Hide,' the new book by Glenn Greenwald, says the NSA eavesdrops on 20 billion communications a day -- and planted bugs in Cisco equipment headed overseas

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

NOKIA Bell Labs

A problem:
Do you trust your datacenter?

TECH'S BOTTOM LINE

By Bill Snyder, InfoWorld | MAY 15, 2014

Snowden: The NSA planted backdoors in Cisco products

'No Place to Hide,' the new book by Glenn Greenwald, says the NSA eavesdrops on 20 billion communications a day -- and planted bugs in Cisco equipment headed overseas

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

1,201 views | Aug 1, 2018, 04:58pm

Supply Chain Attacks Increase As Cybercriminals Focus On Exploiting Weak Links

Tony Bradley Contributor

I cover all things tech and the impact tech has on everyday life.

NOKIA Bell Labs

A problem:
Do you trust your datacenter?

TECH'S BOTTOM LINE

By Bill Snyder, InfoWorld | MAY 15, 2014

Snowden: The NSA planted backdoors in Cisco products

'No Place to Hide,' the new book by Glenn Greenwald, says the NSA eavesdrops on 20 billion communications a day -- and planted bugs in Cisco equipment headed overseas

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

1,201 views | Aug 1, 2018, 04:58pm

Supply Chain Attacks Increase As Cybercriminals Focus On Exploiting Weak Links

Tony Bradley Contributor

I cover all things tech and the impact tech has on everyday life.

ADDING IT UP —

If Supermicro boards were so bug-ridden, why would hackers ever need implants?

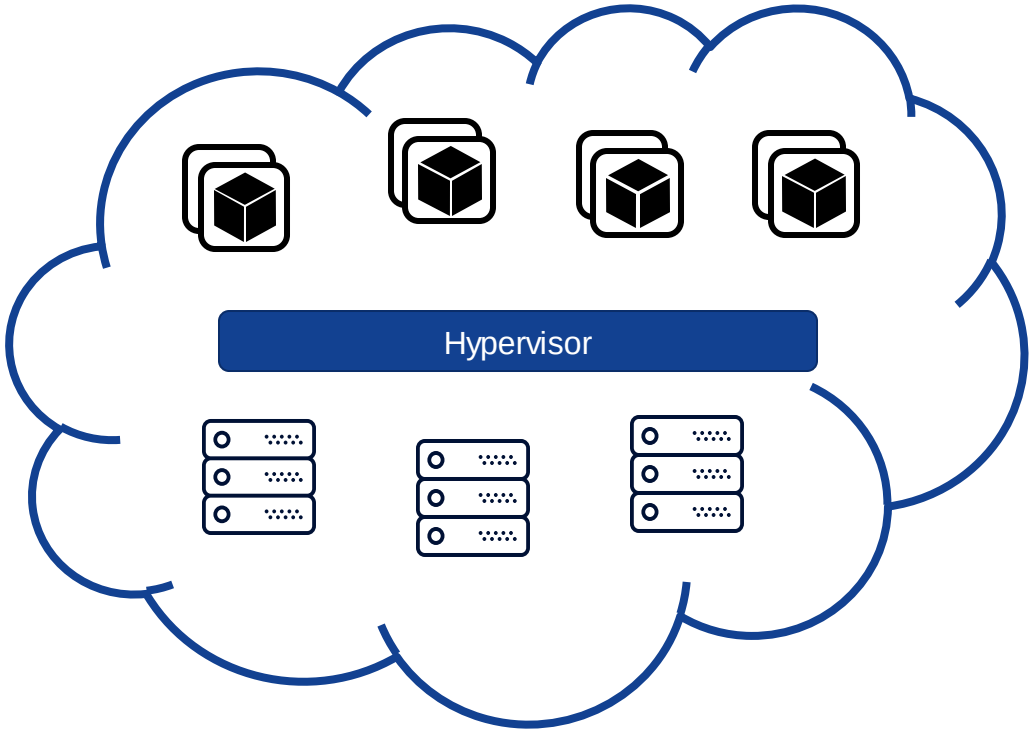
Whether spy chips reported by Bloomberg existed, attackers had much easier options.

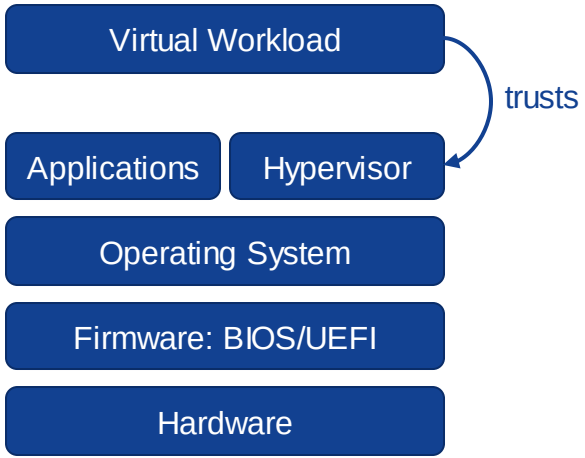
DAN GOODIN - 10/12/2018, 1:00 AM

NOKIA Bell Labs

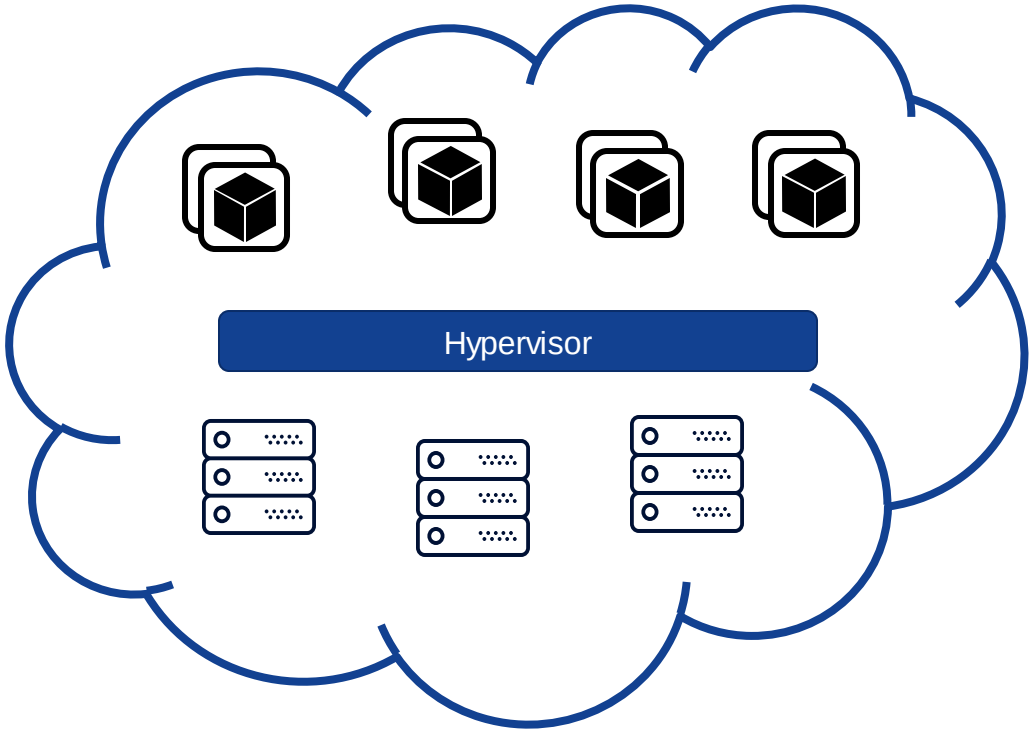
Trust = Identity + Integrity

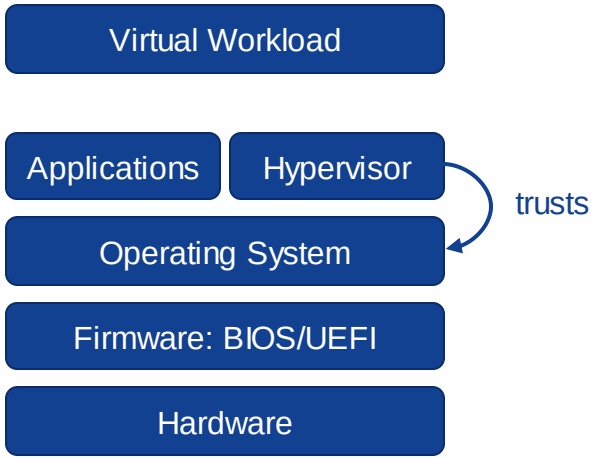
Chain of trust



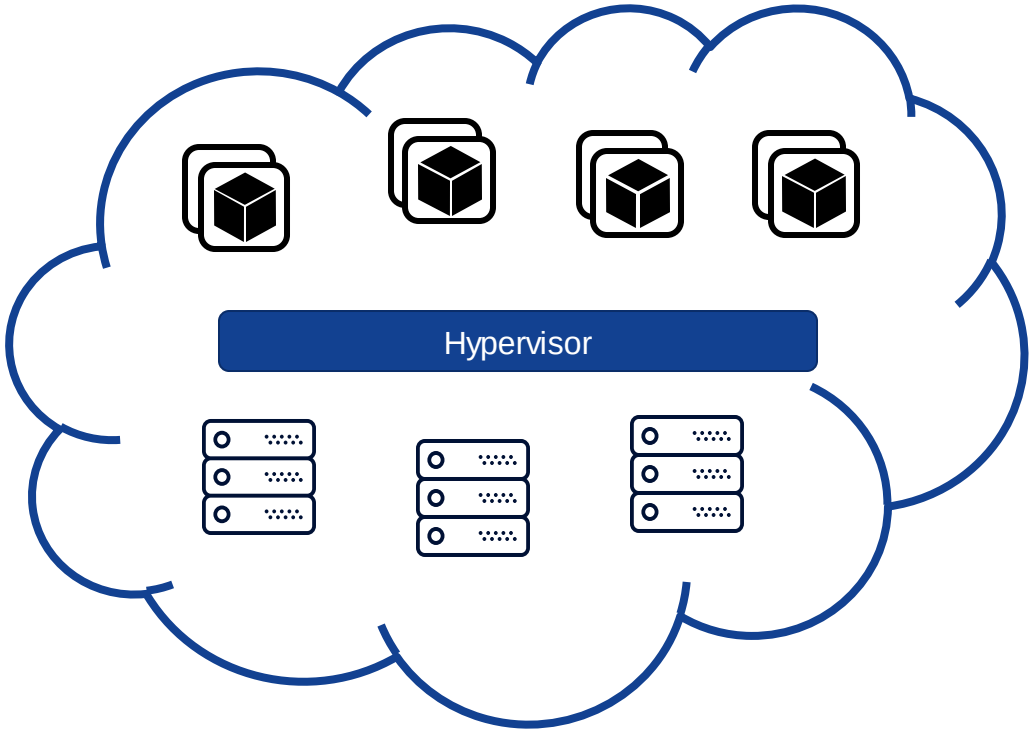


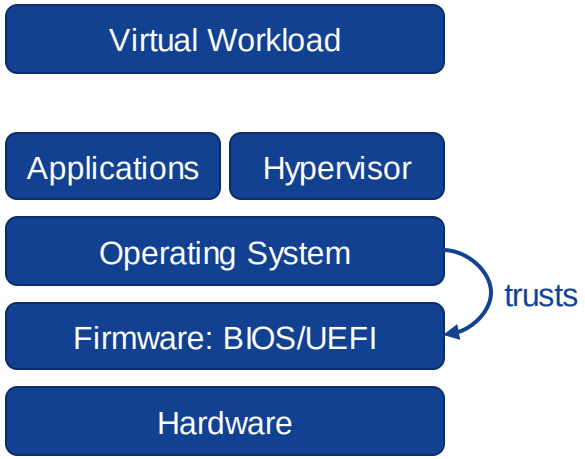
Chain of trust



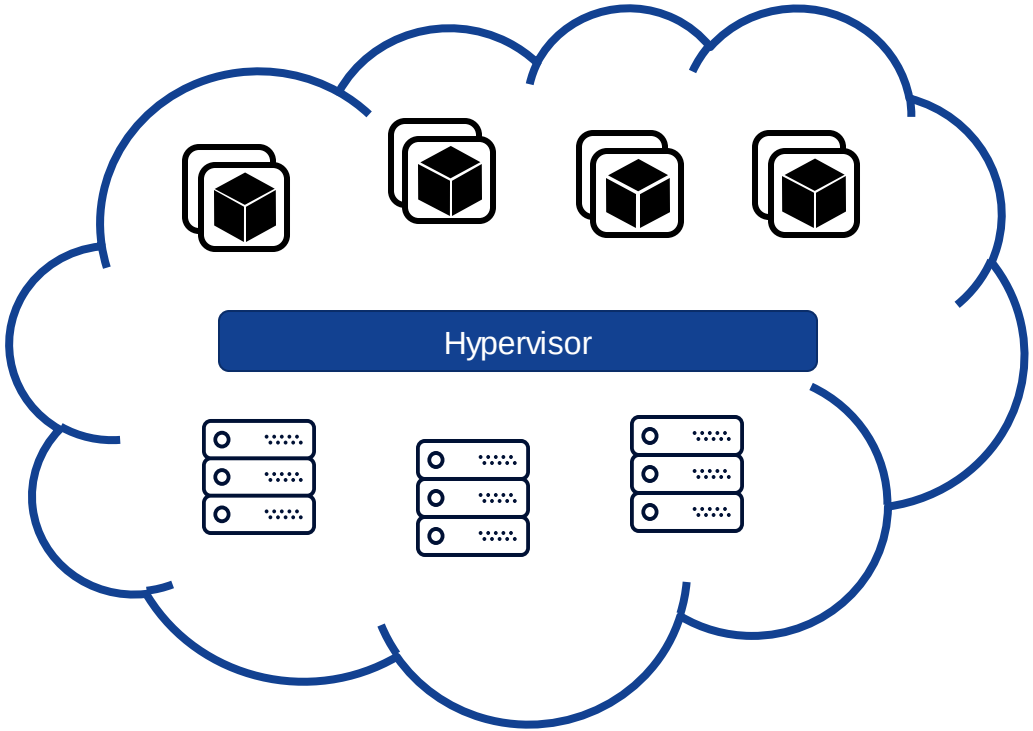


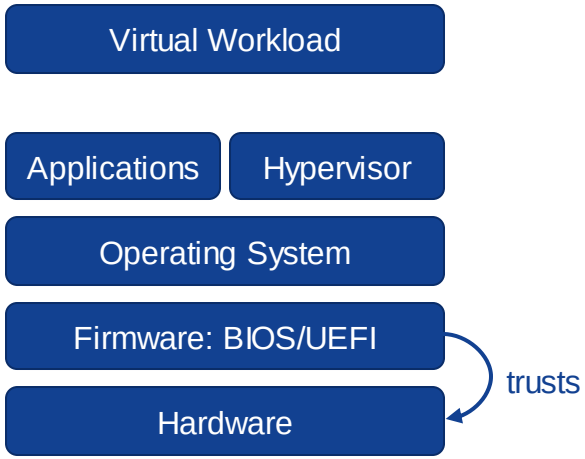
Chain of trust



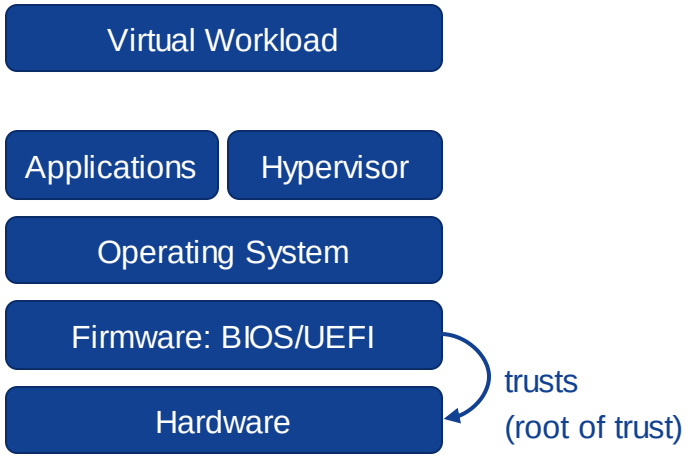


Chain of trust



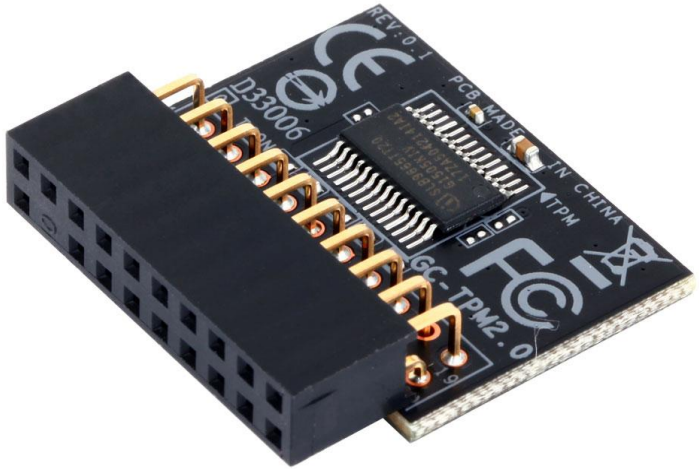


Chain of trust



1. Know what your hardware is running
2. Measure each component
3. Create a Merkle Tree of measurements (or some link...)
4. ...
5. Profit

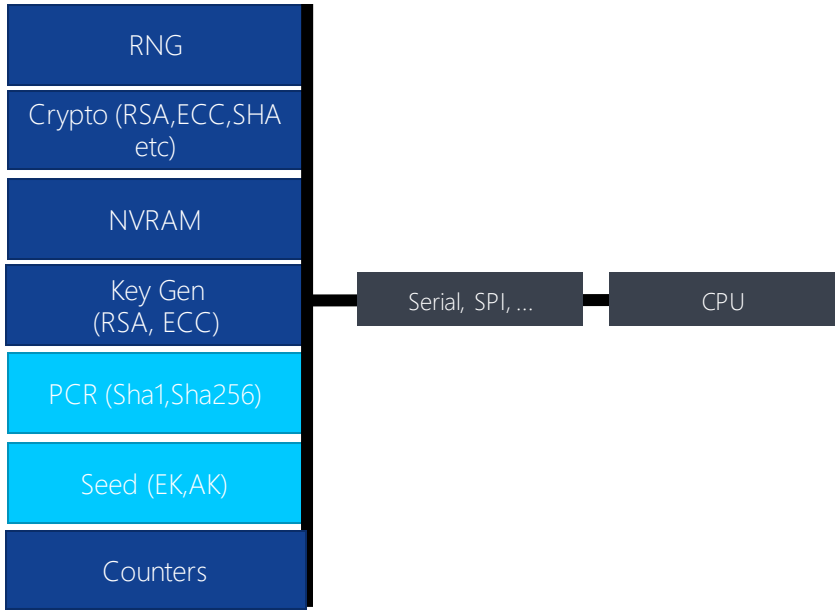
Big surprises, small packages



Trusted Platform Module
Tamper-resistant hardware

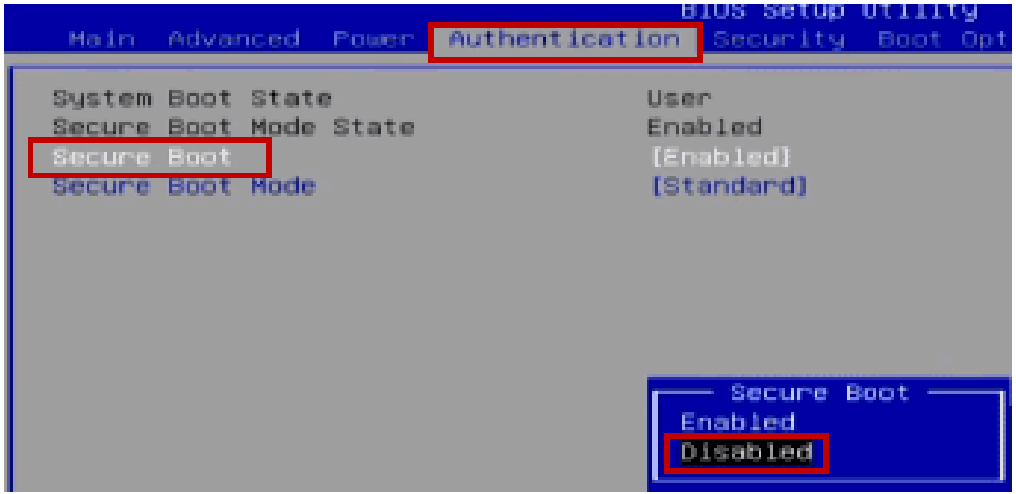
Trusted Platform Module

TPM 2.0

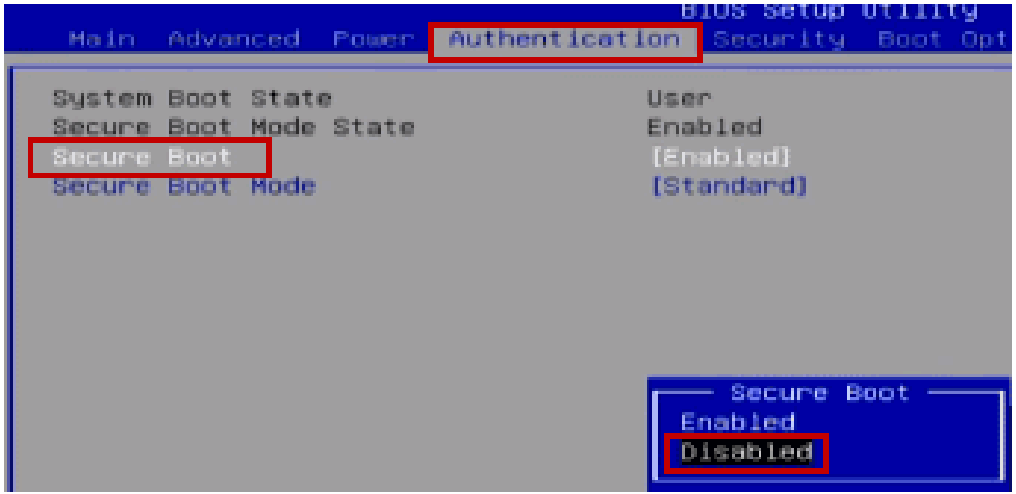


What this talk is **not** about

What this talk is **not** about



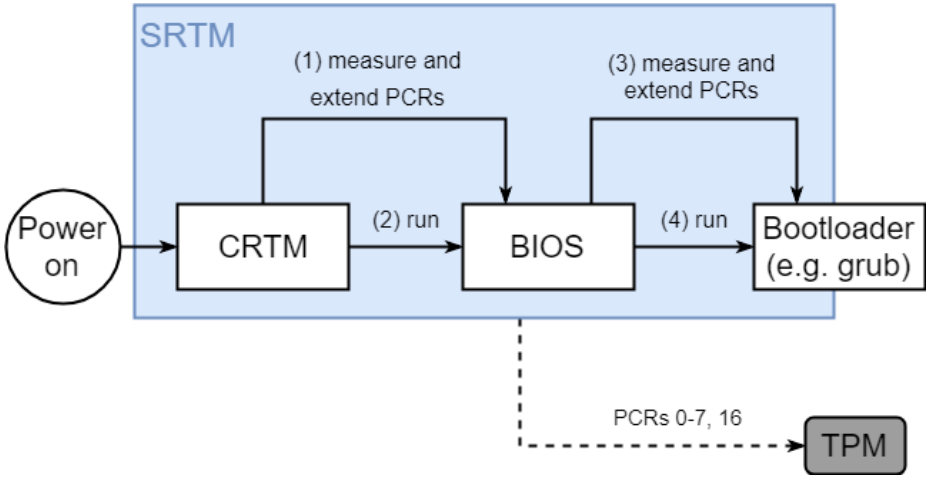
What this talk is **not** about



arm TRUSTZONE

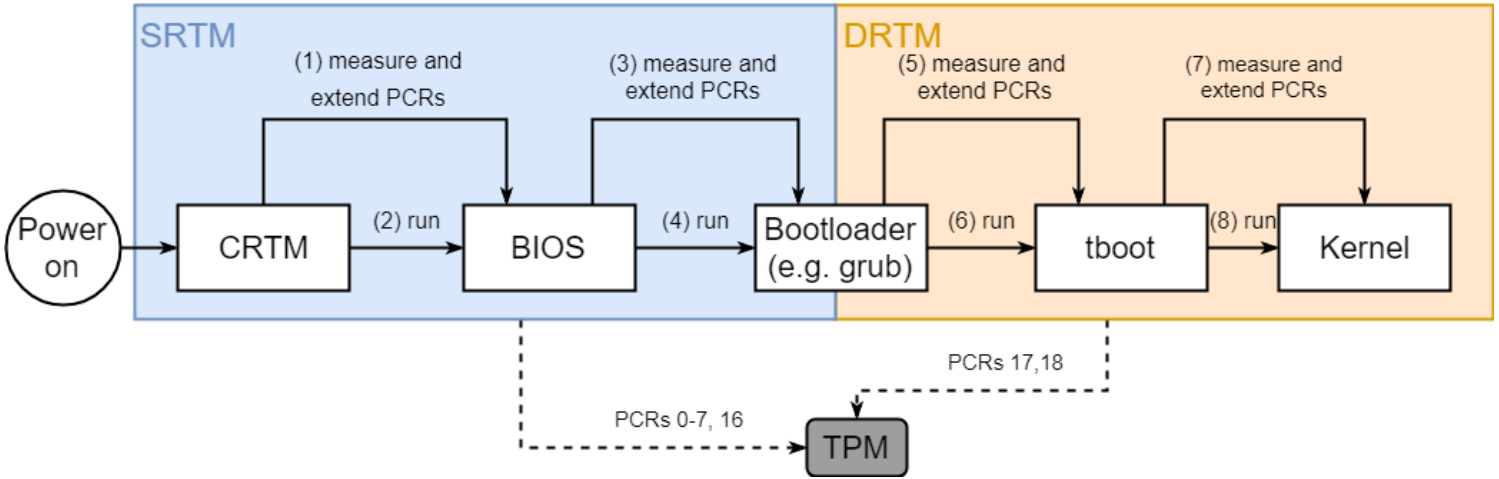
x86 boot process
(very simplified)

x86 boot process
(very simplified)



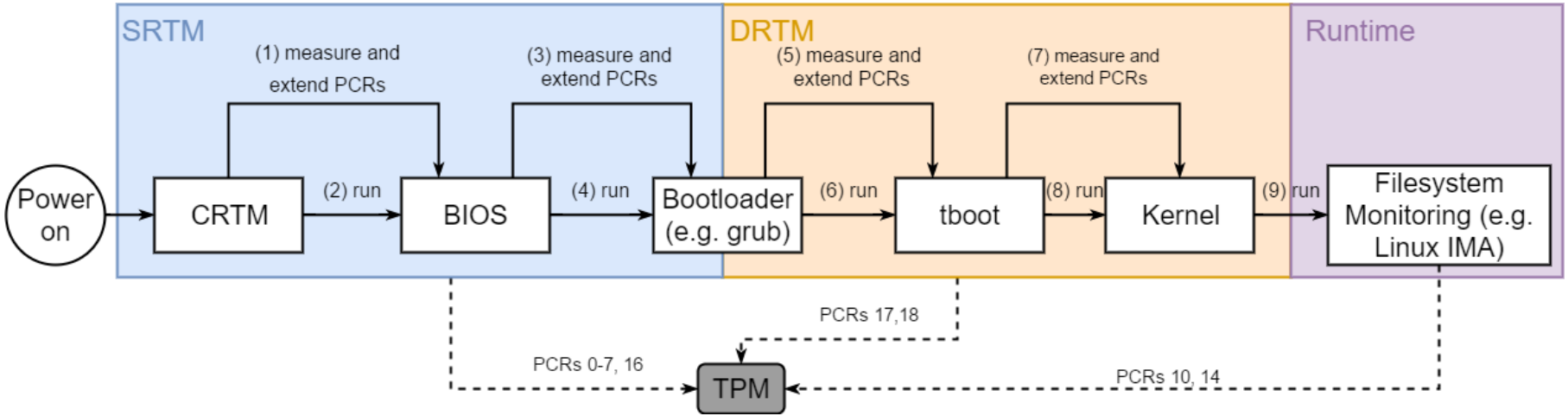
PCR Extend (PCR, *new_value*) = hash(PCR_{old} || *new_value*)

x86 boot process
(very simplified)



PCR Extend (PCR, *new_value*) = hash(PCR_{old} || *new_value*)

x86 boot process
(very simplified)



PCR Extend (PCR, *new_value*) = hash(PCR_{old} || *new_value*)

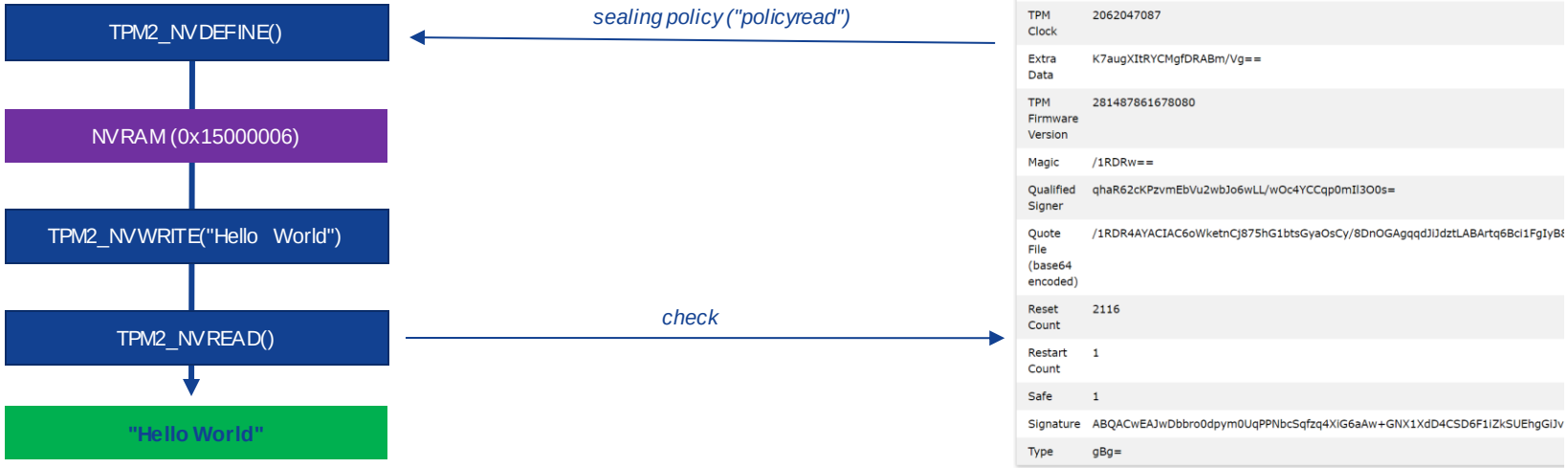
Platform Configuration Registers

sha256	0	580b4aca87f3589542a1a2f9659e7ed83ba7d2f75deae67172f2c19226c12529	CRTM: STRM, BIOS, Host Platform Extensions, Embedded Option ROMs
	1	28690847b179516e80f8f3527d410373e280d533e715b565ba81b88a050eacd9	Host Platform Configuration
	2	1d574e7566c44ba6d566b5e473ba2ba29c94724c603d4cb6c41861fbc8310320	UEFI driver and application Code
	3	3d458cfe55cc03ea1f443f1562beec8df51c75e14a9fcf9a7234a13f198e7969	UEFI driver and application Configuration and Data
	4	3d458cfe55cc03ea1f443f1562beec8df51c75e14a9fcf9a7234a13f198e7969	UEFI Boot Manager (usually MBR and boot attempts)
	5	de6479e9d0cfda1e9a26ad229e04fb9d6bf7b6f70a936e765b047093a354f7ce	Boot Manager Code Config and Data + GPT/Partition Table
	6	3d458cfe55cc03ea1f443f1562beec8df51c75e14a9fcf9a7234a13f198e7969	Host Platform Manufacturer Specific
	7	b5710bf57d25623e4019027da116821fa99f5c81e9e38b87671cc574f9281439	Secure Boot Policy
	8	0000000000000000000000000000000000000000000000000000000000000000	Defined for use by Static OS
	9	0000000000000000000000000000000000000000000000000000000000000000	Defined for use by Static OS
	10	72c3fde4903d142055eb231aadddc786a35850998a71db02879f3e81c165c671	Defined for use by Static OS, eg: Linux IMA
	11	0000000000000000000000000000000000000000000000000000000000000000	Defined for use by Static OS
	12	0000000000000000000000000000000000000000000000000000000000000000	Defined for use by Static OS
	13	0000000000000000000000000000000000000000000000000000000000000000	Defined for use by Static OS
	14	0000000000000000000000000000000000000000000000000000000000000000	Defined for use by Static OS, :eg Linux IMA/EMA
	15	0000000000000000000000000000000000000000000000000000000000000000	Defined for use by Static OS
	16	090781c52623ffd0d4e52ef58f87c9cb2bdab230d2fb3d2d4c0a1256477fb97b	Debug (DRTM)
	17	a92f5e0809ea038ce3a4cb4d33d4a941fcaac5c1d180163d1344f2f89028ff64	DRTM
	18	ee304ccd1dcd0ad63974427ccb71470e1e98b025dac116b0a2392e0f4acd2eb2	Used by DRTM
	19	0000000000000000000000000000000000000000000000000000000000000000	User defined
	20	0000000000000000000000000000000000000000000000000000000000000000	User defined
	21	0000000000000000000000000000000000000000000000000000000000000000	User defined
	22	0000000000000000000000000000000000000000000000000000000000000000	User defined
	23	0000000000000000000000000000000000000000000000000000000000000000	Application Support

Quoting 101: Anatomy of a quote

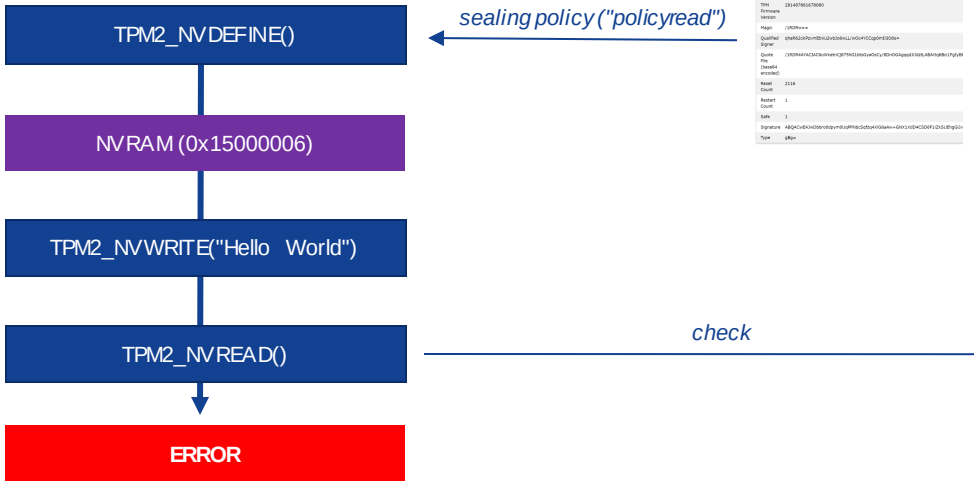
Attested Value	8fO0a76APjYPHId9gP3Yzn53bY9KSh3eGzhgkTTsQQ0=
TPM Clock	2062047087
Extra Data	K7augXItRYCMgfDRABm/Vg==
TPM Firmware Version	281487861678080
Magic	/1RDRw==
Qualified Signer	qhaR62cKPzvmEbVu2wbJo6wLL/wOc4YCCqp0mIl3O0s=
Quote File (base64 encoded)	/1RDR4AYACIAC6oWketnCj875hG1btsGyaOsCy/8DnOGAgqqdJiJdztLABArtq6Bci1FgIyB8
Reset Count	2116
Restart Count	1
Safe	1
Signature	ABQACwEAJwDbbro0dpym0UqPPNbcSqfzq4XiG6aAw+GNX1XdD4CSD6F1iZkSUEhgGiJv
Type	gBg=

Protecting secrets with a TPM
Sealing



NOKIA Bell Labs

Protecting secrets with a TPM
Sealing

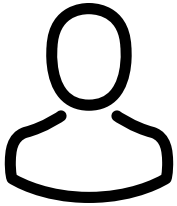


Attested Value	3facB1HiSh7dXpNar7qQqUvqCBwqnlMtvd+SDyriHAc=
TPM Clock	1455524401
Extra Data	bXUO3MQUTJCNT077zL+Z7Q==
TPM Firmware Version	281487861678080
Magic	/1RDRw==
Qualified Signer	GLorsbaim1jap1CXvtEvEsIKrw3Pm6tvPd0IawwOrVg=
Quote File (base64 encoded)	/1RDR4AYACIACxi6K7G2optY2qdQl77RLxLCCq8Nz5urbz3dCGsMDq1YABBtdQ7cxBRMkI1PTvvMv5ntA
Reset Count	18
Restart Count	1
Safe	1
Signature	ABQACwEAI8plsBN/OH86hYSFM0k7/zMg24eCKfG2STmIS466+OgZLbp/3C6YKTgo2WiknqeCu3B7oo1
Type	gBg=

NOKIA Bell Labs

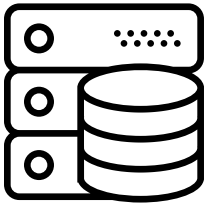
Trusted Cloud

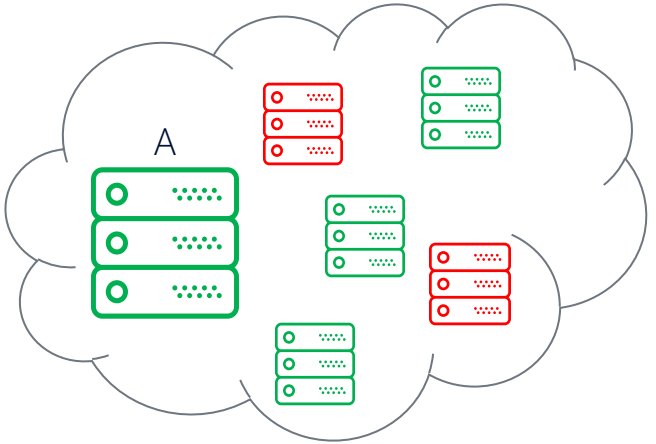
Remote attestation



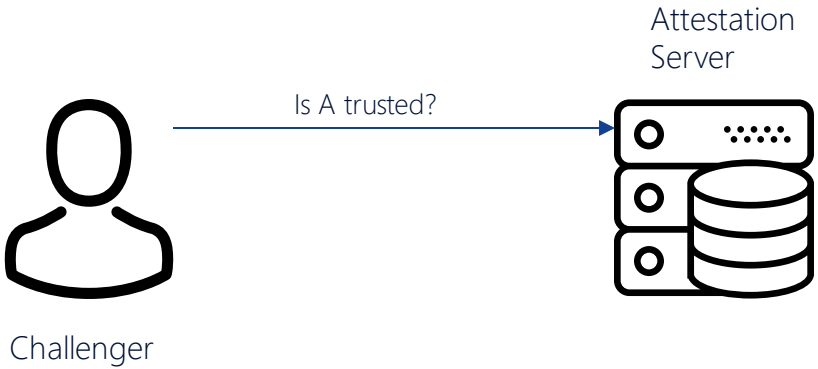
Challenger

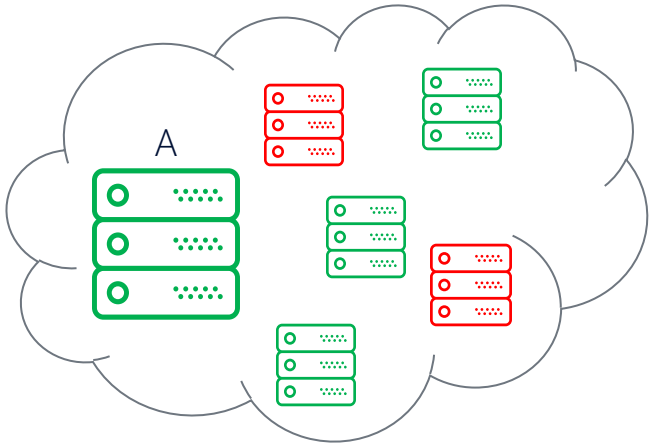
Attestation
Server



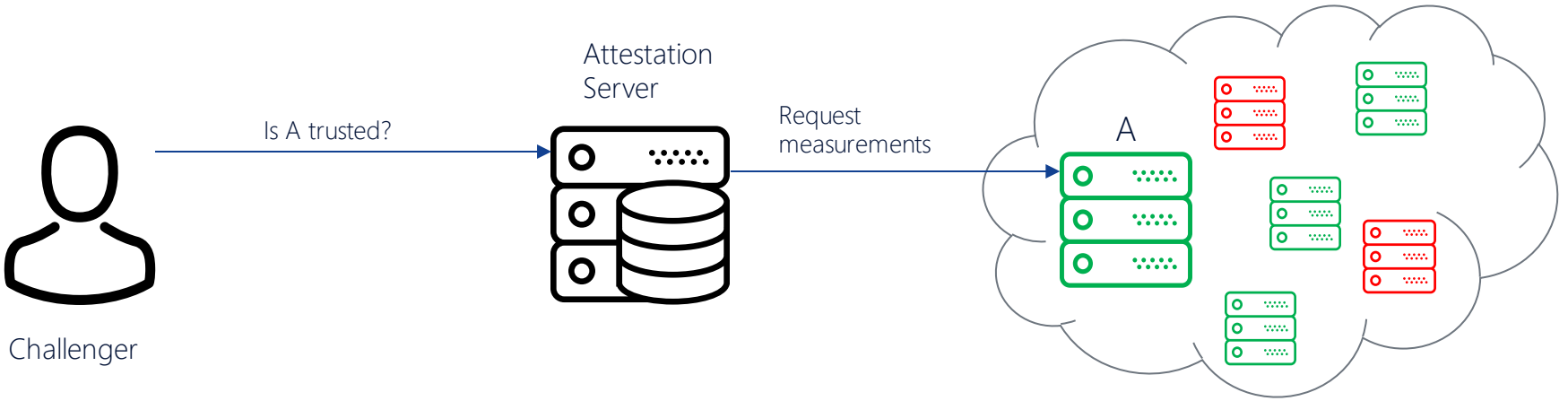


Remote attestation

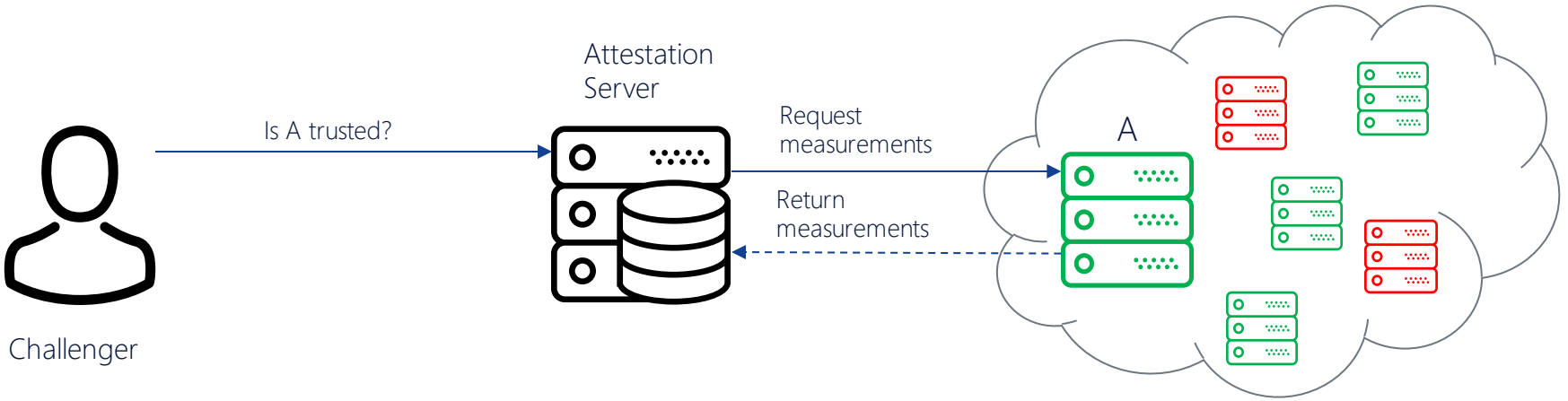




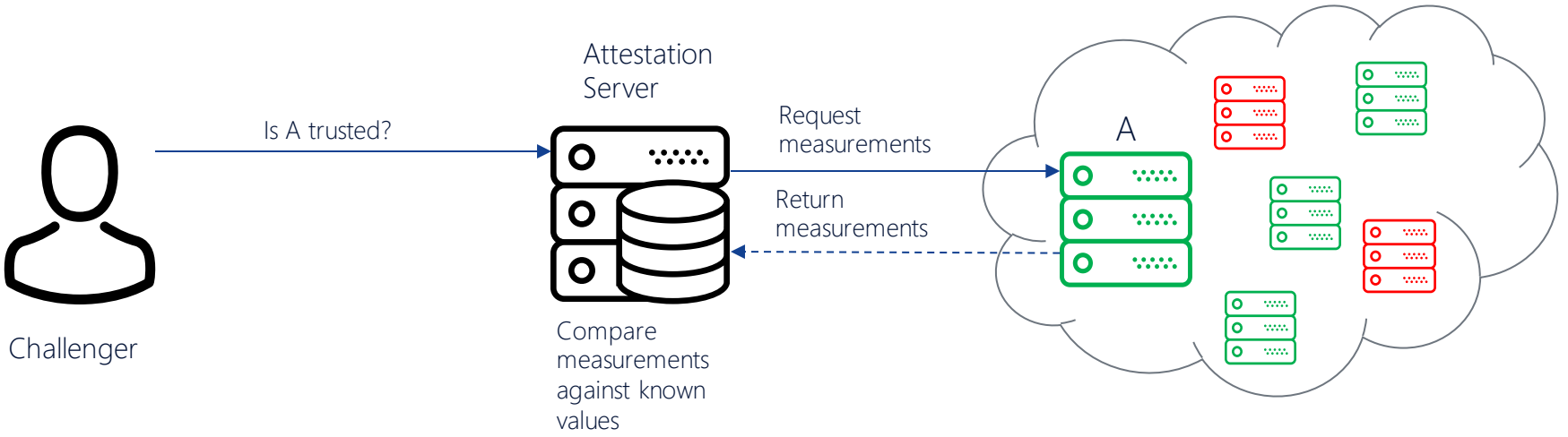
Remote attestation



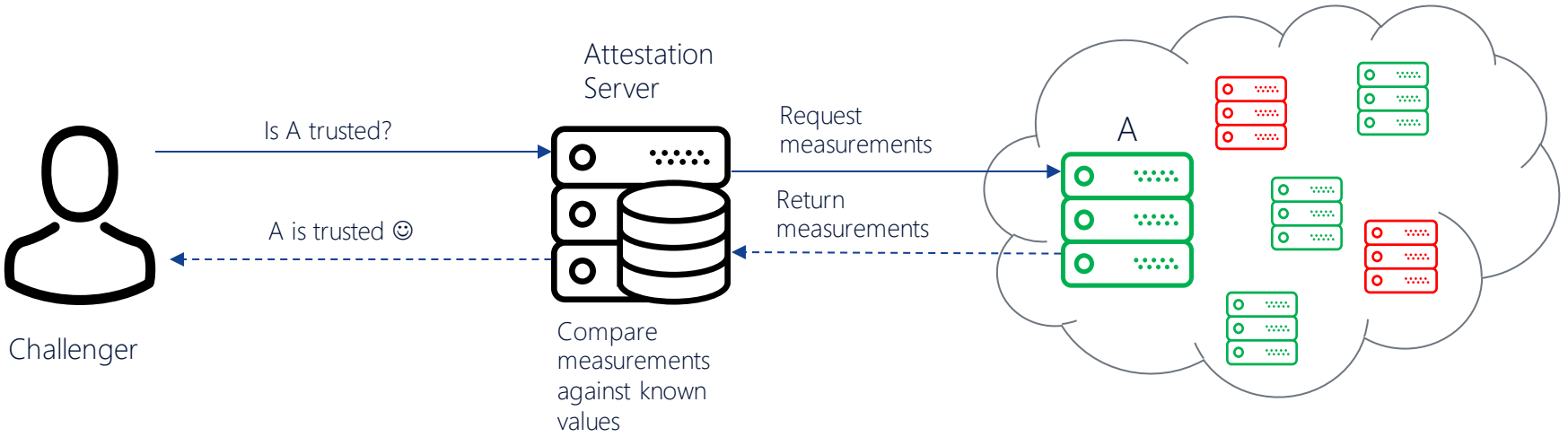
Remote attestation



Remote attestation

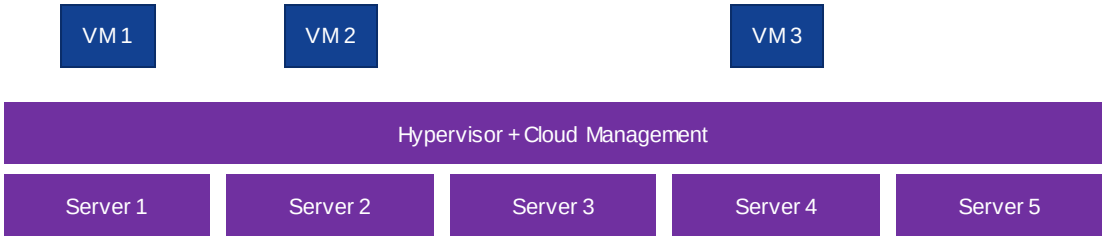


Remote attestation



Virtual Workload Placement

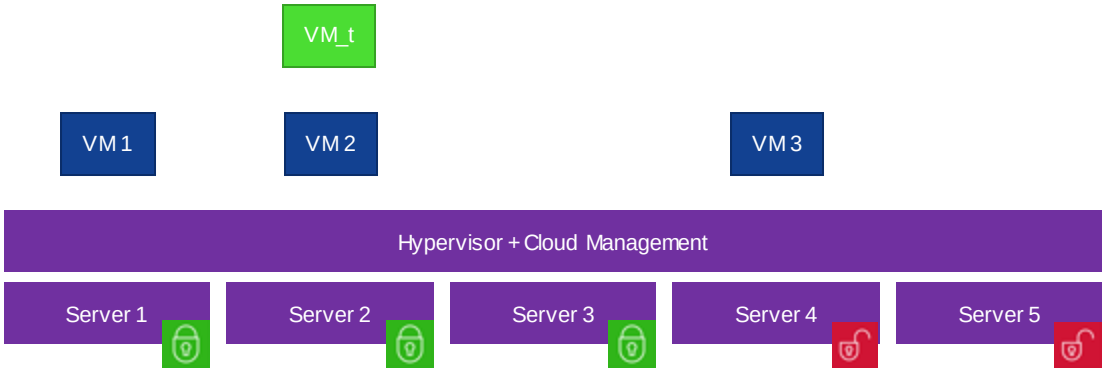
VMs are placed according to required and available vCPU and vMEM



Trusted Virtual Workload Placement

VMs are placed according to required and available vCPU and vMEM

VMs requiring trust are placed only on trusted machines

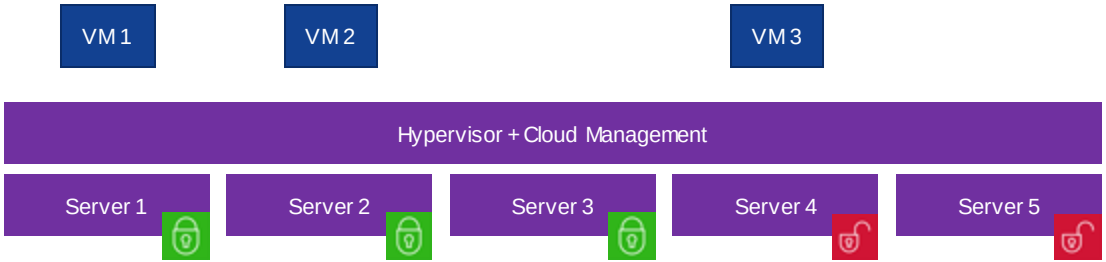


Trusted Virtual Workload Placement

VMs are placed according to required and available vCPU and vMEM

VMs requiring trust are placed only on trusted machines

1. Read VM_t requirements



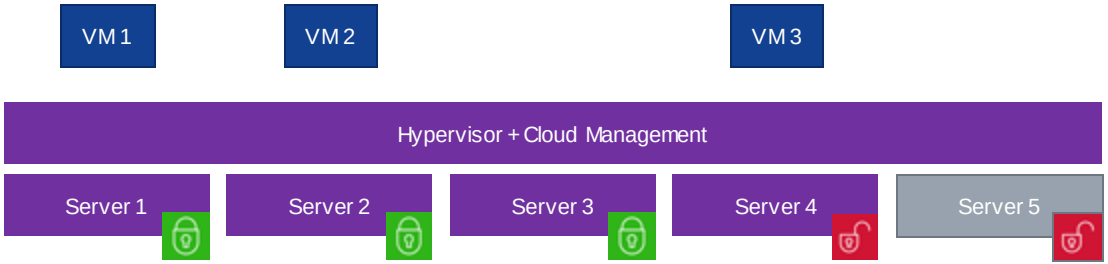
NOKIA Bell Labs

Trusted Virtual Workload Placement

VMs are placed according to required and available vCPU and vMEM

VMs requiring trust are placed only on trusted machines

1. Read VM_t requirements
2. Filter servers vCPU > reqCPU

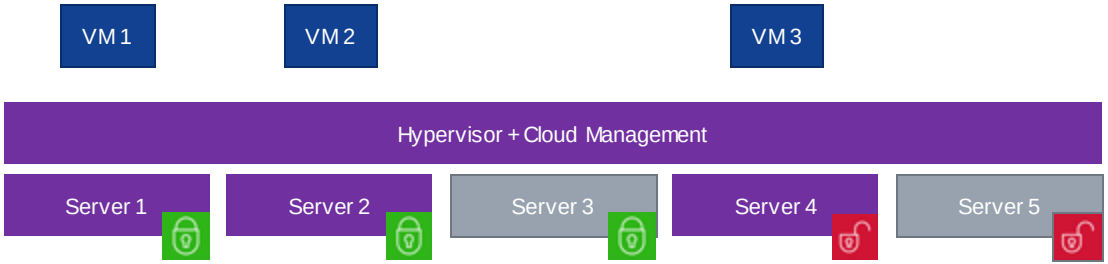


Trusted Virtual Workload Placement

VMs are placed according to required and available vCPU and vMEM

VMs requiring trust are placed only on trusted machines

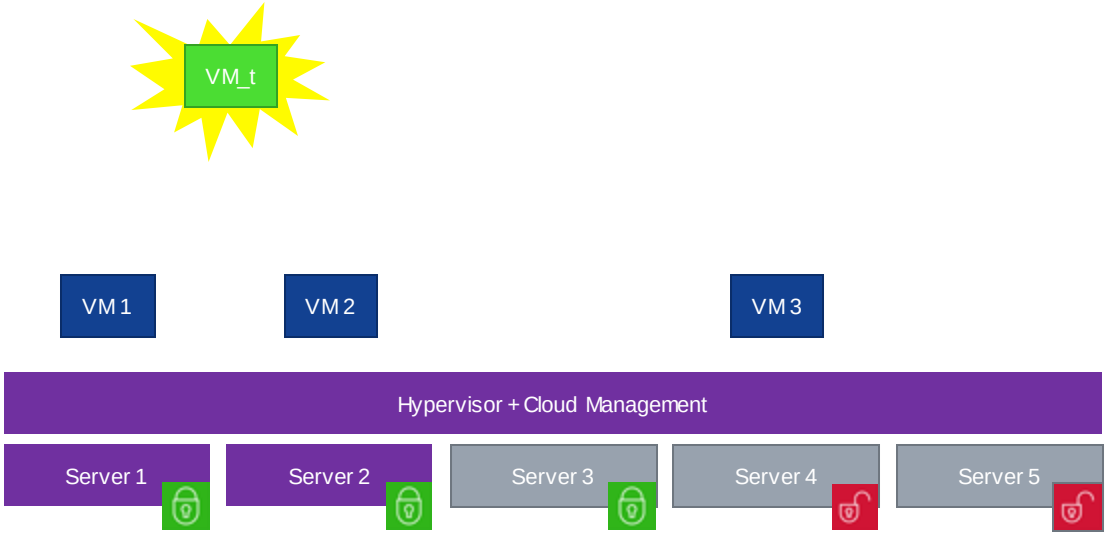
1. Read VM_t requirements
2. Filter servers vCPU > reqCPU
3. Filter servers vMEM > reqMEM



Trusted Virtual Workload Placement

VMs are placed according to required and available vCPU and vMEM

VMs requiring trust are placed only on trusted machines

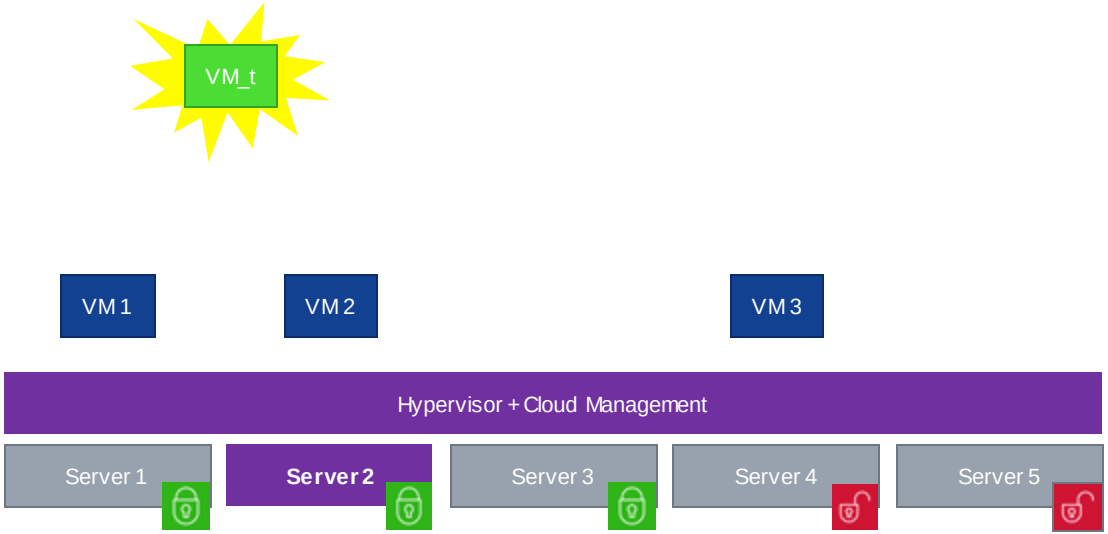


1. Read VM_t requirements
2. Filter servers vCPU > reqCPU
3. Filter servers vMEM > reqMEM
4. Filter servers sTrust == reqTrust

Trusted Virtual Workload Placement

VMs are placed according to required and available vCPU and vMEM

VMs requiring trust are placed only on trusted machines

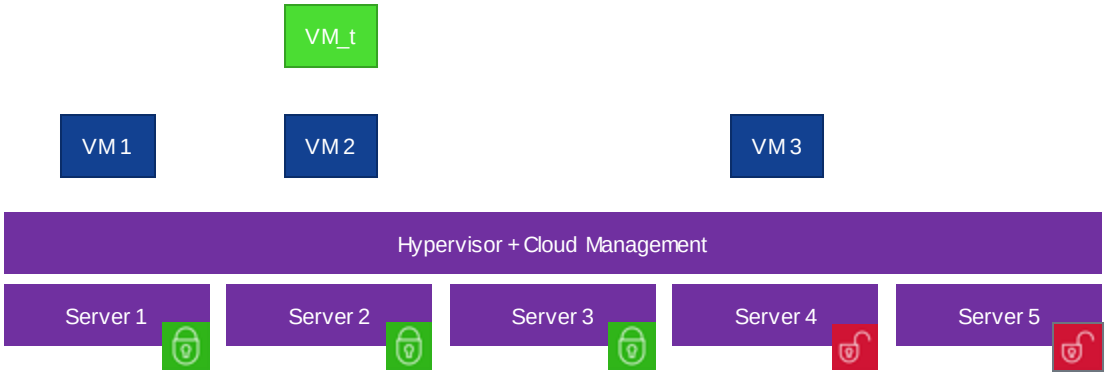


1. Read VM_t requirements
2. Filter servers vCPU > reqCPU
3. Filter servers vMEM > reqMEM
4. Filter servers sTrust == reqTrust
5. Pick a machine

Trusted Virtual Workload Placement

VMs are placed according to required and available vCPU and vMEM

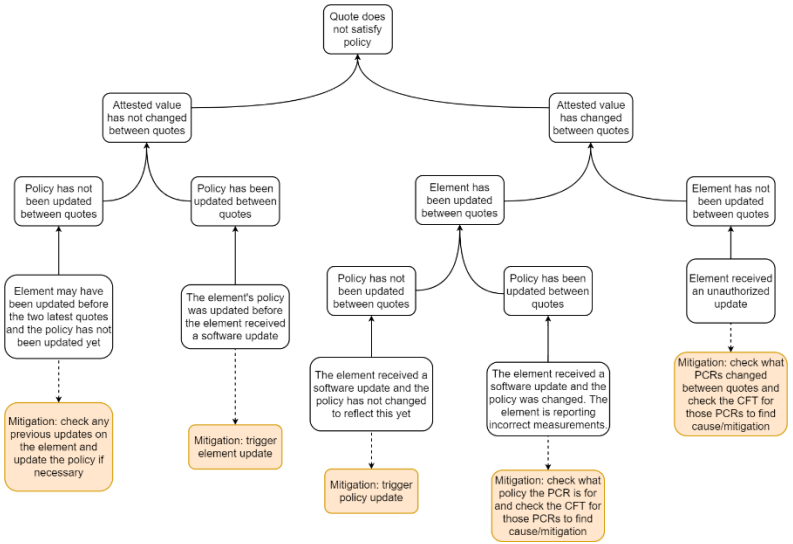
VMs requiring trust are placed only on trusted machines

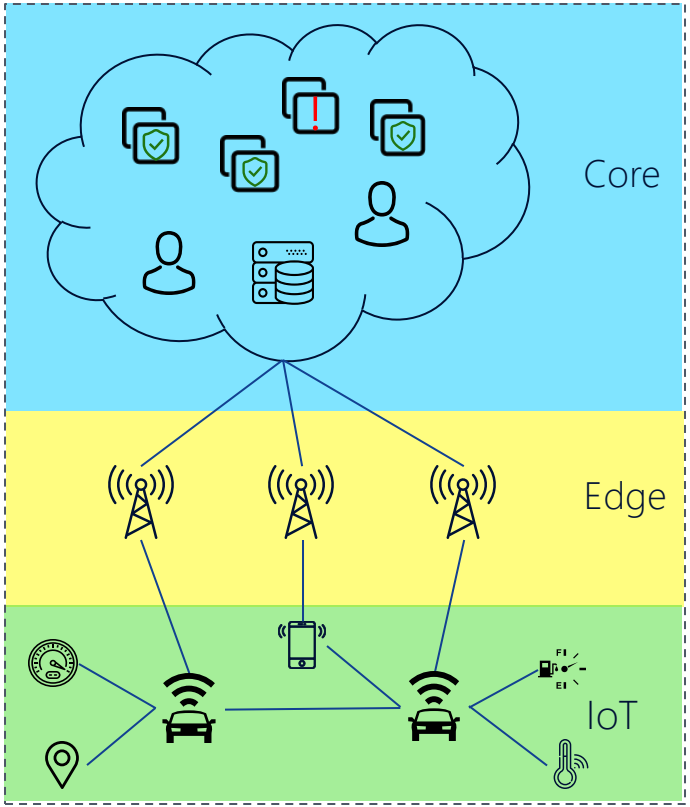


1. Read VM_t requirements
2. Filter servers vCPU > reqCPU
3. Filter servers vMEM > reqMEM
4. Filter servers sTrust == reqTrust
5. Pick a machine
6. Launch VM_t

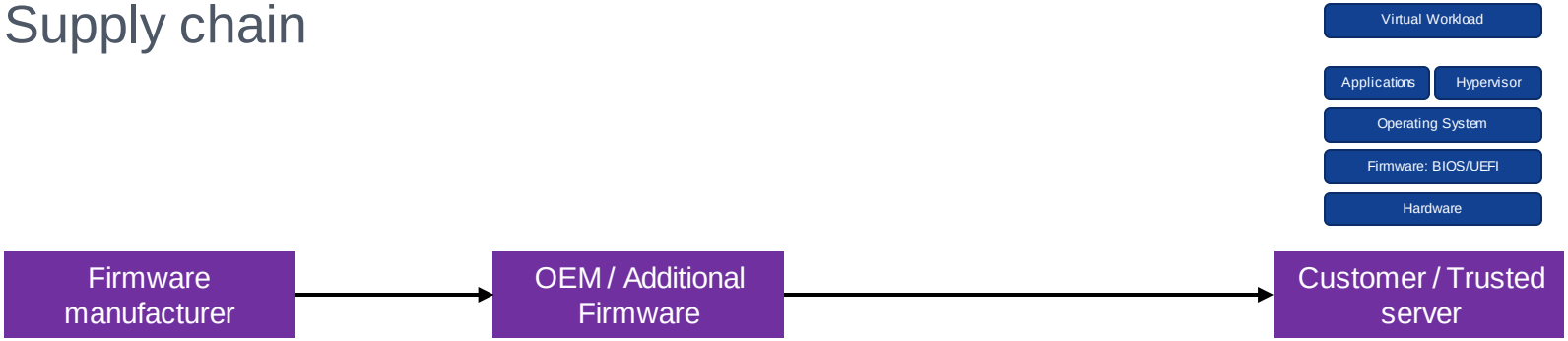
Handling failures and other open questions

- Root cause analysis
- Mitigation and response
- Extending trust across different layers
- Supply chain notarization



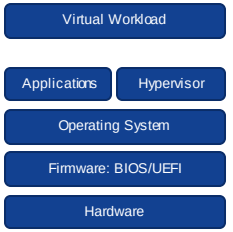


Limits of trust
Supply chain



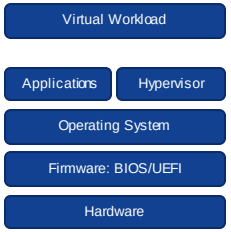
Limits of trust

What do measurements mean?



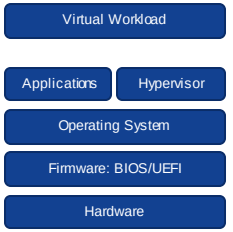
Limits of trust

What do measurements mean?



What if there is tampering along the way?

Limits of trust



Of course, that would never happen…

Firmware manufacturer → OEM / Additional Firmware → Customer / Trusted server

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

Any questions?

Contact:
gabriela.limonta@nokia.com


NOKIA