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

Gabriela Limonta
OWASP Meeting
03.09.2019
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

There is no cloud
it’s just someone else’s computer
The Cloud
(for real this time)
The Cloud
(for real this time)
The Cloud
(for real this time)
The Cloud
(for real this time)
The Cloud
(for real this time)
The Cloud
(for real this time)
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 25, 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
A problem:
Do you trust your datacenter?

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.
A problem:
Do you trust your datacenter?

TECH’S BOTTOM LINE
By Bill Snyder InfoWorld | MAY 23, 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

(T/S/SI/NF) Left: Intercepted packages are opened carefully; Right: A “load station” implants a beacon

1,201 views | Aug 1, 2013, 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.

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
Trust = Identity + Integrity
Chain of trust

- Hardware
- Firmware: BIOS/UEFI
- Operating System
- Applications
- Hypervisor
- Virtual Workload
- Hardware (trusting)
- Operating System
- Applications
- Hypervisor
- Virtual Workload (trusting)
Chain of trust

- Hardware
- Firmware: BIOS/UEFI
- Operating System
- Applications
- Hypervisor
- Virtual Workload

Hypervisor trusts
Chain of trust

- Hardware
- Firmware: BIOS/UEFI
- Operating System
- Applications
- Hypervisor
- Virtual Workload

Hypervisor trusts

Hardware
Firmware: BIOS/UEFI
Operating System
Applications
Virtual Workload
Chain of trust

- Hardware
- Firmware: BIOS/UEFI
- Operating System
- Applications
- Hypervisor
- Virtual Workload

Hypervisor trusts...
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
x86 boot process
(very simplified)
x86 boot process
(very simplified)

\[
\text{PCR Extend (PCR, } new\_value) = \text{hash(PCR}_{old} \parallel new\_value)
\]
x86 boot process (very simplified)

PCR Extend \((\text{PCR, new\_value}) = \text{hash(PCR\_old \| new\_value)}\)
PCR Extend (PCR, new_value) = hash(PCR_{old} || new_value)
<table>
<thead>
<tr>
<th></th>
<th>sha256</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>580b4aca87f3558542e4a29f659e7b2d83ba0d27f5deae717f2c19226c12529</td>
<td>CRTM: STRM, BIOS, Host Platform Extensions, Embedded Option ROMs</td>
</tr>
<tr>
<td>1</td>
<td>2869047b1795162e0f3527d4103732803d53e715b555ba81b88a050eac9d</td>
<td>Host Platform Configuration</td>
</tr>
<tr>
<td>2</td>
<td>1a574e7566c44ba6d566e5e473ba2ba29c94724c603d4bc6c4186fbc8310320</td>
<td>UEFI driver and application Code</td>
</tr>
<tr>
<td>3</td>
<td>3045fcf5cc0e3a1f4413f162be6d8df51c75e14a9f9a7234a13f198e7969</td>
<td>UEFI driver and application Configuration and Data</td>
</tr>
<tr>
<td>4</td>
<td>3045fcf5cc0e3a1f4413f162be6d8df51c75e14a9f9a7234a13f198e7969</td>
<td>UEFI Boot Manager (usually MBR and boot attempts)</td>
</tr>
<tr>
<td>5</td>
<td>de679e59d0cdef8e926ad229e04f9d6bfb76f7b9367e65b04079335f7ce</td>
<td>Boot Manager Code Configure and Data + GPT/Partition Table</td>
</tr>
<tr>
<td>6</td>
<td>3045fcf5cc0e3a1f4413f162be6d8df51c75e14a9f9a7234a13f198e7969</td>
<td>Host Platform Manufacturer Specific</td>
</tr>
<tr>
<td>7</td>
<td>b5710df57d25623e4010027a116821fa9ffccc8f8e38b87671c5749281349</td>
<td>Secure Boot Policy</td>
</tr>
<tr>
<td>8</td>
<td>0000000000000000000000000000000000000000000000000000000000000000</td>
<td>Defined for use by Static OS</td>
</tr>
<tr>
<td>9</td>
<td>0000000000000000000000000000000000000000000000000000000000000000</td>
<td>Defined for use by Static OS</td>
</tr>
<tr>
<td>10</td>
<td>72cf3de4903d42055eb231add65795a35590998a71d02879f9e81c1656c671</td>
<td>Defined for use by Static OS, e.g: Linux IMA</td>
</tr>
<tr>
<td>11</td>
<td>0000000000000000000000000000000000000000000000000000000000000000</td>
<td>Defined for use by Static OS</td>
</tr>
<tr>
<td>12</td>
<td>0000000000000000000000000000000000000000000000000000000000000000</td>
<td>Defined for use by Static OS</td>
</tr>
<tr>
<td>13</td>
<td>0000000000000000000000000000000000000000000000000000000000000000</td>
<td>Defined for use by Static OS</td>
</tr>
<tr>
<td>14</td>
<td>0000000000000000000000000000000000000000000000000000000000000000</td>
<td>Defined for use by Static OS, e.g Linux IMA/EMA</td>
</tr>
<tr>
<td>15</td>
<td>0000000000000000000000000000000000000000000000000000000000000000</td>
<td>Defined for use by Static OS</td>
</tr>
<tr>
<td>16</td>
<td>090781c52623f5d0e52e5f8f7c9c2b2ab230d2fbd3d24c8a125647fb97b</td>
<td>Debug (DRTM)</td>
</tr>
<tr>
<td>17</td>
<td>a92f9e0809a038ce3a4c4d3364a94f0ca8c4c1d180103d1344f279928ff64</td>
<td>DRTM</td>
</tr>
<tr>
<td>18</td>
<td>ee30c4cdcd0a036974427cc714790e198b0255d1160a03239e064acc02e02</td>
<td>Used by DRTM</td>
</tr>
<tr>
<td>19</td>
<td>0000000000000000000000000000000000000000000000000000000000000000</td>
<td>User defined</td>
</tr>
<tr>
<td>20</td>
<td>0000000000000000000000000000000000000000000000000000000000000000</td>
<td>User defined</td>
</tr>
<tr>
<td>21</td>
<td>0000000000000000000000000000000000000000000000000000000000000000</td>
<td>User defined</td>
</tr>
<tr>
<td>22</td>
<td>0000000000000000000000000000000000000000000000000000000000000000</td>
<td>User defined</td>
</tr>
<tr>
<td>23</td>
<td>0000000000000000000000000000000000000000000000000000000000000000</td>
<td>Application Support</td>
</tr>
</tbody>
</table>
### Quoting 101: Anatomy of a quote

| Attested Value | 8fO0a76APJYPHId9gP3YznS3bY9KSh3eGzhgkTTsQ0= |
| TPM Clock | 2062047087 |
| Extra Data | K7augXItRYCMgfDRABm/Vg== |
| TPM Firmware Version | 281487861678080 |
| Magic | /1RDRw== |
| Qualified Signer | qhaR62ckPzvmEbVu2wbJo6wLL/wOc4YCCq0mI300s= |
| Quote File (base64 encoded) | /1RDR4AYACIC6oWkEtNCj875hG1btsGyaOsCy/8DnOGAgqqdJlJdZtLABArtq6Bcl1Fg1yB! |
| Reset Count | 2116 |
| Restart Count | 1 |
| Safe | 1 |
| Signature | ABQACwEAJwDbbr00dpym0UqPPNbcSqvq4XIG6aAvw+GNX1XdD4CSD6F1IZkSUEhGIGv |
| Type | gBg= |
Protecting secrets with a TPM
Sealing

TPM2_NVDEFINE()

NVRAM (0x15000006)

TPM2_NVWRITE("Hello World")

TPM2_NVREAD()

"Hello World"

sealing policy ("policyread")

check

Attested Value: 8DF0a76A9PjyHt29gF3Yzn53hY9h9IeGthgkTThQQe=
TPM Clock: 2062047087
Extra Data:
TPM Firmware Version:
Magic: /KDrw==
Qualified Signer:
Quote File (base64 encoded):
Reset Count: 2116
Restart Count: 0
Safe 1
Signature: ABQACwEAjwDbv0s0dyymRqjPP1c0sQ9zq4X/OG644w+GKX1yD4CSD5F1zX5hEhgGJ4v
Type: g8Gw=
Protecting secrets with a TPM

Sealing

TPM2_NVDEFINE()

NVRAM (0x15000006)

TPM2_NVWRITE("Hello World")

TPM2_NVREAD()

ERROR

sealing policy ("policyread")

check

ERROR
Trusted Cloud
Remote attestation

Challenger

Attestation Server

A
Remote attestation

Is A trusted?

Challenger

Attestation Server

A
Remote attestation

Challenger

Is A trusted?

Attestation Server

Request measurements

A
Remote attestation

Challenger

Is A trusted?

Attestation Server

Request measurements

Return measurements

A
Remote attestation

Challenger

Is A trusted?

Attestation Server

Request measurements

Compare measurements against known values

Return measurements

A
Remote attestation

Challenger

Is A trusted?

Attestation Server

Request measurements

A

Is A trusted?

A is trusted ☺

Compare measurements against known values

Return measurements
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

Diagram:
- VMs: VM1, VM2, VM3
- Servers: Server 1, Server 2, Server 3, Server 4, Server 5
- Hypervisor + Cloud Management
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

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