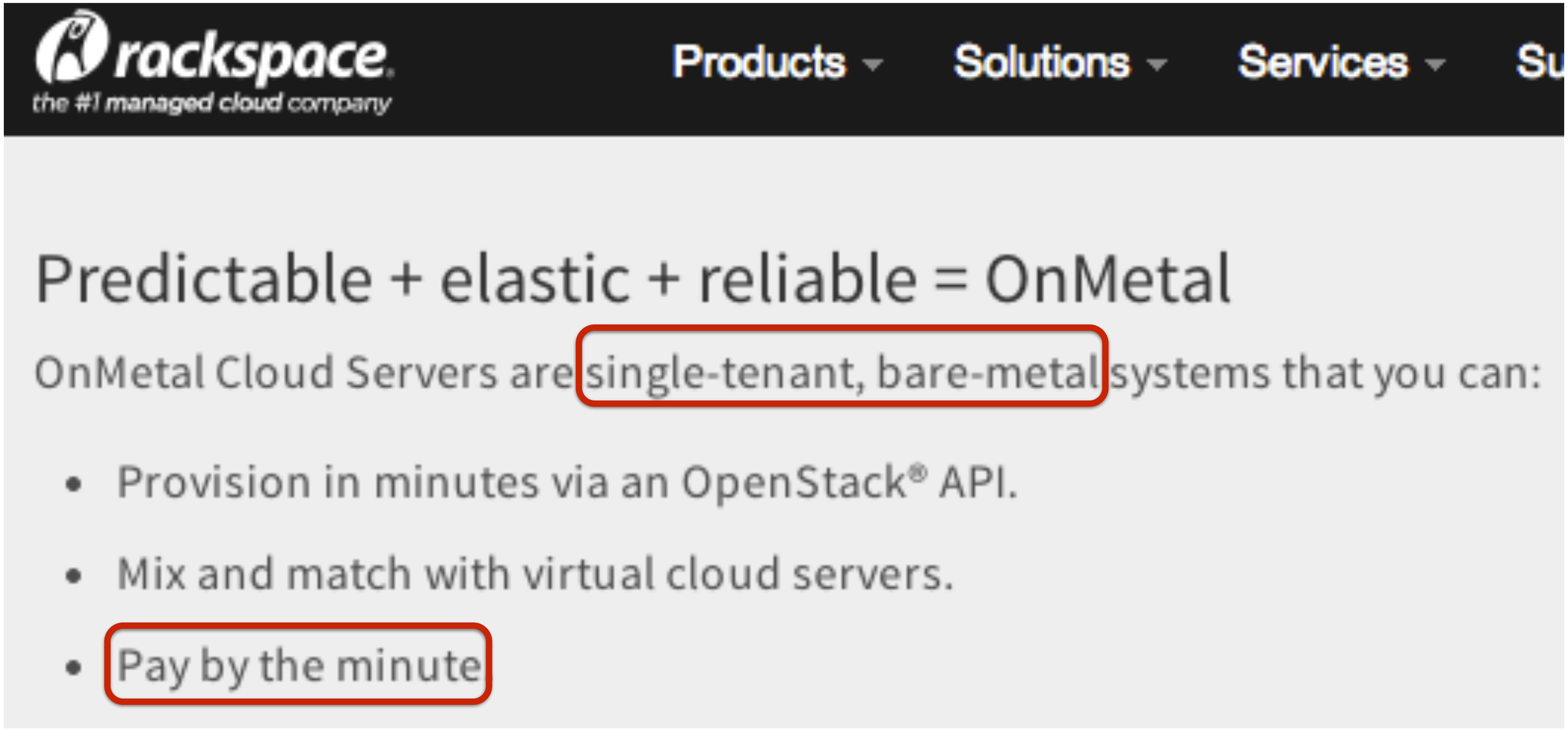
# Trusted Computing & OpenStack

Steve Weis
PrivateCore

OpenStack Security Meetup
July 2014

# How safe are bare-metal clouds?



# Attacks in the wild

SPIEGEL ONLINE

**Shopping for Spy Gear: Catalog Advertises NSA Toolbox**

*By Jacob Appelbaum, Judith Horchert and Christian Stöcker*

Symantec. | Official Blog

**BIOS Threat is Showing up Again!**

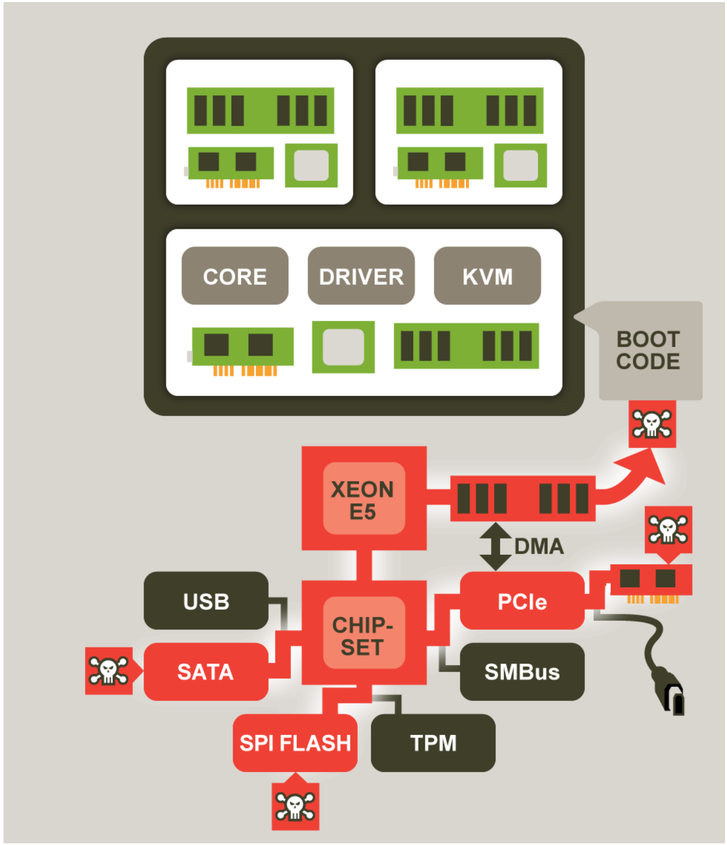
Created: 09 Sep 2011 10:19:42 GMT • Updated: 23 Jan 2014 18:19:11 GMT •

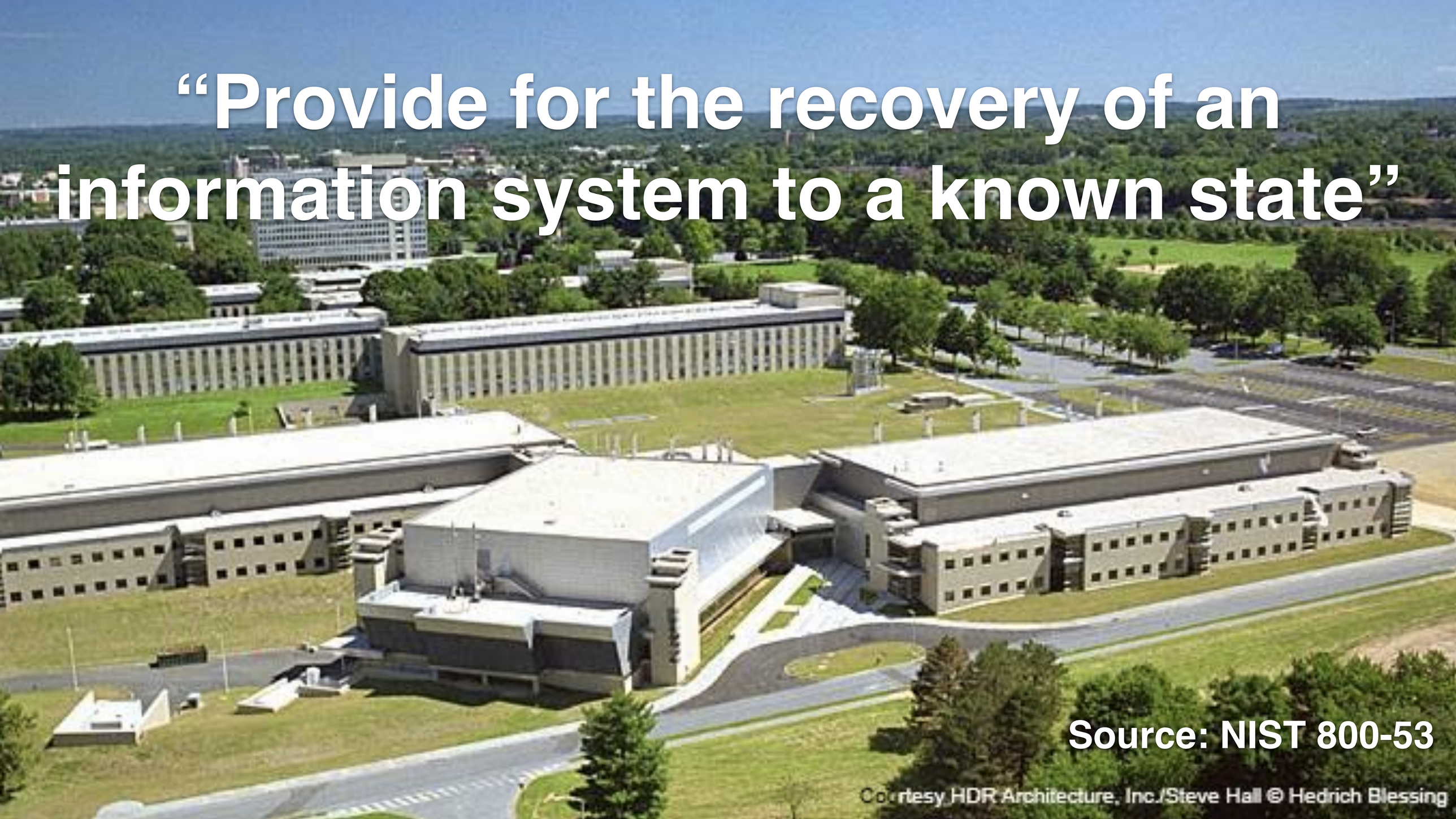
The Register®

**Malware burrows deep into computer BIOS to escape AV**

# Exploit all the things!

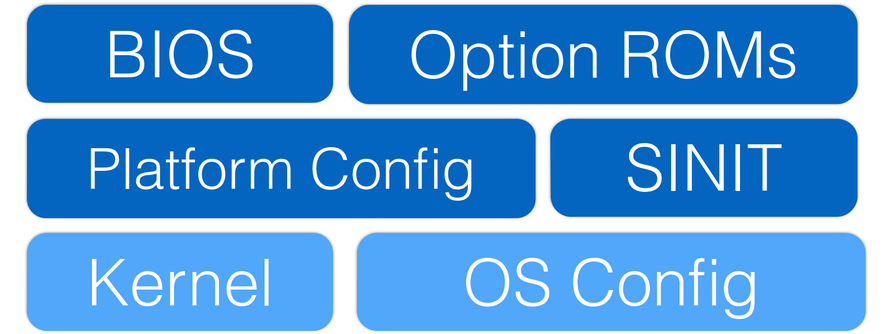
- Operating Systems
- BIOS / EFI
- Device firmware / Option ROMs
- Master boot records
- Keyboard controllers
- Management engines and controllers




“Provide for the recovery of an information system to a known state”
Source: NIST 800-53
Courtesy HDR Architecture, Inc./Steve Hall © Hedrich Blessing

# Trusted Execution Technology

Firmware and software needed to boot




*Remote Attest*

**TPM**

*Measure*

**CPU**

# Example Measurements

| PCR | Entry Type | Valid | Value |
|---|---|---|---|
| 0 | Final Value | Yes | b21ce8dbe22b63119184908f9b9f5b8b5e33c78c |
| 17 | Final Value | Yes | fdbfc169cd6a33f636386c4e6ff9ff8e76634b0f |
| 17 | SINIT Hash | Yes | 69ecaace5107595404b7bf48d07289a7186e0c4f |
| 18 | Final Value | Yes | 907511fe2781ed59d28ddc1446721d30602427e0 |
| 18 | Kernel Command Line | Yes | live_image_url=http://192.168.0.54/fog/public/sweis/ auth_keys_filename=auth_keys.cpio.gz static_ip=192.168.0.57 modules_network=bnx2 console=ttyS0,115200n8 network_wait_secs=2 |
| 18 | Tboot Hash | Yes | 2da41566d02e5636b3564a9de117f5cc63d18f9c |
| 18 | Tboot Command Line | Yes | logging=serial,vga,memory |
| 18 | Kernel Hash | Yes | f609d9a80a8963f9f74dba167e7eb83b02561a53 |
| 19 | Final Value | Yes | ec570d184ee1faedd88f18c064691bb96322ad78 |
| 19 | Initrd Hash | Yes | 52f7b3e74fbdd9d42a0fbf325b79ee34a4619da4 |
| 23 | Final Value | Yes | 7a863ec6c6136b238c6015a7ab67b5d9e7f0464f |
| 23 | User Certificate | Yes | d36a06de3a1dcc588e2924bb53167d10b73bf574 |

Displaying 12 items

**BIOS**

**ACM**

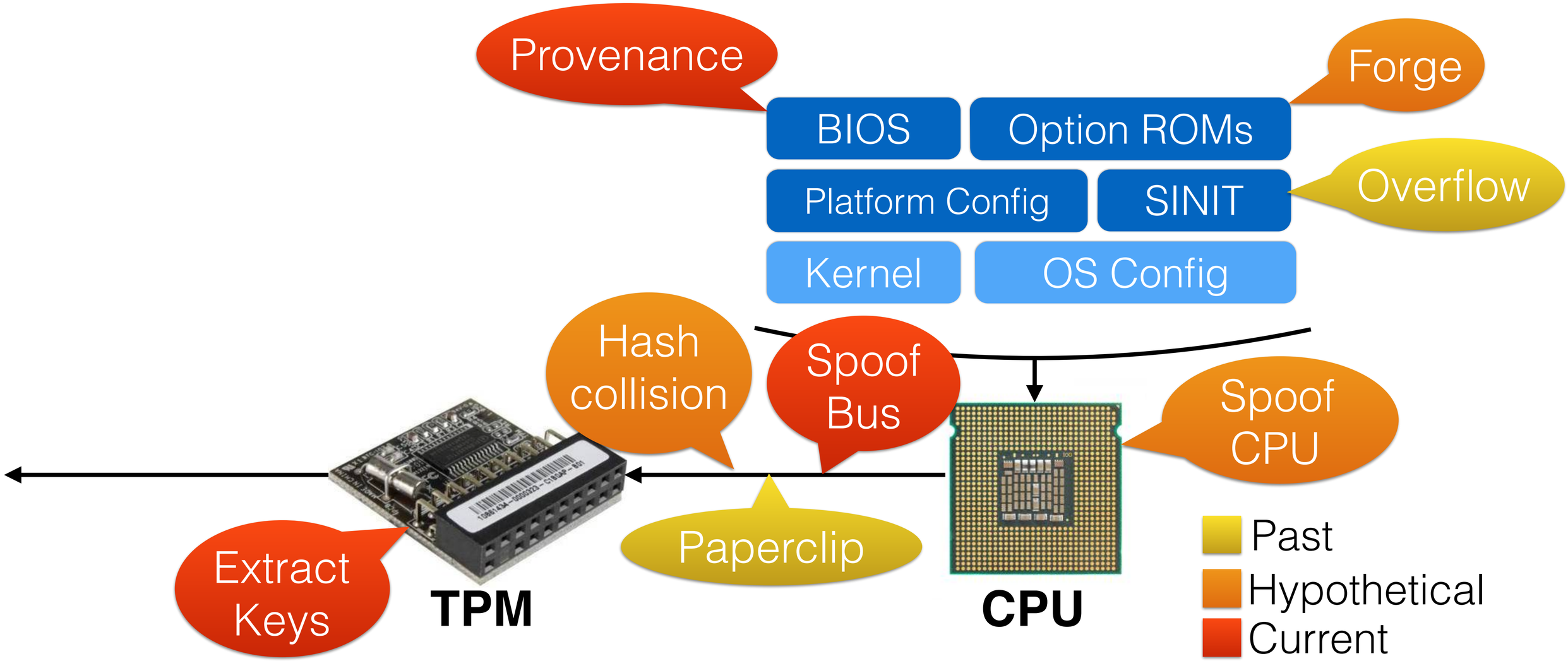
**Config**

**MLE**

**OS**

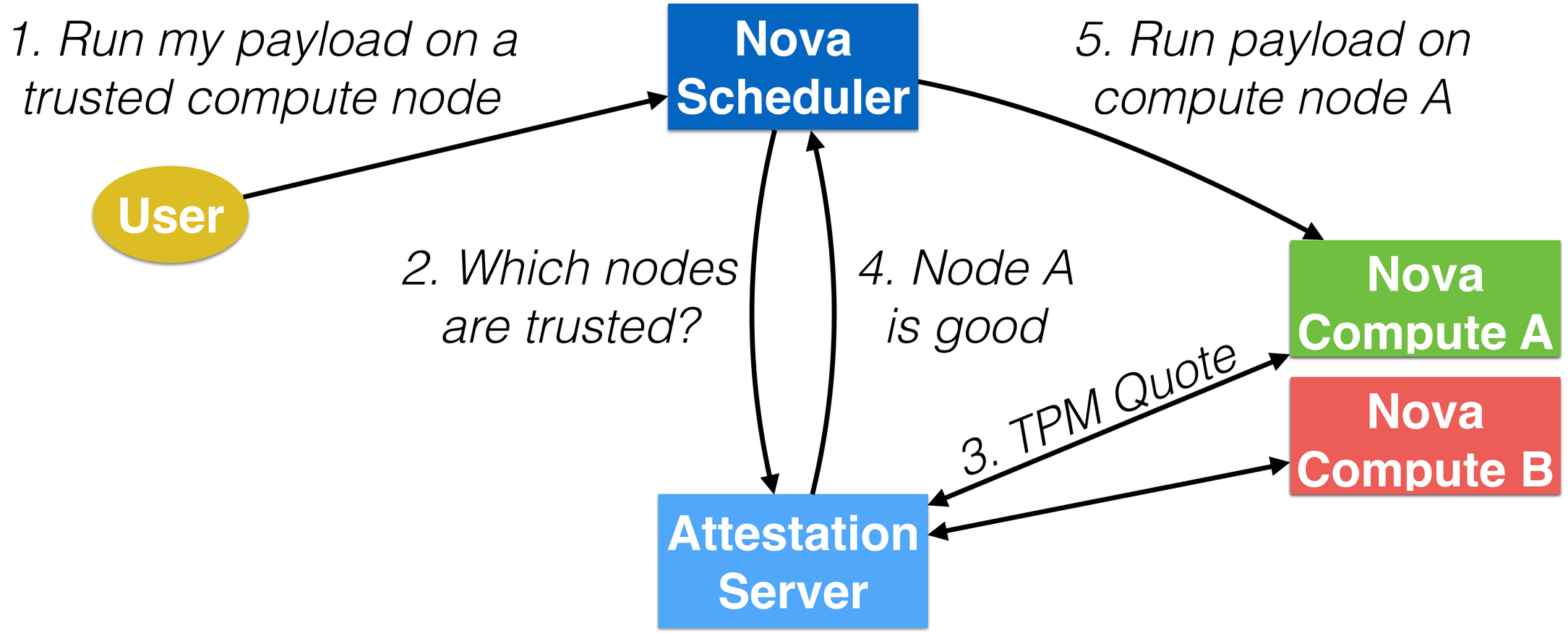
**Credentials**

# Gaps in Trusted Execution



# Attestation in OpenStack

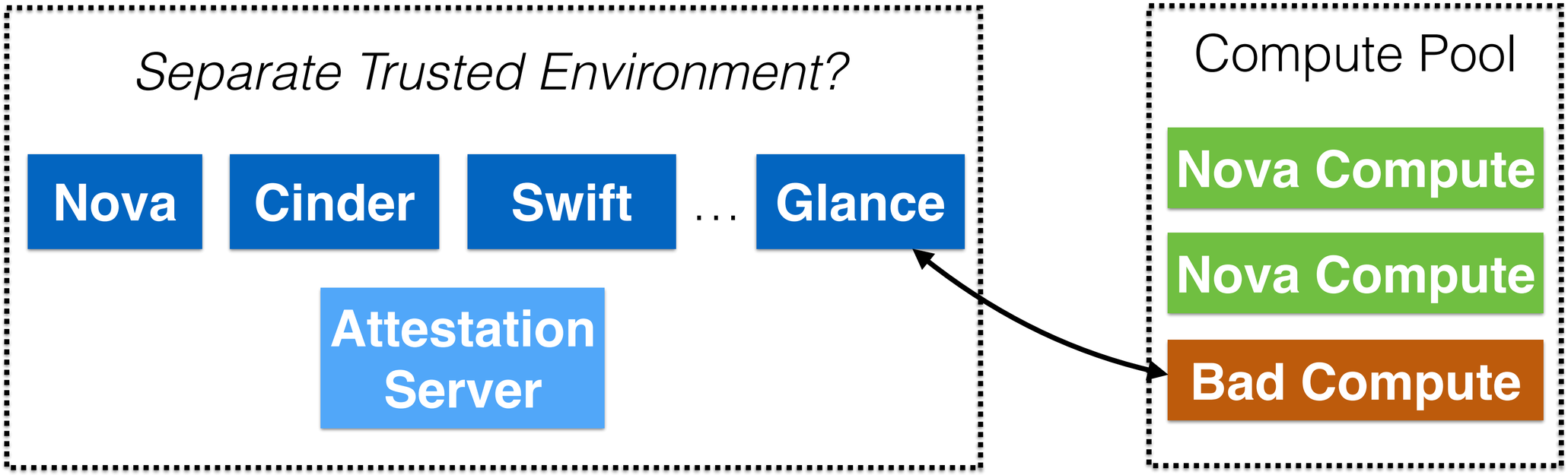
# Trusted Compute Pools



# Implementations

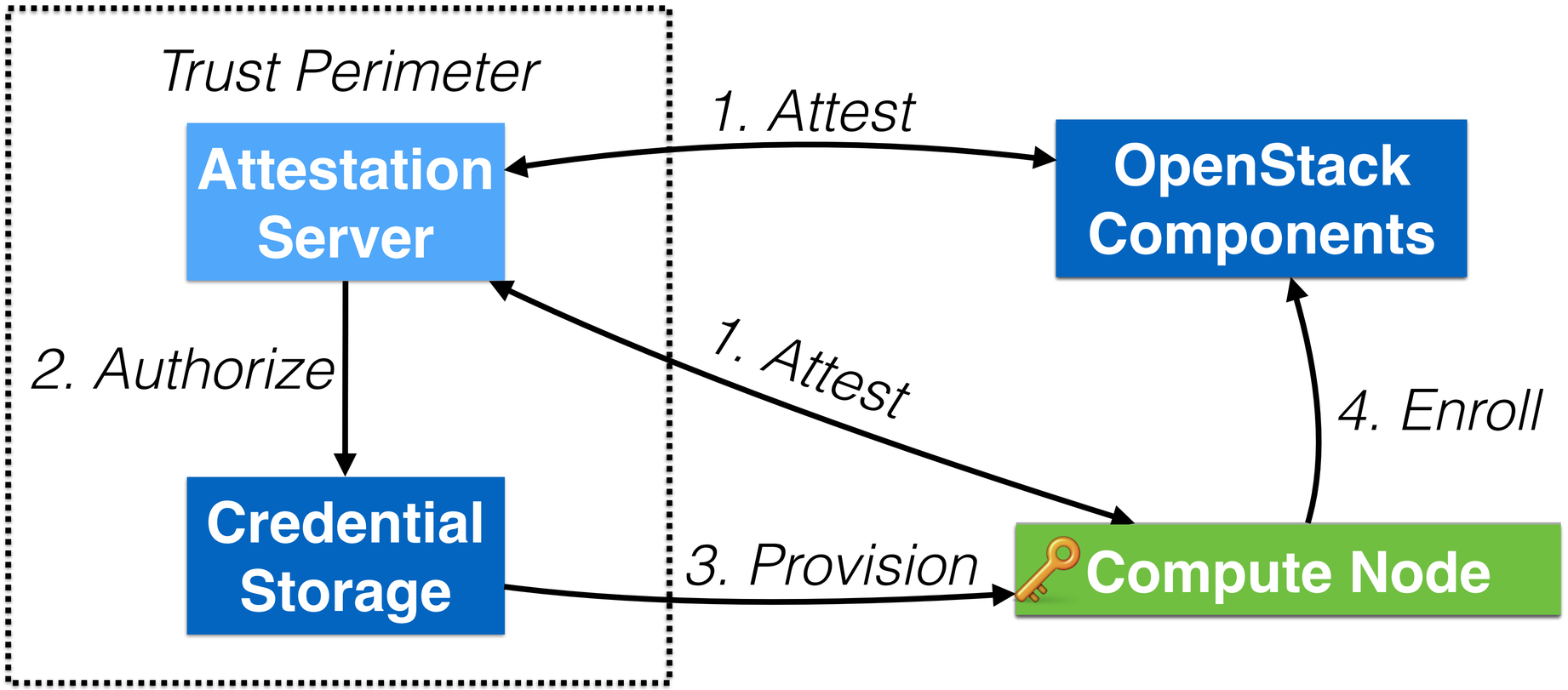
- **Open Attestation** (OAT): https://01.org/openattestation
  - Open source Java attestation server. Mostly developed by Intel.
- **Intel Trust Attestation Solution** (Mt. Wilson): Enterprise OAT
- **PrivateCore vCage**: Python / Django / Horizon attestation server

# Gaps in Trusted Pool Model




*Bad nodes already have control plane access?*

# Toward a Better Model



# Suggested Improvements

1. Attest all servers in OpenStack: Not just compute nodes
2. Cloud providers should provide TPMs and compatible firmware
3. Vendors need to provide authoritative lists of measurement values
4. CPU vendors should ultimately remove dependency on TPMs

# Thank you!

Questions?

steve@privatecore.com
@sweis