UNIVERSITY of WASHINGTON

Hardening our Common Computing Landscape: Toward a High Assurance Private Cloud

Tom Rochat
Information Systems and Technology
Institute of Technology,
University of Washington, Tacoma, WA, USA
RochatT@uw.edu

Committee:
Dr. Sam Chung
Institute of Technology
University of Washington, Tacoma, WA, USA

Dr. Endicott- Popovsky
Center for Info. Assruance &CyberSecurity
University of Washington, Seattle, WA, USA

Intrusion Problem

- In 2011 a survey of 583 US companies conducted by Ponemon research reported **90%** of companies experienced a breach over the past 12 months.
- It was also reported that **95%** of privately owned computers had been breached, in the past 12 months.
- We must secure our sensitive data!

Part of the Solution…

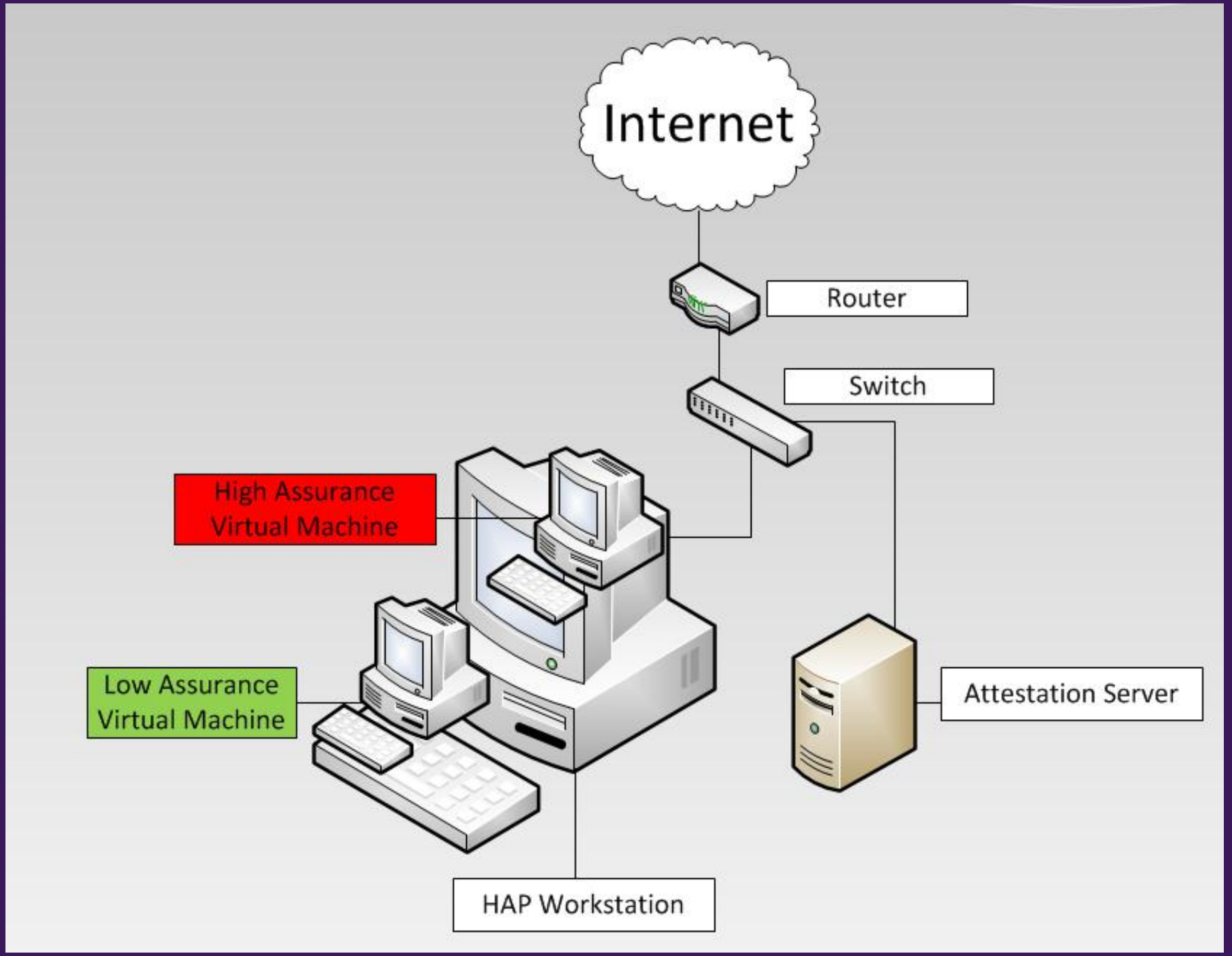
- National Security Agency developed the High Assurance Platform - 1st release was in 2009, 2nd release 2011
- Cloud Computing - IaaS, PaaS, SaaS

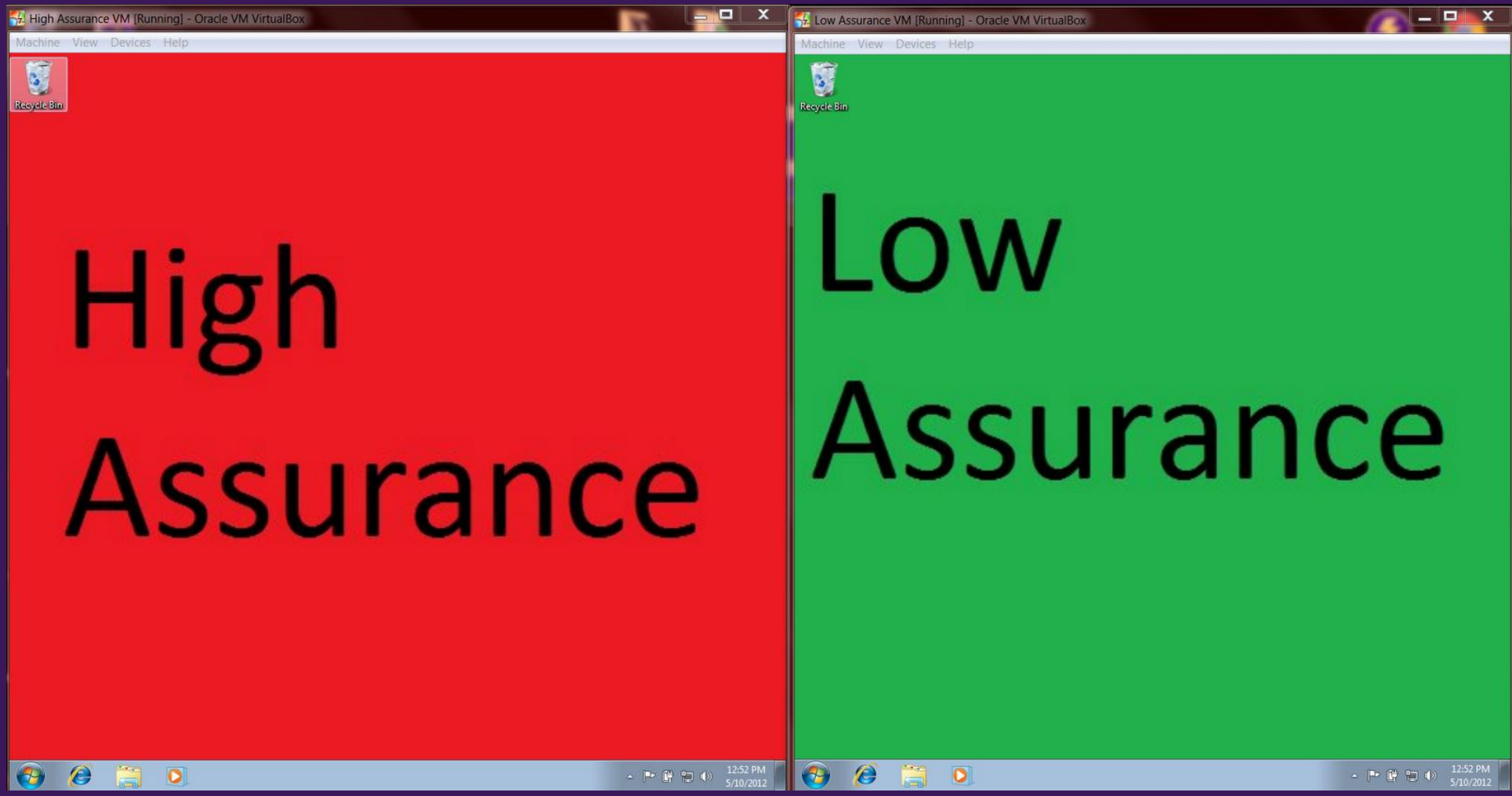
High Assurance Platform (HAP)

- Trusted Platform Module (TPM)
- Embedded Hardware Virtualization Security (Intel VT-d and TxT aka domain separation)
- Trusted Operating System
- Secure Virtualization Software(Hypervisors)

High Assurance Platform (HAP)

- Trusted Boot
  (Authentication with Remote Attestation Server)
- Remote Attestation
  (Compare to a known good)
- Trusted Network Access Control
  (Policy Decision Point and Policy Enforcement Point)


Internet
Router
Switch
High Assurance
Virtual Machine
Low Assurance
Virtual Machine
Attestation Server
HAP Workstation

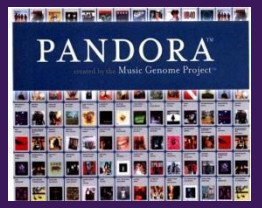

High Assurance VM [Running] - Oracle VM VirtualBox
Machine View Devices Help
Recycle Bin
High
Assurance
12:52 PM
5/10/2012
Low Assurance VM [Running] - Oracle VM VirtualBox
Machine View Devices Help
Recycle Bin
Low
Assurance
12:52 PM
5/10/2012

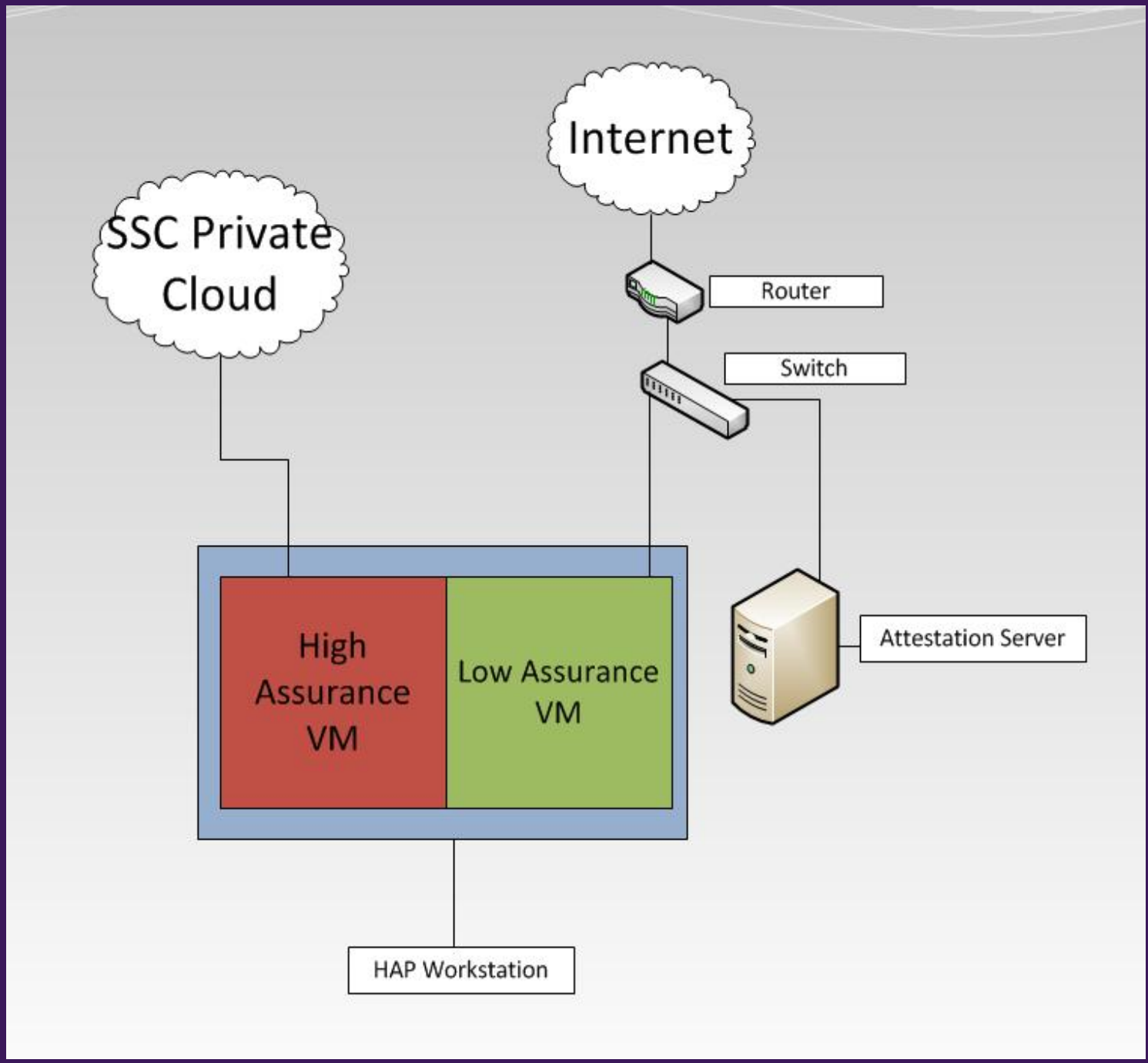
Cloud Computing

IaaS - Infrastructure as a service, use someone else's hardware for your purposes.
(Hypervisors - Xen Cloud Platform)

PaaS - Platform as a service, use someone else's hardware and framework for your purposes.
(Googles App Engine)

SaaS - Software as a service, use someone else's software for your purposes.
(Youtube, Gmail ,Pandora)




Internet
SSC Private Cloud
Router
Switch
High Assurance VM
Low Assurance VM
Attestation Server
HAP Workstation

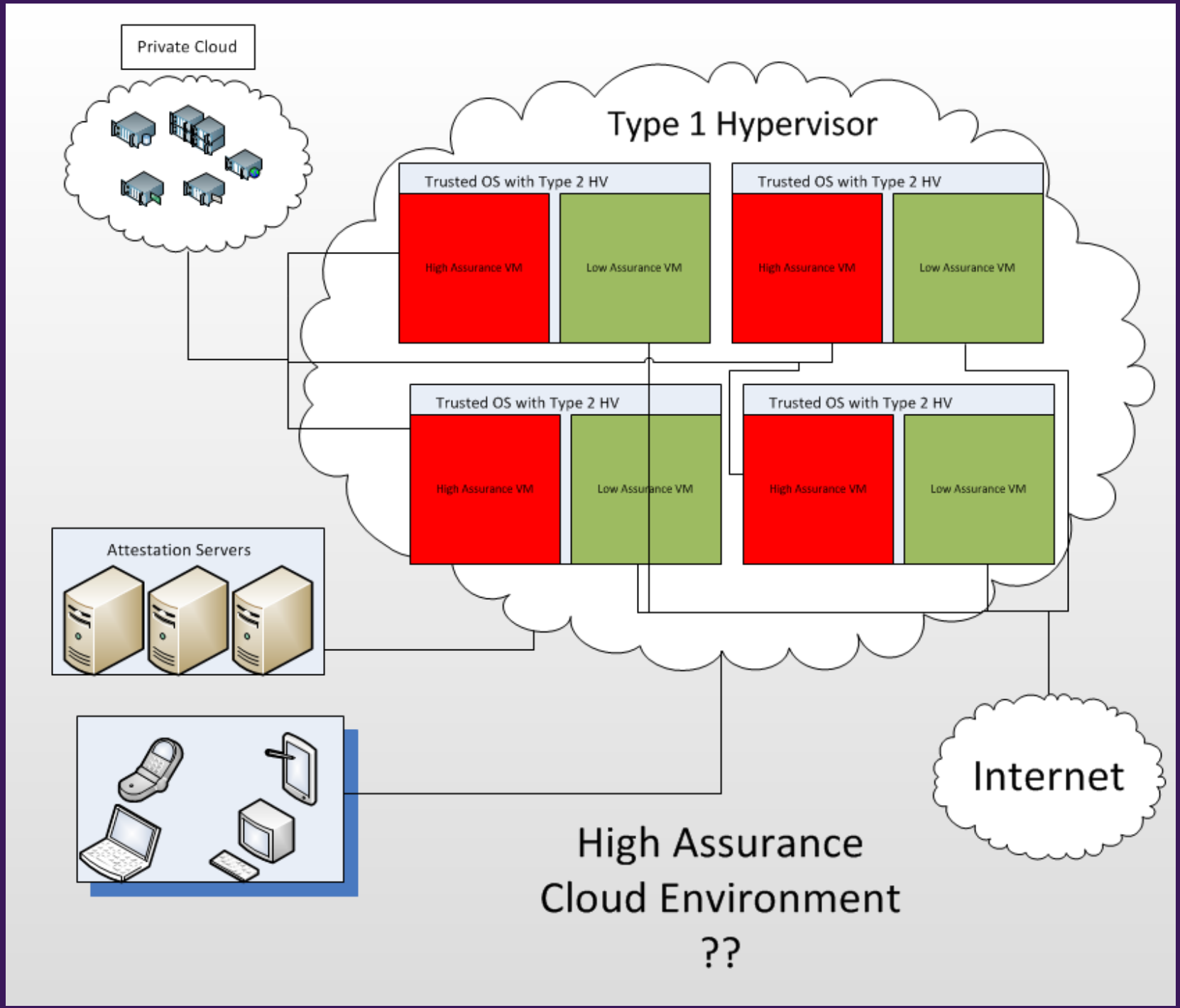

High
Assurance
Low
Assurance

High Assurance Cloud (HAC) ???

- Trusted Operating System
  (Xen, Cyrix, type 1 hypervisor)
- Secure Virtualization Software
  (Integrated with Trusted Operating System, hypervisor and OS = same)
- Trusted Boot
  (Cloud Stacks are rarely rebooted, still necessary? Yes!)

High Assurance Cloud (HAC) ???

- Remote Attestation
  (Possible in an elastic computing environment?)
- Virtualization Technology at this point yet?
- What would that even look like?


Private Cloud
Type 1 Hypervisor
Trusted OS with Type 2 HV
High Assurance VM
Low Assurance VM
Trusted OS with Type 2 HV
High Assurance VM
Low Assurance VM
Trusted OS with Type 2 HV
High Assurance VM
Low Assurance VM
Trusted OS with Type 2 HV
High Assurance VM
Low Assurance VM
Attestation Servers
Internet
High Assurance
Cloud Environment
??

Future Works

- Restructuring of the SSC Private Cloud
  - Windows Server 2012?
  - Physical infrastructure issues need to be resolved
- Build a larger cloud, supporting multiple cloud based research projects
- Need resources (switch, router, racks, rack mounted servers, physical location, AC/Power requirements)
- Build a smaller separate cloud for virtualized HAP workstations
- Integration of all components
- Testing, testing, and more testing

Questions or Comments?