Security

15-719/18-847b
Advanced Cloud Computing

Garth Gibson
Greg Ganger
Majd Sakr

Security readings

- Req: *The state of Public Infrastructure-as-a-Service Cloud Security*, Huang, Ganjali, Kim, Oh, and Lie, ACM Computing Surveys, 2015.
- Opt: *Hey, you get off of my cloud: exploring information leakage in third-party compute clouds*, Ristenpart, Tromer, Shacham, Savage, ACM Computer and Communications Security, 2009.
- Opt: *Security in the cloud*, Anthes, Communications of the ACM, 2010.

Public Infrastructure Cloud Services

- > $130B ?
- < 10 years
- Little VMM or stack diversity
- Data derived from Gartner 2013

Table II. Cloud Service Providers Surveyed

Service Provider	Launch Year	Hypervisor(s)
Verizon Cloud	2014	Xen/VMware
Google	2013	KVM
Savvis Direct	2012	Xen/VMware
HP Public Cloud	2012	KVM
Dimension Data	2011	VMware
Tier 3	2011	VMware
Microsoft Azure	2010	Custom(Hyper-V)
Fujitsu Trusted Public S5	2010	Xen
GoGrid Cloud Platform	2009	Xen
Joyent Compute/Manta Storage	2009	SmartOS
Amazon EC2/S3	2008	Xen
Rackspace Public Cloud	2008	Xen
SoftLayer	Unknown	Xen

[Huang15]

Survey state of art in IaaS security

- Consider IaaS cloud services, based on hypervisors & cloud environment software stacks (e.g. AWS, OpenStack)
- Consider attackers to be of two types:
  - Attacker runs on same machine, but not in cloud service provider (CSP)
  - Attacker has breached CSP on same or other machines in cloud services
- Security issues (Confidentiality, Integrity, Availability)
  - Customer/user data is protected, plus its existence & access patterns
  - Cloud service provider (CSP) provides correct and honest functions
    - Failure to meet Contract SLA (CS) is a security issue (some SLA goals are hard to verify, e.g. how reliable is my cloud data storage?)

Survey of Public IaaS CSP Offerings

[Huang15]

Table III. Summary of Areas where the IaaS Industry has Established Best-Practices

CSP	Hyper-visor	Fire-wall	Data-center Op.	Dedicated VM	Segre-gation	Crypto-Transit	Crypto-Rest	Auth	Delegation/ ACL	CSP security	Location Constraints	SLA	Bill
Amazon	✓	✓	✓	✓	✓	✓	Object	2 factor passwords SSO	Role-based	No spoofing	✓	✓	✗
Verizon	✓	✓	✓	✓	✓	✓	Object	2 factor passwords, PIN	Role-based	Not mentioned	✓	✓	✗
SavvisDirect	✓	✓	✓	✗	✓	✓	Object	Passwords Keystone (SSO)	Access with tokens	Not mentioned	✓	✓	✗
Rackspace	✓	✓	✓	✗	✓	✓	Block	Passwords Keystone (SSO)	Role-based	Not mentioned	✓	✓	✗
Azure	✓	✓	✓	✗	✓	✓	Block	Passwords Keystone (SSO)	Rest-API	Some	✓	✓	✗
DimensionData	✓	✓	✓	✗	✓	✓	Object	Passwords	Role-based	Not mentioned	✓	✓	✗
Tier 3	✓	✓	✓	✗	✓	✓	Object	Passwords REST	Create users	Not mentioned	✓	✓	✗
Joyent	✗	✓	✓	✗	✓	✓	✗	Password SSH Key	Sub users	Not mentioned	✓	✓	✗
Fujitsu	✓	✓	✓	✓	✓	✓	Block	Certificate based	Sub users	Mentioned as risk	✓	✓	✗
GoGrid	✓	✓	✓	✓	✓	✓	Block	Password/ API key	✗	Prevent spam	✓	✓	✗
SoftLayer	✓	✓	✓	✗	✓	✓	Block	Password, API key	Sub users Sub accounts	Not mentioned	✓	✓	✗
HP	✓	✓	✓	✗	✓	✓	Block	Password Keystone (SSO)	Sub users Sub accounts	Not mentioned	✓	✓	✗
Google	✓	✓	✓	✗	✓	✓	Block	Passwords, OAuth2	via OAuth2	Prevent spam	✓	✓	✗

CSP Security Mechanisms (inherited from pre-cloud)

- Systems
  - Hypervisor – Xen, KVM, VMWare, Hyper-V – maturing through use and abuse
  - Firewall – separate from VM to emulate separate hardware
  - Data center operations – best practice human/physical practices from hosting market
  - Dedicated VMs – virtual but not shared, sometimes offered (vs private cloud)
  - Corporate Segregation – usually protected from CSP's other business/staff
- Cryptographic
  - In transit – SSL/TLS, riding Web 2.0 technology (e.g. certificates)
  - At rest – does encryption at rest by CSP offer real protection? CSPs disagree
- Access control
  - Authentication – single sign on (SSO) service diversity (Oauth, Keystone, SAK, IAM)
  - User creation and ACLs – "file system like" plus time, IP address controls; disagreement on how constrained/delegatable/revocable ?

Security Mechanisms con't

- CSP Security – how transparent is CSP security of themselves?
  - Eg. IP address management; banned/blacklist of CSP IP protected
- CSP contract
  - Location of VM – country restrictions, geo-replication for avail/latency
  - SLAs – all vary price based on SLA availability, but few other properties
  - Billing – bytes/hours verify easily, compute quality not so much
    - Project 2 – multiple AZ when you didn't ask for costs more

Survey of Public IaaS CSP Offerings

[Huang15]

Table III. Summary of Areas where the IaaS Industry has Established Best-Practices

CSP	Hyper-visor	Fire-wall	Data-center Op.	Dedicated VM	Segre-gation	Crypto-Transit	Crypto-Rest	Auth	Delegation/ ACL	CSP security	Location Constraints	SLA	Bill
Amazon	✓	✓	✓	✓	✓	✓	Object	2 factor passwords SSO	Role-based	No spoofing	✓	✓	✗
Verizon	✓	✓	✓	✓	✓	✓	Object	2 factor passwords, PIN	Role-based	Not mentioned	✓	✓	✗
SavvisDirect	✓	✓	✓	✗	✓	✓	Object	Passwords Keystone (SSO)	Access with tokens	Not mentioned	✓	✓	✗
Rackspace	✓	✓	✓	✗	✓	✓	Block	Passwords Keystone (SSO)	Role-based	Not mentioned	✓	✓	✗
Azure	✓	✓	✓	✗	✓	✓	Block	Passwords Keystone (SSO)	Rest-API	Some	✓	✓	✗
DimensionData	✓	✓	✓	✗	✓	✓	Object	Passwords	Role-based	Not mentioned	✓	✓	✗
Tier 3	✓	✓	✓	✗	✓	✓	Object	Passwords REST	Create users	Not mentioned	✓	✓	✗
Joyent	✗	✓	✓	✗	✓	✓	✗	Password SSH Key	Sub users	Not mentioned	✓	✓	✗
Fujitsu	✓	✓	✓	✓	✓	✓	Block	Certificate based	Sub users	Mentioned as risk	✓	✓	✗
GoGrid	✓	✓	✓	✓	✓	✓	Block	Password/ API key	✗	Prevent spam	✓	✓	✗
SoftLayer	✓	✓	✓	✗	✓	✓	Block	Password, API key	Sub users Sub accounts	Not mentioned	✓	✓	✗
HP	✓	✓	✓	✗	✓	✓	Block	Password Keystone (SSO)	Sub users Sub accounts	Not mentioned	✓	✓	✗
Google	✓	✓	✓	✗	✓	✓	Block	Passwords, OAuth2	via OAuth2	Prevent spam	✓	✓	✗

Broader academic issues

- Attack targets
  - Cache channel – measure cache access time to deduce what data a co-resident victim code is touching (Ristenpart09)
  - Storage channel – even encrypted, shared storage access pattern can be inferred, unless real data “moves around”
  - Covert channels – conspiring VMs can hide communication using above
  - Image sharing – shared VM root images very useful, so dangerous
  - Leak prevention – hybrid apps split over different CSP/private clouds

Broader academic issues con't

- Integrity, Availability Issues
  - Proof of Possession/Retrieval – challenge/response statistical sampling
  - Storage Integrity – digital signature, P2P tests of mutation ordering
  - Compromised VMM – TPM HW hash of running code,
  - Hardened VMMs – reduce complexity/size of VMM code/API
  - Coping with VMMs – verifiable computation or homomorphic encrypt
- Contractual Issues – trusted auditors, proof of location by latency

Discussion of academic vs industry defenses [Huang15]

Table IV. Summary of comparison between academic and industry cloud security solutions.

Problem	Current Solutions and Results	Summary
Malicious or compromised CSPs	**Academia:** POR/PDP, hypervisor integrity, auditing **Industry:** Marketing	CSPs assume they are trusted and disclaim liability for damages due to security compromises. Academia serves an important role for identifying weaknesses in CSP security that would be hard for CSPs themselves to talk about publicly.
Cross-VM leakage, cache timing channels, covert channels	**Academia:** Evaluation of feasibility of attack, memory placement, deterministic execution **Industry:** Dedicated instances	Industry proposes dedicated instances. Main question is the value of this solution since it costs more for a dedicated instance. Academia could help by definitively establishing the feasibility of such attacks and the associated costs with mounting the attack.
Malicious VM images and leakage through VM images	**Academia:** Demonstrated the size and scope of the problem through measurement. **Industry:** Provide documentation and warnings to users.	A simple tool to detect leakage and malicious VMs has been constructed in academia. There is potential for a more comprehensive solution to solve this problem.
Hypervisor integrity and compromised hypervisors	**Academia:** Hypervisor hardening, using untrusted hypervisors, TPM-based remote attestation by customers. **Industry:** Hypervisor customizations and keeping hypervisor patched.	Direct TPM-based remote attestation by customers is of limited use due to use of industry use of customized hypervisors. Protecting against an untrusted hypervisor is the only viable solution against a malicious CSP.
Billing Integrity	**Academia:** Demonstrate attacks against billing integrity, auditing techniques to ensure that difficult to verify security properties of cloud service are upheld. **Industry:** Bill based on easily verifiable quantities.	Unfortunately, industry billing practice multiplies easily verifiable quantities with rates based on difficult to verify properties. There is potential for research into better auditing and metering techniques.

Attestation

- If you control original code in secure container and secure container signs a computation in secure container, then you are trusting manufacturer

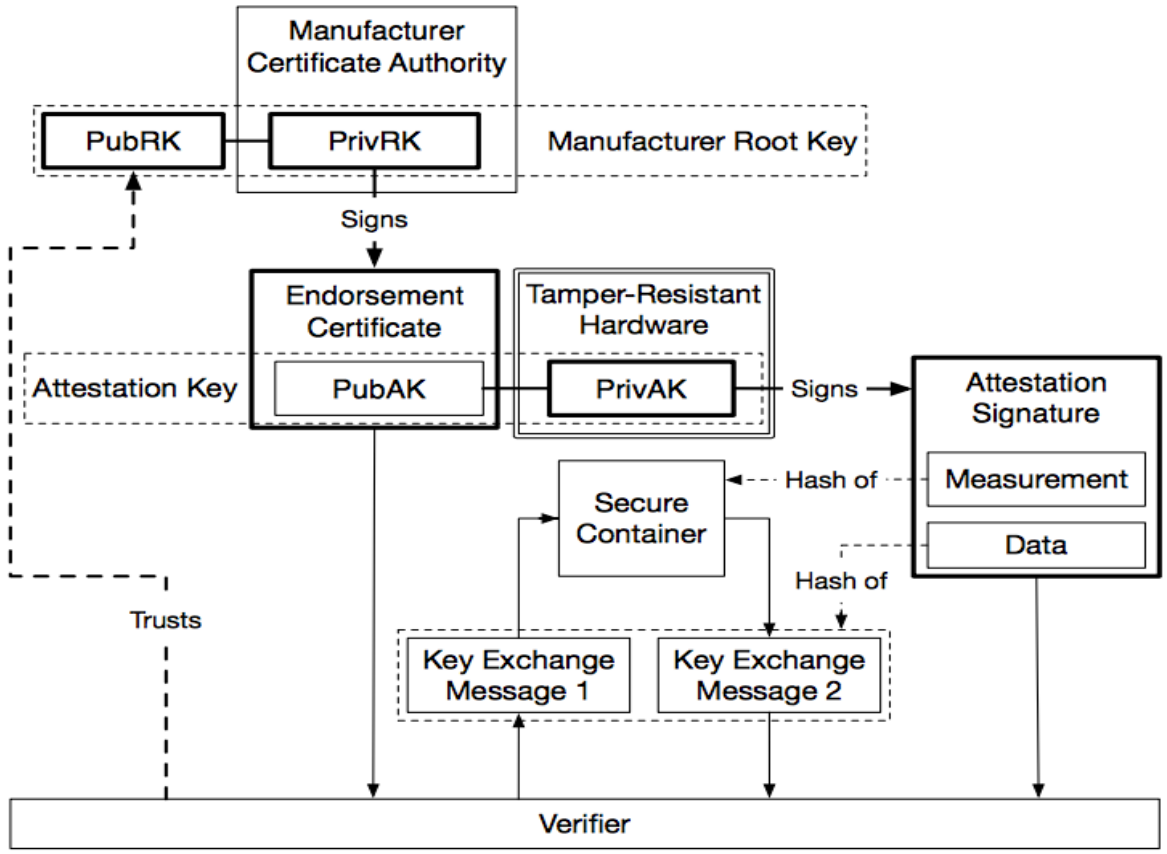


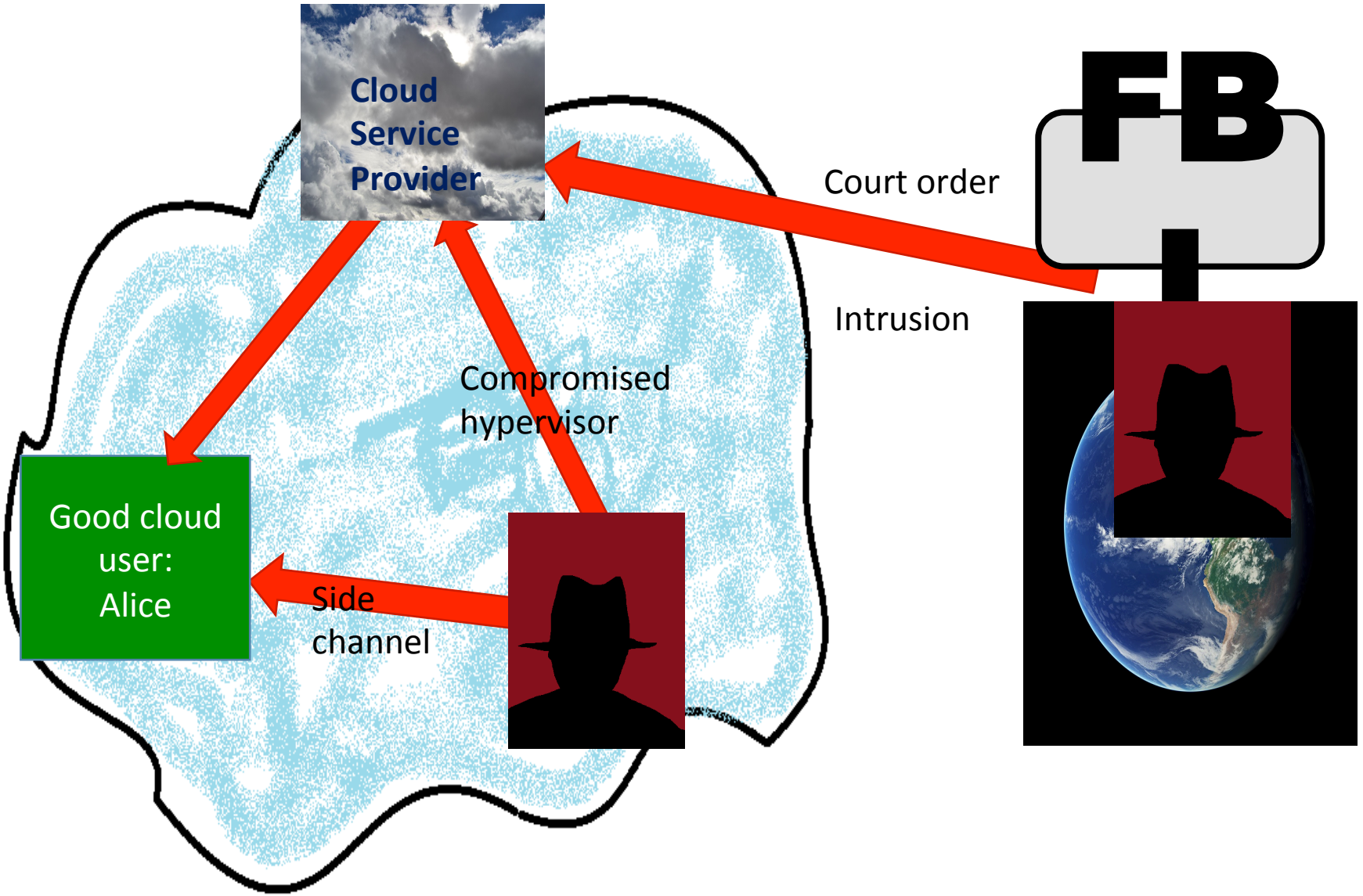
Figure 53: The chain of trust in software attestation. The root of trust is a manufacturer key, which produces an endorsement certificate for the secure processor's attestation key. The processor uses the attestation key to produce the attestation signature, which contains a cryptographic hash of the container and a message produced by the software inside the container.

[Costan16, IACR Cryptology]

Next day plan

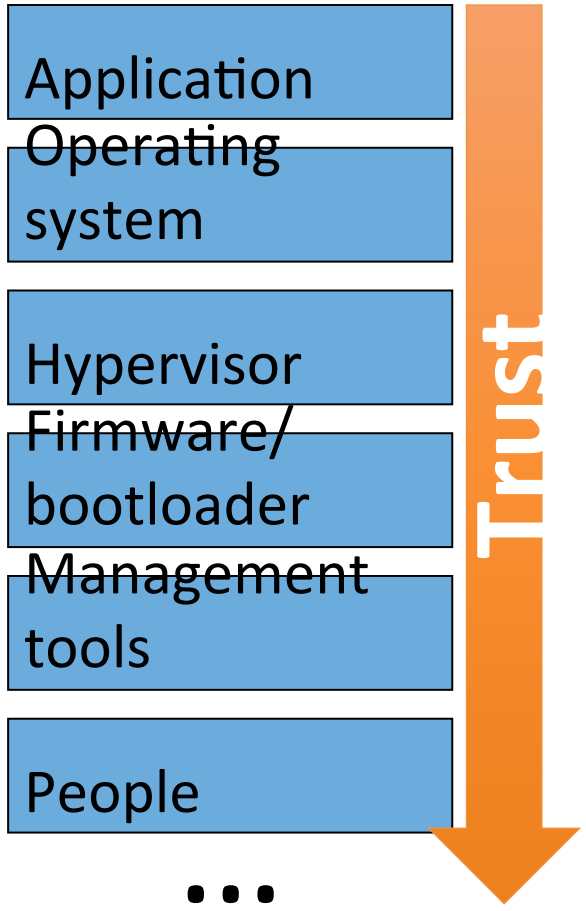
- Monday: Greg will talk about learning to love spot pricing
- Wednesday: Guest lecture on formal verification of cloud services
    - Bryan Parno, CMU
- Monday after: TBD
- Wednesday after: second midterm
    - Closed book, no electronics, one 8.5x11” cheat sheet allowed
    - In-class, sit with an empty sit on both sides of you
    - Topics covered include project 3 (scheduling) and all lectures after exam 1


Cloud Security
Marcus Peinado
Microsoft Research


Cloud
Service
Provider
FB
Court order
Intrusion
Compromised
hypervisor
Good cloud
user:
Alice
Side
channel

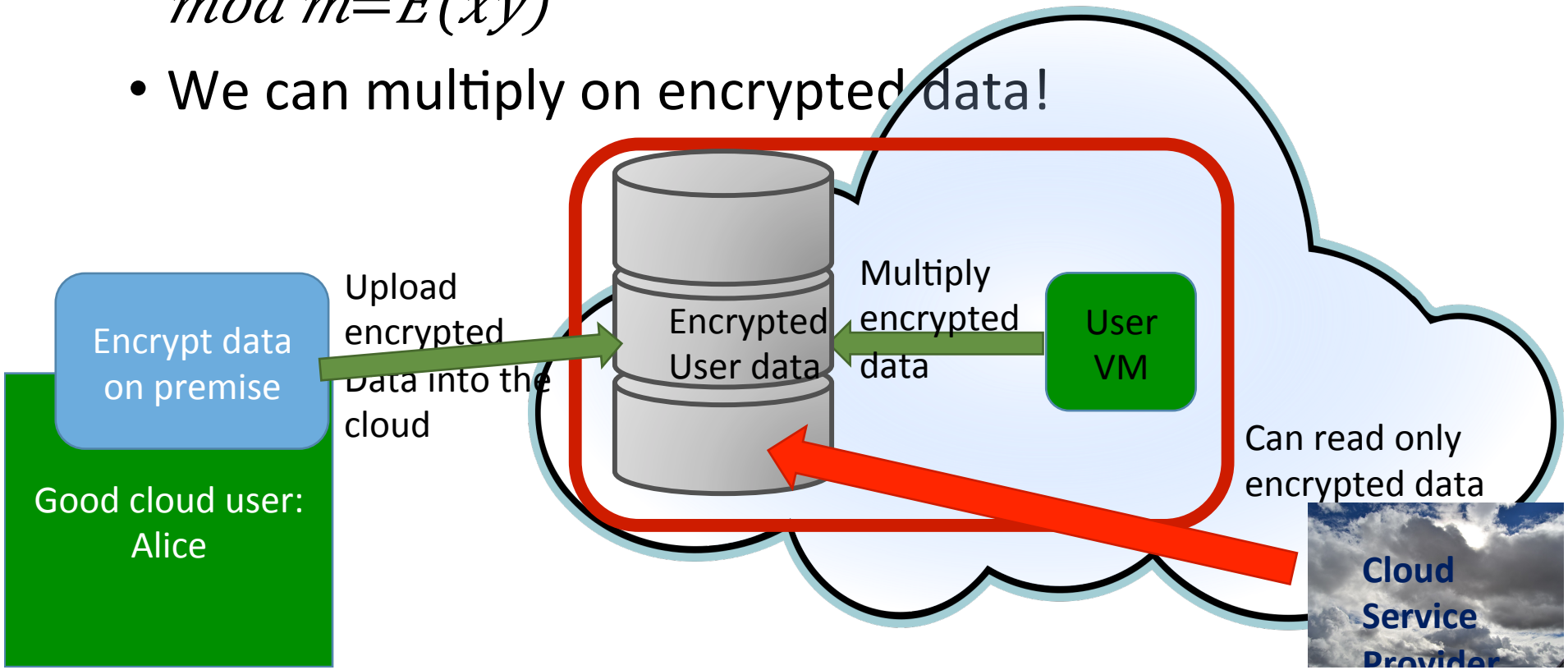
Can you trust the cloud?

- Huge trusted computing base
  - Privileged software
    - Hypervisor, firmware, ...
  - Management stack
  - Staff
    - Sysadmins, cleaners, security, …
  - Law enforcement
- Hierarchical security model
  - Observe or modify any data
  - Even if encrypted on disk / net



Homomorphic Encryption: Toy Example

- RSA encryption: $E(x)=x\uparrow e \mod m$
- $E(x)\cdot E(y)=(x\uparrow e \mod m)\cdot(y\uparrow e \mod m)=(xy)\uparrow e \mod m=E(xy)$
- We can multiply on encrypted data!



Fully Homomorphic Encryption (FHE)

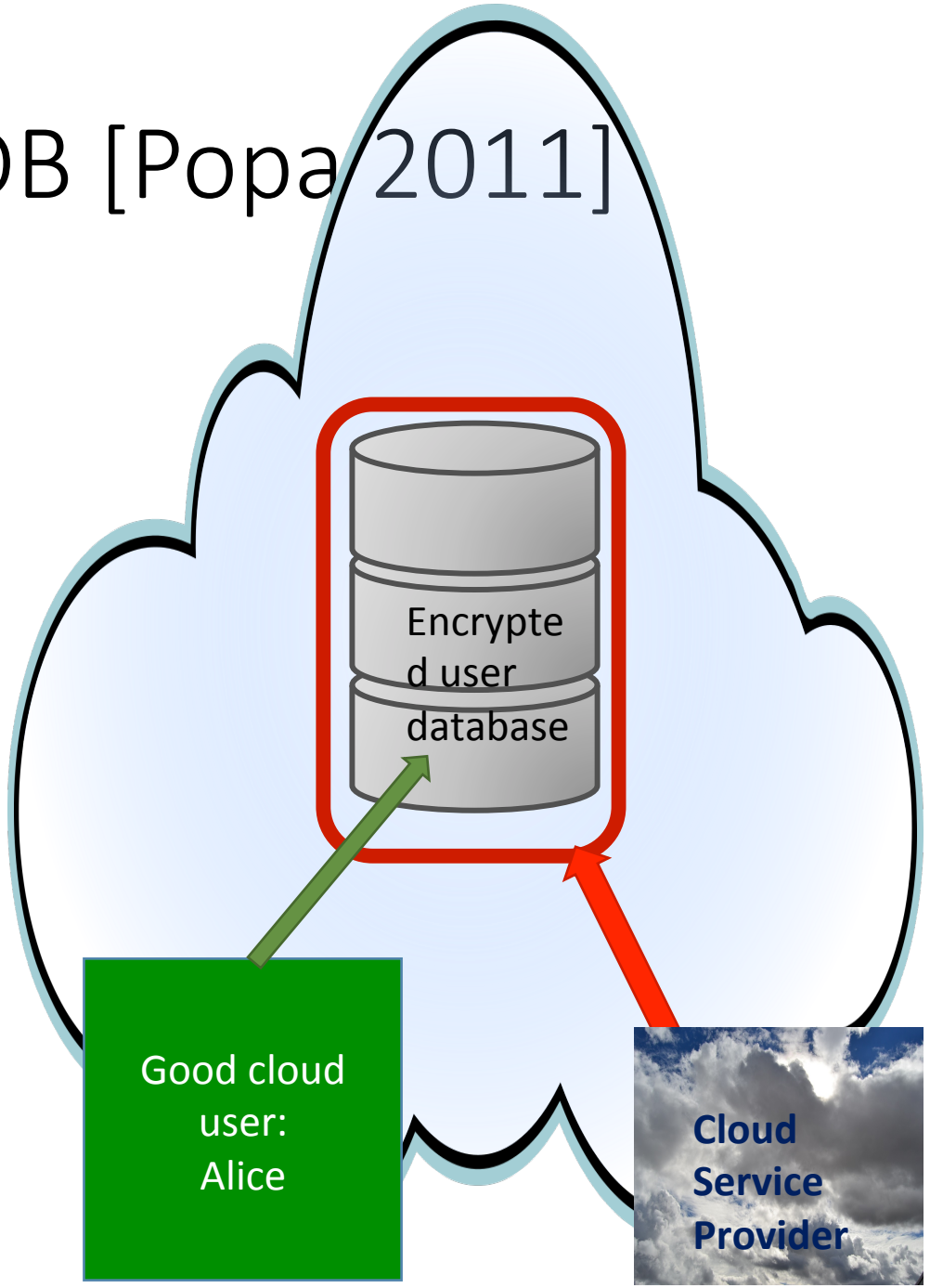
- Can we do more than just multiply?

- Yes. FHE systems can perform arbitrary operations on encrypted data [Gentry 2009].
- But they are very slow (at present)
  - Orders of magnitude slowdown

- Research directions
  - Can we reduce the overhead? (Crypto research)
  - Can we trade off functionality and security for speed?

Example: CryptDB [Popa 2011]

- SQL database that runs on encrypted data.
- DB systems perform only a limited set of operations on the data.
- Weaken encryption for some DB columns to enable interesting queries.



Encrypted Databases

SSN	Patient Name	Age	diagnosis	doctor's comments
xz6f73bdfk	4jruaiu B4ur8w	kjewh	dsasdfs	kljaenfja al ksdfisegj iooi aoeiwrg ioj[erg jioaergj io
45geio809d	jdjncks 7832ibhe	;kds	ghfgh	df,adsmkladfkl slkjdn lkjdf ndkfu isdfdiufuiasds sd
kf9sh23kdfb	kwjek 9e89cjf	rur8f	dsfadf	df,adsmkladfklsfg slkjdn lkjdf ndkfu isdfdiufuiasds sd
8dnklsdjfb3	9r09f 90sd9f	98udc	hghj	tghtrstghfg rweakosaen ser wer ert24rt gwyew5y
dwom58anb	0j98fi0f ikdfm90er	;kds	fgdfg	w545425 456 567 56g wrt bgh rt ert bw5b th wey55by
h698sab4kld	pwoe0 9fuwe	890uefw	ythhgfdg	eoir vwer wrety 67 7iwt w454 34 74t t drjksd fg re ge

Select * from PatientRecords where **SSN = dwom58anb**

Need ***deterministic encryption*** for columns used in simple filters.

This may leak some information.

Select * from PatientRecords where **Age > rur8f**

Need ***order-preserving encryption (OPE)*** for columns used in range queries.

This leaks more information.

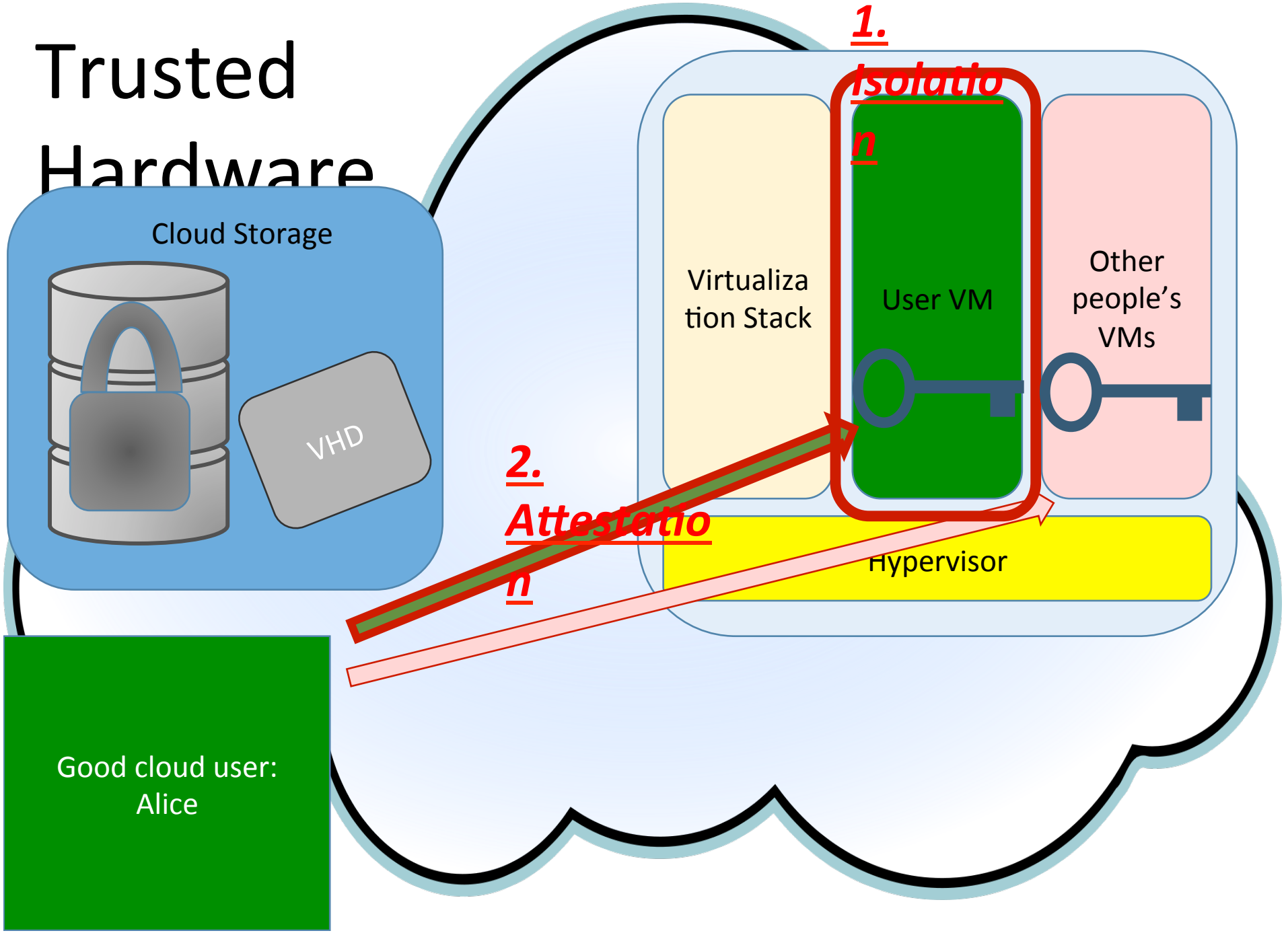
Select * from PatientRecords

If no query depends on a column then we can encrypt it at full strength.

Trusted Hardware

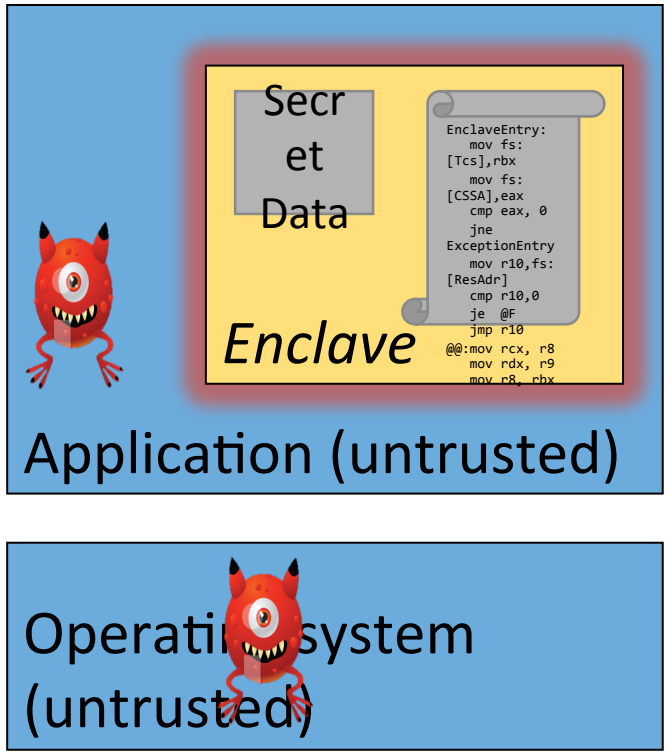
- Assume special hardware features.
- Then we can run regular programs at native speed.
- And the CSP cannot access our data.

Trusted Hardware

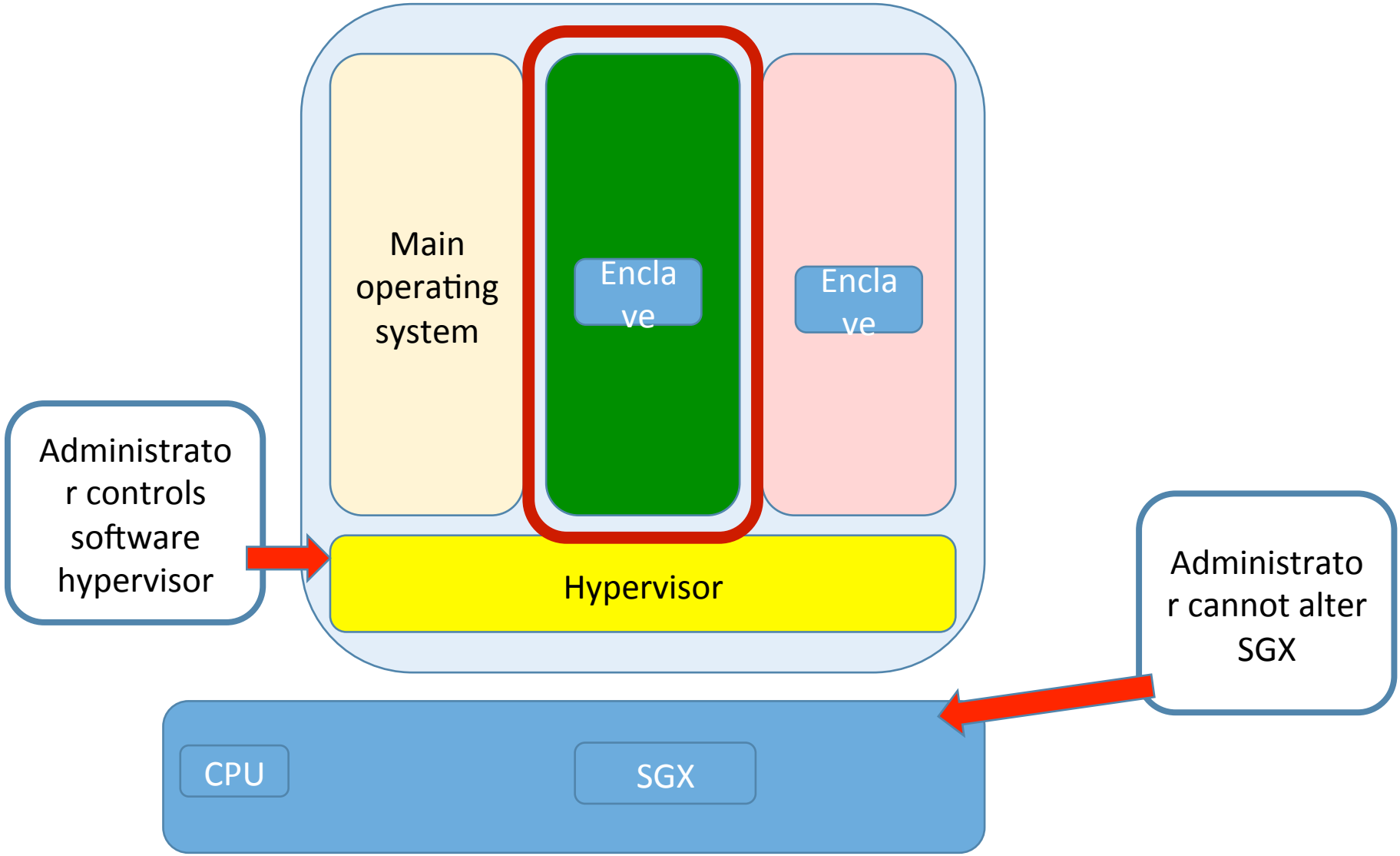


Intel SGX

- Hardware isolation for an *enclave*
  - New instructions to establish, protect
  - Call gate to enter
- Attestation
- Available in the most recent Intel CPUs (Skylake).
  - Only client processors

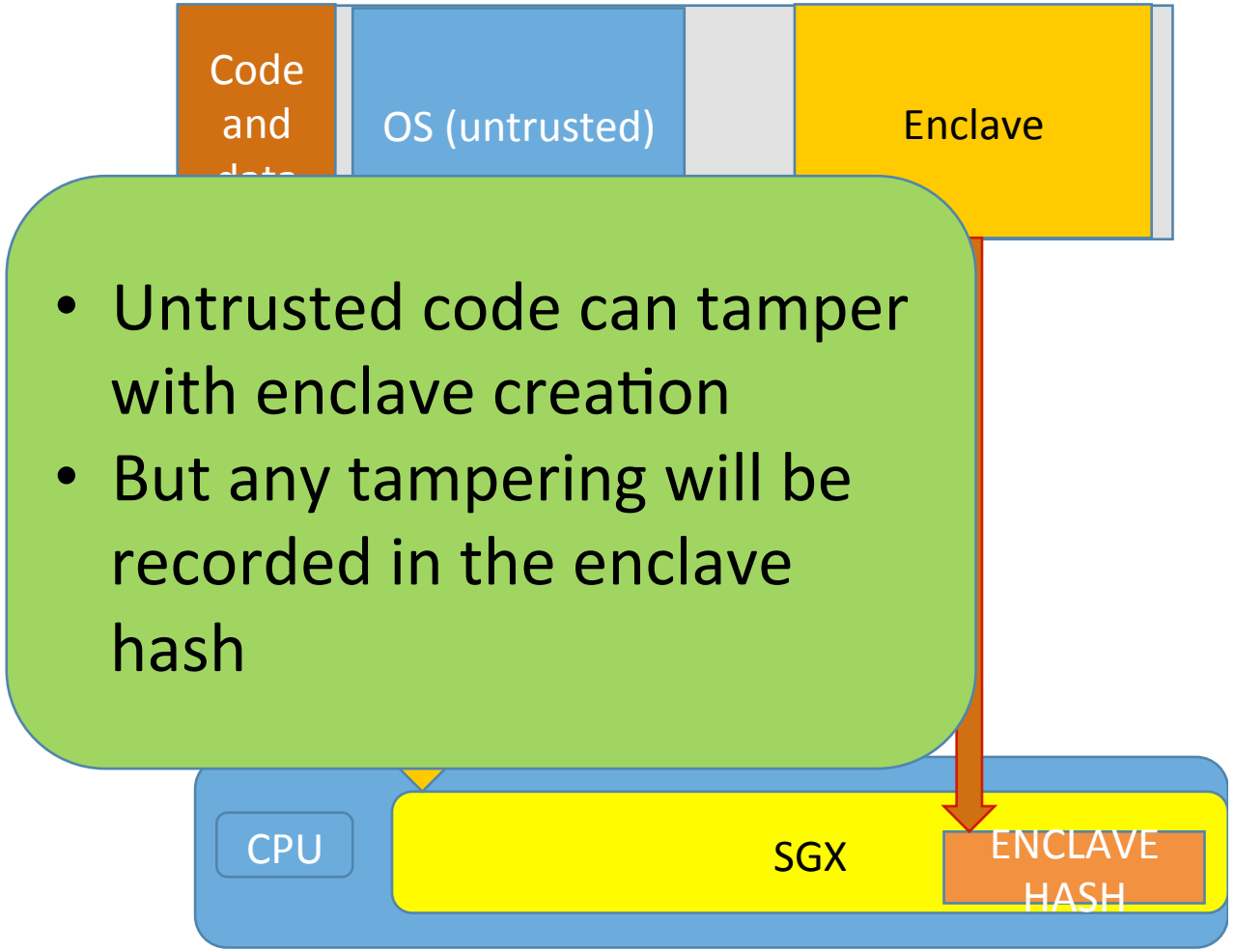


SGX: Isolation (conceptually)



Initialization: Building an Enclave

- Enclaves are built by untrusted code.
  - Enclave code
  - Enclave data
- CPU/SGX records enclave hash.



Enclave Software

- Can run arbitrary code in enclaves.
- Challenges:
  - External dependencies: Cannot trust the system beyond the enclave boundaries.
  - Only Ring 3 (user mode): Hard to run a VM/OS this way.
- First results:
  - Haven [Baumann 2014]: Arbitrary Windows applications.
  - VCCC [Schuster 2015]: Hadoop

Trusted Hardware: Problems

- No SGX hardware available
- SGX does not support VMs
- Limitations
- Still have to trust
  - An entire CPU
  - Intel Corporation
  - Manufacturing plant
- Compromised attestation keys
- Hardware attacks