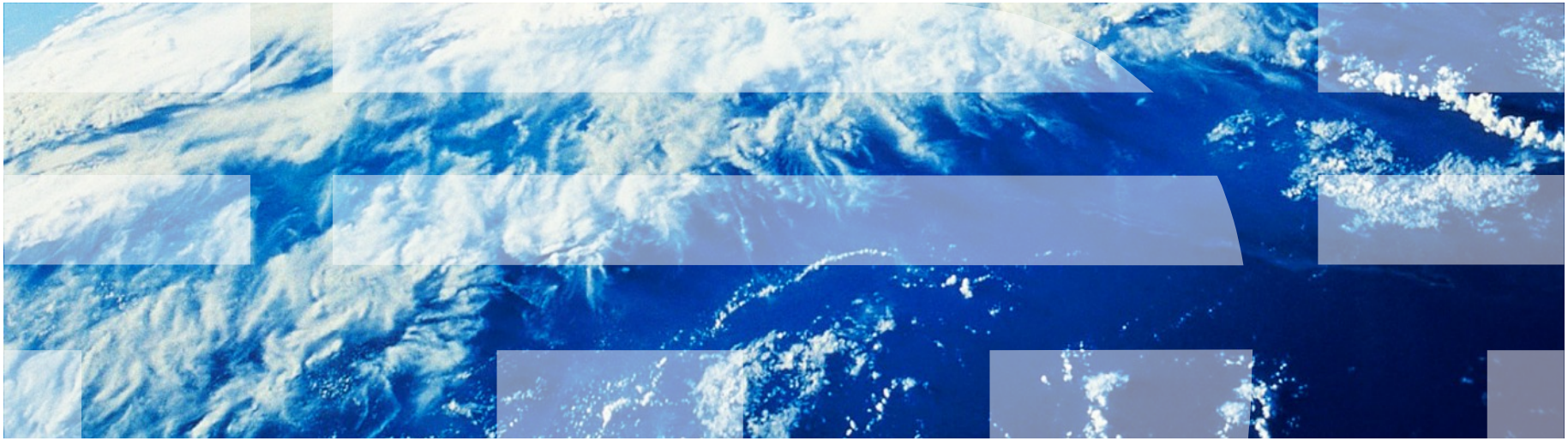
Dr. Michael Waidner, IBM Distinguished Engineer
CTO Security for IBM
wmi@us.ibm.com

IBM

Security and Cloud Computing



Disclaimer

This document represents the author's views and opinions.

It does not necessarily represent IBM's position or strategies.

1. Information Security and Cloud Computing
2. Providing a Secure Cloud
3. Using a Cloud Securely
4. Cloud-delivered Security Services
5. Areas for Research

Chapter 1

Information Security and Cloud Computing

Information Security Risk Management

Threat (and Attack)
Malicious / Accidental
Insider / Outsider

Vulnerability

Resources

Identities
Information
Applications
IT Infrastructure
Physical infrast.

Objectives

Confidentiality
Integrity
Availability
Accountability
(Manageability)

Potential insecurity
Potential loss for a party
Yields risk

Parties Concerned

Provider, subscriber,
end-user, ...,
government

Risk management

Acceptance
Avoidance
Transfer
Mitigation

Risk is estimated based on statistical assumptions, and those are changing over time.
Each party needs to manage *their* risk towards an *acceptable* level (multi-party security)
The residual risk is never zero, there is no absolute security.

Threat Trends

[IBM 10, OWASP 10]

- **Attacks are increasingly economically or politically motivated**
  - Motivates focus on cybersecurity / protecting cyberspace & critical infrastructures
- **The weakest link determines overall risk**
  - Malware (virus, worms, trojans) and phishing
  - Insecure out-of-the-box configurations, cryptic interfaces, standard passwords
  - Attack sophistication is increasing
    - Focus is constantly moving up, from network/OS to application threats
    - Distributed denial-of-service attacks (DDoS)
    - Bot-nets (for DDoS, Spam, etc.)
    - Slow Attacks (prepared over years, combining many elements)
    - Advanced Persistent Threat (ATP; focused, ongoing, resourceful intelligence)
- **Insiders are major source of insecurity**
    - Mostly accidental (“I need to work around security”, trivial password, lost laptop, …)
    - Privileged insiders, e.g., administrators, assistants, management
    - Employees who change role but keep privileges
    - Ex-employees whose access does not get revoked

OWASP Ten Most Critical Web Application Security Risks

OWASP Top 10 – 2010 (New)
A1 – Injection
A2 – Cross Site Scripting (XSS)
A3 – Broken Authentication and Session Management
A4 – Insecure Direct Object References
A5 – Cross Site Request Forgery (CSRF)
A6 – Security Misconfiguration (NEW)
A7 – Failure to Restrict URL Access
A8 – Unvalidated Redirects and Forwards (NEW)
A9 – Insecure Cryptographic Storage
A10 - Insufficient Transport Layer Protection

Source: [OWASP 10]

Cloud Threats

External Threats

Web app vuln's

SOA

Network vuln's
Malware
Force majeur

Empowered end-users

Co-tenants

...

Multi-tenancy / Virt

Cloud Management

Cloud Data Center

Cloud insiders, "privileged users"

Network, server, middleware, app vuln's, physical & organizational threats

New sources of threats

- Co-tenants
- Empowered end-users
- Cloud insiders (½ new)

New technologies

- Physical-to-virtual: Multi-tenancy, virtualization
- Cloud mgmt: co-management of security, self-service
- Web 2.0-ish cross-domain SOA

[Gass 88, Goldberg 74]

At the core this is all well known
Many system aspects do not change at all
But: many new details and constraints

Security Remains the Top Concern for Cloud Adoption

80%

Of enterprises consider security the #1 inhibitor to cloud adoptions

48%

Of enterprises are concerned about the reliability of clouds

33%

Of respondents are concerned with cloud interfering with their ability to comply with regulations

*"**How can we be assured that our data will not be leaked** and that the vendors have the technology and the governance to **control its employees from stealing** data?"*

*"**Security is the biggest concern.** I don't worry much about the other "-ities" – reliability, availability, etc."*

*"**I prefer internal cloud to IaaS. When the service is kept internally**, I am more comfortable with the security that it offers."*

Source: Driving Profitable Growth Through Cloud Computing, IBM Study (conducted by Oliver Wyman)

Specific Customer Concerns Related to Security

Protection of intellectual property and data	**30%**
Ability to enforce regulatory or contractual obligations	**21%**
Unauthorized use of data	**15%**
Confidentiality of data	**12%**
Availability of data	**9%**
Integrity of data	**8%**
Ability to test or audit a provider's environment	**6%**
Other	**3%**

Source: Deloitte Enterprise@Risk: Privacy and Data Protection Survey

Top Security Threats and Risks

Gartner: Top Risks (2008)
- Privileged user access
- Regulatory compliance
- Data location
- Data segregation
- Recovery
- Investigative support
- Long-term viability

[Heiser 09]

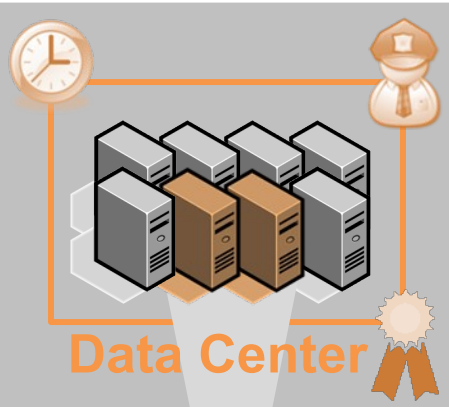
ENISA: Top Security Risks (2009)
- Loss of governance
- Lock-in
- Isolation failure
- Compliance risks
- Management interface compromise
- Data protection
- Insecure or incomplete data deletion
- Malicious insider

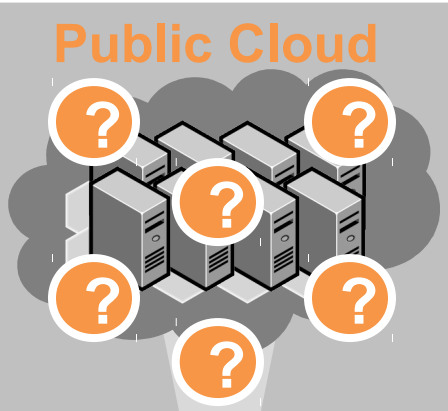
[ENISA 09/a]

CSA: Top Threats (2010)
- Abuse and nefarious use of cloud
- Insecure interfaces and APIs
- Malicious insiders
- Shared technology issues
- Data loss or leakage
- Account or service hijacking
- Unknown risk profile

[CSA 10]

Why is Cloud Security Perceived as Such a Big Problem?





We Have Control

It's located at X.
It's stored in server's Y, Z.
We have backups in place.
Our admins control access.
Our uptime is sufficient.
The auditors are happy.
Our security team is engaged.

Who Has Control?

Where is it located?
Where is it stored?
Who backs it up?
Who has access?
How resilient is it?
How do auditors observe?
How does our security team engage?

- Loss of control, perceived or real
- Lack of experience
- No established standards
- Uncertainty on how to interpret regulations and practices

- Effects
  - Public clouds rarely used for mission critical workloads
  - Preference for application-as-a-service
  - Preference for private and hybrid cloud

Cloud computing also provides the opportunity to *simplify* security controls and defenses

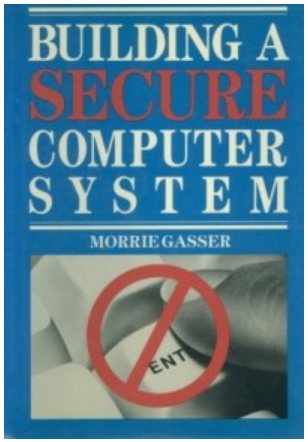
	Cloud Enabled Control(s)	Benefit
People and Identity	• Defined set of cloud interfaces • Centralized repository of Identity and Access Control policies	• Reduced risk of user access to unrelated resources.
Information and Data	• Computing services running in isolated domains as defined in service catalogs • Default encryption of data in motion & at rest • Virtualized storage providing better inventory, control, tracking of master data	• Improved accountability, Reduced risk of data leakage / loss • Reduced attack surface and threat window • Less likelihood that an attack would propagate
Process & Application	• Autonomous security policies and procedures • Personnel and tools with specialized knowledge of the cloud ecosystem • SLA-backed availability and confidentiality	• Improved protection of assets and increased accountability of business and IT users
Network Server and Endpoint	• Automated provisioning and reclamation of hardened runtime images • Dynamic allocation of pooled resources to mission-oriented ensembles	• Reduced attack surface • Improved forensics with ensemble snapshots
Physical infrastructure	• Closer coupling of systems to manage physical and logical identity / access.	• Improved ability to enforce access policy and manage compliance

Building a Secure Computer System

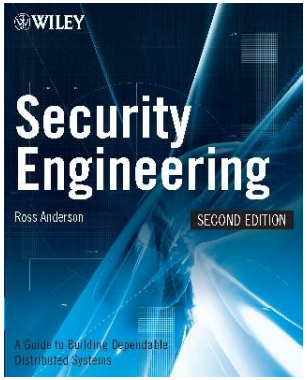
"There is nothing new under the sun
but there are lots of old things we don't know."

Ambrose Bierce, The Devil's Dictionary

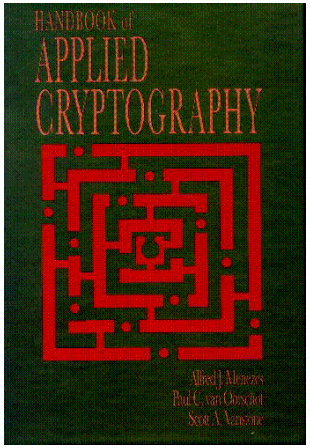
http://www.acsac.org/secshelf/book002.html



http://www.cl.cam.ac.uk/~rja14/book.html



http://www.cacr.math.uwaterloo.ca/hac/



Plus many other good text books.
(But you can download and read these 3 for free; Anderson's in a back-edition.)

Security Mechanisms (Controls)

Security Policy

- Enterprise, identity, access, retention, …
- Ideally derived and propagated top down
- Allow/deny + mandates/ obligations
- Often composite, mandatory and discr.
- Abstract, role based, class based

Security Development

- Practices
- Security testing
- Eg, OWASP

[Allan 10]

Prevention (Avoidance, Enforcement)	Detection (Monitoring, Audit)	Compensation (Recovery, Fail-over)

Cryptography

- Encryption
- Key management
- Channel security, VPN
- MAC, Hash
- Digital Signatures
- Message security

Redundancy

- Fault tolerance
- Backup & recovery
- Fail-over, graceful degradation

Access Control

- Reference monitor
- Authorization
- Data / proc tagging
- Hypervisor
- Memory protection
- Filesystem protection
- Virtual LAN

Intrusion / Extrusion Prevention

- Firewall
- Anti-virus, anti-malware
- Intrusion prevention
- Data leak prevention
- Virtual patching

Intrusion & Fraud Detection

- Signature-based
- Behavior-based
- Server, network based

Identity

- Authentication
- Identity Management

Trusted Computing

- Enforcement through (mutually) trusted hardware

Logging & Auditing

- Immutable logs
- Time stamping

Asset Management
Change and Configuration Management
Physical and Organizational Security

IBM Security Blueprint Overview

Architectural Principles

IBM Security Framework: Business Security Reference Model

- Governance, Risk, Compliance (GRC)
- People & Identity
- Data & Information
- Application & Process
- IT Infrastructure: Network, Server, End Point
- Physical Infrastructure

Foundational Security Management

- Software, System & Service Assurance
- Identity, Access & Entitlement Mgmt
- Data & Information Protection Mgmt
- Threat & Vulnerability Management
- IT Service Management
- Command and Control Mgmt
- Security Policy Management
- Risk & Compliance Assessment
- Physical Asset Management

Security Services and Infrastructure

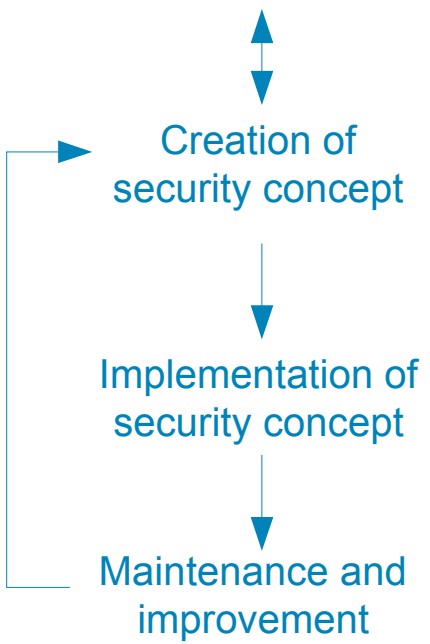
- Security Info and Event Infrastructure
- Identity, Access & Entitlement Infrastructure
- Security Policy Infrastructure
- Cryptography, Key & Certificate Infrastructure
- Network Security
- Storage Security
- Host and End-point Security
- Application Security
- Service Management and Process Automation
- Physical Security
- IT Security Services and Mechanisms

Security Service Level Objectives	Code & Images / Designs	Policies / Configuration Info and Registry	Identities & Attributes / Resources	Contexts / Data	Security Events & Logs / Knowledge

[Buecker 09]

Information Security Process and Management System

- Security is a *dynamic and evolving* property.
- *Risks* are managed through *controls (safeguards),* which need to be *continuously managed.*



- Strategy, objectives (internal, regulatory)
- Organization, resources, education

- Scope
- Documented security policy
- Threat analysis and risk decisions
- Safeguards and controls
  - Security Policy
  - Organization of Information security
  - Asset Management
  - Human Resource Security
  - Physical and Environmental Security
  - Communications and Operations Management
  - Access control
  - Information Systems Acquisition Development and Maintenance
  - Information Security Incident Management
  - Business Continuity Management
  - Compliance

[BSI 100-2, ISO 27002]

- *Mostly about risks and threats, the organization, policy, service management (in particular: asset, change management).*
- *Core technical security capabilities are a relatively small, although important, part of the story.*
- *Supported by studies on "foundational controls."*

Information Security Certification and Audit

"Trust is good, control is better."
Attributed to: Vladimir Ilyich Lenin

"My job is not security,
my job is making sure we pass the audit."
Anonymous CISO

- Internal and external, always organizationally independent
- Three major frameworks for security audit
  - Payment Card Industry Data Security Standard (PCI DSS)
    - Fairly prescriptive. Meant specifically for protecting card holder data.
  - ISO/IEC 27001 (BSI-Standard 100)
    - Technology neutral, but ISO 2700x provides strong security context.
  - Statement on Auditing Standard (SAS) No. 70, Type II
    - Very open, meant for service providers operating transaction systems, and de-facto standard framework for IT outsourcing.
  - Typically significant leeway for auditors
- Related but not yet relevant for cloud computing outside government context
  - Common Criteria Certification

Information Security Process and Management System

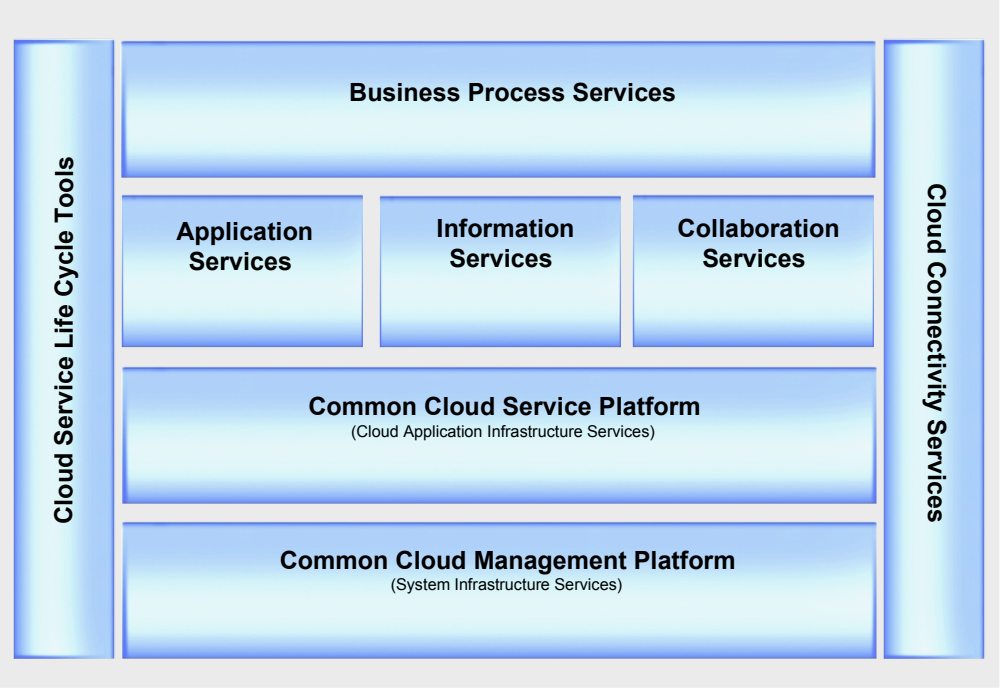
Information Security Risk Management requires

- Policy and Process
- Service Management and IT Governance
- People and Organization
- Education and Incentives
- Measurement and Reporting

Our focus:

- And Security Technology

IBM Common Cloud Platform

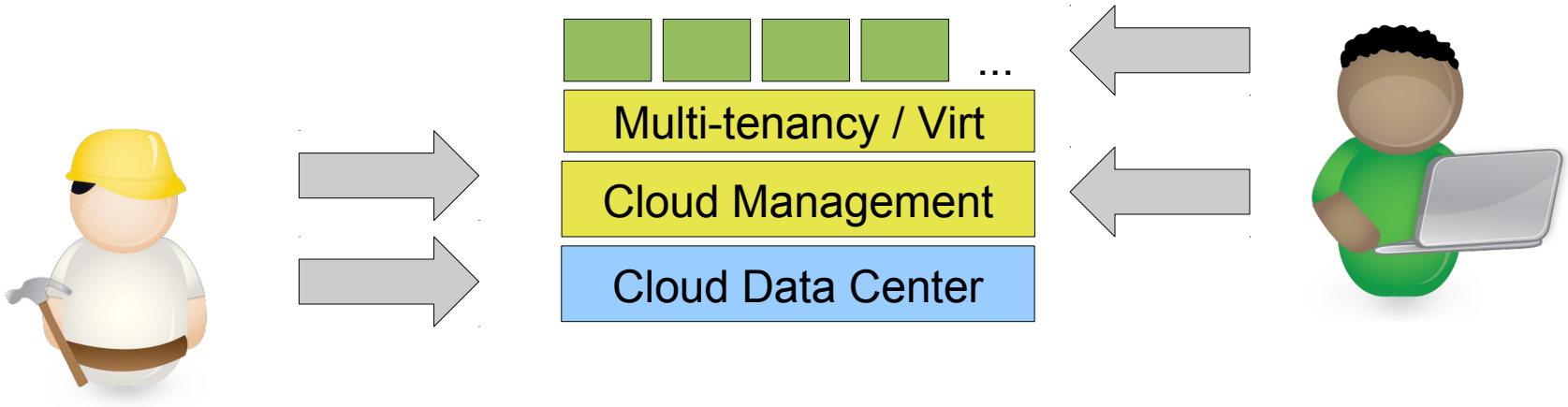


Each of these boxes requires a security architecture and design.

90% standard security engineering, like what one would do for a shared data center.

We will focus only on a few and fairly cloud-specific aspects.

Structure for Following Chapters



Chapter 2
Provider perspective:
Who to provide a secure cloud service?

Chapter 3
Subscriber perspective:
How to select a cloud?
Who to use a cloud securely?

Chapter 4
Security as a Service

Chapter 5
Research topics

References & Reading List: General Information Security

- [Allan 10] Allan, D., Hahn, T., Szakal, A., Whitmore, J. and Buecker, A. Security in Development: The IBM Secure Engineering Framework. IBM RedGuide, New York, 2010.
- [Anderson 08] Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems (2nd ed). Wiley, Indianapolis, 2008.
- [Bishop 02] Bishop, M. Computer Security, Art and Science. Addison-Wesley, Boston, 2002.
- [BSI 100] BSI-Standard 100-1-4. IT Grundschutz. Bundesamt für Sicherheit in der Informationstechnik, Bonn, 2009.
- [Buecker 09] Buecker, A. et. al. Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security. IBM RedGuide, New York, 2009.
- [Cheswick 03] Cheswick, W., Bellovin, S. and Rubin, A. Firewalls and Internet Security: Repelling the Wily Hacker (2nd ed). Addison-Wesley, 2003.
- [Crawford 10] Crawford, S. High Performers and Foundational Controls: Building a Strategy for Security and Risk Management. EMA White Paper, 2010.
- [Gasser 88] M Gasser: Building a Secure Computer System. Van Nostrand Reinhold, New York, 1988.
- [Goldberg 74] Goldberg, R. P. Survey of Virtual Machine Research. IEEE Computer June. 1974, pp 34-45.
- [IBM 10] IBM X-Force 2009 Trend and Risk Report. IBM, Armonk, February 2010.
- [ISO 27001] ISO/IEC 27001. Information Security Management System. ISO 2005.
- [McGraw 06] McGraw, G. Software Security: Building Security In. Addison-Wesley, 2006.
- [Menezes 96] Menezes, A., van Oorschot, P. and Vanstone, S. Handbook of Applied Cryptography. CRC Press, 1996.
- [OWASP 10] OWASP Top 10 – 2010. The Ten Most Critical Web Application Security Risks. OWASP Foundation, 2010.
- [Stallings 10] Stallings, W. Network Security Essentials: Applications and Standard (4th ed). Prentice Hall, Upper Saddle River, 2010.

References & Reading List: General Cloud Security

- [CSA 10] Top Threats to Cloud Computing. Cloud Security Alliance (CSA), 2010.
- [ENISA 09] Cloud Computing: Benefits, Risks and Recommendations for Information Security. European Network and Information Security Agency (ENISA), 2009.
- [ENISA 09a] Cloud Computing Information Assurance Framework. European Network and Information Security Agency (ENISA), 2009.
- [Heiser 09] Heiser J. and Nicolett M. Assessing the Security Risks of Cloud Computing. Gartner Research, 2008
- [IBM 09] IBM Point of View: Security and Cloud Computing. IBM, New York, 2009.
- [Jericho 09] Cloud Cube Model: Selecting Cloud Formations for Secure Collaboration. The Jericho Forum, 2009.
- **[Mather 09] T. Mather, S. Kumaraswamy, S. Latif. Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. O'Reilly, Gravenstein, 2009.**
- [Mell 09] Mell, P. and Grance, T. Effectively and Securely Using the Cloud Computing Paradigm. In ACM Cloud Computing Security Workshop, Chicago, 2009.

Chapter 2

Providing a Secure Cloud

(The cloud provider's perspective)

Outline

- **Responsibilities of Provider and Subscriber**
- **Isolation and Integrity Management**
  - Multi-tenancy
  - Hypervisor-level security services
  - Fully homomorphic encryption (outlook)
- **Identity Management**
  - Managing privileged users
  - On-/off-boarding of users, federated identity

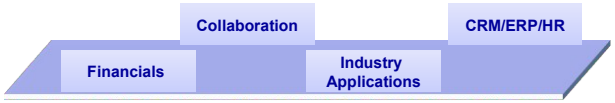
Outline

- **Responsibilities of Provider and Subscriber**

- **Isolation and Integrity Management**
  - Multi-tenancy
  - Hypervisor-level security services
  - Fully homomorphic encryption (outlook)
- **Identity Management**
  - Managing privileged users
  - On-/off-boarding of users, federated identity

Responsibilities of Provider and Subscriber

Business Process-as-a-Service



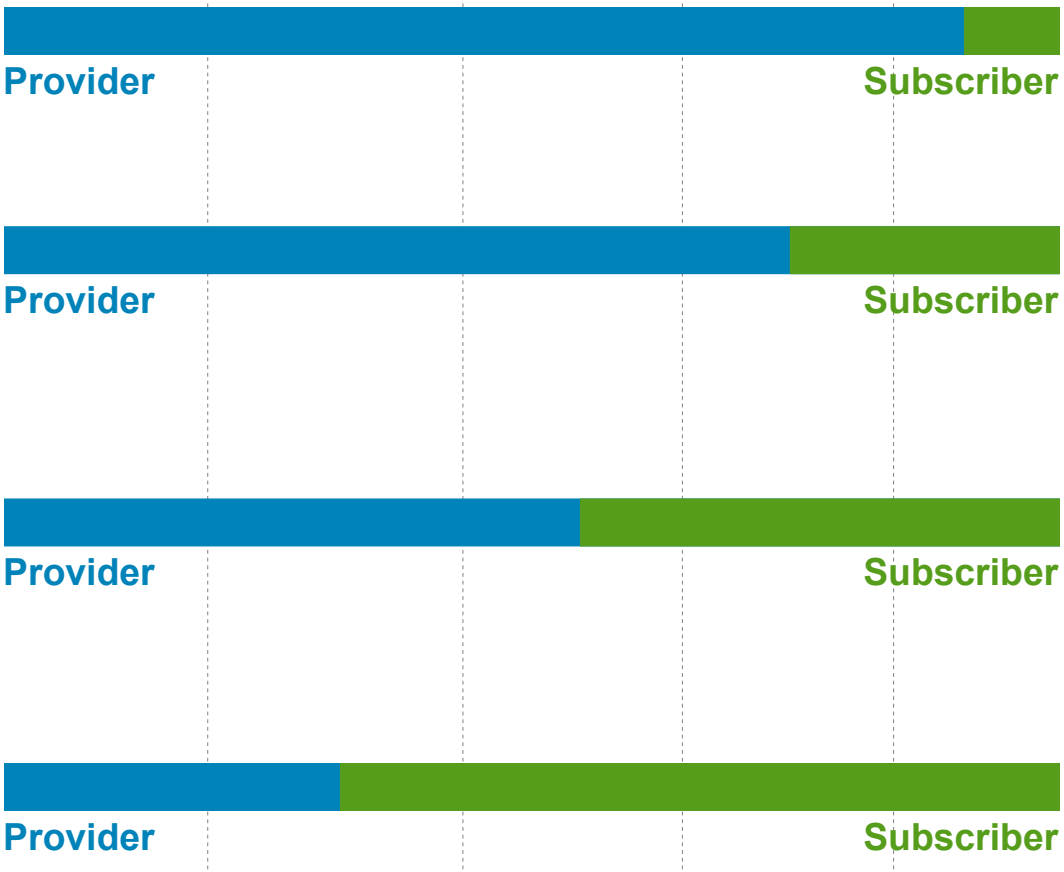
Application-as-a-Service

Platform-as-a-Service

Infrastructure-as-a-Service

Who is responsible for security at the … level?

Datacenter	Infrastructure	Middleware	Application	Process

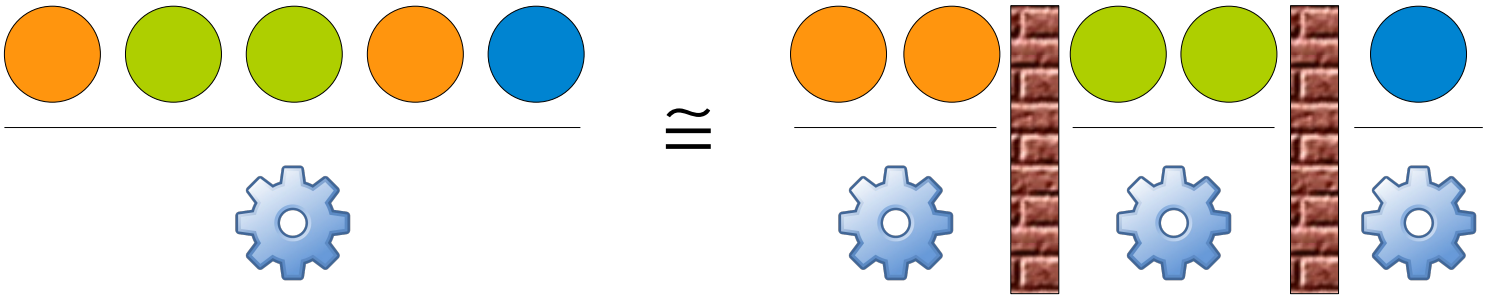


Outline

- Responsibilities of Provider and Subscriber
- **Isolation and Integrity Management**
  - Multi-tenancy
  - Hypervisor-level security services
  - Fully homomorphic encryption (outlook)
- Identity Management
  - Managing privileged users
  - On-/off-boarding of users, federated identity

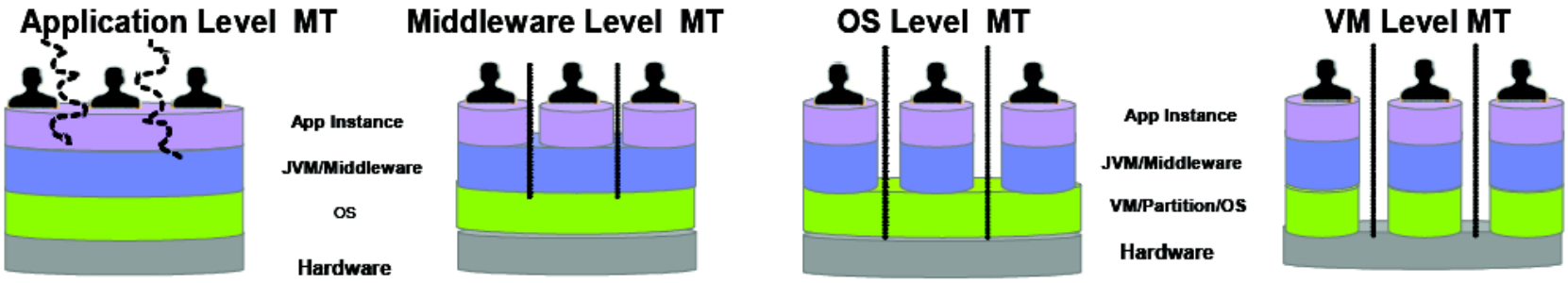
Isolation and Integrity Management: Multi-tenancy

- Users from *different* trust domains are drawing on a *shared* pool of resources
  - Network, storage and server virtualization
  - Shared file system, database, middleware, application, desktop, business service, ...
  - Stack architectures offer choices for implementing multi-tenancy (lower or higher in the stack)
  - Isolation is the key security requirement
- Basic mechanism is *coloring* (aka *tagging, labeling*) and enforcement of isolation between *domains* (aka *zones*) of different colors

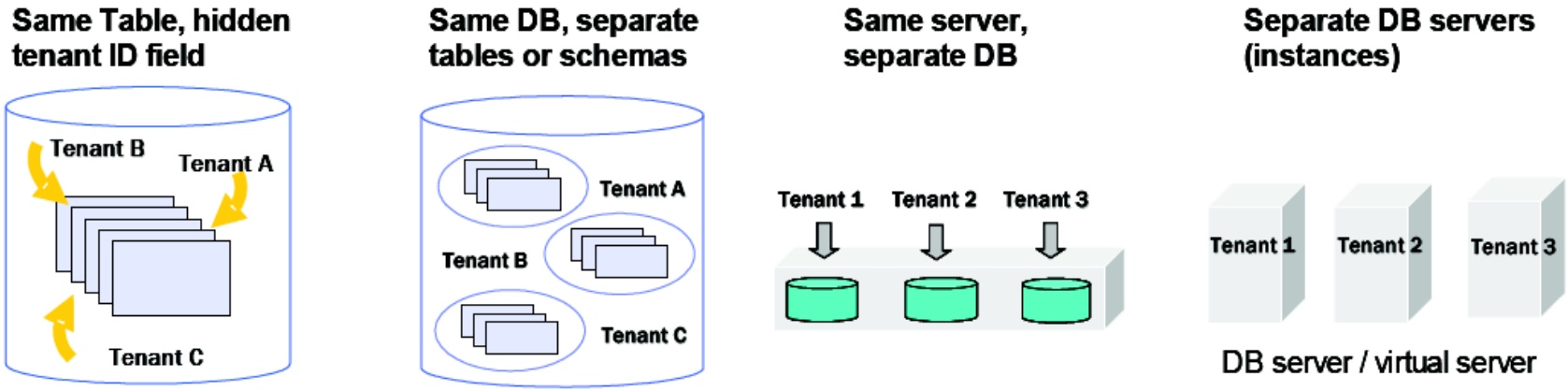


  - Enforcement through
    - Reference Monitor: provisioning, runtime, de-provisioning / cleanup
    - Cryptography (encryption, key management)

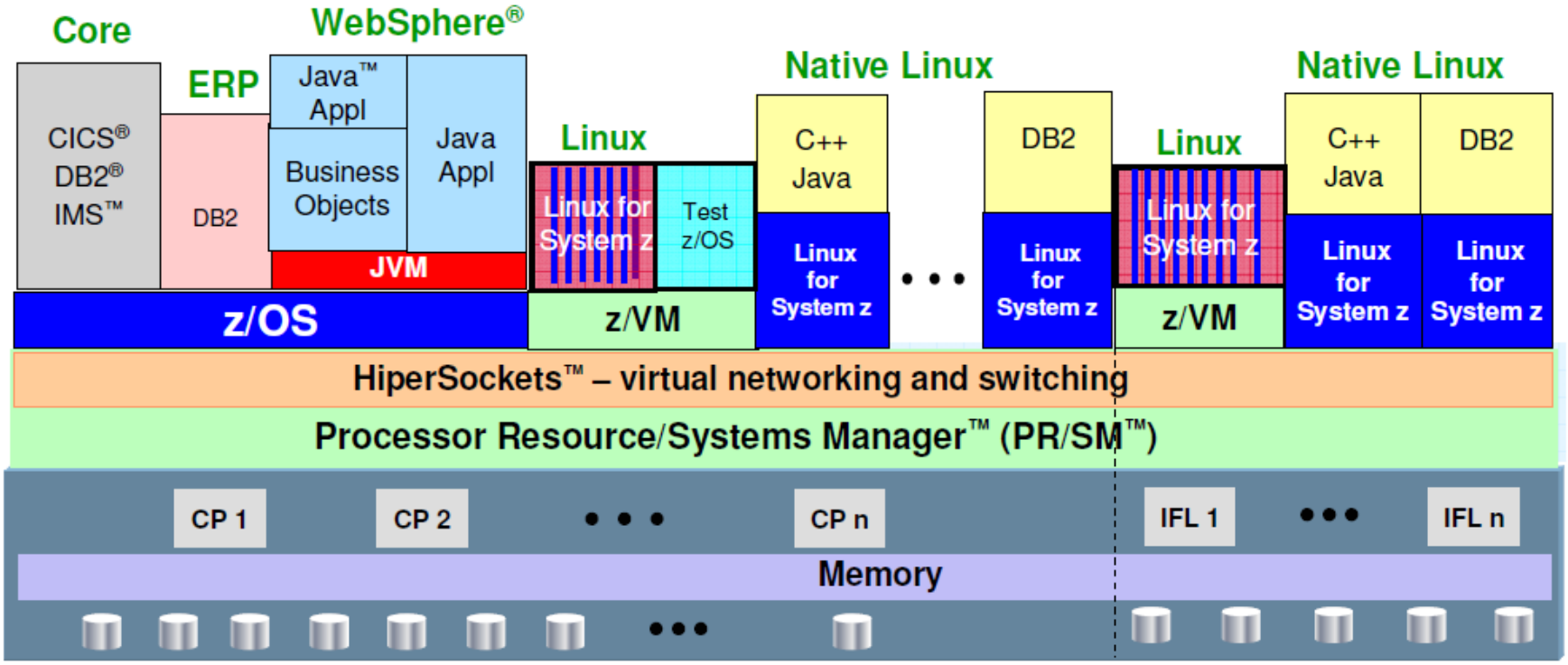
Multiple Tenants (MT) at Different Levels of the Stack



Example: Database Multi-tenancy



Models are Mixed in Real Life. Example: IBM System z



- Massive, robust consolidation platform; virtualization is built in, not added on
- Up to 60 logical partitions on PR/SM; 100's to 1000's of virtual servers on z/VM
- Virtual networking for memory-speed communication, as well as virtual layer 2 and layer 3 networks supported by z/VM
- Most sophisticated and complete hypervisor function available
- Intelligent and autonomic management of diverse workloads and system resources based on business policies and workload performance objectives

Examples of Multi-tenancy Technologies

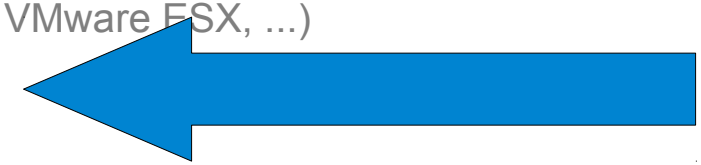
- **All stack layers, all applications**
  - Explicit coloring of all resources (roles/identities, data, application, processes, ...)
    - (Top Secret, Secret, Unclassified, …)
    - (Finance, HR, Marketing, …)
    - Natural generic coloring for clouds: by cloud subscriber contract
  - Runtime separation of domains of different colors
    - Isolation is one mandatory access control policy
    - M(I)LS = Multiple (Independent) Levels of Security
    - LBAC = Label-based Access Control
    - Enterprise zoning policies (external, DMZ, production, test, development, etc.)
  - Provisioning, migration and de-provisioning of resources with security constraints
    - Geographic location (mostly for privacy reasons)
    - Restrictions on co-tenancy (eg, never put X and Y on same Z at the same time)
    - Secure resource management (eg, provenance and health of virtual machine images)
  - All security and system information and events must be colored
    - Includes all events relevant for compliance reports and audits
    - Client-specific compliance reporting is a key requirement
  - Major systems challenge
    - Consistency and visibility of colors across layers and across domains
  - TCG-style Trusted Computing (trusted boot, remote attestation, etc) [Challener 08, Jansen 08, Santos 09]

Examples of Multi-tenancy Technologies

- **Server-focused**
  - Hypervisor (z/VM, LPAR, pHype, Xen, VMware ESX, ...)
  - **Hypervisor-level security services**
- **Network-focused**
  - Security Zones, Trusted Virtual Domains (provisioning, …) [Berger 08, Berger 09]
  - VLAN (IEEE 802.1Q)
  - Trusted / Secure Virtual Private Networks (VPN)
  - Encryption of data in transit (SSL/TLS, SSH, IPSec)
- **Storage-focused**
  - Label-based Access Control (LBAC)
  - Storage zoning (Virtual Storage Area Network (VSAN), Logical Unit (LUN) Masking, ...)
  - Encryption of data at rest (including backups, maintenance) and Key Management
  - Cleanup (caches, files, disks, backups, …)
  - **Fully homomorphic encryption**

Examples of Multi-tenancy Technologies

- **Server-focused**
  - Hypervisor (z/VM, LPAR, pHype, Xen, VMware ESX, ...)
  - **Hypervisor-level security services**

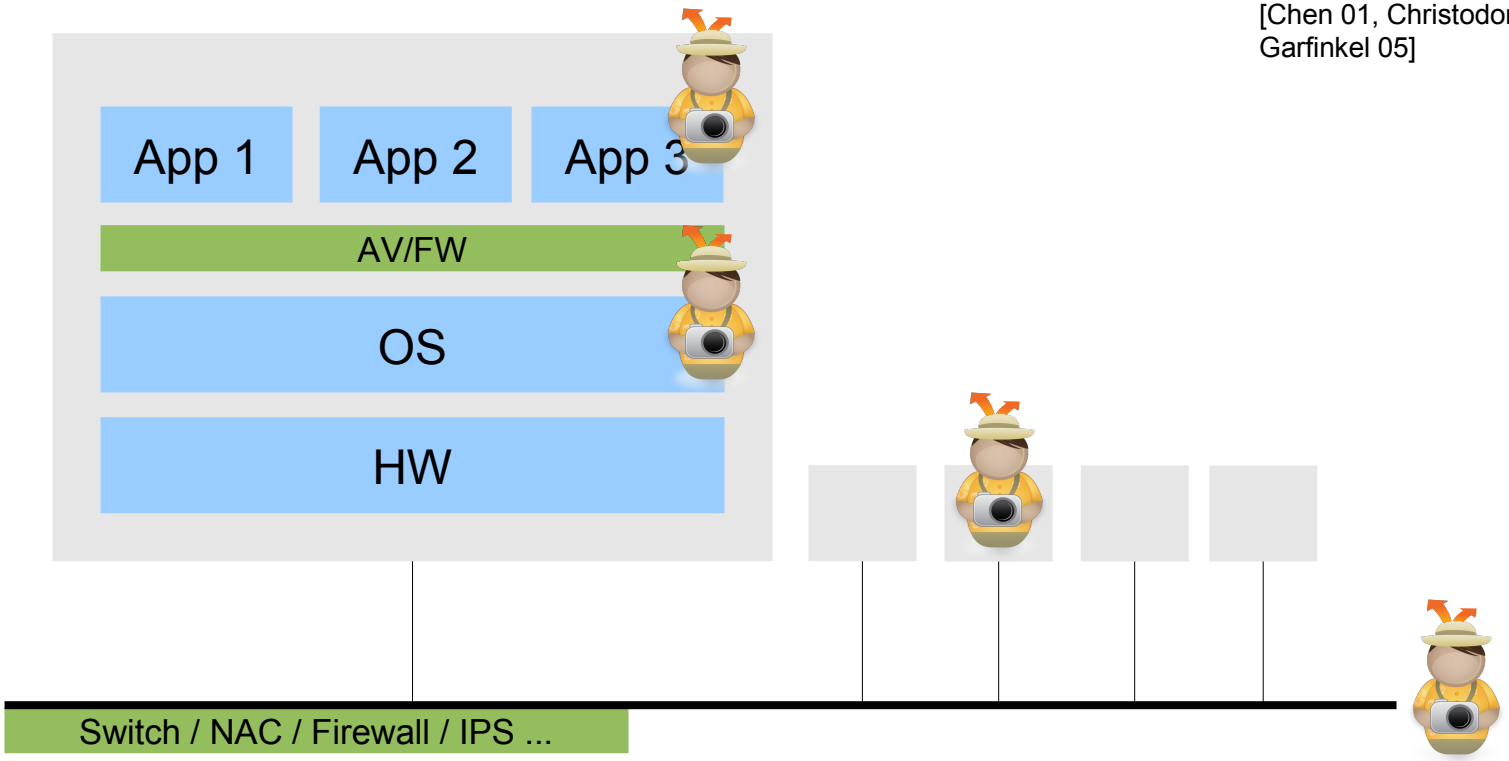


- **Network-focused**
  - Security Zones, Trusted Virtual Domains (provisioning, …) [Berger 08, Berger 09]
  - VLAN (IEEE 802.1Q)
  - Trusted / Secure Virtual Private Networks (VPN)
  - Encryption of data in transit (SSL/TLS, SSH, IPSec)
- **Storage-focused**
  - Label-based Access Control (LBAC)
  - Storage zoning (Virtual Storage Area Network (VSAN), Logical Unit (LUN) Masking, ...)
  - Encryption of data at rest (including backups, maintenance) and Key Management
  - Cleanup (caches, files, disks, backups, …)
  - **Fully homomorphic encryption**

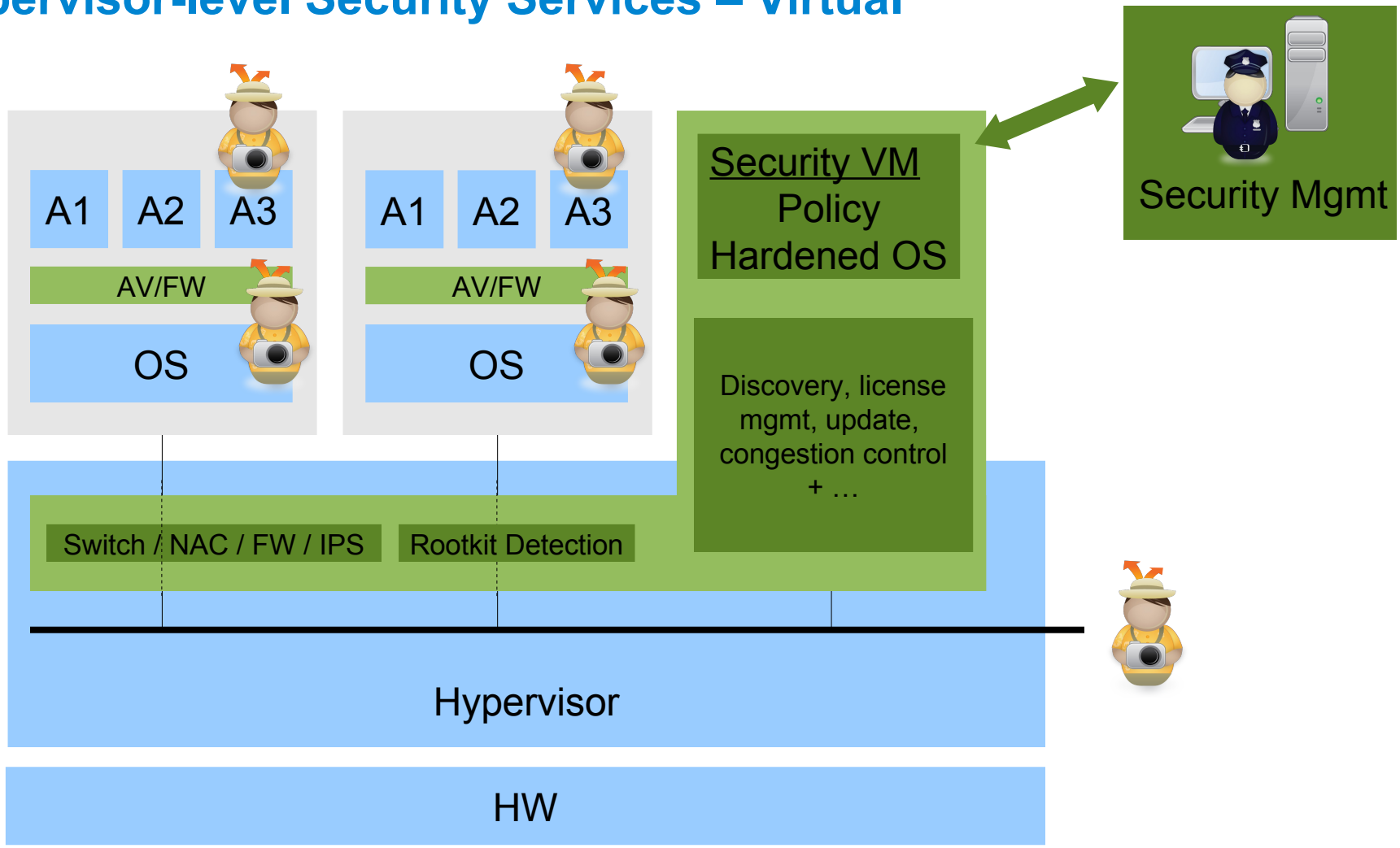
Hypervisor-level Security Services – Physical

- What would change in a naïve transition from physical (this picture) to virtual?
  - Security services are unnecessarily replicated
  - Security becomes harder: VM sprawl, hypervisor as a new component
  - Security becomes easier: move security services out of the OS into the Hypervisor, security system can *introspect* the virtual hardware

[Chen 01, Christodorescu 09, Garfinkel 05]



Hypervisor-level Security Services – Virtual



Example: IBM Tivoli Virtual Server Security for VMware

Examples of Multi-tenancy Technologies

- **Server-focused**
  - Hypervisor (z/VM, LPAR, pHype, Xen, VMware ESX, ...)
  - **Hypervisor-level security services**
- **Network-focused**
  - Security Zones, Trusted Virtual Domains (provisioning, …) [Berger 08, Berger 09]
  - VLAN (IEEE 802.1Q)
  - Trusted / Secure Virtual Private Networks (VPN)
  - Encryption of data in transit (SSL/TLS, SSH, IPSec)
- **Storage-focused**
  - Label-based Access Control (LBAC)
  - Storage zoning (Virtual Storage Area Network (VSAN), Logical Unit (LUN) Masking, ...)
  - Encryption of data at rest (including backups, maintenance) and Key Management
  - Cleanup (caches, files, disks, backups, …)
  - **Fully homomorphic encryption**

Fully Homomorphic Encryption

- **Value of data-at-rest encryption in cloud computing**
  - Data on disks, data on backups
  - Storage-centric: subscriber can en/decrypt, provider never sees data
  - Does not work if & while cloud provider *operates* on encrypted data
- **Fully homomorphic encryption** (idea: Rivest, Adleman, Dertouzos, 1978)
  - Express an algorithm as a circuit (network): $f(x_1, x_2, \ldots) = x_1+x_2*(1-x_3) \ldots$
  - What if we had a public-key encryption function that (roughly) does this:
    - $Enc(x_1)+Enc(x_2)*(1-Enc(x_3)) \ldots = Enc(x_1+x_2*(1-x_3) \ldots$
- **State of the art**
  - Efficient solutions for certain related subproblems (homomorphic in one operation, server-aided computations, voting protocols, …)
  - First provably secure fully homomorphic solution: [Gentry 09]
    - Shows what can be done in priniciple
    - Polynomial, but needs substantial work before it can be used in practice
  - Major area of research in cryptography

Outline

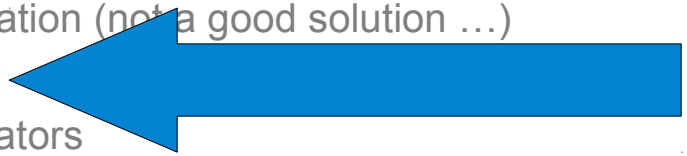
- Responsibilities of Provider and Subscriber
- Isolation and Integrity Management
  - Multi-tenancy
  - Hypervisor-level security services
  - Fully homomorphic encryption (outlook)
- Identity Management
  - Managing privileged users
  - On-/off-boarding of users, federated identity

Identity Management

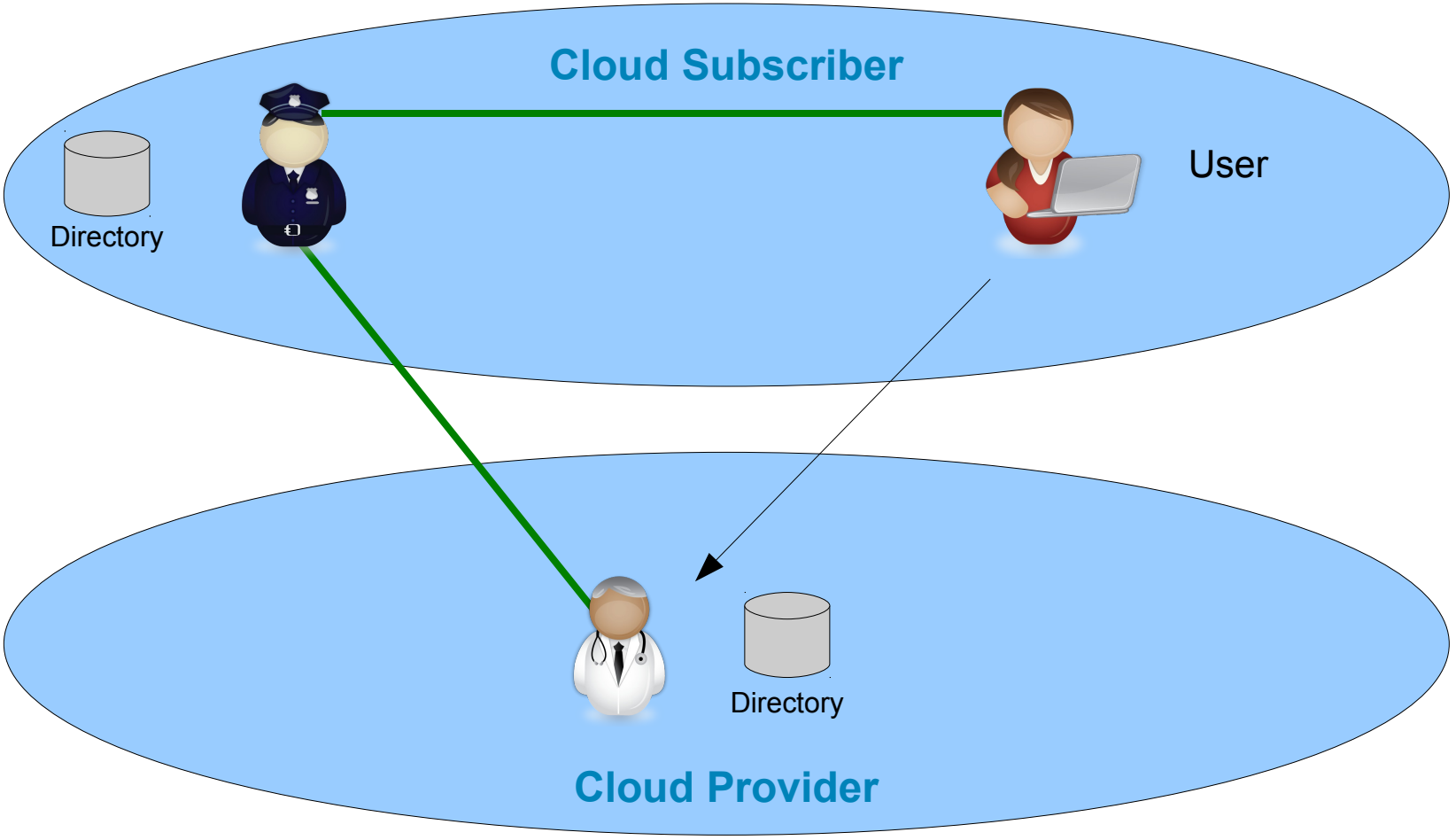
- Identity = set of attributes
- Tightly linked to
  - Users (but devices have identities too)
  - Roles and entitlements
  - Authentication (username/password, strong authentication, two-factor, claims)
  - Authorization and delegation
  - Privacy
  - Fraud and abuse detection
- Main types of identities to consider in a cloud
  - Cloud subscriber's administrators
    - Initial enrollment and proofing of cloud subscriber
    - Trust in identities depends largely on proofing (valid email address … upfront payment … out-of-band signed service contract)
  - Cloud subscriber's end user identities (subscriber's employees, customers)
    - Efficient on-boarding / off-boarding
    - Directory synchronization (not a good solution …)
    - **Federated identity**
  - Cloud provider administrators
    - Main issue: **Control over privileged identities**

Identity Management

- Identity = set of attributes
- Tightly linked to
  - Users (but devices have identities too)
  - Roles and entitlements
  - Authentication (username/password, strong authentication, two-factor, claims)
  - Authorization and delegation
  - Privacy
  - Fraud and abuse detection
- Main types of identities to consider in a cloud
  - Cloud subscriber's administrators
    - Initial enrollment and proofing of cloud subscriber
    - Trust in identities depends largely on proofing (valid email address … upfront payment … out-of-band signed service contract)
  - Cloud subscriber's end user identities (subscriber's employees, customers)
    - Efficient on-boarding / off-boarding
    - Directory synchronization (not a good solution …)
    - **Federated identity**
  - Cloud provider administrators
    - Main issue: **Control over privileged identities**



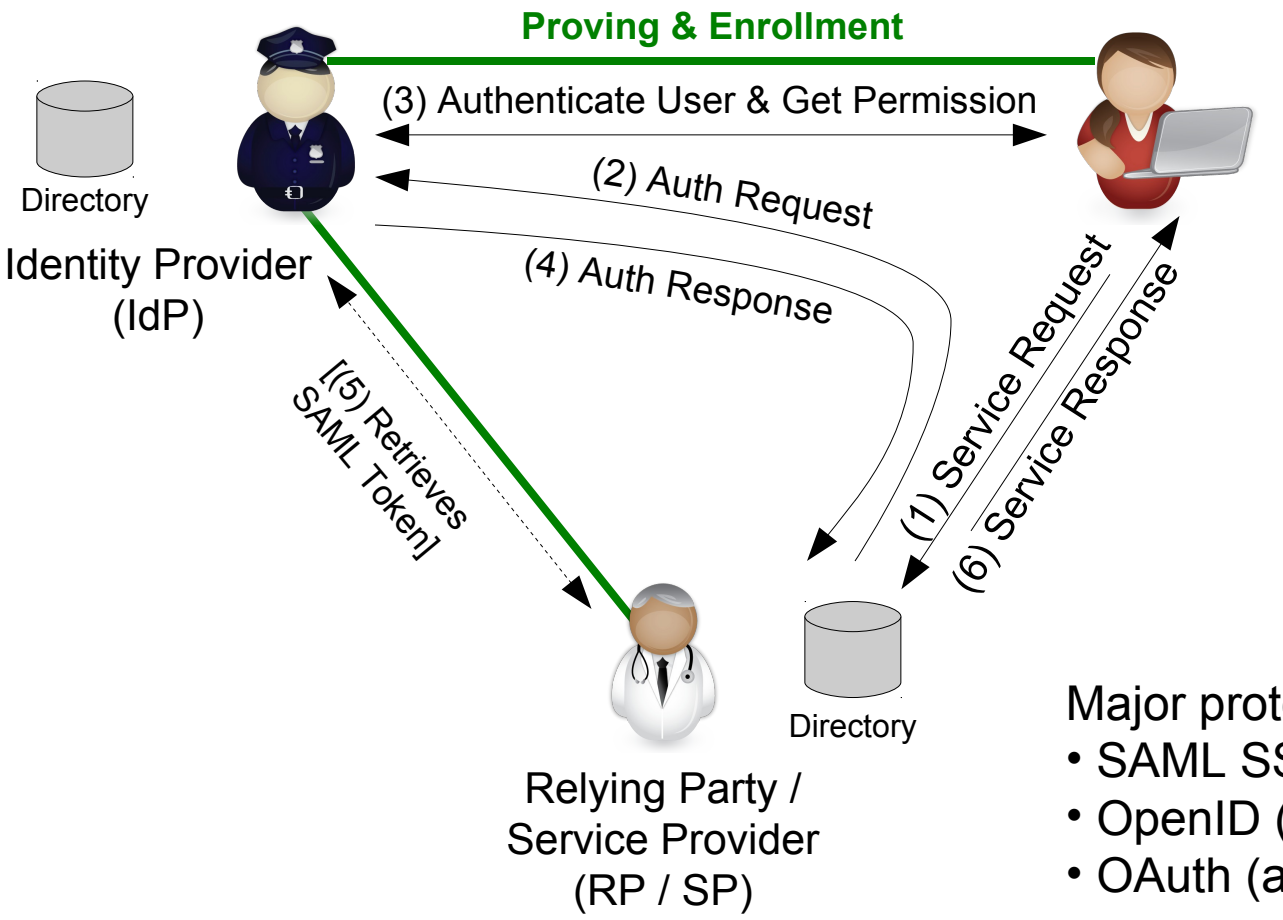
Federated Identity (Single-Sign On & Attribute Exchange)



Trust Relationship

Provider needs to authenticate user, without copying the whole subscriber directory.

Federated Identity (Single-Sign On & Attribute Exchange)



Trust Relationship

Major protocols:
- SAML SSO (enterprise app)
- OpenID (Web 2.0 app)
- OAuth (adds authorization)

•Example: IBM Tivoli Federated Identity Manager

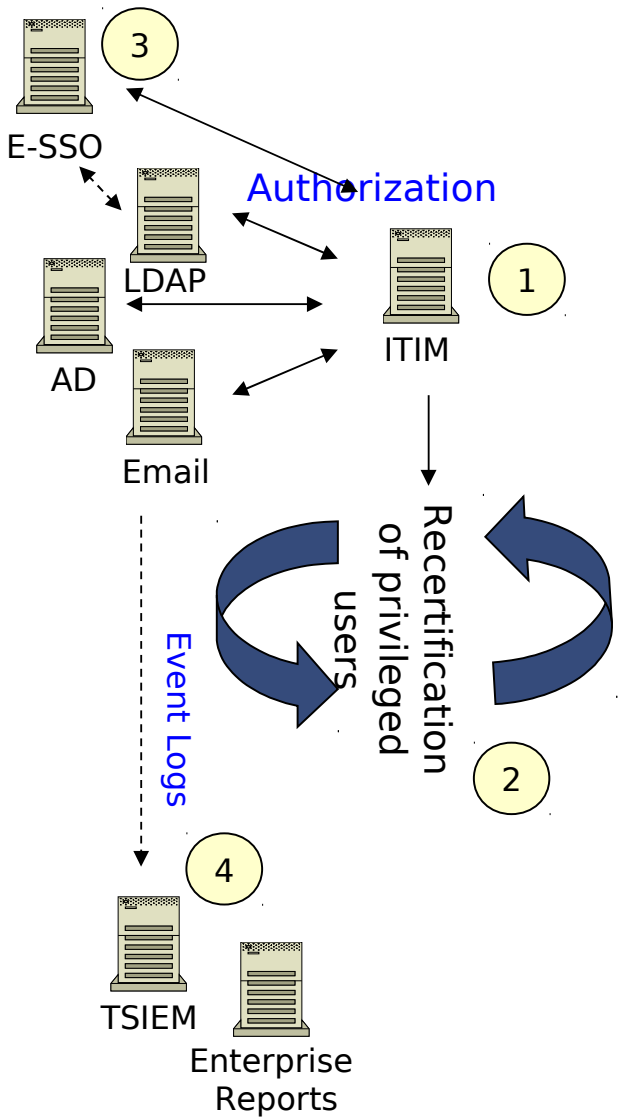
Identity Management

- Identity = set of attributes
- Tightly linked to
  - Users (but devices have identities too)
  - Roles and entitlements
  - Authentication (username/password, strong authentication, two-factor, claims)
  - Authorization and delegation
  - Privacy
  - Fraud and abuse detection
- Main types of identities to consider in a cloud
  - Cloud subscriber's administrators
    - Initial enrollment and proofing of cloud subscriber
    - Trust in identities depends largely on proofing (valid email address … upfront payment … out-of-band signed service contract)
  - Cloud subscriber's end user identities (subscriber's employees, customers)
    - Efficient on-boarding / off-boarding
    - Directory synchronization (not a good solution …)
    - **Federated identity**
  - Cloud provider administrators
    - Main issue: **Control over privileged identities**

Privileged Identity Management (PIM)

- **One of the top security concerns for cloud computing**
  - Fear of losing control
- **Context**
  - Cloud admins need privileged (think: root) access to cloud & client resources
  - Any reasonable policy demands strong accountability for admin actions
  - Cloud admins typically share privileged accounts
    - Because of limitations of many managed systems
    - Because the number of identities to manage would explode otherwise
- **Approach**
  - “Reverse Single-sign on”
  - PIM system manages all privileged accounts
  - Admins need to check out privileged accounts
  - PIM does log on / log out (admin never sees passwords, gets credentials)
  - PIM logs everything, and SIEM system correlates system logs with PIM logs

IBM Tivoli's Privileged Identity Management Solution



1
- TIM with custom module provisions privileged IDs and manages pools of shared IDs
- Shared IDs are stored in a secured data store

2
- Periodically recertify account authorizations through a consistent work flow.

3
- Admin logs into TAM E-SSO
- TAM E-SSO automatically checks out/in shared ID as required to ensure accountability while simplifying usage

4
- TSIEM monitors all logs for end to end tracking

References & Reading List (1/2)

- [Berger 08] Berger, S., Cáceres, R., Pendarakis, P., Sailer, R., Valdez, E, Perez, R., Schildhauer, W. and Srinivasan, D. TVDc: Managing Security in the Trusted Virtual Datacenter. SIGOPS Oper. Syst. Rev. 42/1 (2008).
- [Berger 09] Berger, S., Cáceres, R., Goldman, K., Pendarakis, D., Perez, R. , Rao, J. R., Rom, E., Sailer, R., Schildhauer, W., Srinivasan, D., Tal, S. and Valdez, E. Security for the Cloud Infrastructure: Trusted Virtual Data Center Implementation. IBM Journal of Research and Development 53/4 (2009).
- [Challener 08] Challener, D., Yoder, K., Catherman, R., Safford, D. and Van Doorn, L. A Practical Guide to Trusted Computing. IBM Press 2008.
- [Chen 01] Chen P. M., Noble, B. D. When Virtual is Better Than Real, In USENIX Hot Topics in Operating Systems, Elmau, 2001.
- [Christodorescu 09] Christodorescu, M., Sailer, R., Schales, D., Sgandurra, D., Zamboni, D. Cloud Security Is Not (Just) Virtualization Security. In ACM Cloud Computing Security Workshop, Chicago, 2009.
- [Garfinkel 05] Garfinkel, T., Rosenblum, M. When Virtual is Harder than Real: Security Challenges in Virtual Machine Based Computing Environments. In USENIX Hot Topics in Operating Systems, Santa Fe, 2005.
- [Gentry 09] Gentry, C. Fully Homomorphic Encryption Using Ideal Lattices. ACM Symposium on Theory of Computing, Bethesda 2009.
- [Jansen 08] Jansen, B., Ramasamy, H. and Schunter, M. Policy Enforcement and Compliance Proofs for Xen Virtual Machines. In ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments. Seattle, 2008.
- [King 06] King, S. T., Chen, P. M., Wang, Y.-M., Verbowski, C., Wang, H. J. and Lorch, J. R. SubVirt: Implementing Malware with Virtual Machines. In IEEE Symposium on Security and Privacy, Oakland, 2006.
- [Krautheim 09] Krautheim, F. J.. Private Virtual Infrastructure for Cloud Computing. In USENIX Workshop on Hot Topics in Cloud Computing (HotCloud). San Diego. 2009.
- [Matthews 09] Matthews, J., Garfinkel, T., Hoff, C. and Wheeler, J. Virtual Machine Contracts for Datacenter and Cloud Computing Environments. In ACM Workshop on Automated Control for Datacenters and Clouds (ACDC '09). Barcelona, 2009.

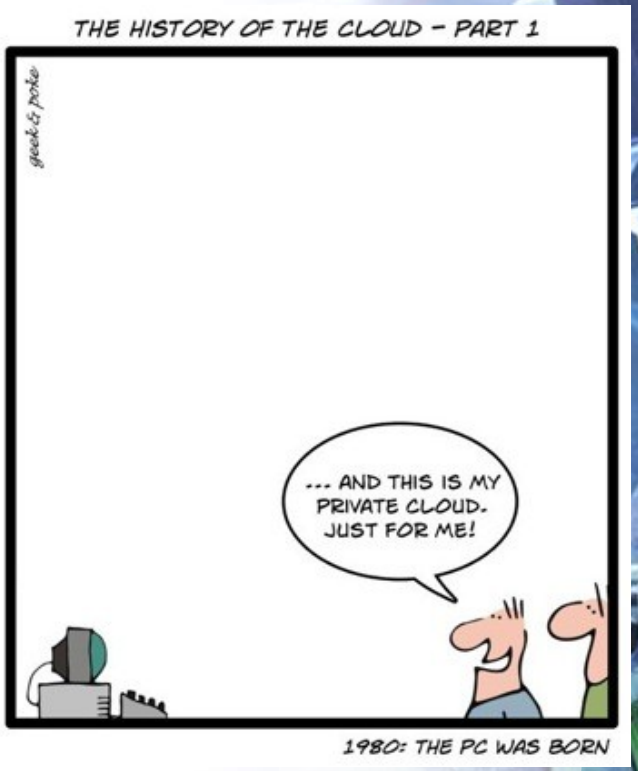
References & Reading List (2/2)

- [OAuth] http://oauth.net
- [Ormandy 07] Ormandy, T. An Empirical Study into the Security Exposure to Hosts of Hostile Virtualized Environments. Google. 2007.
- [OpenID] http://openid.net
- [Ristenpart 09] Ristenpart, T., Tromer, E., Shacham, H., and Savage, S. Hey, you, get off of my Cloud: Exploring Information Leakage in Third-party Compute Clouds. In ACM Conference on Computer and Communications Security, Chicago, ACM, New York, 2009.
- [Rutkowska 08] Rutkowska, J. Security Challenges in Virtualized Enviroments. In RSA Conference, San Francisco, 2008.
- [SAML] OASIS Security Assertion Markup Language. http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security
- [Santos 09] Santos, N., Gummadi, K. and Rodrigues, R. Towards Trusted Cloud Computing. In USENIX Workshop on Hot Topics in Cloud Computing (HotCloud). San Diego. 2009.
- [Sherr 09] Sherr, M. and Blaze, M. Application Containers Without Virtual Machines. In ACM Workshop on Virtual Machine Security, Chicago, 2009.
- [SPML] OASIS Service Provisioning Markup Language. http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=provision
- [XACML] OASIS eXtensible Access Control Markup Language. http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml
- [Wei 09] Wei, J., Zhang, X., Ammons, G., Bala, V., and Ning, P. Managing Security of Virtual Machine Images in a Cloud Environment. In ACM Workshop on Cloud Computing Security, Chicago, 2009.
- [Wimmer 08] Wimmer, M. 2008. Virtual Security, About the Security Pros and Cons of Server Virtualization; In FIRST Annual Conference on Computer Security Incident Handling; Vancouver, 2008.

Chapter 3

Selecting a Secure Cloud & Using it Securely

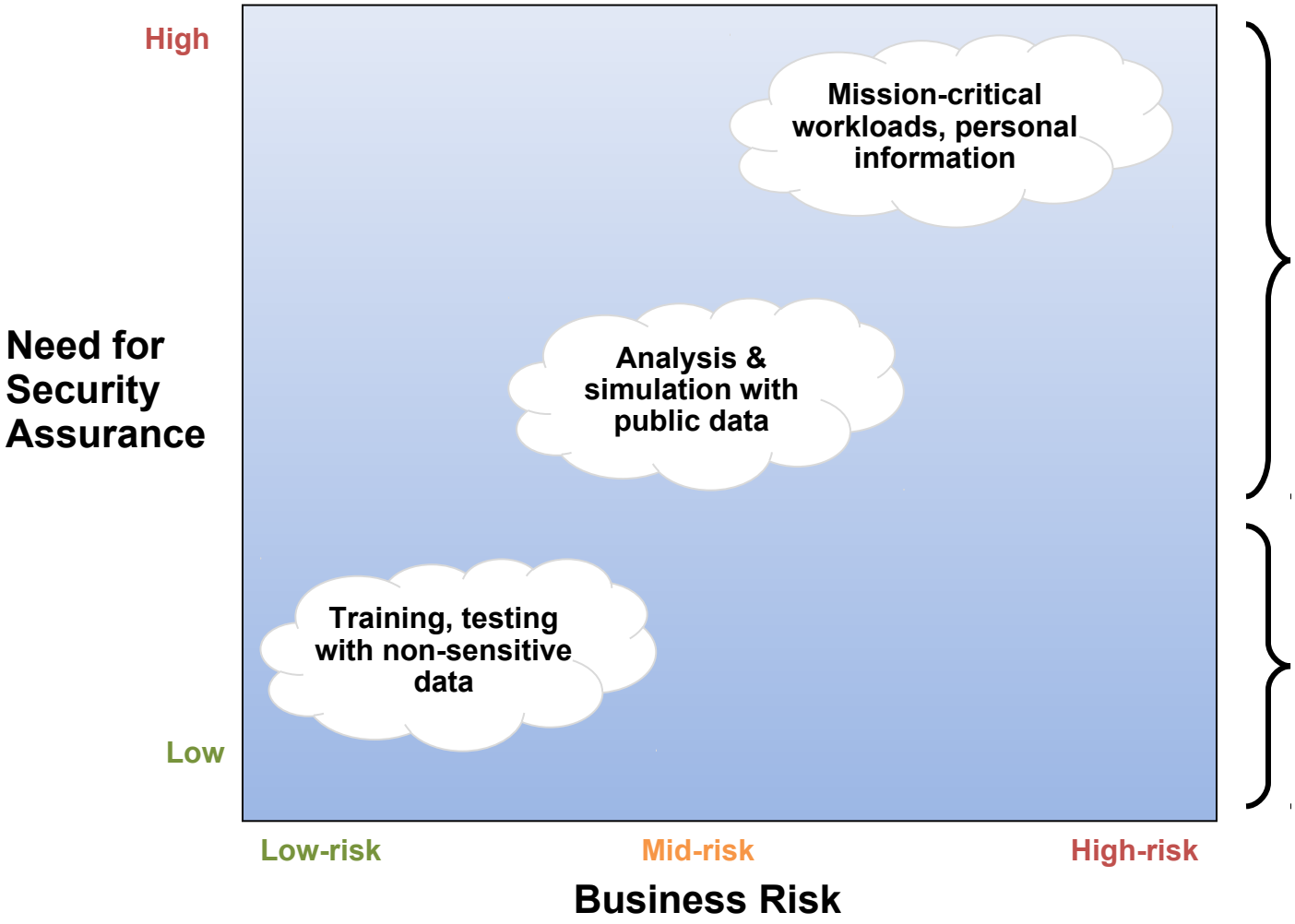
(The cloud subscriber's perspective)



http://geekandpoke.typepad.com/geekandpoke/2009/10/the-history-of-the-cloud-part-1.html

One-size does not fit-all:

Different cloud workloads have different risk profiles



Tomorrow's high value / high risk workloads need:

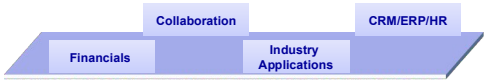
- Quality of protection adapted to risk
- Direct visibility and control
- Significant level of assurance

Today's clouds are primarily here:

- Lower risk workloads
- One-size-fits-all approach to data protection
- No significant assurance
- Price is key

"Subjective Risk" – Enterprise Perspective

Business Process-as-a-Service

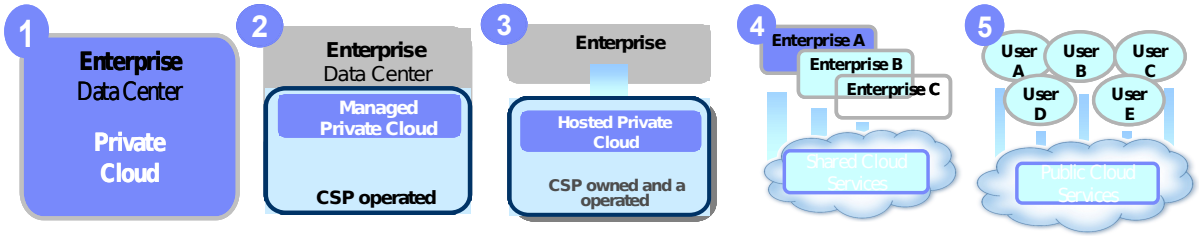


Application-as-a-Service

Platform-as-a-Service

Infrastructure-as-a-Service

More sharing and lower-level service abstraction are perceived as risk increasing factors.



Typical Security Requirements Derived from Privacy and Accountability Regulations

Legislation Area	Covers	Implications on Cloud Architecture
Corporate Financial Accounting and Reporting	Providing evidence of appropriate Business Controls, correct handling of financial data, correct reporting of financial information	**Extensive logging incl. provenance, demonstrable security controls between customers and between layers of the Cloud**
Financial transaction handling	Security measures necessary in order to service financial transactions and customers	Identification and segregation of the cloud elements supporting financial transactions **Data encryption**
Data Privacy	Security measures necessary in handling personal data	**Inability to move data around the cloud, data may have to reside and be processed within a specific country** Requirement on the cllient to manage data protection
Reserved Powers	Discovery, search and seizure powers retained as a matter of law by external agencies	**Data, audit logs, hardware may need to be discovered and surrendered to authorized agencies**
Restrictions on data transmittal and usage	Limitations or requirements to be fulfilled before data can be moved or used in different legislative domains	**Inability to move data around the cloud, data may have to reside and be processed within a specific country**
Industry-specific Regulatory issues	Requirements on specific industry sectors which will impact usage of Cloud	Industry-specific cloud implementations

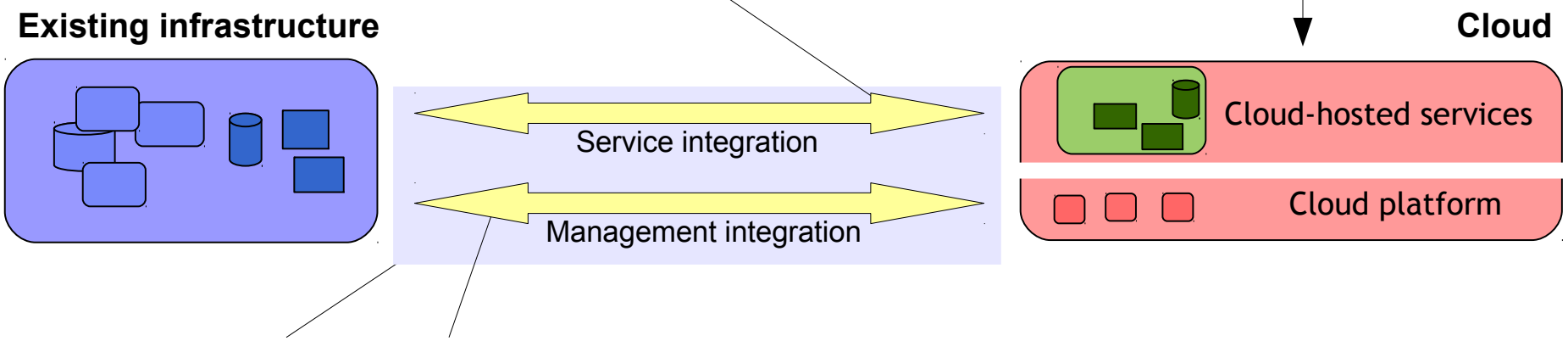
Not a complete listing, not intended as legal advice.

Integrating Cloud and Enterprise Security Management

2. Secure Service Integration

- Federated SSO
- All the usual SOA security capabilities must work
- Evolving preference for REST style

1. Secure Virtualized Runtime



Both arrows:
- VPN/VLAN (several options for endpoints)
- Popular: SSH admin login
- Threat management at the network and web-app level (firewall, IPS, DLP, ...)

3. Security Management Integration

- Efficient on-boarding/off-boarding of identities, roles and entitlements
- Provisioning/de-provisioning of resources with security constraints
- Interfaces for backup and recovery
- Identity (directory) and access management integration, through identity federation
- Monitoring and compliance reporting at the cloud level

Trust in Cloud Provider

- **Subscriber perspective**
  - "Secure Virtualized Runtime" is the provider's responsibility (see Ch. 2)
  - No direct control, hence provider must be *trustworthy*
    - Reputation
    - Stated provider security policies
    - Service-level agreements with regular audits and defined compensations
    - Audits may be general (low-end, standardized) or client-specific (high-end, specialized)
  - Very few technologies enable extension of control into the cloud
    - Cryptography (encryption, integrity checks), to a certain extent
    - TCG-style Trusted Computing (exists but rarely used)
    - Research: homomorphic encryption
- **Best practices, guidance/checklists and audits (see Ch. 1) play major role**
  - Cloud Security Alliance [CSA 09]
  - IBM Cloud Security Guidance [Buecker 09]

References & Reading List

- [BSI 09] SOA-Security-Kompendium: Sicherheit in Service-orientierten Architekturen (Version 2.0). Bundesamt für Sicherheit in der Informationstechnik, Bonn, 2009.
- [Buecker 07] Buecker, A., Ashley, P., Borrett, M., Lu, M., Muppidi, S. and Readshaw N. Understanding SOA Security Design and Implementation. IBM RedBook, New York, 2007.
- [Buecker 09] Buecker, A., Lodewijkx, K., Moss, H., Skapinetz, K., Waidner, M. Cloud Security Guidance. IBM Recommendations for the Implementation of Cloud Security. IBM RedPaper, New York, 2009.
- [Cloud 10] Cloud Computing Use Cases Discussion Group, Cloud Computing Use Cases White Paper Version 3. 2010. Available from http://www.scribd.com/doc/18172802/Cloud-Computing-Use-Cases-Whitepaper.
- [CSA 09] Security Guidance for Critical Areas of Focus in Cloud Computing V2.1. Cloud Security Alliance, 2009.
- [ENISA 09] Cloud Computing: Benefits, Risks and Recommendations for Information Security. European Network and Information Security Agency (ENISA), 2009.
- [Wang 09] Wang, C. Cloud Computing Checklist: How Secure Is Your Cloud? Forrester Research, 2009.

Chapter 4

Cloud-delivered Security Services

(Also known as “Security-as-a-Service”)

Security as a Service

Function	Now	2013	2018
Messaging / Email Security	20%	60%	70%
Secure Web Gateway	10%	35%	65%
Remote Vulnerability Scanning	10%	30%	45%
Security Information and Log Management	1%	10%	25%
Identity & Access Management	2%	20%	28%
Security Intelligence	60%	80%	85%

Source: Kelly Kavanagh, Gartner Research

- Good candidates for security-as-a-service are functions which
  - Can be delivered without on-premises technology
  - Latency-tolerant
  - Require minimal customization
  - Involves one-to-many data management or analysis functions
  - Can be implemented though standard interfaces
  - Unlike managed security services, not labor-intensive

itnews
FOR AUSTRALIAN BUSINESS

News | Technology | Business | Forums | Jobs

Reviews | Galleries | Events | Net Seminars | Whitepapers | Downloads | Newsletter | Videos

Home > News > Technology > Security > Cybercrime-as-a-service takes off

SECURITY

Cybercrime-as-a-service takes off

By Ry Crozier
Mar 12, 2009 11:37 AM
Tags: cybercrime | service | vasco | outsourcing | malware | trojan | toolkits

SHARE

Malware writers that sell toolkits online for as little as $400 will now configure and host the attacks as a service for another $50, a security expert has said.

Speaking at the Vasco Banking Summit in Sydney yesterday, the company's technical account manager, Vlado Vajdic, told delegates that cyber crime was becoming so business-like that online offerings of malicious code often included support and maintenance services.

Additionally, he said, cybercrime outsourcing would become a key trend in 2009.

"It was inevitable that services would be sold to people who bought the malware toolkits but didn't know how to configure them," Vajdic said.

"Not only can you buy configuration as a service now, you can have the malware operated for you, too. We saw evidence of that this year."

2 comments in this discussion

"This is not new, it's been a developing trend for the past couple of years, take a look at dancho danchev's blog..."

By Anon

Related Articles

- Laws to prosecute malware makers flagged
- Bit.ly hits back at Google

http://www.itnews.com.au/News/139682,cybercrime-as-a-service-takes-off.aspx

Chapter 5

Areas for Research

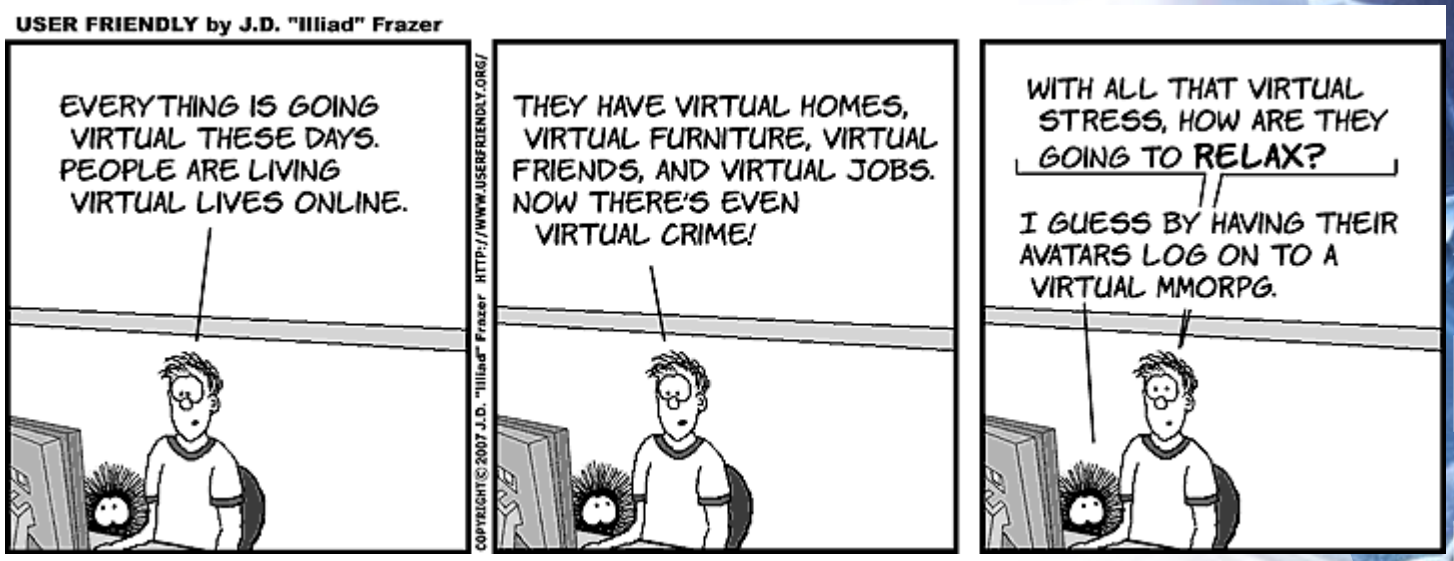
Areas for Research

- **Coloring-based multi-tenancy is a simple concept, building it in reality is always painful**
- **Basic cloud and virtualization security**
  - Security criteria, SLAs, maturity model (easy in principle, but consensus building is difficult)
  - Meaningful security metrics for cloud computing (this is hard)
  - Standard approach for compliance monitoring for cloud computing (easy in principle)
  - Security analysis, hardening and proof/evaluation of real-world hypervisor
  - Hypervisor-based security services (additional platforms, more services)
  - Security in emerging cloud computing programming languages
  - Privacy and cloud computing (think: info sharing, user-created content, Web 2.0)
- **Security for virtual machine images**
  - Embedding security policies and information into images
  - Provenance of virtual images
  - Reconsider proof-carrying code and other “mobile agent” security constructs

Areas for Research

- **Cryptography and cryptographic protocols**
  - Provably secure *and practical* fully homomorphic encryption
  - Provably secure and practical, privacy preserving .....
  - Key management for public clouds
  - Reconsider fault-tolerance and synchronization protocols under cloud computing assumptions
  - Reconsider recovery oriented computing under cloud computing assumptions
  - Reconsider TCG-style trusted computing under cloud assumptions
- **Cloud-next**
  - Build a global-scale cloud capable of surviving massive failures and attacks

That's it.



http://ars.userfriendly.org/cartoons/?id=20080228

© J. D. “Illiad” Frazer