CLOUD SECURITY

Let’s Open the Box

Abu Shohel Ahmed
ahmed.shohel@ericsson.com
NomadicLab, Ericsson Research

FACTS ABOUT ERICSSON

- Ericsson is a world-leading provider of telecommunication equipment and services
- More then 40 percent of mobile traffic passes through Ericsson network
- Ericsson is the 5th largest software company in the world

WHY ERICSSON IN CLOUD

For Clouds:

- It is difficult to optimize the cost of Computation, Networking and Storage at the same time (Revision of Brewer's CAP theorem)

- MNO's can play a key role to optimize the Networking

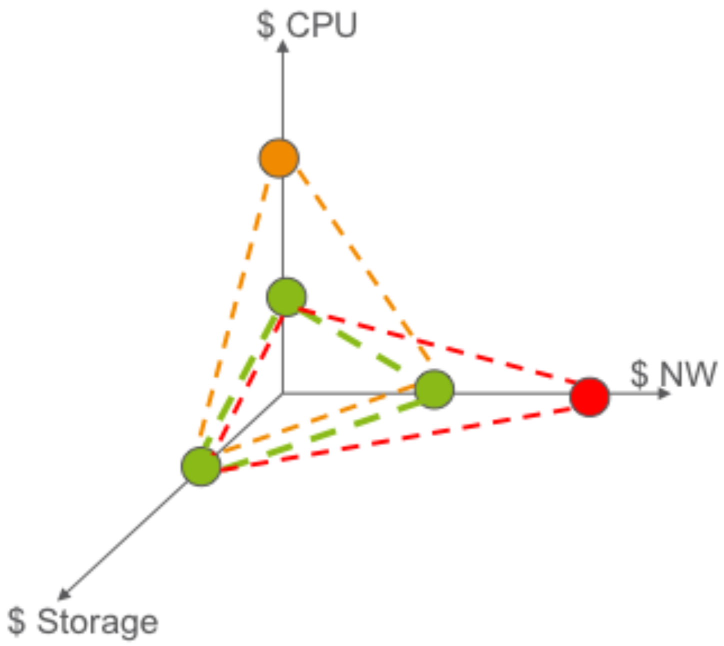
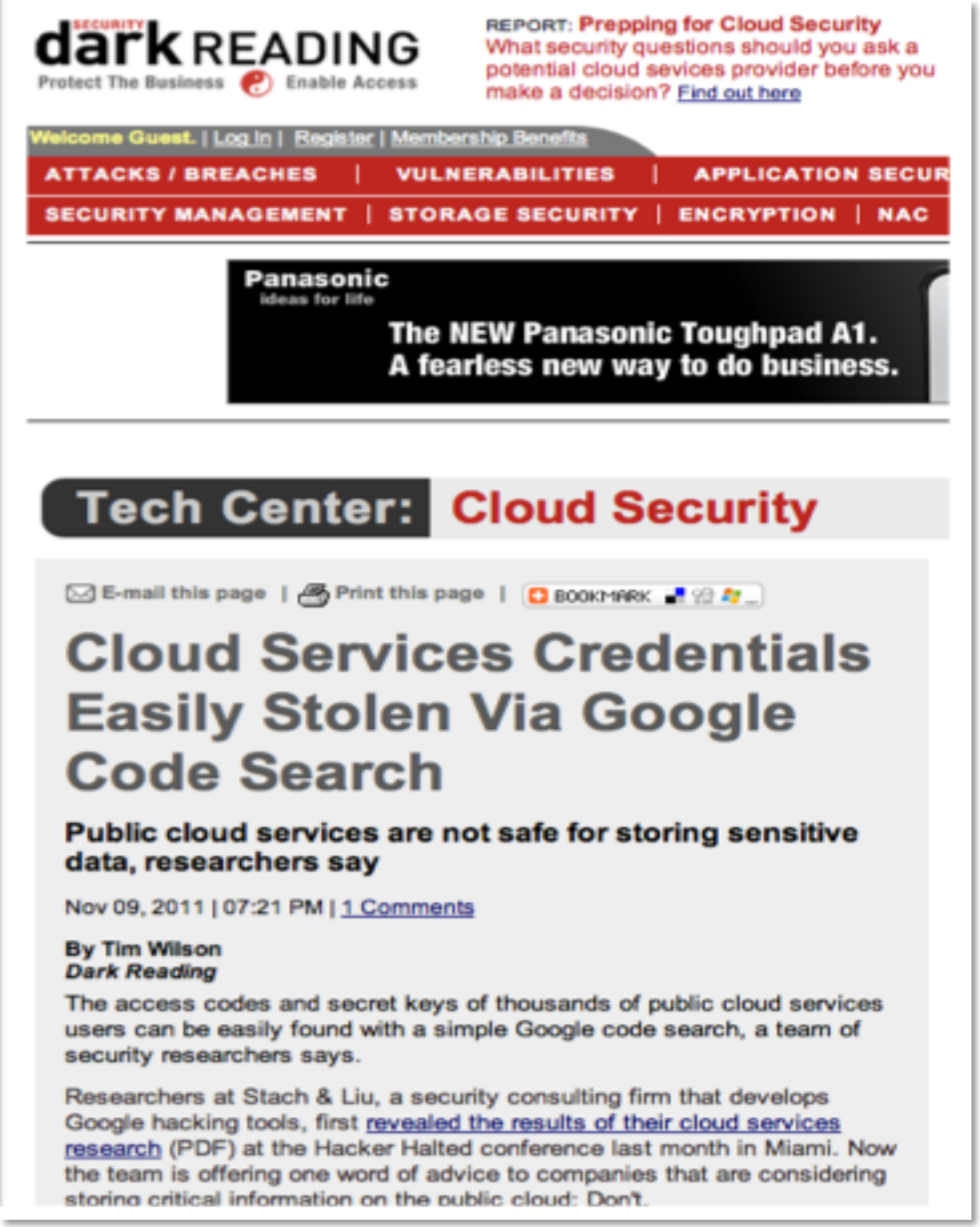


Figure from Ericsson

DARK DAYS OF CLOUD


SECURITY dark READING
Protect The Business Enable Access

REPORT: Prepping for Cloud Security
What security questions should you ask a potential cloud services provider before you make a decision? Find out here

Welcome Guest. | Log In | Register | Membership Benefits
ATTACKS / BREACHES | VULNERABILITIES | APPLICATION SECUR
SECURITY MANAGEMENT | STORAGE SECURITY | ENCRYPTION | NAC

Tech Center: Cloud Security

E-mail this page | Print this page | BOOKMARK

Cloud Services Credentials Easily Stolen Via Google Code Search

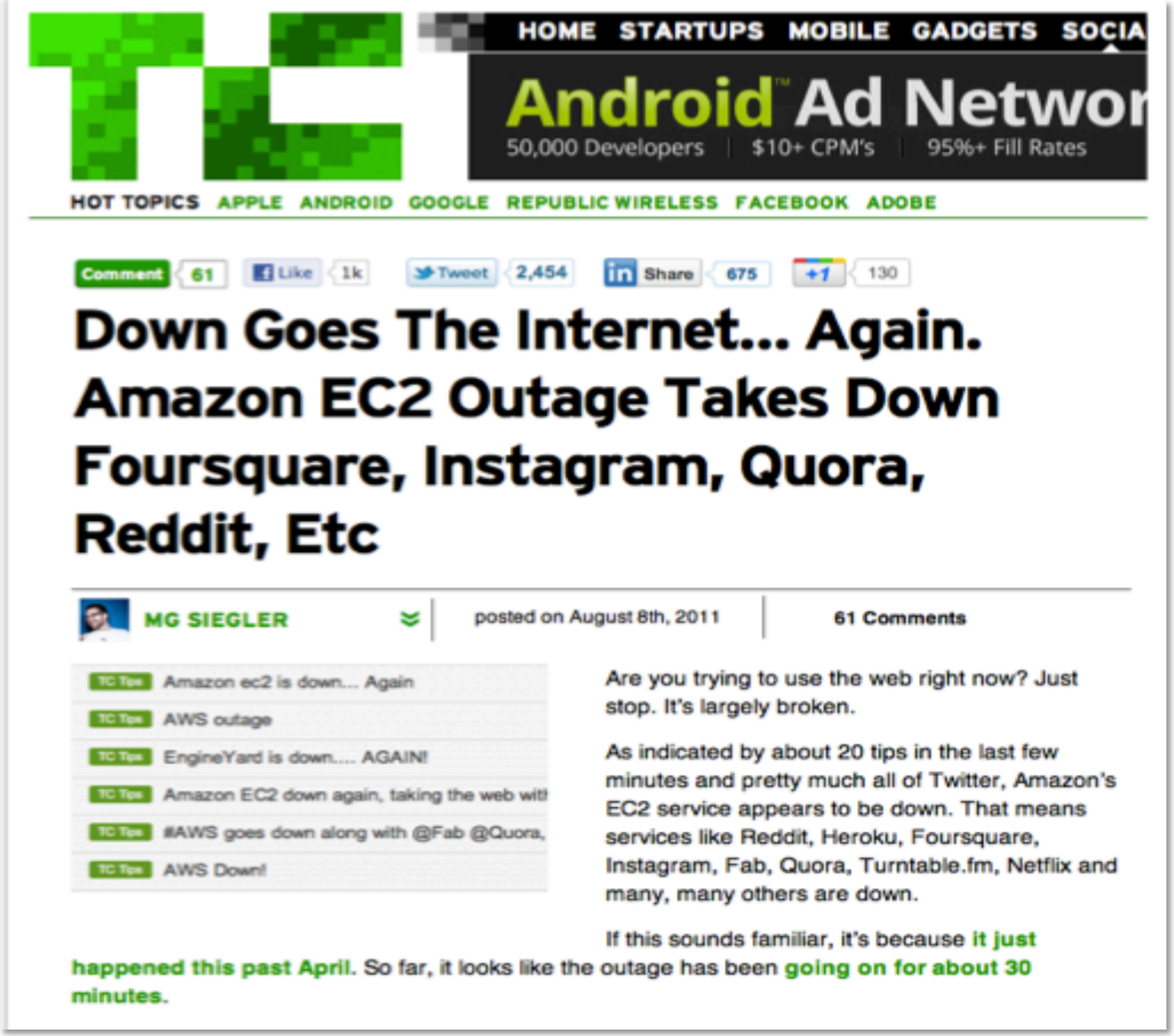
Public cloud services are not safe for storing sensitive data, researchers say

Nov 09, 2011 | 07:21 PM | 1 Comments

By Tim Wilson
Dark Reading

The access codes and secret keys of thousands of public cloud services users can be easily found with a simple Google code search, a team of security researchers says.

Researchers at Stach & Liu, a security consulting firm that develops Google hacking tools, first revealed the results of their cloud services research (PDF) at the Hacker Halted conference last month in Miami. Now the team is offering one word of advice to companies that are considering storing critical information on the public cloud: Don't.



HOME STARTUPS MOBILE GADGETS SOCIA

HOT TOPICS APPLE ANDROID GOOGLE REPUBLIC WIRELESS FACEBOOK ADOBE
Comment 61 Like 1k Tweet 2,454 Share 675 +1 130

Down Goes The Internet... Again. Amazon EC2 Outage Takes Down Foursquare, Instagram, Quora, Reddit, Etc

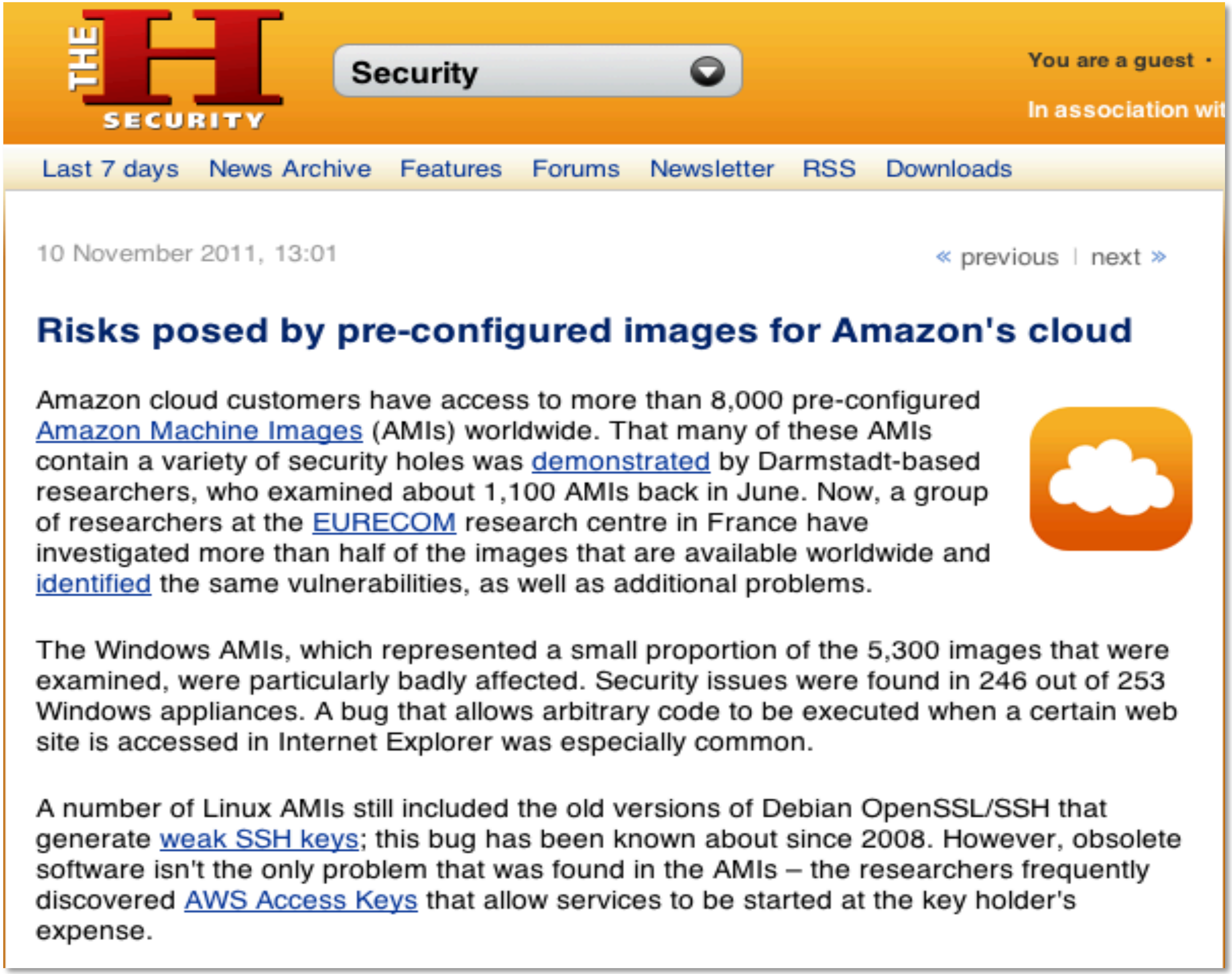
MG SIEGLER | posted on August 8th, 2011 | 61 Comments

- TC Tips Amazon ec2 is down... Again
- TC Tips AWS outage
- TC Tips EngineYard is down.... AGAIN!
- TC Tips Amazon EC2 down again, taking the web wit
- TC Tips #AWS goes down along with @Fab @Quora,
- TC Tips AWS Down!

Are you trying to use the web right now? Just stop. It's largely broken.

As indicated by about 20 tips in the last few minutes and pretty much all of Twitter, Amazon's EC2 service appears to be down. That means services like Reddit, Heroku, Foursquare, Instagram, Fab, Quora, Turntable.fm, Netflix and many, many others are down.

If this sounds familiar, it's because it just happened this past April. So far, it looks like the outage has been going on for about 30 minutes.



10 November 2011, 13:01

Risks posed by pre-configured images for Amazon's cloud

Amazon cloud customers have access to more than 8,000 pre-configured Amazon Machine Images (AMIs) worldwide. That many of these AMIs contain a variety of security holes was demonstrated by Darmstadt-based researchers, who examined about 1,100 AMIs back in June. Now, a group of researchers at the EURECOM research centre in France have investigated more than half of the images that are available worldwide and identified the same vulnerabilities, as well as additional problems.

The Windows AMIs, which represented a small proportion of the 5,300 images that were examined, were particularly badly affected. Security issues were found in 246 out of 253 Windows appliances. A bug that allows arbitrary code to be executed when a certain web site is accessed in Internet Explorer was especially common.

A number of Linux AMIs still included the old versions of Debian OpenSSL/SSH that generate weak SSH keys; this bug has been known about since 2008. However, obsolete software isn't the only problem that was found in the AMIs – the researchers frequently discovered AWS Access Keys that allow services to be started at the key holder's expense.

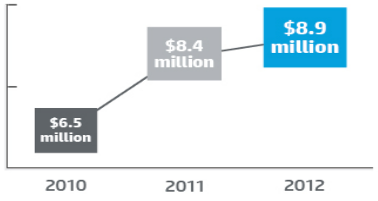
The Growing Cost of Cyber Crime!

Despite widespread awareness of the impact of cyber crime, cyber attacks continue to occur more frequently and result in serious financial consequences. The HP Ponemon 2012 Cost of Cyber Crime Study revealed that cyber attacks have more than doubled and the financial impact has increased by nearly 40 percent in a three year period. At HP, we believe a better understanding of the cost of cyber crime can assist organizations in taking proactive measures to identify, combat and mitigate the potentially devastating consequences of an attack.

HP is changing the enterprise security landscape with advanced security solutions that uniquely leverage leading threat research and powerful correlation of security events and vulnerabilities to deliver security intelligence spanning IT operations, applications and infrastructure.

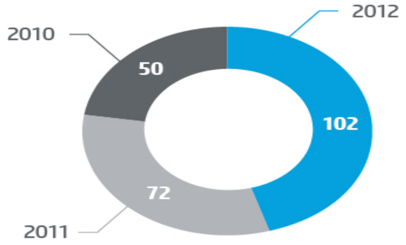
Costs

Cost per year for organisations



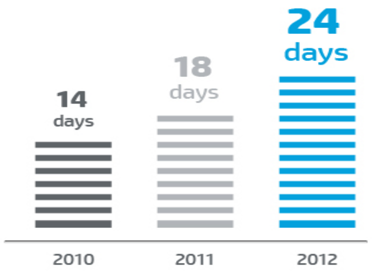
Attacks

Successful attacks per week



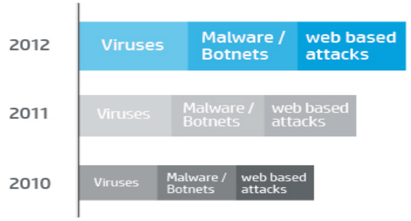
Time

Average time to resolve an attack



Malware

Most common forms of attack



HP | Ponemon Study

This is the third annual Cost of Cyber Crime Study by the Ponemon Research Institute, sponsored by HP Enterprise Security. This year's study is based on a representative sample of 56 organisations in various industry sectors of US companies, many of which are multinational corporations with 1000 enterprise seats or more. For the first time, Ponemon Institute conducted cyber crime cost studies for companies in the United Kingdom, Germany, Australia and Japan.

http://www8.hp.com/us/en/hp-news/press-release.html?id=1303754#.UJt8glF4Epy

WE ARE NOT TALKING ABOUT

- Virtualization security
- Trusted Computing Base
- Every details of Cloud Security

TODAY'S TALK ABOUT

- Security in General, Is cloud security different ?
- What process you should consider before cloud adoption?
- Major Threats against cloud
- Discussion on two focus areas:

  - Identity and access management

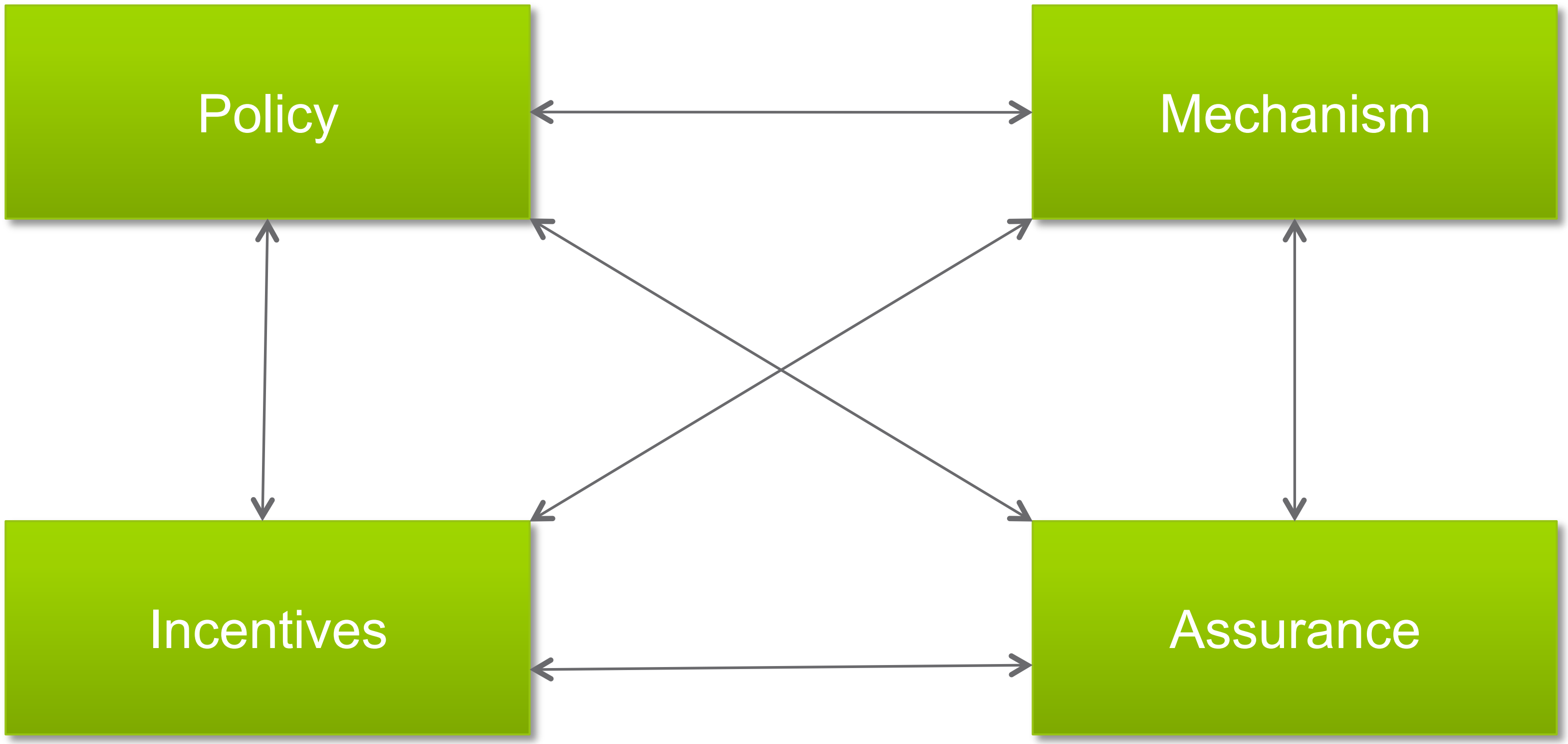
  - Governance and Compliance

SECURITY ENGINEERING

“Security engineering is building systems which remains dependable in the face of malice, error , or mischance”

The goal is to provide critical assurance

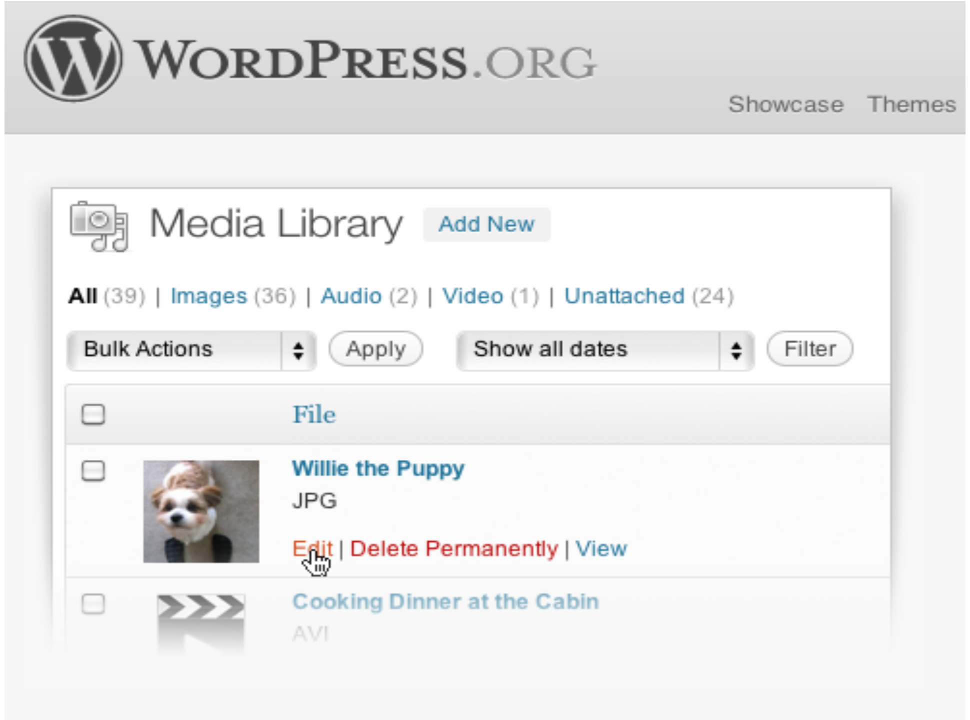
SECURITY ENGINEERING FRAMEWORK



SECURITY ENGINEERING FOR CLOUD EVALUATION

SCENARIO 1

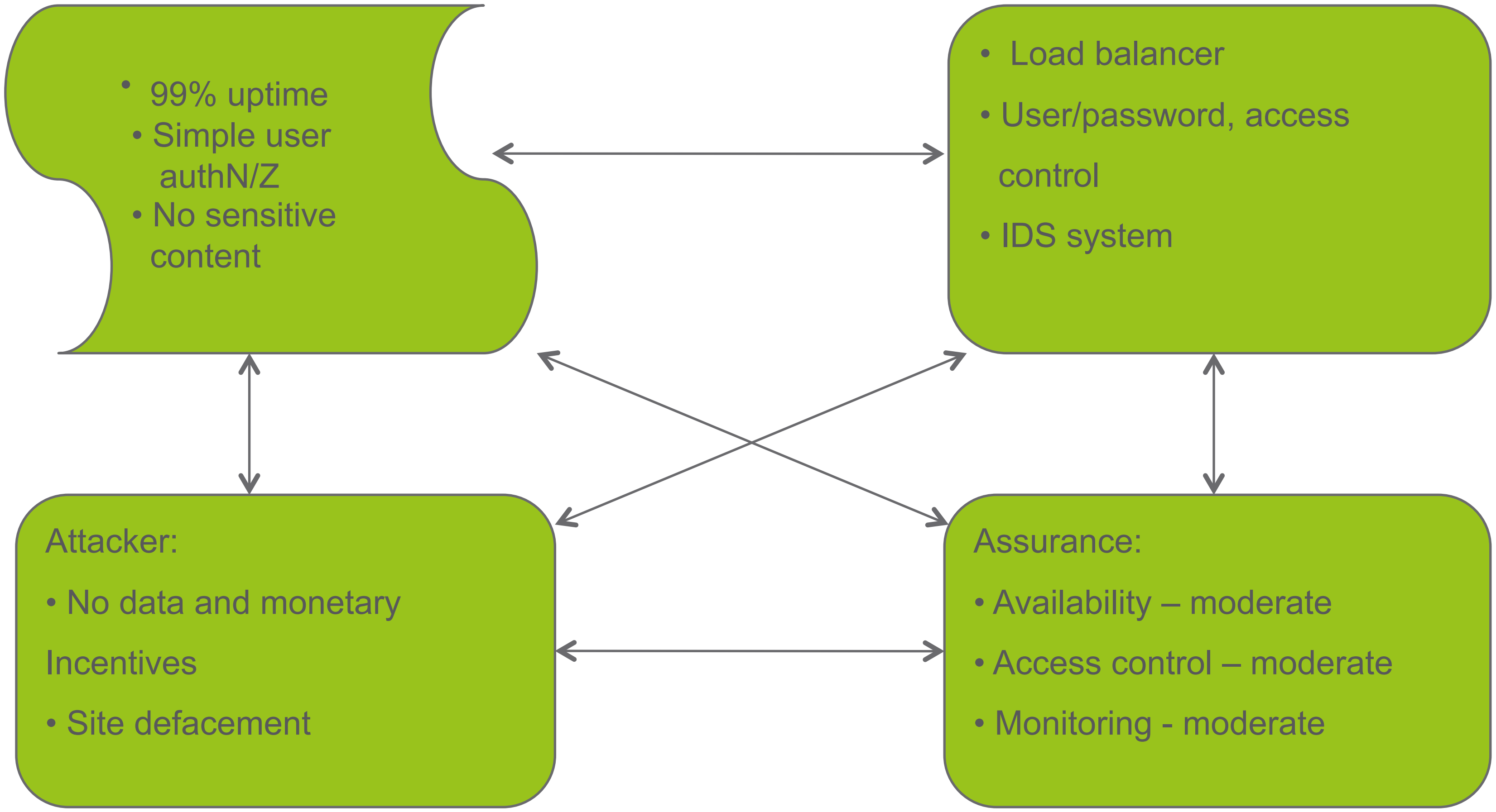
BOB'S BLOG


WordPress.org
Showcase
Themes
Media Library
Add New
All (39) | Images (36) | Audio (2) | Video (1) | Unattached (24)
Bulk Actions
Apply
Show all dates
Filter
File
Willie the Puppy
JPG
Edit | Delete Permanently | View
Cooking Dinner at the Cabin
AVI

Requirements

- Ensure uptime
- No sensitive content
- Simple user authentication
- Monitor the traffic
- Low cost

CLOUD PROVIDER A



- 99% uptime
- Simple user authN/Z
- No sensitive content

- Load balancer
- User/password, access control
- IDS system

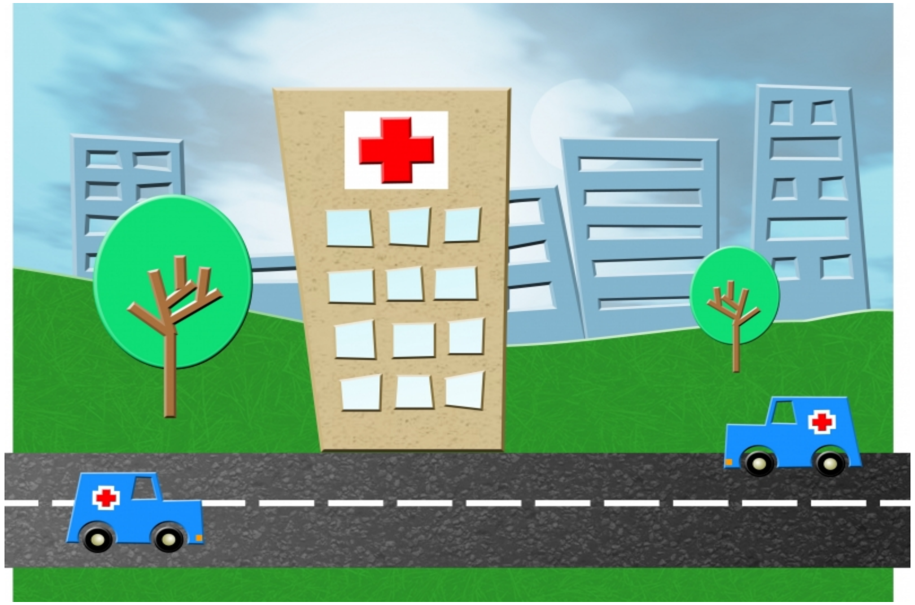
Attacker:

- No data and monetary Incentives
- Site defacement

Assurance:

- Availability – moderate
- Access control – moderate
- Monitoring - moderate

SCENARIO 2



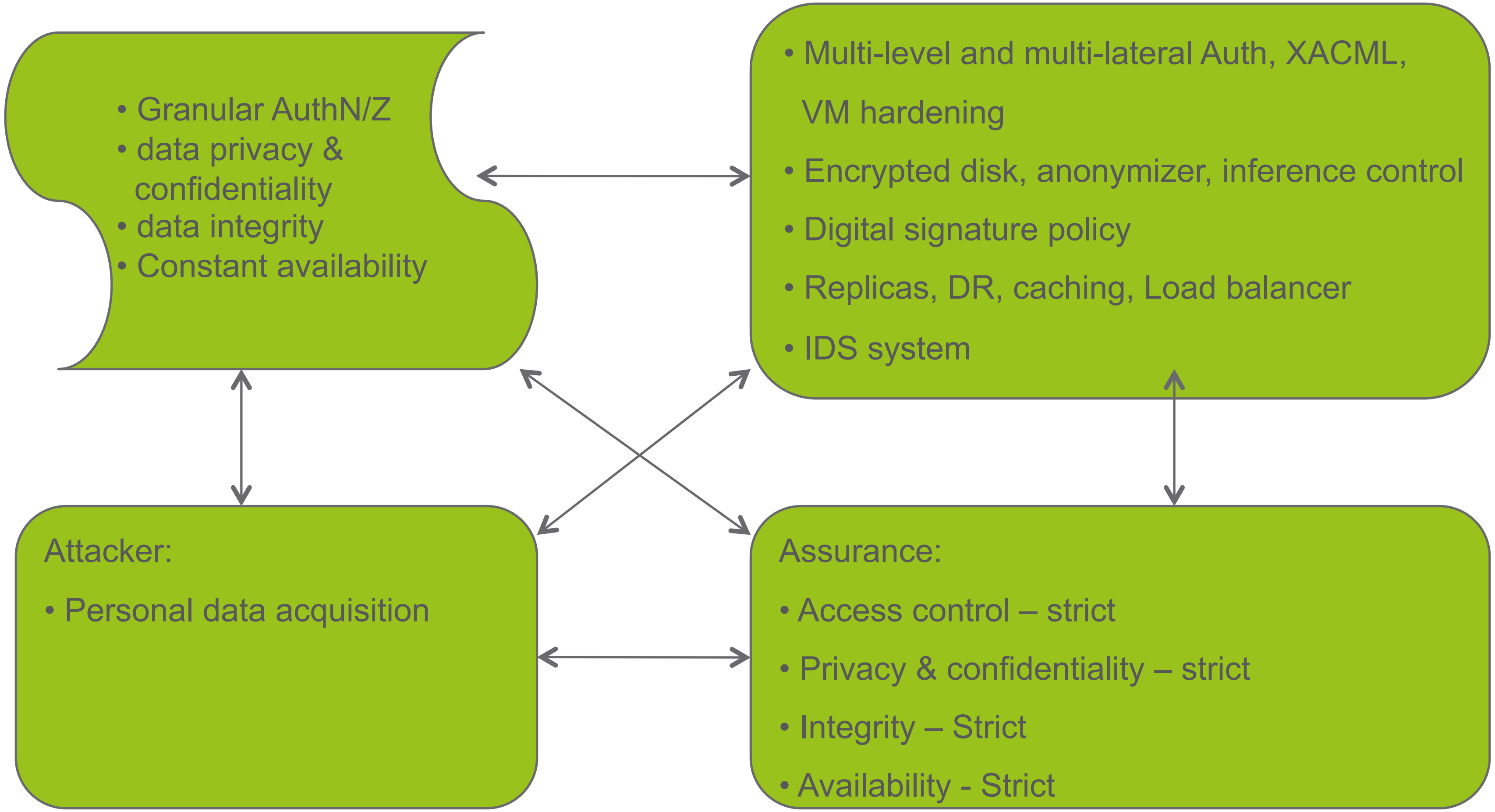
http://www.projectwalk.org/hospitals/

A HOSPITAL SYSTEM

Requirements

- Patients record are strictly confidential
- A nurse can access patient's data of her ward who stayed in last 30 days
- Doctors need strict assurance for life critical data e.g., medical and drug history
- Strict assurance for critical system

CLOUD PROVIDER B



- Granular AuthN/Z
- data privacy & confidentiality
- data integrity
- Constant availability

- Multi-level and multi-lateral Auth, XACML, VM hardening
- Encrypted disk, anonymizer, inference control
- Digital signature policy
- Replicas, DR, caching, Load balancer
- IDS system

Attacker:

- Personal data acquisition

Assurance:

- Access control – strict
- Privacy & confidentiality – strict
- Integrity – Strict
- Availability - Strict

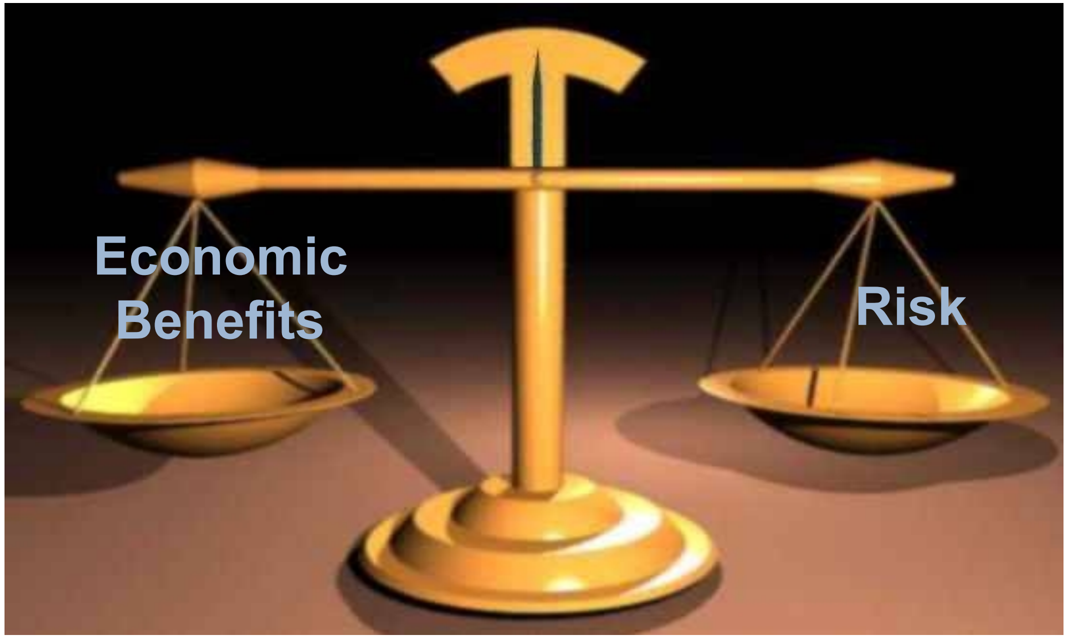
EVALUATION

Requirements	Cloud Provider A	Cloud Provider B
Assurance	Assurance: • Availability – moderate • Access control – moderate • Monitoring - ok	Assurance: • Access control – strict • Privacy & confidentiality – strict • Integrity – Strict • Availability - Strict
Deployment model	Public	Private / Public with VM hardening
Accessible and consumed by	Un-trusted	Trusted
SPI	SaaS	IaaS

SECURITY CONSIDERATIONS BEFORE CLOUD ADOPTION

SECURITY IS A BALANCE BETWEEN BENEFITS AND RISK

Security depends on how much risks we like to take in comparison to economic benefits.

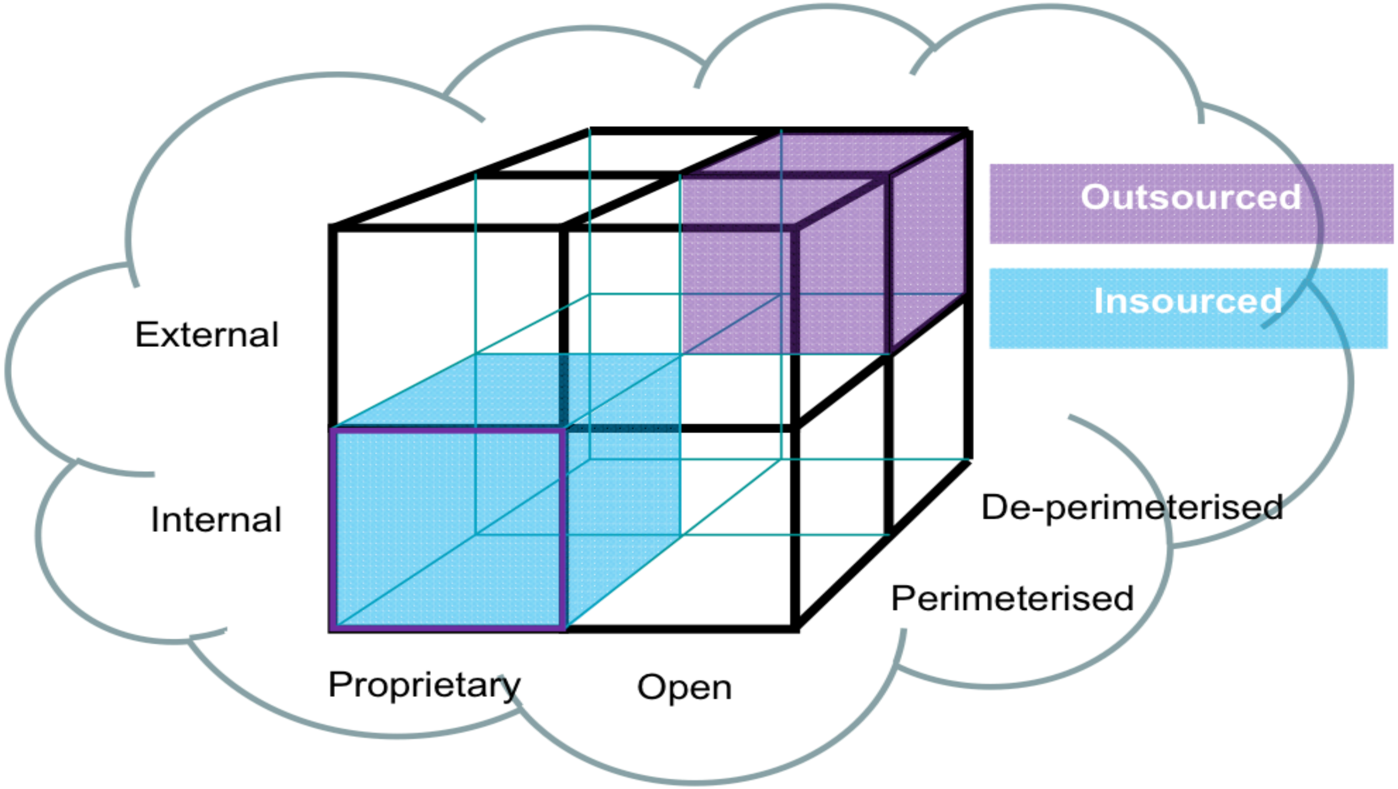


So how will we proceed ? See Next Slides

STEP 1

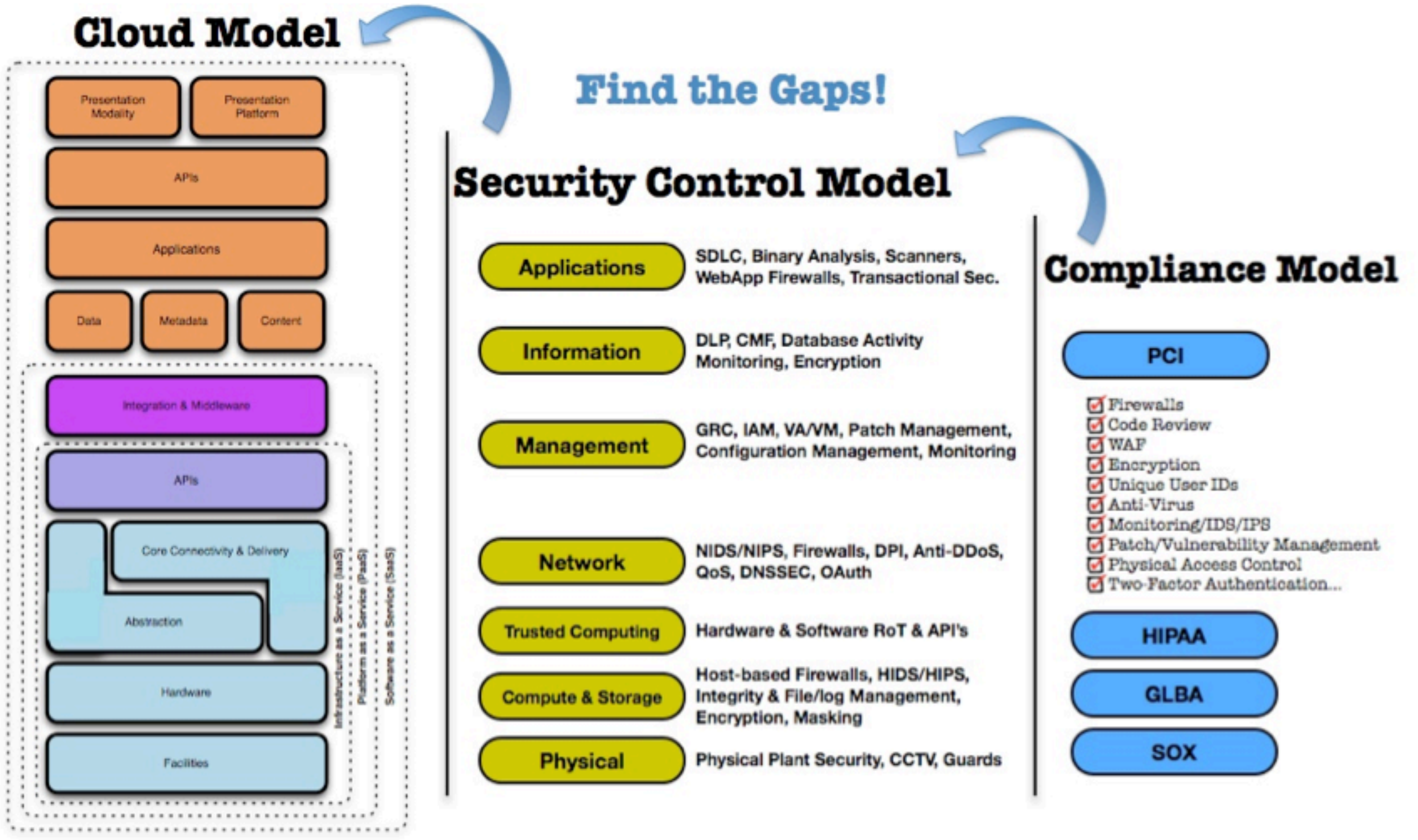
- Define assets, resources, and information being managed
- Who manages and owns them and how
- Which security controls are in place
- Identify your compliance requirements
- Define the risk you can tolerate

STEP 2: CHOOSE CLOUD MODEL



Ref: Cloud Cube, Jericho Forum

STEP 3: FIND THE GAP



Cloud Model

Find the Gaps!

Security Control Model

Applications	SDLC, Binary Analysis, Scanners, WebApp Firewalls, Transactional Sec.
Information	DLP, CMF, Database Activity Monitoring, Encryption
Management	GRC, IAM, VA/VM, Patch Management, Configuration Management, Monitoring
Network	NIDS/NIPS, Firewalls, DPI, Anti-DDoS, QoS, DNSSEC, OAuth
Trusted Computing	Hardware & Software RoT & API's
Compute & Storage	Host-based Firewalls, HIDS/HIPS, Integrity & File/log Management, Encryption, Masking
Physical	Physical Plant Security, CCTV, Guards

Compliance Model

PCI

- ☑ Firewalls
- ☑ Code Review
- ☑ WAF
- ☑ Encryption
- ☑ Unique User IDs
- ☑ Anti-Virus
- ☑ Monitoring/IDS/IPS
- ☑ Patch/Vulnerability Management
- ☑ Physical Access Control
- ☑ Two-Factor Authentication...

HIPAA

GLBA

SOX

Ref: Security Guidance for Critical Areas of Focus in Cloud Computing V3.0

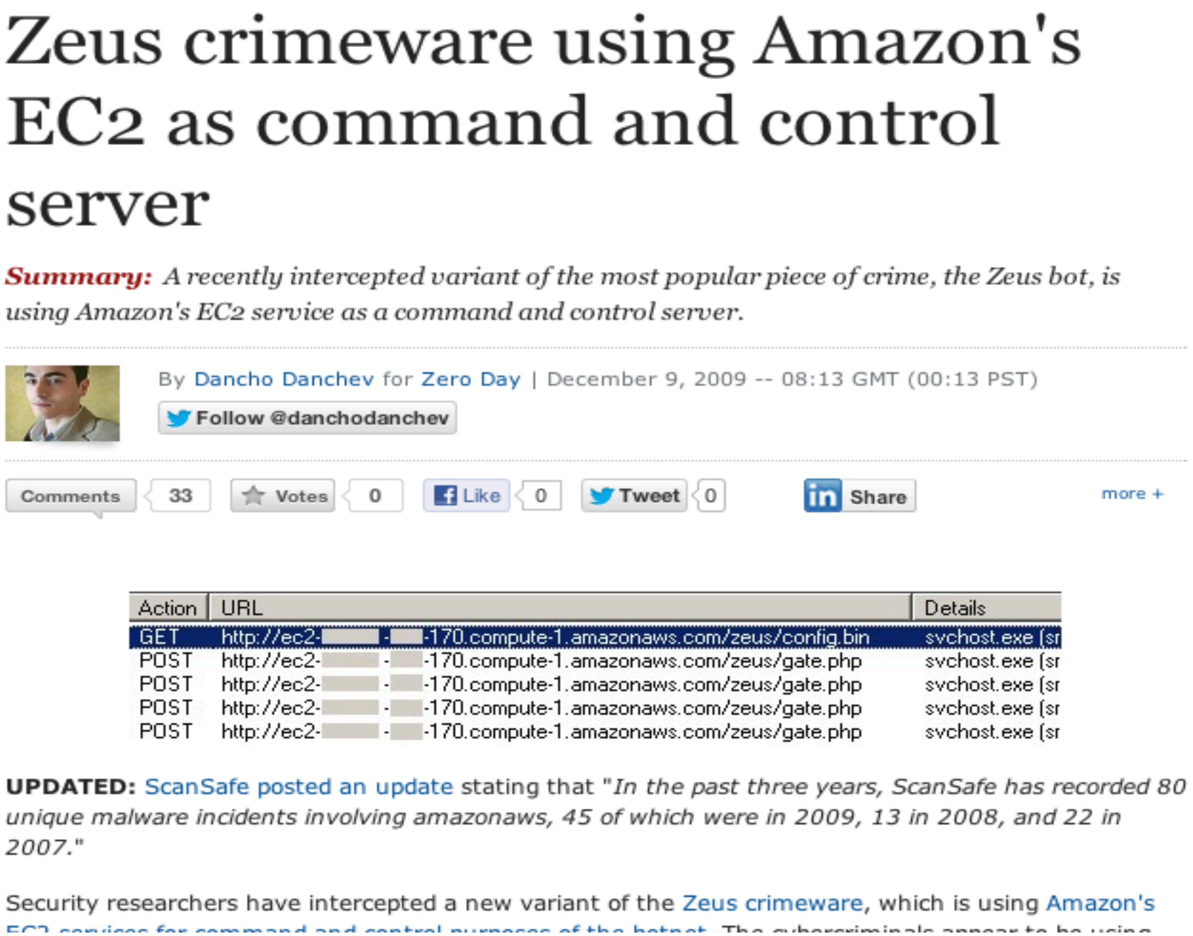
THREATS IN CLOUD

CLOUD SECURITY ALLIANCE - TOP THREATS IN CLOUD

- Abuse and Nefarious use of cloud
- Insecure Interfaces and APIs
- Malicious Insiders
- Shared Technology (Isolation) Issue
- Data Loss or Leakage
- Account or Service hacking
- Unknown risk profile

Source: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

Nefarious use of Cloud



Zeus crimeware using Amazon's EC2 as command and control server

Summary: *A recently intercepted variant of the most popular piece of crime, the Zeus bot, is using Amazon's EC2 service as a command and control server.*

By Dancho Danchev for Zero Day | December 9, 2009 -- 08:13 GMT (00:13 PST)

Action	URL	Details
GET	http://ec2-[redacted]-[redacted]-170.compute-1.amazonaws.com/zeus/config.bin	svchost.exe (sr
POST	http://ec2-[redacted]-[redacted]-170.compute-1.amazonaws.com/zeus/gate.php	svchost.exe (sr
POST	http://ec2-[redacted]-[redacted]-170.compute-1.amazonaws.com/zeus/gate.php	svchost.exe (sr
POST	http://ec2-[redacted]-[redacted]-170.compute-1.amazonaws.com/zeus/gate.php	svchost.exe (sr
POST	http://ec2-[redacted]-[redacted]-170.compute-1.amazonaws.com/zeus/gate.php	svchost.exe (sr

UPDATED: ScanSafe posted an update stating that "*In the past three years, ScanSafe has recorded 80 unique malware incidents involving amazonaws, 45 of which were in 2009, 13 in 2008, and 22 in 2007.*"

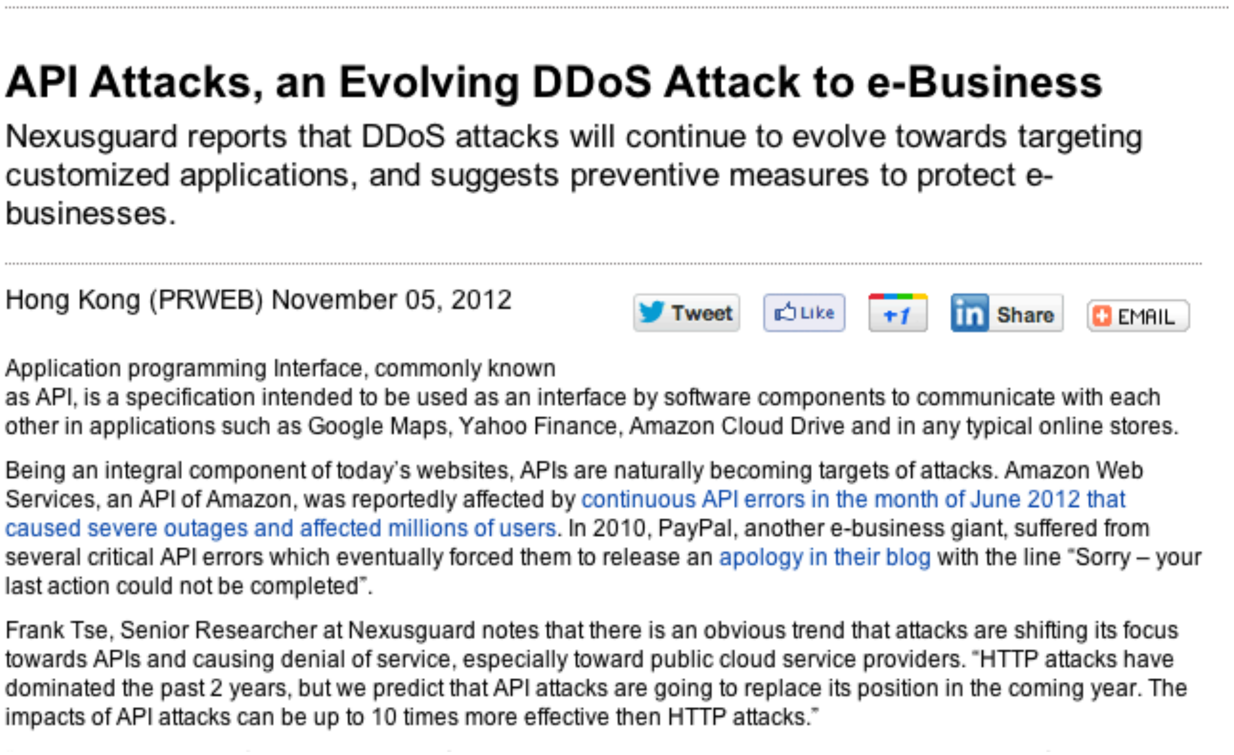
Security researchers have intercepted a new variant of the Zeus crimeware, which is using Amazon's EC2 services for command and control purposes of the botnet. The cybercriminals appear to be using

http://blogs.zdnet.com/security/?p=5110

Recommendations:

1. Strict registration
2. Enhanced monitoring

# Insecure interfaces and APIs



API Attacks, an Evolving DDoS Attack to e-Business

Nexusguard reports that DDoS attacks will continue to evolve towards targeting customized applications, and suggests preventive measures to protect e-businesses.

Hong Kong (PRWEB) November 05, 2012

Application programming Interface, commonly known as API, is a specification intended to be used as an interface by software components to communicate with each other in applications such as Google Maps, Yahoo Finance, Amazon Cloud Drive and in any typical online stores.

Being an integral component of today's websites, APIs are naturally becoming targets of attacks. Amazon Web Services, an API of Amazon, was reportedly affected by continuous API errors in the month of June 2012 that caused severe outages and affected millions of users. In 2010, PayPal, another e-business giant, suffered from several critical API errors which eventually forced them to release an apology in their blog with the line "Sorry – your last action could not be completed".

Frank Tse, Senior Researcher at Nexusguard notes that there is an obvious trend that attacks are shifting its focus towards APIs and causing denial of service, especially toward public cloud service providers. "HTTP attacks have dominated the past 2 years, but we predict that API attacks are going to replace its position in the coming year. The impacts of API attacks can be up to 10 times more effective then HTTP attacks."

http://www.prweb.com/releases/2012/11/prweb10092437.htm

Recommendations:

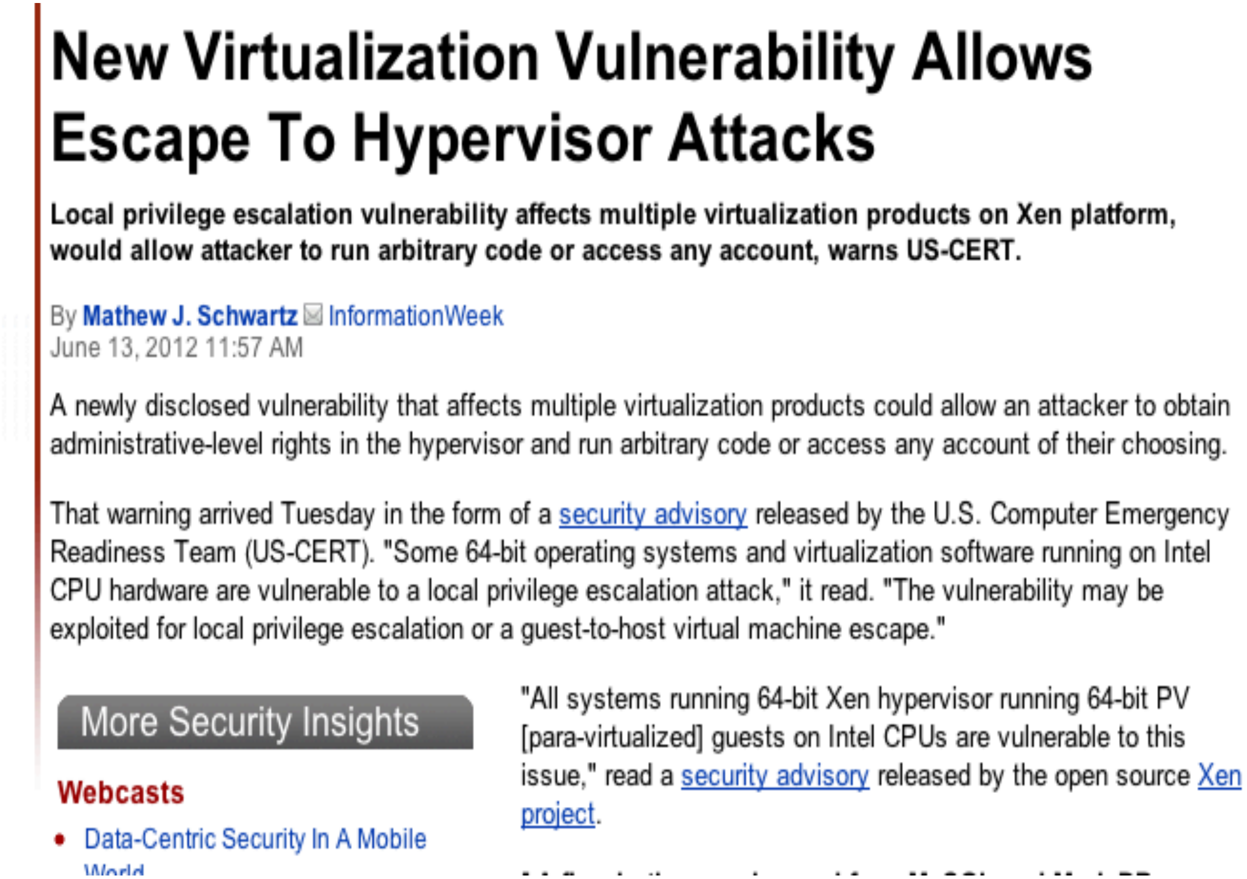
1. Analyze CSP's security
2. Strong access control
3. Understand API dependency chain

# Malicious Insider

Photo credit: http://clicksafe.kensington.com/laptop-security-blog/bid/50771/Tackling-data-theft-from-insiders

Recommendations:

1. Strict supply chain
2. Multi-level and
   Multi-lateral security



New Virtualization Vulnerability Allows Escape To Hypervisor Attacks

Local privilege escalation vulnerability affects multiple virtualization products on Xen platform, would allow attacker to run arbitrary code or access any account, warns US-CERT.

By **Mathew J. Schwartz** ✉ InformationWeek
June 13, 2012 11:57 AM

A newly disclosed vulnerability that affects multiple virtualization products could allow an attacker to obtain administrative-level rights in the hypervisor and run arbitrary code or access any account of their choosing.

That warning arrived Tuesday in the form of a security advisory released by the U.S. Computer Emergency Readiness Team (US-CERT). "Some 64-bit operating systems and virtualization software running on Intel CPU hardware are vulnerable to a local privilege escalation attack," it read. "The vulnerability may be exploited for local privilege escalation or a guest-to-host virtual machine escape."

More Security Insights

Webcasts

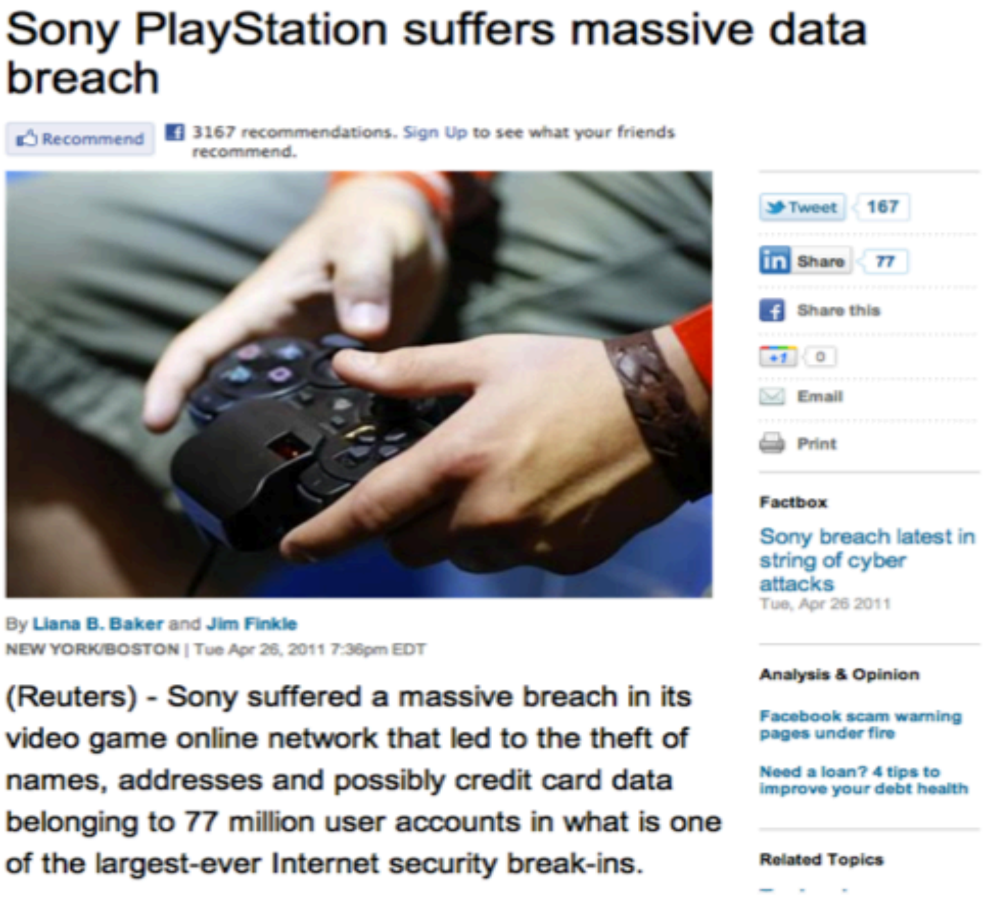
- Data-Centric Security In A Mobile World

"All systems running 64-bit Xen hypervisor running 64-bit PV [para-virtualized] guests on Intel CPUs are vulnerable to this issue," read a security advisory released by the open source Xen project.

# Shared Technology issues

Recommendations:

1. Strong access control
2. Perform vulnerability scanning
3. Monitor environment



Sony PlayStation suffers massive data breach

Recommend 3167 recommendations. Sign Up to see what your friends recommend.

Tweet 167

Share 77

Share this

+1 0

Email

Print

Factbox

Sony breach latest in string of cyber attacks

Tue, Apr 26 2011

By Liana B. Baker and Jim Finkle

NEW YORK/BOSTON | Tue Apr 26, 2011 7:36pm EDT

(Reuters) - Sony suffered a massive breach in its video game online network that led to the theft of names, addresses and possibly credit card data belonging to 77 million user accounts in what is one of the largest-ever Internet security break-ins.

Analysis & Opinion

Facebook scam warning pages under fire

Need a loan? 4 tips to improve your debt health

Related Topics

# Data loss

Recommendations:

1. Strong API access control
2. Encrypt the data
3. Data protection design

CSA
Security Guidance for Critical Areas of Cloud Computing Version 3.0

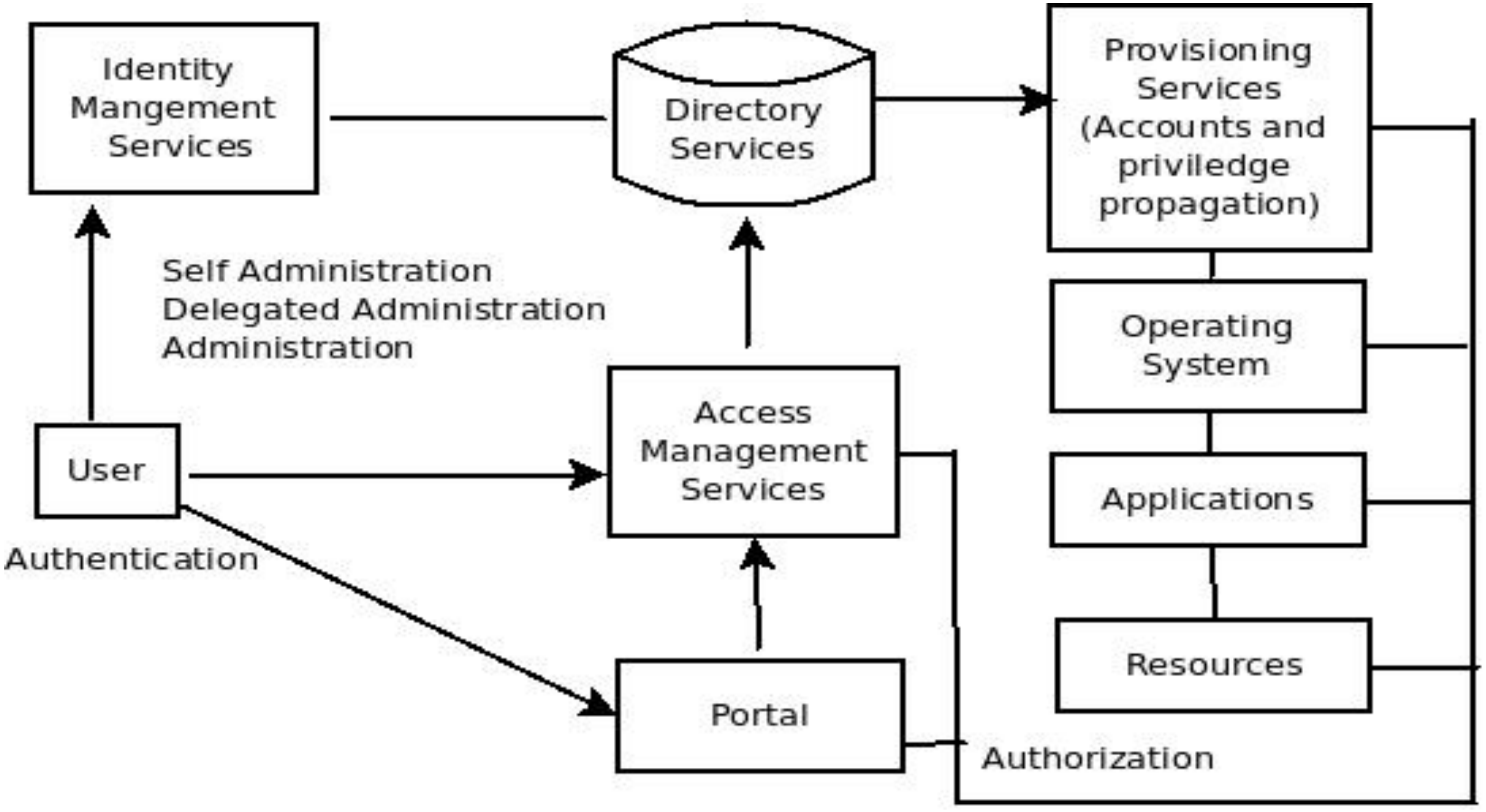
IDENTITY, ENTITLEMENT AND ACCESS MANAGEMENT

"Identity and Access Management (IAM) should provide controls for assured identities and access management."

IDENTITY MANAGEMENT

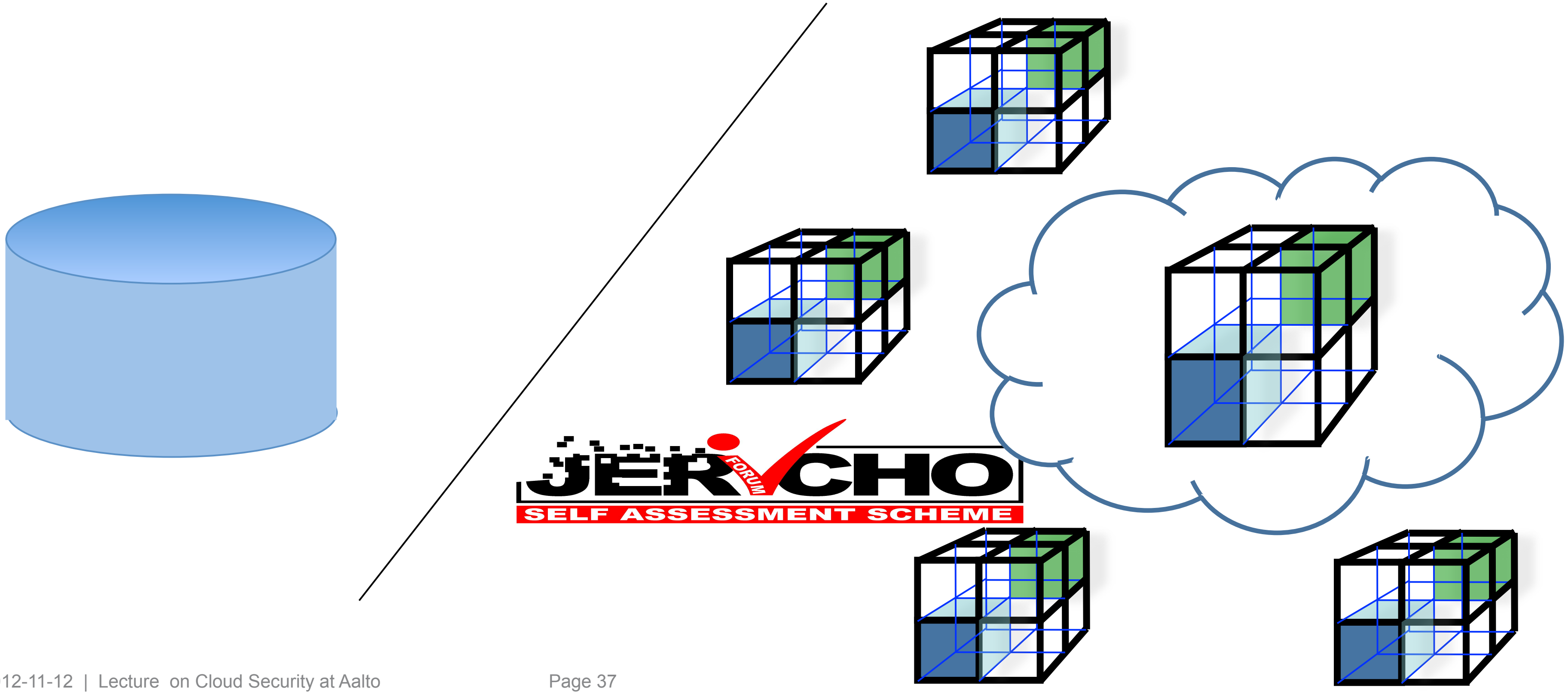
Identification	Authentication	Authorization
Who are you	Prove it	Here is the resource
An identifier that can be used to uniquely recognize a principal	The process to verify the identity of a principal	The granting of rights and capabilities to the principal by the system

OLD SCHOOL OF IAM



WHAT'S NEW IN CLOUD IAM SYSTEM

The changing business need requires a new identity perimeter for the cloud



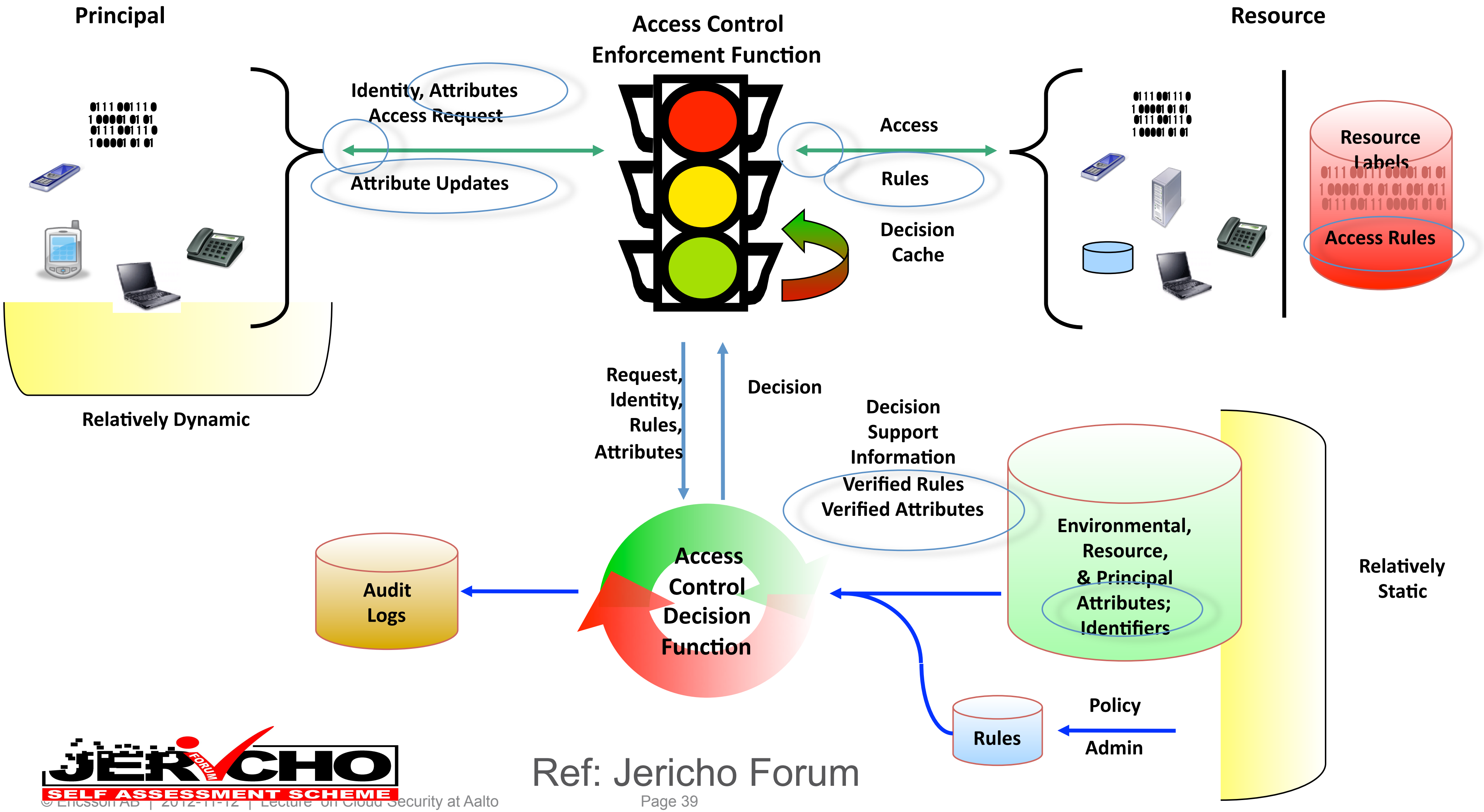
OLD SCHOOL VS. NEW SCHOOL

Old School	New School
Enterprise Centric	Principal Centric
Access Control List	Resource Centric
Directory Server	Rule Based Access
Authentication	Authentication Routing

JERICHO FORUM
SELF ASSESSMENT SCHEME

Symmetrical

Evolving Jericho Authorization Model



Principal

Access Control
Enforcement Function

Resource

Identity, Attributes
Access Request

Attribute Updates

Access

Rules

Decision
Cache

Resource
Labels

Access Rules

Relatively Dynamic

Request,
Identity,
Rules,
Attributes

Decision

Decision
Support
Information
Verified Rules
Verified Attributes

Environmental,
Resource,
& Principal
Attributes;
Identifiers

Relatively
Static

Audit
Logs

Access
Control
Decision
Function

Rules

Policy
Admin

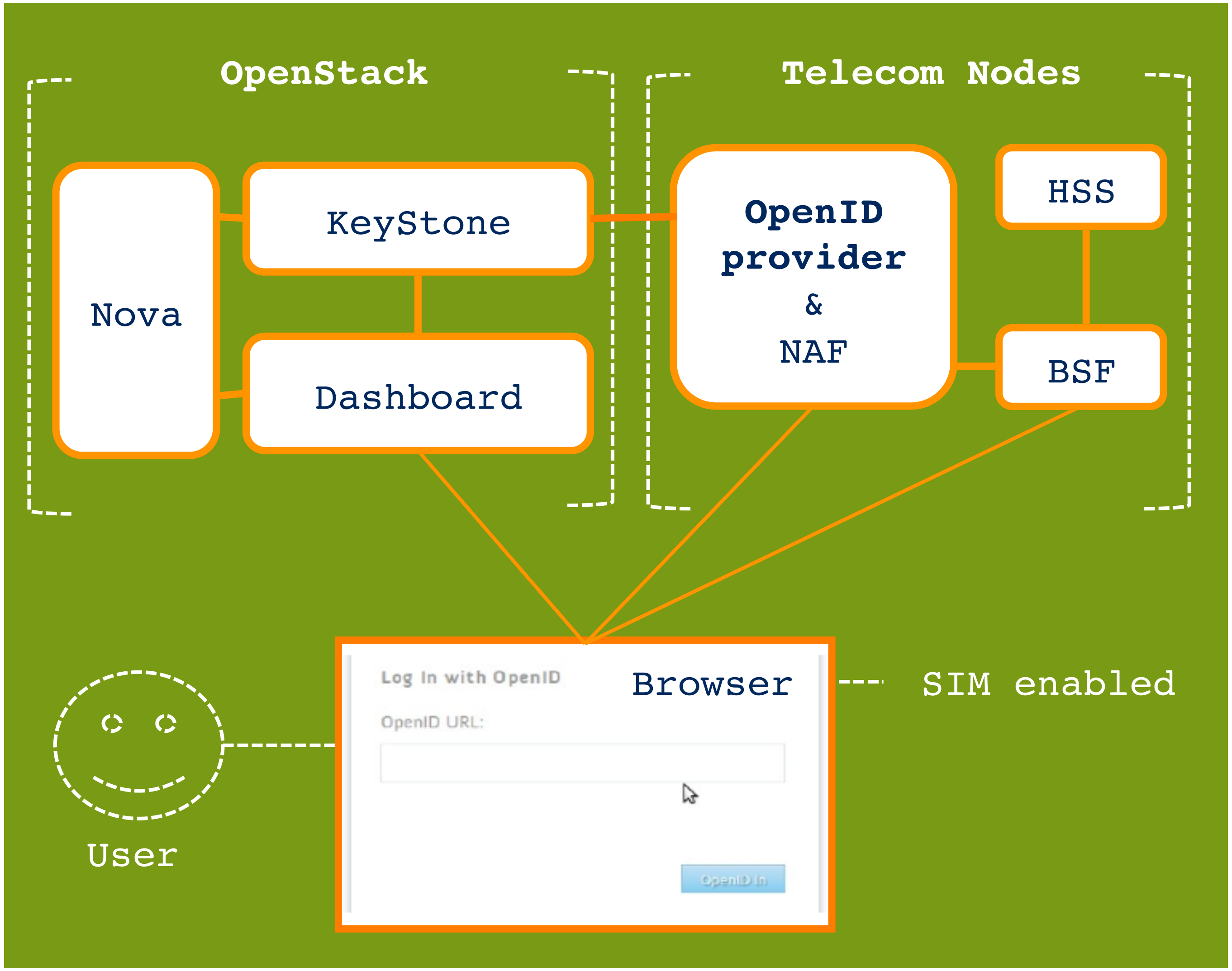
JERICHO FORUM
SELF ASSESSMENT SCHEME

Ref: Jericho Forum

RECOMMENDATION

- Support for SSO & federation (e.g., OpenID, SAML, OAuth)
- Identity attributes need to be consumed from multiple sources
- Support for granular authorization (e.g., XACML)
- Support for standard provisioning languages (e.g., through SPML)
- Be careful about sensitive personal data (SPI)
- Reuse identity rather than create new one

ERICSSON IN CLOUD IDENTITY: OPENID WITH GBA FOR CLOUD AUTHENTICATION



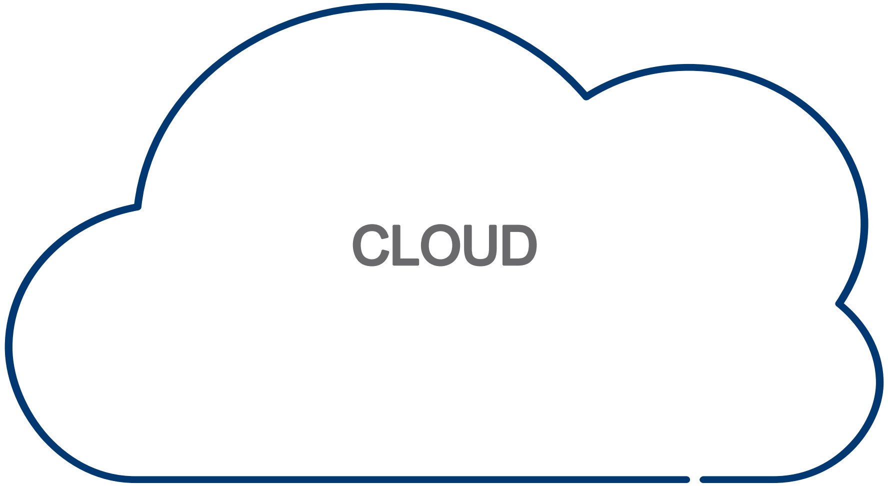
- ✓ A prototype based on 3GPP defined 'OpenID with GBA' to integrate federated and secure SIM-based authentication to the IaaS management layer.

GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE

WHY GRC IS IMPORTANT IN CLOUD

- Lack of user control
- Dynamic allocation means resource is not known beforehand
- Separation of logical and physical entities
- Location independence

COMPLIANCE IN CLOUD



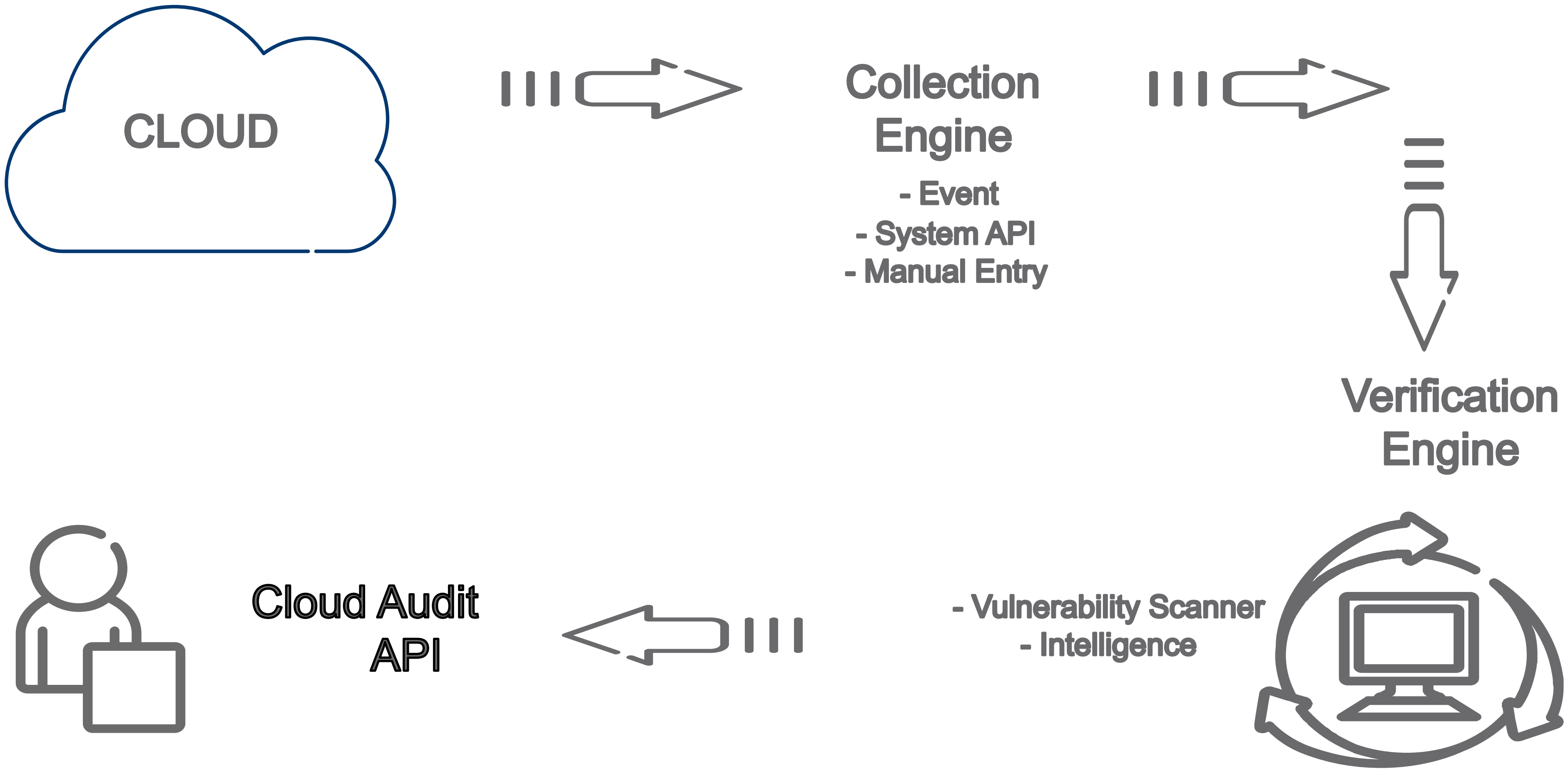
- Can I assess trust in a cloud provider ?
- Is there a way to automatically verify trust in real time?
- Is there an easy way to expose this information?

CSA GRC STACK

	Description
CTP™	- Common technique and nomenclature to request and receive evidence and affirmation of current cloud service operating circumstances from cloud providers
Cloud Audit™	- Common interface and namespace to automate the Audit, Assertion, Assessment, and Assurance (A6) of cloud environments
CAI™	- Industry-accepted ways to document what security controls exist
CCM™	- Fundamental security principles in specifying the overall security needs of a cloud consumers and assessing the overall security risk of a cloud provider

https://cloudsecurityalliance.org/wp-content/uploads/2011/12/GRC-Stack-CSA-Congress-2011-part-1.pptx

AN APPROACH FOR COMPLIANCE MONITORING



CLOUD

Collection Engine

- Event
- System API
- Manual Entry

Verification Engine

- Vulnerability Scanner
- Intelligence

Cloud Audit API

TAKE AWAY

- Security in cloud is not that different, rather risk has changed or new risk has emerged
- Always evaluate the risk of your assets before transition towards cloud
- Remember, Attackers will exploit the threat
- Access control and compliance are important for cloud adoption
- Do design your system based on customer need, but don’t forget security.

REFERENCES

1. https://collaboration.opengroup.org/jericho/cloud_cube_model_v1.0.pdf
2. https://**cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf**
3. **Chapter 1, Chapter 9, Ross Anderson, Security Engineering**
4. **Domain 1, Domain 12, Security Guidance For Critical Areas of Focus in Cloud Computing V3.0, CSA**
5. **OpenID authentication as a service in OpenStack, 7th International Conference on Information Assurance and Security (IAS), 2011**
6. **CSA - Cloud Control Matrix, https://cloudsecurityalliance.org/research/ccm/**

ERICSSON