Wolkenbruch

dn Systems

Angriffe auf Cloud-Infrastrukturen – Wie kann man sich schützen?

Lukas Grunwald

ISD Brühl

Who am I

- Lukas Grunwald
  - Security Consulting since 1998
  - Founder DN-Systems Enterprise Internet Sol. GmbH
  - Speaker at BlackHat, DefCon, PoC, Coinsec …
  - Writes for Heise
    - https://www.heise.de/suche/?q=%22Lukas+Grunwald%22&search_submit.x=0&search_submit.y=0&rm=search&sort_by=date
- DN-Systems
  - Operates own Security Lab
  - Integral Security (not only ICT)
  - Malware and APT Analysis
  - Investigation / Digital Forensics
  - Consulting IT-Companies on global scale

Agenda

- Cloud Concepts
- Top Threats: #1-7
- Challenges: Cloud security
- Vulnerabilities
- Metrics for Vulnerabilities
- Hypervisor in detail
- Attack to Cloud specific designs
- Golden rules to take from this presentation

Hype or reality?

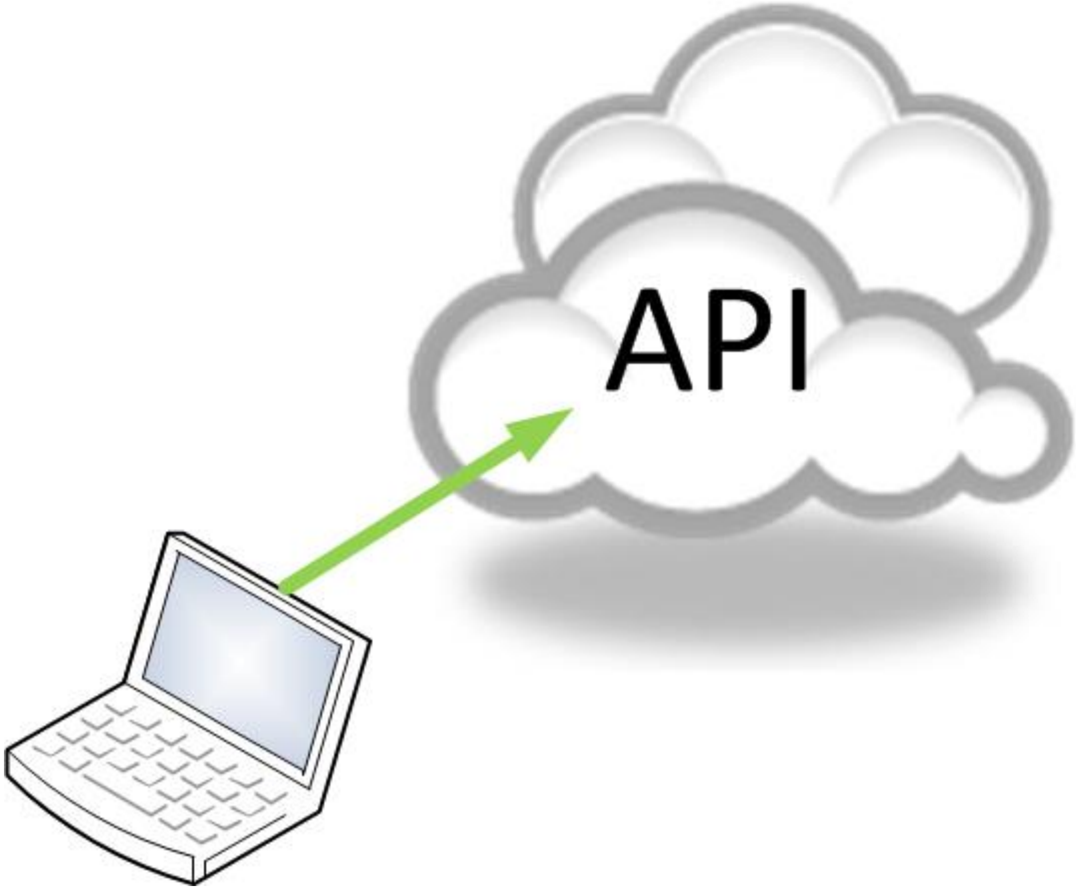
- Gartner: Cloud computing is the most over-hyped term in IT
- Services like Amazon EC2 and Azure are publicly available
- Even if you don’t use Cloud technology there are next to no ways to avoid them
- Millions of customer data end up at “Salesforce.com”

Cloud concepts: IaaS

Cloud concepts: IaaS

- IaaS - “Infrastructure as a Service”
  - Highest level of control available to customers: Customers build VMs and deploy them
  - Cloud service provider’s network
  - Network security ISP
  - System security customer
  - IaaS provider offers
    - Compute power, cooling, and network connectivity
  - The rest of the security equation is the customer’s problem
  - Examples: Amazon EC2

Cloud concepts: PaaS



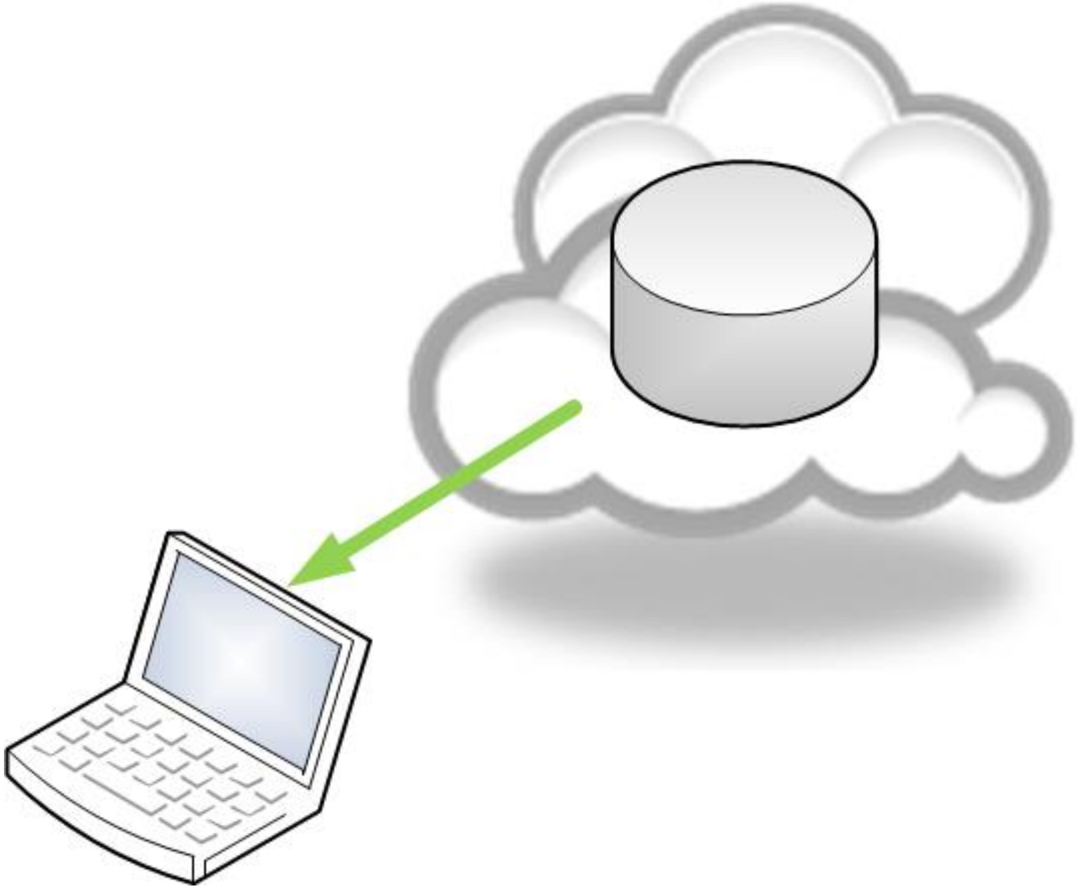
Cloud concepts: PaaS

- PaaS - ”Platform as a Service”
  - Programming model on a development framework.
  - These platforms expose APIs:
    - To developers
    - Abstract the database services and computing platforms
    - Offers rapid development of web enabled services
  - Examples: Cisco Webex Connect, Amazon Web Services

Cloud concepts: PaaS

- PaaS - ”Platform as a Service”
  - Security:
    - Core security is usually handled by the PaaS provider
    - The applications themselves must follow secure coding practices
    - Provider is not claiming to enforce security on systems
    - Network Security by provider
    - System Security by provider
    - Database Security by provider
    - Logical System Separation is handled by provider

Cloud concepts: SaaS



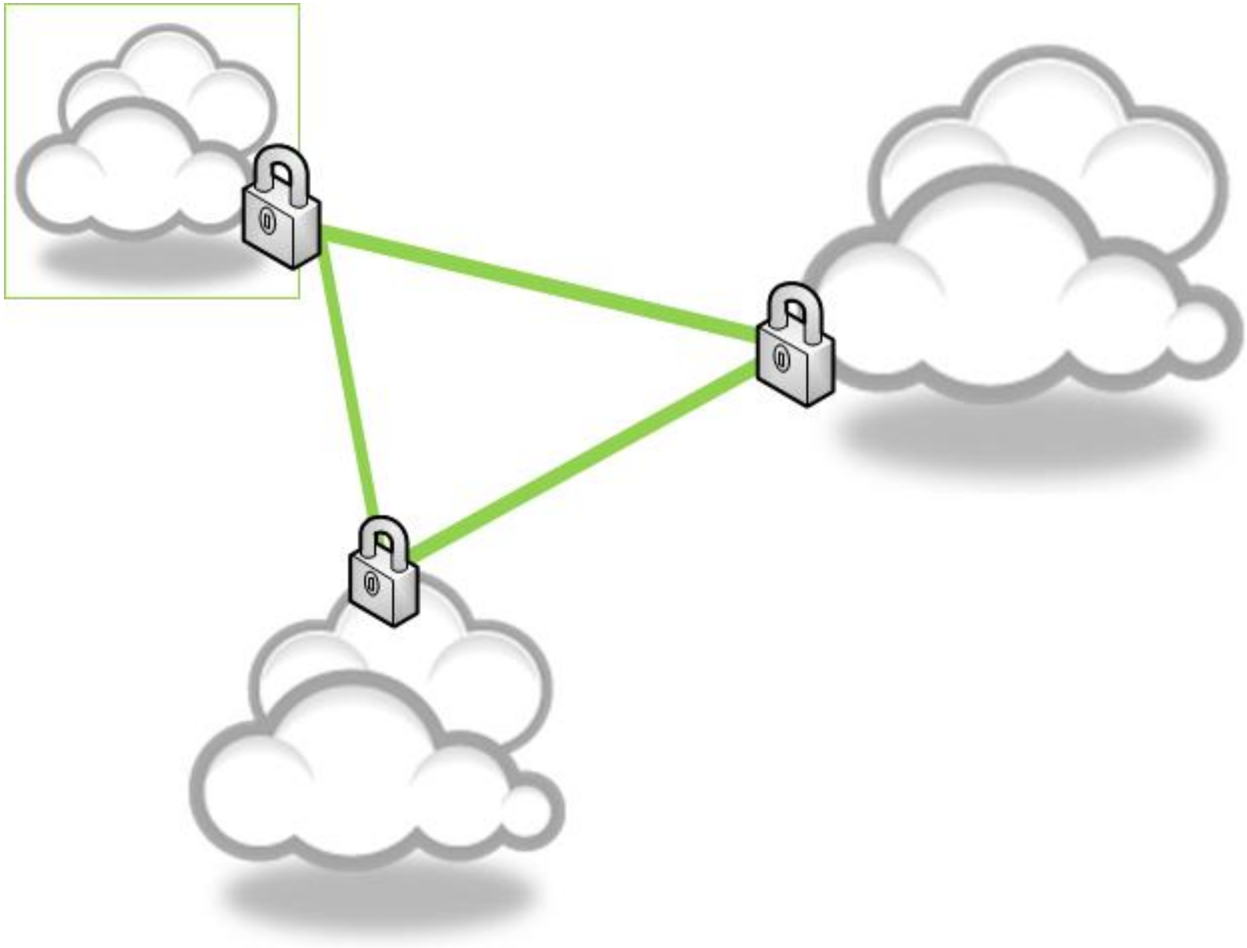
Cloud concepts: SaaS

- SaaS – “Software as a Service”
  - Most common cloud offering
  - Allows a user to purchase seats for an application that is:
    - Hosted by provider
    - Maintained by provider
    - Administered by provider
    - System security by provider
    - Network security by provider
  - Examples: Cisco Webex, Salesforce.com, etc

Cloud concepts: SaaS

- SaaS – “Software as a Service”
  - Security issues:
    - This cloud model offers limited visibility into the security process of the service provider.
    - SLAs are pretty much all you will have to enforce your own security requirements.
    - A SaaS provider often promise a stronger security posture for an organization that does not have the budget or the manpower to implement strong security.

Cloud types: VPC



Cloud types: VPC

- Virtual Private cloud
  - Deployment utilizes VPN technology
  - Create a secure pipe via cloud provider’s network
  - Dedicated computing resources.
    - No shared environment
    - VPN technology is essential
    - Network paths are shared but secured by VPN

Cloud types: C-Cloud

Cloud types: C-Cloud

- Community Cloud
  - A consortium of organizations with similar
    - Service requirements
    - Policies
    - Interests
  - Join together to benefit from a common infrastructure.
  - Examples: Group of schools, collectives, agricultural production cooperative, …

Public Cloud

Cloud types: Public-Cloud

- Public cloud services
  - Offered to the public for a fee
  - Operated by a cloud service provider
  - Everyone who pays for it can be part of this
- Example: Google Apps, Amazon, Microsoft Azure, …

Cloud types: Hybrid-Cloud

- Hybrid Cloud
  - A model that uses any combination of
    - Public, Private or Virtual private Community
    - Mixture of internal applications and services
  - Provides a mechanism to increase capacity on demand
  - Optionally moves less sensitive applications to cloud services.

Agenda

- Cloud Concepts
- Top Threats: #1
- Challenges: Cloud security
- Vulnerabilities
- Metrics for Vulnerabilities
- Hypervisor in detail
- Attack to Cloud specific designs
- Golden rules to take from this presentation

Top Threats: #1

- Malicious use of cloud computing
  - IaaS providers offer customers the illusion of unlimited compute, network, and storage capacity
  - A simple registration process with free trial is offered
    - A valid (stolen) credit card allows a user to immediately use cloud services with total anonymity

Top Threats: #1

- Malicious use of cloud computing
  - Criminals like clouds:
    - Spammers, malicious code authors, hackers and other criminals have been able to conduct their activities on a large scale.
  - PaaS providers have traditionally suffered most from this kind of attacks; however, recent evidence shows that hackers have begun to target IaaS vendors as well.

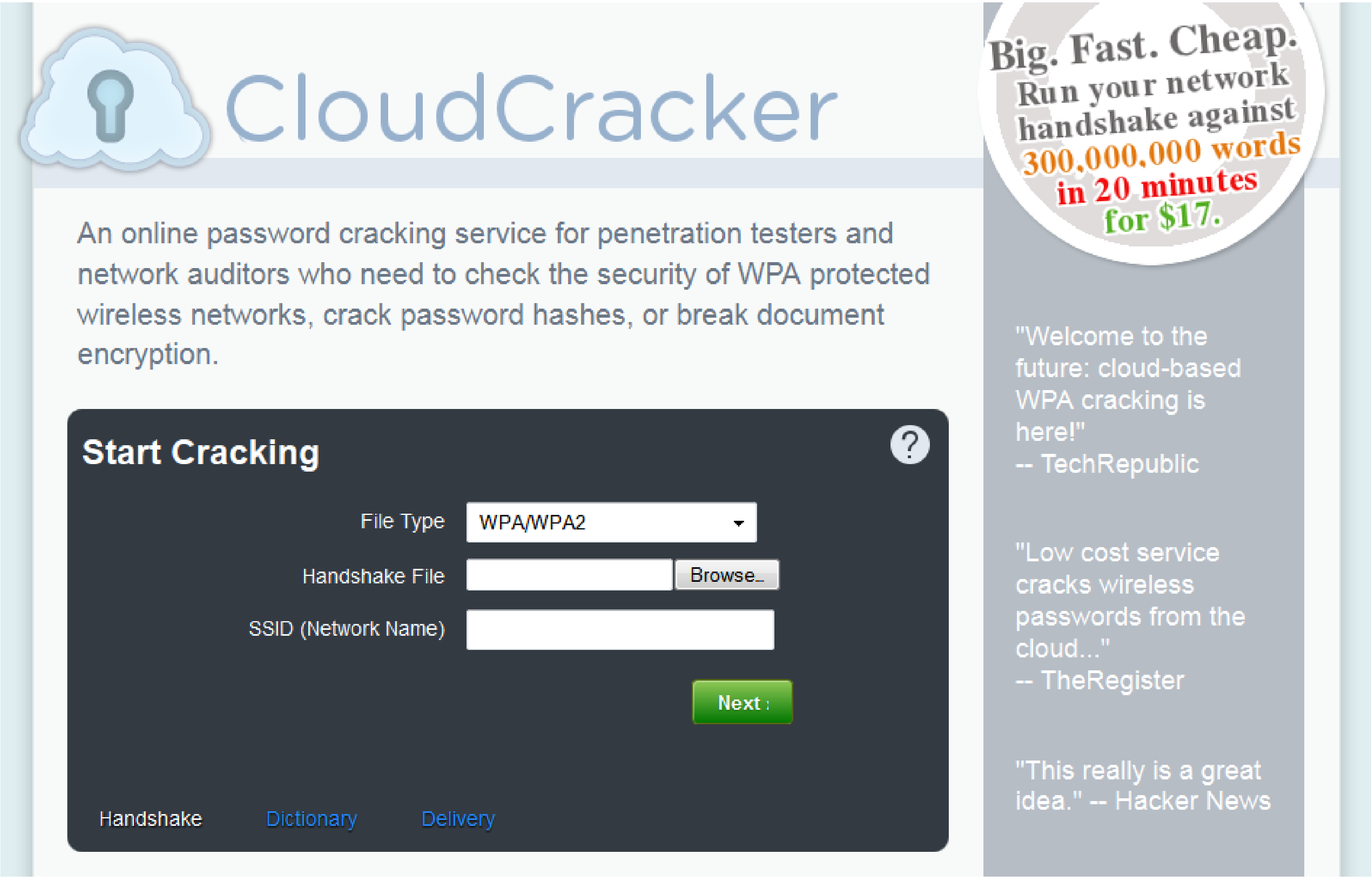
Top Threats: #1

- Malicious use of cloud computing
  - Actual services on a malicious cloud are:
  - Password and key cracking (DES in 5 min.)
  - dDoS as a service
  - Launching dynamic attack points
  - Hosting malicious data and botnet command and control servers
  - Building rainbow tables and captcha solving farms (to crack GSM cipher, etc…).

Top Threats: #1

- Malicious use of cloud computing examples:
  - Hosted the Zeus botnet, InfoStealer trojans
  - Cloud Cracker offers:
    - WPA/WPA2, NTLM, SHA-512 (UNIX PW), MD5 (UNIX PW), MS-CHAPv2 (PPTE, WPA-E) cracking
  - https://cloudcracker.com/
- Reduces the security of these security protocols

Top Threats: #1



CloudCracker

Big. Fast. Cheap. Run your network handshake against 300,000,000 words in 20 minutes for $17.

An online password cracking service for penetration testers and network auditors who need to check the security of WPA protected wireless networks, crack password hashes, or break document encryption.

Start Cracking

File Type: WPA/WPA2

Handshake File: Browse...

SSID (Network Name):

"Welcome to the future: cloud-based WPA cracking is here!"
-- TechRepublic

"Low cost service cracks wireless passwords from the cloud..."
-- TheRegister

"This really is a great idea." -- Hacker News

Agenda

- Cloud Concepts
- Top Threats: #2
- Challenges: Cloud security
- Vulnerabilities
- Metrics for Vulnerabilities
- Hypervisor in detail
- Attack to Cloud specific designs
- Golden rules to take from this presentation

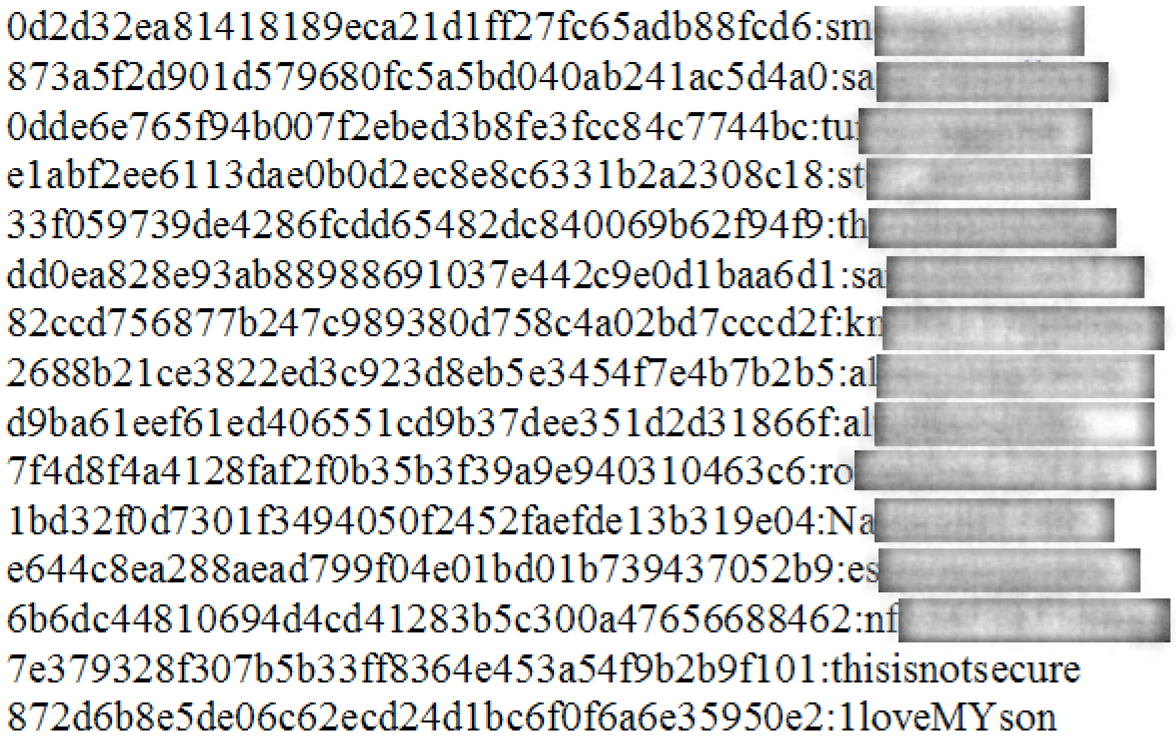
Top Threats: #2

- Cloud Computing providers expose software interfaces or APIs to:
  - Customers and attackers
  - From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to be broken
  - Many times they introduce an additional complexity of new layered API (KISS violation)

Top Threats: #2

- Examples of Cloud Computing providers break-ins:
  - LinkedIn lost Password-Hashes
    - Cloud can be used to crack the leaked passwords (Thread #1)
  - Sony Playstation Network
    - Lost all user credentials as well all credit card numbers

Top 10 Threats: #2



```
0d2d32ea81418189eca21d1ff27fc65adb88fcd6:sm[redacted]
873a5f2d901d579680fc5a5bd040ab241ac5d4a0:sa[redacted]
0dde6e765f94b007f2ebed3b8fe3fcc84c7744bc:tu[redacted]
e1abf2ee6113dae0b0d2ec8e8c6331b2a2308c18:st[redacted]
33f059739de4286fcdd65482dc840069b62f94f9:th[redacted]
dd0ea828e93ab88988691037e442c9e0d1baa6d1:sa[redacted]
82ccd756877b247c989380d758c4a02bd7cccd2f:kn[redacted]
2688b21ce3822ed3c923d8eb5e3454f7e4b7b2b5:al[redacted]
d9ba61eef61ed406551cd9b37dee351d2d31866f:al[redacted]
7f4d8f4a4128faf2f0b35b3f39a9e940310463c6:ro[redacted]
1bd32f0d7301f3494050f2452faefde13b319e04:Na[redacted]
e644c8ea288aead799f04e01bd01b739437052b9:es[redacted]
6b6dc44810694d4cd41283b5c300a47656688462:nf[redacted]
7e379328f307b5b33ff8364e453a54f9b2b9f101:thisisnotsecure
872d6b8e5de06c62ecd24d1bc6f0f6a6e35950e2:1loveMYson
```

Hashes lost, Cloud helps to recover clear-text password from hash

Agenda

- Cloud Concepts
- Top Threats: #3
- Challenges: Cloud security
- Vulnerabilities
- Metrics for Vulnerabilities
- Hypervisor in detail
- Attack to Cloud specific designs
- Golden rules to take from this presentation

Top Threats: #3

- Malicious Insiders
  - The threat of a malicious insider is well-known to most organizations, but within the cloud you relinquish much control to a third party – and their employees
  - Much profitable data in one place
  - This kind of situation clearly creates an attractive opportunity for the full scale of attackers from the hobbyist hacker over organized crime to corporate espionage

Agenda

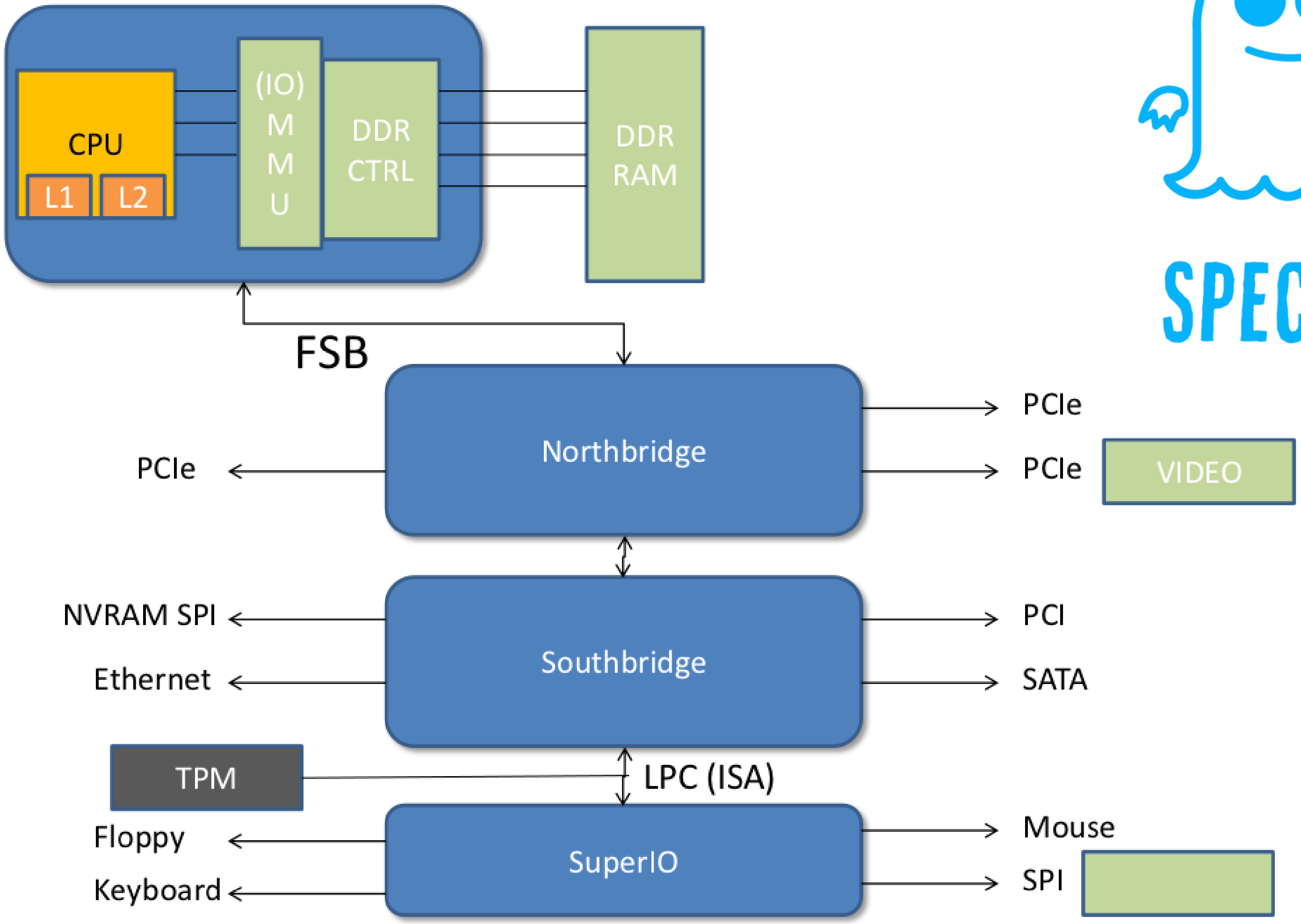
- Cloud Concepts
- Top Threats: #4
- Challenges: Cloud security
- Vulnerabilities
- Metrics for Vulnerabilities
- Hypervisor in detail
- Attack to Cloud specific designs
- Golden rules to take from this presentation

Top Threats: #4

- Shared Technology
  - Cloud vendors deliver their services cheap by sharing infrastructure.
  - Most underlying components (e.g., CPU caches, GPUs, etc.) are not designed to offer strong isolation – Spectre, Meltdown
  - A virtualization hypervisor promises to mediate access between guest operating systems and the physical compute resources
  - Hypervisors are software, and software will fail!

x86-Design

SPECTRE



Top Threats: #4

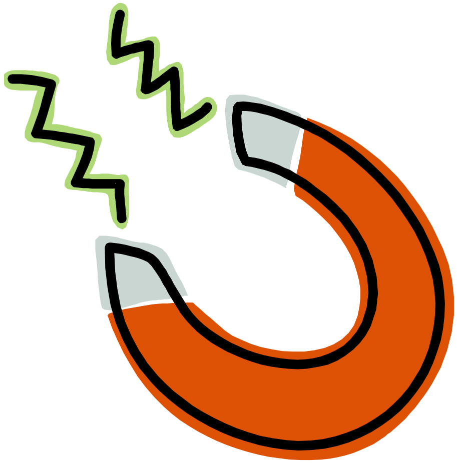
- Shared Technology - Example
  - Cloud Burst
    - Exploit for VMWare based virtualization, to break from a „Guest OS“ into the hypervisor or „Host OS“.
  - Attacker can take over control of the whole cloud
    - Full paper: www.blackhat.com/presentations/bh-usa-09/KORTCHINSKY/BHUSA09-Kortchinsky-Cloudburst-PAPER.pdf

Agenda

- Cloud Concepts
- Top Threats: #5
- Challenges: Cloud security
- Vulnerabilities
- Metrics for Vulnerabilities
- Hypervisor in detail
- Attacks to Cloud specific designs
- Golden rules to take from this presentation

Top Threats: #5

- Data Loss or Leakage
  - Cloud provider was not able to provide proper backup or authentic state of the data.
  - Customer does not have control over his data, so backup media might be shared, and so can be accidently mixed or given away



Top Threats: #5

- Data Loss or Leakage – Example
  - Amazon's huge EC2 cloud services crash permanently destroyed customer data
  - The Sidekick (Microsoft) data outage
    - 800,000 Smartphone Users lost Personal data (Emails, address books & photos)

Agenda

- Cloud Concepts
- Top Threats: #6
- Challenges: Cloud security
- Vulnerabilities
- Metrics for Vulnerabilities
- Hypervisor in detail
- Attacks to Cloud specific designs
- Golden rules to take from this presentation

Top Threats: #6

- Account or Service Hijacking
  - Known and old attack methods get a full new impact
  - Phishing, fraud, and exploitation of software vulnerabilities get a much bigger impact
  - Separation and private operation gets very complicated with access from everywhere any time concepts
  - Tapping of or injection of malware into the infrastructure is a big issue

Top Threats: #6

- Account or Service Hijacking – Examples:
  - Virtual Machine Sniffer on ESX Hosts
  - EBay and PayPal targeted or spear fishing attacks

Agenda

- Cloud Concepts
- Top Threats: #7
- Challenges: Cloud security
- Vulnerabilities
- Metrics for Vulnerabilities
- Hypervisor in detail
- Attacks to Cloud specific designs
- Golden rules to take from this presentation

Top Threats: #7

- Unknown Risk Profile
  - Cloud users shift the focus from security concerns and infrastructure to core business strengths
  - Users can easyly lose track of secure states and key security indicators:
    - Versions of software, code updates, security practices, vulnerability profiles, intrusion attempts, and security design
    - In addition to network intrusion logs, redirection attempts and/or successes, and other logs

Top Threats: #7

- Unknown Risk Profile - Examples
  - Heartland Data Breach: Heartland's payment processing systems were using known-vulnerable software and actually infected
  - http://www.pcworld.com/article/158038/heartland_has_no_heart_for_violated_customers.html

Attack Matrix

- Attacks apply to multiply cloud concepts
- Customer is loosing track of issues compared to fiscal benefit
- Security is up on the service provider
  - Security does not sell unless something bad already happened

	IaaS	PaaS	SaaS
Malicous use	X	X	O
API-Exploitation	X	X	X
Insider attack	X	X	X
Shared Technology	X	X	O
Data loss	X	X	X
Account Hijacking	X	X	X
Unknown Risk Profile	X	X	X

Agenda

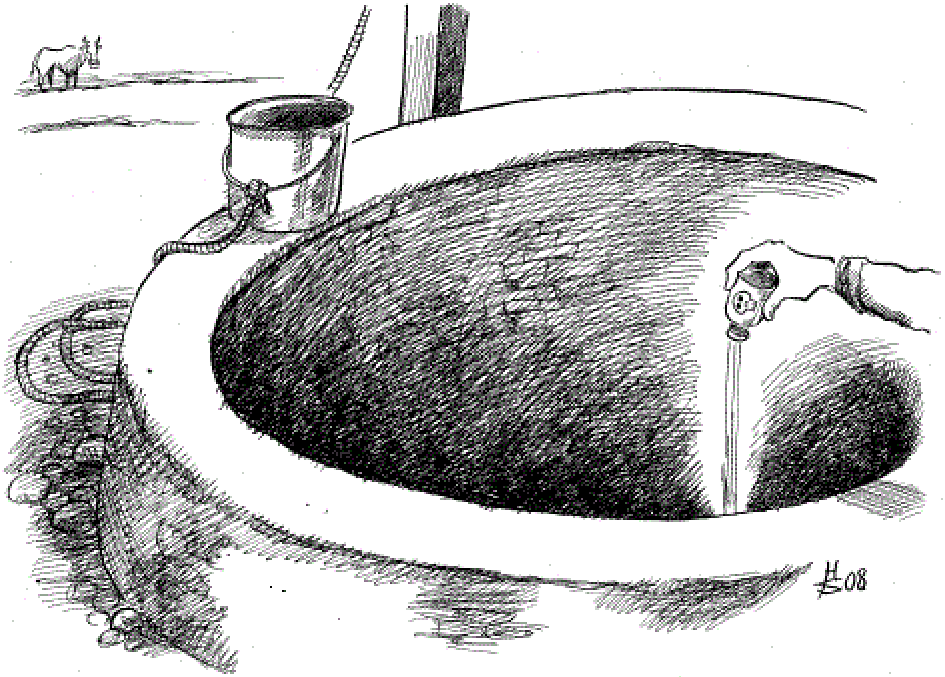
- Cloud Concepts
- Top Threats: #1-7
- Challenges: Cloud security
- Vulnerabilities
- Metrics for Vulnerabilities
- Hypervisor in detail
- Attack to Cloud specific designs
- Golden rules to take from this presentation

Challenges: Cloud security

- Identify specific issues
- Cloud requirements:
  - Confidentiality
    - For traffic and user data
  - Integrity
    - For software and data
  - Availability
    - For customers

Cloud Security

- Poisoning the well
- Expanding the defense perimeter is never a good idea
- Need multiple Lines of Defense and separation



Provider Reliability

- More security will be handled / delivered from service provider
  - Shift from operations to security operations
  - Single end-user or enterprise security solutions might not fit to service providers
- Providers need large scale security solutions for:
  - Access Control, Monitoring
  - Encryption and User Separation (VPN, storage, compute)

Agenda

- Cloud Concepts
- Top Threats: #1-7
- Challenges: Cloud security
- Vulnerabilities
- Metrics for Vulnerabilities
- Hypervisor in detail
- Attacks to Cloud specific designs
- Golden rules to take from this presentation

Exploitable vulnerabilities, more than just SW flaws

- A security risk may be classified as a vulnerability
- A vulnerability with one or more known instances of working and fully-implemented attacks is classified as an exploitable vulnerability, so an exploit is existing
- Security risks that are not SW flaws:
  - Defaults or misconfigurations
  - unauthorized or unsuspected/ unknown installations
  - Compliance deviations or non-compliance
  - Policy deviations or breaches

Window of Vulnerability

- The **window of vulnerability** is the time between
  - When the security issue was introduced or manifested and
  - The vulnerability was discovered and documented
- And
  - A preventive measure was put in place
  - A security fix was available/ deployed
  - The attack was disabled
  - The service/ vulnerability was removed
  - A workaround was put in place

Causes of Vulnerabilities (1/2)

- Complexity: Large, complex systems increase the probability of flaws and unintended access points
- Familiarity: Use of common, well-known code, applications, operating systems and/ or hardware increases the probability an attacker has found or can find the knowledge and tools to exploit a flaw
- Connectivity: More physical connections, privileges, ports, protocols, and services and each time those are accessible increases vulnerability
- Insecure or easy to guess credentials

Causes of Vulnerabilities (2/2)

- Software bugs: The programmer leaves an exploitable bug in a software program
  - The software bug may allow an attacker to misuse an application
- Invalidated user input:
  - The program assumes that all user input is safe
  - Programs that do not check user input can allow unintended direct execution of commands or SQL statements
    - Buffer overflows
    - SQL injection
    - Other non-validated inputs

Agenda

- Cloud Concepts
- Top Threats: #1-7
- Challenges: Cloud security
- Vulnerabilities
- Metrics for Vulnerabilities
- Hypervisor in detail
- Attacks to Cloud specific designs
- Golden rules to take from this presentation

Security Metrics (SCAP)

- Combines a number of open standards
- Is used to enumerate software flaws
- Measure systems to find vulnerabilities
- Offer methods to score those findings
- Help to evaluate the possible impact
- Is a method for using those open standards for automated vulnerability management, measurement and policy compliance evaluation.

Common Vulnerabilities and Exposures

- The **Common Vulnerabilities and Exposures** or **CVE** system provides a reference-method for publicly-known information-security vulnerabilities and exposures.
- MITRE Corporation maintains the system, with funding from the National Cyber Security Division of the United States Department of Homeland Security.
- CVE is the Industry-Standard defined by NIST

CVE®
cve.mitre.org

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Metrics for Vulnerabilities

- Common Vulnerability Scoring System (CVSS) is an industry standard for assessing the severity of computer system security vulnerabilities
- The CVSS assessment measures three areas of concern:
  - Base Metrics for qualities intrinsic to a vulnerability
  - Temporal Metrics for characteristics that evolve over the lifetime of vulnerability
  - Environmental Metrics for characteristics of a vulnerability that depend on a particular implementation or environment

(CVSS) Base Metrics

- **Base Metrics**
  - Is the vulnerability exploitable remotely (as opposed to only locally)?
  - How complex must an attack be to exploit the vulnerability?
  - Is authentication required to attack?
  - Does the vulnerability expose confidential data?
  - Can attacking the vulnerability damage the integrity of the system?
  - Does it impact availability of the system

(CPE) Common Platform Enumeration

- Is a standardized method of describing and identifying:
  - Classes of applications
  - Operating systems
  - Hardware devices
  - Detect enterprise's computing assets

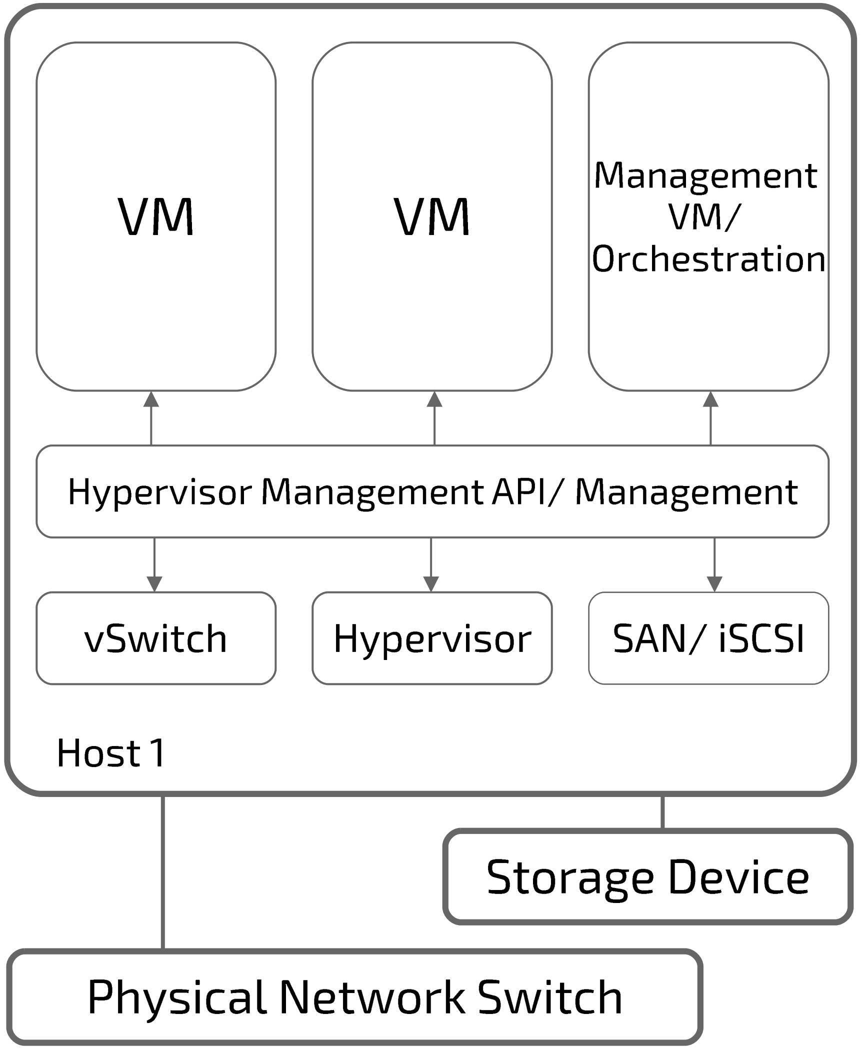
```
192.168.181.34|cpe:/a:openssl:openssl:0.9.8e:e
192.168.181.34|cpe:/o:centos:centos:5
192.168.181.34|cpe:/a:carnegie_mellon_university:cyrus-sasl:2.1.22
192.168.181.34|cpe:/a:isc:dhcp:3.0.5
192.168.181.34|cpe:/a:avahi:avahi:0.6.16
192.168.181.34|cpe:/a:gnu:gzip:1.3.5
```

Agenda

- Cloud Concepts
- Top Threats: #1-7
- Challenges: Cloud security
- Vulnerabilities
- Metrics for Vulnerabilities
- Hypervisor in detail
- Attacks to Cloud specific designs
- Golden rules to take from this presentation

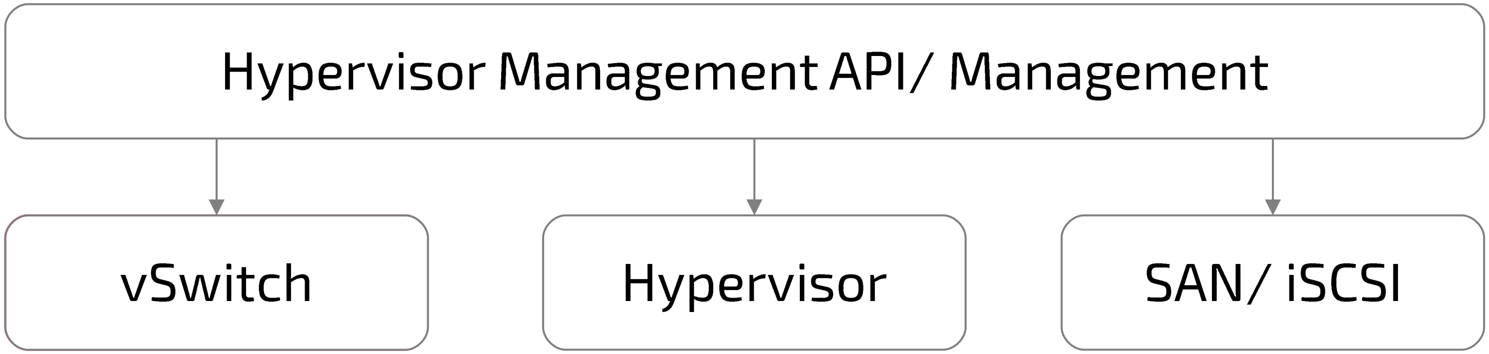
Hypervisor / Virtualization Host

- Resides between Hardware and OS, simulates Hardware (Devices)
  - On top of it is the Guest OS with drivers for virtualized hardware
  - Hypervisor consists of SW components



Hypervisor in detail

- Hypervisor runs on a host OS
  - Microsoft HyperV, Linux QEMU, XEN
- Hypervisor is an OS in itself
  - VMWare vSphere, ESXi, CloudOS



Hypervisor Management API/ Management

vSwitch

Hypervisor

SAN/ iSCSI

Hypervisor is mostly OpenSource Software

- VMWare ESXi is a complete Open Source package
- Large portions of Linux and other OpenSource projects do form the Hypervisor:

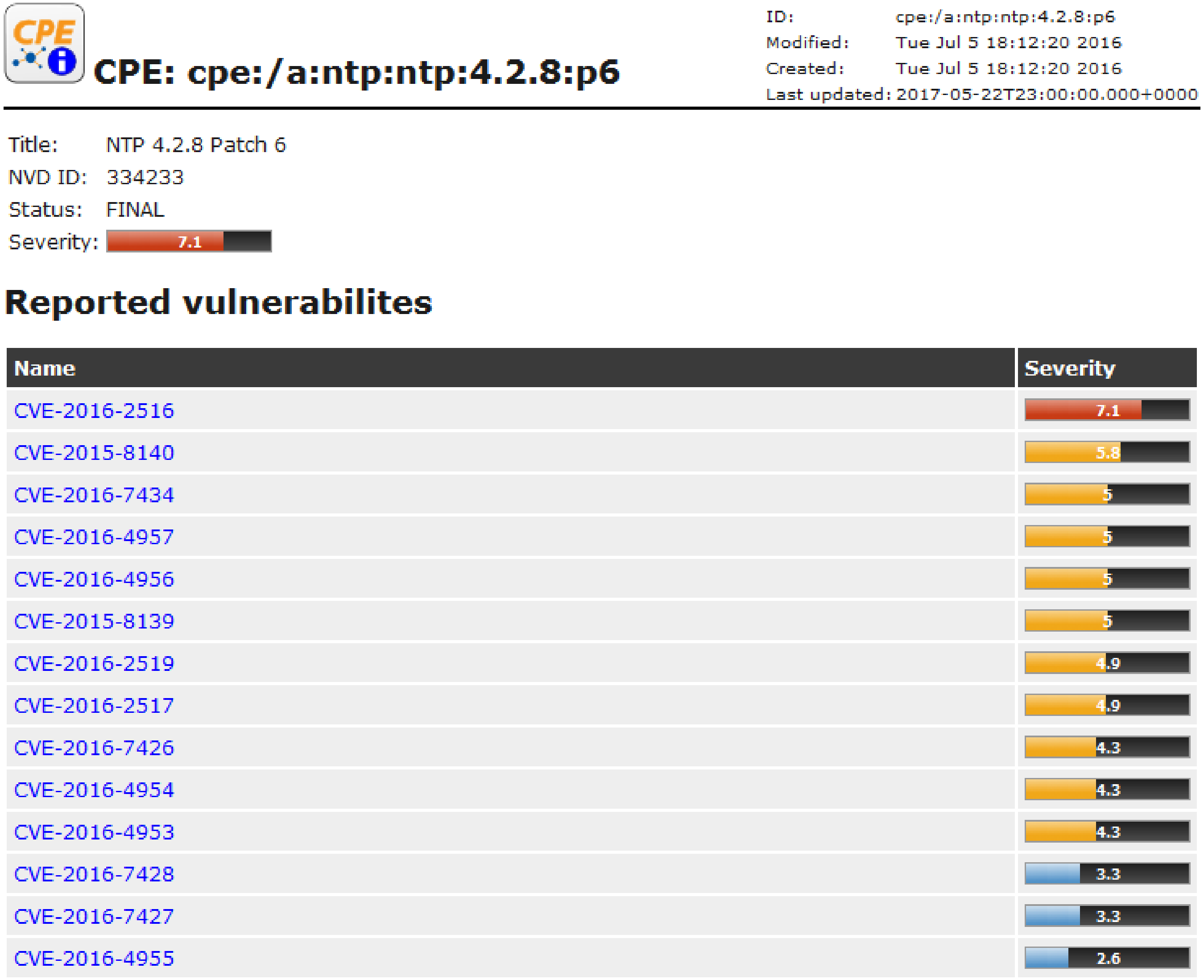
boost-1.55.0, dhcp-4.0.0, dropbear-0.52, expat-2.1.0, jansson-2.3, jquery-1.8.3, jquery-ui-1.10.3, libjpeg-turbo-1.2.1, libogg-1.3.0, libpam-0.99.3.0, libpng-1.2.49, libpng-1.5.12, libusb-0.1.12, libxml2-2.9.1, libxslt-1.1.28, llvm-3.1, mesa-10.1 ntp-4.2.6p2 openssh-6.6.1p1 openssl-1.0.1j rabbitmq-c-0.5.2, rapidjson-0.1, sqlite-3.7.6.3, sqlite-amalgamation-3.7.6.2, tcpdump-4.0.0, xorg-xserver-1.10.4, zlib-1.2.5, busybox-1.20.2, e2fsprogs-1.42.6, open-iscsi-2.0-865, parted-1.8.1, glibc-2.12.2, libusb-1.0.9

Source:

https://my.vmware.com/web/vmware/details?downloadGroup=ESXI600_OSS&productId=489

Quite often these components have vulnerabilities 1/2

- Upstream
  - NTP weakness
  - Exploit allows for direct access to the Hypervisor



CPE: cpe:/a:ntp:ntp:4.2.8:p6

ID:	cpe:/a:ntp:ntp:4.2.8:p6
Modified:	Tue Jul 5 18:12:20 2016
Created:	Tue Jul 5 18:12:20 2016
Last updated:	2017-05-22T23:00:00.000+0000

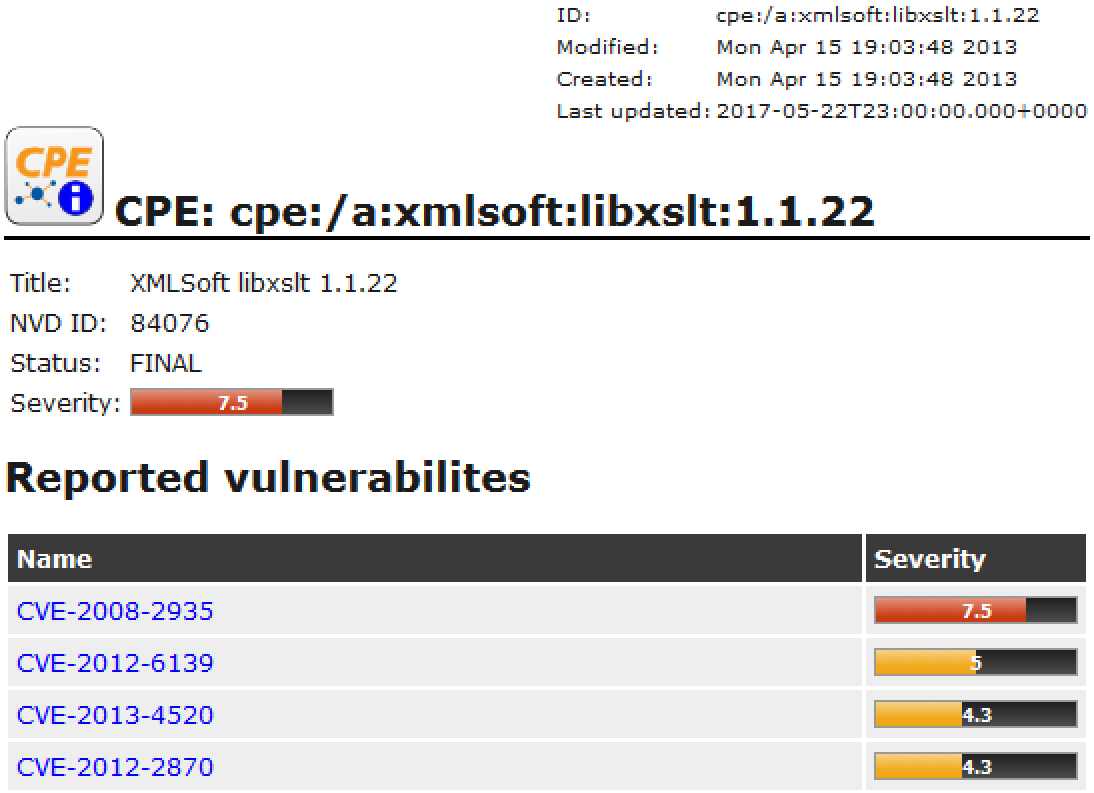
Title:	NTP 4.2.8 Patch 6
NVD ID:	334233
Status:	FINAL
Severity:	7.1

Reported vulnerabilites

Name	Severity
CVE-2016-2516	7.1
CVE-2015-8140	5.8
CVE-2016-7434	5
CVE-2016-4957	5
CVE-2016-4956	5
CVE-2015-8139	5
CVE-2016-2519	4.9
CVE-2016-2517	4.9
CVE-2016-7426	4.3
CVE-2016-4954	4.3
CVE-2016-4953	4.3
CVE-2016-7428	3.3
CVE-2016-7427	3.3
CVE-2016-4955	2.6

Quite often these components have vulnerabilities 2/2

- Upstream
  - libxslt
  - Hypervisor orchestration component
- Intrusion into Hypervisor is possible



ID:	cpe:/a:xmlsoft:libxslt:1.1.22
Modified:	Mon Apr 15 19:03:48 2013
Created:	Mon Apr 15 19:03:48 2013
Last updated:	2017-05-22T23:00:00.000+0000

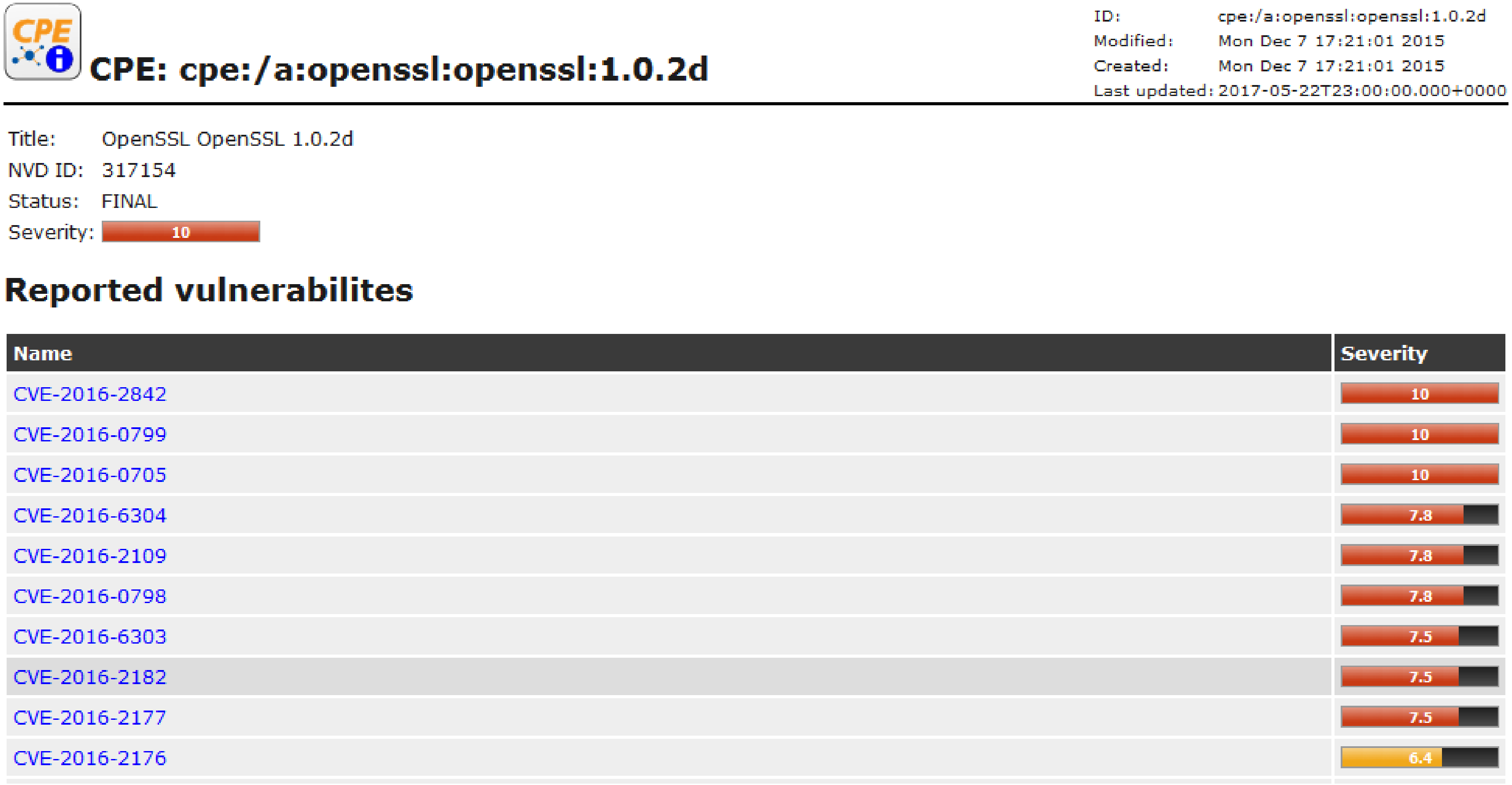
CPE: cpe:/a:xmlsoft:libxslt:1.1.22

Title:	XMLSoft libxslt 1.1.22
NVD ID:	84076
Status:	FINAL
Severity:	7.5

Reported vulnerabilites

Name	Severity
CVE-2008-2935	7.5
CVE-2012-6139	5
CVE-2013-4520	4.3
CVE-2012-2870	4.3

Openssl – A permanent issue for Webserver & Management



CPE: cpe:/a:openssl:openssl:1.0.2d

ID:	cpe:/a:openssl:openssl:1.0.2d
Modified:	Mon Dec 7 17:21:01 2015
Created:	Mon Dec 7 17:21:01 2015
Last updated:	2017-05-22T23:00:00.000+0000

Title:	OpenSSL OpenSSL 1.0.2d
NVD ID:	317154
Status:	FINAL
Severity:	10

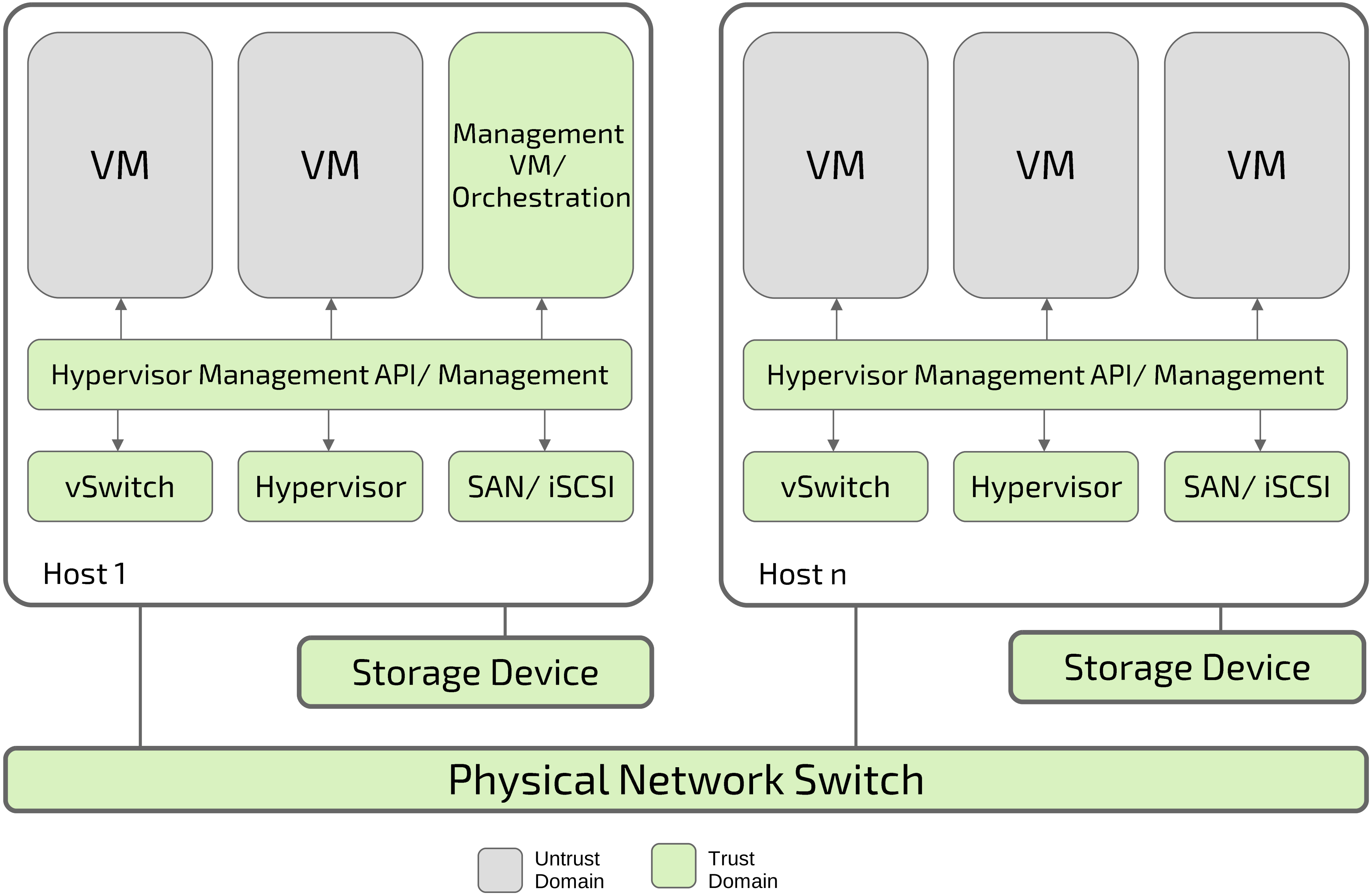
Reported vulnerabilites

Name	Severity
CVE-2016-2842	10
CVE-2016-0799	10
CVE-2016-0705	10
CVE-2016-6304	7.8
CVE-2016-2109	7.8
CVE-2016-0798	7.8
CVE-2016-6303	7.5
CVE-2016-2182	7.5
CVE-2016-2177	7.5
CVE-2016-2176	6.4

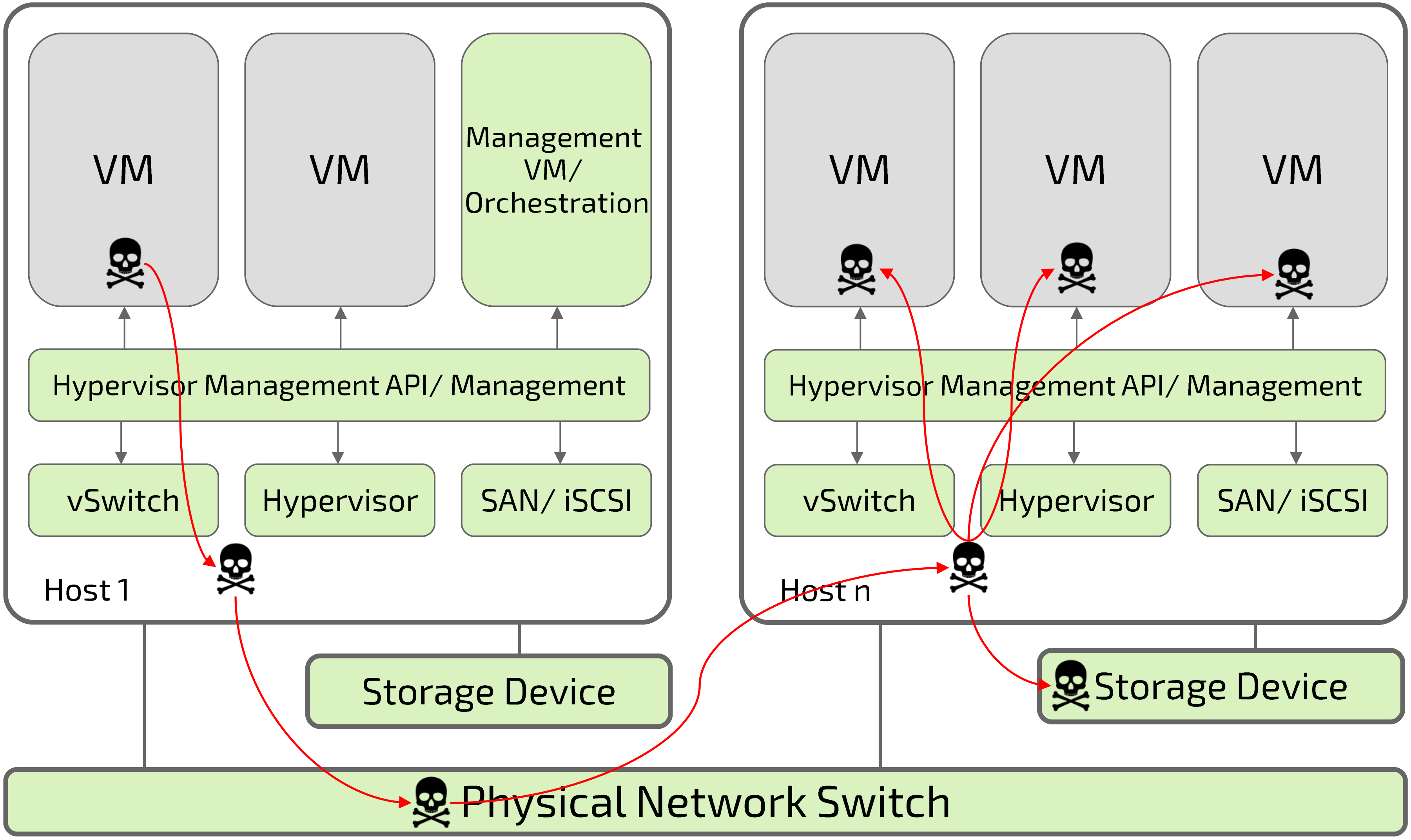
Agenda

- Cloud Concepts
- Top Threats: #1-7
- Challenges: Cloud security
- Vulnerabilities
- Metrics for Vulnerabilities
- Hypervisor in detail
- Attacks to Cloud specific designs
- Golden rules to take from this presentation

Attacks against the infrastructure

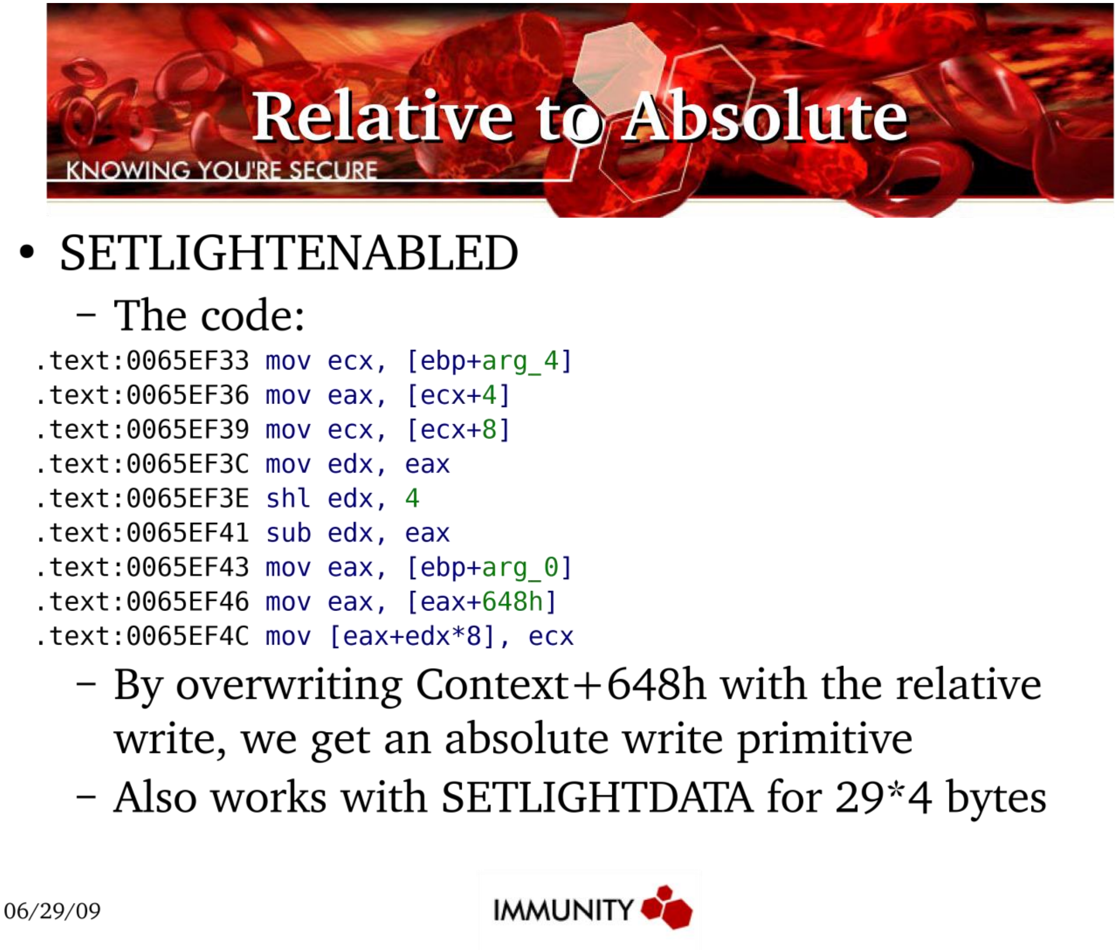


Attacks against the infrastructure



⬜ Untrust Domain
🟩 Trust Domain

Some Examples



Relative to Absolute

KNOWING YOU'RE SECURE

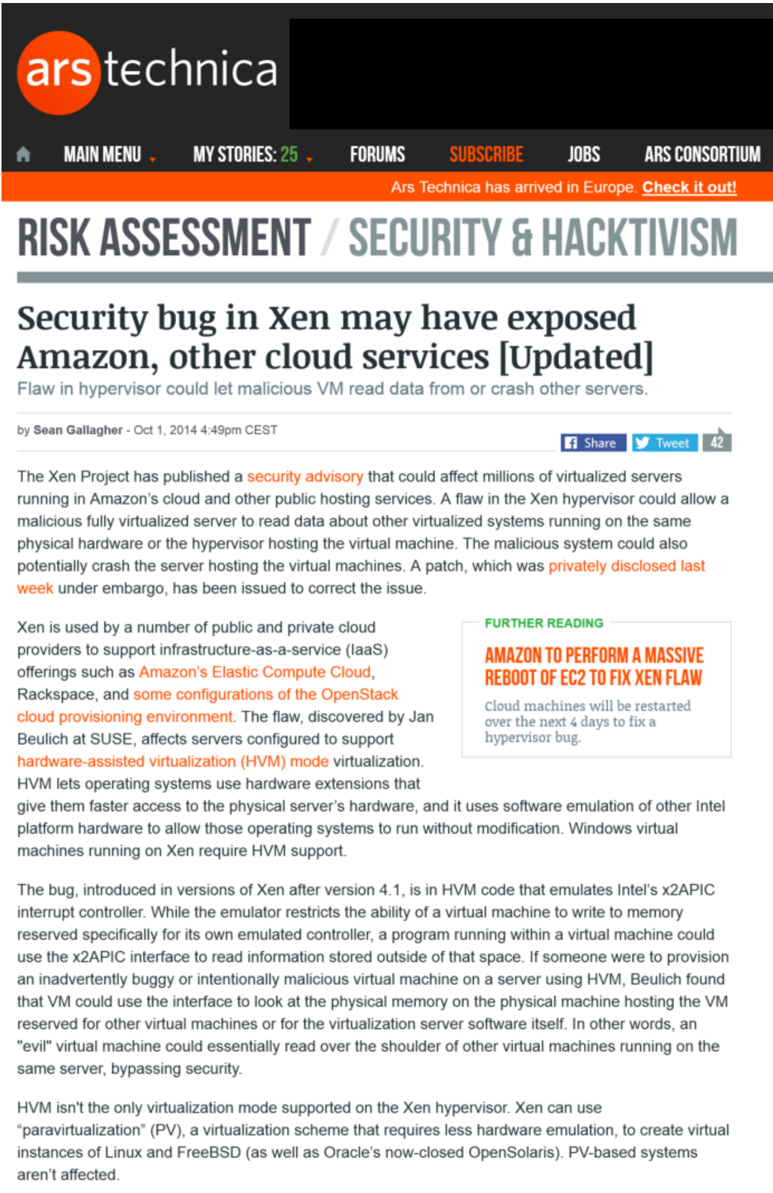
- SETLIGHTENABLED
  - The code:

```
.text:0065EF33 mov ecx, [ebp+arg_4]
.text:0065EF36 mov eax, [ecx+4]
.text:0065EF39 mov ecx, [ecx+8]
.text:0065EF3C mov edx, eax
.text:0065EF3E shl edx, 4
.text:0065EF41 sub edx, eax
.text:0065EF43 mov eax, [ebp+arg_0]
.text:0065EF46 mov eax, [eax+648h]
.text:0065EF4C mov [eax+edx*8], ecx
```

  - By overwriting Context+648h with the relative write, we get an absolute write primitive
  - Also works with SETLIGHTDATA for 29*4 bytes

06/29/09

IMMUNITY



Ars Technica has arrived in Europe. Check it out!

RISK ASSESSMENT / SECURITY & HACKTIVISM

Security bug in Xen may have exposed Amazon, other cloud services [Updated]

Flaw in hypervisor could let malicious VM read data from or crash other servers.

by **Sean Gallagher** - Oct 1, 2014 4:49pm CEST

The Xen Project has published a security advisory that could affect millions of virtualized servers running in Amazon's cloud and other public hosting services. A flaw in the Xen hypervisor could allow a malicious fully virtualized server to read data about other virtualized systems running on the same physical hardware or the hypervisor hosting the virtual machine. The malicious system could also potentially crash the server hosting the virtual machines. A patch, which was privately disclosed last week under embargo, has been issued to correct the issue.

Xen is used by a number of public and private cloud providers to support infrastructure-as-a-service (IaaS) offerings such as Amazon's Elastic Compute Cloud, Rackspace, and some configurations of the OpenStack cloud provisioning environment. The flaw, discovered by Jan Beulich at SUSE, affects servers configured to support hardware-assisted virtualization (HVM) mode virtualization. HVM lets operating systems use hardware extensions that give them faster access to the physical server's hardware, and it uses software emulation of other Intel platform hardware to allow those operating systems to run without modification. Windows virtual machines running on Xen require HVM support.

FURTHER READING

AMAZON TO PERFORM A MASSIVE REBOOT OF EC2 TO FIX XEN FLAW

Cloud machines will be restarted over the next 4 days to fix a hypervisor bug.

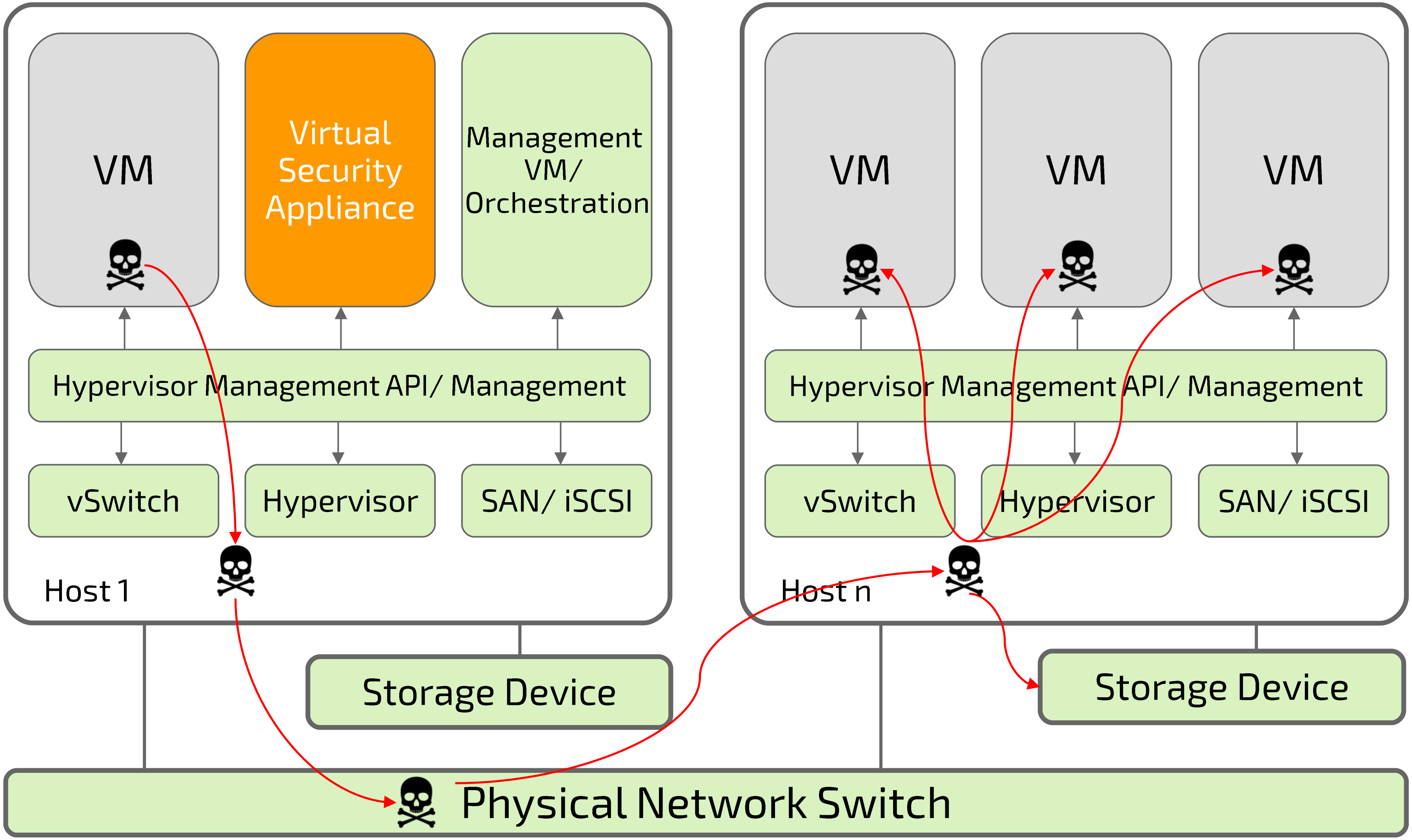
The bug, introduced in versions of Xen after version 4.1, is in HVM code that emulates Intel's x2APIC interrupt controller. While the emulator restricts the ability of a virtual machine to write to memory reserved specifically for its own emulated controller, a program running within a virtual machine could use the x2APIC interface to read information stored outside of that space. If someone were to provision an inadvertently buggy or intentionally malicious virtual machine on a server using HVM, Beulich found that VM could use the interface to look at the physical memory on the physical machine hosting the VM reserved for other virtual machines or for the virtualization server software itself. In other words, an "evil" virtual machine could essentially read over the shoulder of other virtual machines running on the same server, bypassing security.

HVM isn't the only virtualization mode supported on the Xen hypervisor. Xen can use "paravirtualization" (PV), a virtualization scheme that requires less hardware emulation, to create virtual instances of Linux and FreeBSD (as well as Oracle's now-closed OpenSolaris). PV-based systems aren't affected.

Successful attacks

- External attack against orchestration (Management)
- Break-out from VM into Hypervisor level
- Intrusion of each and every VM inside a Trust Domain
- Trust Domain inside the cloud allows attackers to take over the complete domain
- Microsoft-Hyper V „Golden Kerberos Ticket“
- XEN weakness that allows access to Guest OS

A virtual Security appliance doesn‘t help…


VM
Virtual Security Appliance
Management VM/ Orchestration
Hypervisor Management API/ Management
vSwitch
Hypervisor
SAN/ iSCSI
Host 1
VM
VM
VM
Hypervisor Management API/ Management
vSwitch
Hypervisor
SAN/ iSCSI
Host n
Storage Device
Storage Device
Physical Network Switch

Attacks go unnoticed

- The attack from below remains unnoticed, because the VM infrastructure walls off security solutions
- Like a bank job using a tunnel, only that all banks are robbed simultaneously!

If the foundation is unsecure…

- Vulnerability Management and security should be operating independent from Hypervisor and Cloud-Systems

- All public clouds limit the access to the Hypervisor by design, so scanning to proof the security of the underplaying infrastructure is not possible.

Agenda

- Cloud Concepts
- Top Threats: #1-7
- Challenges: Cloud security
- Vulnerabilities
- Metrics for Vulnerabilities
- Hypervisor in detail
- Attacks to Cloud specific designs
- Golden rules to take from this presentation

Who will benefit ?

- Service provider will benefit
- Suppliers for them as well:
  - Network equipment
  - Large scale storage
  - Hypervisors, Central Management, large scale security vendors
- Unaffordable computing problems will get cheap

Who will suffer ?

- Private data will more likely be lost
- Organizations with high security policy and standards will lower them
- Insecure “private” applications will be exposed to the whole hacker community
- Security evolution will be sped up
  - DES, 3DES, MD5, RC4, SHA1… get obsolete
- Unprepared service providers will lose business
- Some business models will shift to the cloud

Golden rules

1. Always backup your cloud data
2. Prepare for data loss
3. **Don’t store your personal data in cloud**
4. Encrypt you data before sending it to the cloud
5. Don’t compute private data on shared systems
6. Don’t rely on passwords - use secure cryptography

Questions ?

Thank You

DN-Systems GmbH
Hornemannstr. 12/13
31137 Hildesheim, Germany
Phone: +49-5121-28989-0
Mail: info@dn-systems.de