Hardware security & the cloud services

Gabriel Labrada

April 2015

OWASP

The Open Web Application Security Project

About Me

OWASP
The Open Web Application Security Project

- Gabriel Labrada
  - Electronic and communications engineer (IPN Mexico)
  - MsC Computer Science CINVESTAV on ECC Crypto, parallell computing and multicore algorithms.
  - Security Researcher at Intel.
  - Security validation of PCH, Servers, uServers and some security technologies like trusted execution technology.

gabriel.labrada@intel.com

OWASP
The Open Web Application Security Project

The HW and FW are the next line of defense on the evolving role of computer security.

- Antivirus
- Network hardening
- Server hardening
- Secure App/Code Development
- End user endpoint hardening
- **HW/FW hardening**

Security Evolution

OWASP
The Open Web Application Security Project

1st Gen

Antivirus

Network hardening

Server hardening

2nd Gen

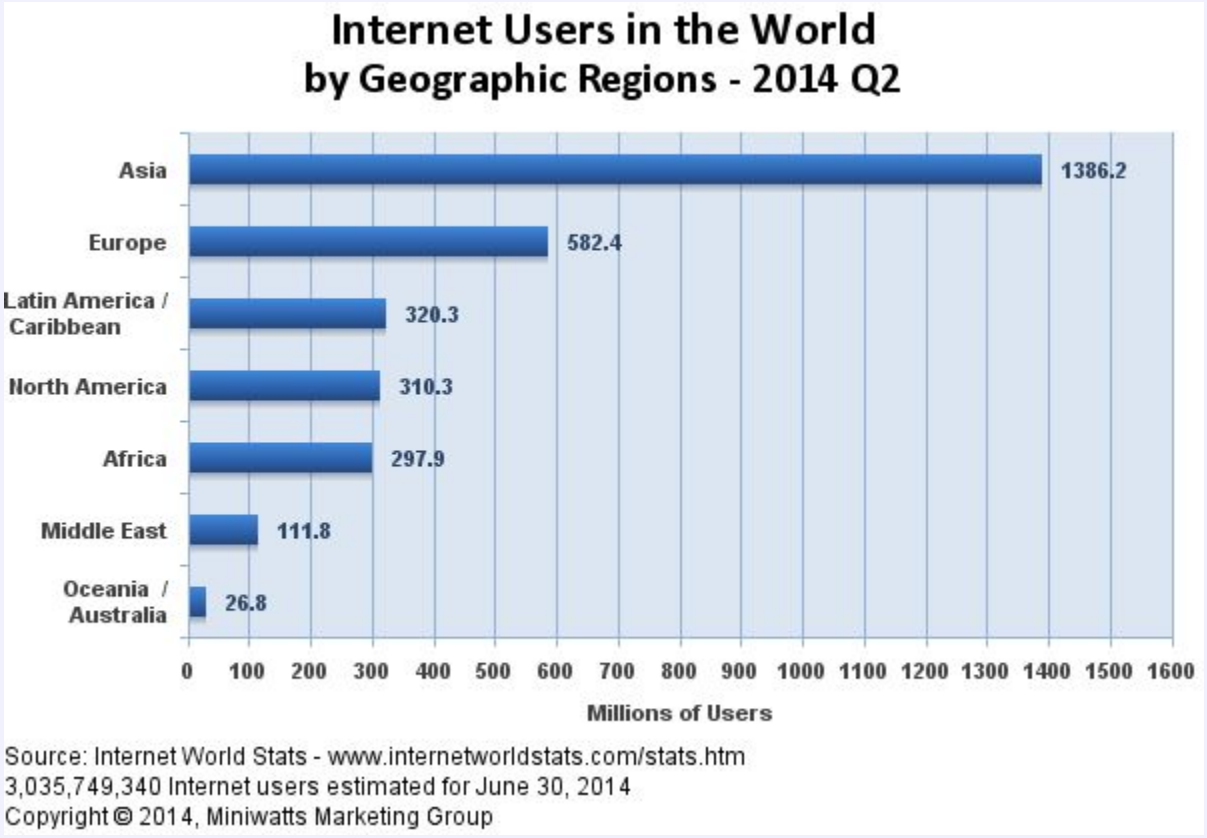
Secure App/Code Development

End user endpoint hardening

3rd Gen

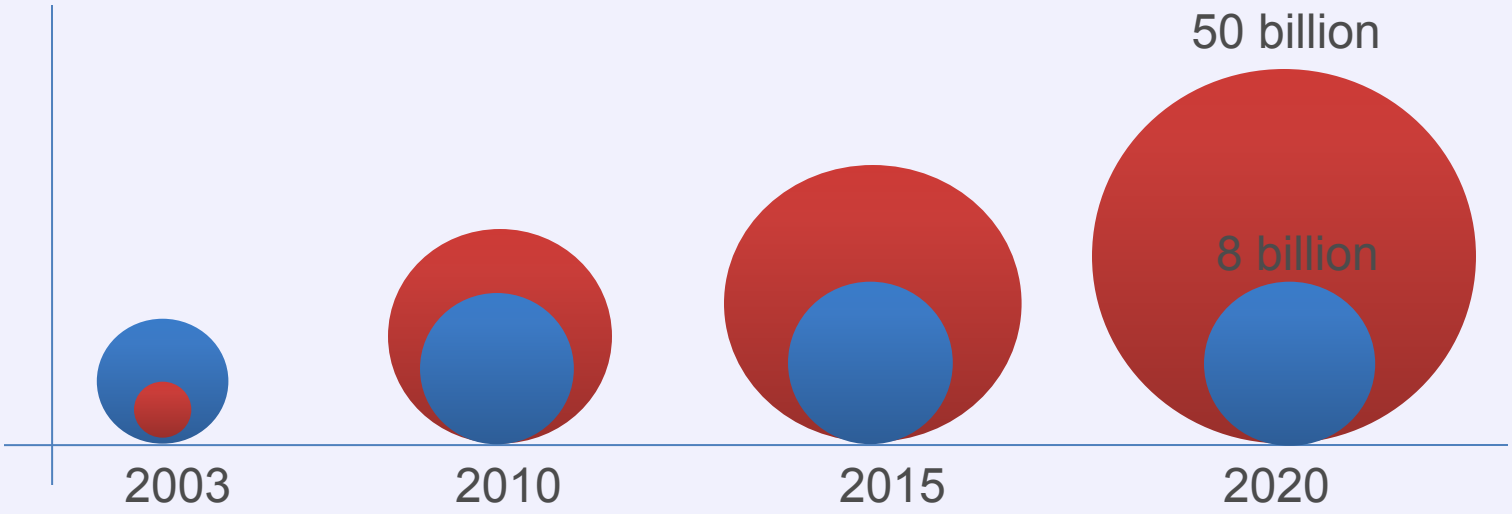
HW/FW hardening

4th Gen


Internet Users in the World
by Geographic Regions - 2014 Q2
Asia
1386.2
Europe
582.4
Latin America / Caribbean
320.3
North America
310.3
Africa
297.9
Middle East
111.8
Oceania / Australia
26.8
0 100 200 300 400 500 600 700 800 900 1000 1100 1200 1300 1400 1500 1600
Millions of Users
Source: Internet World Stats - www.internetworldstats.com/stats.htm
3,035,749,340 Internet users estimated for June 30, 2014
Copyright © 2014, Miniwatts Marketing Group

Lets take a look at this interesting estimation on the

Internet-connected devices vs world population



Source: http://share.cisco.com/internet-of-things.html

What does that mean for security?

Money is becoming digital

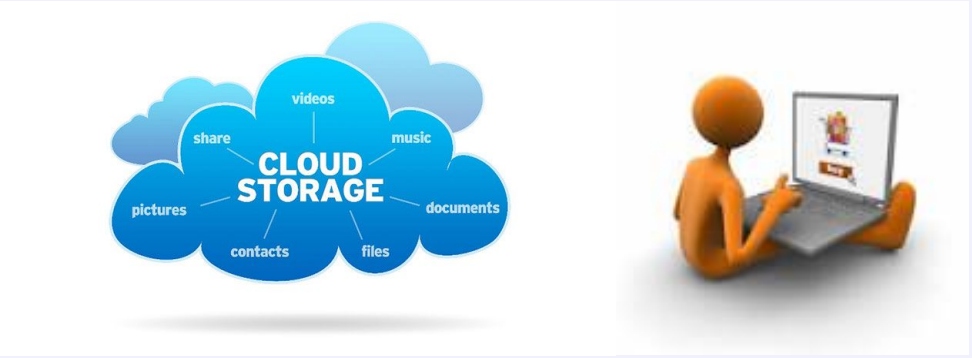
11010101101010010101010110101

What does that mean for security?

•All kind of information is being migrated to its digital form.

Ecommerce - Banking - Financial - Contracts - Health - Traffic control - Intellectual Property - Books – Entertainment – Music – Movies – News –

Money – Videos – Photos – Social relations – Financial records – Tax payment – evoting – advertising – network sensors, phone calls, etc.



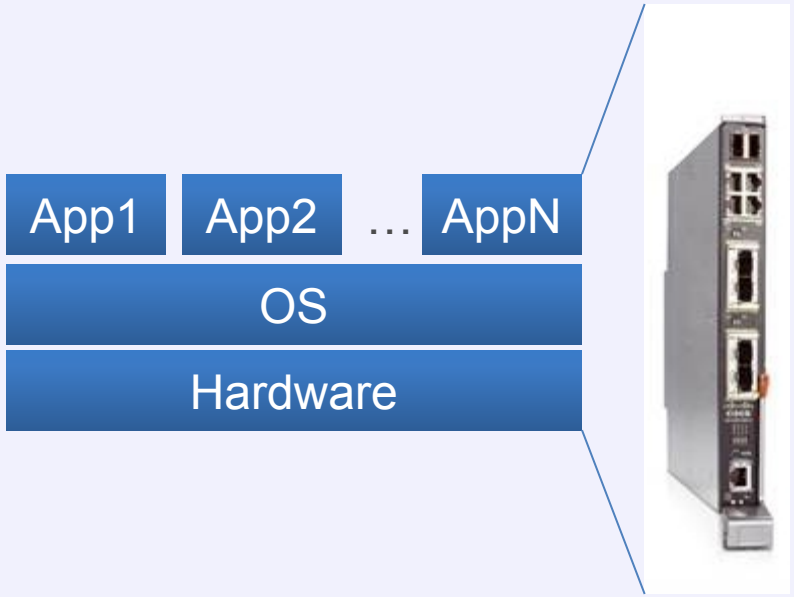
OWASP
The Open Web Application Security Project

So, how to protect the data & services?

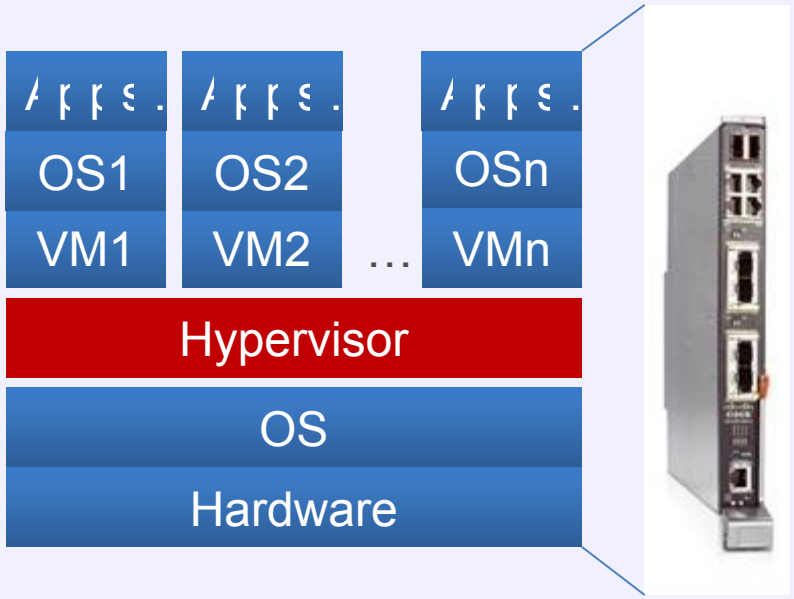
CIA

Computing: Physical VS Cloud

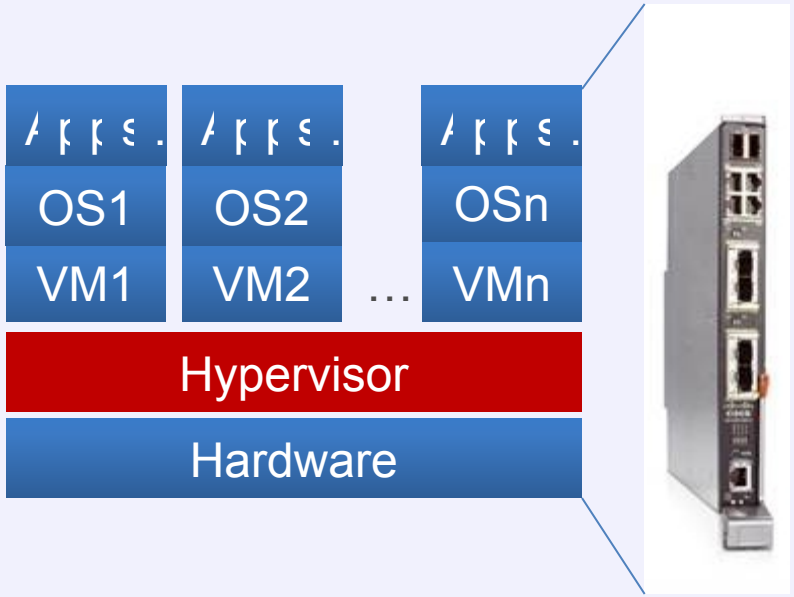
Computing: Physical VS Virtual



Computing: Physical VS Virtual



Computing: Physical VS Virtual



Cloud pros.

- Lower cost
- High availability
- Cloud Companies have security professional configuring and monitoring
- Efficiency savings in terms of power
- Savings in terms of cooling and floor space

Cloud downside.

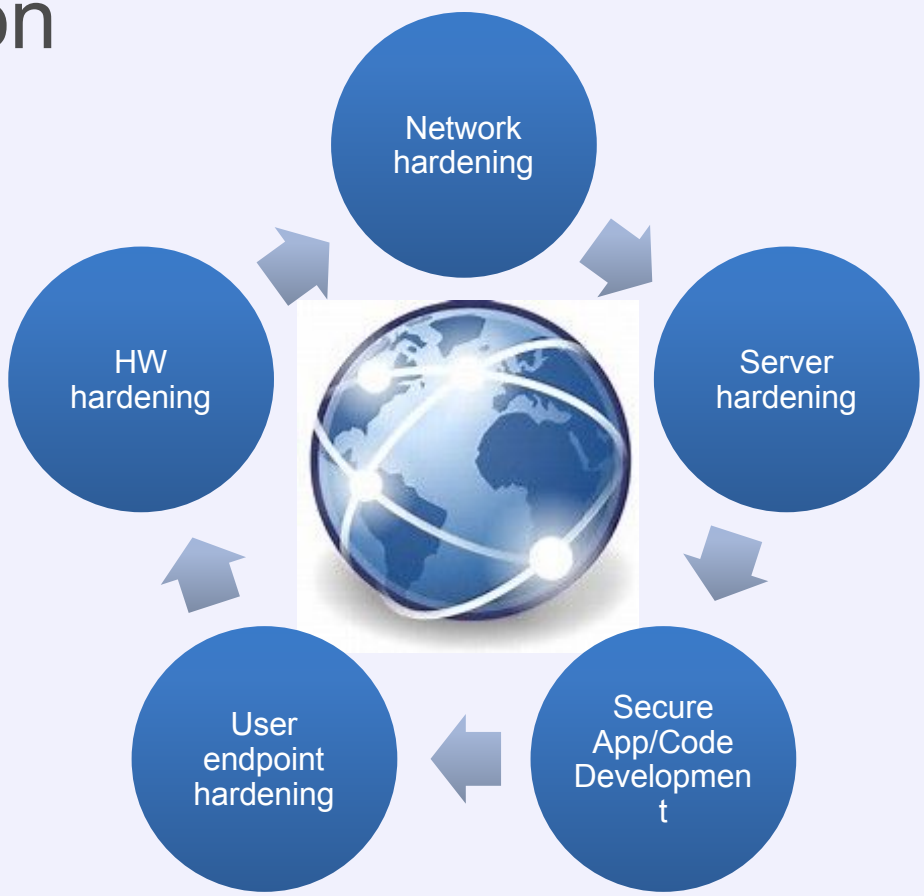
- New infrastructure
- Virtual Networking
- Many eggs into one huge basket
- Hypervisor becomes a key player

OWASP
The Open Web Application Security Project

Two general scenarios for virtualization compromise

- **Hyperjacking**
- **Hyper Jumping**

- Both: Physical and Virtual services require protection



- Network hardening
  - Keep your network devices upgraded
  - Periodically re-verify the file hash of the running firmware
  - Shut down unused physical interfaces
  - Configure restrictive policies
  - Change default passwords/keys immediately
  - Protect the network device configuration file from unauthorized disclosure.
  - Configure alerts when changes or reboot events detected.
  - Shut down unneeded services on network devices.
  - Monitor Logs on a regular basis
  - Only use secure protocol standards (SSHv2; IKEv2/IPsec; TLS v1.0+) when performing remote management of network devices.
  - Restrict remote management connectivity to only controlled machines

OWASP
The Open Web Application Security Project

Server hardening

Server Hardening

•Use Data Encryption for your Communications

•Avoid using insecure protocols that send your information or passwords in plain text.

•Minimize unnecessary software on your servers.

•Keep your operating system up to date, especially security patches.

•Change passwords on a regular basis and do not reuse them

•Lock accounts after too many login failures. Often these login failures are illegitimate attempts to gain access to your system.

•Do not permit easy/empty passwords.

•Disable unused binaries

•Maintain server logs; mirror logs to a separate log server

•Install Logwatch and review logwatch emails daily. Investigate any suspicious activity on your server.

•Use brute force and intrusion detection systems

Limit user accounts to accessing only what they need. Increased access should only be on an as-needed basis.

•Maintain proper backups

•Don't forget about physical server security

OWASP
The Open Web Application Security Project

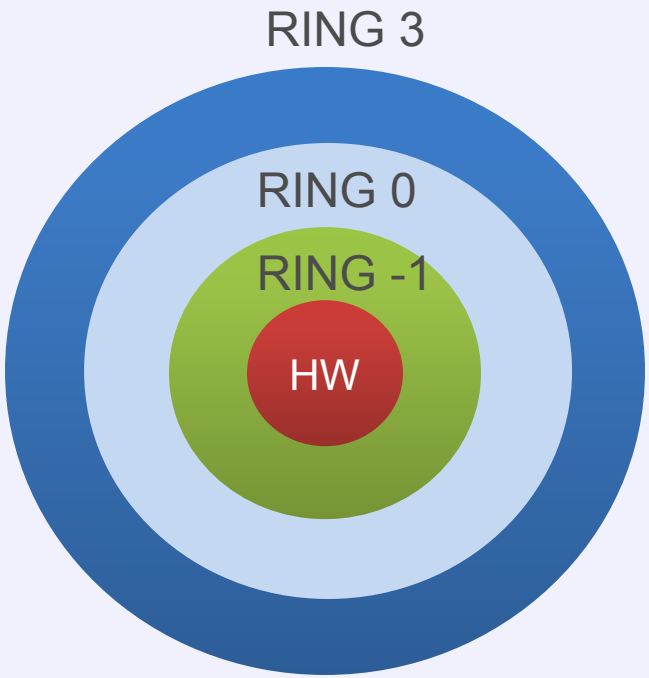
Secure App/Code Development

Secure App/Code Development

1 - Injection
2 - Broken Authentication and Session management
3 - Cross-Site Scripting (XSS)
4 - Insecure Direct Object References
5 - Security Misconfiguration
6 - Sensitive data exposure
7 - Missing Function Level Access Control
8 - Cross-Site Request Forgery (CSRF)
9 - Using Components with known Vulnerabilities
10 - Invalidated Redirects and Forwards

Source:
https://www.owasp.org/index.php/Top10#OWASP_Top_10_for_2013

- Multi-layered, defense-in-depth security architecture.



OWASP
The Open Web Application Security Project

User endpoint hardening

User endpoint hardening

- Use strong auth/passwords
- Prefer multifactor authentication (MFA)
- Update firmware and patches
- Separate work devices from entertainment
- Review security for your Network devices
- Change default access configuration
- Disable unused ports/protocols

OWASP
The Open Web Application Security Project

HW hardening

Hardware hardening

- Control registers
- Memory Range registers and their protections
- Address translation logic
- System fuses and straps
- Module interfaces and buses
- State flows and error handling
- Debug Features (DFX), Design For Test (DFT)
- Error injection
- Crypto modules
- Firmware and patches

OWASP
The Open Web Application Security Project

HW hardening

CHIPSEC: Platform Security Assessment Framework

CHIPSEC is a framework for analyzing security of PC platforms including hardware, system firmware including BIOS/UEFI and the configuration of platform components. It allows creating security test suite, security assessment tools for various low level components and interfaces as well as forensic capabilities for firmware

CHIPSEC can run on any of these environments:

- Windows (client and server)
- Linux
- UEFI Shell

NOTE: This software is for security testing purposes.

Source https://github.com/chipsec/chipsec

Virtual environments

OWASP
The Open Web Application Security Project

If possible isolate VMs network traffic.

Regular patch BIOS/FW/ucode.

At least security management of hypervisor must be kept separate from regular traffic.

Regular patch the hypervisor

Don’t manage hypervisor from guest operating systems.

Monitoring/Management tools should not be installed or used from guest OS.

Wrap up

OWASP
The Open Web Application Security Project

HW security will play an important role on cloud computing

Hypervisors will become a very attractive target for hackers due to the number of potential guest machines that can be compromised and also the computing power of virtualization servers.

Use Automated testing tools to validate recommended configuration on HW

OWASP
The Open Web Application Security Project