Departamento de ENGENHARIA INFORMÁTICA
Instituto Superior de Engenharia do Porto

Systems and Information Security SEGSI

Topic 2

System Security

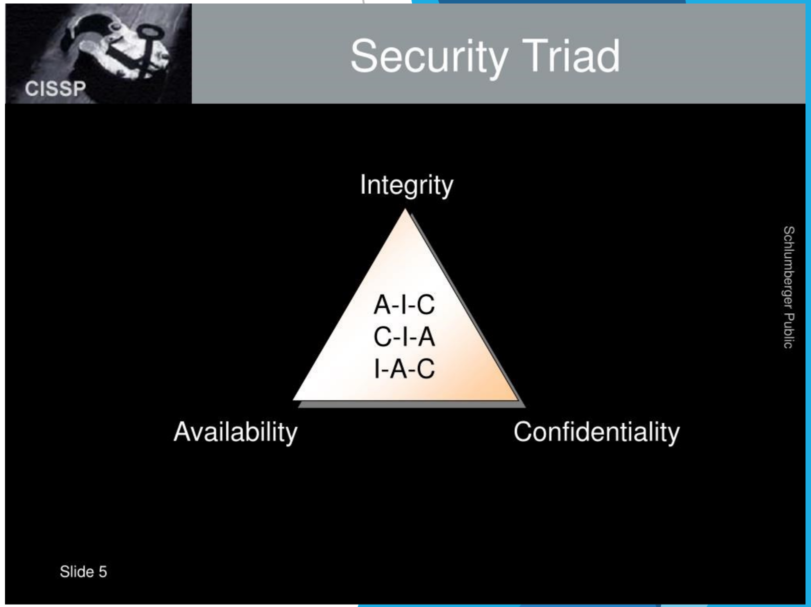
Pinto Leite, Jorge (jpl@isep.ipp.pt)

System Security

- Let’s agree or remember some basic concepts
  - Security triad
  - Vulnerability
  - Exploit
  - Exposure

The security triad

- Remember the definition on access control lecture of confidentiality, integrity and availability?
- These are the sides of a triangle that represents the security needs of anything
- The size of each side depends on the desired objective, or what is more important



CISSP

Security Triad

Slide 5

Schlumberger Public

Source: CISSP

System Security

- Vulnerability
  - A weakness in something that can be exploited and will lead to a purpose other than the one expected
  - Example 1: Improper Input Validation in Apache Tomcat (CVE-2023-45648)[1]
  - Example 2: Dressing a certain way because it expresses who you are

[1] CVE (*Common Vulnerabilities and Exposures*) is a public database that contains all known flaws on technological environments

System Security

- Exploit
  - A tool, a program, or some other thing designed to take advantage of a vulnerability
  - Example 1: Morris worm (1988) a script that exploited vulnerabilities in Unix sendmail, finger and exec
  - Example 2: Tool to open locks and padlocks

Source: Amazon

System Security

- Exposure
  - A vulnerability plus any human related error or misconfiguration
  - Example 1: Personal computer without password to log
  - Example 2: Leaving the front door key outside the lock when leaving the house

System Security

- System security is a mandatory need to keep them free of unauthorized access and / or unexpected behavior
- What layers should we consider when thinking about system security?
- First of all, the system itself, a bunch of processors, connections (in the motherboard yet not only), electronic components, and so on
- To achieve the security of the system, we need to implement measures to avoid or mitigate the inevitability of hardware failure
  - That might jeopardize its function and objectives
- Also, and perhaps on the top of priorities, the physical security

Physical Security

- *"The best network software security measures can be rendered useless if you fail to physically protect your systems"* (Michael Meyers, 2004)
- If someone gets physical access to a system there are plenty of actions he might perform to surpass its security
  - Boot from a pen, for example
- By definition, if an unexpected person gains physical access, he or she has already broken the security
- Physical Access Control Systems (PACS) is a set of security measures to assure that only authorized ones are able to access the protected zone
- It includes or might include the physical access points controls, credentials for authorized people, readers (card reader or PIN insertion) and on the background a control panel (to verify authorization) connected to a server (for accounting / auditing)

Physical Security

- Depending of what one needs to protect, several counterparts must / can be put in place, some of them physical, other technical
  - Guards
  - Dogs
  - Barriers
  - CCTV
  - Credentials
- And don't forget
  - Store the images captured by the CCTV
  - Monitor access
  - Audit all data available that regards physical access
    - Is it feasible that someone that is away (holidays or similar) has been on the premises at the same time?

Source: imgur

Source: Pets Nurturing

Source: leadelementsecurity.co.uk

Source: securitycamering.com

Physical Security

- These considerations has some natural flaws
- If a security company has been contracted, isn’t it natural that their employees has access to everywhere?
    - Just suppose that a fire or a flood starts when only them are on premises
- And shouldn’t they be able to carry out a check and take the first measures?
- Whatever measure you have implemented, all those situations should be considered and evaluated

System Security

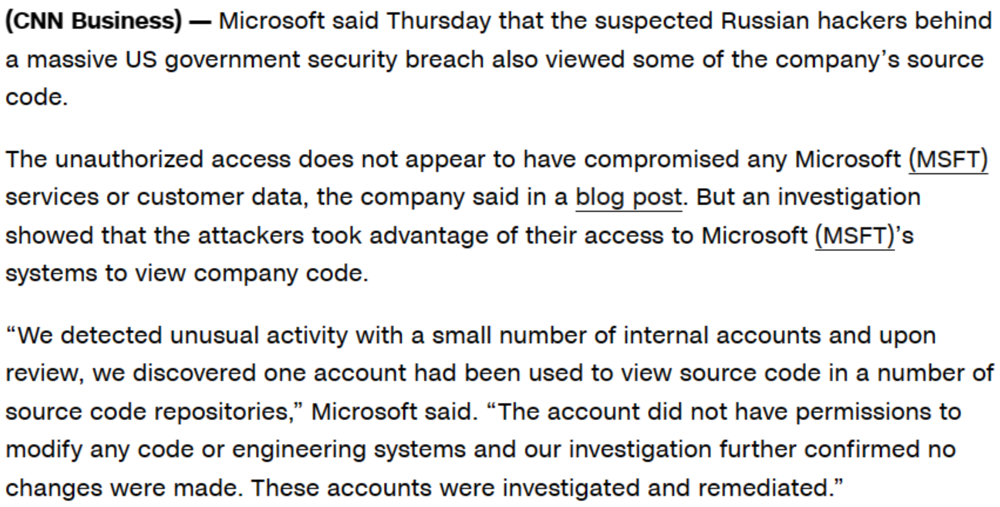
- Assuming the hardware functionality and security is achieved at the best we can, let's dive into system architecture
- It contains *firmware*, an *operating system* and on the top *applications*
- Starting with the firmware, are there any specific care we must be concerned about?
  - Yes, there is, as due to environment issues (heat, for example) or the deployment of a new firmware version, a failure might occur
  - However, due to the large spectrum of this level, different solutions and / or considerations should be performed to mitigate them
    - Is it always possible to downgrade to the previous version of firmware?
    - For heat, dust, fire, humidity, and others related concerns, sensors can be placed to monitor each one of them
      - And if the sensors fails?

System Security

- Continuing with the firmware, it is common sense to assume that for most of the devices it is not accessible by users or attackers, however a new version to update it can be problematic
- New versions of firmware are usually linked with new features of devices, bugs on previous versions, as well as security flaws
- By reverse engineering the firmware, an attacker can obtain knowledge to allow him to impersonate the manufacturer, leading people to update to a hacked version
- Also, an hacker (that probably already read about known vulnerabilities in specific versions of firmware) can target a device with outdated firmware version
- And finally and assuming that physical access is feasible, an hacker can modify device’s firmware to bypass security controls and / or install malicious code

System Security

- Operating system was separated on previous slide as it is a specific, unique and mandatory application
  - However, it is an application almost with the same concerns that we will discuss on next slides

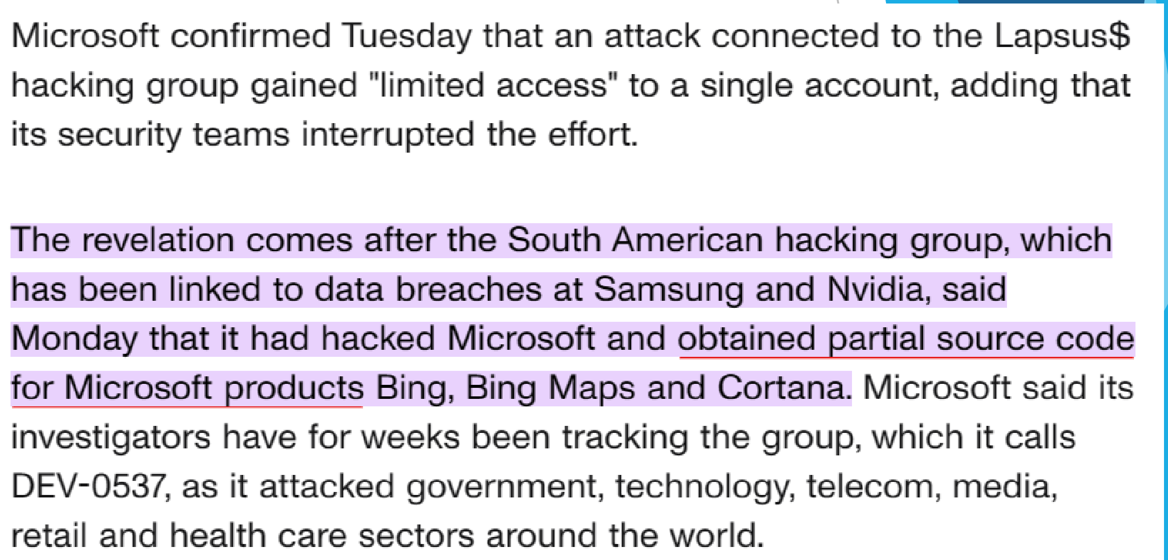


(CNN Business) — Microsoft said Thursday that the suspected Russian hackers behind a massive US government security breach also viewed some of the company's source code.

The unauthorized access does not appear to have compromised any Microsoft (MSFT) services or customer data, the company said in a blog post. But an investigation showed that the attackers took advantage of their access to Microsoft (MSFT)'s systems to view company code.

"We detected unusual activity with a small number of internal accounts and upon review, we discovered one account had been used to view source code in a number of source code repositories," Microsoft said. "The account did not have permissions to modify any code or engineering systems and our investigation further confirmed no changes were made. These accounts were investigated and remediated."

December 2020



Microsoft confirmed Tuesday that an attack connected to the Lapsus$ hacking group gained "limited access" to a single account, adding that its security teams interrupted the effort.

The revelation comes after the South American hacking group, which has been linked to data breaches at Samsung and Nvidia, said Monday that it had hacked Microsoft and obtained partial source code for Microsoft products Bing, Bing Maps and Cortana. Microsoft said its investigators have for weeks been tracking the group, which it calls DEV-0537, as it attacked government, technology, telecom, media, retail and health care sectors around the world.

March 2022

System Security

- Apart from the security breaches that might occur, one must also be concerned with was named *unexpected behavior*
- When anyone is using a system even only with its own firmware and probably an operating system, an usage expectation is always present
    - When it is turned on, when updates are installed, and so on
- But systems by themselves aren't useful, they need to have applications installed
- And depending on the installed one, other expectations emerge
- Assuming those expectations are reasonable, what happens if a different behavior occur?
    - Excel 365 (and previous versions) formula to subtract 177,00 from 182,90 returns 5,90000000000001 if the result cell is formatted as number with 14 decimal places

System Security

- Having solve or mitigate the system in terms of erroneous and unexpected errors, several others aspects needs to be thought
- What services are running and what aren’t?
- Just check the running services / processes on your own computer
  - Windows: [in cmd] **netstat -an**
  - Linux: [in shell] **ss** or **lsof** (eventually with options to filter the output)
- Are all services / IP / ports recognized?
- Which ports are listening (e.g., waiting connections) or with established connections?

System Security

- Antivirus, anti-malware, firewall are all usual applications on every system
- However, are they *really* necessary?
- A 0-day (zero-day) can be defined as an attack vector that the vendor or developer was unaware
- All the artefacts that might be installed and in use rely on recognized signatures of attacks
  - If a new one appears, it is unrecognized and as so unprotected

System Security

- It is commonly believed that a firewall will prevent vulnerabilities in processes / systems
- However, a firewall only blocks incoming traffic to the network (or system, in this case), that *crosses* the firewall
- First of all, it wouldn’t block *internal* traffic on the network (as it does not cross the device)
- Secondly, it would accept traffic to open ports that needs to be listening to external requests
  - Meaning that a exploit can be encapsulated on that allowed traffic
- Finally, what is the default behavior of the firewall of your own system?

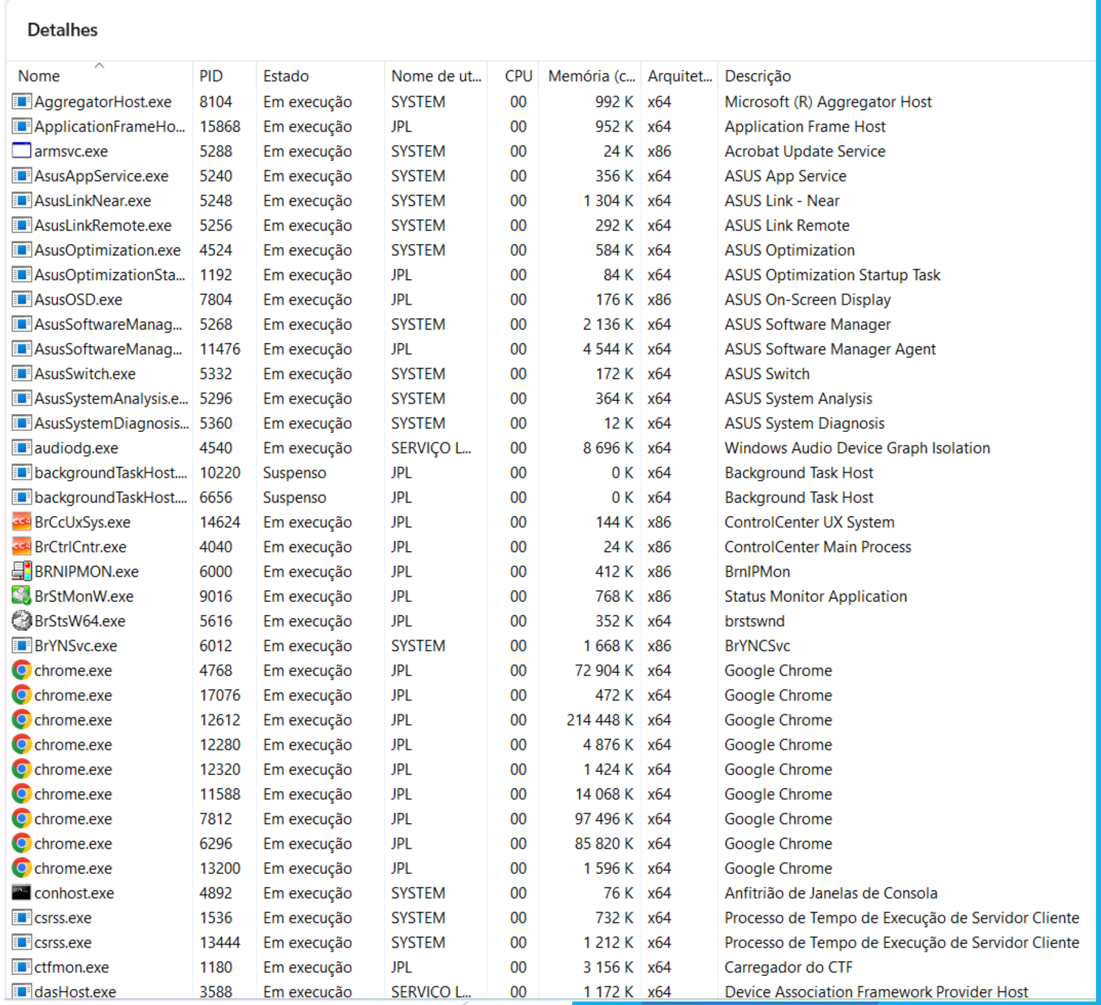
System Security

- The answer to the late question varies according to the operating system
- By default, Windows systems denies all traffic from the exterior except if it is a response to a request initiated on an internal device
- By default, several Linux distributions doesn’t have by default a firewall installed
  - And if *iptables* is installed, the default behavior is to accept all traffic, regardless of its origin
- In either cases, a malware can reside on an internal system that
  - Will initiate a request to the attacker
  - In response, downloads the complete exploit script
  - And once completed, executes it

System Security

- How to avoid this possibility?
- Some artifacts will be discussed on infrastructure class
- Performing regularly the available options (commands) to check the running processes as well as closing the unwanted ports is one of the best options

- However, not simple
- As you might notice on images there are several instances of same process / application with different purposes – assure what ones are needed and what aren't, isn't an easy task



Detalhes

Nome	PID	Estado	Nome de ut...	CPU	Memória (c...	Arquitet...	Descrição
AggregatorHost.exe	8104	Em execução	SYSTEM	00	992 K	x64	Microsoft (R) Aggregator Host
ApplicationFrameHo...	15868	Em execução	JPL	00	952 K	x64	Application Frame Host
armsvc.exe	5288	Em execução	SYSTEM	00	24 K	x86	Acrobat Update Service
AsusAppService.exe	5240	Em execução	SYSTEM	00	356 K	x64	ASUS App Service
AsusLinkNear.exe	5248	Em execução	SYSTEM	00	1 304 K	x64	ASUS Link - Near
AsusLinkRemote.exe	5256	Em execução	SYSTEM	00	292 K	x64	ASUS Link Remote
AsusOptimization.exe	4524	Em execução	SYSTEM	00	584 K	x64	ASUS Optimization
AsusOptimizationSta...	1192	Em execução	JPL	00	84 K	x64	ASUS Optimization Startup Task
AsusOSD.exe	7804	Em execução	JPL	00	176 K	x86	ASUS On-Screen Display
AsusSoftwareManag...	5268	Em execução	SYSTEM	00	2 136 K	x64	ASUS Software Manager
AsusSoftwareManag...	11476	Em execução	JPL	00	4 544 K	x64	ASUS Software Manager Agent
AsusSwitch.exe	5332	Em execução	SYSTEM	00	172 K	x64	ASUS Switch
AsusSystemAnalysis.e...	5296	Em execução	SYSTEM	00	364 K	x64	ASUS System Analysis
AsusSystemDiagnosis...	5360	Em execução	SYSTEM	00	12 K	x64	ASUS System Diagnosis
audiodg.exe	4540	Em execução	SERVIÇO L...	00	8 696 K	x64	Windows Audio Device Graph Isolation
backgroundTaskHost....	10220	Suspenso	JPL	00	0 K	x64	Background Task Host
backgroundTaskHost....	6656	Suspenso	JPL	00	0 K	x64	Background Task Host
BrCcUxSys.exe	14624	Em execução	JPL	00	144 K	x86	ControlCenter UX System
BrCtrlCntr.exe	4040	Em execução	JPL	00	24 K	x86	ControlCenter Main Process
BRNIPMON.exe	6000	Em execução	JPL	00	412 K	x86	BrnIPMon
BrStMonW.exe	9016	Em execução	JPL	00	768 K	x86	Status Monitor Application
BrStsW64.exe	5616	Em execução	JPL	00	352 K	x64	brstswnd
BrYNSvc.exe	6012	Em execução	SYSTEM	00	1 668 K	x86	BrYNCSvc
chrome.exe	4768	Em execução	JPL	00	72 904 K	x64	Google Chrome
chrome.exe	17076	Em execução	JPL	00	472 K	x64	Google Chrome
chrome.exe	12612	Em execução	JPL	00	214 448 K	x64	Google Chrome
chrome.exe	12280	Em execução	JPL	00	4 876 K	x64	Google Chrome
chrome.exe	12320	Em execução	JPL	00	1 424 K	x64	Google Chrome
chrome.exe	11588	Em execução	JPL	00	14 068 K	x64	Google Chrome
chrome.exe	7812	Em execução	JPL	00	97 496 K	x64	Google Chrome
chrome.exe	6296	Em execução	JPL	00	85 820 K	x64	Google Chrome
chrome.exe	13200	Em execução	JPL	00	1 596 K	x64	Google Chrome
conhost.exe	4892	Em execução	SYSTEM	00	76 K	x64	Anfitrião de Janelas de Consola
csrss.exe	1536	Em execução	SYSTEM	00	732 K	x64	Processo de Tempo de Execução de Servidor Cliente
csrss.exe	13444	Em execução	SYSTEM	00	1 212 K	x64	Processo de Tempo de Execução de Servidor Cliente
ctfmon.exe	1180	Em execução	JPL	00	3 156 K	x64	Carregador do CTF
dasHost.exe	3588	Em execucão	SERVICO L...	00	1 172 K	x64	Device Association Framework Provider Host

System Security

- Controls must be implemented to audit the security of the system
- Depending on the used operating system, a deep look into the available event registration might not be feasible
- Monitoring is usually a good turnaround to have knowledge of unexpected behaviors
- However, the controls used for monitoring must be well defined
  - Access type (local, remote, VPN, etc.)
  - Timestamp of access (usual working hours of the worker?)
  - Changes in configuration
  - Among others

To summarise

- System security depends on
  - Where it is hosted
  - How it is configured
  - The applications that run on it
  - The access configured
- Having artifacts like firewall, antimalware, antivirus helps, but it is not a solution
- Auditing and monitoring might help (and will be visited again later)