

ICT Risk Assessment (and Management) (of networks+Cloud Computing+IOT+ ...)

Fabrizio Baiardi
f.baiardi@unipi.it



Why this course ... :-)

Any logical structure that humans can conceive will be susceptible to attacks, and the more complex the structure, the more certain that it can be attacked

John Mc Afee speaking about the defects in AI software

If you don't know how "it" works then you won't manage its risks. Or, as they say in the poker world, if after ten minutes at the table you don't know who the patsy is—you're the patsy.

Daniel E. Geer, Jr.



Syllabus

- Introduction to ICT Security
 - Risk Analysis
 - Countermeasures
- Cloud Computing:
 - Supporting Technologies
 - Virtualization
 - Elasticity
 - Properties and Rules
 - Security of Cloud Computing
 - Threat Model
 - Attacks (Classic + Spectre...)
 - Countermeasures
 - IOT

Fully general

Clouds are interesting!!!

The course structure is updated according to

- new vulnerabilities
- new attacks



Exam

One of

- Written test :-(
 - You choose a topic
 - You choose some papers
 - You prepare the slide
 - You present your lecture

IOT and Cloud are related

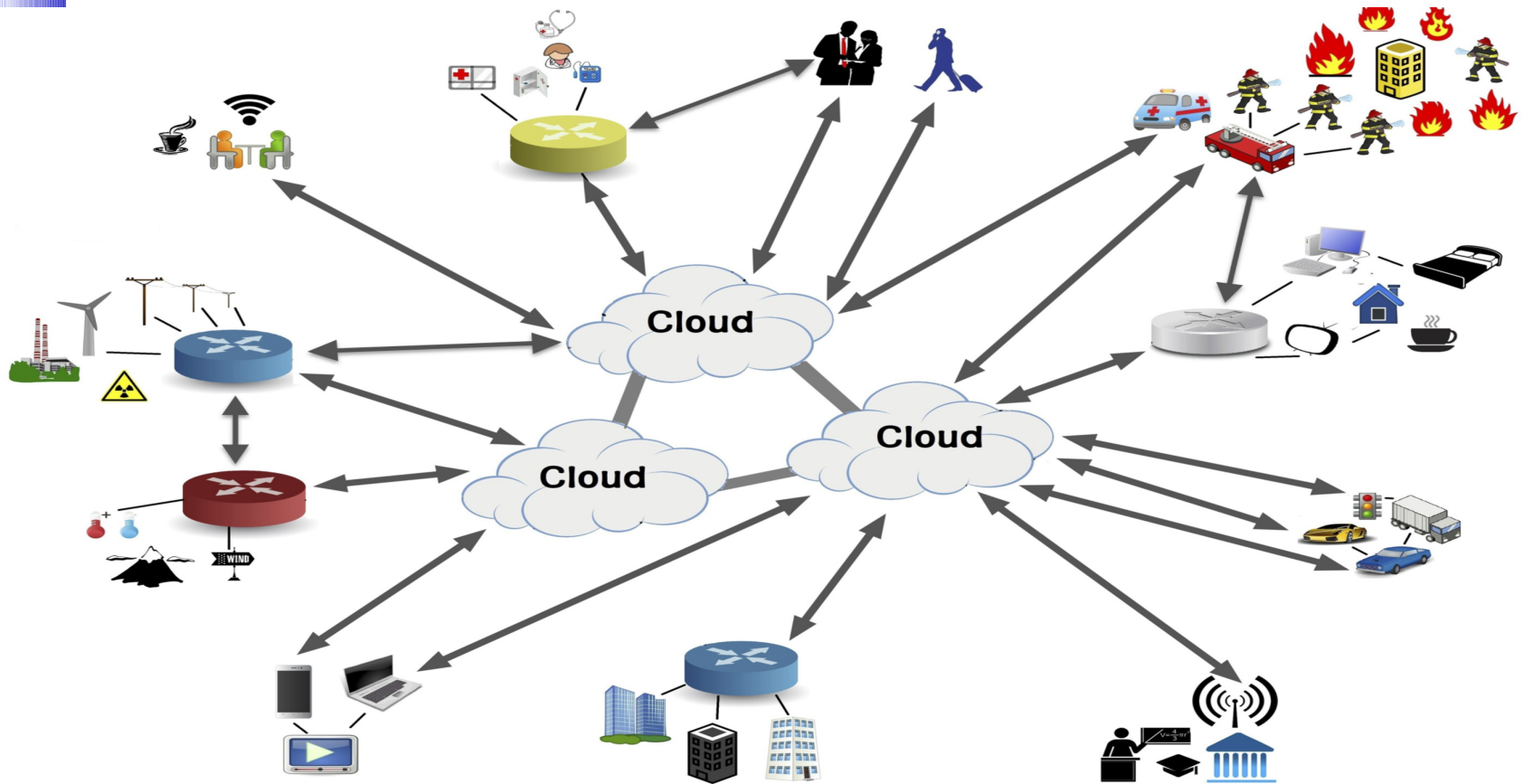
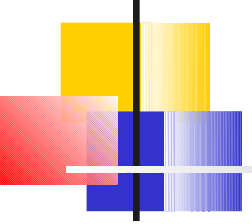
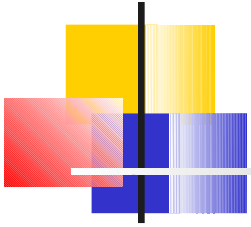


Fig. 1. An illustration of IoT including cloud services (IoT-Cloud).

The beginning of “Cloud Computing”

- 
-
- John McCarthy opined that “Computing may someday be organized as a public utility” - John McCarthy, MIT Centennial in 1961
 - “Comes from the early days of the Internet where we drew the network as a cloud... we didn’t care where the messages went... the cloud hid it from us” – Kevin Marks, Google
 - First cloud around networking (TCP/IP abstraction)
 - Second cloud around documents (WWW data abstraction)
 - The emerging cloud hides details to final users by abstracting infrastructure complexities of servers, applications, data, and heterogeneous platforms

Utility vs Cloud Computing

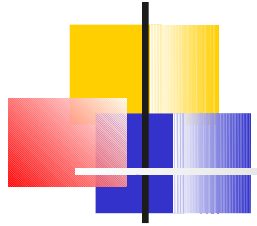


Utility computing

- customers receive computing resources from a service provider (hw and/or sw) and “pay by the drink,” as for electric service at home
- requires a cloud-like infrastructure
- focused on better economics. Corporate data centers are usually underutilized, with resources often idle = overprovisioning = more hardware to handle peaks
- allows companies to only pay for the computing resources they need, when they need them.

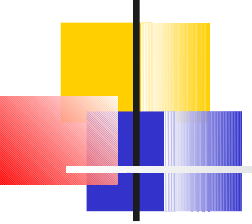
Cloud computing is a broader concept that relates to the underlying architecture where services are designed. It may be applied equally to utility services and internal corporate data center

Fog vs Cloud Computing



- Fog Computing should extends Cloud computing and services to the edge of the network. Its distinguishing characteristics are its proximity to end-users, its dense geographical distribution, and its support for mobility. Services are hosted at the network edge or even end devices such as set-top-boxes or access points.
- Fog aims to reduce service latency and to improve QoS, resulting in superior user-experience.
- Fog Computing supports emerging Internet of Everything (IoE) applications that demand real-time/predictable latency
- Unlike traditional data centers, fog devices are geographically distributed over heterogeneous platforms, spanning multiple management domains.

A Working Definition of Cloud Computing




Cloud computing is a model for enabling
convenient,
on-demand
network access

to a shared pool of configurable and geographically distributed
resources (e.g., networks, servers, storage, applications,) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

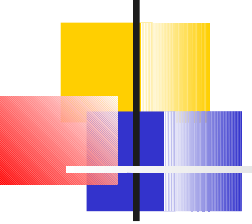
This cloud model promotes availability and is defined in terms of
five essential **characteristics**,
three **service models**,
four **deployment models**.

Design space

5 Essential Cloud Characteristics

- 
-
- On-demand self-service
 - Broad network access = web access
 - Resource pooling = Location independence through web / broad band access
 - Rapid elasticity
 - Measured service
 -
 - Cloud computing is possible only because of web+broadband and it is not available if/when/where internet access is not available
 -
 -

Common Cloud Characteristics

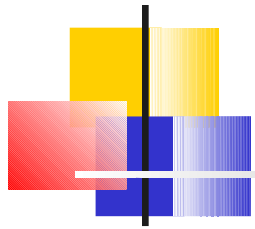
- 
-
- Massive scale
 - Homogeneity
 - Virtualization
 - Resilient computing
 - Low cost software
 - Geographic distribution
 - Service orientation
 - Advanced security technologies



NIST framework and terms

- This course adopts and follows a framework developed by the National Institute of Standard and Technologies
- This framework has been and is used in the USA to drive the adoption of cloud computing in most of federal and state offices
- Focused on
 - the kind of access to the cloud system (service model)
 - the underlying architecture (deployment model)

The NIST Cloud Definition Framework



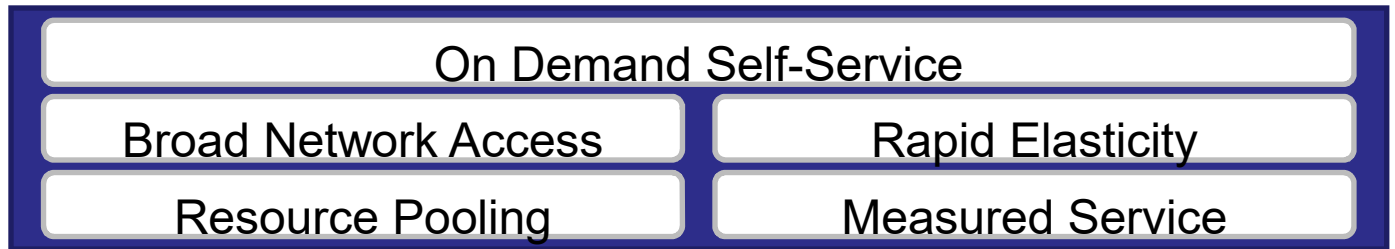
Deployment Models



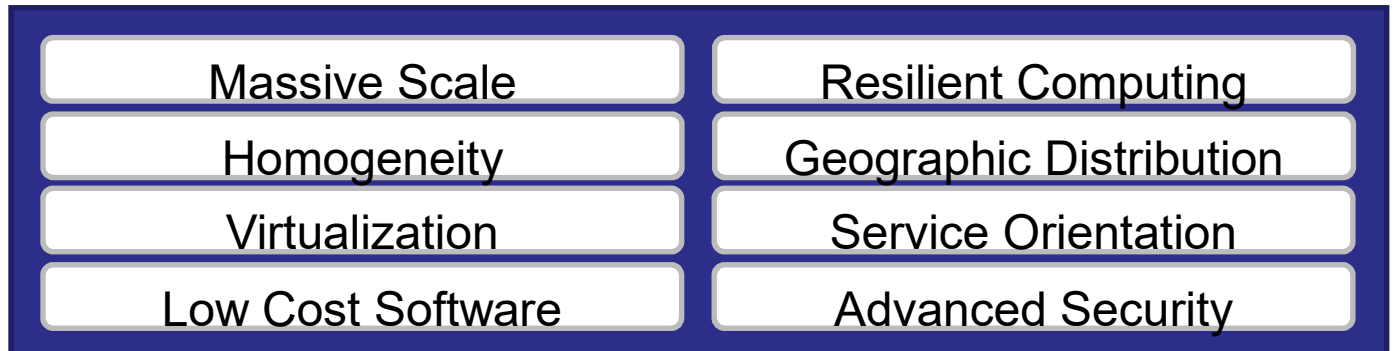
Service Models



Essential Characteristics



Common Characteristics





Cloud and Security - I

Economy and flexibility



**Private
Cloud**

Software as a
Service (SaaS)

**Community
Cloud**

Platform as a
Service (PaaS)

Public Cloud

Infrastructure as a
Service (IaaS)



Economy and flexibility



Cloud and Security - II

Complexity of security problems



**Private
Cloud**

Software as a
Service (SaaS)

**Community
Cloud**

Platform as a
Service (PaaS)

Public Cloud

Infrastructure as a
Service (IaaS)



Complexity of security problems

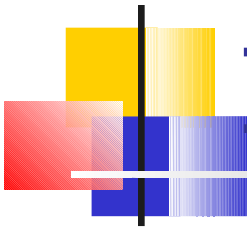


IOT

"The Internet of Things (IoT) is the interconnection of uniquely identifiable embedded computing devices within the existing Internet infrastructure. Typically, IoT is expected to offer advanced connectivity of devices, systems, and services that goes beyond machine-to-machine communications (M2M) and covers a variety of protocols, domains, and applications. Things, in the IoT, can refer to a wide variety of devices such as heart monitoring implants, biochip transponders on farm animals, automobiles with built-in sensors, or field operation devices that assist fire-fighters in search and rescue." Wikipedia

- *IoT network resilience to cyber attacks*
- *Individual as a Data cluster*
- *Privacy*
- *Concrete cyber threats*
- *Influencing human behavior*





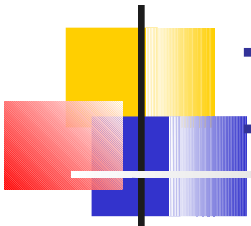
IOT = Smart Thing

- Anything that is “smart” is smart because it has a computer and the computer can be attacked
- An important component of the IOT are sensors
- Several attacks against sensors exploit the physics a sensor exploits
 - attacks using ultrasound against a microphone
 - attacks sending fake information to GPS sensors
 - ...
- Complexity of security increases because of the lack of computational resources in the computer



ICT Security & Risk

- A topic at the intersection of three areas
 - Computer Science
 - Human Resources and Management
 - Economy
- From ICT security to ICT risk assessment and management
- “Kids speaks about security real women/men about risk assessment and management ” :-)
- Risk = Risk(probability, damage (or impact))
- Risk management = an approach strongly related to probability, impact, cost effectiveness of solutions



ICT Security & Risk

Largest risks in this year

	Likelihood*	Impact**	Risk score
Cyber attack & data breach	3.25	2.17	7.05
IT and telecom outage	3.12	1.91	5.95
Adverse weather/natural disaster (e.g. hurricane/earthquake)	3.01	1.82	5.47
Critical infrastructure failure	2.48	2.19	5.43
Reputation incident	2.53	2.02	5.11
Regulatory changes	2.95	1.63	4.80
Lack of talent/key skills	2.73	1.68	4.58
Supply chain disruption	2.5	1.78	4.45
Interruption to utility supply	2.67	1.65	4.40
Political change	2.66	1.58	4.20
Introduction of new technology (Blockchain, AI, IoT)	2.63	1.57	4.12
Health and safety incident	2.69	1.53	4.11
Lone attacker/active shooter incident	1.71	2.32	3.96
Exchange rate volatility	2.31	1.57	3.62
Disease outbreak	2.01	1.7	3.41
Higher cost of borrowing	2.1	1.48	3.10
Political violence/civil unrest	1.96	1.55	3.03
Product quality incident/product recall	1.83	1.6	2.92
Natural resources shortage	1.75	1.54	2.69





ICT Security & Risk

- A topic at the intersection of three areas
 - Computer Science
 - Human Resources and Management
 - Economy
- From ICT security to ICT risk assessment and management
- “Kids speaks about security real women/men about risk assessment and management ” :-)
- Risk = Risk(probability, damage (or impact))
- Risk management = an approach strongly related to probability, impact, cost effectiveness of solutions



Why security is important

- Any organization strongly depends upon
 - Its private ICT resources
 - The ICT resources of its partners
 - The ICT systems that connect its private resources with the partners' resources
- Any organization should be able to prove to other ones that it controls its ICT resources
- Security = the owner controls the resources
- Anytime an organization has to show to someone that it satisfies some standards (not only an ICT one) it has to give some assurance it controls its ICT resources



Information Security

- Confidentiality

- An information can be read only by those that are entitled

- Integrity

- An information can be updated only by those that are entitled

- Availability

- An information can be read and updated by those that are entitled when they require the operation

- An ICT resource should be available to those that are entitled to use it



Other properties

- Authentication = you are who you say you are
- Traced = who has invoked an operation
- Accountability = pay for what you have used
- Auditability = evaluate the effectiveness of security solutions
- Forensics = information to prove that that some laws have been violated
(authentication + integrity)
- Privacy = protection of personal information
(stronger requirements, no inference)



Vulnerability

- A first key concept for security
- A vulnerability is a defect (an error, a bug) in a person, a component, a set of rules that makes it possible to violate a security property = it enables an attack
- While all vulnerabilities are bugs (errors...) not all bugs are vulnerabilities



Threat agent

- A second key concept for security
- A source of attacks = actions that exploits vulnerabilities to violate some security property
- An agent may be natural (flooding, earthquake) or man-made
- Man-made may be random or malicious
- We can assess risk only if we know both vulnerabilities and threat agents for a system



Attack against an ICT system

- An attack is a sequence of actions to (illegally) gain the control of (a subset of) an ICT system
- The actions can be implemented by a program (exploit)
- Each attack is possible because of some vulnerabilities (defect) of the target system or of its user
- Who controls an ICT (sub)system can
 - Collect any information in the (sub)system
 - Update any information in the (sub)system
 - Prevent someone from accessing any resource/information in the (sub)system



Our perspective

- Attack focused= a cost effective defense from attacks against an ICT system
- Why/Which/When attacks may be successful
- How the risk due to attacks can be managed (prevented, reduce their frequency or their damage ...)
- Selection and deployment of cost effective countermeasures (changes to the system)
- Cost, return, investment,



Alternative approaches

- Unconditional security
 - Any vulnerability in the system will be exploited by the attackers irrespective of cost and complexity
- Conditional security (risk management)
 - Discover which vulnerabilities are convenient to exploit by those interested in attacking the system
 - Some vulnerabilities will not be exploited due to the high cost/complexity of the attacks they enable (they pose too large a risk or are too complex for



Risk analysis

A modern approach to security:

1. Asset analysis (resources to be protected)
2. Vulnerability analysis
3. Attack analysis
4. Threat analysis (sources of attacks)
5. Impact analysis (damages)
6. Risk management =
 - Classify risk
 - Define acceptable risk
 - Select and implement countermeasures



Asset Analysis

- Which logical and physical resources of the ICT system we want to protect
- Who is entitled to access these resources and which operation they are entitled to invoke
 - Who is entitled to read an information
 - Who is entitled to update an information
 - Who is entitled to run a given application
 -
- The analysis defines the goal of our strategy: which resources are we going to defend



Risk analysis and management

- Not all the attacks are worth preventing
- Economy driven solution = Which attacks
 - can be prevented
 - is worth preventing = defence cost less than impact
- A complete and standard methodology is not currently available but several proposals in development
- Quantitative approaches are needed
- Several partial solutions to be integrated



The steps of an intrusion (kill chain)

1. Collection of information about a system
2. Discovery of system vulnerabilities (can be automated)
3. Search or build of a program (=exploit) to implement the attack (even partially)
4. Implementation of the attack \Leftrightarrow

Execution of the exploit +

Execution of human action

1. Install tools to control the system
2. Remove any attack trace on the system
3. Access, update, control a subset of the system information



Local vs remote attack

- An attack is
 - Local if it can be executed provided that the attacker can access a system account
 - Remote if it can be executed even if the attacker cannot access a system account
- A remote attack is obviously more dangerous



Automated attack

- No human action is required, the implementation of the attack is the execution of the exploit
- This is the most dangerous kind of attacks
- Automated attacks characterize ICT security with respect to security in other fields
- The time to execute an automated attack is neglectable
- No know how or abilities are required to the attacker to execute an exploit



Automated Attack and Malware

- A malware is a software designed to attack a system after being installed on the system
- Sometimes this installation requires the user cooperation (phishing)
- A particular kind of exploit because it has to be executed on the system it attacks
- A computer worm is a malware that tries to replicate itself onto other nodes

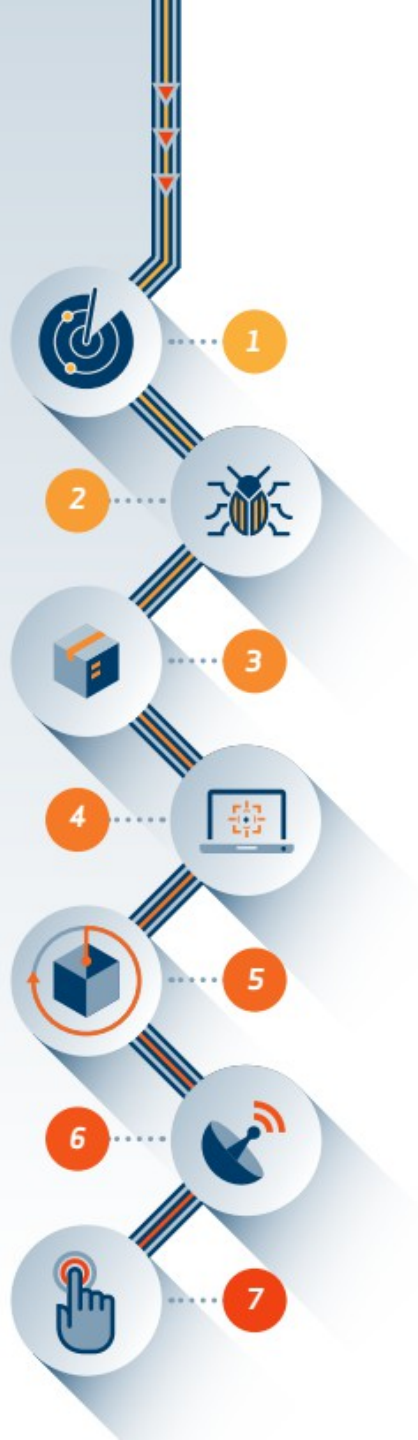
THE LOCKHEED MARTIN CYBER KILL CHAIN®

The Cyber Kill Chain® framework is part of the Intelligence Driven Defense® model for the identification and prevention of cyber intrusions activity. The model identifies what the adversaries must complete in order to achieve their objective.

Stopping adversaries at any stage breaks the chain of attack! Adversaries must completely progress through all phases for success; this puts the odds in our favor as we only need to block them at any given one for success. Every intrusion is a chance to understand more about our adversaries and use their persistence to our advantage.

The kill chain model is designed in seven steps:

- ▶ Defender's goal: understand the aggressor's actions
- ▶ Understanding is Intelligence
- ▶ Intruder succeeds if, and only if, they can proceed through steps 1-6 and reach the final stage of the Cyber Kill Chain®.





Description of the seven steps

- Step 1: Reconnaissance. The attacker gathers information on the target
- Step 2: Weaponization. The attacker creates a malicious payload .
- Step 3: Delivery. The attacker sends the malicious payload to the victim by email or other means.
- Step 4: Exploitation. The actual execution of the exploit, which is, again, relevant only when the attacker uses an exploit.
- Step 5: Installation. Installing malware on the infected computer is relevant only if the attacker used malware. The installation is a point that takes months to operate.
- Step 6: Command and control. The attacker creates a command and control channel in order to operate his internal assets remotely.
- Step 7: Action on objectives. The attacker performs the steps to achieve his actual goals inside the victim's network.

RECONNAISSANCE *Identify the Targets*

ADVERSARY

The adversaries are in the planning phase of their operation. They conduct research to understand which targets will enable them to meet their objectives.

- ▶ Harvest email addresses
- ▶ Identify employees on social media networks
- ▶ Collect press releases, contract awards, conference attendee lists
- ▶ Discover internet-facing servers

DEFENDER

Detecting reconnaissance as it happens can be very difficult, but when defenders discover recon – even well after the fact – it can reveal the intent of the adversaries.

- ▶ Collect website visitor logs for alerting and historical searching.
- ▶ Collaborate with web administrators to utilize their existing browser analytics.
- ▶ Build detections for browsing behaviors unique to reconnaissance.
- ▶ Prioritize defenses around particular technologies or people based on recon activity.

1



WEAPONIZATION *Prepare the Operation*

ADVERSARY

The adversaries are in the preparation and staging phase of their operation. Malware generation is likely not done by hand – they use automated tools. A “weaponizer” couples malware and exploit into a deliverable payload.

- ▶ Obtain a weaponizer, either in-house or obtain through public or private channels
- ▶ For file-based exploits, select “decoy” document to present to the victim.
- ▶ Select backdoor implant and appropriate command and control infrastructure for operation
- ▶ Designate a specific “mission id” and embed in the malware
- ▶ Compile the backdoor and weaponize the payload

DEFENDER

This is an essential phase for defenders to understand. Though they cannot detect weaponization as it happens, they can infer by analyzing malware artifacts. Detections against weaponizer artifacts are often the most durable & resilient defenses.

- ▶ Conduct full malware analysis – not just what payload it drops, but how it was made.
- ▶ Build detections for weaponizers – find new campaigns and new payloads only because they re-used a weaponizer toolkit.
- ▶ Analyze timeline of when malware was created relative to when it was used. Old malware is “malware off the shelf” but new malware might mean active, tailored operations.
- ▶ Collect files and metadata for future analysis.
- ▶ Determine which weaponizer artifacts are common to which APT campaigns. Are they widely shared or closely held?

2



DELIVERY *Launch the Operation*

ADVERSARY

The adversaries convey the malware to the target. They have launched their operation.

- ▶ Adversary controlled delivery:
 - ▶ Direct against web servers
- ▶ Adversary released delivery:
 - ▶ Malicious email
 - ▶ Malware on USB stick
 - ▶ Social media interactions
 - ▶ “Watering hole” compromised websites

DEFENDER

This is the first and most important opportunity for defenders to block the operation. A key measure of effectiveness is the fraction of intrusion attempts that are blocked at delivery stage.

- ▶ Analyze delivery medium – understand upstream infrastructure.
- ▶ Understand targeted servers and people, their roles and responsibilities, what information is available.
- ▶ Infer intent of adversary based on targeting.
- ▶ Leverage weaponizer artifacts to detect new malicious payloads at the point of Delivery.
- ▶ Analyze time of day of when operation began.
- ▶ Collect email and web logs for forensic reconstruction. Even if an intrusion is detected late, defenders must be able to determine when and how delivery began.

3



EXPLOITATION *Gain Access to Victim*

ADVERSARY

The adversaries must exploit a vulnerability to gain access. The phrase “zero day” refers to the exploit code used in just this step.

- ▶ Software, hardware, or human vulnerability
- ▶ Acquire or develop zero day exploit
- ▶ Adversary triggered exploits for server-based vulnerabilities
- ▶ Victim triggered exploits
 - ▶ Opening attachment of malicious email
 - ▶ Clicking malicious link

DEFENDER

Here traditional hardening measures add resiliency, but custom capabilities are necessary to stop zero-day exploits at this stage.

- ▶ User awareness training and email testing for employees.
- ▶ Secure coding training for web developers.
- ▶ Regular vulnerability scanning and penetration testing.
- ▶ Endpoint hardening measures:
 - ▶ Restrict admin privileges
 - ▶ Use Microsoft EMET
 - ▶ Custom endpoint rules to block shellcode execution
- ▶ Endpoint process auditing to forensically determine origin of exploit.

4



INSTALLATION *Establish Beachhead at the Victim*

ADVERSARY

Typically, the adversaries install a persistent backdoor or implant in the victim environment to maintain access for an extended period of time.

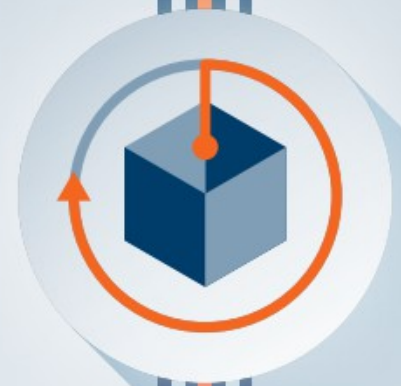
- ▶ Install webshell on web server
- ▶ Install backdoor/implant on client victim
- ▶ Create point of persistence by adding services, AutoRun keys, etc.
- ▶ Some adversaries “time stomp” the file to make malware appear it is part of the standard operating system install.

DEFENDER

Endpoint instrumentation to detect and log installation activity. Analyze installation phase during malware analysis to create new endpoint mitigations.

- ▶ HIPS to alert or block on common installation paths, e.g. RECYCLER.
- ▶ Understand if malware requires administrator privileges or only user.
- ▶ Endpoint process auditing to discover abnormal file creations.
- ▶ Extract certificates of any signed executables.
- ▶ Understand compile time of malware to determine if it is old or new.

5



COMMAND & CONTROL (C2) *Remotely Control the Implants*

ADVERSARY

Malware opens a command channel to enable the adversary to remotely manipulate the victim.

- ▶ Open two way communications channel to C2 infrastructure
- ▶ Most common C2 channels are over web, DNS, and email protocols
- ▶ C2 infrastructure may be adversary owned or another victim network itself

DEFENDER

The defender's last best chance to block the operation: by blocking the C2 channel. If adversaries can't issue commands, defenders can prevent impact.

- ▶ Discover C2 infrastructure thorough malware analysis.
- ▶ Harden network:
 - ▶ Consolidate number of internet points of presence
 - ▶ Require proxies for all types of traffic (HTTP, DNS)
- ▶ Customize blocks of C2 protocols on web proxies.
- ▶ Proxy category blocks, including "none" or "uncategorized" domains.
- ▶ DNS sink holing and name server poisoning.
- ▶ Conduct open source research to discover new adversary C2 infrastructure.

6



ACTIONS ON OBJECTIVES *Achieve the Mission's Goal*

ADVERSARY

With hands-on keyboard access, intruders accomplish the mission's goal. What happens next depends on who is on the keyboard.

- ▶ Collect user credentials
- ▶ Privilege escalation
- ▶ Internal reconnaissance
- ▶ Lateral movement through environment
- ▶ Collect and exfiltrate data
- ▶ Destroy systems
- ▶ Overwrite or corrupt data
- ▶ Surreptitiously modify data

DEFENDER

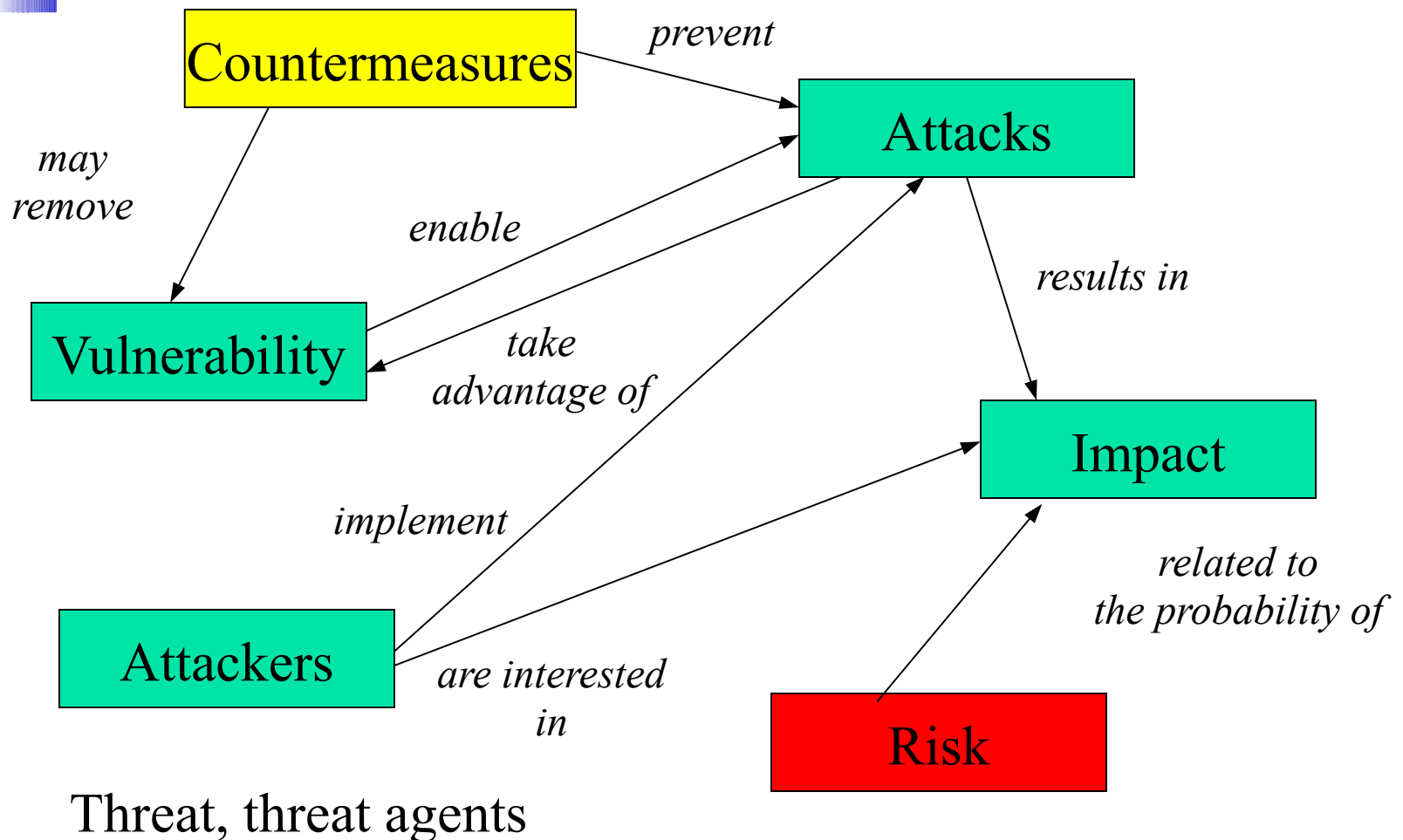
The longer an adversary has CKC7 access, the greater the impact. Defenders must detect this stage as quickly as possible by using forensic evidence – including network packet captures, for damage assessment.

- ▶ Establish incident response playbook, including executive engagement and communications plan.
- ▶ Detect data exfiltration, lateral movement, unauthorized credential usage.
- ▶ Immediate analyst response to all CKC7 alerts.
- ▶ Forensic agents pre-deployed to endpoints for rapid triage.
- ▶ Network package capture to recreate activity.
- ▶ Conduct damage assessment with subject matter experts.

7



Terminology and relations ...





Partial points view on sec– I

- Security = Confidentiality \Leftrightarrow Cryptography
- A set of algorithms to hide information so that only those who know another information (the key) can read it
- A fundamental but partial property because it cannot guarantee availability
- It simplifies but not solves a problem
- *If you think cryptography by itself solve your problem either you do not understand cryptography or you do not understand your problem*



Partial points of view – II

- Several security problems are related to the triple $\langle \text{user, resources, rights=operations on the res} \rangle$
- that determines who can execute what
- Several security mechanisms are related to the solution of these problems
 1. Identifying the user
 2. Identifying the resource
 3. Discover the user rights on the resources
- Sophisticated identification system (biometrics etc.) can solve 1 but neither of the other ones



Partial point of view - III

- Security is not safety that consider random events
- In a system with $10^n - 1$ safe states and 1 unsafe state were the state is randomly chosen,
 - the probability of an unsafe behavior = $1/10^n$
 - system safety increase with n
- If a system has one state out 10^n that is not secure, the threat agent will force the system to enter that state
- Security depends upon the success probability of the agent rather than on the overall number of states
- Attackers are intelligent, adaptive and not random



Partial point of view - IV

- Red team exercises aka penetration test
- You pay someone for attacking your system
 - If the attack fails, you assume your system is ok
 - If the attack is successful you improve it
- Inconsistent approach because you cannot be sure that
 - Your improvement is effective (Braess paradox)
 - The red team has find all the possible attack
 - A red team failure has a large number of reasons ...
-



Safety vs Security

- Triple modular redundancy is a standard strategy to increase safety that introduces three instances of each module
 - Any input is copied to each module
 - The modules compute in parallel
 - Vote on the output and selection of the output with the largest number of votes
- If a module is affected by a vulnerability then the attacker has two more opportunities to be successful



Safety vs Security

- To make thing worst in the IOT you cannot have safety without security or a lack of security results in a lack of safety
- If terrorist controls a smart semaphore the traffic can become rather unsafe and result in several security problem
- A robot that is not secure can kill workers and so on



Some examples

- Vulnerability
- Attack
- Some countermeasures

We describe a stack overflow, a popular attack that is an instance of buffer overrun

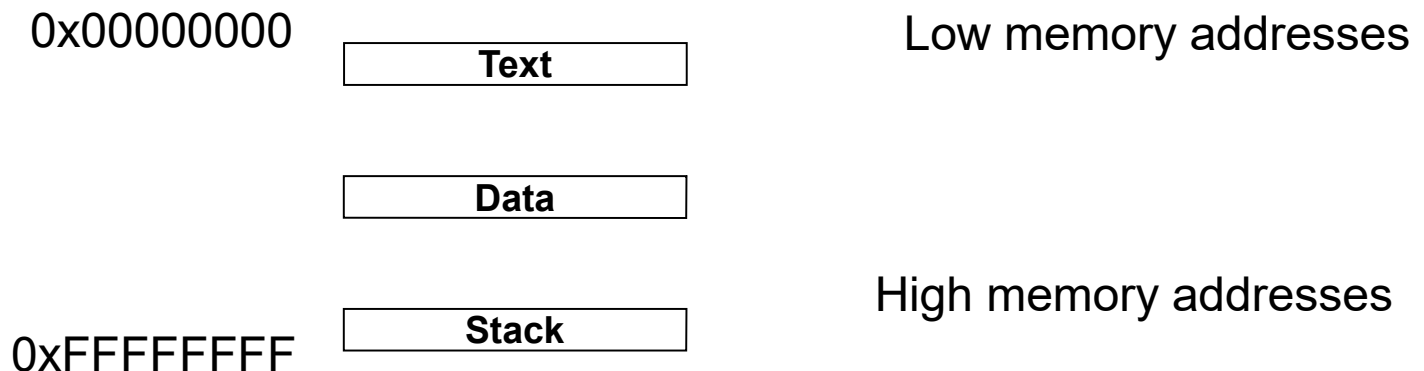


Buffer overflow

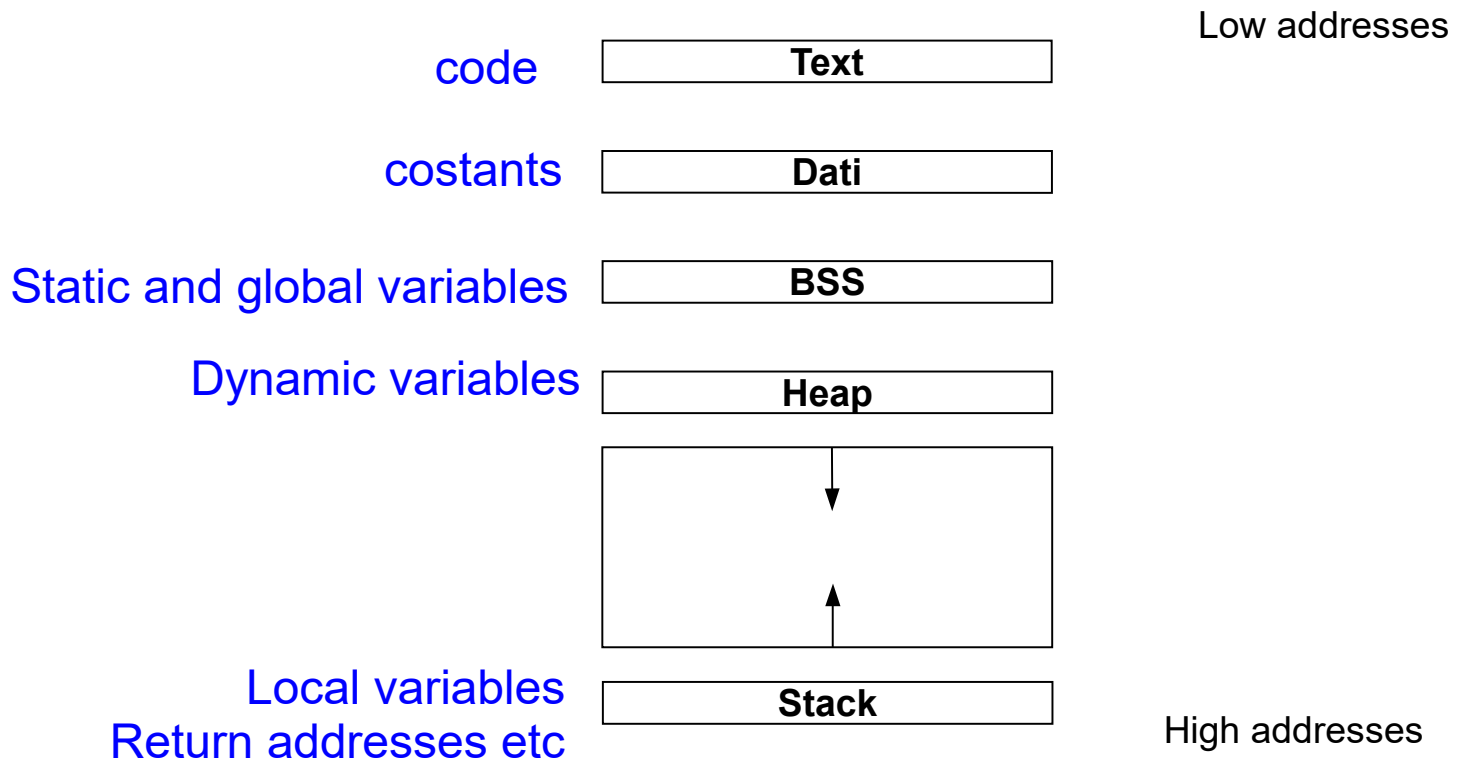
- The *buffer overflow* problem
 - the most common problem among all the vulnerability of C code
 - it does not arise in high level languages where the programmer is not involved in memory management or with strong data types
 - The most important security issue in the last 10 years (not replaced by web vulnerabilities)
 - based on a **forced write of some data with a size larger than expected**. If the program type system does not discover this inconsistency, then some data is replaced in memory.
- In this way, some program can be inserted (code injection) into a system that can, among other execute some shell command. If the program is executed at root level, then it fully control any system function.
- A buffer overflow can exploit any of the following areas **stack, heap e bss (block started by symbol) static variables that are allocated by the compiler.**

A process memory

- To understand buffer overflow, we have to recall the structure of a process memory.
- A process memory is partitioned into three segments: *text*, *data* and *stack*.
- The *text segment* is fixed, stores the program code and it is read only. Any write attempts results in a segmentation error (segmentation fault – core dump)
- The *data segment* stores the process static and dynamic variables
- The *stack segment* stores the data to manage function calls and returns

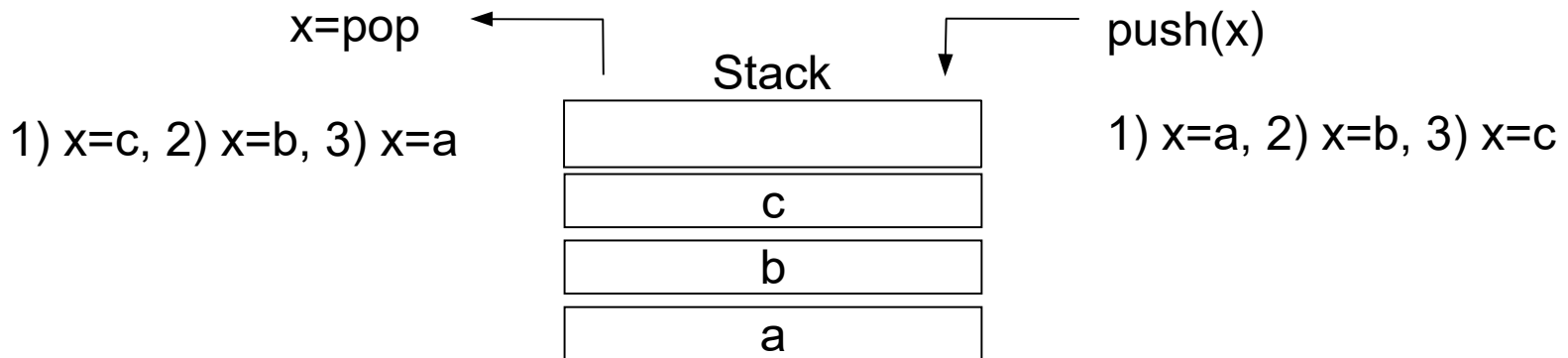


A process memory



Stack

- A Lifo (Last In First Out) data structure that stores a dynamic amount of information
- It is used to manage function calls and returns (call assembly instruction).
- The stack memory area is logically partitioned into records (stack frame) one for each call





Stack and system registers

- The memory address of the instruction to be executed is stored in the **EIP** (Extended Instruction Pointer) register
- **EBP** (Extended Base Pointer) points to the beginning of a *stack frame* while **ESP** (Extended Stack Pointer) points to the end of the stack frame
- When a function is called, the system
 - pushes onto the stack
 - the return address = **EIP+4**,
 - the base address of the current frame = **EBP**
 - **copies ESP** into **EBP** to initialize the new *stack frame*.

Stack and system registers

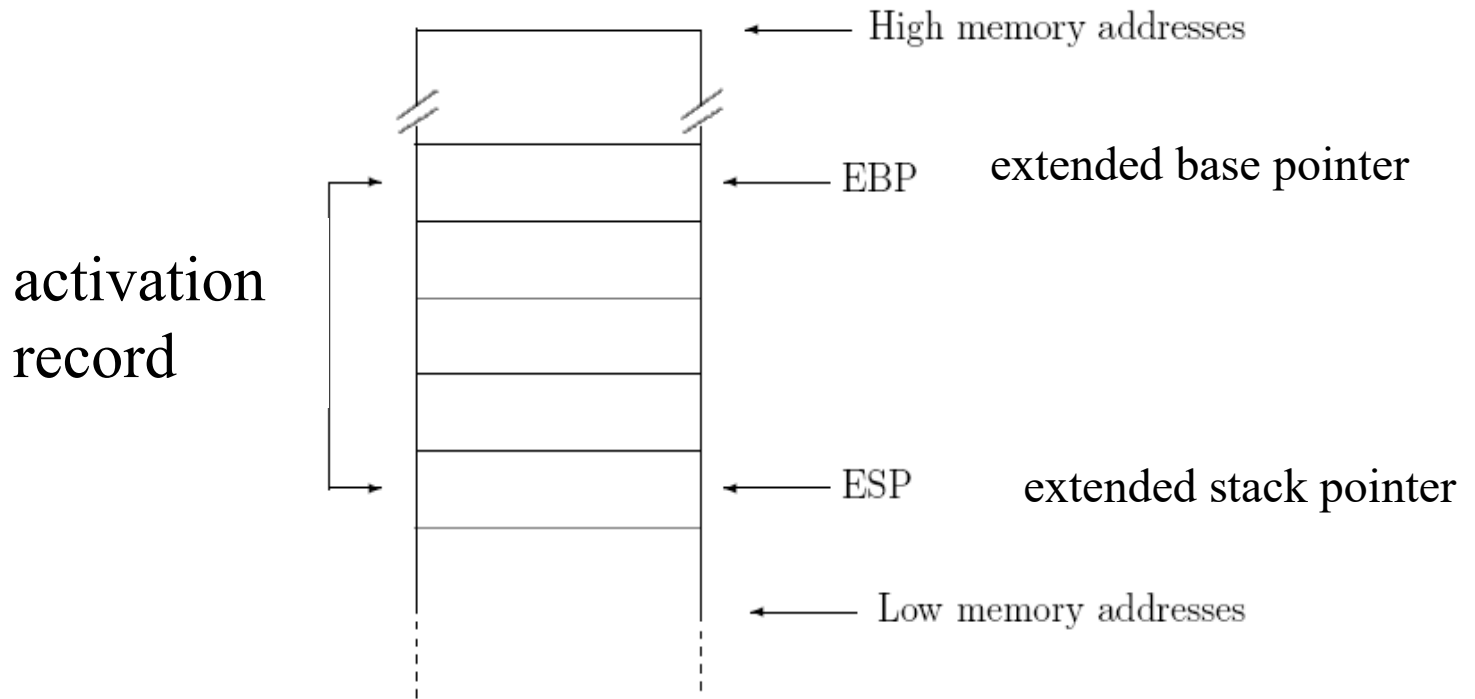
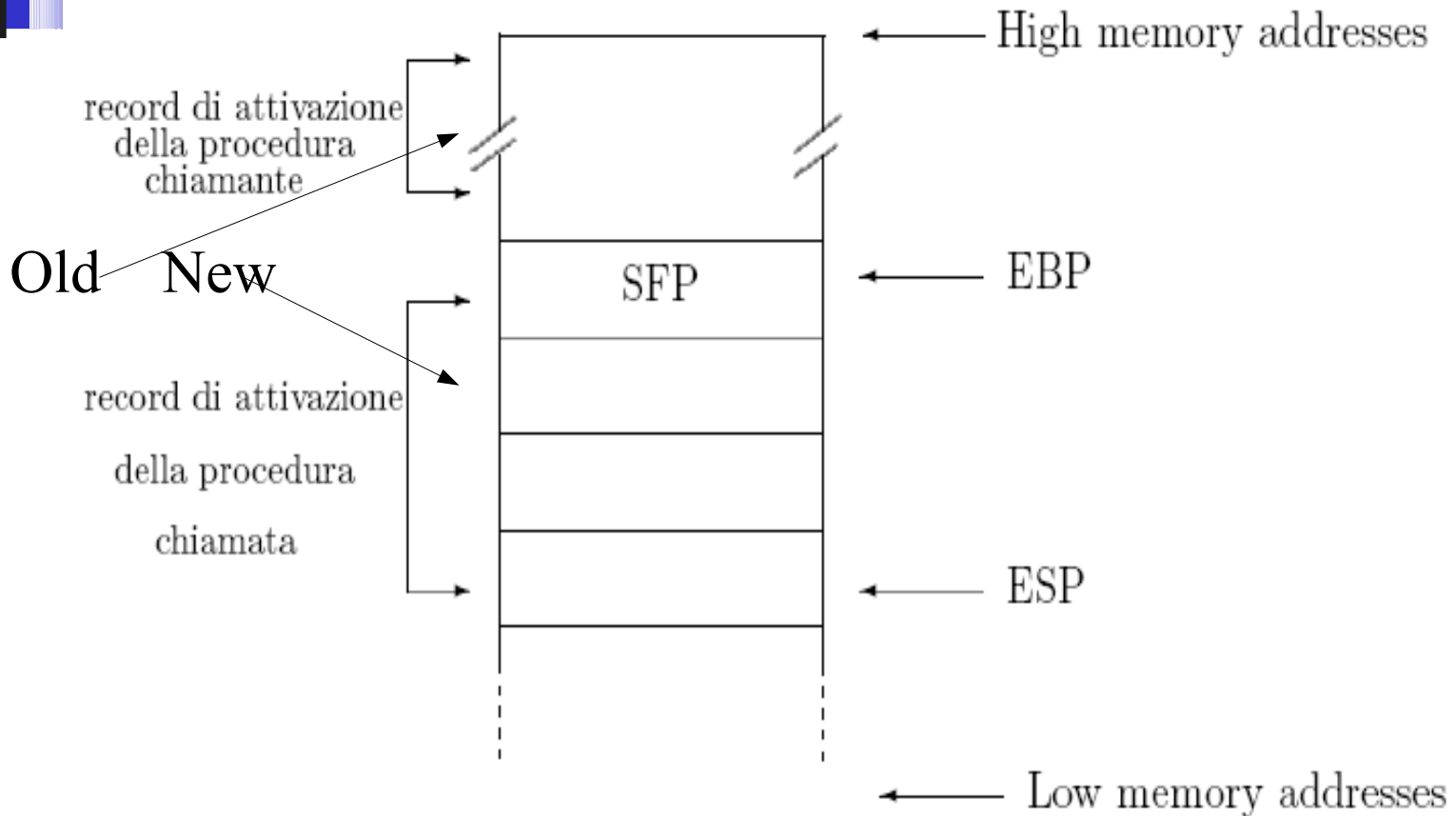


Figura 4: Stack pointer e frame pointer

Stack and system registers

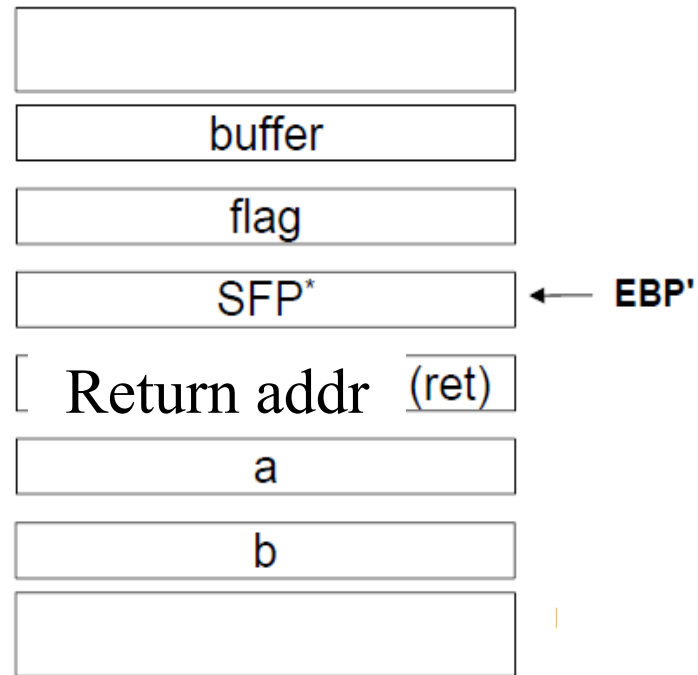


C: an example

This is a simple example to see how all the stuff works

```
void test_function (int a, int b)
{
  char flag;
  char buffer[10];
}
```

```
int main()
{
  test_function (1,2);
  exit(0);
}
Return address = EIP + 4 byte
```



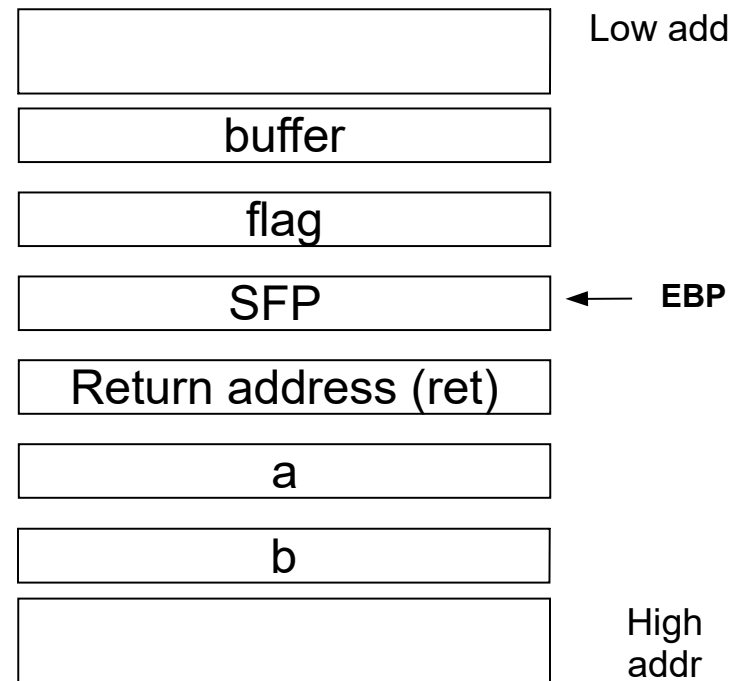
SFP = saved frame pointer = it is used to restore the original value of EBP on a return

The stack frame

- Local variable of *test_function* are addressed by subtracting a displacement from **EBP** while the function parameters are addressed by a positive displacement

- When a function is called EIP points to the function code.

- The stack stores both local variables and parameters of a function. When the function ends, the whole stack frame is removed before returning (**ret**).





Overflow: an example

This C code results in a stack overflow:

```
void overflow_function (char *str) {  
    char buffer[20];  
  
    strcpy(buffer, str); // This function copies str into buffer  
}
```

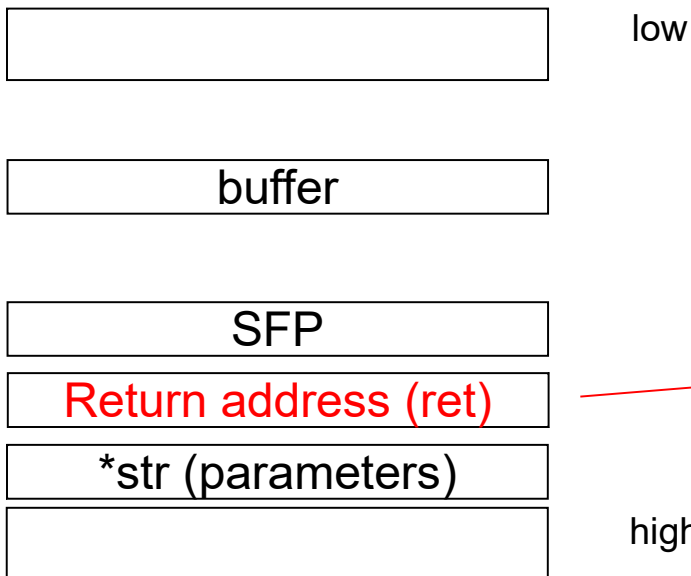
```
int main() {  
    char big_string[128];  
    int i;  
  
    for(i=0; i < 128; i++)  
    {  
        big_string[i] = 'A';  
    }  
    overflow_function(big_string);  
    exit(0);  
}
```

This results in an overflow!

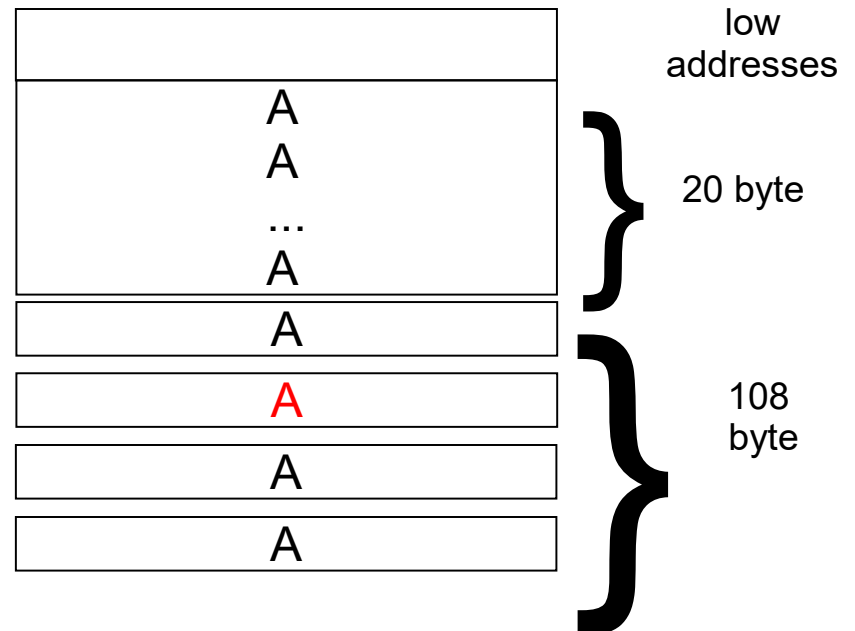
Segmentation fault

The previous code results in a segmentation fault

1) The first call to `overflow_function` correctly initializes the stack frame



2) When `overflow_function` ends, the return address has been overwritten by the character **A** (segmentation fault!)





Buffer (stack) overflow

What happens if the return address (`ret`) stores a valid memory address?

- In this case no exception is signalled and the process continues by executing the instruction pointed by `ret`.
-
- *A stack based buffer overflow* exploits this opportunity by replacing `ret` with a pointer to some code injected by the attacker maybe into the stack itself
- How can we update the return address and inject some code in the system?



A Buffer Overrun

- It occurs when some variable is larger than expected and it overwrites other variables
- It may be implemented if the language lacks a typing system
- Four kinds:
 - Stack based buffer overrun
 - Heap based buffer overrun
 - V-table and function pointer overrun
 - Exception handler overrun
- Rather popular among computer worms (malware)



Stack Overflow

- By copying `x` into the stack we destroy (update ??)
 - The return address
 - Other values on the stack
- The values that are copied codify a program
- The new return address points to the program we have copied onto the stack
- Overall result: an administrative shell
- This is possible only if the procedure that is attacked is executed in root mode

A local fully automated attack



Stack overflow

Vulnerability = alternative perspectives

1. Lack of control on the size of program variables
2. Bad type system
3. Incorrect memory operation
4. Growth direction of the stack
- 5....



Overflow: countermeasures

- Strong typing
- Controls on string lengths
- Insert a “canary” into the stack
- Not executable memory
- Ad hoc checks in the compiler
- ASLR: address space layout randomization



Canary

- A value that differs at each invocation
- Inserted into the stack before any parameter
- Before returning we check that the canary has not been updated
- Randomly chosen at each invocation so that the attacker cannot know its value



Not executable stack

- Controls when fetching an instructions, they can be supported by the MMU
- No data structure can store instructions
- NX bit (the last one) introduced in AMD processors
- It does not work with Linux that stores some drivers in the stack to manage i/o devices



Address Space Layout Randomization ASLR

- The starting point of the various segment is selected randomly
- The attacker cannot know in advance the starting address of data structures of interest
- The first step of the attack has to compute the starting address
- Attack more complex and slower



ASLR – entropy

Type	Description	Protection	Granularity of Rebasing
Free	Free space	Inaccessible	Not rebased
Code	Executable or DLL code	Read-only	15 bits
Static data	Within executable or DLL	Read-Write	15 bits
Stack	Process and thread stacks	Read-Write	29 bits
Heap	Main and other heaps	Read-Write	20 bits
TEB	Thread Environment Block	Read-Write	19 bits
PEB	Process Environment Block	Read-Write	19 bits
Parameters	Command-line and Environment variables	Read-Write	19 bits
VAD	Returned by virtual memory allocation routines	Read-Write	15 bits
VAD	Shared Info for kernel and user mode	Unwritable	Not rebased

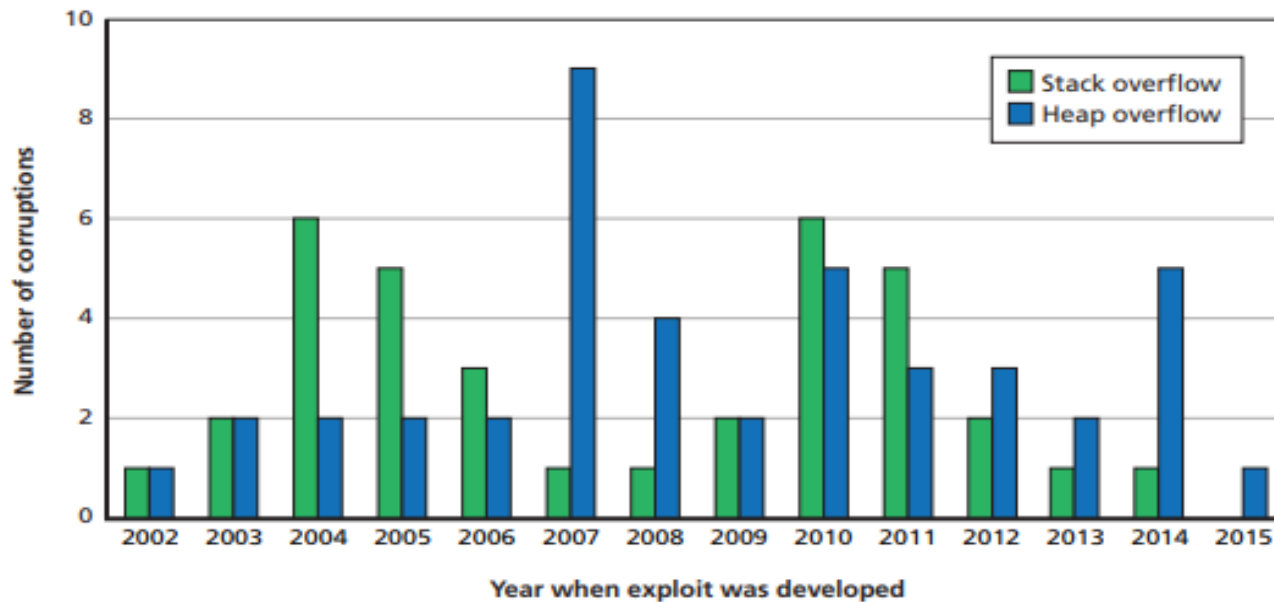


Cost of the countermeasures

- Each countermeasure has a distinct cost
 - Strong typing = 10-30% run time overhead
 - Checks on string length = large cost but lower than the previous one
 - Canary = specialized control, low cost
 - ASLR supported by MMU translation low cost
 - Not executable stack = lowest cost because it exploits an hardware/firmware support

Stack vs heap

Figure C.1
Type of Memory Corruption, Counts by Year (n = 101)





Structural vulnerability TCP/IP

- When the TCP/IP stack has been defined, the
- main goal was resilience against physical
- attack against the network (attack = bombing)
- Main goal = availability
- ⇒ Some mechanism defined to discover which nodes are alive and reachable
- ⇒ No mechanism is available to guarantee \ (authenticate) the source of a message



Structural vuln: an Example

1. A node can send an ECHO message to check whether another node is alive and reachable, The receiver replies by returning the same message.
2. The sender can specify a partial IP address to broadcast a message to check a set of other nodes
3. There is no control on the fields of an IP packet a node sends



All together now ..

1. R is a network with 1000 nodes, X is a partial IP address that matches the addresses of all nodes of R
2. A sends a ECHO message to the address X but it specifies the address of B as the packet sender address
3. Any node in R replies to B
4. B cannot interact with other nodes because its communication lines are overflowed by the ECHO messages

Distributed Denial of Service



All together now +IOT

OVH France-based hosting provider, was the victim of a wide-scale DDoS attack carried via network of over **152,000 IoT devices**.

According to OVH the DDoS attack reached nearly **1 Tbps at its peak**. Of those IoT devices participating in the DDoS attack, **they were primarily comprised of CCTV cameras and DVRs**. Many of these types devices' network settings are improperly configured, which leaves them ripe for the picking for hackers that would love to use them to carry out destructive attacks. **OVH originally stated that 145,607 devices made up the botnet, but recently confirmed that another 6,857 cameras joined in on the attack.**

The DDoS peaked at 990 Gbps on September 20th thanks to two concurrent attacks, and according to OVH, the original botnet was capable of a **1.5 Tbps DDoS attack** if each IP topped out at 30 Mbps.



Security as an holistic property

- A system security is not implied by (cannot be deduced from) the one of each of its modules
- The overall system may be unsecure even when each module is secure
- In a virtual machine hierarchy the security of a machine may be destroyed by a vulnerability in an underlying machine



Impact and countermeasures

- The DDOS impact
 - depends upon the numbers of nodes, zombies, whose address matches that in the message
 - may be amplified by further messages
- Very few effective countermeasures because B is aware of the attack when it starts to receive messages
- This is structural vulnerability, it depends not upon the building blocks but upon the composition



Design approaches vs vulns

When designing and building a system we may adopt one of two approaches

- a) pretend there are no vulnerabilities in the components (penetrate and patch)
- b) be aware that there are vulnerabilities and try to anticipate them even if we still do not know which vulnerabilities (proactive approach)



Penetrate and patch

- Vulnerabilities have not been anticipated
- Since we have assumed there are no vulnerabilities, we should remove (patch) a vulnerability as soon as it is discovered.
- There is a competition between
 - discovering and exploiting vulnerabilities
 - patching the system to remove them



Security Patch (wikipedia)

- A security patch is a change applied to an asset (OS, application, ...) to correct the weakness described by a vulnerability.
- This corrective action will prevent successful exploitation and remove or mitigate a threat's capability to exploit the vulnerability to attack an asset.
- Security patches are the primary method of fixing security vulnerabilities in software. Currently Microsoft releases its security patches once a month, and other operating systems and software projects have security teams dedicated to releasing the most reliable software patches as soon after a vulnerability announcement as possible.
- Security patches are closely tied to responsible disclosure.

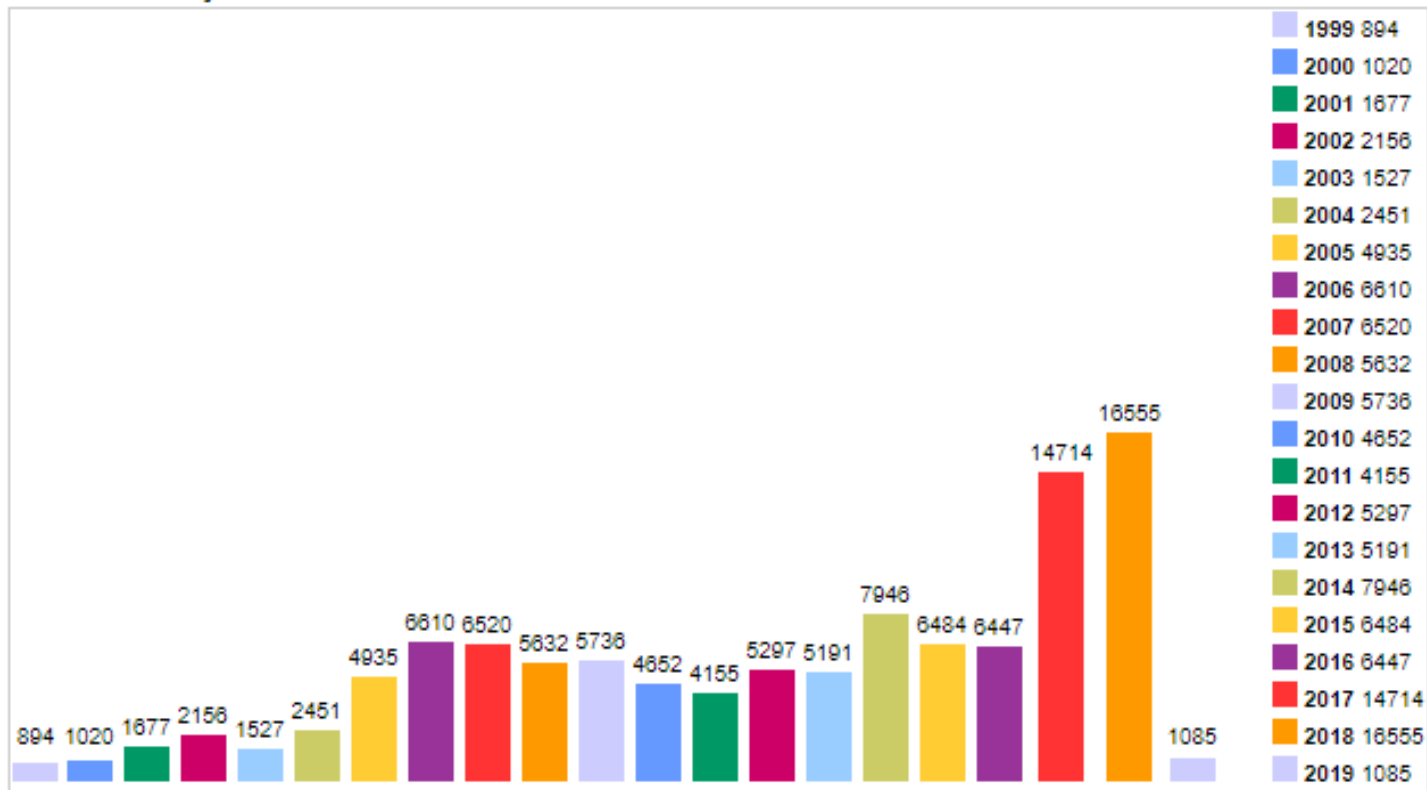


Patches: problem

- Any patching updates a software component and changes its behaviour
- The change may influence the users
- A patch can be applied only after checking that the changes can be accepted
- Sometime a patch cannot be applied, eg certification of a system where the software is just one component

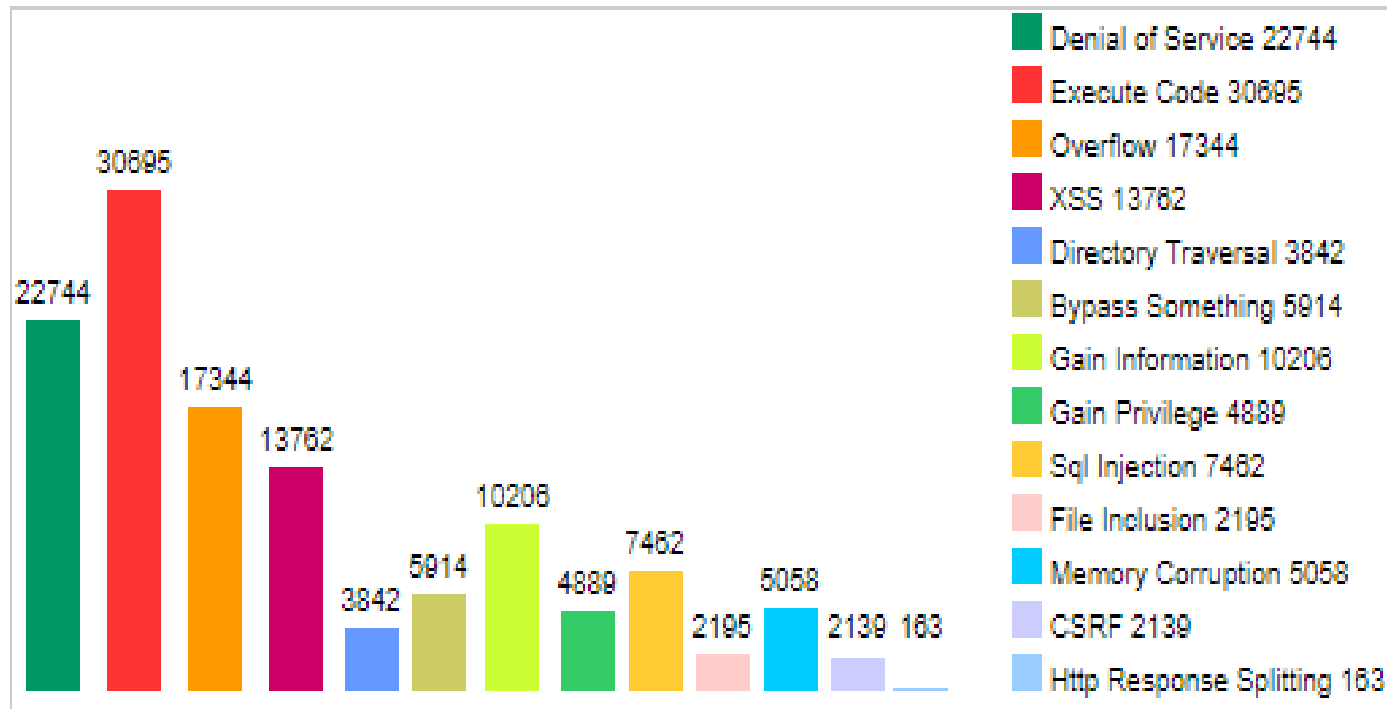
Number of vulnerabilities discovered

Vulnerabilities By Year

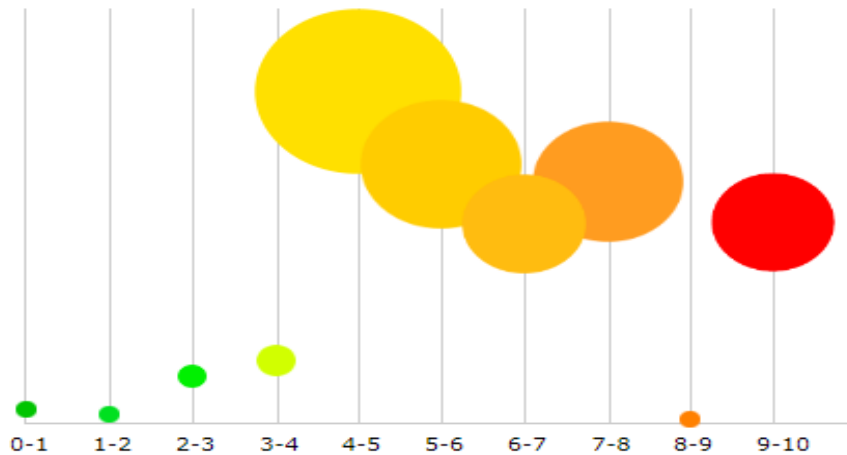


Number of vulnerabilities discovered

Vulnerabilities By Type



How dangerous (not risk)

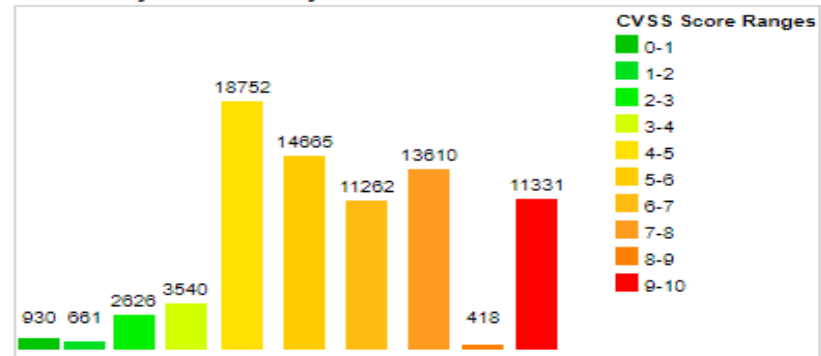


Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	930	1.20
1-2	661	0.80
2-3	2626	3.40
3-4	3540	4.60
4-5	18752	24.10
5-6	14665	18.90
6-7	11262	14.50
7-8	13610	17.50
8-9	418	0.50
9-10	11331	14.60
Total	77795	

Weighted Average CVSS Score: 6.6

Vulnerability Distribution By CVSS Scores





Top 10 Vulnerabilities - Windows Systems

1. Internet Information Services
2. Microsoft SQL Server
3. Windows Authentication
4. Internet Explorer
5. Windows Remote Access Services
6. Data Access Components(MDAC)
7. Windows Scripting Host
8. Outlook and Outlook Express
9. Peer to Peer File Sharing
10. Simple Network Management



Top 10 Vulnerabilities - Unix Systems

1. BIND Domain Name System
2. Remote Procedure Calls (RPC)
3. Apache Web Server
4. Accounts with No Passwords or Weak Passwords
5. Clear Text Services
6. Sendmail
7. Simple Network Management Protocol
8. Secure Shell (SSH)
9. Misconfiguration of NIS/NFS
10. Open Secure Sockets Layer (SSL)



Other lists - I

- Top Vulnerabilities in Windows Systems
 - W1. Windows Services
 - W2. Internet Explorer
 - W3. Windows Libraries
 - W4. Microsoft Office and Outlook Express
 - W5. Windows Configuration Weaknesses
- Top Vulnerabilities in Cross-Platform Applications
 - C1. Backup Software
 - C2. Anti-virus Software
 - C3. PHP-based Applications
 - C4. Database Software
 - C5. File Sharing Applications
 - C6. DNS Software
 - C7. Media Players
 - C8. Instant Messaging Applications
 - C9. Mozilla and Firefox Browsers
 - C10. Other Cross-platform Applications



Other lists - II

- Top Vulnerabilities in UNIX Systems
 - U1. UNIX Configuration Weaknesses
 - U2. Mac OS X
- Top Vulnerabilities in Networking Products
 - N1. Cisco IOS and non-IOS Products
 - N2. Juniper, CheckPoint and Symantec Products
 - N3. Cisco Devices Configuration Weaknesses



Hippa vulnerabilities

- Firewall and System Probing
- Network File Systems (NFS) Application
- Electronic Mail Attacks
- Vendor Default Password Attacks
- Spoofing, Sniffing, Fragmentation and Splicing
- Social Engineering Attacks
- Easy-To-Guess Password
- Destructive Computer Viruses
- Prefix Scanning (Illegal Modem)
- Trojan Horses

Life cycle of a vulnerability in a penetrate and patch world



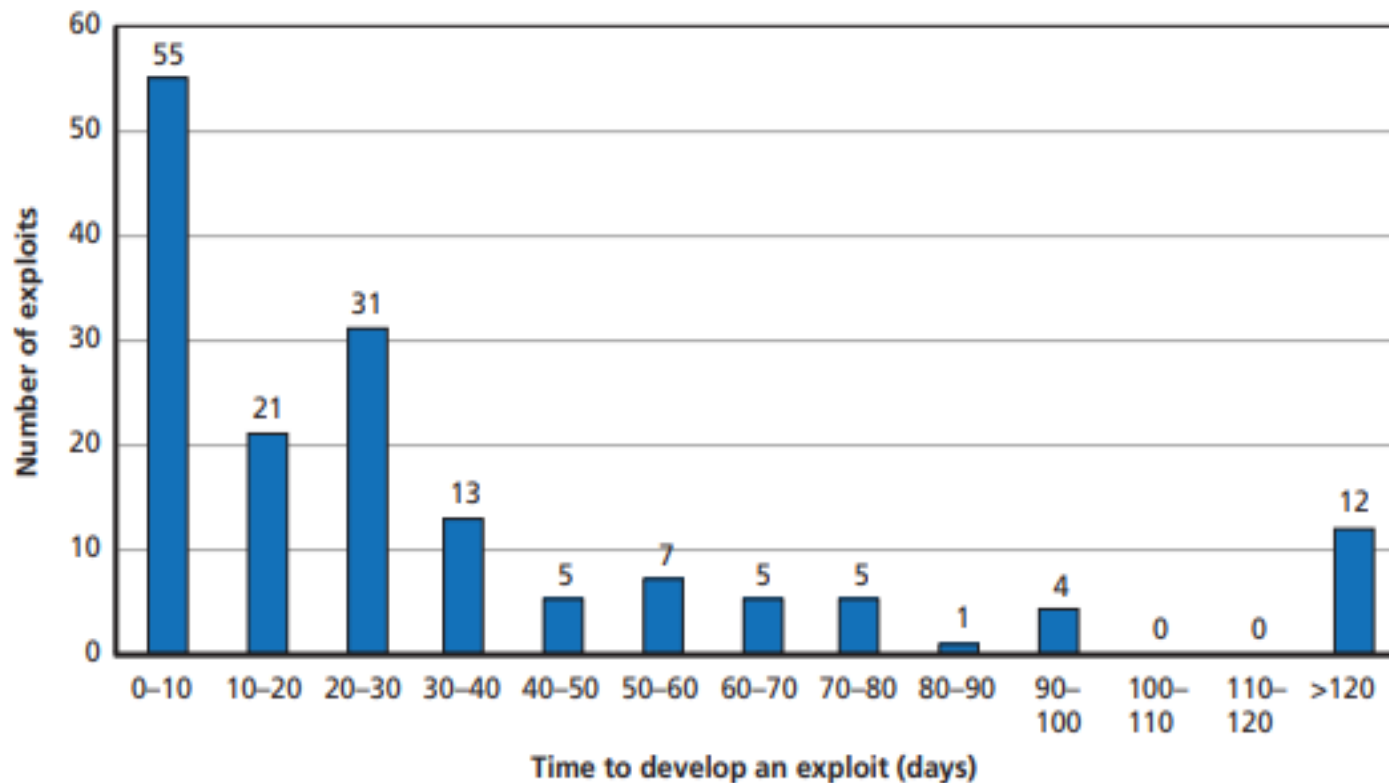


State of a vulnerability - 1

1. The vulnerability has been discovered
2. Both the vulnerability and an exploit that takes advantage of the vulnerability have been discovered
3. Both the vulnerability and a patch that removes the vulnerability have been discovered (a race with 2)
4. The vulnerability, the exploit and the patch have been discovered

Time for an exploit

Frequency Count of Time to Develop an Exploit (n = 159)





State of a vulnerability - 2

- Sometimes a system is attacked even if a vulnerability is in the last status
- It is well known that sometimes the owner of a system does not apply a patch even if it is available
- Asymmetry between the owner and the software supplier (applying the patch is the owner responsibility rather than the supplier one)

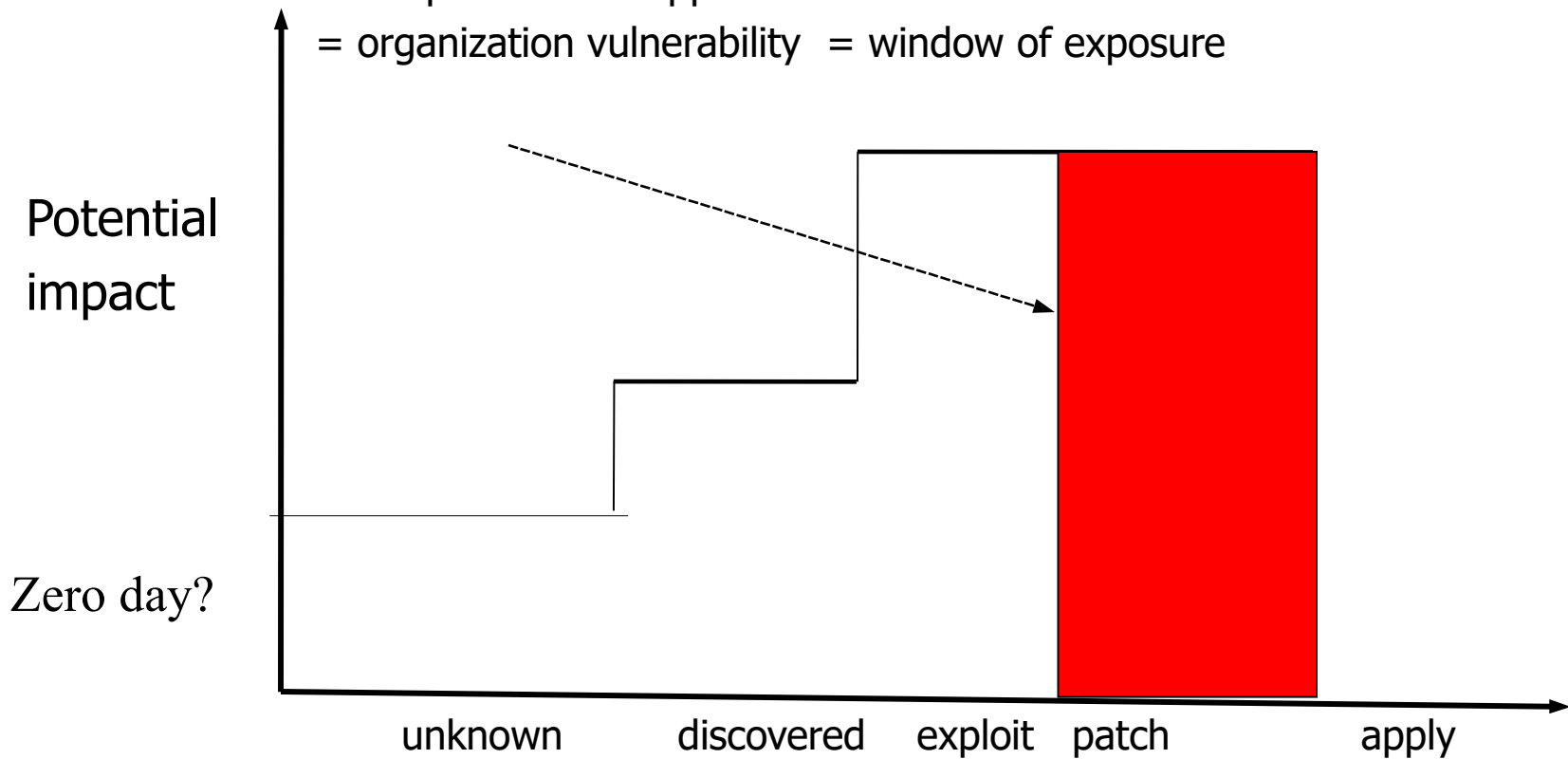


Zero day exploit

- An exploit for a vulnerability that has been discovered but not disclosed to all the users
- Sometimes those who discover a vulnerability sell it to those interested in attacking the system (black market of vulnerabilities)
- Can we design a system that resists attacks even when a vulnerability is discovered?

Potential impact of a vulnerability

If the patch is not applied because of the owner
= organization vulnerability = window of exposure





Potential impact

- In the best case, a patch is available before an attack is known
- If the owner does not apply the patch, then any benefit of discovering the patch before the attack is lost
- It is the application of the patch not its definition that reduces the danger

Time to develop a patch

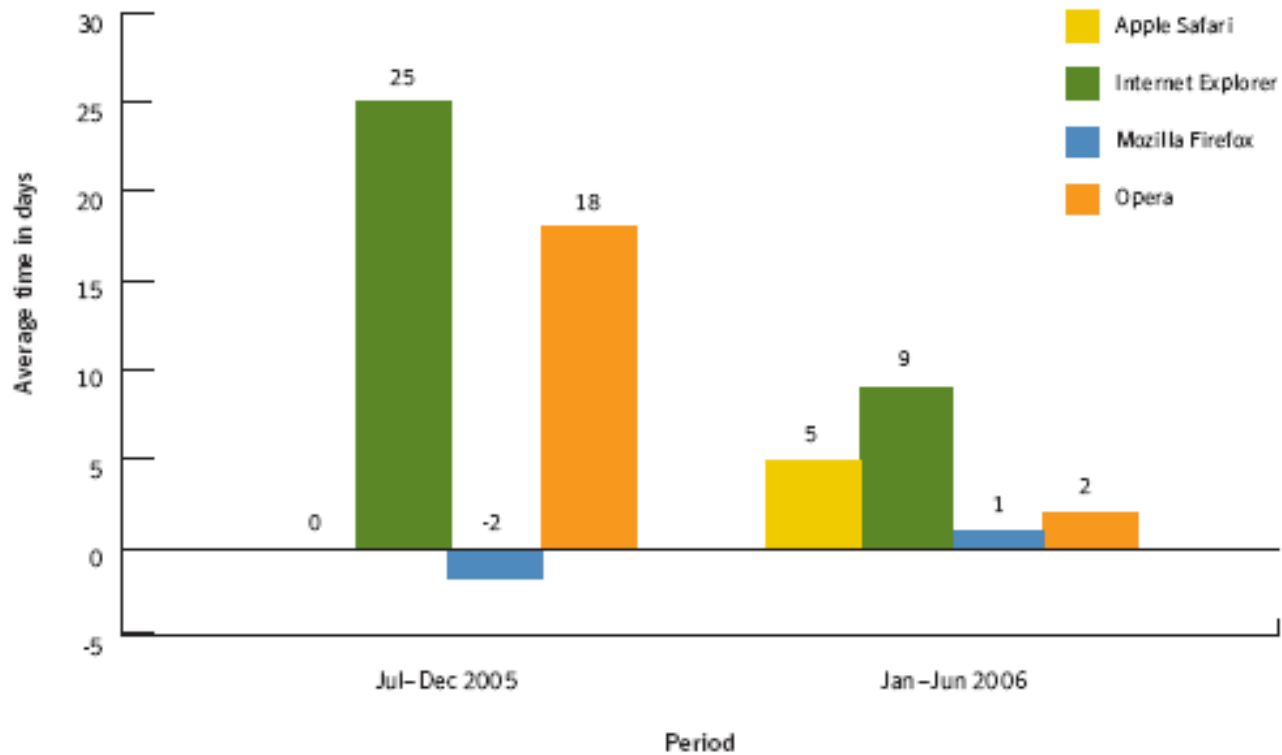
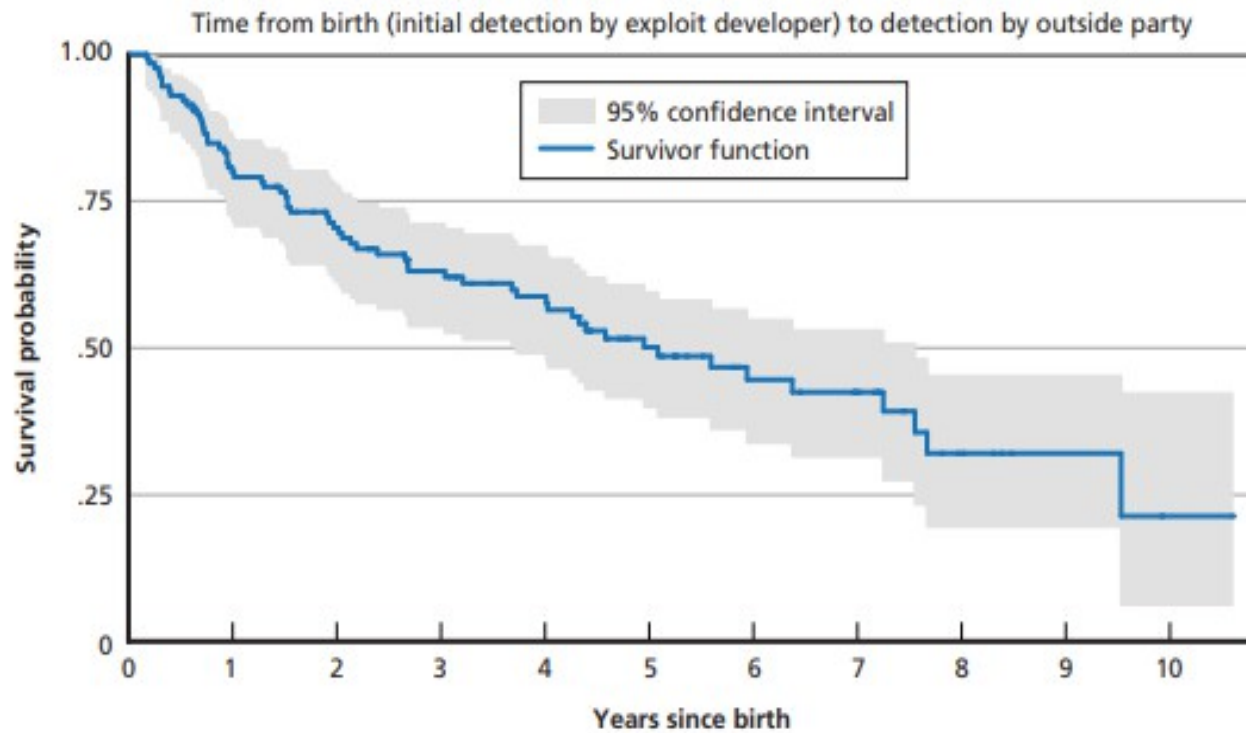


Figure 4. Web browsers window of exposure

Source: Symantec Corporation

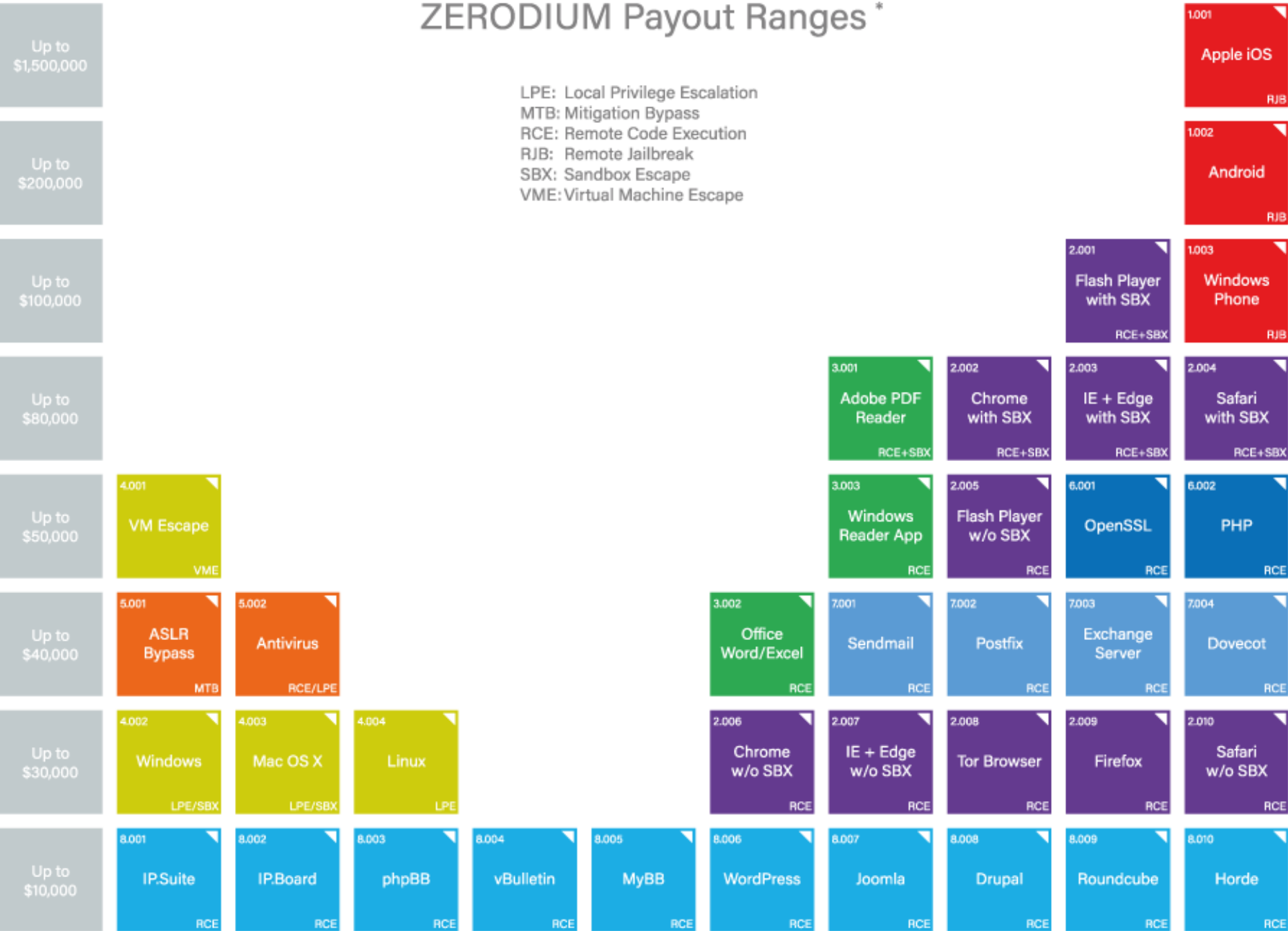
Window of exposure

Kaplan-Meier Survival Probability Estimates (n = 127)



ZERODIUM Payout Ranges *

LPE: Local Privilege Escalation
MTB: Mitigation Bypass
RCE: Remote Code Execution
RJB: Remote Jailbreak
SBX: Sandbox Escape
VME: Virtual Machine Escape



* All payout amounts are chosen at the discretion of ZERODIUM and are subject to change or cancellation without notice.

2016/09 © zerodium.com



Other buyer ...

ADOBE READER	\$5,000-\$30,000
MAC OSX	\$20,000-\$50,000
ANDROID	\$30,000-\$60,000
FLASH OR JAVA BROWSER PLUG-INS	\$40,000-\$100,000
MICROSOFT WORD	\$50,000-\$100,000
WINDOWS	\$60,000-\$120,000
FIREFOX OR SAFARI	\$60,000-\$150,000
CHROME OR INTERNET EXPLORER	\$80,000-\$200,000
IOS	\$100,000-\$250,000



Number of vulnerability vs quality

- The number of vulnerabilities **discovered (= known)** in a module is always lower than **existing ones**
- This number depends upon
 - the availability of the source code
 - the number of applications and of people using the module
 - the expected benefit of an attack against the module
- If a module is scarcely used, very few vulnerabilities are known but this does not imply they do not exist
 - ⇒ The number of disclosed vulnerability cannot be used to evaluate the quality of the module code



Genetic difference

- A system is more robust if it composes components from distinct suppliers
- The joint existence of vulnerabilities and a monopoly in the component supplying can results in several problems because all the instances of a component are affected by the same vulnerabilities
- How much configuration influences vulnerabilities (??!!)



Defence in depth

Any system component can be affected by a vulnerability

- A security expert
 - Does not need to know any vulnerability
 - Can design a system so that the discovery of a vulnerability in a component does not make the whole system useless
 - Layered defence or defence in depth = redundancies and diversities in the controls
- Alternative approach from the application of a patch



Adopted Approach - I

- A solution that tries to anticipate any vulnerability in any component has an huge cost
- Hence some vulnerabilities cannot be anticipated
- According to their potential impact we want to understand which vulnerabilities
 - should be accepted
 - should be anticipated
 - should be patched asap
- Problem: how to classify each vulnerability



Adopted Approach - II

- A vulnerability classification (handling) depends upon the corresponding risk
- Risk
 - 1) Average impact if the vulnerability is successfully exploited
 - 2) Risk of a vulnerability = $F(P_{\text{attsucc}}, \text{Imp})$
- P_{attsucc} = probability of a successful attack
- Imp = impact due to a successful attack



Adopted Approach - III

P_{attsucc} is a function of several parameters

- Threat agents that
 - are interested in implementing the attack
 - have the know how and the resources to implement the attack
- Complexity of the implementation (automated ?)
- Are there other vulnerabilities that can be exploited to reach the same goal?
- Are these attacks more or less complex?



Probability and impact

- A detailed evaluation of the probability an attack is attempted and is successful is extremely complex
 - No historical information available
 - Quick hardware/software evolution
 - Human factor
- Similar problems are faced for the impact because of loss of new clients, damage to the reputation etc



Probability - II

- Sometimes both the success probability and the impact are approximated
{low, medium, high} or
{low, medium-low, medium ...}
- We also need a risk matrix to compute the risk given the approximated input values



Risk Matrix

Prob Impact	VL	L	M	H	VH
VH	H	H	H	VH	VH
H	M	H	H	H	H
M	L	L	M	M	M
L	L	L	L	M	M
VL	VL	L	M	H	VH



A critical problem

- Any probability assumes some information about the past behavior of a system and of attackers
- From this information we can extrapolate the future behavior under a continuity assumption
- A breakthrough in the technology for the attacker or the owner can invalidate the continuity assumption and results in distinct probabilities



Summing Up

- A risk attitude is defined by two parameters
 - Penetrate and patch/Proactive (choose one)
 - Conditional/Unconditional (choose one)
- In penetrate and patch
 - each vulnerability may be critical, in proactive is critical if it has not been anticipated
 - the number of critical vulnerabilities (there is a risk) is much higher than in proactive
- If a vulnerability is critical
 - conditional sec = assess the risk and remove only if
 - there is a non zero risk (Probsucc, Impact)
 - if it is cost effective
 - unconditional security: remove



Evaluating risk with no data

- Current research is focused on risk evaluation even if no data is available
- Solutions exist to produce accurate and realistic data to replace historical one that, in general, is not available or is not public



Risk Based Approach

The formalization of the approach we have described, it includes:

1. Asset analysis
2. Vulnerability Analysis
3. Attack Analysis
4. Threat Analysis
5. Impact Analysis
6. Risk Evaluation
7. Risk Management = which countermeasures are to be adopted

Risk Assessment



Risk Assess & Management

- The most modern approach to ICT security
- It consider the overall risk for an organization and it frames the risk due to ICT system with other risks
- A larger context has to be considered because ICT security should not be seen as a technological problem only



Return on investment ROI

- The security analyst should be able to justify the cost of the countermeasures that are selected to be implemented (deployed)
- A countermeasure should be adopted only for those vulnerabilities that enable attacks that have both/at least one of
 - A large success probability
 - A large impact
 - = they have a large risk
- An interesting debate about **both/at least one**



Return of investment

- It is the difference between
 - The overall risk before the countermeasures
 - The overall risk after the adoption of countermeasures
- The difference arises because decrease the success probability or the impact of an attack
- The case where a vulnerability is removed or patched ($0 =$ success probability) is a particular one



Return of investment=Earning

- It is the difference between the potential impact and the cost of countermeasures
- The difference should be at most zero
- An alternative definition consider the ratio between the ROI and the countermeasure cost
- The ratio should be larger than 1



Next steps

- Asset analysis
- Security policy
- Vulnerability Analysis
- Possible countermeasures
- Attack Analysis
- Risk Management = countermeasure selection



Next Steps - II

- In principle, the security policy is a countermeasure
- In practice, it is defined independently of, and before, risk assessment because it defines the goals of an organization and the rules for its ICT resources
- Its satisfaction is an assessment goal
- Without a policy you do not know if you are secure