Exploiting Software Vulnerabilities

Vulnerability Management and Assessment

Universidad Zaragoza

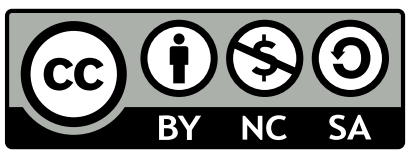
Dept. of Computer Science and Systems Engineering
University of Zaragoza, Spain

Course 2022/2023

Master's Degree in Informatics Engineering

University of Zaragoza

Seminar A.22, Ada Byron building



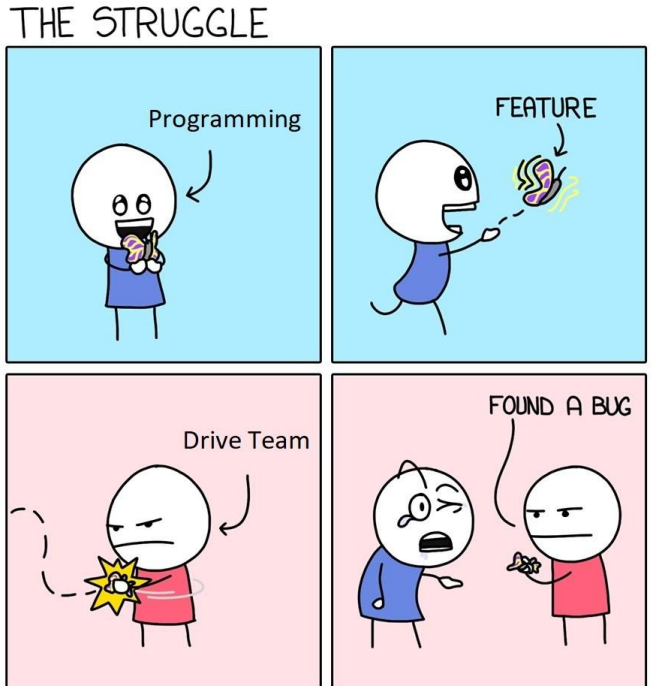
Outline

Universidad Zaragoza

Outline

Universidad Zaragoza

Introduction



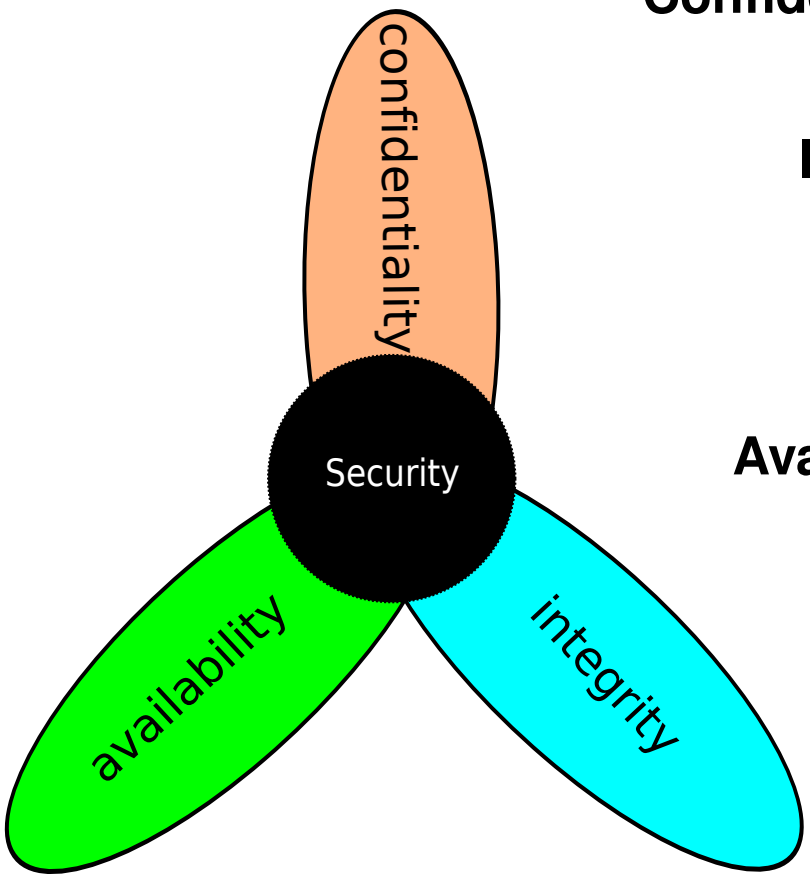
Definition of vulnerability

- **Software or design flaw**
- **Allows an intruder to reduce the security of information on a system**
- **Requirements**:
  - A weakness in the system
  - An adversary's access to that weakness
  - Ability of the adversary to exploit the weakness using a tool or a technique

Credits: https://www.reddit.com/r/FRC/comments/ay7tri/its_not_a_bug_its_a_feature/

Introduction

The CIA triad of infosec



Confidentiality *Information is not accessed by unauthorized persons*

Integrity *Information is not altered by unauthorized persons in an undetectable way by authorized users*

Availability *Reliable (and timely) access and use of information, while preventing unauthorized retention of information*

- **Other attributes**: authenticity, authorization, accountability, non-repudiation/anonymity

Universidad Zaragoza

Introduction

Security challenges

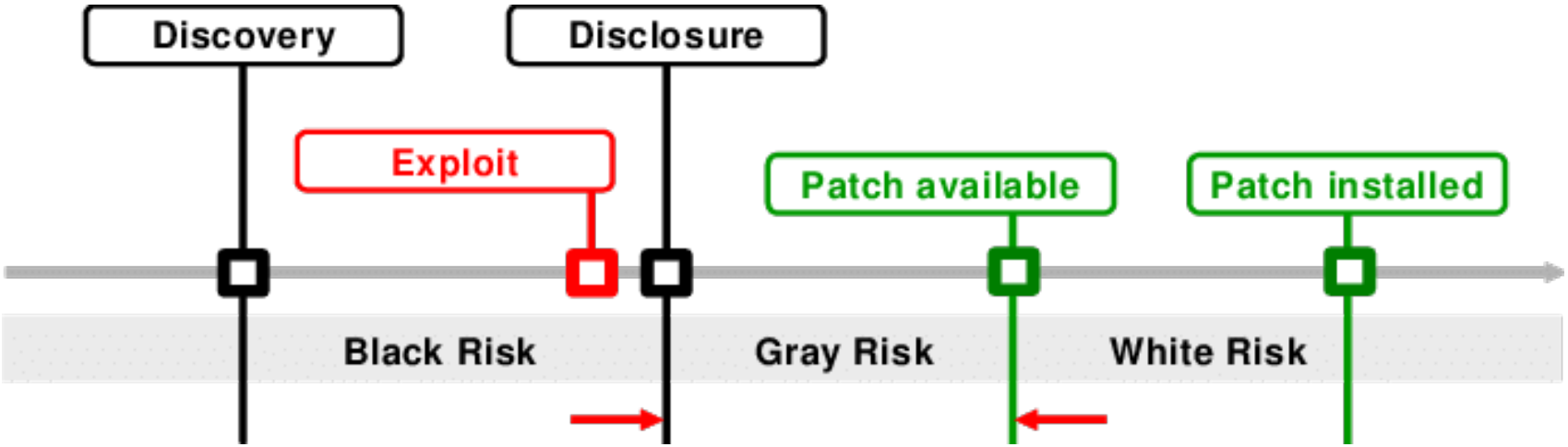
- **Lack of security awareness**
- **Sophistication of attack tools and methodologies**
  - Little or no knowledge or skills are required to carry out some attacks
  - Script-kiddies – *hackers de botón gordo*
- **Complexity of the systems**
- **Growth of interconnected and heterogeneous devices** (e.g., IoT)
- **Lack of vulnerability/patch management processes**

There is **ALWAYS** a trade-off between security and usability

Universidad Zaragoza

Introduction

Life-cycle of a vulnerability



Zero-day vulnerability (0-day)

- **Unknown to the software vendor (and to the public) until disclosed**

Credits: *0-Day Patch Exposing Vendors (In)security Performance*, S. Frei, B. Tellenbach, B. Plattner, BlackHat EU 2008

Universidad Zaragoza

Introduction

Bug bounty programs

Get a bug if you find a bug.

Show us a bug in our VRTX® real-time operating system and we'll return the favor. With a bug of your own to show off in your driveway.

There's a catch, though.

Since VRTX is the only microprocessor operating system completely sealed in silicon, finding a bug won't be easy.

Because along with task management and communication, memory management, and character I/O, VRTX contains over 100,000 man-hours of design and testing.

And since it's delivered in 4K bytes of ROM, VRTX will perform for you the way it's performing in hundreds of real-time applications from avionics to video games.

Bug free.

So, to save up to 12 months of development time, and maybe save a loveable little car from the junkyard, contact us. Call (415) 326-2950, or write Hunter & Ready, Inc., 445 Sherman Avenue, Palo Alto, California 94306.

Describe your application and the microprocessors you're using—Z8000, Z80, 68000, or 8086 family. We'll send you a VRTX evaluation package, including timings for system calls and interrupts. And when you order a VRTX system for your application, we'll include instructions for reporting errors.*

But don't feel bad if in a year from now there isn't a bug in your driveway.

There isn't one in your operating system either.

HUNTER ◆ READY

VRTX

Operating Systems in Silicon.

*Call or write for details. But, considering our taste in cars, you might want to accept our offer of $1,000 cash instead. © 1983 Hunter & Ready, Inc.

Further reading: *Bounties Mount for Bugs*, P. Marks, Communications of the ACM, Aug 2018.

Introduction

Types of vulnerability disclosures

- **Non-disclosure**
  - **Keep the vulnerability a secret** instead of contacting the software vendor or a computer security coordinating authority
  - **The number of undisclosed vulnerabilities is unknown**

Introduction

Types of vulnerability disclosures

- **Non-disclosure**
  - **Keep the vulnerability a secret** instead of contacting the software vendor or a computer security coordinating authority
  - **The number of undisclosed vulnerabilities is unknown**
- **Full disclosure**
  - **Inform the community at large**, without first checking with the software vendor
  - **Minimal documentation**: how found, software products (with versions) affected, and how to exploit or mitigate it
  - **Controversial method**
    - Rapid acknowledgement and patch of software vendors
    - Increase the risk of widespread exploitation

Universidad Zaragoza

Introduction

Types of vulnerability disclosures

- **Non-disclosure**
  - **Keep the vulnerability a secret** instead of contacting the software vendor or a computer security coordinating authority
  - **The number of undisclosed vulnerabilities is unknown**
- **Full disclosure**
  - **Inform the community at large**, without first checking with the software vendor
  - **Minimal documentation**: how found, software products (with versions) affected, and how to exploit or mitigate it
  - **Controversial method**
    - Rapid acknowledgement and patch of software vendors
    - Increase the risk of widespread exploitation
- **Responsible disclosure** (aka partial/limited disclosure)
  - Usually accompanied by a **test suite to verify that future releases do not contain similar bugs**
  - **Inform software vendor and wait for a response** (depends on their disclosure policy)
  - **If no response, go to full disclosure**

Universidad Zaragoza

What I have to do?

- **Contact a CERT/CC or the software vendor involved**
  - CERT/CC stands for Computer Emergency Response Team/Coordination Center
  - There are many CERTs (all countries and large organizations have one)
  - **Software vendors now provide direct communication with their security teams** to handle vulnerability discoveries
  - **Each CERT/vendor may have different disclosure policies**
  - **Industrial systems usually have special disclosure processes**, due to their critical activity (e.g., `https://www.cisa.gov/coordinated-vulnerability-disclosure-process`)

Introduction

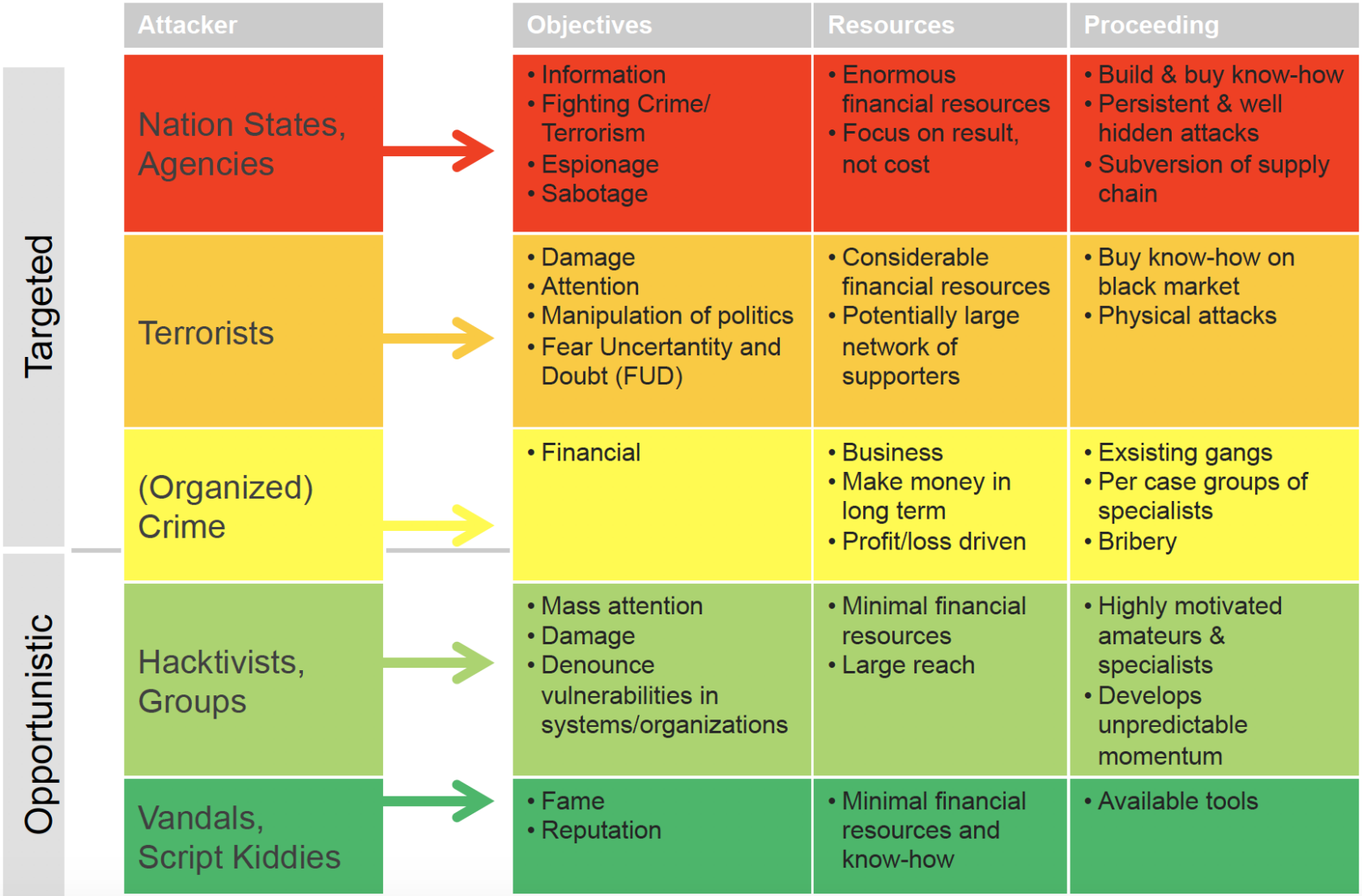
What I have to do?

- **Contact a CERT/CC or the software vendor involved**
  - CERT/CC stands for Computer Emergency Response Team/Coordination Center
  - There are many CERTs (all countries and large organizations have one)
  - **Software vendors now provide direct communication with their security teams** to handle vulnerability discoveries
  - **Each CERT/vendor may have different disclosure policies**
  - **Industrial systems usually have special disclosure processes**, due to their critical activity (e.g., `https://www.cisa.gov/coordinated-vulnerability-disclosure-process`)
- **Get a CVE** (Common Vulnerabilities and Exposures)
  - MITRE, ZDI, etc
  - Known syntax: CVE-YYYY-ID
    - *Example*: Zerologon vulnerability `https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1472`
  - **Useful to unequivocally identify a vulnerability**

Universidad Zaragoza

Introduction

Actors and attackers



Credits: *(IN)SECURITY, RISK & THE LIFECYCLE OF VULNERABILITIES*, Dr. Stefan Frei, ETH

Introduction

Adversaries / attackers

- **Hacktivists**
  - **Individuals or groups of hackers**
  - Main motivation: **promoting a political agenda, a religious belief, or a social ideology**
- **Internal threats** (insiders)
  - **Current or former (upset) employees**. It can also arise from third parties (contractors, temporary workers, clients)
  - Different types: malicious, accidental, negligent
  - Main motivation (of malicious insiders): **money, espionage, gain strategic advantage**
  - *Examples*: (taken from `https://www.varonis.com/blog/insider-threats/`)
    - On Tesla, a malicious insider sabotaged systems and sent proprietary data to third parties
    - On Facebook, a security engineer abused his access to harass women
    - On Coca-Cola, a malicious insider stole a hard drive full of worker's personal data
    - On Suntrust Bank, a malicious insider stole personal data (including account information) for 1.5M customers and provided it to a criminal organization

Universidad Zaragoza 1542

Introduction

Adversaries / attackers

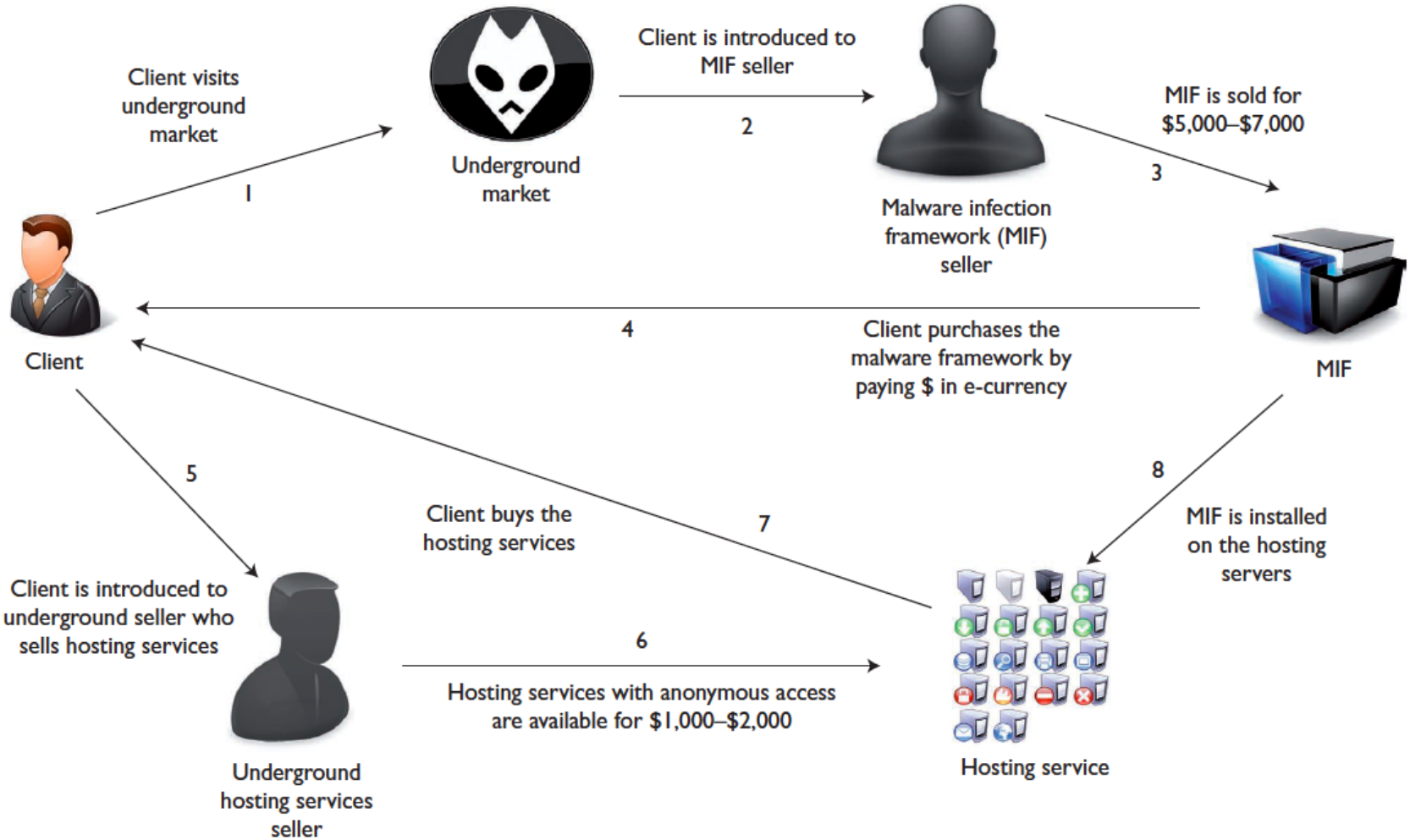
- **Cyber criminals** – *the traditional mob moves to the digital world*
  - **Individuals or groups of people who use technology to commit cybercrimes**
  - Main motivation: **generate profits by different means** (stealing confidential company or personal data, sabotage, scam, etc.)
  - **The most prominent and active type of attacker**
- **State-sponsored attackers**
  - Individuals or groups of people who have **particular objectives aligned with the political, commercial or military interests of their country of origin**
  - **Highly trained hackers**, specialized in detecting and exploiting vulnerabilities
  - **Most dangerous attacker**: no resource limit

Universidad Zaragoza

Further reading: *Cyber Guerilla*, Jelle van Haaster, Rickey Gevers and Martijn Sprengers, Syngress, 2016

Introduction

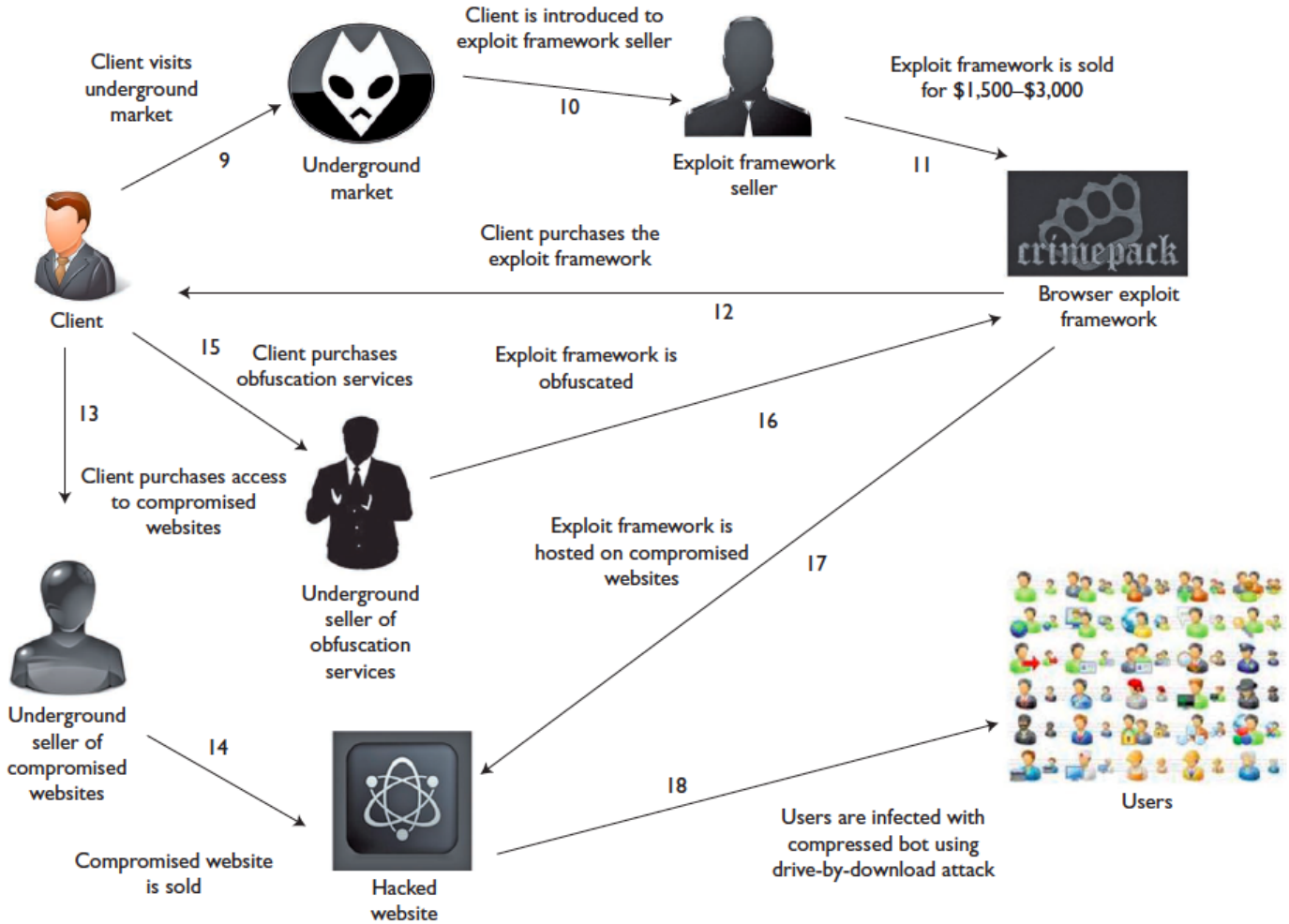
Cybercrime lifecycle – cycle 1



Credits: Sood, A. K.; Bansal, R. & Enbody, R. J. *Cybercrime: Dissecting the State of Underground Enterprise*. IEEE Internet Computing, 2013, 17, 60–68.

Introduction

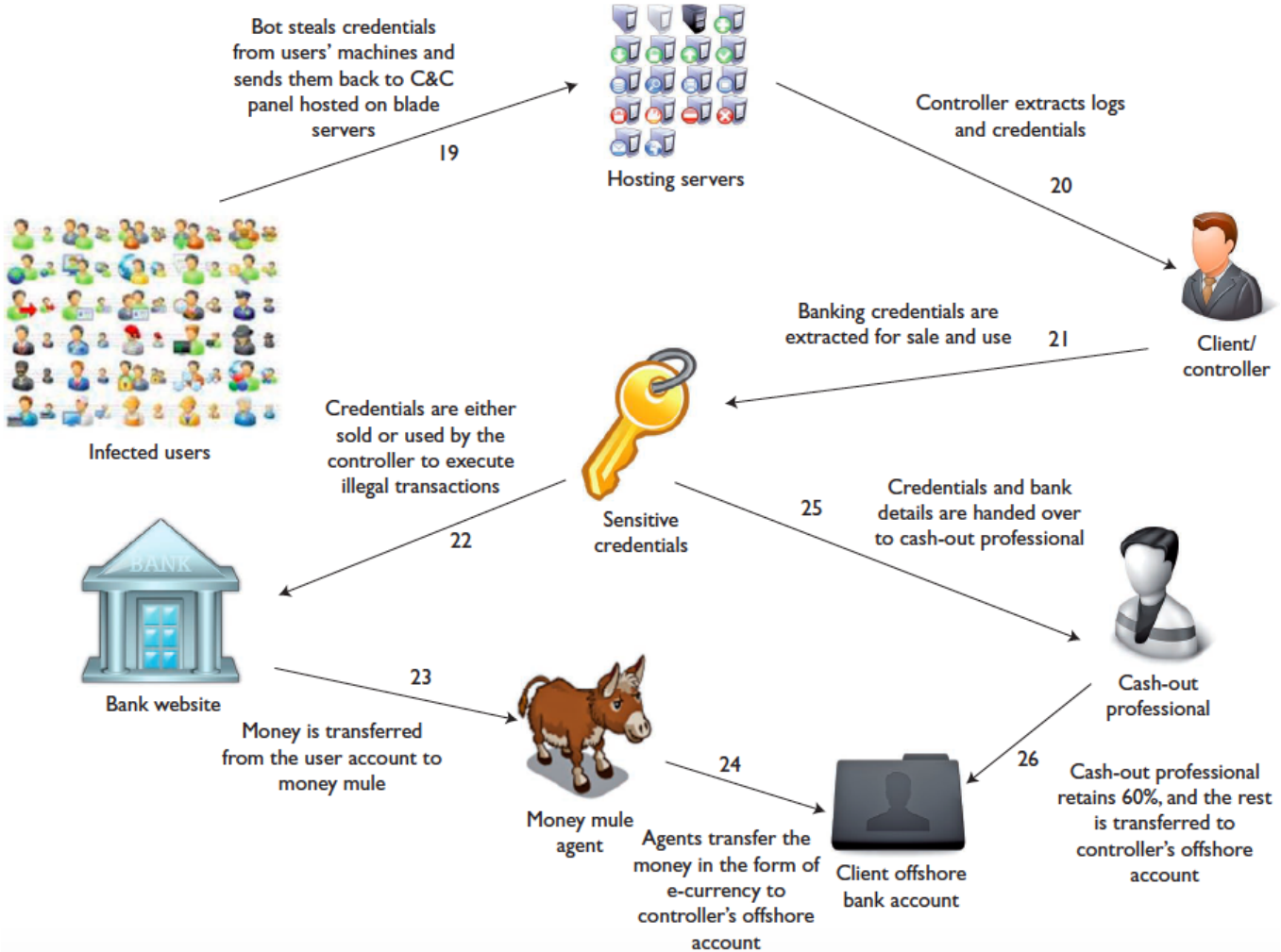
Cybercrime lifecycle – cycle 2



Credits: Sood, A. K.; Bansal, R. & Enbody, R. J. *Cybercrime: Dissecting the State of Underground Enterprise*. IEEE Internet Computing, 2013, 17, 60–68.

Introduction

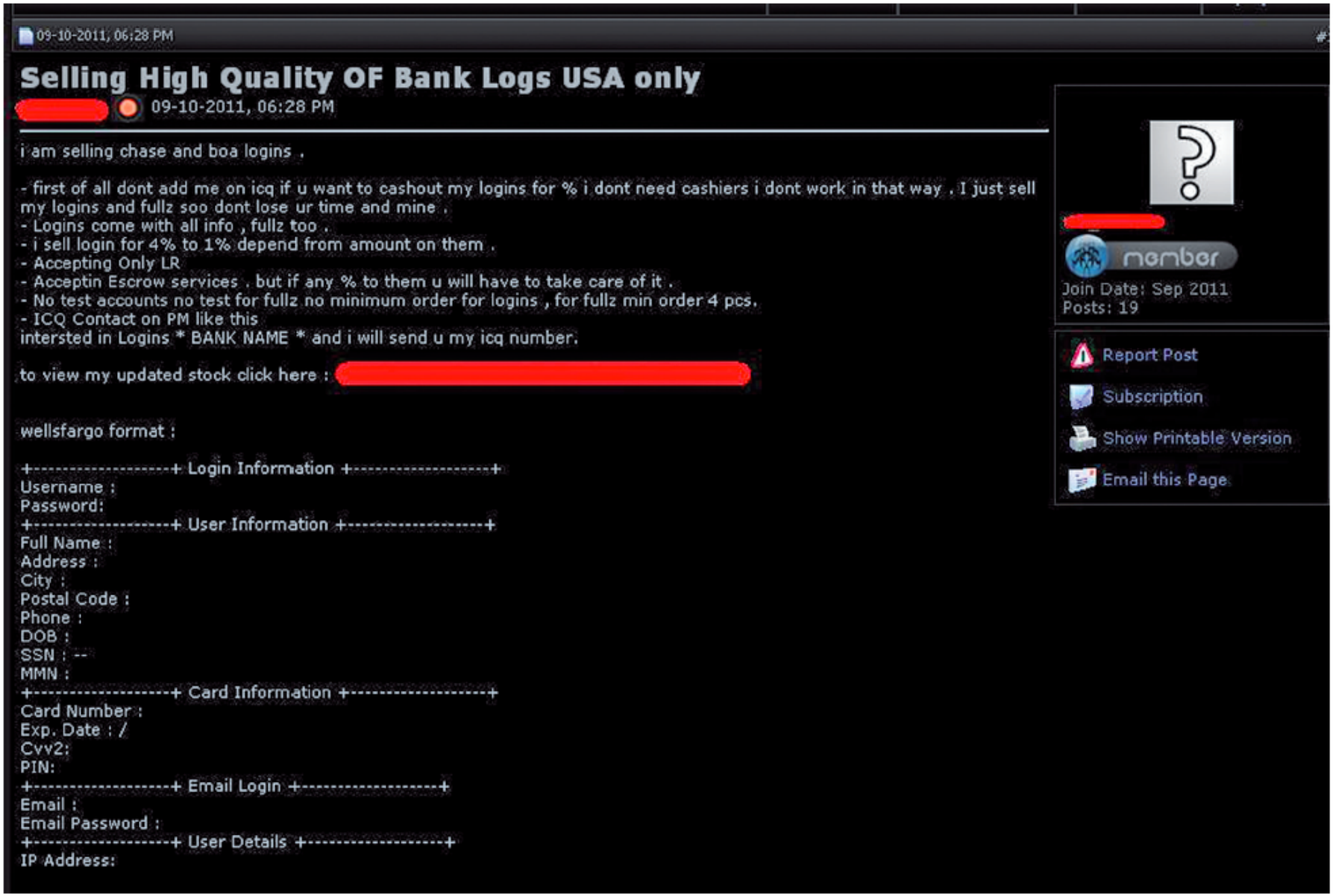
Cybercrime lifecycle – cycle 3



Credits: Sood, A. K.; Bansal, R. & Enbody, R. J. *Cybercrime: Dissecting the State of Underground Enterprise*. IEEE Internet Computing, 2013, 17, 60–68.

Introduction

Some examples about the underground market



09-10-2011, 06:28 PM

Selling High Quality OF Bank Logs USA only

[redacted] 09-10-2011, 06:28 PM

i am selling chase and boa logins .

- first of all dont add me on icq if u want to cashout my logins for % i dont need cashiers i dont work in that way . I just sell my logins and fullz soo dont lose ur time and mine .
- Logins come with all info , fullz too .
- i sell login for 4% to 1% depend from amount on them .
- Accepting Only LR
- Acceptin Escrow services . but if any % to them u will have to take care of it .
- No test accounts no test for fullz no minimum order for logins , for fullz min order 4 pcs.
- ICQ Contact on PM like this

intersted in Logins * BANK NAME * and i will send u my icq number.

to view my updated stock click here : [redacted]

wellsfargo format :

+----------+ Login Information +----------+
Username :
Password:
+----------+ User Information +----------+
Full Name :
Address :
City :
Postal Code :
Phone :
DOB :
SSN : --
MMN :
+----------+ Card Information +----------+
Card Number :
Exp. Date : /
Cvv2:
PIN:
+----------+ Email Login +----------+
Email :
Email Password :
+----------+ User Details +----------+
IP Address:

[redacted]
member
Join Date: Sep 2011
Posts: 19

Report Post
Subscription
Show Printable Version
Email this Page

Introduction

Some examples about the underground market

Experts at BitDefender have discovered a Cryptolocker/Cryptowall Ransomware Kit offered for sale at $3,000, source code included.

Yesterday I wrote about a new Ransomware-as-a-service, the FAKBEN, surfaced from the criminal underground, requesting customers 10 percent profit cut. In the previous days I reported other cases involving ransomware, such as a malicious code that infected the UK Parliament, an off-line ransomware and a Linux.Encoder1 ransomware revealing the decryption key.

The cybercrime is looking with increasing interest to ransomware, today I want to write about the availability of the source code of Cryptolocker/Cryptowall in the underground.

According to Bitdefender, a Cryptolocker/Cryptowall Ransomware Kit is offered for sale for $3,000, including its source code.

Universidad Zaragoza

Credits: http://securityaffairs.co/wordpress/41977/cyber-crime/ransomware-kit-for-sale.html

Introduction

Some examples about the underground market

HOSTMAN Ransomware

Price: Basic – USD 9.95(Limited use) Big – USD 49.95(Unlimited use)

Ransomware Affiliate Network

Price: FREE

Profits: 25/75 Split, 25% - Ransomware Author 75% - Affiliate

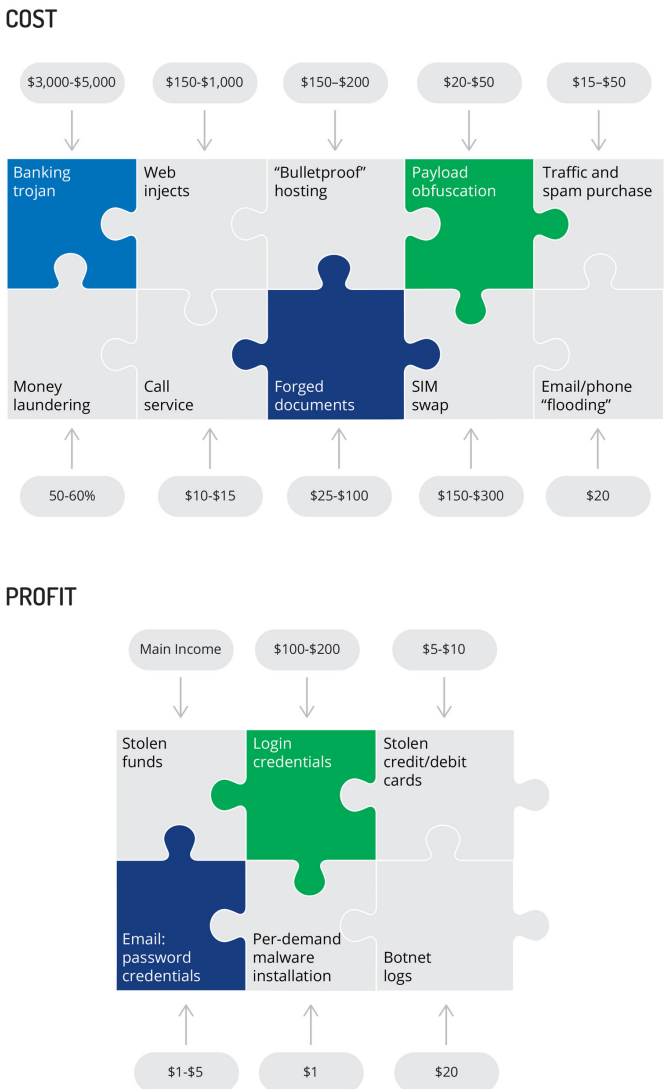
For 100,000+ installations per month:

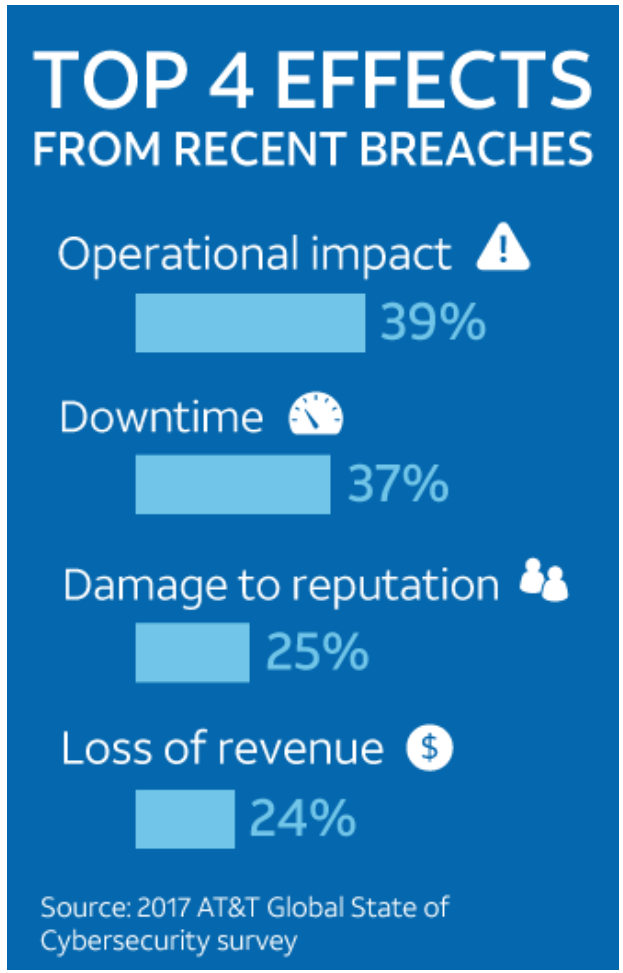
15/85 Split, 15% - Ransomware Author 85% - Affiliate

Credits: https://blog.fortinet.com/

Introduction

Estimating the costs and benefits of cybercrime (2017)

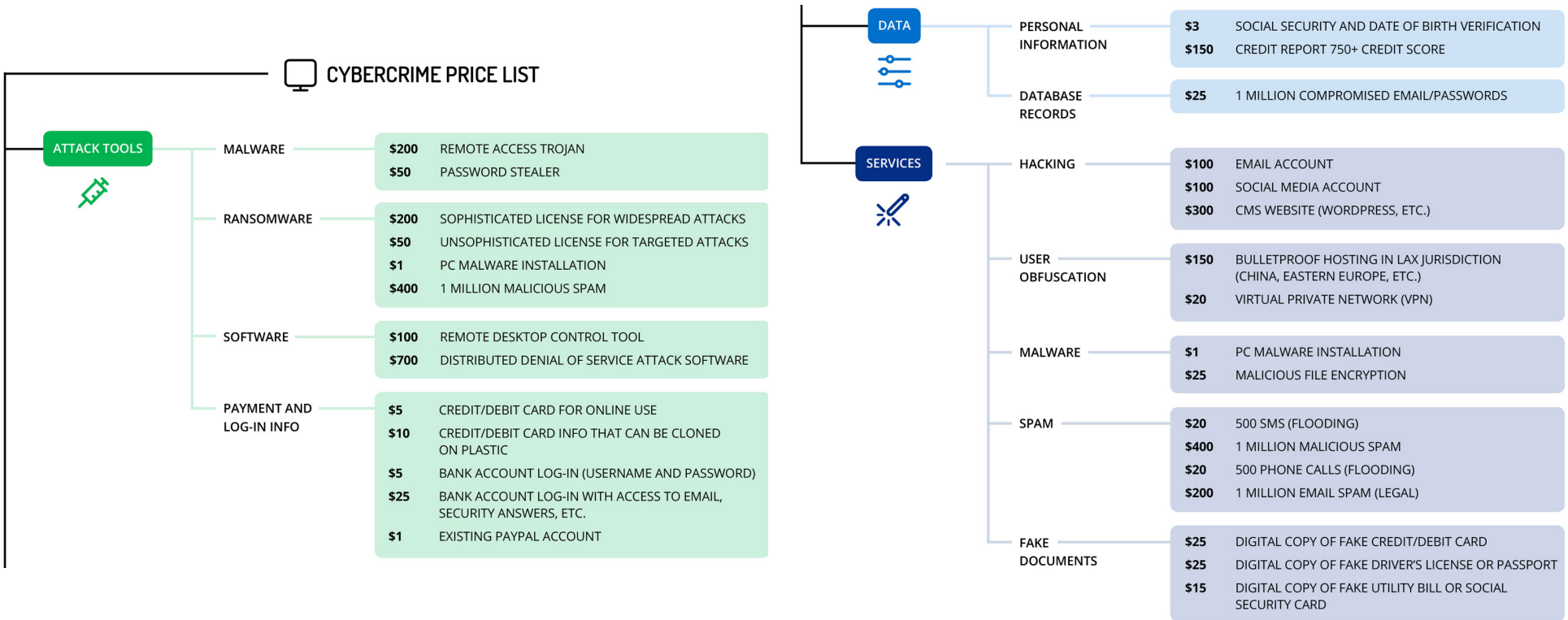




Credits: `https://www.recordedfuture.com/cyber-operations-cost/`

Introduction

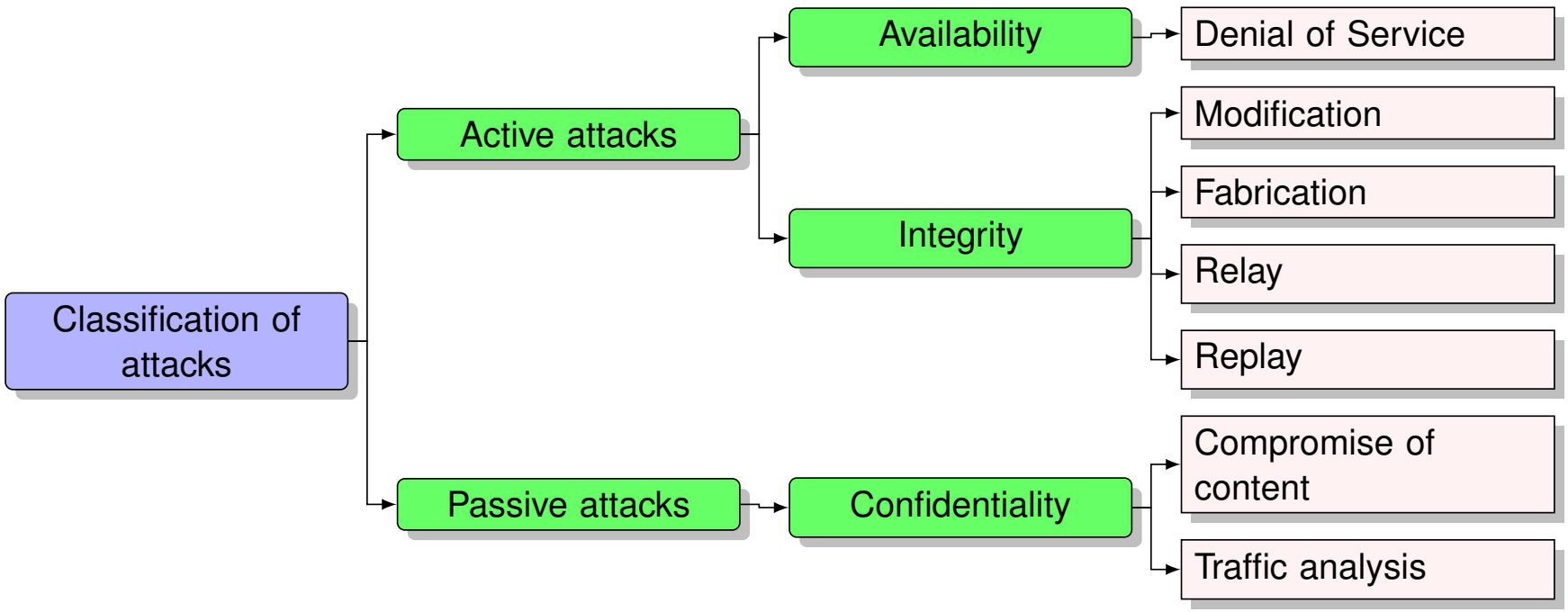
Let's go shopping, folks! (2017)



Credits: `https://www.recordedfuture.com/cyber-operations-cost/`

Introduction

Classification of attacks



Credits: adapted from *(IN)SECURITY, RISK & THE LIFECYCLE OF VULNERABILITIES*, Dr. Stefan Frei, ETH

Outline

Universidad Zaragoza

Ethical concerns

Vulnerability research

- *Some concerns...*
  - We are testing systems and analyzing products created and maintained by someone else
  - **But we help others to prevent or mitigate damage to third parties due to vulnerable products and operations...**

Universidad Zaragoza

Ethical concerns

Vulnerability research

- *Some concerns...*
  - We are testing systems and analyzing products created and maintained by someone else
  - **But we help others to prevent or mitigate damage to third parties due to vulnerable products and operations...**
- *What about legality?*
  - State and federal computer intrusion statutes or intellectual property rights are violated
  - **But vulnerability research helps us anticipate the problems...**
  - When the disclosure is legally mandated, irreparable damage has generally occurred

Universidad Zaragoza
1542

Ethical concerns

Code of conduct

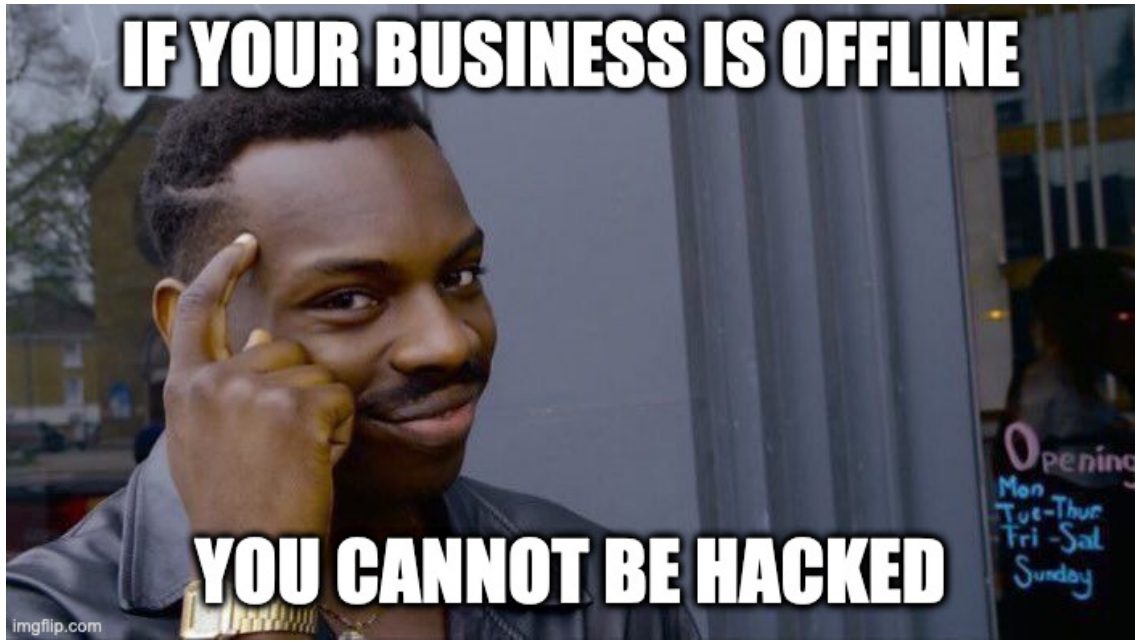
- **Duty not to harm**
- *Before starting your research...*
  - **Reveal intent and investigation**
  - **Seek legal advice**
- *During and after your research...*
  - **Responsible data handling**
  - **Report serious vulnerabilities**

Universidad Zaragoza

Outline

Universidad Zaragoza

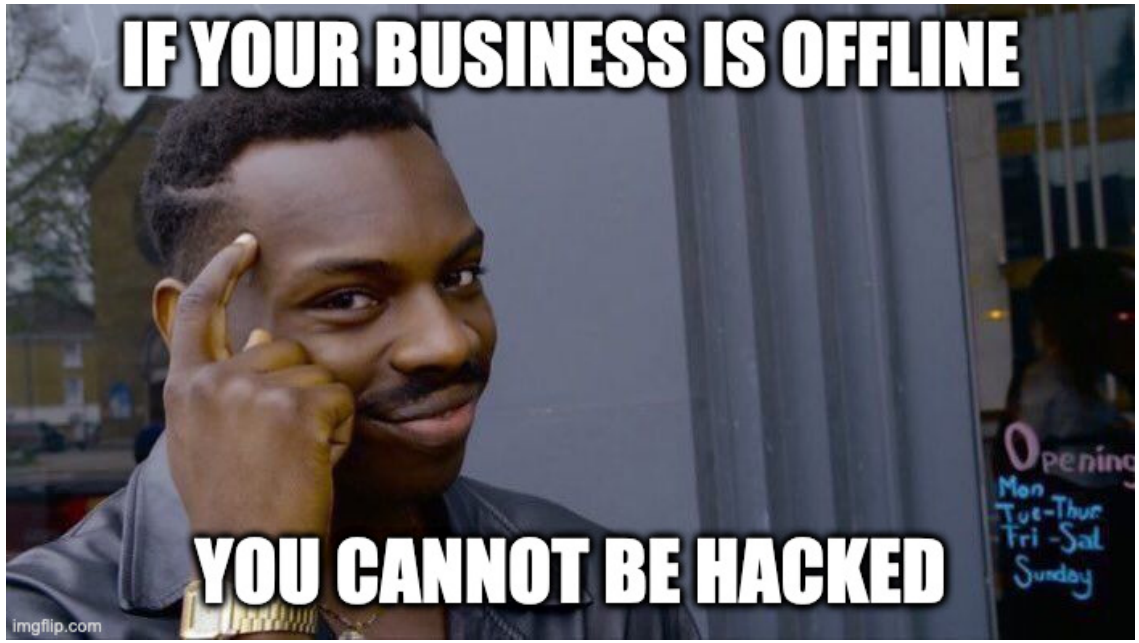
Vulnerability Management and Assessment



Absolute security does not exist

- **There are always trade-offs**: usability, social, financial, etc...
- TAKE-HOME MESSAGE: **the correct security metric is RONI** (Return Of Non Investment)
  - You cannot calculate the return on your security spending, but you can calculate your loss from not investing in security after an incident occurs

Vulnerability Management and Assessment



Absolute security does not exist

- **There are always trade-offs**: usability, social, financial, etc...
- TAKE-HOME MESSAGE: **the correct security metric is RONI** (Return Of Non Investment)
  - You cannot calculate the return on your security spending, but you can calculate your loss from not investing in security after an incident occurs

What are you willing to give up to get the level of security that you want?

- **Vulnerability management helps make decisions**

Universidad Zaragoza

Vulnerability Management and Assessment

Vulnerability management

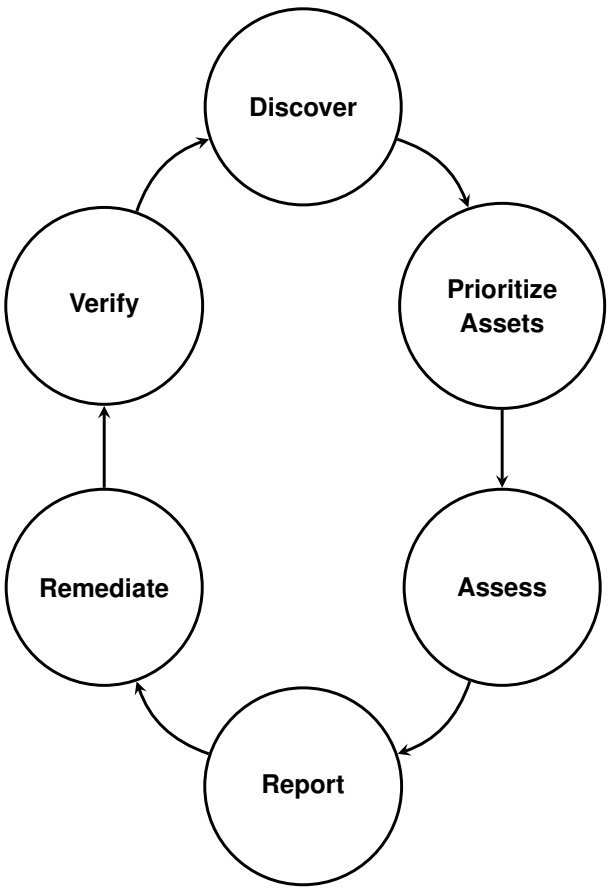
- **Identification of vulnerabilities in systems**
- **Assessment of risks associated with these vulnerabilities**

Universidad Zaragoza

Vulnerability Management and Assessment

Vulnerability management

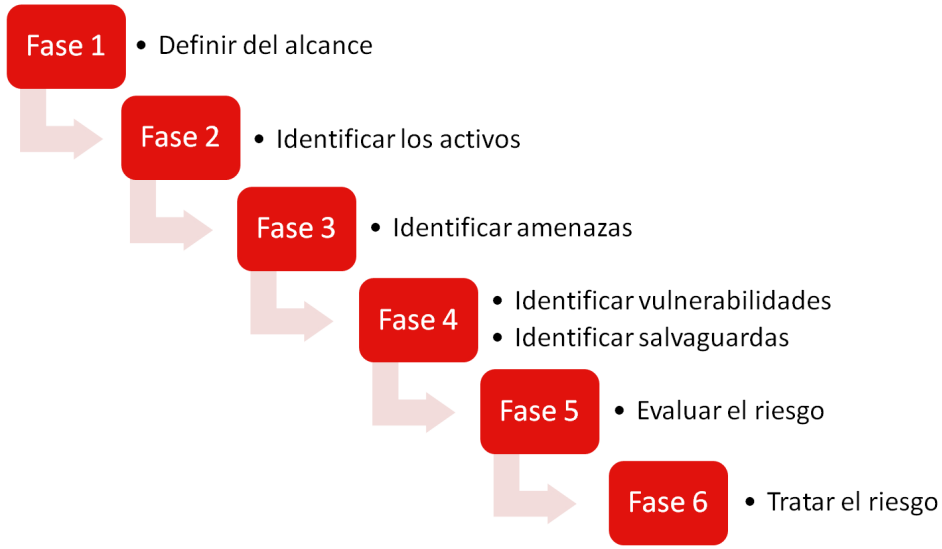
- **Identification of vulnerabilities in systems**
- **Assessment of risks associated with these vulnerabilities**



- **Discover**: inventory all assets and identify vulnerabilities
- **Prioritize assets**: categorize assets into groups, assigning a value based on their importance for the operation of your business
- **Assess**: determine a baseline risk profile
- **Report**: measure the level of risk associated with assets, in accordance with the current security policies
- **Remediate**: prioritize and fix vulnerabilities
- **Verify**: audit the system to verify that threats no longer exist

Vulnerability Management and Assessment

Risk analysis process



- **Identify threats**. The use of standard methodologies such as MAGERIT v3 can help (see `https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html`)
- **Manage risk**. Four possibilities:
  - *Transferring the risk to a third-party* (i.e., buying an insurance)
  - *Avoid the risk*
  - *Accept risk* (be careful with this)
  - *Mitigate (decrease) risk*

Credits: `https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo`

Universidad Zaragoza

Vulnerability Management and Assessment

Vulnerability assessment

- **Systematic review of security weaknesses in a system**
- **Assessing the system for known vulnerabilities, prioritizing them, and recommending action** (remediation, mitigation, avoidance)

Vulnerability Management and Assessment

Vulnerability assessment

- **Systematic review of security weaknesses in a system**
- **Assessing the system for known vulnerabilities, prioritizing them, and recommending action** (remediation, mitigation, avoidance)

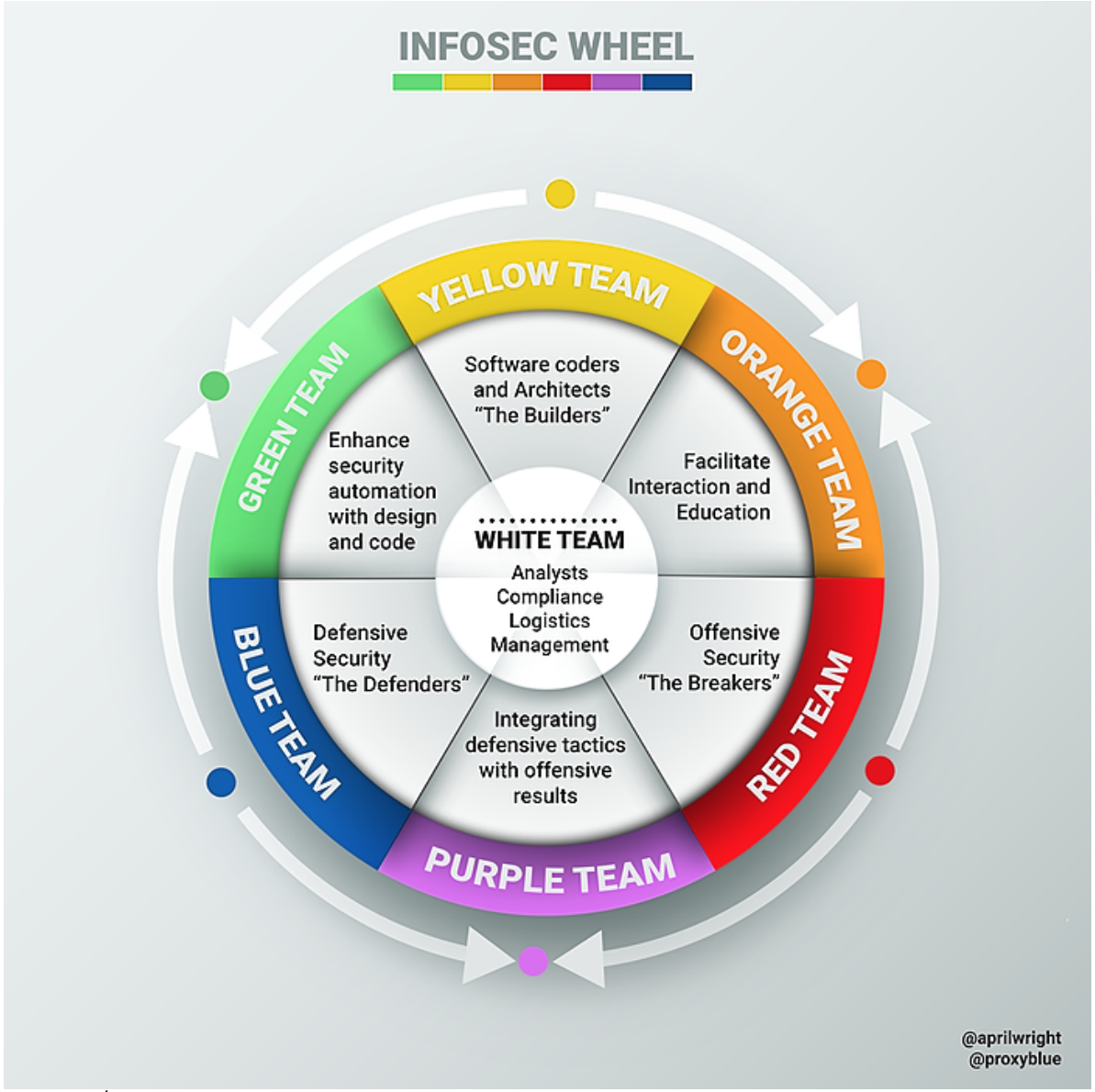
Types of assessments

- **External analysis**: focused on components accessible to external users
- **Internal scans**: any system component on the internal network (not exposed to external users)
- **Environmental scans**: focused on specific operational technologies used by the organization (e.g., cloud services, mobile devices, etc.)

Universidad Zaragoza

Vulnerability Management and Assessment

Red, blue, and... even purple?



Credits: https://hackernoon.com/

Vulnerability Management and Assessment

Vulnerability assessment reports

- **The shorter, the better: it will be straight to the point**
- Aimed at the management and security staff of an organization
- **Common structure**:
  - Executive summary
  - Introduction: scope, extent and limitations
  - Laws, regulations, and policies
  - Identification of assets
  - Threat assessment
  - Audit process
  - Summary

Universidad Zaragoza

Outline

Universidad Zaragoza

Vulnerability Metrics

Common Vulnerability Scoring System (CVSS)

- **Metric to assess the criticality of vulnerabilities**
- Recognized and tested internationally for years
- **Three groups of metrics**
  - **Base Metric Group**
  - **Temporal Metric Group**
  - **Environmental Metric Group**
- **Proposed by FIRST**
  - "[Joint] incident response and security teams from every country across the world to ensure a safe internet for all"
- **Online calculator**: `https://www.first.org/cvss/calculator/3.1`

Universidad Zaragoza

Vulnerability Metrics

CVSS v3.1

Base Score

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)

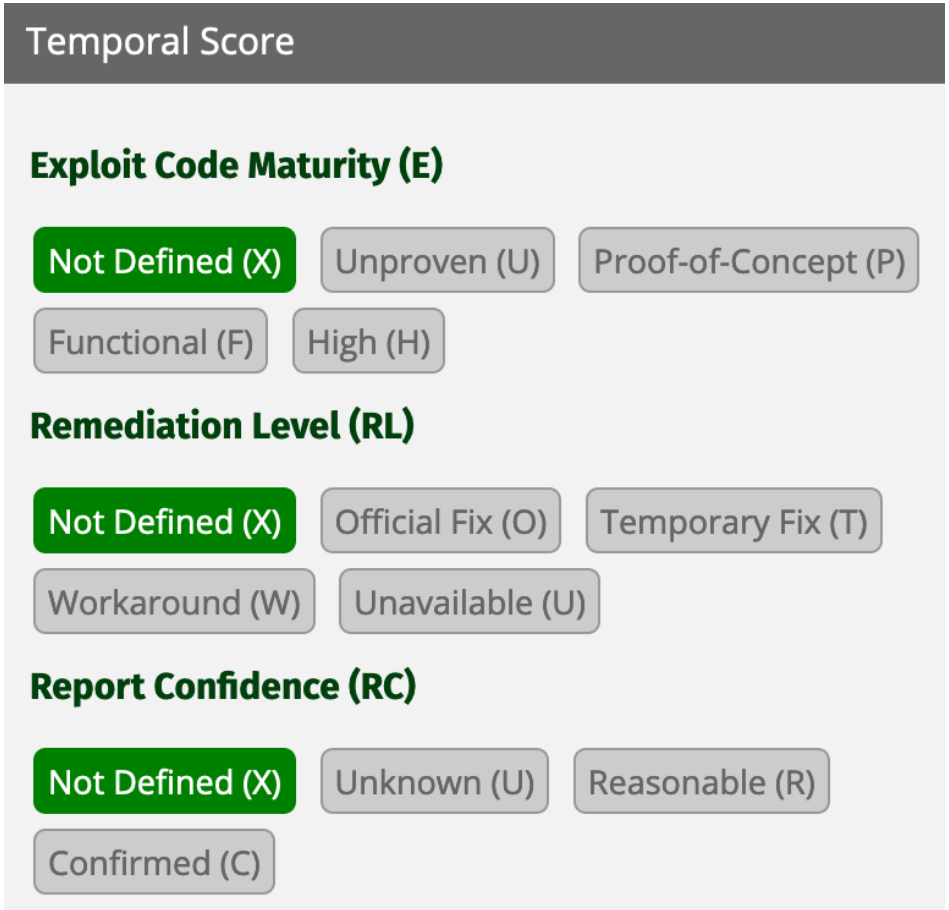
Availability (A)

None (N) | Low (L) | High (H)

Universidad Zaragoza

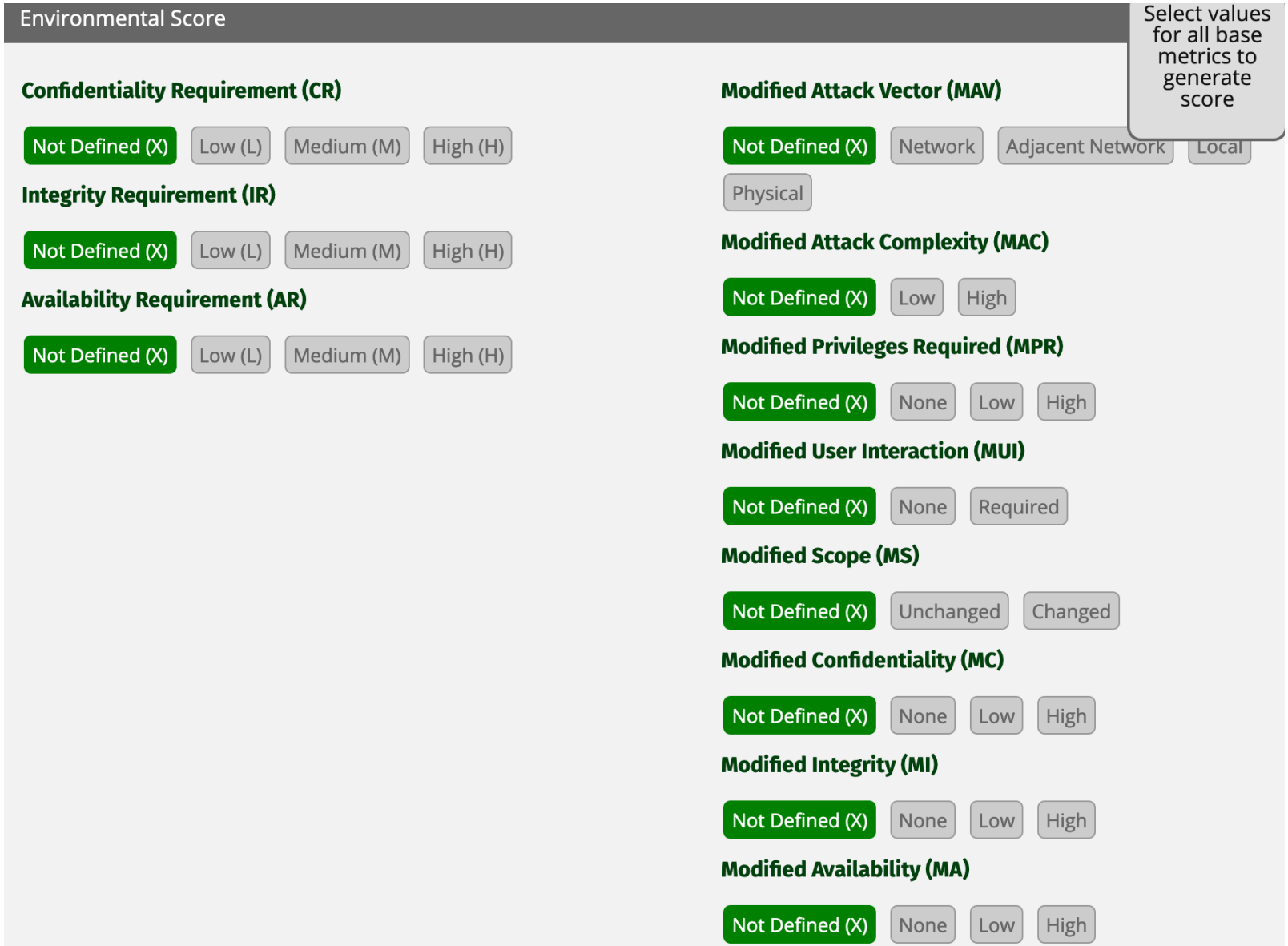
Vulnerability Metrics

CVSS v3.1



Vulnerability Metrics

CVSS v3.1



Universidad Zaragoza

Vulnerability Metrics
CVSS v3.1

- **Qualitative criteria severity rating scale** from version 3.0
- Good for prioritizing vulnerabilities (as part of vulnerability assessment)

Score	Severity
0	None
[0.1, 3.9]	Low
[4.0, 6.9]	Medium
[7.0, 8.9]	High
[9.0, 10]	Critical

Exploiting Software Vulnerabilities

Vulnerability Management and Assessment

Universidad Zaragoza

Dept. of Computer Science and Systems Engineering
University of Zaragoza, Spain

Course 2022/2023

Master's Degree in Informatics Engineering

University of Zaragoza

Seminar A.22, Ada Byron building