Introduction à la Cybersécurité (Inter-Semestre 1A)

Mounira Msahli
https://msahli.telecom-paris.fr/

Telecom Paris, Institut Polytechnique de Paris

6 février 2024

Main References

Rajesh Kumar.
Truth or dare : quantitative security risk analysis via attack trees.
2018.

Dan Boneh and John Mitchell.
Computer and network security.
cs155.stanford.edu.

Massimiliano Albanese, Sushil Jajodia, Anoop Singhal, and Lingyu Wang.
An efficient framework for evaluating the risk of zero-day vulnerabilities.
In *International Conference on E-Business and Telecommunications*, 2013.

Lingyu Wang, Tania Islam, Tao Long, Anoop Singhal, and Sushil Jajodia.
An attack graph-based probabilistic security metric.
In *Data and Applications Security XXII : 22nd Annual IFIP WG 11.3 Working Conference on Data and Applications Security London, UK, July 13-16, 2008 Proceedings 22*.

Ben Thorne.
Using attack graphs to understand vulnerabilities.
2018.

Amit Klein.
More web + attacks.
cs155.stanford.edu.

Dan Boneh.
Unwanted traffic : Denial of service and spam email.
cs155.stanford.edu.

Plan

- Cybersecurity Attacks
- Attack examples
  - Password Attack
  - SQL Injection Attack
  - Cross Site Scripting (XSS) Attack
  - DOS Attack
  - Replay Attack
- Attack Modeling

Learning Outcomes

- Introducing Cybersecurity attacks and how to prevent it
- Understanding of principles of secure design, security goals and attacker capabilities
- It should be mentioned that our objective is not a mere transfer of knowledge but we aim at developing a cognitive learning. In part, the goal is to show how the behaviour of attacker could be predicted and controlled (Ethical Hacking)

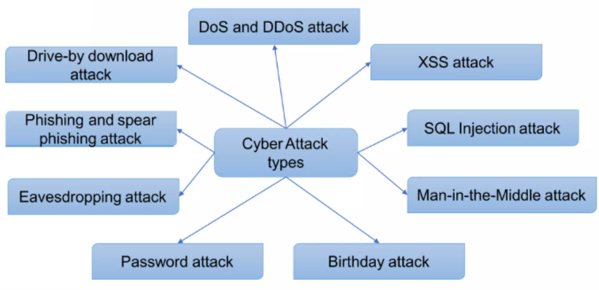
Evaluation et Examen

- Note finale = 100% Contrôle de Connaissance
- Date du contrôle de connaissance : le 09/02/2024 entre 15h :00 et 17h :00
- Cours autorisé, notes de cours autorisées et les appareils électroniques non autorisés

Cybersecurity Attacks

- Active Attack
- Passive Attack
- Black Box Attack
- White Box Attack
- Network, Data, Soft-Ware and Hard-Ware security attacks

Cyber Attack Types



Cyber Attack types

DoS and DDoS attack

XSS attack

SQL Injection attack

Man-in-the-Middle attack

Birthday attack

Password attack

Eavesdropping attack

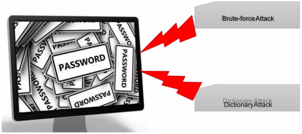
Phishing and spear phishing attack

Drive-by download attack

Password Attack

Password Attack

Brute-Force Scenario



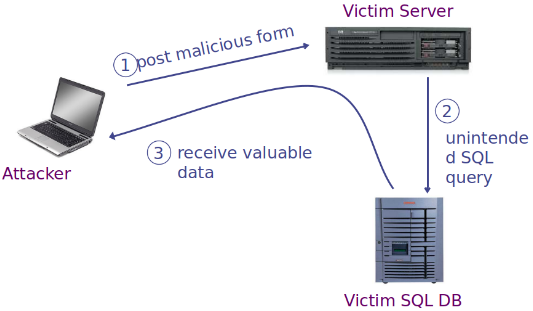
Brute-Force Attack

In cryptography, a brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found.

SQL Injection

SQL Injection : SQLI

SQL injection Scenario



SQL injection Attack

SQL injection is a code injection technique used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).

SQL Injection Examples : The Worst Attacks Ever

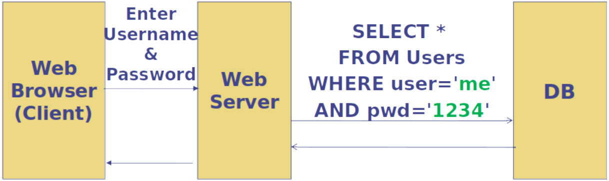
Heartland Payment Systems	2008	Compromised 130 million credit and debit card numbers	Two Russian hackers who installed malware on their systems
Sony Pictures	2011	Leak of thousands of confidential documents emails and unreleased films	Cody Kretsinger, 23 ans, student of Phoenix
Yahoo !	2012	breach of 450,000 Yahoo user credentials	The D33Ds Company

SQL Injection Examples : The Worst Attacks Ever

TalkTalk	2015	157,000 customers' details accessed, including bank account numbers	10 hackers involved
Estonian Central Health Database	2020	compromised the health records of nearly all of Estonia's citizens	
Drupal	2014	An SQL Injection attack vulnerability that affected millions of websites	CVE-2014-3704

SQL Injection Attack

Buggy Login Page


Web Browser (Client)
Enter Username & Password
Web Server
SELECT * FROM Users WHERE user='me' AND pwd='1234'
DB

Bad Input

- Suppose user = " 'or 1=1 – " (URL encoded)
- Then scripts does :
  ok = execute(SELECT ok = execute(SELECT . . .
  WHERE user= ' ' or 1=1 — . . .)
  The " " causes rest of line to be ignored
- Now ok.EOF is always false and login succeeds.
- The bad news : easy login to many sites this way.

SQL Injection : SQLI

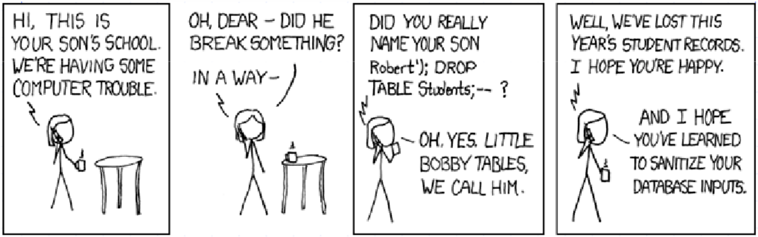
Worst Case

Suppose user = " ; DROP TABLE Users – "

Then script does :

ok = execute(SELECT.. WHERE user= ' '; DROP TABLE Users..)

Deletes user table


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH, YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

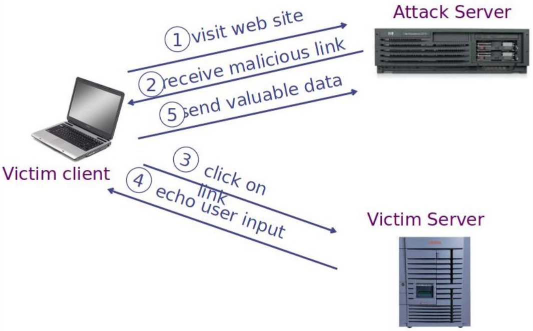
- Similarly : attacker can add users, reset pwds, etc.

Cross Site Scripting (XSS)

Cross Site Scripting(XSS) Attack

- An XSS vulnerability is present when an attacker can inject scripting code into pages generated by a web application
- Methods for injecting malicious code :
    - Reflected XSS (“type 1”)
        - The attack script is reflected back to the user as part of a page from the victim site
    - Stored XSS (“type 2”)
        - The attacker stores the malicious code in a resource managed by the web application, such as a database

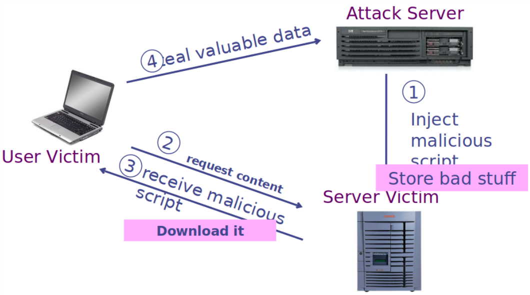
Cross Site Scripting(XSS)



Reflected XSS Attack

- Bad web site sends innocent victim a script that steals information from an honest web site
- Attacker's malicious code executed in victim browser

Cross Site Scripting(XSS)



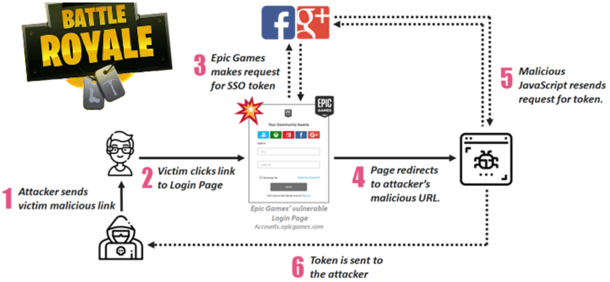
Stored XSS Attack

- Stored attacks are injected script is permanently stored on the target servers, such as in a database, in a message forum, visitor log, comment field, etc...
- The victim then retrieves the malicious script from the server when it requests the stored information. Stored XSS is also sometimes referred to as Persistent

XSS Attack : Real Life Attacks Examples

British Airways	2018	Personal data of 420,000 customers were leaked + a fine of 20 million pounds	Attacked by Magecart
Fortnite	2019	compromised the Fortnite account players	
eBay	2014	Retriving the cookies of ligitimate eBay users + pop-up « 1337 »	Jordan Lee Jones 19 years old

Fortnite Allowed Hackers to Takeover Gamers' Accounts

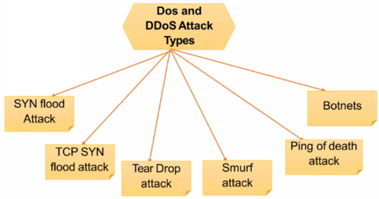

BATTLE ROYALE
3 Epic Games makes request for SSO token
5 Malicious JavaScript resends request for token.
EPIC GAMES
2 Victim clicks link to Login Page
4 Page redirects to attacker's malicious URL.
1 Attacker sends victim malicious link
Epic Games' vulnerable Login Page
Accounts.epicgames.com
6 Token is sent to the attacker

XSS Attack Scenario

- Check Point researchers have discovered multiple security vulnerabilities in Fortnite
- Allowing remote attackers to completely takeover player accounts just by tricking users into clicking an unsuspectable link
- Fortnite flaws include an SQL Injection or Cross-Site Scripting (XSS) bug
- Full account takeover for players a hugely popular online game that has been played by 80 million users worldwide
- Good Fortnite account has been sold on eBay for over $50,000

DOS Attack

DOS Attack



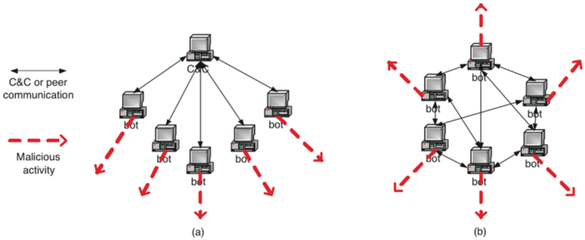
- Goal : take out a large site with little computing work How : Amplification, Small number of packets ⇒ big effect
- Two types of amplification attacks :
    - DoS bug : Design flaw allowing one machine to disrupt a service
    - DoS flood : Command bot-net to generate flood of requests

DOS Attack

Botnet

- A malware instance that runs autonomously and automatically on a compromised computer (zombie) without owner's consent
- Botnet (Bot Army) : network of bots controlled by criminals
- "A coordinated group of malware instances that are controlled by a botmaster via some CC channel"
- Coordinated group of bots
- C&C channel : command and control channel

DOS Attack



Botnet

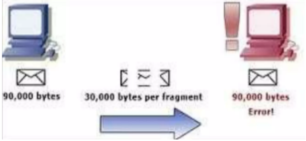
- Centralized : IRC botnet(s) Internet Relay Chat channels
- Distributed
- The Command and Control (*CC*) channel is needed so bots can receive their commands and coordinate fraudulent activities
- The *CC* channel is the means by which individual bots form a Botnet

DOS Attack

Estonia Botnet Attack

- Attacked sites : (started apr. 2007, lasted two weeks, Estonian ministerial sites)
- Various Estonian commercial sites
- Attack types detected : 115 ICMP (Internet Control Message Protocol) floods, 4 TCP (Transmission Control Protocol) SYN floods
  Bandwidth :
  12 attacks : 70-95 Mbps for over 10 hours 12 attacks : 70-95 Mbps for over 10 hours
  All attack traffic was coming from outside Estonia
  Estonia's solution :
  Estonian ISPs (Internet Service Provider) blocked all foreign traffic until attacks stopped
  => DoS attack had little impact inside Estonia

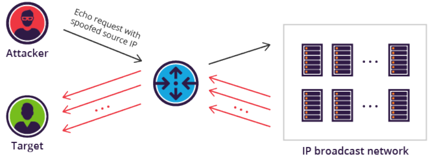
DOS Attack



Ping of Death Attack

- The ping of death is a form of denial-of-service (DoS) attack that occurs when an attacker crashes, destabilizes, or freezes computers or services by targeting them with oversized data packets.
- This form of DoS attack typically targets and exploits legacy weaknesses that organizations may have patched.

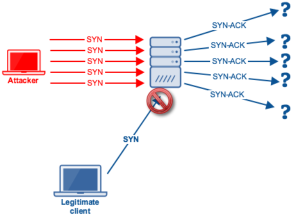
DOS Attack



Smurf DDoS Attack

- A Smurf attack uses crafted Internet Control Message Protocol (ICMP) echo request packets to overwhelm a targeted device. The size of the ensuing DDoS attack is measured in packets per second (PPS)
- The attacker spoofs the victim's IP address as the source IP and sends ICMP echo requests (pings) to the network's broadcast address. Routers on the network receive the ICMP echo request and flood it to all hosts per the broadcast address destination.
- Each host that receives the ICMP request replies back to the source IP with an echo reply packet containing the target's IP address.
- All the responses are sent back to the victim, overwhelming it with traffic and causing a denial of service (DoS).
- The attacker's initiating ping is multiplied by all the hosts responding, creating an amplification effect that can generate floods of traffic directed at the target's network or device(s).

DOS Attack



SYN Flood

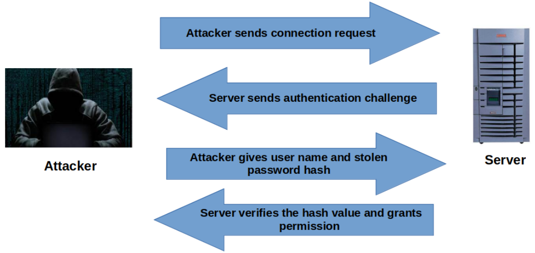
In a normal TCP connection :

- The client sends a SYN packet to the server to initiate the connection
- The server responds with a SYN/ACK packet to acknowledge the communication
- The client sends an ACK packet back to the server to confirm the receipt and complete the handshake

In a SYN flood attack :

- The attacker exploits the fact that the server responds to each SYN packet by leaving an open port ready to receive the response
- The attacker floods the targeted server with a high volume of SYN packets, often using spoofed IP addresses
- As the server waits for the final ACK packet, which never arrives, the attacker continues to send more SYN packets, occupying new open ports
- All available ports are utilized, preventing the server from functioning normally

Replay Attack


Attacker sends connection request
Server sends authentication challenge
Attacker gives user name and stolen password hash
Server verifies the hash value and grants permission
Attacker
Server

- A replay attack occurs when a cybercriminal eavesdrops on a secure network communication, intercepts it, and then fraudulently delays or resends it to misdirect the receiver into doing what the hacker wants.
- The added danger of replay attacks is that a hacker doesn't even need advanced skills to decrypt a message after capturing it from the network.
- The attack could be successful simply by resending the whole thing.
- How replay attacks could be prevented ?

Attack Modeling

Attack Tree

An attack tree AT is a tuple (V, Child, Top_node, L) given as follows. The set of all attack trees is denoted T.

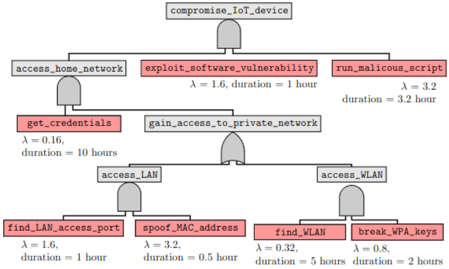
- V is a finite set of nodes.
- Child : $V \to V^\star$ maps each node to its (ordered) child nodes.
- Top_node $\in V$ is the unique top level node, representing the goal of the attacker or the successful compromise of the AT.
- $L : V \to Elements$ is a labelling function such that :
  - L labels all leaves in V with BASs, i.e., L(v) = Basic Attack Steps BAS, if v is a leaf.
  - Hence, non-leaf nodes are labelled with Gates where $Gates = \{AND, OR\}$, i.e., $L(v) \in Gates$ if v is not a leaf.

Attack Tree

The propositional semantics of ATs is a function $I : T \rightarrow F$ that assigns to each attack tree a propositional formula, in a recursive way, as follows, for $b \in BE, where\ BE = BAS, T_i \in T, 1 \leq i \leq k$:

- $I(b) = x_b$, where x_b is the corresponding propositional variable for basic attack step b indicating whether the basic attack step is satisfied.
- $I(AND(T_1, ..., T_k)) = I(T_1) \wedge ... \wedge I(T_k)$
- $I(OR(T_1, ..., T_k)) = I(T_1) \vee ... \vee I(T_k)$

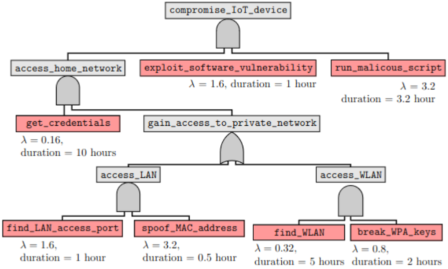
Attack Tree



Consider the attack tree below. The interpretation of the tree as propositional formula is given as :

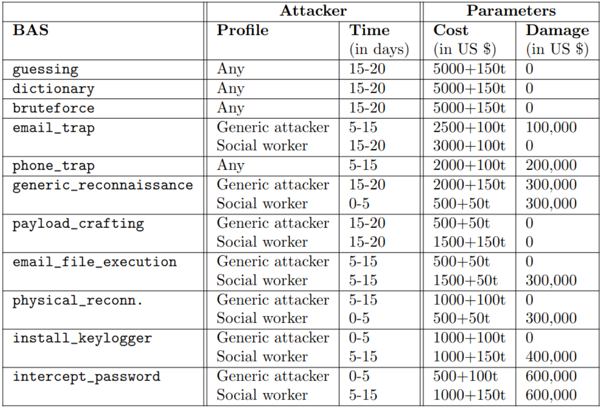
$x_{get\_credentials} \wedge ((x_{find\_LAN\_access\_port} \wedge x_{spoof\_MAC\_address}) \vee (x_{find\_WLAN} \wedge x_{break\_WPA\_keys})) \wedge x_{exploit\_software\_vulnerability} \wedge x_{run\_malicious\_script}$

Attack Tree



- Duration : duration to complete the attack step
- λ : an execution rate λ, quantifying the probability of success of the attack step over time. We obtain the value of λ, assuming that each attack step has a successful % in a given duration.

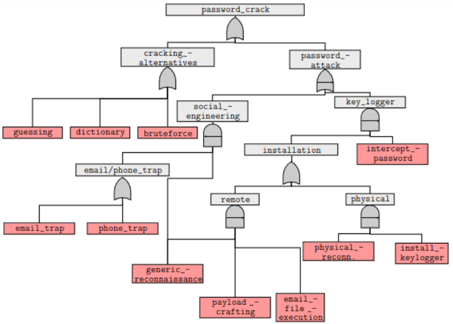
Attack Tree

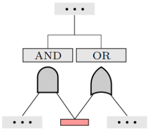


	Attacker		Parameters	
BAS	**Profile**	**Time** (in days)	**Cost** (in US $)	**Damage** (in US $)
guessing	Any	15-20	5000+150t	0
dictionary	Any	15-20	5000+150t	0
bruteforce	Any	15-20	5000+150t	0
email_trap	Generic attacker Social worker	5-15 15-20	2500+100t 3000+100t	100,000 0
phone_trap	Any	5-15	2000+100t	200,000
generic_reconnaissance	Generic attacker Social worker	15-20 0-5	2000+150t 500+50t	300,000 300,000
payload_crafting	Generic attacker Social worker	15-20 15-20	500+50t 1500+150t	0 0
email_file_execution	Generic attacker Social worker	5-15 5-15	500+50t 1500+50t	0 300,000
physical_reconn.	Generic attacker Social worker	5-15 0-5	1000+100t 500+50t	0 300,000
install_keylogger	Generic attacker Social worker	0-5 5-15	1000+100t 1000+150t	0 400,000
intercept_password	Generic attacker Social worker	0-5 5-15	500+100t 1000+150t	600,000 600,000

Parameters used for annotating the AT

Attack Tree

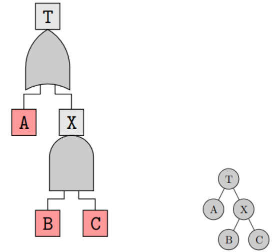




- Sequential-AND gate (SAND gate) and the Sequential-OR gate (SOR gate).
- Basic Attack Steps (BASs) : shown in red rectangular boxes represent the individual atomic steps within a composite attack, and appear as leaves of the AT

Note : that the basic attack step of generic reconnaissance is a shared node. are executed successfully in the direction from right to left, as pointed by the arrow.

Attack Tree



(a) Attack tree

$$\mathbb{P}(T = true | A = true \vee X = true) = 1$$
$$\mathbb{P}(A = true) = 0.4$$
$$\mathbb{P}(X = true | B = C = true) = 1$$
$$\mathbb{P}(B = true) = 0.3$$
$$\mathbb{P}(C = true) = 0.4$$

(b) Bayesian network

A Bayesian network consists of two parts :

- A graph consisting of nodes and edges, where the nodes are the Bernoulli random variables $X_1 ... X_k$ and an edge from nodes X_i to X_j represents a stochastic dependency if i < j ;
- A conditional probability table that quantifies the dependencies between these nodes are executed successfully.

Any Question ?

Please remember that : “A vulnerability that is too complicated for anyone to ever find”   Will be found :)