Moving Target Defense

Simona David

Who am I?

Simona David

- I love CTFs
- Bounty
- You can find me on social media – but you will have to do your OSINT
- Security Researcher @Orange Services

Why?

- I love it
- New and innovative
- Not many presentations in this topic

Agenda

- Introduction
- Strategy
- Examples
- MTD in storing secrets
- Q&A

Introduction

- The question is not if a company will get hacked.
- The question is when a company will get hacked.

- How long can the attackers study the environment?
- How long can the attackers go undetected?

Introduction

- 280 days

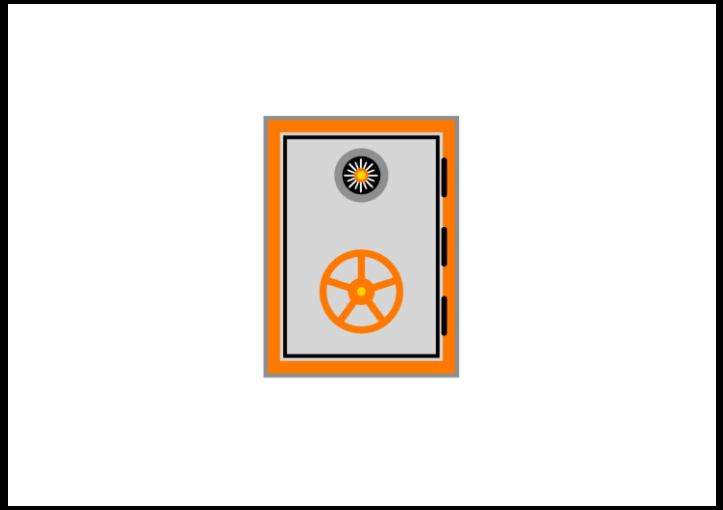
Attacks:

- Targeted
- Un-targeted

Conventional approach

Secure systems by:

- patching all vulnerabilities
- keeping application up-to-date
- staying alert



There is no such thing as perfect security.

Moving Target Defense (MTD)

- 2009 National Cyber Leap Year Summit.

There is no such thing as perfect security, so the focus should be on building alternative defensible systems.

Moving Target Defense (MTD)

Purpose: balance the asymmetry between attackers and targets

How: changing or reducing the attack surface

Attack surface: any property of the system that can be used for an attack

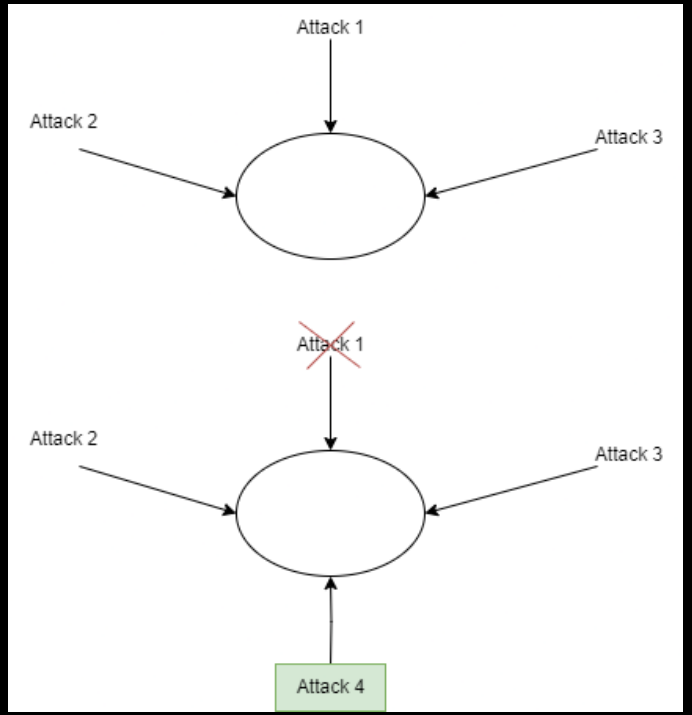
Examples:

- Vulnerabilities
- IP
- Port
- Anything that constitutes a pattern

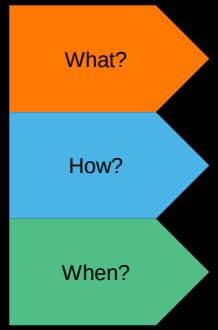
Introduction

Attackers thrive on patterns!

MTD is designed to increase the time and effort an attacker needs to make the attack successful.



Strategy



What parameter to change?

How will it be changed?

When will it be changed (periodically, after a certain event)?

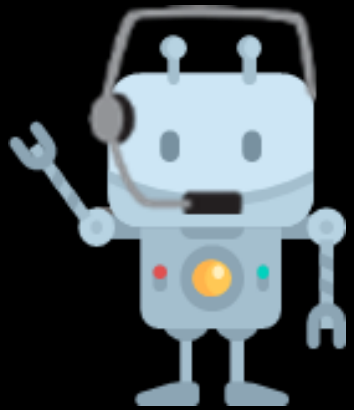
Strategy

If changed periodically, what time interval to use?

Too often -> impacts system's performance.

Too rare -> it may not help.

If changed after a certain event, what event will be the trigger?
Do we cover events on every part of the attack surface?



Challenges

Coverage

The exploitable elements must be covered by MTD.

Unpredictability

The state of the system should be unpredictable.

Timeliness

The changes should be done between the attacker observations and the subsequent attacker actions.

Examples

- Instruction Set Randomization (ISR)
- NOP insertion
- Address Space Layout Randomization (ASLR)
- IP shuffling
- Honeypot
- Etc

The moving part can be done at these levels:

- Network
- Application
- Software

Detailing examples

ASLR (Address Space Layout Randomization) is an effective MTD technique against buffer overflow and other code injection attacks that rely on the address location of the memory layout.

It randomizes the addresses of the memory areas associated with a process.

Detailing examples

Ways to bypass ASLR:

Leaking just one pointer to a given segment/region is typically sufficient to find anything in the segment/region, because distances are preserved under ASLR.

ASLR in Linux is applied at page granularity, meaning that on x86_64 systems with 4KB pages, the lower 12 bits of an address will always stay the same (as only the virtual page number changes from run to run).

Time + Effort > Results

The shell game

In the “shell game”, an operator places a target such as a pea under one of the three identical face-down shells and shuffles them quickly for many times. When stopped, the player who can correctly identify which shell contains the pea, wins.

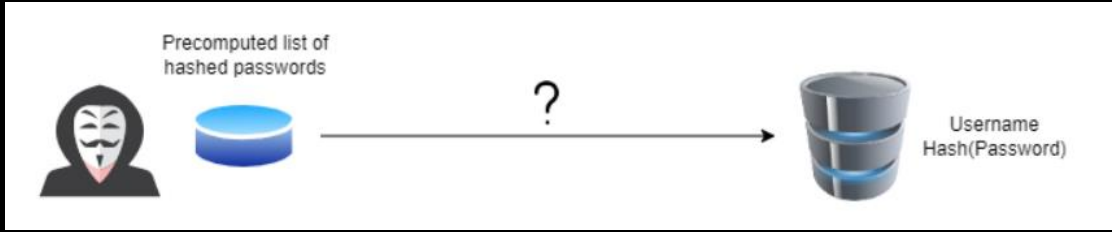
Sufficient movement of the shells will lead to confusion => Moving Target Defense

MTD in cryptography

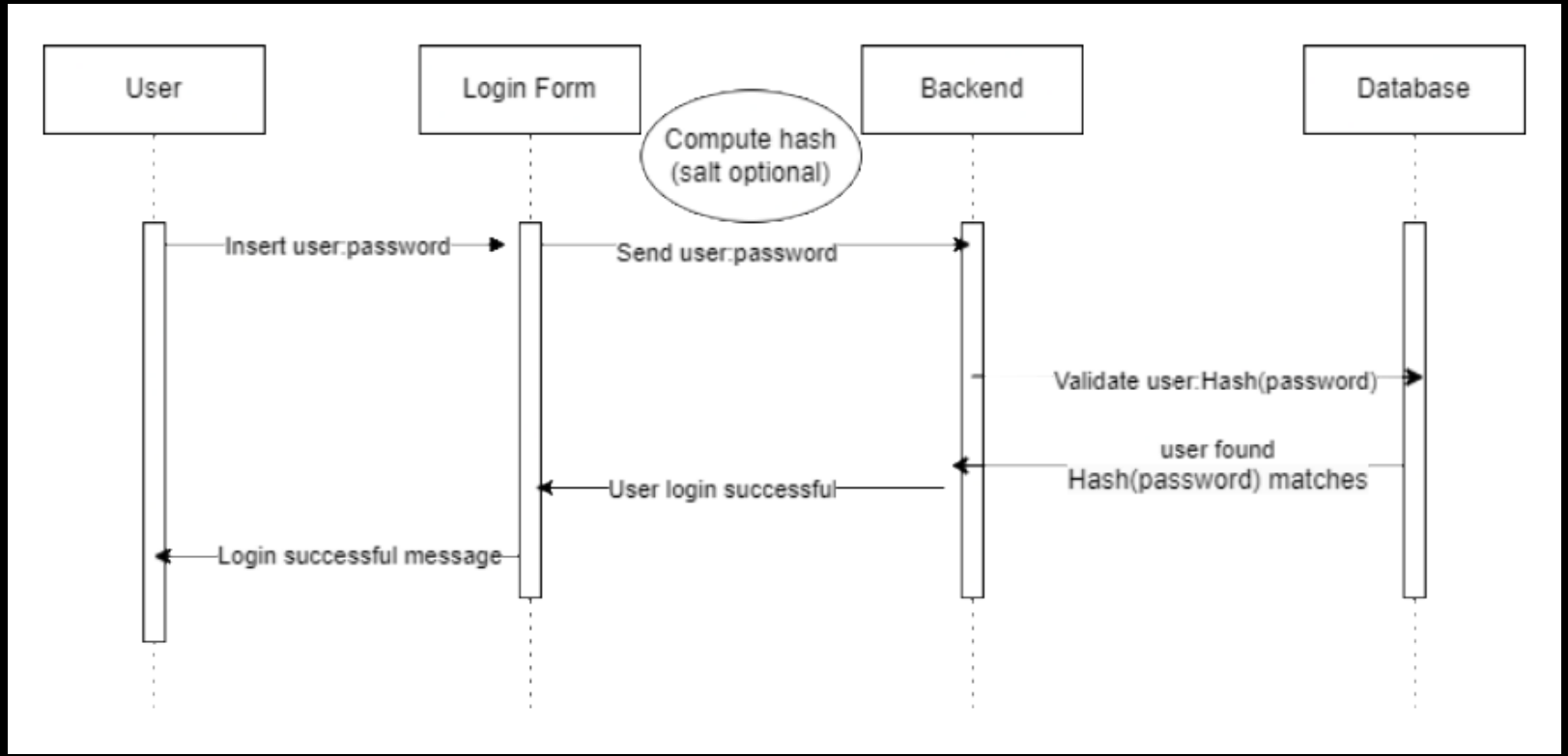
- changing the encryption key periodically
- switching between multiple cryptosystems

MTD in storing secrets

When attackers gain access to a database containing passwords, they will try to find the plaintext passwords associated to the values in the database.



MTD in storing secrets



MTD in storing secrets

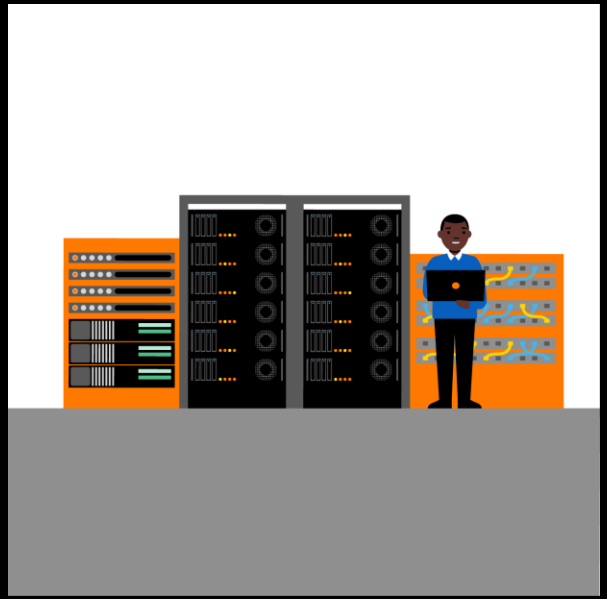
This provides an attacker with a lot of info on the algorithm used.

MD5 – 32 chars

SHA1 – 40 chars

SHA256 – 64 chars

SHA 512 – 128 chars

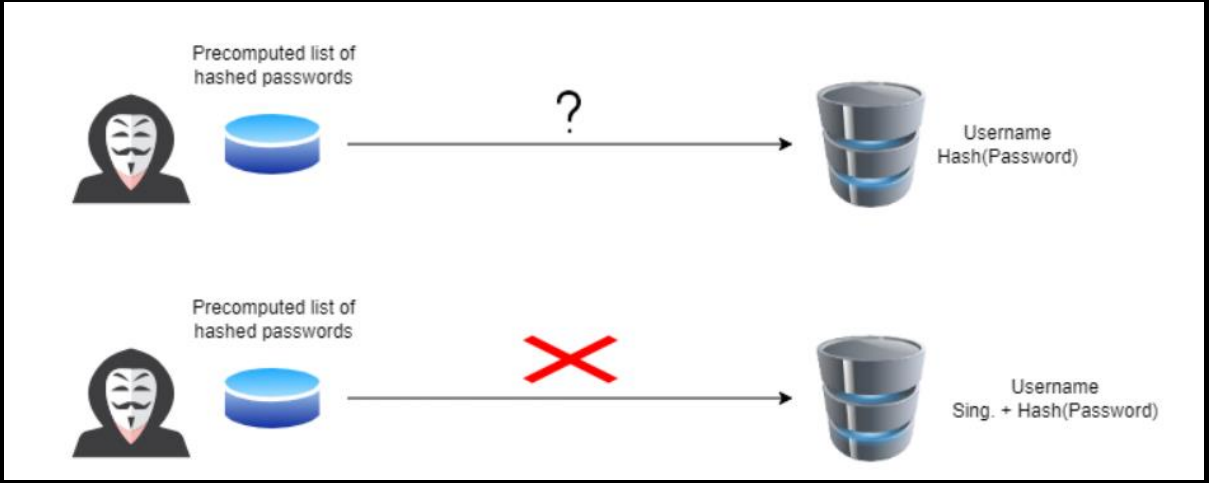


MTD in storing secrets - Singularization

What would happen if each secret will be stored in a different format?

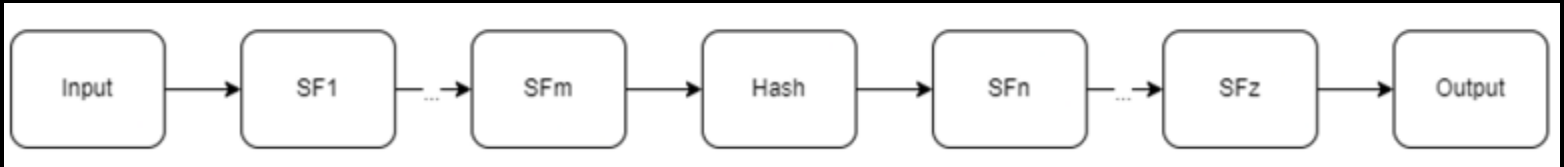
The dictionary attack will be unusable.

Cost + effort > results

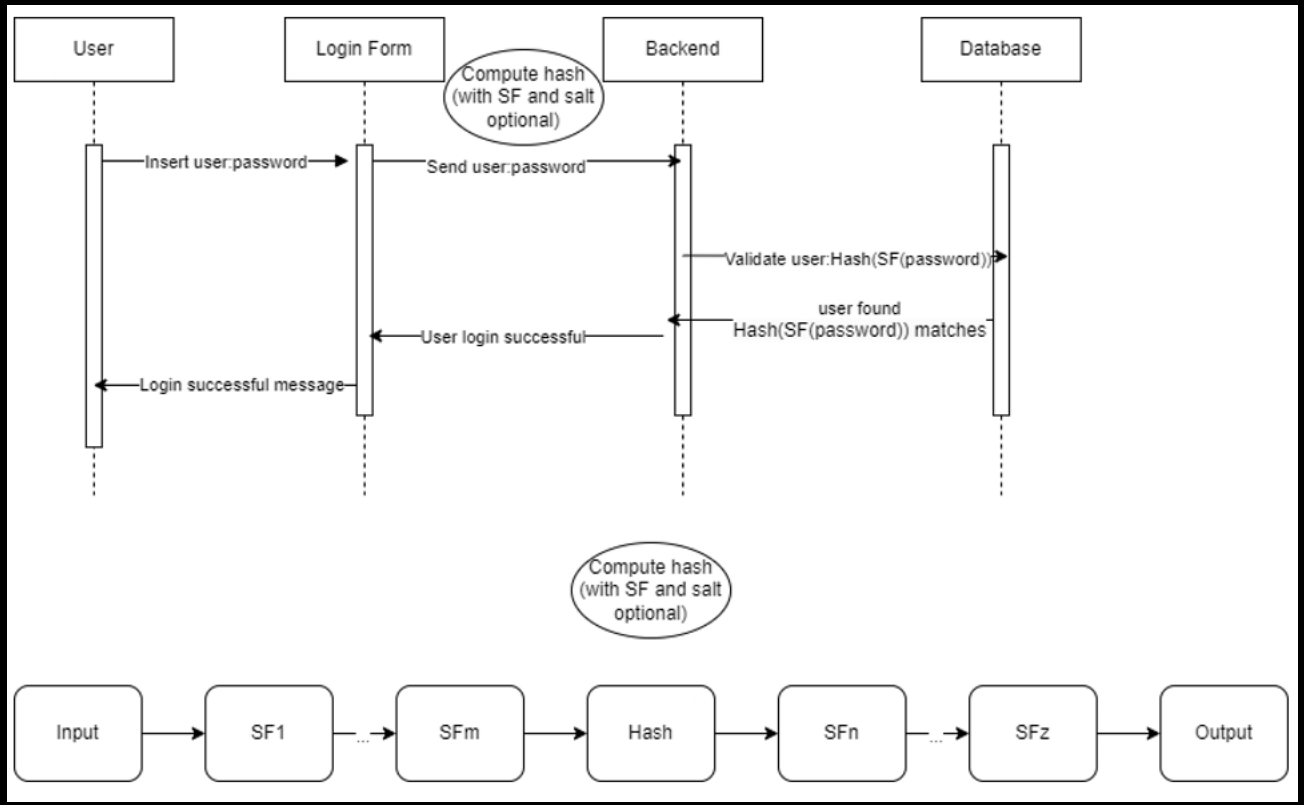


MTD in storing secrets - Singularization

Singularization – a sequence of functions, different for each entry/each group of entries



MTD in storing secrets - Singularization



Summary

Why: balance the asymmetry between attackers and targets

What: part of the attack surface
How: changing or reducing the attack surface
When: time/event

Attackers thrive on patterns!
Cost + effort > results

Bibliography

- Breaking ASLR
- Zheng J, Namin AS. A survey on the moving target defense strategies: An architectural perspective. JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY 34(1): 207–233 Jan. 2019. DOI 10.1007/s11390-019-1906-z
- Pratyusa K. Manadhata. Game Theoretic Approaches to Attack Surface Shifting
- Cai et al. / Front Inform Technol Electron Eng 2016 17(11):1122-1153. Review: Moving target defense: state of the art and characteristics

Questions?


Thank you!
orange™