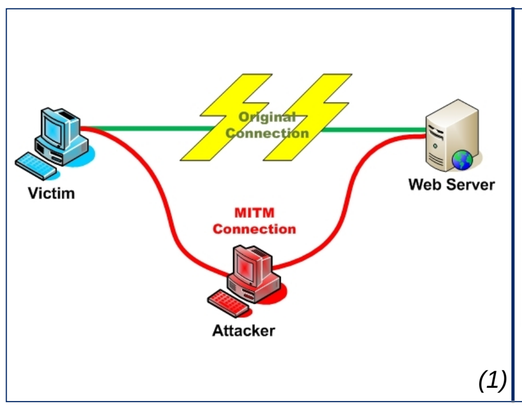
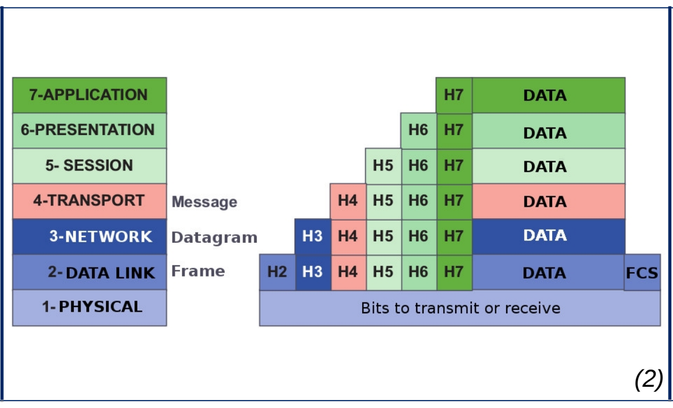
Man-in-The-Middle
Attacks & Countermeasures Analysis

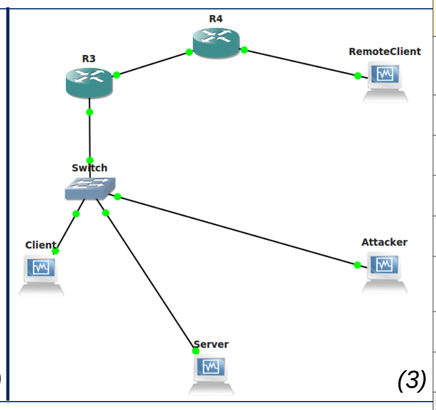
MSc. Ethical Hacking & Computer Security, Abertay University
Email: 1404780@abertay.ac.uk



(1)



(2)



(3)

Attacks				Defences efficiency											
Layer	Vector	Range of[2] efficiency	Range of action[3]												
2	**ARP**	LAN/ FLAN	🔒	✓	✓	✓									
2	**CAM**	LAN	🔒	✓	✓								✓		
2	**STP**	LAN	🔒				✓	✓	✓						
3	**ICMP**	FLAN	🔒							✓					
3	**IRDP**	FLAN	🔒								✓				
3	**IGPs**	FLAN/ WAN	🔒									✓			
7	**DNS**	All	🔒										✓	✓	
7	**DHCP**	FLAN	🔒	✓										✓	
Advanced															
Name	Target Protocol														
Filter	**IPSEC**	🔓												✓	
DC[1]	**SSH**	🔓													✓
Inject	**HTTP**	🔓													
Defences															
Availability on[4]				S R	S R	T	S	S	S	T R	T R	R	T	T	S R	T	T	T
Name				Port security	**DAI**	Static **ARP**	Disable **STP**	Root Guard	BPDU Guard	Disable **ICMP** redirect	Disable **IRDP**	**IGPs ACLs** / Authentication	**DNSSEC**	Static **DNS**	**DHCP** Snooping	No auto rollback to clear-text	Disable weak cyphers	Use secure protocol **(HTTPS)**

Abstract

Man-in-The-Middle (MiTM, see Illustration 1) attacks still remain widely used by attackers because exploiting key-role mechanisms, by default used by the systems. This project investigates the different vectors to perform a Man-in-The-Middle attack, and the corresponding defences on the lower layer (Illustration 2) they are available on. Protocols from each and every vectors have been included in the project, in order for all areas to be covered.
MiTM attacks are technically easy to perform for most of them, allows passive eavesdropping or active modifications, and more than disrupting the network, they can remain unseen to the user for long.

Introduction

Internet has not been designed in first place for such a use, authentication and security appeared later. As consequences, an important amount of protocols and technologies leave flaws or exposures. An important work has also been done to address those issues by various and different means, such as the generalization of HTTPS on the Web. In order to complete this project, the first step is the identification of the mechanisms and the vectors of attack that they can represent. These vectors allow the identification of the different direct defences available. The second step will expose the defences. efficiency, ease of use and implementations in an existing architecture. The focus will be brought to the vectors and protocols interactions, same for the defences. The output aims to highlights commons weaknesses, or mechanisms, in order to draw a wider picture of the field.

Method

Environment for testing is virtual.
It disposes of two clients distributed between two LANs. One server is present with the client and the attacker on the LAN. One switch manages the link between the terminals and the gateway to interconnect the two LANs. Via a third LAN identifying the inter-networks link (Illustration 3).

Vectors analyzed (defences list will be presented in the results):
- ARP spoofing
- ARP port stealing
- STP mangling
- ICMP redirect
- IRDP spoofing
- Route mangling
- DNS spoofing
- DHCP spoofing

Process:
- Implementation of the vulnerable protocol
- Exploitation and testing
- Defence(s) implementations
- Defence(s) testing

Advanced MiTM exploitation performed, specific target choice and defence(s):
- Filtering packets
- Downgrading cypher
- Injections

Results

Results have brought interesting information concerning the range of efficiency and action, visible in the following table.
The main defence are there to implement authentication/access control lists to prevent unauthorized changes, as well as signature and encryption to prevent alteration and eavesdropping.

Notes (refer to the table in-line indexes):
1. Downgrading Cypher.
2. Indicates what can be intercepted:
   - **LAN**: The attack can target intra-network communications;
   - **FLAN**: The attacker can see packets leaving the **LAN** (=From **LAN**);
   - **WAN**: Packets sent or received to another **LAN** can be intercepted.
3. Indicates if the attack is efficient for clear text protocols only (🔓) or includes the access to encrypted ones (🔒).
4. Defences can be implemented on the servers or clients (T for Terminals), switches (S), or routers (R). Multiple letters indicate multiple possibilities.

These results however have to be mitigated based on the findings of the second phase, and the advanced exploits. Encryption can build false hopes of security because of outdated cyphers still in use for backward compatibility, or misconfiguration. Old protocols that do not implement any security mean are simply deprecated to turn to more recent ones.

Conclusion

Encryption seems to provide all necessary means to defend against all consequences of MiTM. However it does not fix the existing vulnerabilities, and raises concerns about cypher resistance, the key length…
Actual problems that require to be thought from the development process, as the amount of vectors highlight a real concern.

Illustrations: *(1) Open Web Application Security Project (OWASP) - (2) Servin, C., 2003. Réseaux et télécoms [French] [translated by: Gontharet Florent]*