Progress report (Iteration II)

Daria Vaskovskaya (d.vaskovskaya@innopolis.ru)

February 2020

1 Intro

- **Student Name**: Daria Vaskovskaya
- **Topic**: Man In The Middle Attacks: Execution and Detection
- **Supervisor**: Rasheed Hussain
- **Iteration number**: 2

2 Initial plan

- Submit the project proposal (create a plan for the project)
- `Iteration I` Study different variants of simulation platforms and set up the environment for Man In The Middle Attacks, perform some MITM attacks on simulation platforms
- `Iteration II` Continue to perform some MITM attacks on simulation platforms, study common detection and prevention techniques from Man-in-the-Middle attacks, test detection and prevention techniques on the simulation platforms
- `Iteration III` Continue to test detection and prevention techniques on the simulation platforms, study ways to bypass some of the detection and prevention techniques found earlier.
- `Iteration IV` Study ways to bypass some of the detection and prevention techniques found earlier, test ways to bypass detection on the simulation platforms
- `Iteration V` Test ways to bypass detection on the simulation platforms, start to prepare for the Internal presentation (prepare the scripts, prepare a fast way to set up the project, prepare the presentation itself)

- `Iteration VI` Finish to prepare for the Internal presentation (prepare the scripts, prepare a fast way to set up the project, prepare the presentation itself).
- Fix issues related to the remarks got during the Internal presentation, prepare project for the final Delivery(EoSP).

3 Done during second iteration

- `task` Read the papers about MITM detection and make short summaries about the noteworthy ones , pick paper/papers to investigate further during the 3rd iteration
- `hours spent` 12 hours
- `status` Done
- `results` will be available below

4 Current issues

- Change of study direction leads to plan changes, probably new plan will be presented during the next iteration.
- Lack of mathematical experience can lead to some problems in future studies of papers.

5 Results

5.1 Introduction

The ways to detect MITM attacks are complex, that means that in addition to the methods to detect the presence of MITM attack regardless of the mechanism used to launch it, there are a lot of methods focusing on detecting those mechanisms (ARP spoofing, DNS spoofing etc.) Firsly, I wanted to study both of the methods types (for this purpose the ARP spoofing attack was launched during the last iteration). However while reading the papers it became clear that I should reduce study area, so I decided to focus on methods to detect the presence of MITM attack regardless of the mechanism used to launch it. During this iteration I present summaries about the noteworthy papers in this area.

5.2 Papers

- Vesper: Using Echo-Analysis to Detect Man-in-the-Middle Attacks in LANs [4]

Detector captures the impulse response of a LAN by measuring the roundtriptimes (RTT) resulting from a short intense burst of ICMP echo requests. This impulse response is used to model the normal behavior of the network in the perspective of two communicating hosts. When a third party intercepts traffic, the harmonic composition of the impulse response between the hosts changes significantly. Vesper detects this change using an autoencoder neural network as an anomaly detector. The method is nonintrusive (no packet inspection), incurs a minimal overhead on the network, and is not dependent of the hardware and software of the LAN or the attacker's device. The contributions of this paper include a framework for deploying the technique on a LAN (Vesper). Four possible adversarial attacks against Vesper are presented, which would be helpful if I choose to study how to be silent against detection tools which use the same technology as Vesper.

- The Security Impact of HTTPS Interception [3]

  Their methodology for identifying interception is based on detecting a mismatch between the browser specified in the HTTP User-Agent header and the cryptographic parameters advertised during the TLS handshake.

  For example, none of the four browsers (Chrome, Safari, Internet Explorer, and Firefox) have ever supported the TLS Heartbeat extension. If a browser connection advertises its support,It is known that the session was intercepted.

  It is worth noting that there are detection tools based on this paper, for example Caddy has the ability to detect certain MITM, mitmengine which is used to build MALCOLM.

  These tools can not detect proxies which closely mimic the request of the client, because they can not detect a mismatch in this case. It is interesting to study if those kind of proxies exist or not and try to omplete the existing ones if this feature is not provided.

- Detection of MITM Attack in LAN Environment using Payload Matching [2]

  The proposed scheme is based on detecting the similarity in traffic to discover the presence of an MITM attack.

  The paired frames will be tested for matching of content. The matching starts at an offset from the start of frame to skip the parts that are likely to be modified by the attacker.

  Sample of all traffic that passes through the network is gathered by the monitoring station.

  In typical MITM attack, the header information of the two frames of MITM pair will be different as some fields of the header (typically layer 2 header) need to be modified in order to direct the traffic to desired destination (attacker or the other victim). The remaining of the frame remains usually unmodified unless the attacker is carrying an active attack.

That is how they collect MITM pairs (two frames, the frame received from one victim and the corresponding frame relayed by the attacker).

Then they match the payload of the frame pairs.

A drawback of the proposed scheme is that the computational and memory requirements may become high in heavy traffic conditions, that is why even though this method shows good results and worth noticing it is unlikely for it to be widespread.

- Client-Side Web Proxy Detection from Unprivileged Mobile Devices [1]

  The methodology presented in this paper tries to detect proxies without access to low-level packet traces, nor access to Web servers, therefore provide a way to infer that there is a Web proxy based only at information gleaned from the application layer at the client. Two problems appear: 1) controlling when traffic is subject to proxy interposition, and 2) detecting the impact of this interposition.

  To address the first problem, they rely on results from previous studies (and reconfirmed in their study), that Web proxies operate on traffic only to certain ports (e.g.,port 80 for HTTP), but not others (e.g., port 443 for HTTPS). They run back-to-back experiments to fetch the same Web page over HTTP and HTTPS from the same server, where the latter is not subject to proxy interposition. To address the second problem, they use a combination of features that include latency differences and content modification.

6 Future plans

"Client-Side Web Proxy Detection from Unprivileged Mobile Devices" focuses on specific type of proxy.Method presented in "Detection of MITM Attack in LAN Environment using Payload Matching" is unlikely to be widespread due to computational and memory requirements, so I will not investigate it further during next iteration.The RTT analysis ("Vesper: Using Echo-Analysis to Detect Man-in-the-Middle Attacks in LANs") is interesting, however there can be some problems due to not enough comprehension of some topics mentioned in the paper. As was mentioned above, tools based on "The Security Impact of HTTPS Interception" paper can not detect proxies which closely mimic the request of the client, because they can not detect a mismatch in this case. It is interesting to study if those kind of proxies exist or not and try to complete the existing ones if this feature is not provided.

The most optimal solution in my case is to start investigating "The Security Impact of HTTPS Interception" paper.

Hours: 12

References

[1] *Client-Side Web Proxy Detection from Unprivileged Mobile Devices.* URL: https://arxiv.org/pdf/1511.04493.pdf.

[2] *Detection of MITM Attack in LAN Environment using Payload Matching.* URL: https://www.researchgate.net/publication/279192958_Detection_of_MITM_attack_in_LAN_environment_using_payload_matching.

[3] *The Security Impact of HTTPS Interception.* URL: https://jhalderm.com/pub/papers/interception-ndss17.pdf.

[4] *Vesper: Using Echo-Analysis to Detect Man-in-the-Middle Attacks in LANs.* URL: https://arxiv.org/pdf/1803.02560.pdf.