Removing SSL using MitM on a Wireless Access Point

Radboud Universiteit Nijmegen

{ Carlo Meijer, Roland Verbruggen and Eduardo Novella } The Kerckhoffs Institute

UNIVERSITEIT TWENTE.

Objectives

(i) Measure the security awareness among students social sciences and science faculty
(ii) Check our hypothesis : Science students are more aware than social sciences
(iii) Set up wireless access points in both faculties
(iv) Perform SSL-removing man-in-the-middle attack

Introduction

This paper presents a method of measuring the difference in degree of security awareness among students between the social sciences and science faculty. The degree of security awareness is measured by observing subjects that connect to our unsecured wireless access points set up by us. On these access points we perform a man in the middle attack and wait for clients to enter credentials for a website.

Materials & Methods

The following materials were required to complete the research:

- A PC running Linux
- WiFi APs: Hostapd & several WiFi cards
- SSLStrip from scratch (Carlo Meijer)
- Debriefing & Web questionnaire
- Apache2 & PHP

A web form is launched if subject logs into any website or after a 10 minute timeout

- Collect opinions from users
- Do a statistical analysis in order to verify our hypothesis

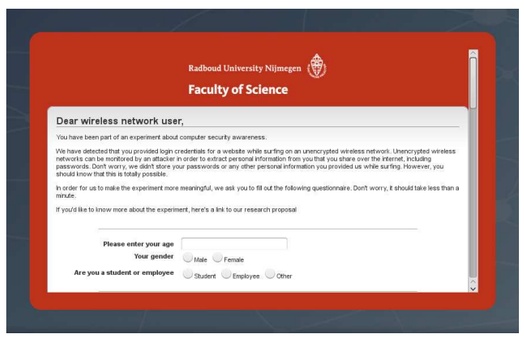


Figure 2: Web questionnaire

Characteristics

The subjects age range from 17 to 34. Also the subjects differ in the amount of perceived security awareness. The characteristics of the subjects are provided in Table 1.

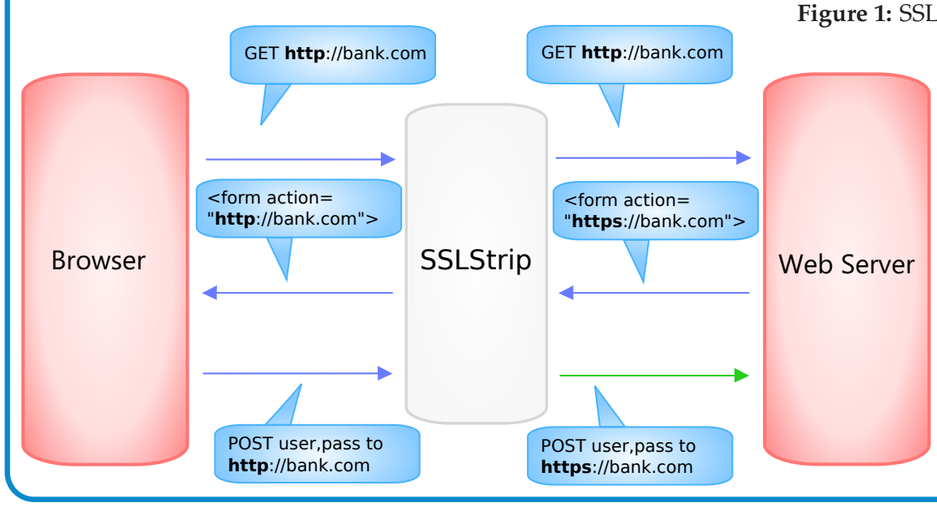
Property	Number	Perc.
Total number of subjects	59	100%
Social sciences subjects	25	42%
Science subjects	34	58%
Percent female	28	47%
Median age	20	
Students	52	88%
Employees	2	3%
Others	5	8%
Subjects that saw banner	29	49%
Subjects that saw flyer	21	36%
Subjects that saw neither	23	39%
Logins	26	44%
Timeouts	33	56%

Table 1: Characteristics of the subjects

The attack explained

HTTP offers no features that guarantee either confidentiality or integrity. Since we are in a man in the middle position, we can exploit the this fact by making slight modifications to the HTTP responses: we swap out all references to HTTPS urls and replace them with HTTP. Internally, we keep track of which urls are referenced as HTTPS urls. Whenever we receive a request for such a url, we then know that the request was actually supposed to be sent over HTTPS. Hence, we forward the request over HTTPS. The response for that request is then sent back to the user over HTTP. In this scenario, the server receives all the requests over HTTPS that it expects. It cannot reliably detect whether or not a client is under attack. The client sends everything that is actually supposed to be sent over HTTPS over HTTP, but it is unknown to the client what is supposed to be sent over HTTPS and what not. The result is that the client sends everything, including sensitive information such as user names and passwords, over HTTP. Hence we can read this sensitive information. The only visible difference the client may notice when under attack is that the "lock icon" in the browser is missing and the url states HTTP instead of HTTPS.

Figure 1: SSLStrip diagram



Conclusion

Other studies confirm the notion that science students are more security aware than other students. Hence, we suspected there is a difference between students from the social sciences faculty and the science faculty regarding loggin into websites while under attack by SSLStrip. However, since the difference we found between the two groups is insignificant (p = .597), we reject this hypothesis. We suspect the reason for not finding a significant result may be the small number of subjects (n = 59). We hope this paper inspires other researchers to repeat the experiment with a larger number of subjects, and hopefully find a significant result.

References

[1] Moxie Marlinspike. News tricks for defeating ssl in practice. *BlackHat DC*, 2009.

[2] S. Basagni M.B. Kowalski, K. D. Bertolino. Monitoring wireless security awareness in an urban setting.

Future work

We hope this paper inspires other researchers to repeat the experiment with a larger number of subjects, and hopefully find a significant result. Fortunately, we did find evidence that subjects were reluctant to logging into websites in the case they saw a banner or received a flyer, warning them about the risks that apply when using unsecure wifi.

Contact Information

Eduardo Novella e.novellalorente@student.ru.nl
Carlo Meijer carlo.meijer@student.ru.nl
R. Verbruggen rolandverbruggen@student.ru.nl