



HSTS IMPLEMENTATION & SECURITY ISSUES

MOHAMMED ABDULLA

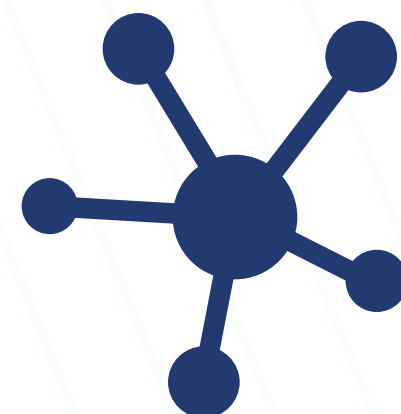
School of Applied Computing, Faculty of Architecture,
Computing and Engineering, University of Wales Trinity St David, Kings Road Swansea, SA1 8PH
Email: abdulla.152058@student.uwtsd.ac.uk

Introduction

One of the commonly used protocols is the secure socket layer (SSL) used to secure communication between the client and the web server [1], to enhance information integrity, authentication and ensuring data confidentiality during Website transactions [2]. The SSL is now known by its new name as the transport layer security (TLS) as it provides better data encryption and authentication between the client and the server.

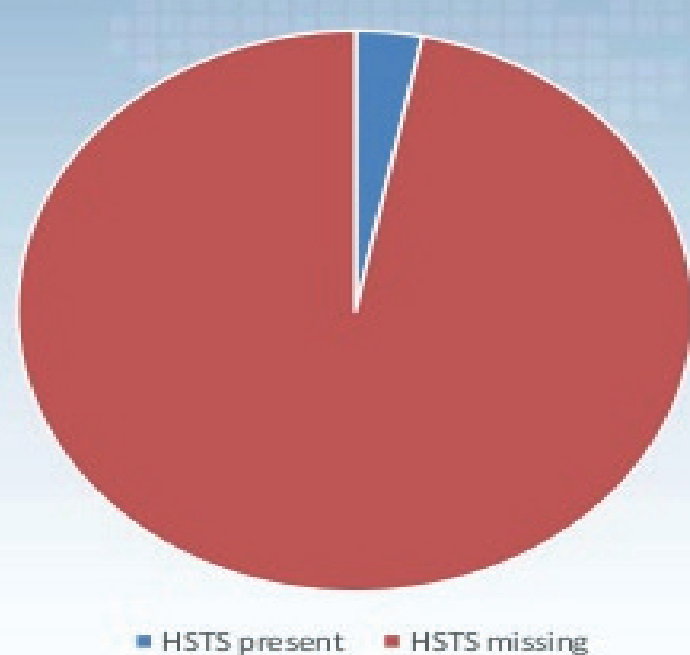


SSL stripping rescuers – HSTS and HSTS preload, either not implemented by majority of websites or not properly configured helping the attacker to compromise the web browsers.



less than 5% of secure websites enable this important security feature

How many sites use HSTS?

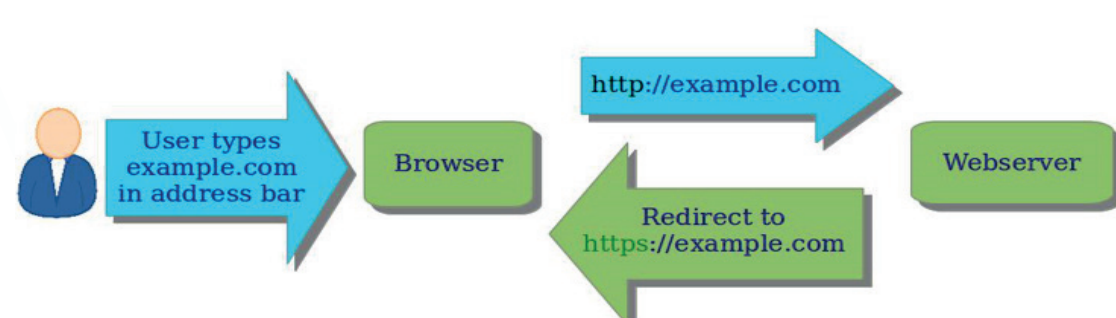


■ HSTS present ■ HSTS missing

SO...



HTTP Strict Transport Security

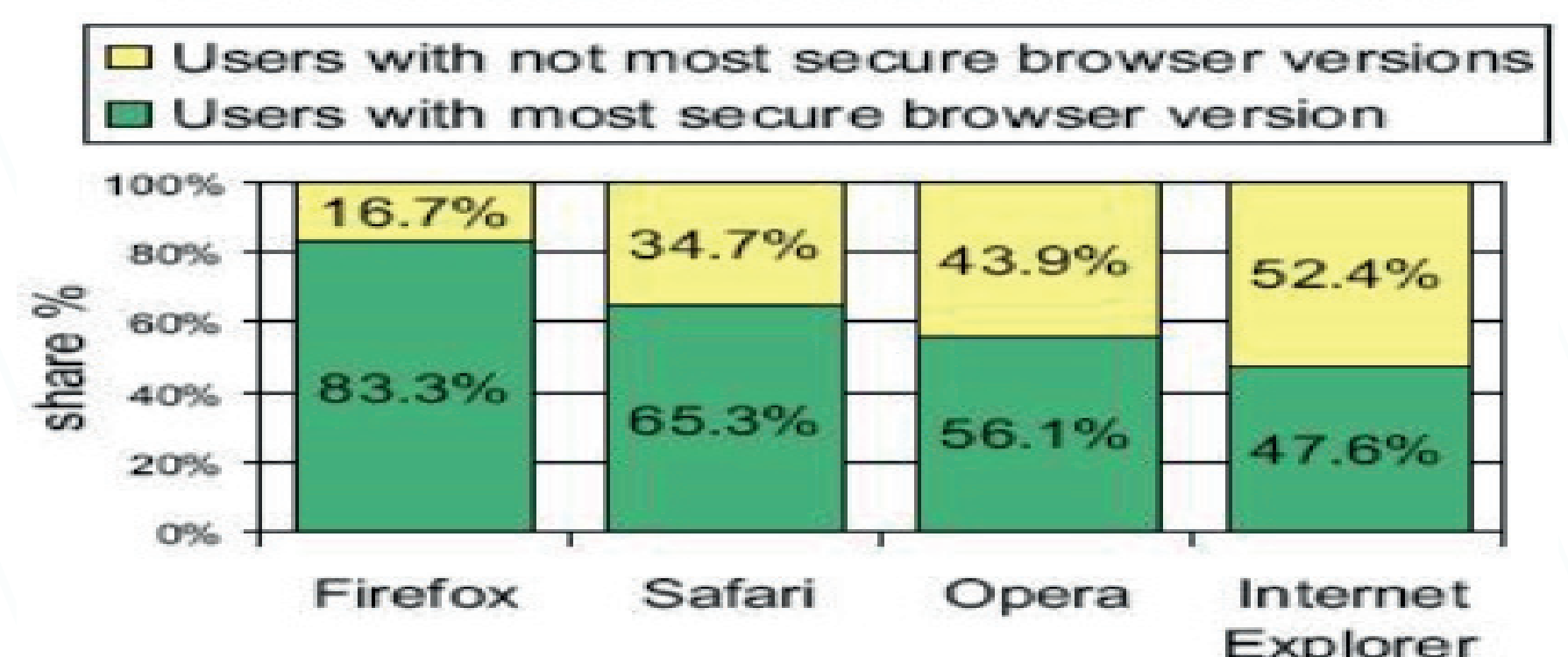


AIM & Objectives

- To investigate the potential vulnerabilities that could put end-user credential at risks when browsing.
- To assess HSTS different implementation.
- To assess approaches that can be used to enforce connections to HTTPS and authenticate the web URL for protecting against the SSL Stripping MITM attack.
- To assess the three main web browsers Firefox, Internet Explorer and Opera behaviour when facing downgrading (SSL stripping) attack.
- To identify potential areas for research in the future in efforts to improve the client's experience while serving.

HTTPS everywhere is Firefox, chrome and opera extension that encrypt your communication with many major websites, make your browsing more secure. Encrypt the web. Install web browser that is HSTS aware.

Share of most secure browser versions



Websites owners:  HTTPS Everywhere

Not just logging pages!!!!!!

TESTS SHOWS THAT:

- The websites that are correctly implemented for HSTS and are also preloaded to the browser are immune to SSL stripping attacks.
- The websites that are not properly implemented for HSTS are vulnerable to SSL stripping.
- The SSL stripping works on against web sites that are not configured with http strict transport-security (HSTS) at all

How to mitigate this problem?

- Web site should be available only in HTTPS
- Use HSTS and preload it into the browser.
- End users should use web browser that is HSTS aware

References

[1]. A. Chordiya, S. Majumder and A. Javaid, "Man-in-the-Middle (MITM) Attack Based Hijacking of HTTP Traffic Using Open Source Tools", 2018 IEEE International Conference on Electro/Information Technology (EIT), 2018.
[2]. D. Fairweather, H. Mozer, S. Rinehart and D. Shin, "An enhanced approach to preventing the SSL stripping attack", 2015 International Conference on Information and Communication Technology Convergence (ICTC), 2015.

[2] <https://www.thesecuritybuddy.com>
[3] <https://cryptoworld.su/obxod-https-s-pomoshhyu-sslstrip/>
[4] https://www.slideshare.net/OWASP_Poland/wroclaw-4-web-application-security-headers2-hsts-hpkp