An Empirical Study of Visual Security Cues to Prevent the SSLstripping Attack

Shin, Dongwan, and Rodrigo Lopes.
"An Empirical Study of Visual Security Cues to Prevent the SSLstripping Attack."
In *Proceedings of the 27th Annual Computer Security Applications Conference*, 287–296.
ACSAC '11. New York, NY, USA: ACM, 2011.
doi:10.1145/2076732.2076773.

Oral Report Presented by Sam Grace

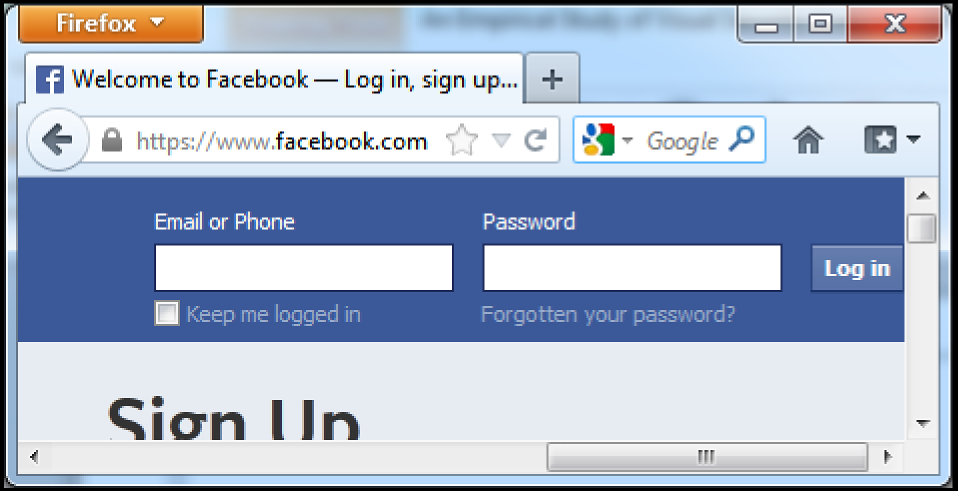
Outline

- Article Summary in 3 Parts
  - SSL Stripping Attack
  - SSLight Browser Extension
  - User Study
- Criticism
- Appreciation
- Question

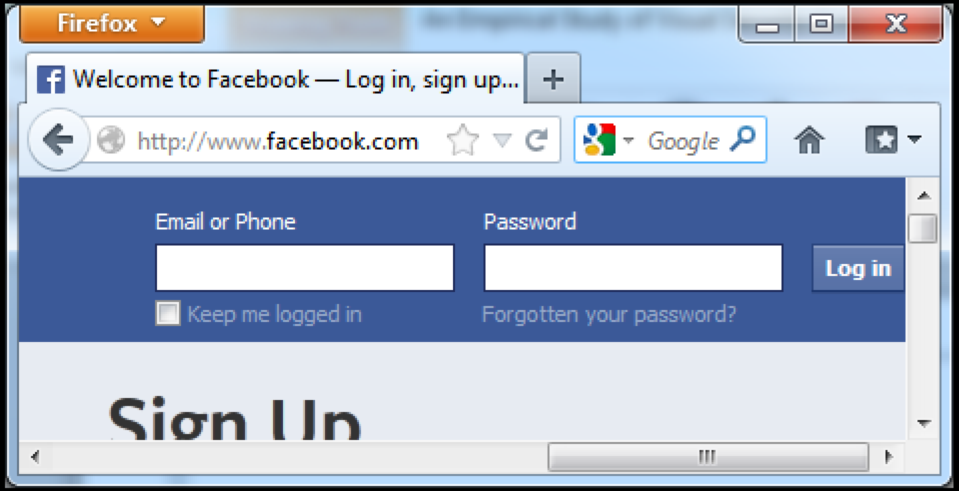
SSL Stripping Attack

- Introduced at the Blackhat conference in 2009 by Moxie Marlinspike
- Form of Man in the Middle Attack (over LAN)
- Attacker intercepts all content sent between user and web server and strips all SSL references from web pages
- Allows attacker to see the users login name and password
- According to the article, the attack has the potential to affect tens of millions of users of banking and social network users in 2011

Facebook.com in a normal situation



Facebook.com under SSL Stripping Attack

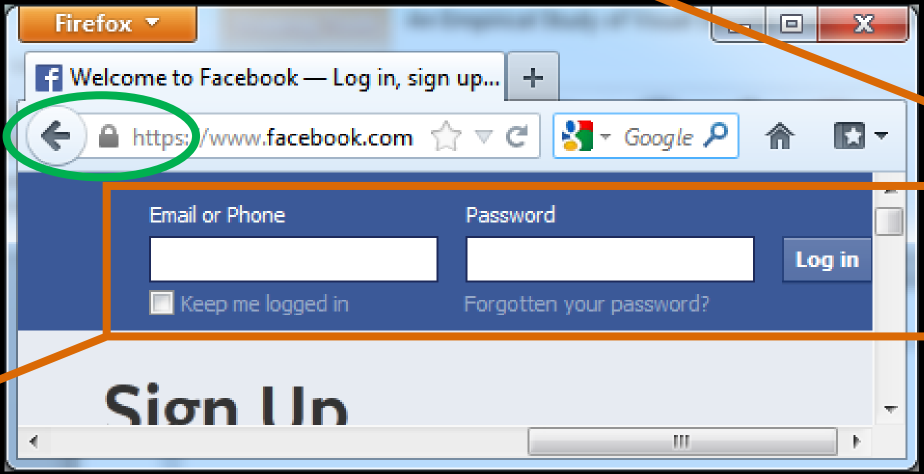


Welcome to Facebook — Log in, sign up...

http://www.facebook.com

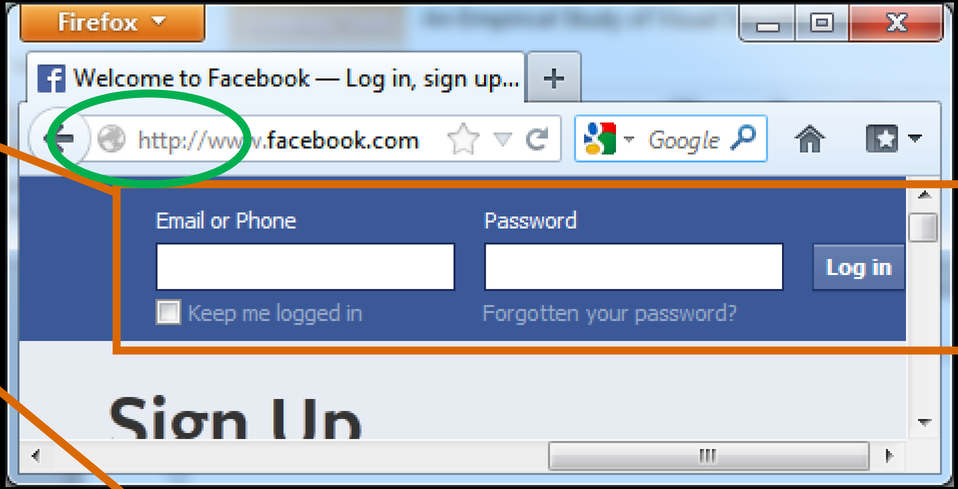
SSL Stripping Attack comparison

normal situation



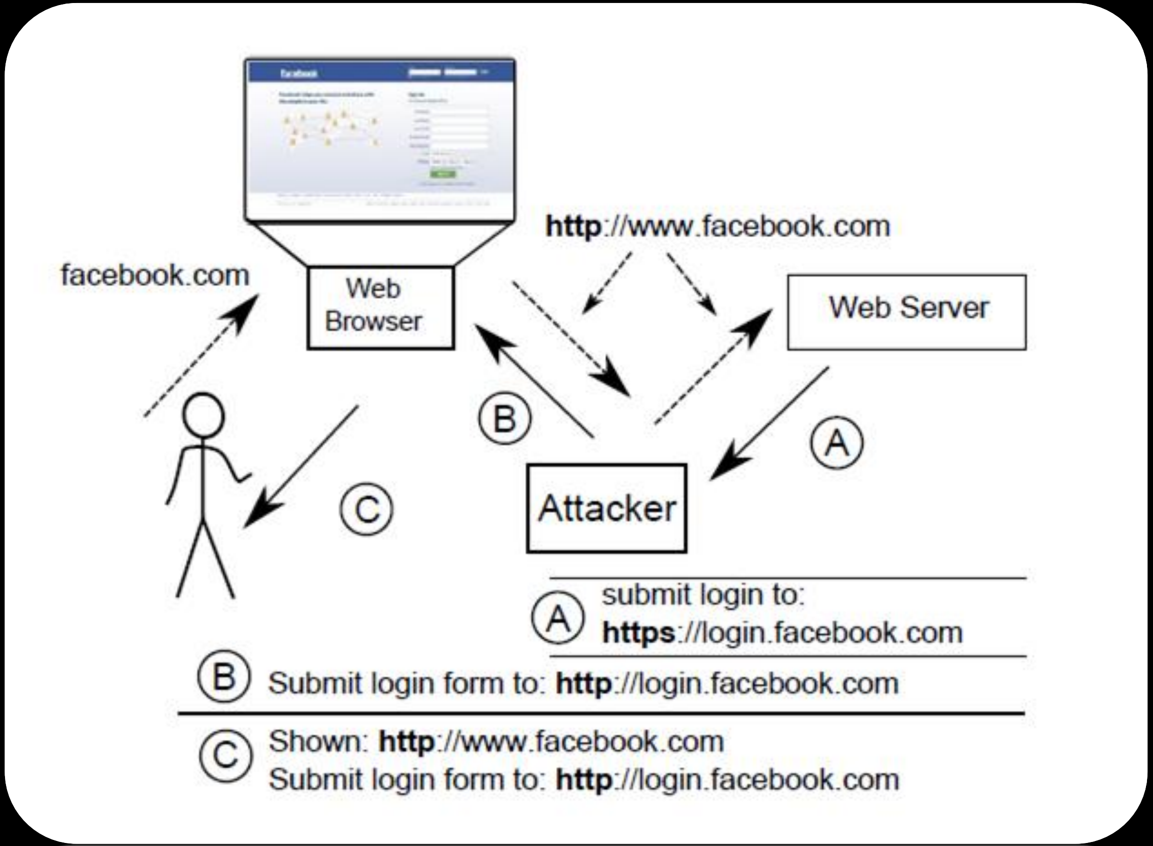
```
<form id="login_form"
action="https://www.facebook.com/login.php?login_attempt=1"
method="post“
…
```

under SSL Stripping Attack



```
<form id="login_form"
action="http://www.facebook.com/login.php?login_attempt=1" method="post“
…
```

How the Attack Works



Ⓐ submit login to: **https**://login.facebook.com

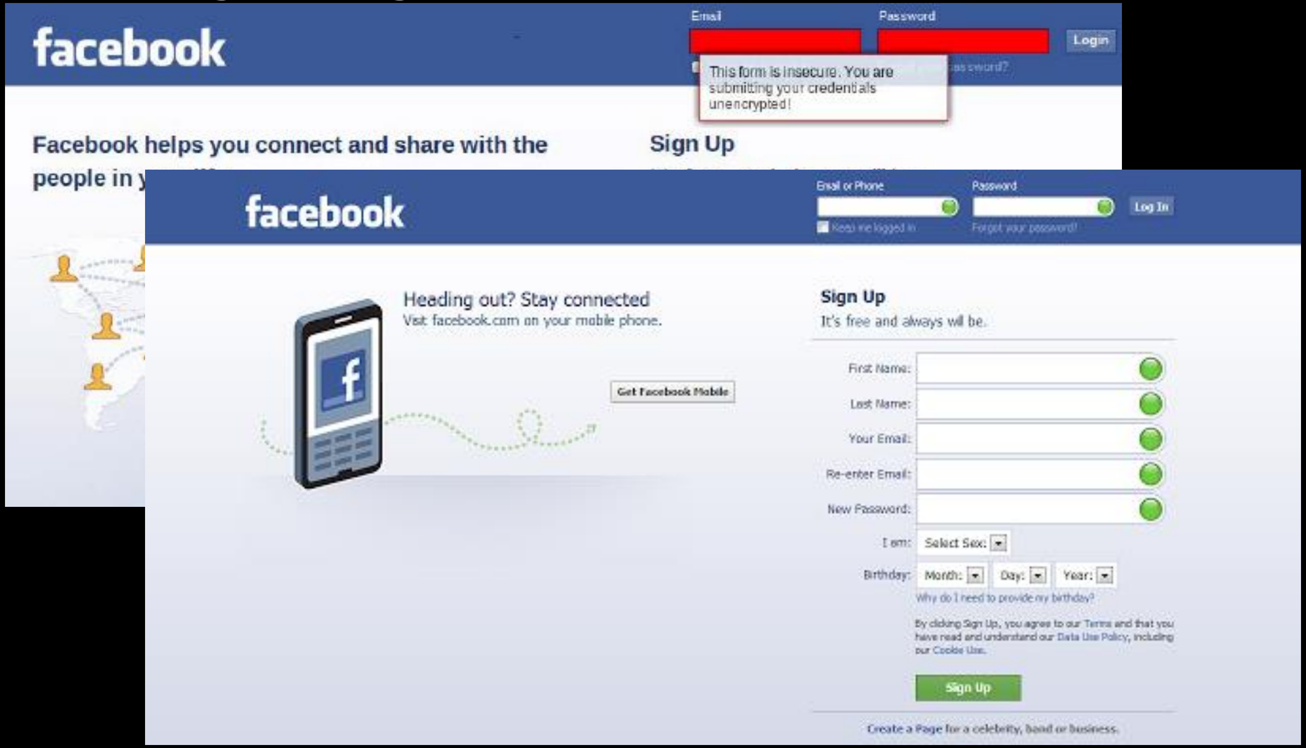
Ⓑ Submit login form to: **http**://login.facebook.com

Ⓒ Shown: **http**://www.facebook.com
Submit login form to: **http**://login.facebook.com

*In 2011 Facebook let you login from **http:**//www.facebook.com
Today Facebook redirects you to **https:**//www.facebook.com to login.

SSLight Browser Extension

Blinking Background



This form is insecure. You are submitting your credentials unencrypted!

Facebook helps you connect and share with the people in y

Heading out? Stay connected
Visit facebook.com on your mobile phone.

Sign Up
It's free and always will be.

By clicking Sign Up, you agree to our Terms and that you have read and understand our Data Use Policy, including our Cookie Use.

Create a Page for a celebrity, band or business.

Security Status Light (SSLight)

- Green light indicates form is secure.
- Red light indicates form is insecure.
- Yellow light indicates cases where SSL light cannot make a definite assertion.

SSLight allows you to easily check the security status of login forms. SSLight will identify, analyse, and label login forms so that you know when it is safe to submit your information

Experimental Design

100 Participants. 4 groups of 25

- Group 1: Exposed to the attack with no warning
- Group 2: Exposed to the attack with the standard pop-up warning dialog
- Group 3: Exposed to the attack with the SSLight warning in the login form fields
- Group 4: Exposed to the attack with the blinking background in the login form fields

User Study Hypotheses

1. General awareness of secure form submission	Confirmed
2. Effectiveness of SSLstripping	Confirmed – 0/25 noticed attack
3. Unhelpfulness of pop up warning method	Confirmed – 24/25 submitted form
4. Helpfulness of our visual cue-based methods	Confirmed – less submitted form
5. Effectiveness of both our different visual cue methods	Failed - 16/25 & 8/25 submitted

Criticism

- In the Background Section the article makes the following statements, which appear to contradict the goals of SSLight.

> “The general consensus is that security indicators that **rely** on the **user** to make a **correct decision** tend to be **ineffective** in [2, 3, 7].”

> “**Warnings** should be **avoided** when possible and **decisions** should be made for the user in an **automated**, under the hood fashion [17].”

Criticism

- In the Our Approach section the article declares the following benefits of SSLight, which appear to be in contrast to the statements in the Background section.

> “(SSLight) can be used to **help simplify** the **decision making** management for both lay and technically savvy users when they are about to submit their sensitive login credential.”

> “(SSLight) will better assist (users) to understand the current security situation that they are faced with and to make better, **more informed decisions** when they need to submit their sensitive information to a remote website.”

Criticism

- Is SSLight really helping users make better decisions?

“45% of the most popular websites still do not use HTTPS, not even for login purposes, as shown in a recent study [16].”

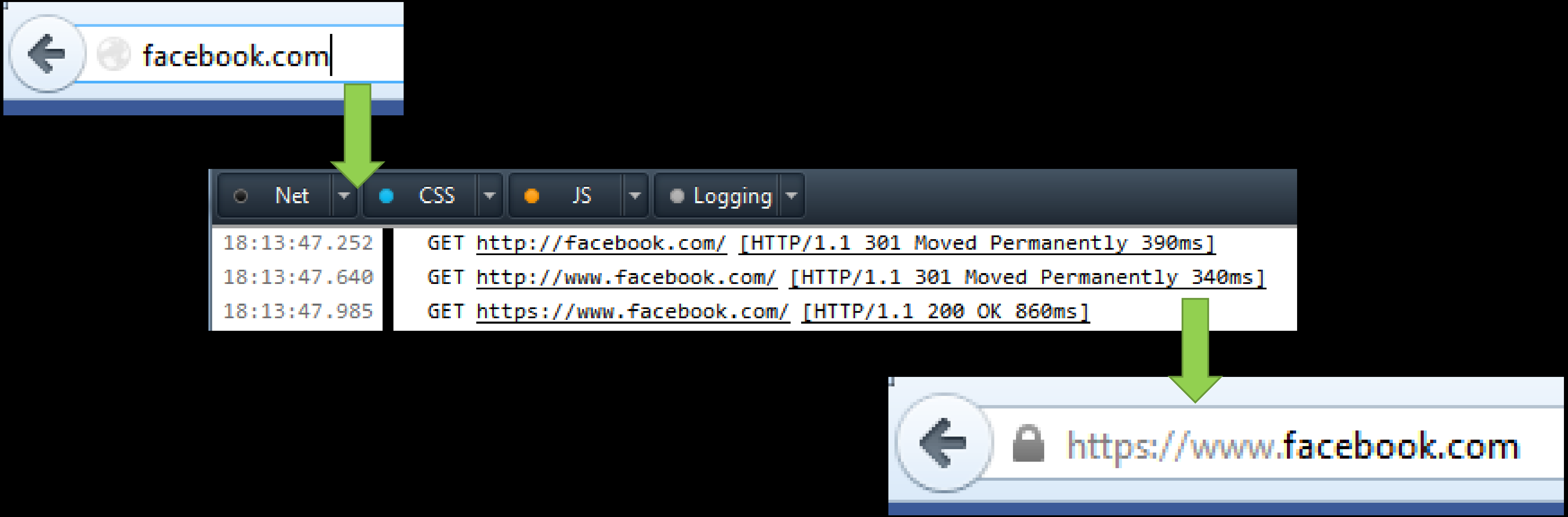
- Based on the SSLight algorithm, 45% of the most popular websites are going to get a Red Light. Will the user start ignoring SSLight if they are warned not to login to these popular websites?

Appreciation

- While SSLight mas not have been a success as a product – 76 users on Google Chrome – it may have helped draw attention to usability issues faced by browsers and flaws in SSL technology.
- Since the article was published in 2011, changes have been made to both web browsers and web sites such as Facebook to help prevent attacks.

Appreciation

- Facebook now requires users to login from a secure URL.
  - Though this does not stop the SSL Stripping attack.



facebook.com

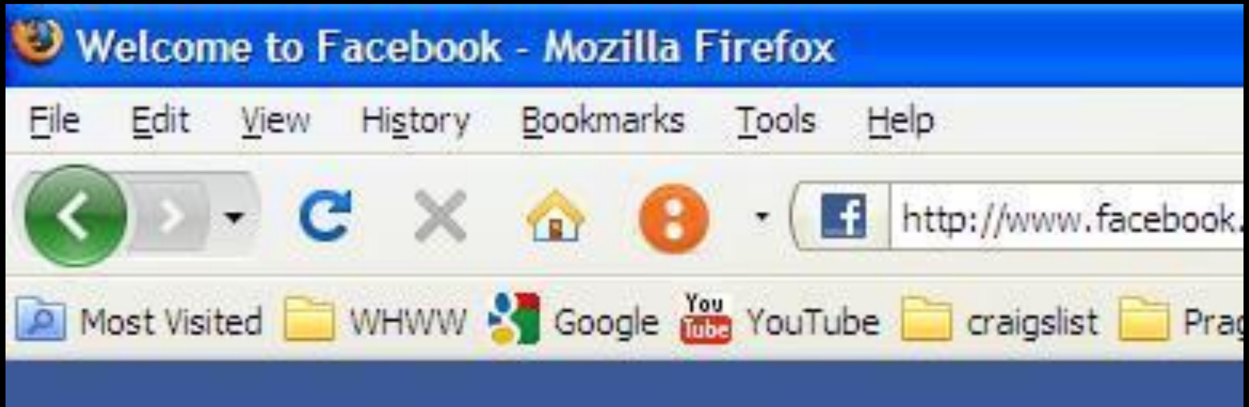
```
18:13:47.252    GET http://facebook.com/ [HTTP/1.1 301 Moved Permanently 390ms]
18:13:47.640    GET http://www.facebook.com/ [HTTP/1.1 301 Moved Permanently 340ms]
18:13:47.985    GET https://www.facebook.com/ [HTTP/1.1 200 OK 860ms]
```

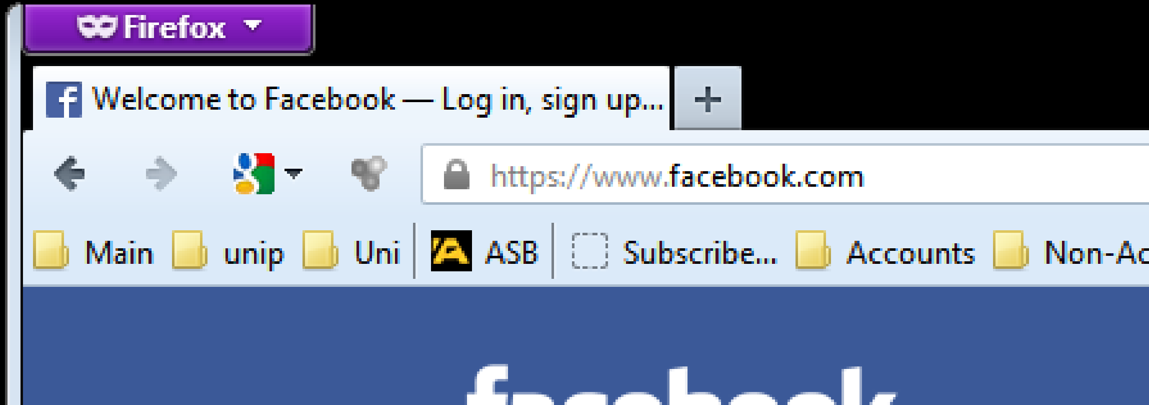
https://www.facebook.com

Appreciation

"it is important to notice that many browsers allow a page to display a small icon on the address bar, which can be made to look like a lock regardless of a secure connection being established or not."

- Out of IE 10, Firefox 23, Chrome and Safari, only IE still displays the favicon near the address bar.


Welcome to Facebook - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.facebook.
Most Visited
WHWW
Google
YouTube
craigslist
Prag



Question

- It can be difficult for the average user to notice whether their connection to a web server has been compromised in a web browser under an attack such as the SSL Stripping Attack. However there are clues in the address bar, presence of padlock icons, pop-up warnings and the HTML code itself.
- Are there any measures that could be taken in computer programs such as mobile phone apps, where the user logs in to a web service through the program itself rather than a browser, so that they can know they are logging in over a trusted connection?