Counting sheep:
Analysing online authentication security

M. (Marc) Sleegers, BA
mail@marcsleegers.com

dr. ir. H. L. (Hugo) Jonker
hugo.jonker@ou.nl

Introduction

Securely handling authentication cookies after the login process is vital. This was notably demonstrated by Eric Butler's Firesheep in 2010. Back then, it was extremely common for websites to protect passwords by encrypting the initial login but surprisingly uncommon for these sites to encrypt everything else. This left cookies extremely vulnerable and trivialised session hijacking. The fact that many wireless networks lacked any type of security was the cherry on top. By connecting to such networks Butler was able to capture all visible and insecure cookies easily. This allowed attackers to log in as someone else with a single click!

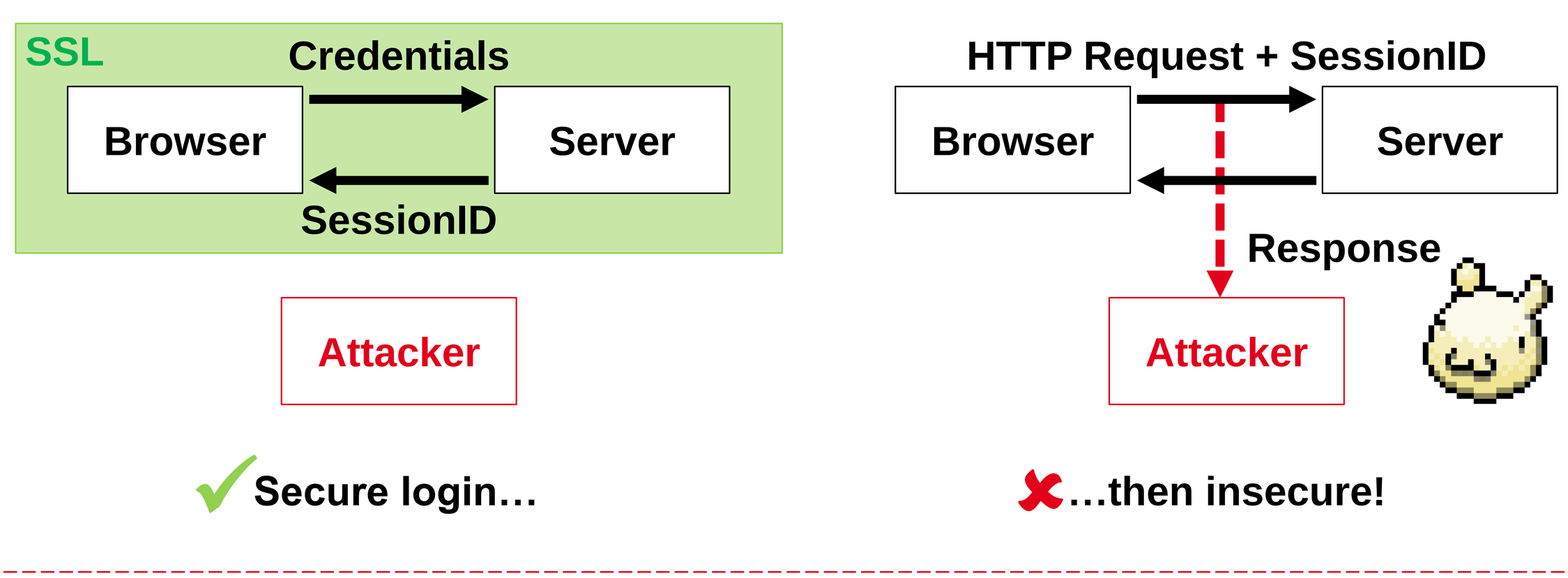
Beyond Firesheep

Firesheep is truly successful when it no longer works. Since 2010, it appears that a lot of progress has been made to this extent. Unfortunately, this may not have been enough. Mozilla warned for an increase in ‘secure login then insecure’ behaviour just earlier this year. This type of 'security' fails to protect the end users after authentication. In other words: sheep that must be herded.

Goal

This study will conclude the current state of (faux) web security.

Faux web security



✓ Secure login…

✘ …then insecure!

Research question

This study counts the sheep and measures how far online authentication security has really come since Firesheep in 2010. How widespread is the ‘secure login then insecure’ problem still?

Approach to herding the sheep

1. Identify test cases using existing techniques (e.g. Firesheep) and investigate account creation processes on a handful of sites.
2. Develop proof-of-concept webscraper (e.g. based on Selenium + Scrapy). The scraper will be able to automatically register and login using existing (e.g. sourced from BugMeNot) or new (e.g. using Mailinator) credentials.
3. Following local testing, we will first run a limited field test to verify functionality in a laboratorium setting.
4. Finally, we will count the sheep by analysing the top 1 million Alexa sites and default installs of the top 10 site creation tools.

Department of Computer Science, Open Universiteit