Securing the Web Platform

Collin Jackson
Stanford University
The Web Platform

- Pages
- Dynamic Interactive
- Web Applications
- Ubiquitous Instant updates
- Programs
The Web in 1996

- A security policy is born
- One page, one principal
The Web in 2009

- Many tabs
- Many sources of content
- Concurrent sessions
Meet the Web Attacker

A server with an introduction
Non-Assumption

"The user is confused"


Collin Jackson, Dan Simon, Desney Tan, and Adam Barth. An Evaluation of Extended Validation and Picture-in-Picture Phishing Attacks (USEC 2007)
The Web Attacker wants:

- Your pixels
- Your keystrokes
- Your messages
- Your session
- Your browsing history
- Your IP address
A blacklist approach?
Servers are cheap

- Domain and hosting: $10
- Domain-validated HTTPS: $0
- Targeted introductions $1 per 2000
Value of an introduction
Leveraging the Introduction

- Your pixels
- Your keystrokes
- Your messages
- Your session
- Your browsing history
- Your IP address


Helen J. Wang, Xiaofeng Fan, Jon Howell, and Collin Jackson. Protection and Communication Abstractions for Web Browsers in MashupOS. (SOSP 2007)


Adam Barth, Collin Jackson, and John C. Mitchell. Robust Defenses for Cross-Site Request Forgery (CCS 2008)

Collin Jackson, Andrew Bortz, Dan Boneh, and John C. Mitchell. Protecting Browser State from Web Privacy Attacks (WWW 2006)

Collin Jackson, Adam Barth, Andrew Bortz, Weidong Shao, and Dan Boneh. Protecting Browsers from DNS Rebinding Attacks (CCS 2007)
Web Attacker vs. Keystrokes

Adoption:
Web Attacker vs. Messages

- Could hijack frames and read their secret messages
- Proposed a revised protocol
- Adoption:
Web Attacker vs. Sessions
Understanding Referer Privacy
Stronger Threat Models

- Network attacker

Collin Jackson and Adam Barth. ForceHTTPS Cookies: A Defense Against Eavesdropping and Pharming (WWW 2008)

Collin Jackson and Adam Barth. Beware of Finer-Grained Origins (W2SP 2008)

- Malware containment

Collin Jackson, Dan Boneh, and John C. Mitchell. Transaction Generators: Rootkits for the Web (HotSec 2007)

Adam Barth, Collin Jackson, Charles Reis, and the Google Chrome Team. The Security Architecture of the Chromium Browser (Tech Report)
The Web in 2019

- Cheaper introductions
- Less confusing authentication
- Different problems, same Web Attacker