Timing is Everything — the Importance of History
Detection

Gunnar Kreitz

KTH – Royal Institute of Technology
gkreitz@kth.se

ESORICS 2011, September 12
Attack Demonstration
Introduction

Background

Flow Stealing

Attack Outline

Key Attack Pieces

Attack Demonstration

UR THEORY HAS MERIT – Lolcats 'n' Funny Pictures of Cats – I Can Has Cheezburger?


Previous | Stay Home K? I dont fart, pleez Next |

Search

Follow or Fan Us

Subscribe by email:

Enter email

Popular Videos

The Kittens of...

VIDEO: Baby Sloth...

Gunnar Kreitz

Timing is Everything
Introduction
Background
Flow Stealing

Attack Outline
Key Attack Pieces

Attack Demonstration

*Works equally well with other navigation (bookmark, link, ...)

Gunnar Kreitz
Timing is Everything
Attack Demonstration
Introduction

Background

Flow Stealing

Attack Outline

Key Attack Pieces

Attack Demonstration

Timing is Everything
Attack Demonstration

A Google approach to email.

Gmail is built on the idea that email can be more intuitive, efficient, and useful. And maybe even fun. After all, Gmail has:

- **Lots of space**
  - Over 7623.960111 megabytes (and counting) of free storage.

- **Less spam**
  - Keep unwanted messages out of your inbox.

- **Mobile access**
  - Get Gmail on your mobile phone. Learn more

New to Gmail? It's free and easy.

© 2011 - Gmail for Organizations - Terms & Privacy - Help
Attack Summary

- Evil tab was able to control victim tab
- Even after user had navigated victim tab manually
- Was able to control timing to when user navigated to site
- Multiple attack scenarios building on this
- Intercepts user’s browsing flow: *Flow Stealing*
How the Redirect Works

- Evil tab runs malicious JavaScript
- Victim tab is opened from Evil tab
- Evil tab retains a JavaScript window handle
- Via window handle, Evil tab can navigate Victim tab
- No restrictions on such navigation, except in Opera
How does the Evil Tab Know when to Redirect?

- Evil tab needs to know when to redirect
- Fairly easy if it can see victim’s network traffic
- (Actually easier than in paper - use XHR Level 2)
- In most web attacks, we cannot see victim’s network traffic
- What can we learn from history?
A history detection attack allows attacker to test if victim has visited some URL.

Violates visitor’s privacy expectation:
- Did you visit competitor’s site?
- What are your surfing habits?
- Where do you live (did you check out the weather in Stockholm) [Janc, Olejnik’10]?
Did you watch porn?

GOOD BOY! YOU DIDN'T WATCH ANY PORN RECENTLY.
Unless, of course, we are **wrong**.

Now find out [what your friends watched](http://didyouwatchporn.com) :)

♥ brought to you by [didnbns.com](http://didnbns.com) ♥
A Historical History Detection Attack

- CSS history detection is a well known attack
- Visited links are rendered differently from unvisited
- evil.com wants to know if visitor has visited gmail.com
  - Use CSS to make visited links render differently from unvisited
  - Add link to gmail.com
  - Have JavaScript that determines how link was rendered
History of the attack

Bugzilla@Mozilla – Bug 57351

Bug 57351 - css on a:visited can load an image and/or reveal if visitor been to a site

Last modified: 2009-10-17 23:04:06 PDT

Reported: 2000-10-19 16:57 PDT by Jesse Ruderman

Modified: 2009-10-17 23:04 PDT (History)

CC List: 11 users (show)

Crash Signature:

Status: VERIFIED DUPLICATE of bug 147777

Product: Core

Component: Security

Version: Trunk

Platform: All

Importance: P3 major with 2 votes (vote)

Target Milestone: mozilla1.2alpha

Assigned To: Mitchell Stoltz (not reading bugmail)

QA Contact: ckritzer (gone)

URL: http://gemal.dk/browserspy/css.html

Duplicates: 427944 (view as bug list)

Depends on:

Blocks:

Show dependency tree / graph

Attachments
History of the attack

Bugzilla@Mozilla – Bug 57351

**Bug 57351 – css on a:visited can load an image and/or reveal if visitor been to a site**

Last modified: 2009-10-17 23:04:06 PDT

Status: VERIFIED DUPLICATE of bug 147777

Whiteboard: privacy, testcase

Keywords: Security, TexteCase

Product: Core

Component: Security

Version: Trunk

Platform: All

Importance: P3 major with 2 votes (vote)

Target Milestone: mozilla1.2alpha

Assigned To: Mitchell Stoltz (not reading bugmail)

QA Contact: ckritzer (gone)

URL: http://gemal.dk/browserspy/css.html

Reported: 2000-10-19 16:57 PDT by Jesse Ruderman

Modified: 2000-10-19 16:57 PDT (History)

CC List: 11 users (show)

See Also:

Crash Signature:
Plugging the CSS History Detection Hole

▶ A solution was proposed in [Baron ’10]
  ▶ Lie to JavaScript about link colors
  ▶ Restrict what rendering visited can affect (timing attacks, etc.)
▶ Now used in latest versions of most major browsers
▶ …but not Opera or IE8 (last for Windows XP)
From Past to Present

- How to use this to time our attack?
- Polling!
- Periodically test target URLs
- When one becomes visited, trigger redirect
Limitations

- Can only trigger on URLs which
  - we can guess (no long, random parameter)
  - start out unvisited (!)
- CSS History Detection is patched in most browsers
- Seems difficult to build on other history detection attacks
  - Cache timing attacks are one-shot
  - Attacks where user is involved are too slow
Preventing Future Flow Stealing

- Even without history detection, network attacks still work
- Can we prevent the actual redirection?
- Yes, updating JavaScript window handle navigation policy
- Opera restrict cross-site navigation when current page in victim tab uses https
Proposed new JavaScript Policy

▶ What is an appropriate policy for when a tab can navigate another?
Proposed new JavaScript Policy

- What is an appropriate policy for when a tab can navigate another?
- Should correspond to users’ expectations for when pages can be changed
- Proposal: re-use Popup-blocker policy
- All browsers have one
- Appears to work reasonably well in practice
Summary

- Flow stealing — new type of attack
- New use of history detection
- Suggested stricter JavaScript window navigation policy
Thank you! Questions?
gkreitz@kth.se