Timing is Everything — the Importance of History Detection

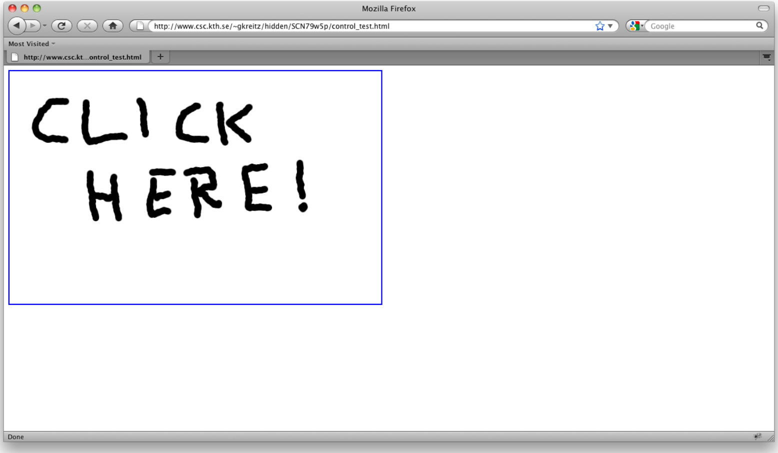
Gunnar Kreitz

KTH – Royal Institute of Technology
gkreitz@kth.se

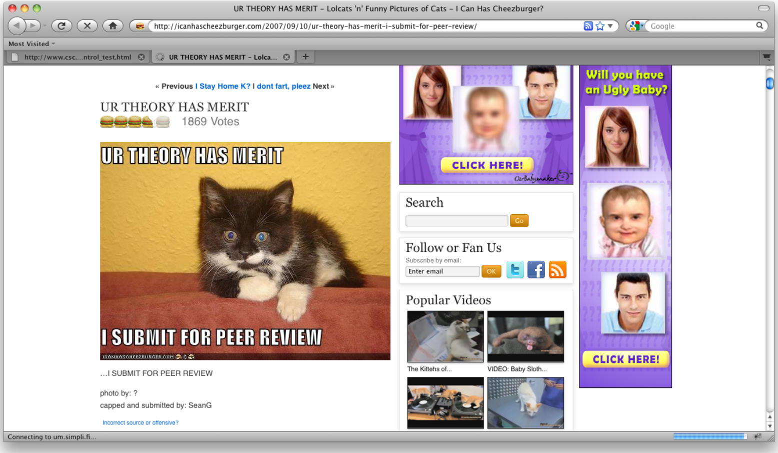
ESORICS 2011, September 12

KTH Computer Science and Communication

Attack Demonstration


Mozilla Firefox
http://www.csc.kth.se/~gkreitz/hidden/SCN79w5p/control_test.html
Google
Most Visited
http://www.csc.kt...ontrol_test.html
+
CLICK
HERE!
Done

Attack Demonstration



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

http://icanhascheezburger.com/2007/09/10/ur-theory-has-merit-i-submit-for-peer-review/

« Previous I Stay Home K? I dont fart, pleez Next »

UR THEORY HAS MERIT

1869 Votes

...I SUBMIT FOR PEER REVIEW

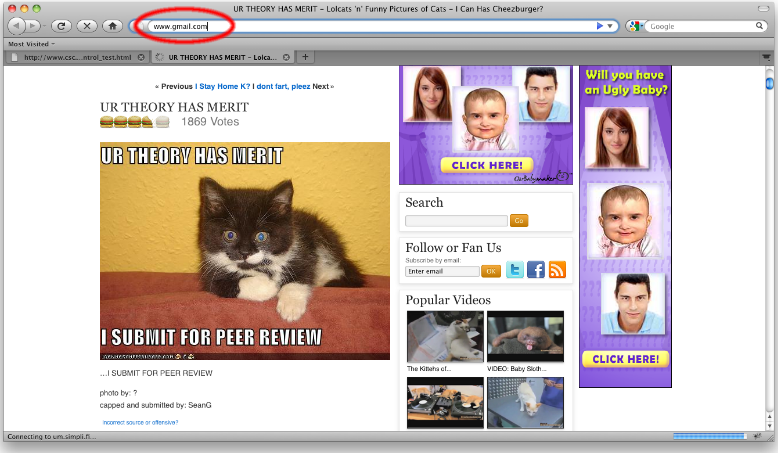
photo by: ?

capped and submitted by: SeanG

Incorrect source or offensive?

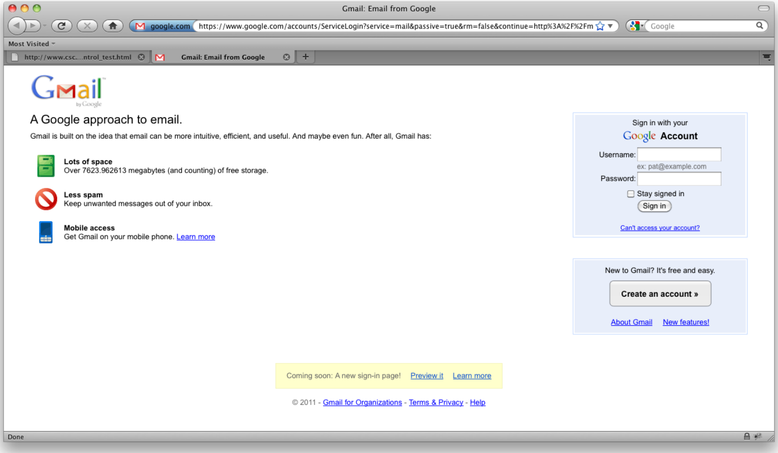
Connecting to um.simpli.fi...

Attack Demonstration


UR THEORY HAS MERIT – Lolcats 'n' Funny Pictures of Cats – I Can Has Cheezburger?
www.gmail.com
Google
Most Visited
http://www.csc....ntrol_test.html
UR THEORY HAS MERIT – Lolca...
« Previous I Stay Home K? I dont fart, pleez Next »
UR THEORY HAS MERIT
1869 Votes
UR THEORY HAS MERIT
I SUBMIT FOR PEER REVIEW
ICANHASCHEEZBURGER.COM
...I SUBMIT FOR PEER REVIEW
photo by: ?
capped and submitted by: SeanG
Incorrect source or offensive?
CLICK HERE!
Search
Go
Follow or Fan Us
Subscribe by email:
Enter email
OK
Popular Videos
The Kittehs of...
VIDEO: Baby Sloth...
Will you have an Ugly Baby?
CLICK HERE!
Connecting to um.simpli.fi...

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

Attack Demonstration


Gmail: Email from Google
google.com
https://www.google.com/accounts/ServiceLogin?service=mail&passive=true&rm=false&continue=http%3A%2F%2Fm
Google
Most Visited
http://www.csc....ntrol_test.html
Gmail: Email from Google
Gmail by Google
Done

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 7623.962613 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

Sign in with your
Google Account

Username:
ex: pat@example.com
Password:
□ Stay signed in
Sign in

Can't access your account?

New to Gmail? It's free and easy.

Create an account »

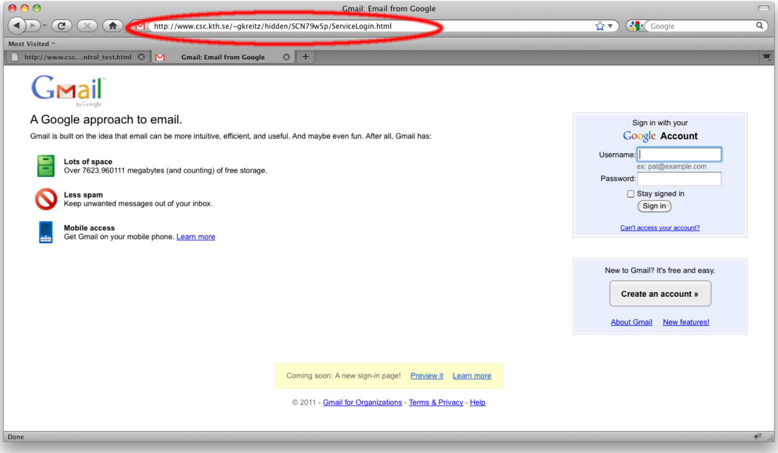
About Gmail New features!

Coming soon: A new sign-in page! Preview it Learn more

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

KTH Computer Science and Communication

Attack Demonstration



Gmail: Email from Google
http://www.csc.kth.se/~gkreitz/hidden/SCN79w5p/ServiceLogin.html
Google
Most Visited
http://www.csc....ntrol_test.html
Gmail: Email from Google
Gmail by Google
Done

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

Sign in with your
Google Account

Username:
ex: pat@example.com
Password:
□ Stay signed in
Sign in
Can't access your account?

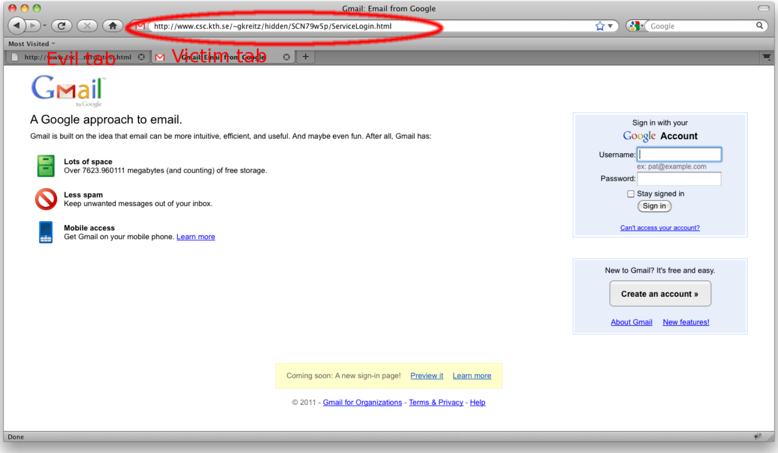
New to Gmail? It's free and easy.
Create an account »
About Gmail New features!

Coming soon: A new sign-in page! Preview it Learn more

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

KTH Computer Science and Communication

Attack Demonstration



http://www.csc.kth.se/~gkreitz/hidden/SCN79w5p/ServiceLogin.html

http://www.csc...ntrotest.html

Gmail: Email from Google

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

Sign in with your
Google Account

Username:
ex: pat@example.com
Password:
□ Stay signed in
Sign in
Can't access your account?

New to Gmail? It's free and easy.
Create an account »
About Gmail New features!

Coming soon: A new sign-in page! Preview it Learn more

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

KTH Computer Science and Communication

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*

KTH Computer Science and Communication

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?

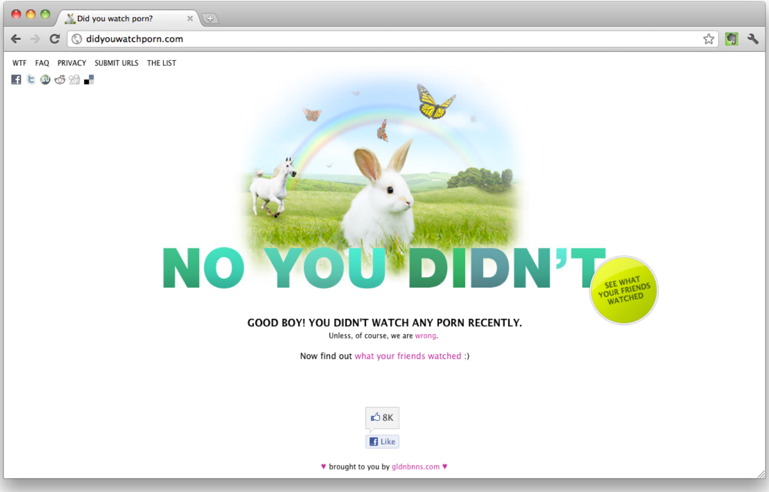
Photo by Earls37a `http://www.flickr.com/photos/indraw/4857101224/`, CC BY SA 2.0

History Detection

- 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]?

KTH Computer Science and Communication

Did you watch porn?



Did you watch porn?
didyouwatchporn.com
WTF FAQ PRIVACY SUBMIT URLS THE LIST
NO YOU DIDN'T
SEE WHAT YOUR FRIENDS WATCHED
8K
Like

GOOD BOY! YOU DIDN'T WATCH ANY PORN RECENTLY.

Unless, of course, we are wrong.

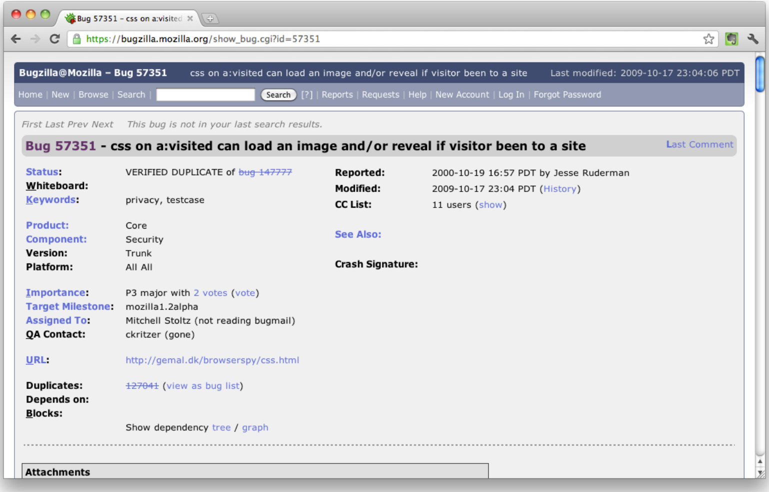
Now find out what your friends watched :)

♥ brought to you by gldnbnns.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 form unvisited
  - Add link to `gmail.com`
  - Have JavaScript that determines how link was rendered

History of the attack


Bug 57351 – css on a:visited
https://bugzilla.mozilla.org/show_bug.cgi?id=57351
Home | New | Browse | Search | Search [?] | Reports | Requests | Help | New Account | Log In | Forgot Password

Bugzilla@Mozilla – 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

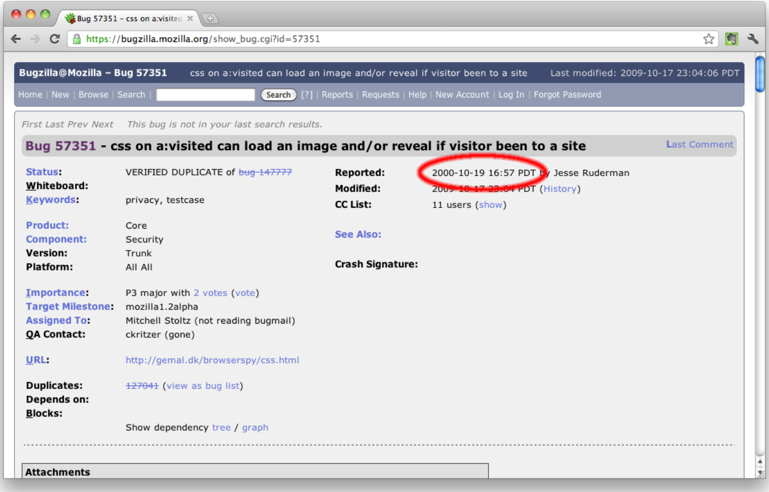
First Last Prev Next This bug is not in your last search results.

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

Status:	VERIFIED DUPLICATE of ~~bug 147777~~	**Reported:**	2000-10-19 16:57 PDT by Jesse Ruderman
Whiteboard:		**Modified:**	2009-10-17 23:04 PDT (History)
Keywords:	privacy, testcase	**CC List:**	11 users (show)
Product:	Core		
Component:	Security	**See Also:**	
Version:	Trunk		
Platform:	All All	**Crash Signature:**	
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:	~~127041~~ (view as bug list)		
Depends on:			
Blocks:			
	Show dependency tree / graph		

Attachments

History of the attack


Bug 57351 – css on a:visited
https://bugzilla.mozilla.org/show_bug.cgi?id=57351

Bugzilla@Mozilla – 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

Home | New | Browse | Search | Search [?] | Reports | Requests | Help | New Account | Log In | Forgot Password

First Last Prev Next This bug is not in your last search results.

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

Status: VERIFIED DUPLICATE of ~~bug 147777~~
Whiteboard:
Keywords: privacy, testcase

Product: Core
Component: Security
Version: Trunk
Platform: All 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: ~~127041~~ (view as bug list)
Depends on:
Blocks:
Show dependency tree / graph

Reported: 2000-10-19 16:57 PDT by Jesse Ruderman
Modified: 2009-10-17 23:04 PDT (History)
CC List: 11 users (show)

See Also:

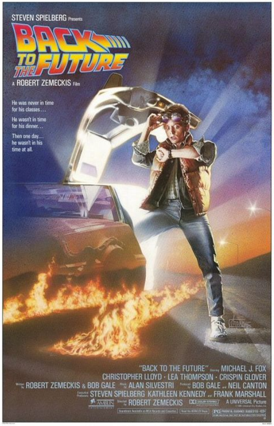
Crash Signature:

Attachments

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


STEVEN SPIELBERG Presents
BACK TO THE FUTURE
A ROBERT ZEMECKIS Film
He was never in time for his classes...
He wasn't in time for his dinner...
Then one day... he wasn't in his time at all.
"BACK TO THE FUTURE" MICHAEL J. FOX
CHRISTOPHER LLOYD · LEA THOMPSON · CRISPIN GLOVER
ROBERT ZEMECKIS & BOB GALE ALAN SILVESTRI BOB GALE NEIL CANTON
STEVEN SPIELBERG KATHLEEN KENNEDY FRANK MARSHALL
ROBERT ZEMECKIS
A UNIVERSAL Picture

- How to we 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

KTH Computer Science and Communication

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

KTH Computer Science and Communication

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

KTH Computer Science and Communication

Thank you! Questions?

`gkreitz@kth.se`

KTH Computer Science and Communication