Clickjacking: An empirical study with an automated testing/detection system

Marco `embyte` Balduzzi
iSecLab @ EURECOM

http://www.iseclab.org/people/embyte

OWASP
BeNeLux 2010

The OWASP Foundation
http://www.owasp.org

Introduction

Robert Hansen and Jeremy Grossman (Sept. 2008)

- SQL injections and XSS are much older...

Has received a wide media coverage by the security industry and the web community

- Forums, blogs, mailing-list, etc..

Google: 386,000 entries in the last 3 months

Is Clickjacking a real threat for Internet users?

How many “clickjacked” pages are out there?

Clickjacking

Web Vulnerability for benign and malicious sites

Construct a malicious web-page to trick their visitors into performing unintended clicks that results in malicious actions:

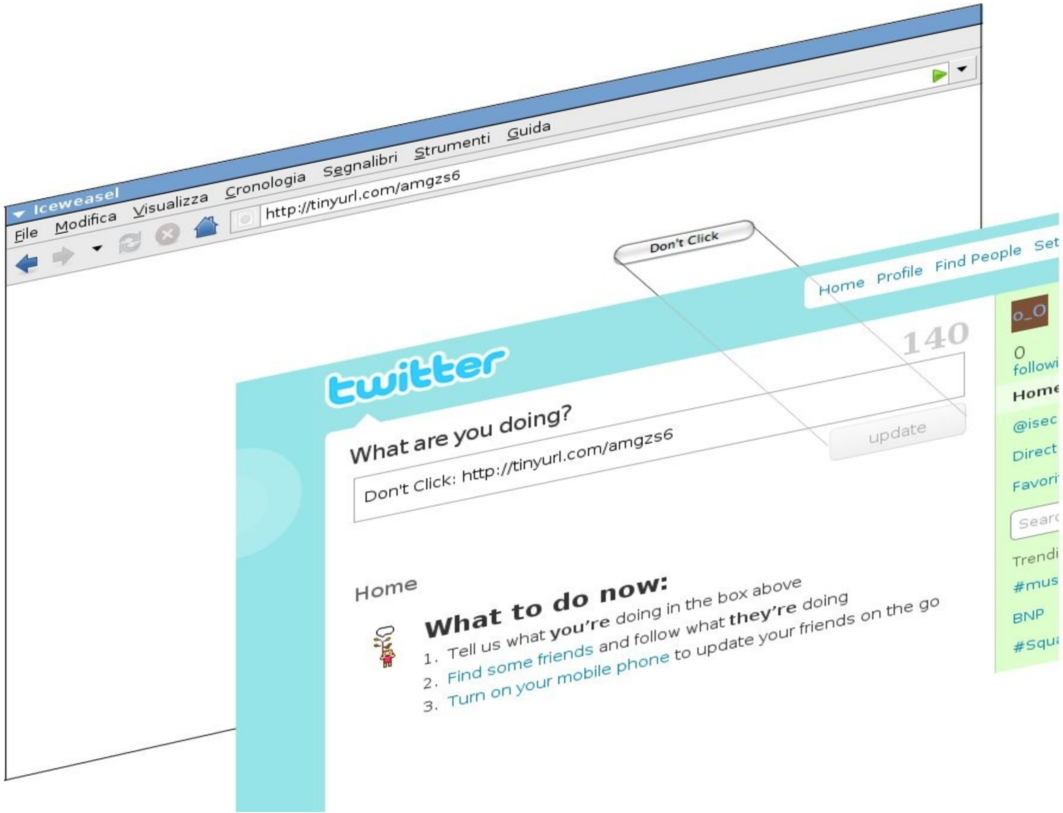
- Propagate worms, steal confidential information (passwords, session cookies), send spam, delete personal e-mails, etc...

XSS vulnerabilities can be exploited to run Clickjacking attacks by injecting malicious FRAMEs

Clickjacking in examples: the “Twitter bomb”

Abuse some HTML/CSS features (transparent IFRAMEs)

```
<IFRAME style={z-index:2; opacity:0; filter:alpha(opacity=0); }
scrolling=”no” src=”http://www.twitter.com/?status=Don't Click: http://tinyurl.com/amgzs6" >
```



What are you doing?

Don't Click: http://tinyurl.com/amgzs6

Home

What to do now:

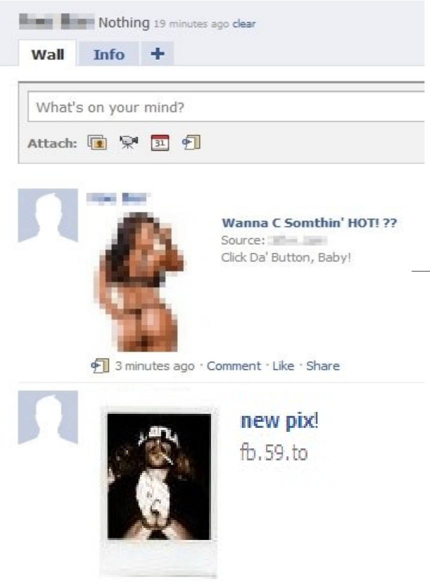
1. Tell us what you're doing in the box above
2. Find some friends and follow what they're doing
3. Turn on your mobile phone to update your friends on the go

Iceweasel
File Modifica Visualizza Cronologia Segnalibri Strumenti Guida
http://tinyurl.com/amgzs6
Don't Click
Home Profile Find People Set
twitter
140
update
o_O
0 followi
Home
@isec
Direct
Favori
Searc
Trendi
#mus
BNP
#Squ

Self-replicating message that is twitter via Clickjacking

Harmless but could link to drive-by-download content

Clickjacking in examples: the Facebook worms



[redacted] Nothing 19 minutes ago clear

Wall Info +

What's on your mind?

Attach:

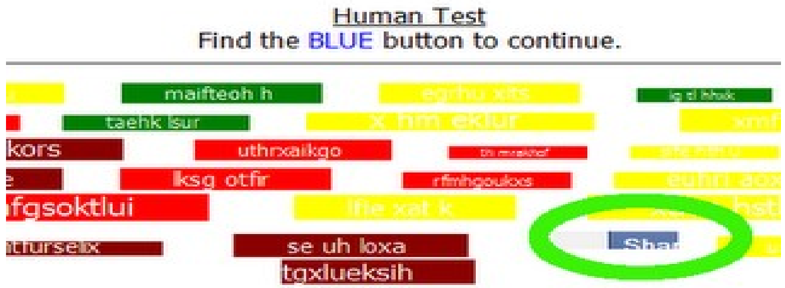
[redacted]

Wanna C Somthin' HOT! ??
Source: [redacted]
Click Da' Button, Baby!

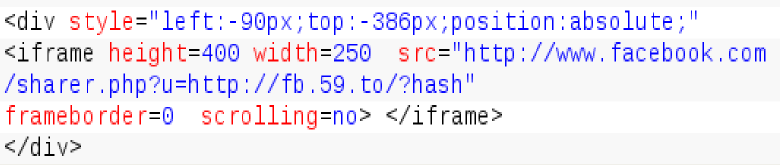
3 minutes ago · Comment · Like · Share

new pix!
fb.59.to

→

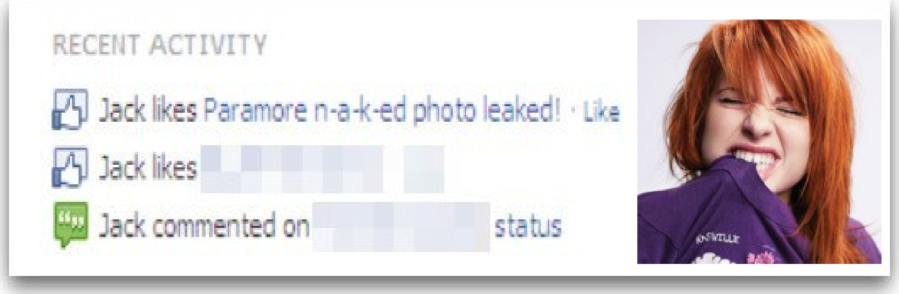


Human Test
Find the BLUE button to continue.



```
<div style="left:-90px;top:-386px;position:absolute;"
<iframe height=400 width=250  src="http://www.facebook.com
/sharer.php?u=http://fb.59.to/?hash"
frameborder=0  scrolling=no> </iframe>
</div>
```

→ Worm propagation



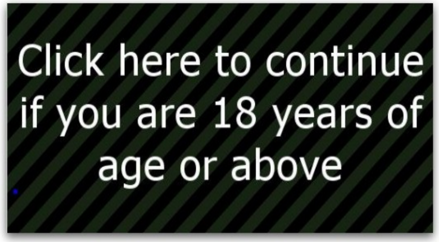
RECENT ACTIVITY

Jack likes Paramore n-a-k-ed photo leaked! · Like

Jack likes [redacted]

Jack commented on [redacted] status

→



Click here to continue if you are 18 years of age or above

→ Worm propagation

Motivation

Clickjacking has received a wide media coverage by the security industry and the web community,

but has not been studied before

Our goal

Determinate the prevalence of Clickjacking

on the Internet by analyzing online web pages

How?

Automated system for Testing live Internet sites and Detecting clickjacking attempts

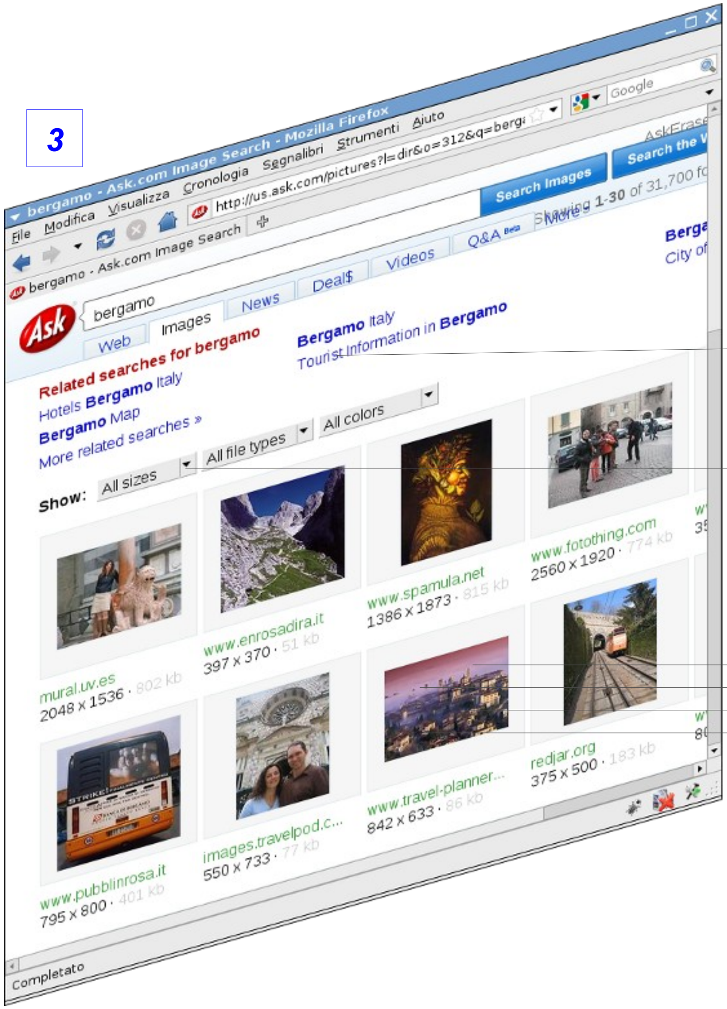
Automated testing

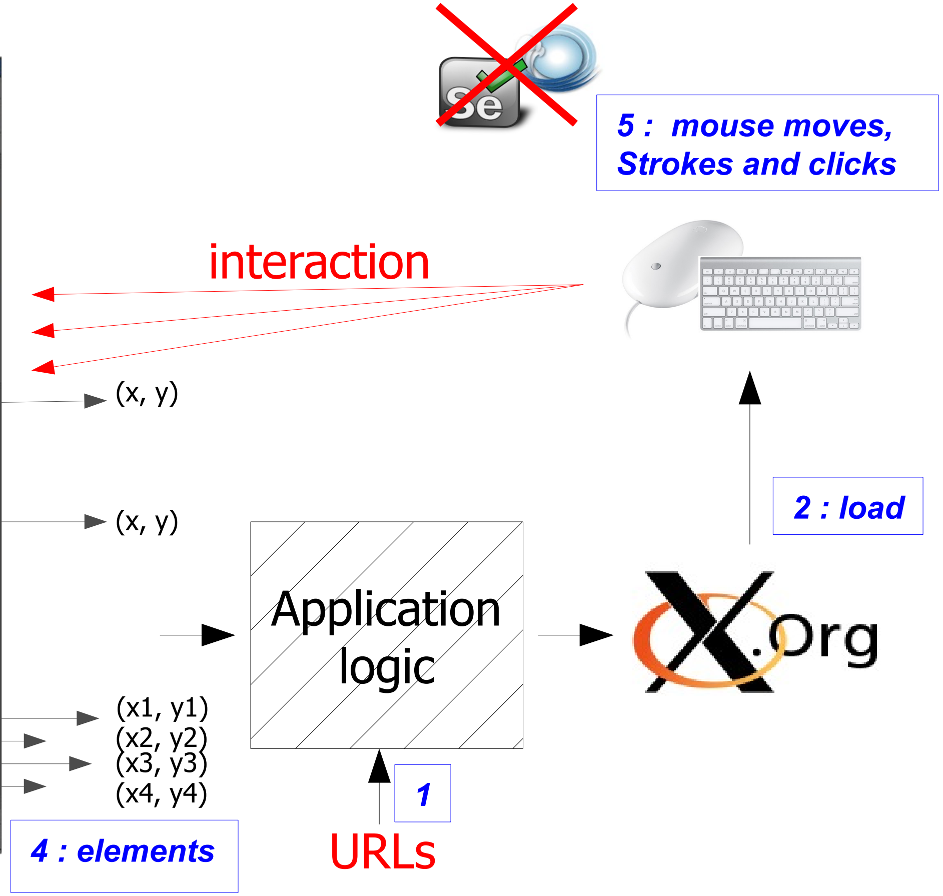
- Native browser (full languages support – e.g. Javascript)
- Instruct a browser to generate user-real actions:
  - Mouse clicks, movements, keyboard strokes
  - Opening new web-pages
  - X.Org support

Efficient detection

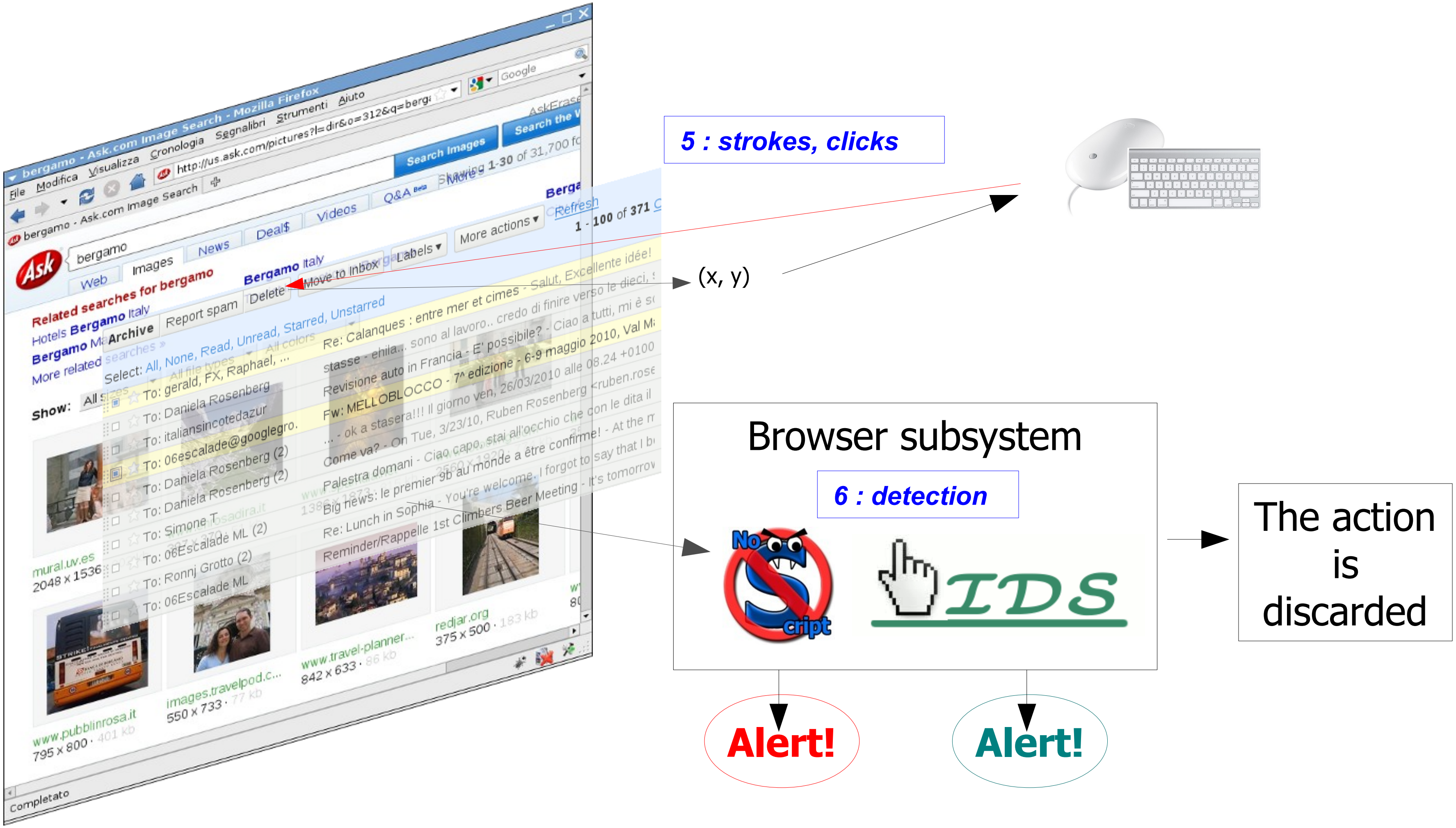
- Analyze the clicks with two independent browser extensions: NoScript and ClickIDS
- Reduction of False Positives

Page loading and Elements extraction


3
bergamo - Ask.com Image Search - Mozilla Firefox
File Modifica Visualizza Cronologia Segnalibri Strumenti Aiuto
http://us.ask.com/pictures?l=dir&o=312&q=berg
Google
bergamo - Ask.com Image Search
Ask
bergamo
Search Images
Search the W
Web Images News Deal$ Videos Q&A
Showing 1-30 of 31,700 fo
Related searches for bergamo
Hotels Bergamo Italy
Bergamo Map
More related searches »
Bergamo Italy
Tourist Information in Bergamo
Show: All sizes All file types All colors
mural.uv.es 2048 x 1536 · 802 kb
www.enrosadira.it 397 x 370 · 51 kb
www.spamula.net 1386 x 1873 · 815 kb
www.fotothing.com 2560 x 1920 · 774 kb
www.pubblinrosa.it 795 x 800 · 401 kb
images.travelpod.c... 550 x 733 · 77 kb
www.travel-planner... 842 x 633 · 86 kb
redjar.org 375 x 500 · 183 kb
Completato



Actions and Detection



5 : strokes, clicks

(x, y)

Browser subsystem

6 : detection

The action is discarded

Alert!

Alert!

Data Sources

Initial seed of 70,000 unique URLs:

- Popular: Alexa's Top 1000
- Social-networks: 20.000 MySpace public profiles
- Google and Yahoo queries for malicious keywords (download warez, free ringtones, porn, etc...)
- Malicious domains for *malwaredomains.com*
- Phishing URLs from *PhishTank*

Fed into a crawler:

- Recursive form submissions and link extractions
- 1,065,420 web pages
- 830,000 unique domains

Set-ups

10 Linux Virtual Machines (VMWare Server)

2 months (71 days) → Testing speed: 15,006 pages/day

Statistics:

- 92% of the visited pages embeds clickable elements such as links and buttons
- 143 million clickable elements
- 37.3% IFRAMES (3.3% standard frames)

- 0.16% Transparent FRAMES

The Findings: True Positives

Identified two real-world clickjacking attacks

1) Click fraud: Tricks users into clicking on a transparent IFRAME that contains a concealed banner

2) Twitter attack: as in the example

Note> Anti-clickjacking defense in place:

(If page is Framed → substitute it with empty content)

Examples posted on security-related sites

Not aware of them. Detected automatically.

Detection	Total	True Positives	Borderlines	False Positives
ClickIDS	137	2	5	130
NoScript	535	2	31	502
Both	6	2	0	4

Discussion – False Positives

NoScript:

1. Pop-ups that appear in response to particular events
2. Iframed banners in the proximity of the click
3. Hidden Iframes located outside the page margins

ClickIDS:

1. Visible Iframes that overlap and contain clickable elements

Note> Observed multiple sites that were "Frame-defaced": A javascript loads the attacker page and displays it fullscreen

Detection	Total	True Positives	Borderlines	False Positives
ClickIDS	137	2	5	130
NoScript	535	2	31	502
Both	6	2	0	4

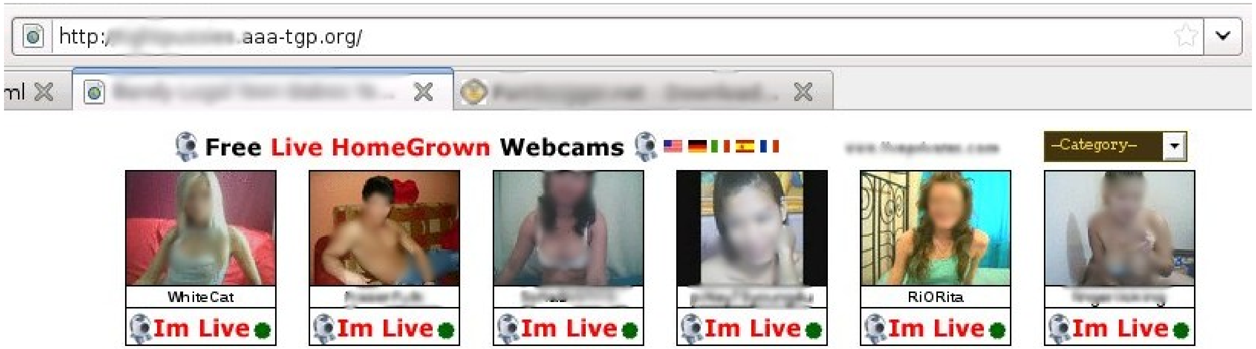
Discussion of Borderline Cases

Reverse Clickjacking

A cross-domain Iframe encapsulated into a link tag:

```
<A href="http://evil.com"><IFRAME src="http://site.com" /></A>
```

Users interact with the framed page *site.com* but the clicks are grabbed by the link tag and sent to *evil.com*



505 Frame

IFRAME with CSS-transparent background and no content

```
allowtransparency:true & background-color: transparent
```

Normally employed for banner or blogging systems

Looking at the future

Use of *Javascript* or *URL fragment identifiers* to accurately align the transparent IFRAME

Inject controlled text into a form field using the browser's drag-and-drop API (HTML5)

→ same-origin policy does not applied here

→ Java allow to override the default behavior → initiate the drag with a simple click

Steal the content (and HTML) of a cross-domain page

→ Stone, BH Europe 2010, Next generation clickjacking

Some mitigation techniques

1. The HTTP X-FRAME-OPTIONS header (proposed my Microsoft and adopted by IE8, Chrome, Opera, Safari, NoScript)

2. The use of *frame-busting:*

```
if (top.location.hostname != self.location.hostname)
                                        top.location.href = self.location.href;
```

   Thwarted by forcing IE to treat the site as restricted (javascript disabled)

   Other variants go around this issue [1]

   A recent paper discusses this problem in detail [2]

3. The *ClearClick* feature offered by NoScript or *ClickIDS*

4. CAPTCHA to protect sensitive actions

Summary of experiments

IFRAMES are largely adopted on the Internet and it seems that have overcome traditional frames

→ a new space vector?

Few transparent frames (~3%)

Despite of the wide media coverage, we observed very few clickjacked pages and a bunch of borderline cases

Clickjacking is not among the preferred attack vector adopted by miscreants on the Internet

It is complicated to setup and is not easily portable (different browsers / configurations render the page differently)

Conclusions

Motivations:

- Analyze a recent web threat that has received wide media coverage but has not been studied before

Approach:

- All-in-one solution for an automated testing and detection of clickjacking attacks

Experiments:

- Tested one million live web pages
- Found 2 real cases and some borderline attacks

Is <u>currently</u> Clickjacking posing an important threat for the Internet users?

Some references

More details on ClickIDS and our experiments:

→ A Solution for the Automated Detection of Clickjacking Attacks, Balduzzi et Al. , *http://www.iseclab.org/people/embyte/papers/asiaccs122-balduzzi.pdf*

Frame Busting research:

→ [1] Preventing Frame Busting and Click Jacking (UI Redressing*)* *http://coderrr.wordpress.com/2009/02/13/preventing-frame-busting-and-click-jacking-ui-redressing/*

→ [2] Busting Frame Busting: a Study of Clickjacking Vulnerabilities on Popular Sites *http://w2spconf.com/2010/papers/p27.pdf*

Examples of Clickjacking Attacks:

→ [X] Mahemoff, Explaining the "Don't Click" Clickjacking Tweetbomb, Febr. 2009, *http://softwareas.com/explaining-the-dont-click-clickjacking-tweetbomb*

→ [A] Krzysztof Kotowicz, New Facebook clickjacking attacks on the wil*d* *http://blog.kotowicz.net/2009/12/new-facebook-clickjagging-attack-in.html*

→ [B] Joey Tyson, Facebook worm uses clickjacking in the wil*d* *http://theharmonyguy.com/2009/11/23/facebook-worm-uses-clickjacking-in-the-wild*

→ [C] May 2010 Worms, Attack spreading through "likes" *http://mashable.com/2010/05/31/facebook-like-worm-clickjack/*

Clickjacking: An empirical study with an automated testing/detection system

Marco `embyte` Balduzzi
iSecLab @ EURECOM

http://www.iseclab.org/people/embyte

OWASP
BeNeLux 2010

QUESTIONS?

The OWASP Foundation
http://www.owasp.org