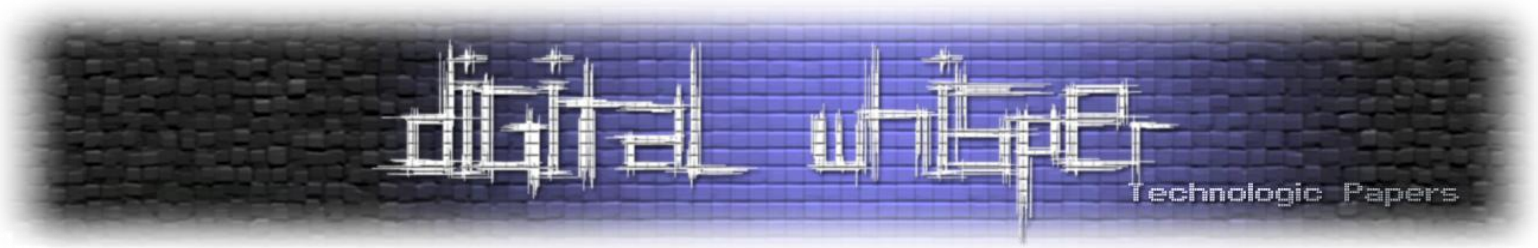


UI Redressing A.K.A. Clickjacking

מאת שלומי נרקולייב

(התמונה במקור: http://www.pc1news.com/articles-img/small/mouse.jpg)

הקדמה

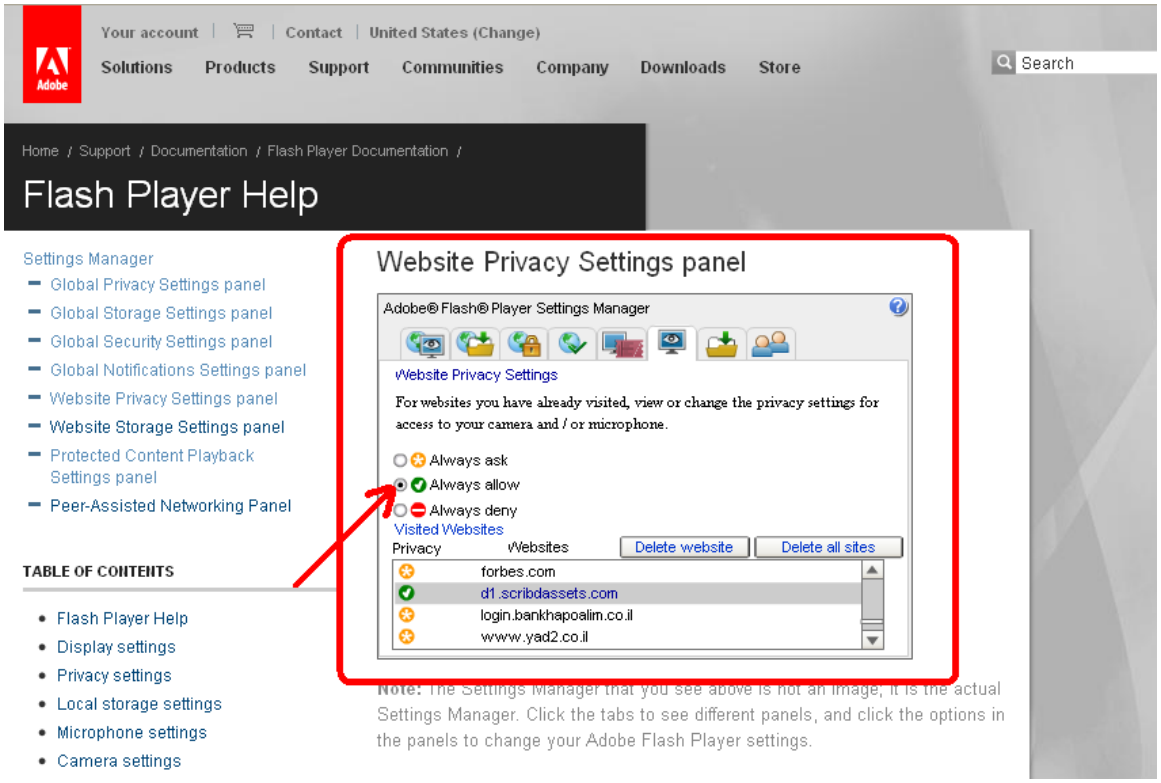
במאמר זה אציג בפניכם התקפה בשם UI Redressing (UI אלה ראשי תיבות של User Interface) הידועה גם כ-ClickJacking, בנוסף, אציג את היכולות אשר ניצול מוצלח של התקפה זו מקנות לתוקף, דוגמאות קוד, דרכי ההתמודדות הקיימים כיום ומספר עובדות נוספות.

ClickJacking היא טכניקה זדוניות אשר נועדה לגנוב את לחיצות העכבר (ניתן גם לנצל את המקלדת לטובת ההתקפה) של המשתמש על ידי הטעיית המשתמשים ושליחת לחיצות העכבר שלהם לטובת הפעלתם של פעולות שונות באתר, כגון: לחיצה על פרסומות בצד האתר, אישור פעולה אשר דורשת לחיצת עכבר (כדוגמת העברה בנקאית, רכישת/מכירת מניות וכדומה), או בעצם כל דבר אשר דורש לחיצה על כפתורים וקישורים. ברב המקרים, הדבר מתבצע בתוך IFrame מוסתר המצביע לאתר אחר בו המשתמש מנוי (קיימות טכניקות שונות על מנת לזהות האם המשתמש מבקר באתר מסויים, ואף האם הוא מזוהה ברגע זה לחשבונו באתר מסויים) ולבצע פעולות בתוך האפליקציה של האתר בשמו של הנתקף.

המונח "ClickJacking" נטבע על ידי חוקרי האבטחה ג'רמיה גרוסמן ורוברט הנסן (המוכר גם כ-RSnake) בשנת 2008 .

דוגמאות התקפה

1) Alice גולשת באתר של Eve אשר מכיל משחק בול פגיעה, Alice מחליטה לשחק בו. האתר של Eve פותח IFrame נסתר לאתר הגדרות של Flash ומאפשר את הפעלת המצלמה על ידי גורם שלישי במחשבה של Alice:



עכשיו Eve יכול לראות ולשמוע את Alice בלי רשותה.

התקפה זו עובדת אך רק על משתמשים בעלי Flash Player בעלי גרסה פחותה מ-9.0.124.0.
קישורים הקשורים לתרחיש התקפה זו:

- דמו: http://guya.net/security/clickjacking/game.html
- הסבר על ידי ג'רמיה גרוסמן: http://cnettv.cnet.com/clickjacking/9742-1_53-50072110.html

2) נשתמש באותה דוגמא של משחק בול פגיעה כמקודם, רק הפעם לא נפתח IFrame נסתר, אלא נגנוב כל לחיצה של המשמש ונפנה את הלחיצה על פרסומות שונות בדף.

כיום קיימות המון תוכניות של שיתוף Web Traffic, על כל הפנייה מקבלים סכום כסף מוגדר (תלוי בתחום האתר), כמו-כן ישנם המון חברות פרסום כגון Google AdWords ודומיו שמשלמים את רוב הכסף על לחיצה של המשתמש על הפרסומות - PPC (Pay Per Click).

בדרך כלל אתרים שיש להם המון מבקרים, עדיין אחוז ההקלקה על הפרסומות נמוך מאוד, עם שיטה זו בעלי האתרים יוכלו להגדיל/להגדיר את יחס ההקלקה וככל הנראה לעשות מיליונים ☺.

- דמו: http://narkolayev-shlomi.blogspot.com/2010/02/clickjacking-advertisement.html (בתחתית הדף יש דמו אינטרקטיבי.)

3) Eve מעוניין שמספר רב של משתמשי הרשת החברתית "פייסבוק" יתקינו את האפליקציה שלו אשר גונבת את פרטיהם הפרטיים למטרות ספאם, ביצוע סטאטיסטיקות, למטרות ביון/האזנה (על ידי אישור הפעלת המצלמה- כפי שתואר לעיל) ועוד.

כל שעליו לעשות זה לפתח תולעת אינטרנט שפותחת IFrame לפייסבוק. ה-IFrame צריך להיות מוסתר (בכדי שה"קורבנות" לא יראו על מה באמת הם לוחצים), על ה-IFrame הוא ישים תמונה מעניינת (תפעילו את הדמיון שלכם) ולכתוב מתחתיה "לחץ כאן לתמונות נוספות".

כל מי שילחץ על "לחץ כאן לתמונות נוספות", בעצם ילחץ על כפתור בתוך ה-IFrame הנסתר (שהוא עצמו עמוד באתר "פייסבוק") המורה להתקין את האפליקציה של Eve!

ובכדי שמתקפה זאת תיהיה באמת תולעת (הפצה עצמית לשאר חבריו של הקורבן) פשוט נבקש מהקורבן ללחוץ שוב פעם על הלינק (בעזרת תירוץ שונה), והפעם נשלח לכל חבריו ברשת לינק לאותו עמוד זדוני.

דמו: http://narkolayev-shlomi.blogspot.com/2010/01/clickjacking-facebook.html

- בדמו זה יש וידאו המתאר את ההתקפה. בתחתית הדף יש דמו אינטרקטיבי המאפשר לבעלי אתרים לבדוק אם האתר שלהם פגיע להתקפה זו.

שיטות הגנה

קיימות שתי גישות על מנת למנוע התקפות ClickJacking:

1) על ידי Client Side:
- למשתמשי דפדפן Firefox יש הרחבה בשם NoScript, אשר מתריעה ומונעת התקפות אלו.

2) על ידי Server Side:
- שימוש ב-HTTP Headers יעודיים:

X-FRAME-OPTIONS Header: מיקרוספוט פיתחה ארכיטקטורה המאפשרת למפתחי יישומי האינטרנט להשתמש ב-Header המורה לדפדפן אם לאפשר לדף מדומיין חיצוני להכניס דף זה ל-IFrame או לא.

דפדפים תומכים: IE8, Safari ו-Chrome.

- Frame Busting Code: ניתן לכתוב JavaScript פשוט שירוץ בעת העלאת דף אינטרנט אשר לא יאפשר להכניס דף זה לIFrame. קיימים שיכלולים לנושא, כמו למשל: דומיין חיצוני לא יוכל להכניס לIFrame דפים מהאפליקציה, אך דומיין פנימי כן יוכל – מתאים לאתרים שמבצעים כבר שימוש של IFrames באפליקציה.

דוגמא לסקריפט זה:

```
<script type="text/javascript">
      if(top != self) top.location.href = location.href;
</script>
```

מגבלות שיטות ההגנה

1) <u>על ידי Client Side:</u>

NoScript:

- לאחר שזיהה כי המשתמש לחץ על IFrame נסתר, יתריע בפני המשתמש – משתמש לא מנוסה יבטל את ההגבלה ובכל זאת ההתקפה תצליח.
- זוהי תוספת לדפדפן ולא פתרון מובנה. רוב המשתמשים בכלל לא מכירים תוספת זו או לא רוצים להשתמש בה מהיבטי Usability.

2) <u>על ידי Server Side:</u>

שימוש ב-Headers:

- רוב המשתמשים בעולם לא משתמשים ב-IE8 או בדפדפן החדש של Safari ו-Chrome ולכן מפתחי המערכות לא יכולים להיות בטוחים שהמערכת שלהם מוגנת.

Frame Busting Code:

תיאור מפורט יותר של הבעיות בשימוש ב-Frame Busting Code אפשר למצוא במצגת הבאה:

*http://*w2spconf.com/2010/slides/rydstedt.ppt

להלן מספר דוגמאות לשימוש במאפיין Security בדפדפני IE:

על ידי הגדרת מאפיין זה ב-IFrame ה-Frame Busting Script לא ירוץ.
הבעיה בשיטה זו היא שכל הסקריפטים האחרים גם לא ירוצו, עקב כך יחסמו שאר האפליקציות שמסתמכות על שימוש ב-JavaScript. תחביר:

```
<IFRAME SECURITY=restricted>
```

ניתן לבצע את אותו הדבר בעזרת שימוש במאפייני HTML5: Design mode ו-Sandbox, **מאפיינים אלו עובדים בכל הדפדפנים שתומכים ב-HTML5.**

דוגמא:

```
<iframe sandbox src="http://www.victim.com">
```

ניתן למנוע התקפת ClickJacking על ידי שימוש ב-"Security=Restricted" או בשימוש במאפייני HTML5 דומים על ידי הסתרת הדף בברירת מחדל, הצגת הדף תתבצע אך ורק על ידי ה-Script Busting Code, פעולה זו תבטיח את הרצת הסקריפט. גם שיטה זו ניתן לעקוף בקלות, אך זה כבר מירוץ התחמשות של יכולות ההגנה נגד יכולות ההתקפה שאותו לא אפרט במסמך זה.

להלן מספר דוגמאות:

1. **Double Framing:** ניתן להגדיר IFrame ובתוכו להגדיר IFrame נוסף אשר מצביע לאפליקציה המותקפת. במידה ומפתחי האפליקציה משתמשים ב-FrameBusting Code אשר פונה ל-Parent, הקוד לא ירוץ עקב הפרת אבטחה:

```
if(top.location!=self.location){
      parent.location = self.location;
}
```

2. **ניצול ה-XSS Filters של דפדפנים:**

IE8: על מנת שה-FrameBusting לא ירוץ, במידה וה-FrameBusting Code הוא:

```
<script>
      if(top!=self{
         top.location=self.location;
      }
</script>
```

התוקף יכול להגדיר את שדה ה-SRC של ה-IFrame לערך:

```
<iframe src="http://www.victim.com/?v=<script>if">
```

מה שיתקבל מכך, הוא זיהוי False Positive של ה-FrameBusting Code ע"י ה- XSS Filter הקיים בדפדפן IE8 וניטרולו.

3. **דריסת משתנה ה-Location:**

נקח לדוגמה את הקוד הבא:

```
if(top.location != self.location){
   top.location = self.location;
}
```

במידה ונגדיר:

```
<body>
<script>
      varlocation = "clobbered";
</script>
```

```
<iframe src="http://www.victim.com"></iframe>
</body>
```

הקוד שאחראי לבצע FrameBusting שהוגדר באתר Victim.com לא יעבוד!

בכדי לבצע דריסה ב-Internet Explorer 7:

```
var location = "clobbered";
```

בכדי לבצע דריסה ב-Safari:

```
window.__defineSetter__("location", function(){});
```

סיכום המגבלות של ה-Frame Busting Code:

1. המגבלות אשר הוצגו במאמר זה:
   - Double framing
   - Exploiting the XSS Filter
   - Clobbering top.location
   - IE Restricted Zone
   - Sandbox attribute
   - Design mode
   - Mobile Sites
2. מגבלות אשר לא הוצגו במאמר זה, אך צורפו לקישור חיצוני רלוונטי:
   - onBeforeUnload-204 Flushing
   - שימוש ב-onBeforeUnload להתקפות פישינג.
   - Referrer checking problems
   - "Ray of Light".

שימושים נוספים:

1. ניתן להשתמש בהתקפה זו באתרי אינטרנט אשר הותאמו במיוחד למכשירים סלולארים, להלן רשימת אתרים (לגלישה סלולארית) המתארת איזה מהאתרים משתמשים ב-FrameBusting Code:

Site	URL	Framebusting
Facebook	http://m.facebook.com/	YES
MSN	http://home.mobile.msn.com/	NO
GMail	http://m.gmail.com	NO
Baidu	http://m.baidu.com	NO
Twitter	http://mobile.twitter.com	NO
MegaVideo	http://mobile.megavideo.com/	NO
Tube8	http://m.tube8.com	NO
PayPal	http://mobile.paypal.com	NO
USBank	http://mobile.usbank.com	NO
First Interstate Bank	http://firstinterstate.mobi	NO
NewEgg	http://m.newegg.com/	NO
MetaCafe	http://m.metacafe.com/	NO
RenRen	http://m.renren.com/	NO
MySpace	http://m.myspace.com	NO
VKontakte	http://pda.vkontakte.ru/	NO
WellsFargo	https://m.wf.com/	NO
NyTimes	http://m.nytimes.com	Redirect
E-Zine Articles	http://m.ezinearticles.com	Redirect

(הרשימה המקורית פורסמה במצגת של Gustav Rydstedt, Elie Bursztein, Dan Boneh ו-Collin Jackson)

המסקנה מרשימה זו היא שניתן לעשות העברות כספים, גניבת זהות וכל פונקציונליות אחרת אותם מאפשרים אתרים אלו על משתמשים אשר גולשים דרך הפלאפון לאתרים אלו.

2. לאחרונה, Paul Stone פרסם בכנס BlackHat שיטה המשדרגת את יכולות ההתקפה של ClickJacking, הוא קרא לה: Drag&Drop. שימוש במתקפה זו משפרת את יכולות התוקף במספר היבטים, לדוגמה:
   - ניתן לרמות את המשתמשים ולגרום להם למלא טפסים **לפני** שליחת הבקשה לאפליקציה.
   - ניתן לרמות את המשתמשים ולגרום להם להוציא מידע מתוך האפליקציה: פרטים אישיים, Source Code וכו'.

מומלץ מאוד לעבור על המאמר של Paul Stone בכדי להבין לעומק את הרעיון.

לסיכום

כפי שאפשר לראות, זוהי התקפה ברמת חומרה זהה למתקפות Cross Site Request Forgery, החומרה היא ברמה **גבוהה**. חשוב לזכור שתנאי הכרחי להצלחת ההתקפה הוא שה"קורבן" יהיה מזוהה למערכת הפגועה או שיש לו Plugin בדפדפן המזין בצורה אוטומאטית את פרטי ההזדהות.

לפני כשלוש שנים Jeremiah Grossman כינה את CSRF כ-"The Sleeping Giant", לפי דעתי ClickJacking היא "הענק הרדום" של שנת 2010.
מה שמשותף לטכנולוגיה חדשה ולסוג חדש של התקפה הוא "זמן ספיגה". בשני המקרים הללו לעולם לוקח זמן-מה להבין את המשמעות, להעריך את הפוטנציאל ולקבל החלטות. לרוב, משך הזמן הזה הוא שנתיים. במקרה של ClickJacking, מכיוון שלא פשוט להגן על מתקפה זו בצורה הרמטית כך שלא תגרום למקרי False Positives או ל-False Negative "זמן הספיגה" גדל, לפי הערכתי ל-3 או 4 שנים(!).

"זמן ספיגה" זה גדול יחסית, מה שמאפשר, חלון זמן גדול לתוקפים לנצל את הפרצה ולשלשל לכיסם כספים ולחזק את יכולות ההתקפה שלהם.

אזכורים וסנפחים:

כתבות אודות פרצת ה-ClickJacking אשר שלומי מצא בפייסבוק:
כתבות בארץ:

http://www.calcalist.co.il/internet/articles/0,7340,L-3388723,00.html

כתבות בחו"ל:

http://blogs.zdnet.com/security/?p=5293&tag=content;col1
http://news.cnet.com/8301-27080_3-10436698-245.html

על המחבר:

שלומי נרקולייב הוא אבא גאה לשני ילדים, יוצא 8200, בעל תואר ראשון במדעי המחשב עם התמחות באבטחת מידע, הנדסאי אלקטרוניקה ובעל תשוקה עזה ליצירת פתרונות חדשניים.
מומחה אבטחת מידע, בעל נסיון למעלה מ-13 שנים בתחום הפריצה, האבטחה ופיתוח מערכות אבטחה.
שלומי שירת את המוסדות הגדולים בארץ, ייסד סטארט-אפ בתחום הפריצה למערכות.
כיום הוא עובד בחברת F5 Networks בתור מהנדס אבטחת מידע ואחראי על כלל פן האבטחה במוצר הפיירוול האפליקטיבי של F5.
חוקר ומוציא לאור מחקרים בתחום הפריצה ועקיפה בבלוג:

http://Narkolayev-Shlomi.blogspot.com

מידע נוסף:

http://blogs.msdn.com/b/ie/archive/2009/01/27/ie8-security-part-vii-clickjacking-defenses.aspx

http://en.wikipedia.org/wiki/Clickjacking

http://www.owasp.org/index.php/Clickjacking

http://seclab.stanford.edu/websec/framebusting/index.php

http://blogs.zdnet.com/security/?p=5293&tag=content;col1

http://www.calcalist.co.il/internet/articles/0,7340,L-3388723,00.html

http://narkolayev-shlomi.blogspot.com/2010/01/defeating-frame-busting-scripts-one-of.html

http://narkolayev-shlomi.blogspot.com/2010/01/clickjacking-facebook.html

http://narkolayev-shlomi.blogspot.com/2010/02/clickjacking-advertisement.html

https://wiki.mozilla.org/Security/Features#X-Frame-Options

http://w2spconf.com/2010/slides/rydstedt.ppt