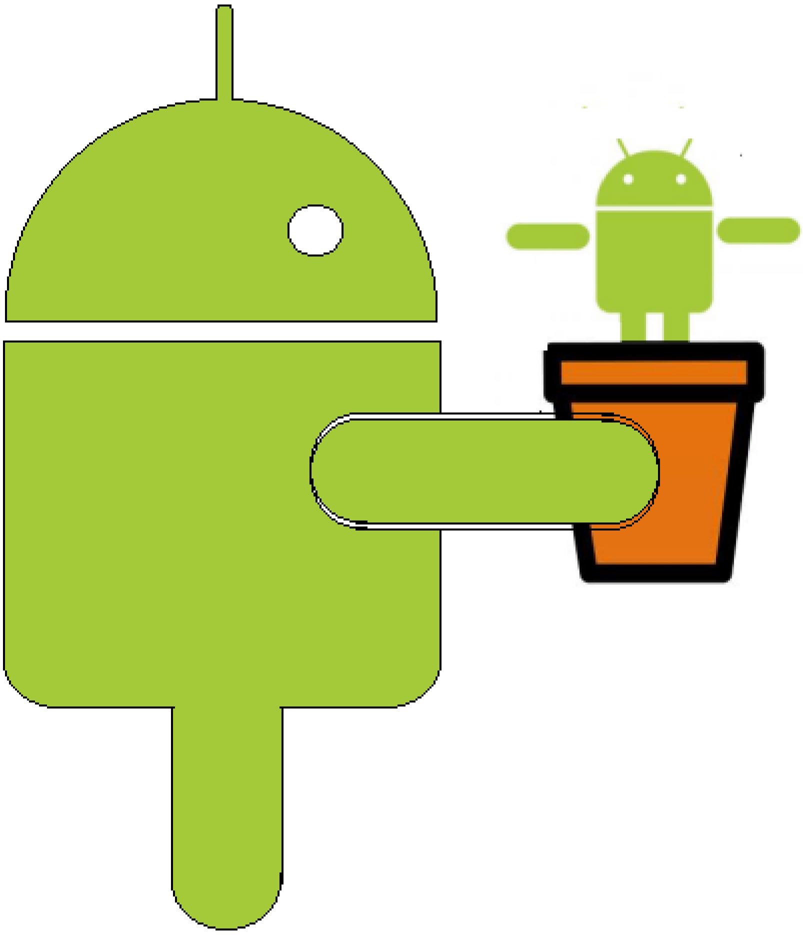
Lets Play Applanting



Ajit Hatti

(ajit.hatti.sec_at_gmail.com)

Black Hat Europe 2013

Contents

1. Abstract
2. Motivations
3. Whats Applanting
4. Outline of the Attack
5. Future Scope
6. About Author
7. References

Abstract

Your mobile is your identity; you are not only connected to friends and family, but you are also connected to your banks, social networks, and various service providers.

The cyber world is plagued with thousands of security issues today. Ever increasing vectors of Spams, XSS, and injection attacks are making the security issues complex. This leads mobile platforms to add more complexity to this.

With the world quickly adopting speedy and convenient way of computing offered by mobiles, security is always traded for convenience.

There are many talks about making and sneaking malicious apps into an app store, and then targeting the victims for fun and profit; but before attacker comes to the fun and profit part, the most difficult hurdle is to install a rouge app on the victims Mobile.

In this talk I will be introducing a new attack methodology – APPLANTING, which the attacker can install an app on the victim’s Android device, without the victims knowledge.

APPLANTING attack combines CSRF with XSS to transparently install an app on victims’ Android device & successfully become man in the mobile to carry out further damage.

Motivations

During my research for “How secure is interent banking in India”, I was working on user authentication and password resetting mechanism adopted by Banks.

http://nullcon.net

How Secure is Internet Banking in INDIA?

Ajit Hatti

ajit.hatti.sec@gmail.com

nullcon International Security Conference delhi 2012

In india many bank use phone as an additinal authentication factor. The One-Time-Password sent to users mobile is considered as the strongest and most relaiable authentication factor.

Not only banking sites but also social networking sites like Facebook and Google use One-Time-Password as reliable authentication Factor.

With increase in use of mobile as authentication for all our banking and social networking activities, phone can also become a sinlge point to loose all credentials.

This is where I started to explore the possibilities of collecting all the “One-Time-Passwords” sent to users mobile. And also in September 2012, found and XSS vulnerability in Google play which further proplled the idea to install and app on a victims android phone capable of forwarding teh “One-Time-Password” messages in real time.

Whats Applanting

Google account is a very powerful service. It provides seamless integration of services like Gmail, Drive, Play app-store, & complete Android device management.

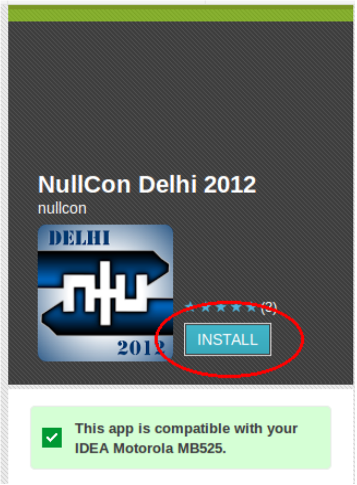
The Single Sign On feature of Google Account makes it possible for an attacker to craft a link and mail it to a targeted or a random victim.
Clicking on the link can direct the victim to a specific Application in Google Play store and initiate an automatic installation of the attacker chosen app on the Android device connected with that Google Account.

This is a methodology which combines XSS & CSRF and results in to automatic installation of an application on victims Android phone.

Technical Details:

Over the Air App installation
Google allows “Over the Air” application installation from the Google's andrioid application store called “Play Store”.

PlayStore can be considered as a web-based client for Android Applicaiton Market. From “Play Store” a user with valid Google account configured on his Android device can select and app from the stroe and choose to install it from his desktop and the application will get installed on the Android device without user's intervention.



This app is compatible with your IDEA Motorola MB525.

Behind the Scenes

When a user selects and app an app and choses to install, browser submits a post request as shown below :

```
POST /store/install HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded;charset=utf-8
Referer: https://play.google.com/store/apps/details?
id=com.nullcon.android&feature=search_result
Accept-Language: en-US
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64;
Trident/6.0)
Host: play.google.com
Content-Length: 139
DNT: 1
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: __utma=45884901.1454077777.1354703478.1354703478.1354710207.2;
__utmb=45884901.5.10.1354710207;
__utmz=45884901.1354703478.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none);
__utmc=45884901; hlSession2=en;
```

```
PREF=ID=039ba4488bbc7e93:U=539a9f5e8e30448b:FF=0:LD=te:TM=1353568374:L
M=1354703631:S=WxOeFTmcDxlCbC35;
NID=66=thFWPFdFuXsSMyN2i8Jk11GJAfLX6ltoxUJhAD_isXFg1jN6-2atIzvmb6Lq
IQgjsyWRNDkw8qSHrI3P27z1xXe9L_XhAy1pjNPnH_jtLWvSQT2fwkHXnu0R8hJlF
e9kzdog78LjccdtwrhN21-j42qYqmRkJdYlPeve67XBnxAFjoAXfDVowbjBtd8Lqa86v
Y59KQ; GMAIL_LOGIN=T1354698419824/1354698419824/1354698436034;
SID=DQAAAMIAAAARgFboHT3Fv_FMC0TgaK908IdzBMtALZR87zLuyL9uQjxCi
jgfr6yI0USHQWvrzuMflJV_rFK-Kqda4zItUmF04Yb3qWZiWBqHqtlg76i2ODOorA0
egHrHym5E_oeumKYnfsmKmdZWJoYcoDulPs6DvVnZgrtIT0AD4ypCM32gAoaQjv
GkvFItffhYfkE7yVmd0yTfXgOlwMMyWtTypkY3WgibOLL1hz42UMDNmRT1cke
WTrYNYRQPaWWuXLSpYDbOJG1GAdJXrUNueP0o5NDd;
HSID=Az1w5eyNQuI5E6jNP; SSID=AxxxdSaCnrF9iEV1P;
APISID=Wcvdn7UmMBDXGObB/A2WmlP3Z492w5oEYC;
SAPISID=1fl09lTnuC6XTt2Y/AILf9HURq8lqgXg6O

id=com.nullcon.android&offerType=1&device=g2ed6a8be00731246&token=QRnhw2
PHSRv6icuuUn1z9wyEI_U%3A1354698436000
```

Understanding the Parameters

Few important fields in the above request are as follows :

1. APP ID – Typpically this id is like “**com.company.app**”

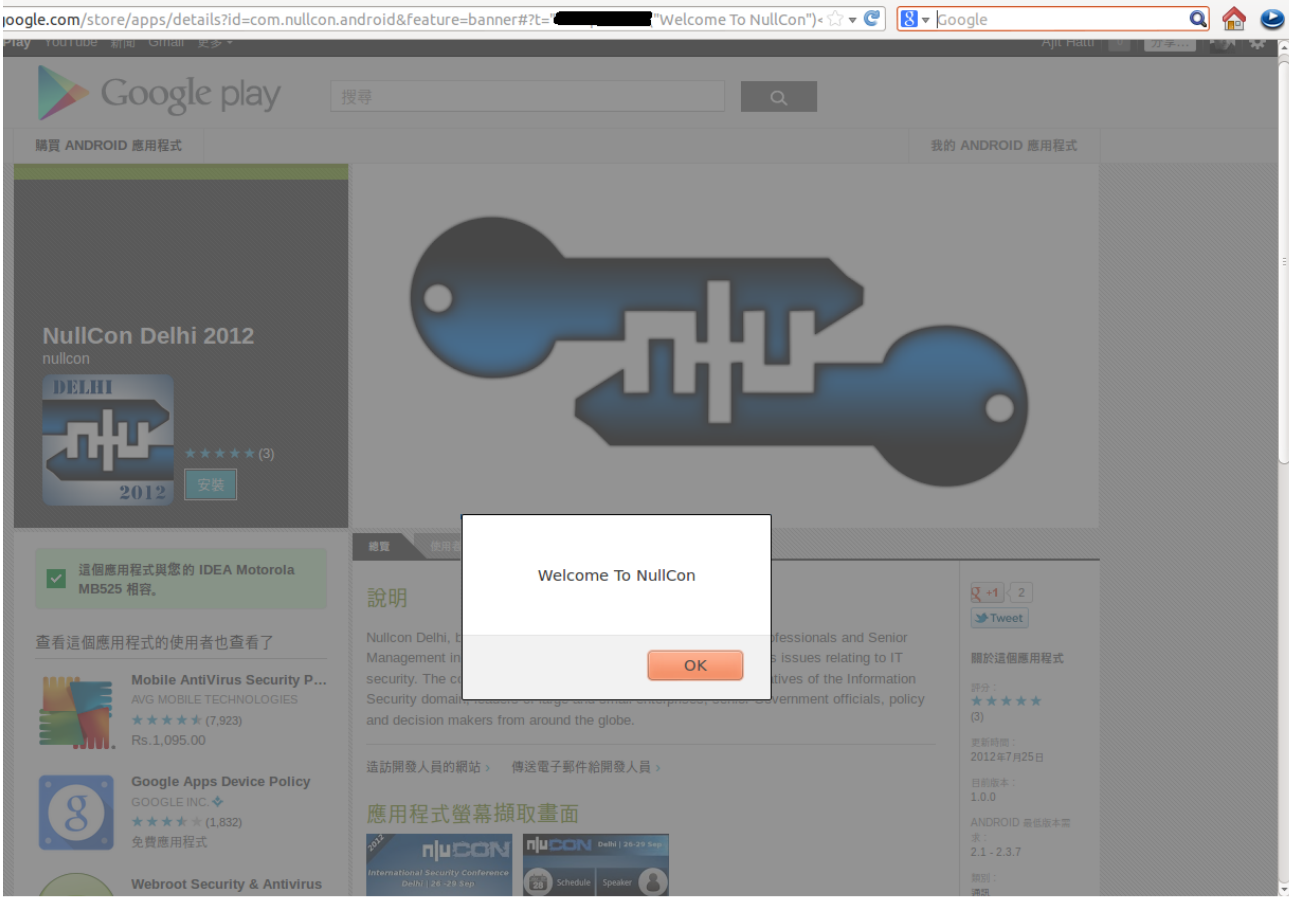
2. Device ID – Unique Id for each of the android device liked with Goolge Account. This peice of information remains constant.

3. USER ID – Is part of the GMAIL_LOGIN token as highlighted above (in yellow).

All the above parameters are part of the cookie. The field SID in the cookie is nothing but a blob pay load which is nothing but a BASE64-encoded structures complying to “protobuf” protocol.

What we have in our Hand now?

During August-September 2012, there many discoveris of XSS in Google services including Play store.



google.com/store/apps/details?id=com.nullcon.android&feature=banner#?t="[redacted]("Welcome To NullCon")<

Welcome To NullCon

The XSS vulnerability in the Play Store enables us to run a predetermined script in the users browser.

With this XSS capability now we can carry out few intersting further attacks like

1. Grab the cookie and ues the informaiton present inthe cookie to forge a request.
2. Initiate a post request behalf of the user
3. Submit the “Install” request behalf of the user.

And in this way we can initiate installation of an application of our choice on a users android device.

All this could be carried out crafting a malicious link to an app which we want to install form Play store with the XSS pattern in it.

Based on the capabilities of installed app attacker can carry out further information gathering or actual exploitation on the victim's device.

Future Scope

By the end of November 2012, Google had fixed XSS issues at various google services also changed the desing of google play. This made Applanting attack difficult.

Conceptually as there will be advances in exploitation techniques and newer disclosuers will be made, installing an app will be a popular attack pattern may be used for serving advertises, Business Intelligence or for any and many malicious perposes.

About Author

Ajit Hatti is a Co-founder of "null -Open security community" (http://null.co.in) the largest community of Hackers in India. Apart form securing technologies and products, he loves to design puzzles, CTFs at NullCon (http://nullcon.net) and other conferences.
Along with organizing "NullCon -The favorite International Hacking and Security Conference of India", he is also a Jailer of the major hacking event "JailBreak" at NullCon.
His work is focused on providing Trusted Computing On Hostile Platforms & most of his papers are in social interests. Recently he had presented a paper "How secure is Internet Banking in India" which grabbed good attention of the banking Institutes in India.
He regularly speaks and contributes at various security initiatives like NULL, NullCon, OWASP, COCON, ClubHack and various other security symposiums.

References

Understanding App install request :
http://jon.oberheide.org/blog/2011/05/28/when-angry-birds-attack-android-edition/

Google's guide for Protobuf :
http://code.google.com/p/protobuf/

Collecting the Bits :

http://thomascannon.net/blog/2011/02/android-market-security/

The XSS discovered by Oberheide in Play Store :
http://jon.oberheide.org/blog/2011/03/07/how-i-almost-won-pwn2own-via-xss/

The XSS discovered & reported.
http://comradex.co/index.php?/topic/396-xss-found-in-google-play/