Idevices and Security

By Bhashit Pandya
At Hcon Meet

Acknowledgment

The presentation is dedicated to my dad
and mom who always supported me and never let me down..

I would also Like to thank **Ashish Mistry**
to give me a platform to show my skill's
and spread my knowledge with him!

Disclaimer

The Presentation is for ethical and learning purpose. Don't use this knowledge for hacking and Defacing or any kind of damages.

I am not responsible for what you do with this presentation.

I expect you to be positive and no evil purpose and never inspire to do so.

About me!

Hello Friends,
I am a student in Security and
web app testing!!
Now a days working to share knowledge on
Web Security and spreading awareness
about common securities..

Lets Start

During the 4.5 year lifespan of the iPhone there are about 146,500,000 iPhones sold out.
This is a huge success but as a product goes wild all over the world, Security becomes a concerned too!
It is the responsibility of the company to see after the security of users privacy!
As the users increased the iPhone app developers increased too!
Here we will be talking about users privacy too and possible ways to breach it!

Tools available

Information Gathering:

Deep Whois

JaNet – Network Tools

zTools – Network Utility

Tcpdump - To capture network traffic on phone

Nice Trace - Trace Route app

Network “Swiss-Army-Knife”

Openfient - Collects lots of UDID

*iNetTools

*Net Tools

Tools available

Network Tools:

*Nmap GUI

IP Network Scanner

iNet Pro

Scany

LANScan

Net Master

*Fing

SetnetInsight

iNetQCheckPro - network testing app with reporting capability

*iNetTools

*Net Tools

*Port Scan

*PortScanners

Tools available

Penetration:

Nada

zScan Pro

*Mptcp

*Metasploit

Verification:

iSSH

OpenSSH

SSH Term Pro

*zatelnet

Survey

As per viaforensics.com

-76 percent of mobile apps stores user data in phone

-10 percent Apps store passwords in clear text

Privacy Metters

Every idevice has its own UDID which represents your Unique ID.
This UDID are used by iTunes which approves your device and then allows an
app to
download it on your iphone!
These UDID contains lot of information which can be reviled easily!
Just get the UDID and paste it on your browser and all the information will be on
your screen like
-Browser
-Apps used
-Apps Login details
-Geo Location etc..

Privacy Metters

On march '12 AntiSec claimed to have 12 millions of UDID. They leaked
1 million out of them having personal details , Device and Models ,
and other information as a proof.

Plist

Property List Files:

-Designed to store user information like uname,pass,cookies,session info in plane text.

-Used to store information of an app.

Dir:/var/mobile/Applications/[appid]/Documents/Preferences

-This info is Stored in Binary format.

-They are in filename.plist format.

-They are easy to extract and modified via plist editors like Erica utility, plutil tool(Cydia),property list editor...

APPLICATION AUTHENTICATION

While pentesting do check if any of your app contains application authentication.
If so then you can also find that auth pass in plist files.
If admin=0 replace 0 with 1
For instance admin=1
This will bypass that authentication.
So it is not a good idea to store session, passwords or any critical information in plist because they can be easily extracted.

Keychain

-SQLite database
-Stores important and sensitive data storage by programmers.
-Its an api or a library provided by apple.
-Encrypted with a hardware encryption key.
-Cannot be Decrypted
They are not of a same group but when a device is jailed breaked by writting a application we can create a same group of these keychains and get access to all the keychains.

Keychain

There is a tool which is used to dump all the Keychain from the device. As explained in the previous slide we can write an application which gives same level group.
Keychain dumper is the tool created by Github guys to dump all the keychain!
so storing information in Keychain is also not a secure way!

Error Logs

idevices app developers use NSLog calls for
-Debugging
-Troubleshooting

Such applications may store sensitive information(Depends on the type of app) like Uname, Password, request and Response and other error details.

Error Logs

DIR:/private/var/log/syslog

To view logs:
Console App(From AppStore)

Sync it to iTunes and we can get all the error logs on our system!

Screenshots

Yes, Even screenshots can be harmful but this is not those screenshots which you do it but lock button and home button at the same time.
This screenshots are taken by the system automatically.
When ever we push the back button, to give it a good shrinking effect where system automatically takes its screenshot . This may contain sensitive information.

Screenshots

Suppose,
I got a mail regarding my site hosting or Bank account information on my phone and suddenly I got another work and I pushed the back button.
This will lead to storage of cheches.
Now what an attacker will do?
He/she will navigate to the screenshot dir and will extract all the information.

Screenshots

That attacker can find the screenshots here:
DIR:App directory/Library/Cheches/Snapshots

Now we can imagine what can be done if any of your hosting or bank account is compromised.
Please Don't imagine its a nightmare! :D

Home Directories

Now you must be thinking “Oh no even Home Directories??”
The answer is yes, even home directories!
Apart from all the possibles discussed till now we are now talking about the Home Directory.
Home Directory stores sensitive information as well.
They can store encryption mechanism in a file.
With the above information an attacker can write their own tool to find the encryption key with rev. engg.

Physical Threats

-My phone is password protected.

-Encrypted sensitive files.

What is the threat then?

Physical Threats

Now adays it is easy to lose mobile phones if you dont take a proper care of it. Once you lose your phone the person can do is to use Boot Rom Exploit.

-Boot Rom Exploit:

All the files on the devices can be copied in less then 15mins.With Boot Rom we can boot a custom os which contain open ssh (USB) and copy all the files even if the device is not jail broken. This is possible using boot rom exploits(Ipad2 is not vuln to boot rom exploit).

Physical Threats

-Passcode bruteforce:

4 digit passcode can be brute force in a very less time.

Problem:

If the wrong passcode entered you can even endup with delay of few mins. This cause brute forcing process to halt.

What can be the alternative method for this?

Any one from the audience?

Physical Threats

The validation is performed at 2 locations:
-String board level
-Kernel level

Spring board level:
Here the os is completely boots up and the brute forcing we were talking about in the prev. slide was a spring board level where we end up with data loss.
(BAD IDEA to brute-force here)

Physical Threats

The validation is performed at 2 locations:
-String board level
-Kernel level

Kernel Level:
The file encryption process starts only after complete os boot. The 4 digit passcode can be cracked in 20mins. When brute force done on kernel level the delay wont be the problem any more! The process will be smooth!

End

There are many other ways tooo!!
Where data can be manipulated by few techniques and methods!

But It is a deep sea!
There is no end in security and pentesting!

Thank You

Thank you to attend the Hcon Group session here in Ahmedabad.
Hope you all enjoyed and learned new things!

You can get this presentation from:
Groups.hcon.in/resources.html

You can contact me here:
fb.com/bhashit.pandya

Email:
bhashitpandya@yahoo.com