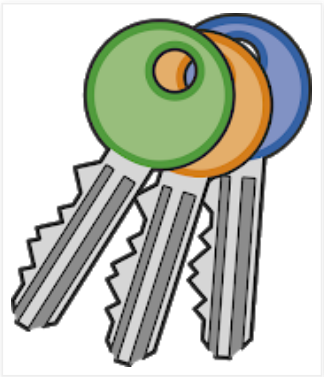
Cybersecurity Blog

Everything about threat intelligence, blue team, red team, pentesting, security audit, security review, testing and assessment.

Saturday, September 16, 2017

Android Kiosk Browser Lock down Security Testing Checklist



What is Kiosk Browser Lockdown?
In simple words, if you want to restrict the usability of the device that you are giving to your employee/customer's hand, you can use kiosk browser lockdown facility to make that device single purpose used.

Generally, all finance companies use that at their branches when the customer comes to their branch and any kind of help and representative approaches them with a tablet which has that bank/company's application running on it. Now that device may land into many hands such as a company's all employees and sometimes clients too. So to restrict that device's all functionalities such as settings, other apps on home screen etc.., a company uses kiosk lockdown which can be paid or free software.

Post setting up Kiosk, when that Android OS based device boots up, it automatically runs only allowed the application. Which will not have any exit feature or may be an exit to the home screen, notification area or settings menu is locked down with the password.

Scenario - Consider there is a device with Kiosk lockdown, then what all test cases can be performed on that device?

Goal - We can set multiple goals here based on the impact that we are looking for:

1. After bypassing Kiosk lockdown go to settings menu and change the device settings
2. After bypassing kiosk lockdown, launch a default Android-based browser(Chrome) and install any sample malicious application

Translate Language

Search

Search

Subscribe via email

Email address... Submit

Blog Archive

- 2020 (2)
- 2019 (6)
- 2018 (4)
- 2017 (5)
  - September 10 (1)
    - Android Kiosk Browser Lock down Security Testing C...
  - April 30 (1)
  - April 2 (1)
  - March 26 (1)
  - February 26 (1)
- 2016 (11)
- 2015 (4)
- 2014 (22)

To aim above goals, I have a small and handy checklist of test cases:

- Check if USB debugging is enabled or not, try connecting device with USB and see if you can use ADB commands or not.

- The application running in kiosk mode can be an exit by long pressing on the “Background process”.

- Check if you can root the device or not

- If none of the above is possible, if the application itself as a upload option, try to install burp cert and proxy or adb.

- Use a help/faq which may have any external link of web reference which will be opened by default tablet browser can be used to download malicious apk afterward.

- Try to open android device in safe mode and disable/uninstall kiosk application.

- Check if kiosk application has any exit button which requires a password, then give 0000 as default password or go to the kiosk application vendor website and find if there is any fallback/reset functionality procedure mentioned or not which you can use in your testing.

- Check if USB debugging is enabled and you can install FRIDA hooking application, then use FRIDA to disable kiosk running on startup.

- Sometimes USB debugging is disabled in normal mode, but it can be enabled in fastboot/samemode boot mode. So try opening tablet in safeboot or fastboot mode and then check if USB debugging is working or not.

- Sometimes installing alternative homescreen can also bypass kiosk browser lockdown.

- Try to find out which kiosk lockdown software (commercial/free) that company is using, go to their website find documentation if there are default password or anything like that you can access. Check for any backdoor in the configuration file.

- Try to find out if any researcher/company in the world has bypassed it or produced any vulnerability/exploit regarding that software, if yes apply it in your engagement.

Posted by Frogy at 9/16/2017

Labels: android, android security, bypass android kiosk lockdown, bypass android kiosk security, bypass kiosk security, kiosk, kiosk security

1 comment:

Atul said...

Good work Chintan. You covered almost every possible test cases for Android Kiosk.

September 28, 2017 at 5:42 AM

Post a Comment

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)