MOBILE PENETRATION TESTING

what pentesting can do

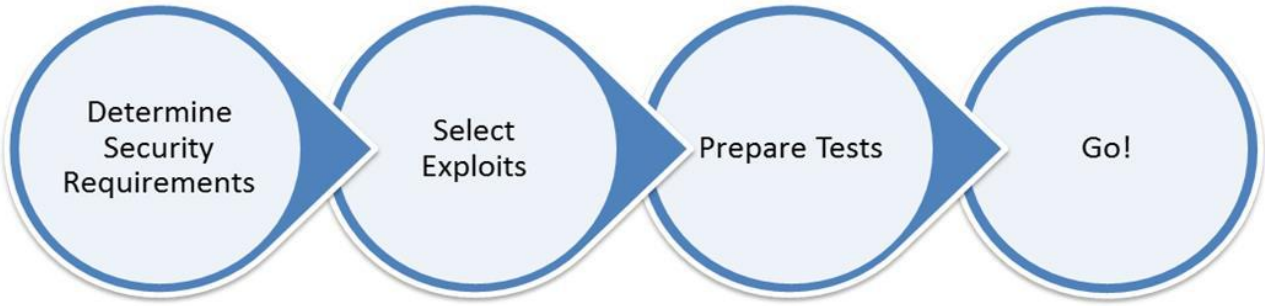
Developing applications for mobile devices has become an important market for programmers and designers. With smart phones and tablet computers becoming almost as powerful as desktop and laptop computers the possibilities are endless. But … security seems to be at the bottom of the list for most companies. This is bad, considering the data that is being handled nowadays.

secureapps

WHAT IS PENETRATION TESTING?

Penetration testing, or pentesting, has been a popular subject within the area of security engineering the last couple of years. Letting hackers, white hats, try to break your system in order to make it safer. It is an important element in the total process of creating a secure system. It is part of validating all measures taken during the process of developing a mobile app. Penetration testing needs to be part of every complete security strategy.

A penetration test consist of performing a, not specified, amount of known exploits against a selected target. The exploits need to be selected carefully based on the security demands and the amount of time and resources available.



Because recorded attacks are, by definition, known attacks it is important to include a pentest in your security strategy. Being vulnerable to a well know attack is never a good sign and will have impact on your reputation. It is also important to repeat this periodically. The world keeps on changing after your system has been deployed. New exploits will surface and you might be vulnerable.

> ” A **penetration test**, occasionally **pentest**, is a method of evaluating computer and network security by simulating an attack on a computer system or network from external and internal threats.” Wikipedia

Actually, a pentest is simulating an attack by bad guys, the black hats. The attack itself is not simulated, it is real. You need to perform an actual attack to really understand the strength of a system. This is also a danger that needs to be understood by everyone involved. You might, accidentally, bring a system down by performing a penetration test.

WHAT IS PENETRATION TESTING NOT?

A penetration test is not a complete security assessment nor is it a complete security strategy. It is an important part of your strategy but it cannot give you a complete picture of the effectiveness of your security measures or determine the mechanisms you need to implement. It merely shows you have missed something. A penetration test is a test and needs to been seen as a test.

- A pentest is based on the available knowledge of that moment.
- A pentest consists, by definition, of known attacks.
- The very latest attacks are probably not yet generally known.
- A pentest is always a selection of test and can never cover everything.

A penetration test can show you that there is something wrong but can never show you that everything is secured. A statement Edsget Dijkstra made about testing can be aplied to penetration testing as well.

> ”Program testing can be a very effective way to show the presence of bugs, but it is hopelessly inadequate for showing their absence.” Edsger W. Dijkstra

Known exploits are mostly fairly generic attacks. They expose problems in the operating system, platform, frameworks or in the API’s you might be using. When your mobile application is popular enough or might yield very valuable information, chances are you will be specifically targeted by hackers. These types of attacks need to be mitigated with security by design, a good a developers team and well placed monitoring mechanisms.

Penetration tests can help you here but the problems you might find will turn out to be design issues. Each attack strategy will take a fair amount of time to research, design and execute and fixing the problems found will inevitably bring you back to the drawing board.

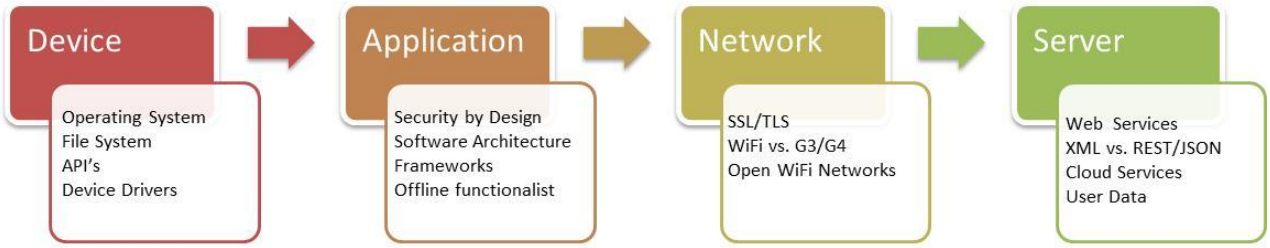
PREPARING A PENTEST ON A MOBILE APP

You need a lot of information. The most important is knowing what your security requirements are. What needs protecting? What is the damage potential if something does go wrong? Gathering good security requirements is a separate subject altogether but an important one.

A good architectural view of the mobile application is needed. The entire chain, technical and functional, needs to be clear. Does the app store information locally on the device? What information is used? Is there server side activity? Is key functionality executed on the device or on the server? How is communication secured? What mechanism is used for authenticating a user? Is authorization needed?

These are just some of the questions that need to be answered to get a good picture of the app. Only then can the penetration test can be designed. This mainly mains selecting the most appropriate tests based on up-to-date knowledge of exploits and the expertise of security engineers.

This process needs to be repeated for all mobile platforms that are used. Exploits for Android are not the same as the ones for iPhone or Windows Phone. For each mobile platform a pentest needs to be a separate process.



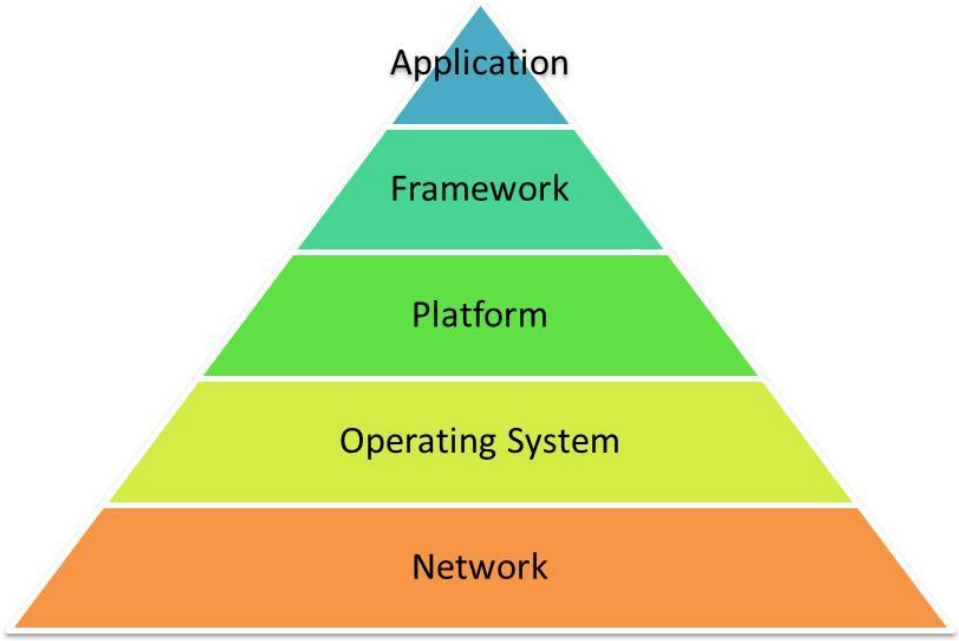
The same also holds for the actual tests. Performing and documenting the tests and the results needs to be done for all mobile platforms separately. Different API's, differences in architecture or different release schedules are just some reasons to keep pentests for each platform separate. You will need to revisit the tests and the result separately in the near future. New issues will pop up one platform at a time, rarely synchronised.

SETTING UP A PENTEST

Setting up a good penetration test will take time.

Exploits are often aimed at very specific areas. A certain version of device driver on a certain version of an operating system when a specific setting is used. This means you need very specific information on your application and how it can be used.

The attack surface of any system is huge nowadays. This is why complete coverage can never be reached. There are just to many layers in any application to do it all yourself.



You will simply need to trust that other areas will be kept as safely as possible by the responsible organisations and by the community as a whole. Aim your energy at your application and do not bother to much about the underlying mechanisms. Unless you are a big government organization or multinational you won't have the resources.

Keeping Android secure is the responsibility of Google and iOs is Apple's duty. This still leaves you with a lot of responsibility. Best practices, API guides, patterns are published by companies like Google and Apple. Use them.

THE IMPACT OF A PENTEST

A pentest can show the presence of a problem but never the absence of one. It is important to keep this in mind. A pentest only proofs itself when it does find security issues. This tells you that your system is vulnerable to known exploits. Fix it!

Known exploits are mostly fairly generic attacks. If you find such a problem you might feel it is not actually your problem. The problem lies with the OS or the supplied API's. To some extend this is true but you do need to deal with the problem. Find a way around it or come up with alternative mechanisms.

A penetration is very much snapshot in time. Last year's penetration test doesn't really add any value today. It needs to be repeated. When performing the next test it will likely look different from the last one. New exploits, techniques and mechanisms are now around.