MOBILE SECURITY

developing secure apps

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

INFORMATION SECURITY

Protecting information is difficult, mainly because you do not want to protect it from everyone and everything. Information is kept for future use not just to hide it. A problem arises when unauthorized people are interested in this information and they know where it is being kept. Cyber criminals see opportunities to make a profit from your information.

> ”**Information security** is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (electronic, physical, etc...)” Wikipedia

There are many examples of information that needs protecting. Credit card details, medical data, bank and insurance accounts are well known but there are many other examples and the list is growing with increasing speed. Money is going around in gaming, gambling, app stores, on-demand content etcetera. This money attracts criminals as well, cyber criminals. Information security needs to be incorporated seriously and very early on.

Another subject concerning information is social media. A lot of information is beyond your control. The big social networks offer you their basic services for free. This is only possible because the money is coming in from other sources. When you are not paying for a service, you are the product not the customer. A lot is happening on social networks and everything is recorded, analysed and sold. Just a simple example: knowing your interests allows a site to place well aimed adds to people who most likely will react to that message. This is not necessarily bad but your employees, your partners and customers are on those social networks as well.

Not only do you need to protect the data that is entrusted to you but you also need to keep an eye out on the what’s happening around you.

REASONS FOR SECURING INFORMATION

The starting point when securing information always needs to be the question: why? If you do not know why you are doing something you will fail. This does sound obvious, but in a lot of cases some security is implemented just to be able to say it has been taken care of. This in itself is a reason why but in lot of cases it turns out not to be the case. You demanded a secure system and your supplier told you it is of course a secure system. You will always find out when it is already too late.

The following list provides some examples of why you would need to implement security measures. Use it as inspiration but know there are many more possible reasons.

- Compliance with laws and regulations.
- Protection of intellectual property.
- Protecting customer or financial data.
- Distinguishing your company from the competition on security.
- Keeping your reputation as a safe partner.
- Being able to proof criminal activity when attacked.

There are many reasons to implement security mechanism. Knowing why you need security is imperative to actually create a working solution. This will be different depending on the products and services that are being offered.

A creator of maps and navigation systems wants to offer the best maps and functionality to its users but it needs to make sure other parties can't just steal the maps and use them for their own purposes.

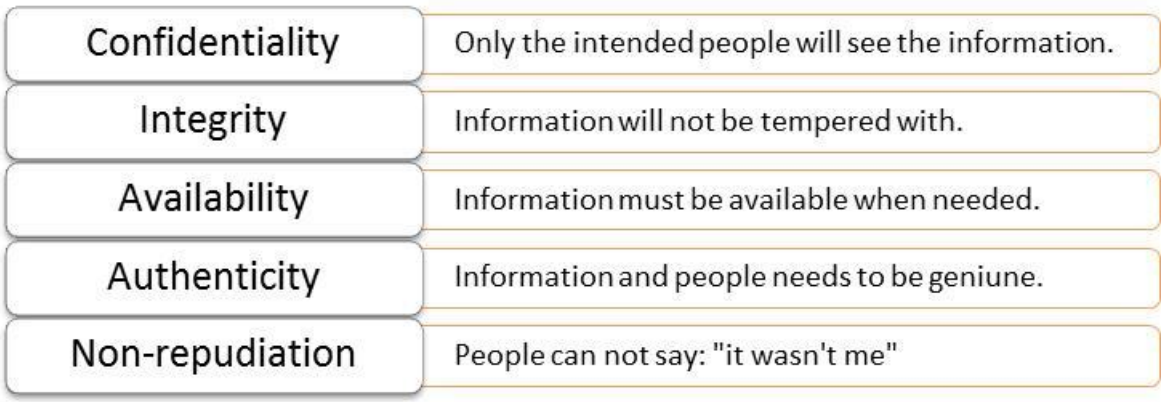
When offering administrative and financial system from the cloud, trust and security are very important. First of all your system needs to be available most of the time but it is also important that a customer knows his financial administration is safe.

Security requirements, knowing what you need, is the important first step.

THE BASIC CONCEPTS

What is security? What do we expect from security mechanisms? Obviously they need to protect our information but how do you actually do that? A good understanding of the key concepts is needed to know what we can actually accomplish.

The following list are well known principles of information security. When implementing a security mechanism it should result in realising one or more of these concepts. It should of course also help bring you a step closer to achieving your security goals.



All these concepts are about creating trust. You want to know who you are dealing with and that you can communicate safely. In a grocery store this is easy. We pick up some oranges, pay the cashier and walk out, a few euros lighter but with our oranges. We could see the quality of the product, take it with us after paying and both you and the cashier were reasonably sure the payment would be a success.

When the consumer and the seller are separated by the internet this situation changes completely. Will I get my oranges after paying? Will they be any good? Will they be delivered on time? Information security is about bringing the same trust from the local grocery store to the internet.

The information security concepts are about breaking down the subject and making it understandable and manageable.

SECURITY ENGINEERING

Building secure systems is hard to do. It is almost impossible to imagine what hackers can come up with to break a system and do it before they will. The hacker can choose its targets, make a selection based on his chances of success. When looking at just a simple a web application there are many parts that make up the complete system. The browser, PC or mobile device of the user, the network, the web server, the operating system, the application software, the database and many more. Each of those elements have weaknesses that might be used to get to the information a hacker wants. You need to protect this entire technical chain while the hacker can pick and choose.

> **"Security engineering** is about building systems to remain dependable in the face of malice, error, or mischance. As a discipline, it focuses on the tools, processes, and methods needed to design, implement, and test complete systems, and to adapt existing systems as their environment evolves." Ross Anderson, Security Engineering

"Good security engineering requires four things to come together. There's policy: what you're supposed to achieve. There's mechanism: the ciphers, access controls, hardware tamper-resistance and other machinery that you assemble in order to implement the policy. There's assurance: the amount of reliance you can place on each particular mechanism. Finally, there's incentive: the motive that the people guarding and maintaining the system have to do their job properly, and also the motive that the attackers have to try to defeat your policy." Ross Anderson, Security Engineering (second edition).

With today's web and mobile technologies and their ever growing role in society, security engineering needs to be placed prominently within all projects in these areas.

THREAT MODELING

Knowing why is only the beginning. We also need to know what we need to protect and how we will be doing just that. This is where threat modelling comes in. What elements are open to attacks, how vulnerable are they and how could an attack be prevented.

> "**Threat modeling** is an engineering technique you can use to help you identify threats, attacks, vulnerabilities, and countermeasures in the context of your application scenario. The threat modeling activity helps you to: Identify your security objectives, Identify relevant threats and Identify relevant vulnerabilities and countermeasures." Microsoft, Threat Modeling Web Applications

A well-known classification scheme is DREAD. This is a simplified formula to calculate the risk a certain threat poses.

Risk = (Damage Potential + Reproducibility + Exploitability + Affected Users + Discoverability) / 5

In the end it is all about economics. Does investing in countermeasures outweigh the risk. Investing in the right measures and mechanisms is of course the important part and thus the difficult part.

SECURING MOBILE APPS

Finally, the mobile applications. In essence all practices from the field of security engineering also apply to mobile development. But the huge variety in platforms and versions make it just a little bit more difficult. First of all there are the different platforms: Android, Apple's iPhone, Windows Phone, Blackberry, etc. These platforms have their own specific architecture, API's and frameworks. All these platforms are out there in different versions. Older versions of Android or iOs are still used a lot. Android has the added complexity of having specific versions for some manufacturers as well.

When building a mobile app, you can't just choose a platform. You will likely want to support multiple platforms to reach as many people as possible. Different development teams will create a mobile applications that will offer similar functionality. This makes security by design more difficult and more necessary. Not only needs it to be done for multiple platforms, it also needs to work similarly. Worst case scenario: you might even need to implement server side specific interfaces for the different platforms.

Use the information available. Many people and organisations are taking an interest in security and in securing mobile application. Make sure you stay up-to-date. One example is OWASP, the open web application security project. Recently they have added mobile as a important subject as well.

Their information on the most common problems and their take on the solution can be very helpful. Below is the top ten they publish on mobile threats. There is information on testing, tools and threat modelling as well.

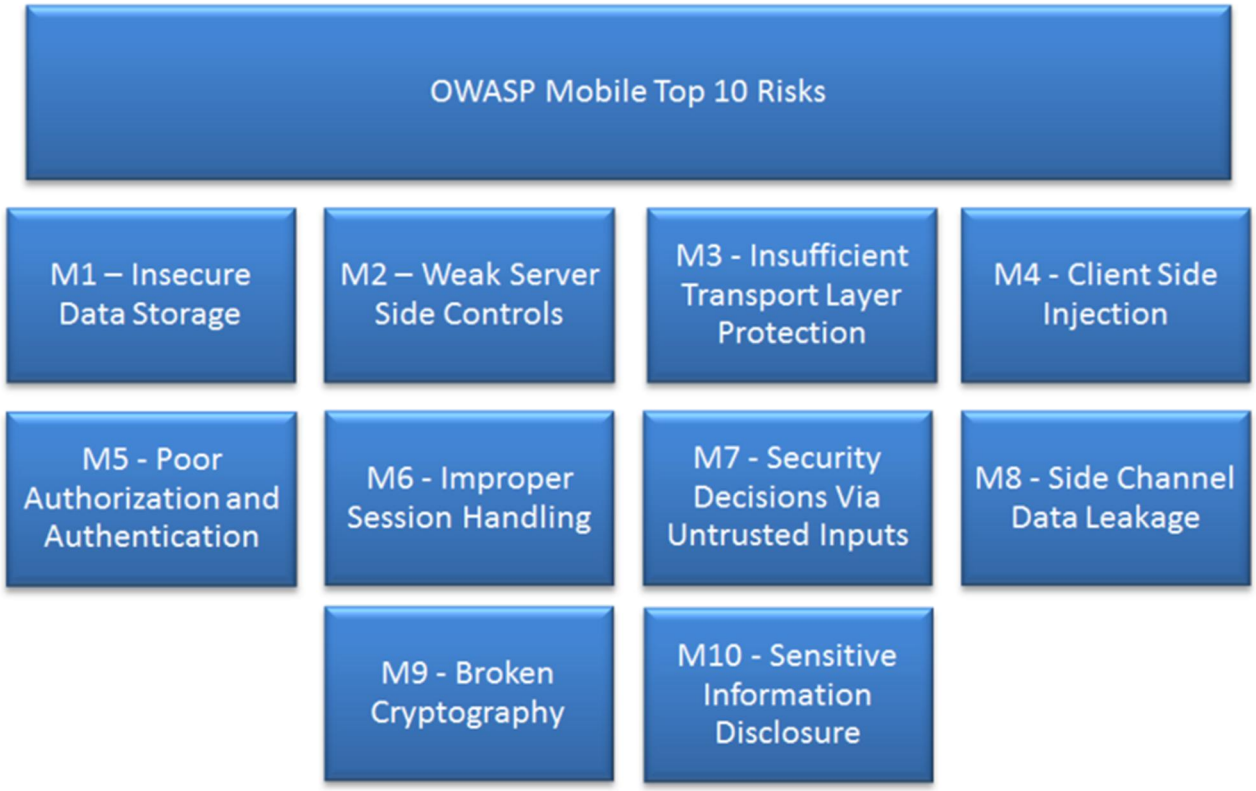


image from: https://www.owasp.org/index.php/OWASP_Mobile_Security_Projec