GROUP 5:

Raditya Arief
Eren Celik
Ana Guerra
Luigi Tuttobene

Draft Assignment Block 4

Part 1

Select 3 actors (including the problem owner) involved in the security issue (you can draw on the previous assignment).

Market Operator

The perspective of the market owner has detailedly been investigated in the previous assignment. In particular, we have analysed cost and benefits of the Android Vulnerability Reward Program introduced by Google in 2015. Despite the imprecision in our measurement, we are confident about the positive results of such programs. As a matter of facts, similar projects has been developed for years with the same aim on different platforms, computer programs in primis.

Its positive effect on Android security has already been acknowledged by Google in [REF]. In its first year, the program has rewarded researchers with more than $550.000 , and the investment has increased by 33% this year.

Can a competitor pursue a similar strategy?
critical factors:
- the reward might be a limitation;
- the number of users (people who download from your market);
-setting up costs are limited (almost irrelevant for google, affordable for smaller markets like Baidu or 360).

Advantage: ideally the cost is proportional the effective number of issue solved.

Perspective of other actors:
It is an efficient solution against attackers, as similar programs address
the problem of zero-day vulnerability exploit.
App developers would enjoy the result of the program as free riders. Surely, they can contribute to the success of the program by establishing alliances and sharing resources. However, they can also enjoy positive externalities, free riding the security brought by the program.
For the final user is an interesting solution. It might work as awareness campaign as well, increasing the level of brand loyalty.

Customer

There are different countermeasures that application users can undertake to mitigate the presence of malware, and thus its terrible consequences, in their devices. One the most rational/recommended actions is to download applications from reputable, sources such as the official Android application store, only. According to Google Android security review, Google play has the lowest rate of malware infection and the company constantly works for enhancing its security performance (Google, 2015). However, as we know, not all consumers have access to official application markets, this is the case for China, where Google and all it services were blocked in mid-2014. Therefore, this is not an option for the Chinese application consumers.
The second option is using mobile antimalware, generally known as mobile antivirus, for android devices to mitigate the infection risk. Antivirus (anti-virus) is a software program that prevents, detects, and remediates malware infections on individual computing devices. The name antivirus was originally given to programs that identified and removed a particular type of malware called virus. However, nowadays, antivirus are utilized for preventing infections caused by different type of malware such as worms, Trojan horses, rootkits, spyware, keyloggers, ransomware and adware (Rouse, 2005).

Using mobile antivirus applications involve two main actors: mobile antivirus application vendors and consumers. As we saw in Economics of Security, edX edge videos, there are not incentives for vendors to come up with better products than the competition. Therefore, they prefer to invest money in marketing and promoting activities rather that in enhancing the malware detection capacity of their products.
Customers, on the other hand, are able to choose between different antivirus alternatives. AVTEST, an independent IT-Security Institute, provide monthly information about the best antivirus software for Android.

The institute classifies vendors according to antivirus protection (detection of the latest Android malware in real-time, detection of the latest Android malware discovered in the last 4 weeks), usability (performance

regarding battery use, slowing down devices, traffic generation; and false warnings), and special features.

that users paid is to give access to all data, information, applications, search engines, and device capabilities to an application for being safe.

Among the benefits of mobile antivirus applications, the best mobile antivirus applications offer not only malware detection and prevention, but also a range of privacy and anti-theft features that include the ability to back up contacts and other data, track phones or tablets via GPS, snap a picture of a phone thief with the device's camera, and even use Android Wear smartwatch to locate user's phone (Tom's Guide Staff, 2016).

Some criticism of mobile antivirus applications is first, signature-based antivirus scanners, which efficiently detect known malware, have serious failures with new and unknown malware. In addition, malware developers test their application using the most popular antivirus application. Second, unlike desktop antivirus software, mobile antivirus have resources limitation on mobile devices. Furthermore, mobile operation systems impose restrictions to those applications. Finally, the rapidly growing number of mobile application is outpacing the industry's ability to analyze, catalog, and construct the signatures necessary for identifying embedded viruses and malware (Li & Clark, 2013).

Consequently, there are doubts regarding how effective is the use of antivirus in mobile devices, and there is not supported evidence that shows a decrease in the security issue due to antivirus. However, customers who perceive that the benefits overweight costs will have the incentive to use antivirus as a countermeasure. Briefly reflect on the role of externalities around this security issue.

App Developers

There are several countermeasures that the app developers can pursue. One of those countermeasures is to apply secure software development life cycle. In brief, secure software development life cycle prompts software developers to implement security best practices at each stage of its software development process. Secure software that is up to the highest standard is achievable by following the latest best practices. Most of the times, the owner of each software platform would provide guidelines and documentations describing what security features available and which best practices to follow to achieve the highest security level as possible.

The cost and benefits are one interesting perspective to look at in the issue of secure software development. The benefits of secure software will be perceived by the users. On the other hand, the implementation of security best practice will not only incur benefits but also costs to the app developers. The costs of secure software development include the longer development time and the necessity to hire qualified programmers.

Does the benefit secure software development will outweigh the cost from the app developers' perspective? The answer might be yes and no. For the big and famous IT companies that have already secured a share of the market, the benefits of secure software development arguably outweigh its costs. However, for the smaller IT companies, also called startup companies, the outcome might be quite different. This difference can be attributed to one of the impacts of network effect to the IT industry; the fastest company to gain the majority of market share has a substantially higher chance of becoming the market leader. Therefore, these startup companies often sacrifice app security for faster deployment time. In brief, depending on the condition of the company, the secure software development practice can be either beneficial or detrimental.

Looking at the costs and benefits analysis of implementing secure software development countermeasure from the app developers' perspective, it can be understood why most app developers, at least in the beginning, have a very weak incentive in implementing it. The secure software development practice not only incurs costs but also brings minimum benefits to the app developer. The longer software development time may cost the company the chance of becoming the market leader. Moreover, in such case where there is any adverse consequence happened caused by the lack of security, the actor that will bear the biggest loss usually is the users, not the app developers. Looking from this perspective, however unethical it might be, the implementation of this countermeasure is unattractive for most app developers.

The security issue in app development reflects an apparent externalities issue; the lack of effort to secure applications by the developers will likely inflict harmful consequences to the app's users while it imposes insignificant to almost none impact to the developers themselves.

Attacker

The attacker has a different dynamic when it comes to strategies. The attacker strategies in the case of app-markets involve evading detection. Be it hiding malware from preemptive scans to evasion analysis by emulation/sanboxing this is also known as dynamic analysis.
Unique malware code is safe from conventional malware scans. It becomes more challenging when heuristics come into play. With dynamic analysis it becomes possible to analyse the behaviour of an app over time. It is here where even (original) code can be caught. So it is imaginable that most well hidden malware will be picked up at the emulation/sanboxing stage. Thus a good strategy is to evade detection under emulation.
Dynamic analysis will alert for any suspicious behaviour. Malware programmers have two options in trying to evade detection. Stall or detect. By stalling any malicious action is delayed for an extended period. This is done in hope that the dynamic analysis lasts shorter than the stalling period. This is hard to implement as the clock of a system can be emulated and fast forwarded as well in hope of uncovering stalled malware. If the malware stalls too long it will also not be as effective as it possibly could be. The other option is that the malware is able to detect that it is in an emulation. Once it detects this it will only engage in benign processes. This detection can be relatively easily implement by checking for various information like device names, product numbers, sim card information, operator name, APIs, etc (source). Currently attackers and defenders are in a constant arms race in this field (source).
For the attacker it is fairly easy to implement detection techniques. Especially since such attackers can be very well organized businesses. It takes time and effort indeed to take part in the arms race. "Compromising a

method is only one vulnerability away." On to of that, techniques can quickly spread amongst attacker groups and organizations. An attacker can of course greatly benefit from such strategy.
Defenders are in a constant process of improvement. They can never know what vulnerability will be (ab)used next and are therefore in a constant reactive battle. This battle is constant because it is the most important front. This reactiveness can be costly because when malware makes it through it infects many devices. Knowing the predominant reactive nature of this fight means that malware will evade it, infect devices and ultimately turn a profit for the attacker. On the defenders end remediation can be expensive and damaging to the brand name. Depending on how well an attacker can keep evasive code secret from other attackers it will have a longer lifecycle. Also if the attacker is dependent on how vigilant a user base is. If users are quick to flag apps as suspicious then it becomes increasingly harder to stay undetected. The effect is that the code has a much shorter lifecycle and will force the attacker to find another way to stay undetected.