International approaches for mobile security

BIC Discussion Paper **June 2012**

Abhishek Sharma [1]

[1] Beyond Evolution Tech Solutions Pvt Ltd, India

This project is supported within the portfolio of the European Commission's DG-CNECT Unit H.4, Trust and Security, and has received funding by European Commission's Seventh Framework ICT Programme under grant number 25258655 for the period January 2011 to December 2013.

Introduction

The extent and dimensions of the usage of mobile devices flooded with numerous applications has extended to practically all spheres of human life. These devices are now used for communication by voice, entertainment, social media, utility, information gathering - news, sports etc are assuming unimaginable proportions. With organizations increasingly looking toward mobile devices (e.g., iPhones, iPads, and Android smart devices) to deliver content and functionality to both their employees and their customer base and the people started utilizing power of mobile applications more and more, the mobile devices are becoming the fastest growing consumer technology. However, most find it difficult to understand and evaluate the security concerns that surround mobile platforms. Since mobile computing is a relatively new concept in the enterprise, many organizations have not yet updated their information security policy to cater for it. With about 600 million smart phones in 2010, they are poised to crossing approximately the 1.9 billion mark by the year 2013. Moving along with this, the growth and availability of mobile applications are multiplying the threat factors exponentially. Hence, Smart Phones, mobile apps, remote data, consumerization of IT and the rise of malware and criminal intent presents a lethal cocktail of security threats to the consumer, corporation and the mobile networks.

Mobile Security Scenario

In the world of computers and communications, the more widely a technology is used, the more likely it is to become the target of hackers. The enormously growing popularity of mobile applications has attracted enough hackers to make the potential for serious security threats a reality. More than 55,000 new pieces of malware are seen on a daily basis as per the report. Research shows that the number of mobile malware more than doubled in 2011 from 2010.

Ten years ago, CTOs wanted company phones locked down, camera phones and iPods banned from the office. Now they are being forced to contemplate bring-your-own-device (BYOD), whether that's a smart phone or a tablet, which is probably a CTO's worst nightmare. Meanwhile, consumers and business people alike are adopting a laissez-faire attitude to downloading mobile apps – powerful computer programs that could potentially contain malicious code – from unknown authors, something few people would do on their PC. Yet, a staggering 96 percent of Smart Phones and tablets do not have third-party security software installed. On the other hand, 2,500 different types of mobile malware were discovered in 2011.

What is under Threat?

Mobile devices increasingly face various types of threats, from mere annoyance to invasion of privacy, propagation, malicious tools or stealing money. Some of the most threatened mobile applications are money transfers or mobile commerce; Stored data on phone devices – this is growing in volume with growing storage capacity of the devices; Remote Data Storage OTA-with applications allowing data storage on cloud the three elements - Transmission, Storage and Access - have become vulnerable; Mobile Health Care, a very potential and fast growing area for mobile applications; OS Platform- they make the mobile itself useless; many other utility applications such as Maps, Location Based Services; Games, other entertainment applications – here the hackers take advantage of people's weakness to get glued to games and thereby ignore warnings.

Threats to mobile money transactions could be one of the most dangerous and painful security threat. The value of mobile payment transactions is projected to reach almost $630 billion by 2014. Mobile money transactions are an attractive target for attackers as they allow direct monetization of attacks.

App Vulnerability: Like desktop / laptop computers, mobile apps too suffer from a myriad of security vulnerabilities. Many of these vulnerabilities are unintentional, caused by poor programming practices. Vulnerabilities can also be intentional and malicious, hidden within a seemingly safe and legitimate app. Some security vulnerabilities occur when sensitive data is transmitted to and from remote servers over unencrypted channels. Perhaps the most severe app vulnerabilities are those that exploit lax security of stored data.

How does the Threat work?

In addition to analyzing the vulnerability, it is important to analyze the sources of such threats and how they manage to cause damage. The damage from a threat is a combination of source and channel to carry out the threat. While few of the main sources causing security threat are malicious applications, spyware and phishing besides many more, of which the commonly used channels are social networking, Bluetooth, Wi–Fi Hotspot and Botnets.

Briefly describing a few major ones – a Botnet is a collection of compromised devices connected to the Internet. The malware gives hackers remote control of the compromised devices, which can then be instructed to perform harmful acts. The easiest way for an attacker to benefit from a mobile Botnet is to send an SMS or multimedia message service (MMS) communications to a premium phone account that charges victims fees per message. Malicious applications are usually free and get on a phone because users voluntarily install them. Once on a handset, the programs steal personal information such

as account passwords and logins and send it back to the hacker. Social Networking has seen growth in enormous proportion with the similar growth in the use of smart phone. As fallout, mobile malicious links on social networks are effectively spreading malware. Participants tend to trust such networks and are, thus, willing to click on links that are on "friends'" social networking sites. Spyware available online are used to hijack a phone by hackers, allowing them to hear calls, see text messages and e-mails, and even track a user's location through GPS updates. Bluetooth enables direct communication between mobile devices. Such Wireless devices broadcast their presence and allow unsolicited connections. In the case of Wi-Fi, hackers intercept communications between smart phones and Wi-Fi hotspots. In such a scenario, with no encryption to protect transmitted data, the hacker gets in between the user and the hotspot provider and hijacks the session via a man-in-the-middle attack. Phishing poses the same risk on Smart Phones as it does on desktop platforms. Mobile phishing is particularly tempting because wireless communications enable phishing not only via e-mail, as is the case with PCs, but also via SMS and MMS. Social media phishing is becoming a major issue as social networking sites contain an increasing amount of personal information. So to sum it up, the way the threat works may be classified as follows:

- Intentional & Malicious Vulnerabilities: These are
  - Malware hidden within seemingly safe Apps – they attack OS and make the devices unusable.
  - Rogue Apps – they lead to some undesirable performances or even some intentional misdirected actions such as stealing personal data or money transfers
  - Attacking stored Data-once the access to the data is achieved, almost any misuse of someone's data is possible.
- Unintentional Vulnerabilities: these are mainly attributable to mistakes committed by users themselves such as not using password protection or weak password, download Apps without verification of source, unprotected use of mobile internet etc.
- Programming Practices & Languages: App developers at times fail to validate input from the Web, allowing adversaries to access protected files, or they might hardcode passwords, allowing unauthorized access to user files and the app's source code. Some vulnerabilities arise from the programming languages with which apps are implemented. For example, languages such as JavaScript open the possibility of attacks via those who exploit Web browser vulnerabilities. Older programming languages such as C are prone to a host of well-known security vulnerabilities, such as buffer overflows, heap overflows, format string attacks, etc. Using third-party libraries, regardless of the implementation language, can also open up the potential for vulnerabilities.

How to address the Threat?

At the core of addressing such security threat in the mobile environment are two basic concepts - Wireless Intrusion Detection System (WIDS) & Wireless Intrusion Prevention System (WIPS). Keeping these basics as the building blocks, it is required to focus at few specific approaches, including:

- Vetting the Apps by Purchasing organizations or a third-party labs before buying them is another approach. Currently, app stores don't incorporate a vetting process that thoroughly examines potential security vulnerabilities in apps. This is partly attributable to the cost and time associated with vetting an app, as well as the complex and contentious interactions needed with developers, given the growing potential for dangerous and widespread vulnerabilities, it's becoming increasingly critical to vetting apps for such vulnerabilities.
- Creating Strong Mobile platform with robust OS and associated with traditional safety approaches such as preventive measures like firewall and usage of anti-virus software.
- Increased usage Encryption software and encouraging more and more researchers and industry elements such as companies to work on this area. At present there are not many such apps as there development is complicated and challenging and the market is limited.
- Incorporating some regulatory aspects ensure and manage the usage of encryption software which takes into account some other associated aspects related to laws of the land, other security concerns of the government such as lawful interceptions to address crime and terrorism.
- Inclusion of certain E-Services that are specifically designed and developed to Protect Privacy such as vetting the mobile apps before they are allowed to be used, defining limits for accessibility to stored data etc. it's also necessary to vet the app store. However, the vetting process poses several challenges, such as specifying security and analysis requirements; identifying appropriate tools, mechanism, and approaches for analyzing security vulnerabilities and finding appropriate personnel to manually vet the apps.. and an infrastructure for testing the apps for security.
- Enhancing the scope of App certification process to pay special emphasis on the Trust & Security aspect of the App to be certified is another way to ensure threat avoidance from third party apps. Today the app certification approach and extent varies with platform – Java, Symbian etc.

- Education is key: It all comes down to education. Users have to be made aware of the threat and ways to protect their devices and Apps. But also it is important to build devices that protect the user without them having to make informed decisions – but as we have seen with PCs this isn't easy. Awareness about Mobile Access confidentiality is a simple and effective way which although already provided by the OEMs, the lack of awareness and the indifferent attitude of users pose a major challenge to the success of this approach.

Way Forward - Key suggestions

- Collaborative efforts: Considerable amounts of work is going on across the globe to address threat to the mobile security and associated entities. Unfortunately, a majority of all that are happening in isolation, in pockets. Major collaborative efforts are required, in highly organized manner to achieve the maximum out of all those efforts and to derive the best possible results optimally.. The coordination and collaboration is required to Create a Centralized Body (like ITU) who shall Formulate Regulatory Policies, define Standards, Tools & Test Beds, organize Coordination amongst different scattered research bodies and entities involved in developing mobile security measures and apps, organize consolidation and compilation of available and ongoing work and organizing their development and dissemination through industry sources. The International Advisory Group (IAG) within BIC can make major contributions in this direction through its supporting Core Working Group (CWG) and Extended Working Groups (EWG).
- Structured Management: In order to achieve the organized coordination, structured management approach is essential. Apex body at the core supported by bodies and groups formed function wise and region wise with similar dissemination further on to micro level ensuring the numbers of layers kept at bare minimum are essential to manage such huge, complex and critical objective.
- Focused Objectives: The research work has inherent weakness of growing out of proportion and at times also loosing focus. It is imperative at the part of the all coordinating and managing bodies to start the work with well defined objectives and stay focused on the same.
- Introducing specific Regulatory mechanism through ITU: In addition to the above, one of the most important and possibly most effective measure would be to create a mandatory regulated mechanism controlling security aspects right at the device OEM level. The greater possibility of these attacks will place an increasing importance on mobile device makers to include security features and configuration options in place. The central Telecom regulatory body ITU need to setup an empowered body within itself to impress upon the OEMs and ensure that suitable security measures are incorporated within the devices such that only certified applications be made available to users either for Free usage or paid ones. This aspect will of course impose certain restrictions on the genuine App developers but by way of keeping the costs of such certifications low (e.g. just few dollars) but at the same time making the tests procedures thorough and comprehensive particularly against any security threats, would go a long way in ensuring the safety of the mobile, mobile apps and mobile users.

Why is international cooperation important in this particular topic?

Today, the information and communication technologies, be it voice or data, has made the geographical boundaries irrelevant. Along with this today and more so in future, significant amounts of confidential operation like banking transaction, mail/ data exchanging will take place from mobile only. In addition, critical utility services management of power, water and other infrastructure services too besides services like health care and education would have mobile phones and apps playing major role. However, despite the world getting connected, the regional elements on the demands, requirements, behaviour and need of the people still vary to a great extent. At the same time the provisioning of the mobile systems - devices and applications are happening across the globe cutting across the regional boundaries. Devices and applications developed in one corner of the globe are equally utilized across the globe. The same is the case with the creation and proliferation of malware, rogue applications and such security risks. Accordingly, since the smartphone / mobile penetration is increasing globally, it makes a lot of sense that all regions of the world - Europe, Asia/ India/China, Americas, Africa collaborate closely for the Research & Industrial Developments. It is therefore not just natural but essential that the research and development work to address the threats and risks to mobile security is pursued with help of intense International cooperation and managed with globally collaborative mechanism.

Conclusion

As the spread and utilization of mobile devices grow, they will face risks of growing attacks in number and variety. It is critical to understand what is there to lose before a mobile security breach occurs. The ultimate goal is not about aiming to achieve something unrealistic -complete elimination mobile security risks. Such ultimate safety and risk prevention may not be possible. However it is rather essential to have

systems in place to minimize the impact when breaches occur. Towards this goal, there is need for regular and sustained work across all stakeholders - Device OEMs, App developers, VAS providers, Network Service Providers/ TELCOs and, last but not the least, the mobile users themselves to first, take the threat seriously and then, constantly participate in the lookout for threats and search for their solutions.

The full presentation can be found at http://www.bic-trust.eu/files/2012/04/4-ASharma.pdf

About the Author

Abhishek Sharma is founder, MD & CEO of Beyond Evolution Tech Solutions Pvt Ltd(beTS). Abhishek has built beTS from scratch developing many mobile application and Solutions offering niche Utility VAS as ASP to large mobile users through many large Telcos like Vodafone, BSNL, MTNL, Idea, Airtel etc in India and abroad. Prior to founding beTS, Abhishek has worked for Indian Air Force for about 22 yrs and then for large corporate in India and abroad such as Programme Manager, GSM Backhaul/ Microwave Services, Tata Telecom, India; Country Head – Telecom SBU at TCS/ Tata Infotech, India; MD at Globacom Cellular, Nigeria etc where he managed large ICT Projects & Operations such as Radar, Telecom NW, BSS, OSS etc. Abhishek is also a renowned consultant on Mobile VAS, Telecom Network, Radar Data Systems & Avionics. Abhishek is B.E. in Electronics & Telecommunications, M.Tech Computer Sc (IISc) & M.B.A. in Marketing..