Trust & Security for Mobile Communication Services – EU- India cooperation – Abhishek Sharma

Speaker: **Abhishek Sharma** is Co-founder, MD & CEO of NetEdge Tele-Solutions (NTS). He is a veteran of the ICT domain with authority on Telecom & Radar. Abhishek has a B.E. Degree in Electronics & Telecom Engineering, from GEC, Jabalpur, M.E. in Computer Sc & Automation from I.I.Sc, Bangalore, Masters in Management Studies from College of Defense Mgmt & M.B.A. in Marketing from IGNOU Delhi. His company develops mobile applications on Utility VAS for GSM/ CDMA mobile users. Abhishek is also international consultant on Mobile VAS, Telecom Network, Radar Data Systems and Avionics. He has rich experience of managing large business, Operations & projects, setting up GSM, CDMA, Satellite & Radar NW and BSS, OSS solutions. Abhishek has participated in many national 7 international seminars and events and has pitched novel product & solution ideas.

INTRODUCTION

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. Such is the case with mobile technology, particularly Smart Phones, which have exploded in popularity in recent years. Smart Phones becoming very popular among people and a considerable part of the population owns at least one of them. The main reason behind this growing popularity is the availability of variety of applications for them, be it for entertainment, utility or just better user experience. This popularity has attracted enough hackers to make the potential for serious security threats a reality. McAfee Labs' threat report for 2010's fourth quarter reported a 46 percent increase in malware targeting mobile phones over the same time period the previous year. More than 55,000 new pieces of malware are seen on a daily basis as per the report. Visiongain research shows that the number of mobile malware more than doubled in 2011 from 2010 with over 200 new variants in the first half of 2011 alone

Mobile devices are the fastest growing consumer technology, with about 600 million smart phones today to crossing 1.74 billion by the year 2012. Mobile applications are likewise booming. In June 2011, for the first time ever people on average spent more time using mobile applications (81 minutes) than browsing the mobile web (74 minutes). With this scenario, Mobile devices increasingly face various types of threats from mere Annoyance to invade privacy, propagation, malicious tools or Steal Money. Threat 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, up from $170 billion in 2010[5]. Vendors, retailers, merchants, content providers, mobile operators, and banks are all actively establishing new payment services. Mobile payments create an attractive target for attackers, as they allow direct monetization of attacks.

MOBILE SECURITY THREATS & MOBILE APP VULNERABILITY:

Security Threats: It important to analyze the sources of such threats besides analyzing the vulnerability. Mentioning a few major ones – **Botnet**, which 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 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 grown enormous as smart phone use has grown, so

has mobile Malicious links on social networks can effectively spread malware. Participants tend to trust such networks and are thus willing to click on links that are on "friends'" social networking sites, even though a hacker may have placed them there. **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. Wireless devices can broadcast their presence and allow unsolicited connections. Though on rare occasions, mobile malware has used Bluetooth to propagate. In case of Wi-Fi Hackers can intercept communications between smart phones and Wi-Fi hotspots. In this scenario with has no encryption to protect transmitted data., the hacker gets between the user and the hotspot provider and hijacks the session via a man-in-the-middle attack. **Phishing** poses the same risk on smartphones 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.

App Vulnerability: Like traditional applications for desktop / laptop computers, mobile apps too suffer from myriad 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.

SECURITY APPROACHES

Traditional Security Approaches: Mobile communications can use the same types of security-antivirus and firewall products as fixed communications. Vendors include Fortinet, F-Secure, Juniper Networks, Trend Micro etc. Mobile security software can also better use the cloud to offload some of the processing.

Mobile Encryption software is another approach but there are only a few such as Cryptech by Caspertech, Cellcrypt by Cellcrypt Mobile, ComSecure by NetEdgeTeleSolutions, Phonecrypt. They're scarce primarily because they're challenging and expensive to develop.

Vetting the Apps by Purchasing organizations or a third-party labs before buying them is another approach. . However, the vetting process poses several challenges, including specifying security and analysis requirements; identifying appropriate tools, mechanism, and approaches for analyzing security vulnerabilities and finding appropriate personnel to manually vet the apps. To foster the availability of only "safe" apps, it's also necessary to vet the app store. However Before you can analyze an application, you need an infrastructure for testing the application and reporting the results.

STATUS & DEMAND

Currently, app stores don't incorporate a vetting process that thoroughly examines potential security vulnerabilities in apps made available to consumers. This is likely due in part to the cost and time associated with vetting an app, as well as the potentially complex and contentious interactions needed with developers to resolve identified vulnerabilities. Given the growing potential for dangerous and widespread vulnerabilities, however, it's becoming increasingly critical to vet apps for such vulnerabilities, but in a cost- and time-efficient manner.

As the mobile ecosystem evolves and hackers probe for vulnerabilities, devices will face a growing number of a variety of attacks viz a viz those traditionally launched

against desktop systems. The need is to increase analyzing the attacks. The greater visibility of these attacks will place an increasing importance on mobile device makers to include security features and configuration options in place. Also to make it necessary that security is to be considered in all phases of application development to ensure that resiliency against attacks is built into mobile devices from the start.

Commercially, the global market for Mobile Security is projected to reach $14.4 billion by 2017, primarily driven by rapid proliferation of feature phones and intelligent mobile computing devices. Increasing use of mobile devices for accessing data services and corporate networks and the emergence of open network concept, which opens up potential risk avenues from security and privacy perspective will boost market prospects over the next few years. Robust demand from Asia-Pacific market also augurs well for the future of this market.

CONCLUSIONS

In future, there will be significantly more confidential operations like banking transaction, mail exchanging will take place from mobile only. In these cases, it is very necessary to protect the customer data and application from various attacks. Since the Smartphone/ Mobile penetration is increasing globally, it makes a lot of sense that large regions, particularly regions like Europe and India/ Asia collaborate closely for the Research & Industrial Developments. Many companies are already putting efforts in making their consternation for securing mobile data and application.

Finally, it's critical to understand what there is to lose before a mobile security breach occurs. The ultimate goal is not about completely eliminating mobile security risks but rather having the proper systems in place to minimize the impact when breaches occur. Well thought out controls involving the proper security technologies combined with the proper documentation and business processes are essential.

BIC CONTRIBUTION

Today, the realisation has come and lots of efforts are in progress at different locations, organisations & institutions and different levels towards addressing the issues related to Trust & Security. There is also lots of focus towards mobile Security. However all these efforts are happening largely in isolation and wherever there is any cooperation and coordination between different organisations, it is very limited. Focussed and targeted international cooperation shall play a major role in this massive & coordinating efforts for research, development and implementation of measures required to be taken to address this menace of the "breach of Trust & Security for Mobile". Towards this, BIC can and have to be a key player in ensuring this critical coordination. Following actions are suggested:

- Increase the degree and level of Industry participation from the level where it is today.
- An appropriate combination of SMEs and large corporate with balanced mix with research bodies would be ideal.
- Suitable selection criteria, based on result orientation & capabilities of the participants may be worked out.
- Special incentive coupled with delivery commitments be accorded to SMEs who are more oriented and geared up for faster deliveries.
- Increasing the frequency of interactions by way of seminars and events.
- Create a Project Management Team or a sub group under the Programme Manager, comprising of representatives from Institutions and industry (SME & Corporate) with defined leadership, targets & timelines.

A mobile has already become a full time companion. Soon it shall be a full time friend, philosopher & guide and all in one service provider. Most of the “Delivery of Services” shall happen through mobile, world over. It would not be any exaggeration to say that these are “desperate” times ensuring “Trust & Security for Mobile” and *desperate times need desperate measures.*