Phishing Attacks in Mobile Platforms

Thangavel M.
Thiagarajar College of Engineering, India

Yaamine A. M.
Thiagarajar College of Engineering, India

Nandhini J. T.
Thiagarajar College of Engineering, India

INTRODUCTION

Mobile phones are mainly targeted by malware and they can also be used in botnets. Mobile devices are equipped with high – end, power-intensive resources with more memory, and variety of sensors. These are mainly used to provide a majestic, rich and for a sophisticated purpose. As far as Windows and Mac dominate the laptop world, where Apple and Android rule the smartphone and the tablet universe. Mobile apps were offered for the general productivity and for information retrieval which includes email, calendar, contacts, messages, and weather information. Now a day's mobile phones are also targeted by phishing attacks. So we can't say that mobile phones are not only used to make calls. We can say that mobile phones are a small computer. Smartphones are mainly used for social media which usually means to affect the bottom line security.

In mobile devices, user interfaces are constrained in a very small screen. In mobile operating systems, there is a lack of secure application identity indicators. The end user definitely can't tell what the website he/she is interacting with most of the end users i.e. 60% of mobile users will enter a password at least twice a day. By launching an application stored through app store phishing application can be done. Most of the phishing applications are launched with the help of the Android app store. By reliving the sensitive information, the attacker can easily hack the details of the users. Trojan Activity should in a suitable way. This will direct the end user to make a mistake in the malicious application of a trusted one.

The goal behind phishing is data, money and personal information glomming through the fictitiously unauthentic website. The best strategy for eschewing the contact with the phishing web site is to detect authentic time malignant URL. Phishing websites can be tenacious on the substructure of their domains. They customarily are cognate to URL which needs to be registered (low-level domain and upper-level domain, path, query). Recently acquired status of intra-URL relationship is utilized to evaluate it utilizing distinctive properties extracted from words that compose a URL predicated on query data from sundry search engines such as Google and Yahoo.

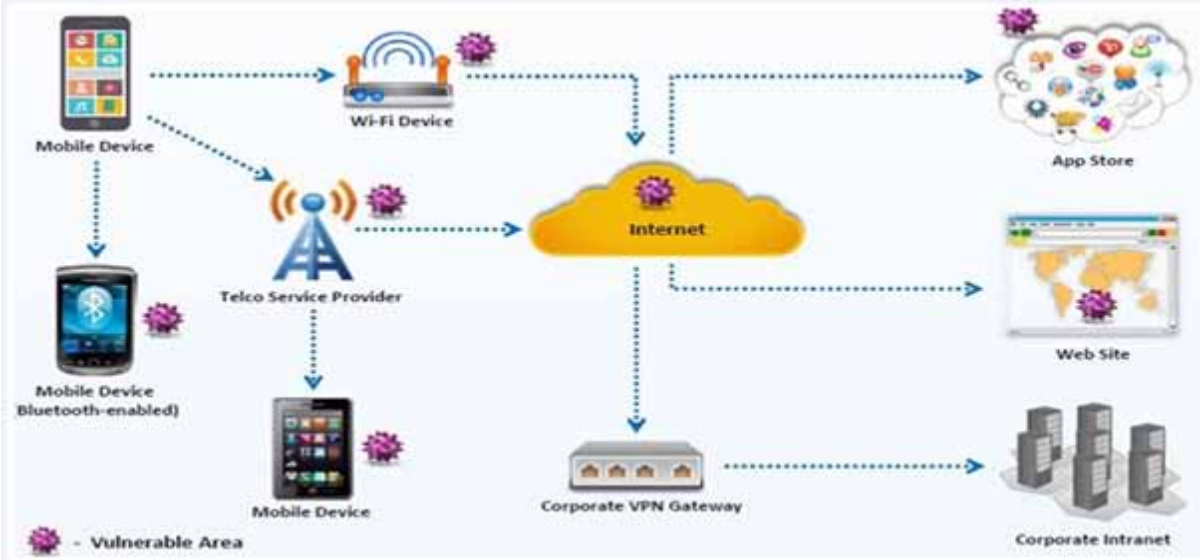
Now a day the threat of phishing attacks on mobile computing platforms is getting incremented as many of the users use mobile phones to access the net banking, Gmail, Face book and some other application. MobiFish is automated bulwark scheme, where users no desideratum to make the final decision, but it is the users who conclusively abstract the phishing app. Authentically, they do not require to explicitly make the decision at all, since the only explication for the authenticate failure is a phishing attack. Here there is no desideratum of developer to design the browser UIs, MobiFish is compatible with all subsisting websites and apps. In this paper, we propose specialized form of phishing attacks which target

DOI: 10.4018/978-1-7998-3473-1.ch084

at the sedulous account registry function of mobile OSs. We employ the optical character apperception (OCR) technique to extract text from the screenshot of a authenticate interface, which achieves better performance on mobile phones than on PCs.

Due to the lack of secure identity indicators which means that an inter-application link could be subverted. Next, the user will be directed to the wrong target. In a direct phishing attack, the sender will have some malicious application which links the user to the spoofed screen instead of the real target application. We are in need to address the problem of phishing by implementing the Trojan which commits phishing via preinstalled mobile applications. In a man-in-the-middle attack, the sender will be benign, but some other malicious party intercepts the link and he/she will load a spoofed target application in the place of the target application.

Figure 1. Vulnerable areas in mobile business environment



Trojan activity is a kind of malicious type which can be implemented in the built-in application. The trojan activity asks the user to enter some data that will appear in the form of a popup dialog. This popup dialog will collect some sensitive information. After finishing these steps the details collected will send to the hacker. The most vulnerable activity is sending the smishing messages this is also one of the phishing techniques. For example, a person gets a message that he needs to enter the bank details to claim some prizes. Through this activity, the attacker will get the sensitive information from the user so he can easily hack the mobile.

The other ways to hack the mobile by using Wi-Fi phishing. Wi-Fi Phishing will occur when a person gets connected to the internet through hotspots. If it is wireless, then an attacker will use evil twin for eavesdropping. If it is wired, then the attacker will use Starbucks for hacking the information. To overcome this, we can move to content-based filtering. It will have a set of rules which can easily predict the suspect the phishing contents.

Websites and mobile applications which commonly link the user to the social network which has password protected facility and obviously, payment applications. After it will ask the user to reflexively enter their basic information for gaining the credentials of the user to perform a phishing attack. By