Security threats to mobile devices and countermeasures essay examples

Law, Security

ASSIGN BUSTER

Over the past few years, mobile phone technology has evolved to fulfill the general role of the computation platforms. The mobile devices have gained advanced capabilities similar to the personal computers. However, the advancement of the mobile technology has made them more vulnerable to the attackers. With the advancement of technology, there is a possible increase of the security attacks and threats. Various mobile devices have open operating systems that are susceptible to executable formats that enhance major virus attack. Therefore, mobile devices call for security measures so that they can be able to achieve their objectives such as integrity, availability, and confidentiality. Solution must be developed to counter the risks of attacks and threats to the mobile devices so that this technology can sufficiently and conveniently accomplish its mission. According to the Government Accountability Office (GAO) report, " Mobile devices face an array of threats that take advantage of numerous vulnerabilities commonly found in such devices. These vulnerabilities can be the result of inadequate technical controls, but they can also result from the poor security practices of consumers," (Kaiser and Library of Congress, 2007) . It has been realized that, the threats to mobile devices are exposed to susceptibilities that continues to affect the security. There is an increased number of malicious software affecting the mobile devices rising from 14, 000 to 40, 000 in a period of one year. The relevant federal agencies together with private companies have implemented security steps to eliminate the anticipated worries in mobile devices. Despite the efforts, security controls have failed terribly and the recommended practices have proved to be futile.

Numerous problems and challenges associated with security threats to mobile devices continue to reveal themselves. For instance, mobile devices have the technical ability to accommodate passwords, pattern screen locks or PIN for authentication. In addition, some mobile devices have the capability to have a biometric reader that scans fingerprints in the process of authentication (Harkins, 2013). The problem regarding the instances above is that, the consumers rarely apply these mechanisms to ensure that mobile security is enhanced. For the users who decide to use passwords, they have a tendency to select easier passwords that can be predetermined, like 1111 or 0000. However, failure to set passwords in mobile devices gives the unauthorized users the chance to access the sensitive information in a lost or stolen mobile device.

The two-factor authentication is not put into considerations when performing sensitive transactions on mobile phones. Studies reveal that consumers apply the use of static passwords in places where the two-factor authentication opt to remain the best option. The use of static passwords in the authentication process presents security drawbacks, the passwords are easy to guess, forget, steal or eavesdrop. The two-factor authentication promotes an advanced level regarding mobile security than the traditional passwords and PINs. The power of the two-factor authentication is that it allows the user to include two different factors that offers a high-level security. Due to the inability to implement the two-factor authentication systems, the vulnerabilities are increased and third parties can easily access the sensitive information from mobile devices without their consent.

Another challenge affecting the operation of mobile devices is exposure to malware. Downloading certain applications introduces malware that affects the operations of the mobile device. Unknowingly, the malware might be downloaded disguised as either a game, security patch or other applications of help. The users find it difficult to notice the underlying difference between genuine applications and those containing malware (Kaiser and Library of Congress, 2007). For instance, an application designed with the inside malware may be downloaded into a mobile device and this may intercept the data in the devices. In addition, the wireless transmission allows the eavesdroppers to access sensitive information since that data is never encrypted.

During the manufacture of mobile devices, security software is not preinstalled to prevent the phones from malevolent applications, spyware and malware-based attacks. The users fail to take a further step to install the security software because they purchased the device without it. Similar software causes slow operations affecting the life of the battery on mobile devices. The absence of security software increases the prevalence of mobile devices to be affected by the viruses, spyware, Trojans, and spam that interferes with the confidential information of users.

Mobile devices operating systems may be outdated. The patching process takes time to be accomplished, and in most instances, they fail to be implemented in a timely manner. The devices may also be affected because of the failure of the security updates to be conducted in time. Considering the nature of vulnerability, many complexities are associated with the patching process (Harkins, 2013). For example, Google Inc. gives a solution to the Android OS by fixing the security weaknesses but leaves the manufacturers with the responsibilities to come up with specific updates to incorporate the vulnerability fix. The process requires much time and it can present interference to other mobile device operations.

The devices are also susceptible to exposure of unauthorized modifications that may damage the way security is handled. " Jail breaking" appears useful since they give a chance to users to access the operating system of the mobile devices and license the installation of unauthorized software. For the users who take advantage of the jailbreak to install applications, they increase the risks and break the rules of the manufacturer (Kaiser and Library of Congress, 2007).

Mobile technology exposes devices to various threats such as BlueBugging, bluejacking, Bluesnarfing, Cryptanalytic, Device Cloning, Eavesdropping, Falsification of Content, and Man-in-the-middle attack. The first three threats are applicable to the mobile device Bluetooth technology. BlueBugging and Bluebugging threats commonly attack the mobile Bluetooth technology allowing the attacker to access the victim's phone, and, therefore, he can undertake any activity on the attacked mobile device (Sathyan & Sadasivan, 2010). When the Bluetooth is enabled, the Bluejacking threat allows the attacker to send spontaneous message to the victim's phone. Device cloning involves the electronic identity of one device so the subscriptions, calls and purchases are charged on the victim device. This threat also allows the attackers to hack the information of the cloned device. The Eavesdropping allows the attacker surreptitiously to listen to the victim's mobile conversations without having the owner's consent. The attackers can also edit the owner's information or content through the Falsification of Content threat. Man-in-the-middle attack allows an attacker to intervene illegally with the conversation messages making the victims believe that they are communicating directly.

However, technology is put in place to provide, procedure, device, action or other measures that can be used to counter the threat to the mobile device systems. Various software are developed to promote the protection of the mobile devices. For example, Software-Based Fault Isolation is a technique applied to neutralize the untrusted programs that are written in illicit language such as C. this software allows such programs to be executed in a safe and appropriate manner “ within a single virtual address space of the application” (Sathyan & Sadasivan, 2010). This software transforms the interpretable code modules of the untrusted device so that all memory accesses are restrained to data and code segment in their fault domain. This technology is known as sandboxing.

Some of the technologies that are commonly used to countermeasure the threats of mobile devices include the out-of-band and mutual authentications. Out-of-band authentication involves techniques that allow the user of the mobile devices to verify the transaction before completing it. The verification channel is different from the one used by the user to initiate the transaction. Whenever the online transaction is engaged, the user is required to verify the transaction using the number based code that is send through email, SMS and telephone calls among others. For example, the Gmail account enables the users to verify their account before accessing it using the telephone call or the text send to the user’s mobile device. On the other hand, the mutual authentication is a two way process that allows the involved parties to validate each other before they initiate a transaction to ensure that the transaction is conducted on a safe environment (Jansen, 2000). For instance, the Secure Socket Layer (SSL) allows the two-way authentication and confidential communication using the cryptography technology. Through the http requests, a systematic authentication between the informed users is used to enhance security of the information transmitted.

Technology has also promoted the use of a digital signature and one time password (OTP). The Public Key Infrastructure (PKI) maintains a certificate that allows the use of the digital signature that authenticates the information shared by the users. Through the digital signature, the receiver of mobile information can confirm that the source of the information is sent by authorized and known person. According to Jansen (2000), OTP guarantees the confidentiality of the information flowing between the sender and the receiver. On the other hand, the OTP is a valid password that is created to for only single session and is regenerated every time the owner ought to use it. The one-time passwords are not prone to attacks or other threats because they are randomly generated after every session.

Currently, the mobile service providers have adapted the Service Provider Validation. This validation ensures that all the mobile devices have built in fingerprint that allow transmission signal to be unique irrespective of the device changes of MIN or ESN. This solution is significant to the device cloning allows the attackers to clone the victim's information illegally. The service providers are able to identify the cloning devices with these fingerprints and the MIN or ESN. Other technological solutions to the mobile device security threat include the use of the GPS (Global Positioning System), multifactor authentication, memory/files encryption and poison and pill messages.

As expounded above, numerous challenges interfere with the security to mobile devices. The users are exposed to various hurdles that affect the operations of mobile devices when measures are not taken into place. The manufactures have and continue to introduce mobile technology applications that help to prevent the threats to these devices. To sup up, the counter measures offer solutions to the security threats observed in mobile devices

References

Harkins, M. (2013). Managing risk and information security: Protect to enable. New York: Apress.

Jansen, W. A. (2000). Countermeasures for mobile agent security. Computer Communications. doi: 10. 1016/S0140-3664(00)00253-X

Kaiser, F. M., & Library of Congress (2007). GAO: Government Accountability Office and General Accounting Office. Washington, D. C: Congressional Research Service, Library of Congress

Sathyan, J., & Sadasivan, M. (2010). Multi-layered collaborative approach to address enterprise mobile security challenges. doi: 10. 1109/COSEC. 2010. 5730691