Government Mobile Apps Security Assessment and Strategy

Malintha Liyanage

School or Institution Name (University at Place or Town, State)

**Government Mobile Apps Security Assessment and Strategy**

**Introduction:**

During the last few decades' information and communication technologies have made tremendous improvements and the journey still continues. We are living in a mobile communication age. The advent of mobile phones and cellular networks was not thought to be that much powerful. People rely more and more on their handheld devices instead of mainframe computers. Modern mobile phones are more powerful than earlier supercomputers. They are capable of handling massive processing loads that were not manageable by third generation mainframe computers. That shows the immense power of mobile technologies and investments being made in the technology by global technology giants. Mobile phones are continuously being improved (Abelson et al., 2015). Given the fact that digital paradigm has shifted from mainframes to mobile environments, the government has also decided to be mobile friendly. It is evident by the public law in which the federal government has regulated that any agency going to build a public website must ensure that it is mobile friendly. The regulation issued in 2017 is not directing government agencies to start from scratch, but any new public facing website must be mobile friendly.

 The immense power of mobile phones is due to the application technologies that can be supported on a tiny platform. People rely more on their mobile devices from online shopping to anything digital that can be imagined. Modern mobile phones are capable of measuring heartbeats using sophisticated sensors and algorithms used in their driving applications. Various government agencies have already launched their mobile apps to bridge the gaps between the public and their representatives in power. These applications provide extensive possibilities form lodging complaints to get useful services. There is no need to visit any physical office of the state agency; their mobile app will address most of the cases remotely. Such as a useful mobile application developed by the federal government known as MyTSA that can solve queries related to the materials that can be allowed for air travel on an airplane (Enenkel et al., 2015). Most of the applications linked to governments services collect and process personally identifiable information of citizens such as name, sex, address, and social security numbers. Therefore, protecting such information is the obligation of the government as well. These applications must be based on secure architecture to ensure confidentiality, integrity, and availability of data being processed by the application. The government has provided application developers with the requirements of application security that must be ensured for an application compatible with government services.

**Government’s Requirements for Mobile Applications Security:**

The government has taken an initiative to be more mobile friendly by building mobile compatible websites and applications. As these applications deal with the personally identifiable information of citizens, these applications have become a potential target of cybercriminals. They can compromise mobile devices with malicious applications to gain access to an individual's data and breach privacy. In order to make the mobile ecosystem more user-friendly government has issued guidelines and security requirements for mobile applications security. Usually, mobile applications are provided to the general public through an application store hosted by the operating system vendor or any other third party (Kotz, Gunter, Kumar, & Weiner, 2016). The federal government requires by law extensive testing of the application before its launch to the general public. Application developers must perform aggressive testing of the mobile application in real-world environments before releasing it at a larger scale. The testing phase of applications is known as the beta phase that is issued with a warning that it must be used with caution and should never be used on production devices as it may cause stability issues. Voluntary beta testers help application developers to identify and resolve any potential issues that can be targeted by criminals before the public release of the applications.

 Most of the mobile applications require specific permissions on the target device on which they are being used. Such as an application that provides weather information may require access to the geolocation of the device. The government requires the application developers to explicitly ask for permission of the user as a particular user may not want to reveal geolocation of the device. As the applications collect usage data or certain patterns of the data, application developers are required to limit the data storage. For example, if an application does not require the access to the location of the mobile device, the data related to the location of the device must not be stored or processed by the developer (Downer & Bhattacharya, 2015). Majority of mobile applications require users to create an account on the remote server of the developer to use the full functionality of the application. These user accounts are often accessed by a combination of usernames and passwords. Application developers are required by the government not to store passwords in plain text format. Storing credentials in plaintext format makes them potentially vulnerable to security and privacy threats.

**Industry’s Requirements for Mobile Applications Security:**

Mobile application development industry also provides guidelines to the application developers for securing mobile applications against possible security breaches. Any mobile application developer must not rely on the platform security features of the target device. Security must be built in the application as well to raise further the bar for cybercriminals to breach the security infrastructure of mobile devices. Most of the mobile applications are built using open source software libraries. Open source software is a piece of software that is provided to the general public, and it can be used in any way. There are benefits and drawbacks to this approach.

Open source code and software development kits allow programmers to base their work on proven architectures and technologies. On the other hand, it will be easier for criminals to use the same code to exploit the existing application infrastructure. Application developers are required to carefully examine the available code for security holes before using it as a baseline for new applications. It will help them in the identification of vulnerabilities in the system (Serra, Carvalho, Ferreira, Vaz, & Freire, 2015). Many applications send data and communicate with the server maintained either by the developer itself or any third party. The developers are required to verify the security of the server an application is connecting to. Any compromised server may contaminate the whole mobile ecosystem. Applications dealing with health-related data must comply with data protection regulations and standards of healthcare systems. Otherwise, applications and user data will be at higher risk of being stolen or misuse by criminals infiltrating the defense systems.

**Recommendations:**

All of the mobile applications connect to the corresponding server using wireless fidelity network. As the internet itself was not designed with much security in mind, any application relying on the network for proper functioning must implement cryptography to protect user information. Applications must not use Rivest Cipher version 4 of cryptography for communication. As the algorithm use symmetric keys and repeats the same key of encryption after five thousand internet packets to encrypt the contents of the packet. Therefore, an attacker can compromise such a system in just four hours analyzing sniffed packets from the network. Mobile devices must be physically secured as well. Most of the mobile devices allow manual disks for storage, all of these disks along with the internal storage of the device must be encrypted using sophisticated encryption algorithms. It will keep the data on the device secure and intact even if the device is lost or stolen. Criminals will not be able to recover any useful information from the encrypted device. Many modern devices are equipped with a trusted platform module that is a hardware component for cryptographic keys generation and credentials storage. Mobile applications must support trusted platform module chips to protect user information. These measures will reduce the attack surface of mobile devices and will reduce the risk of being compromised.

**Summary:**

People rely more on mobile devices and applications for their digital needs. The government has initiated to make government websites mobile friendly in an attempt to utilize the potential of mobile platforms. Government applications and other third-party applications are required by law to be secured. Applications must be designed based on the security frameworks designed by the government and industry specialists. Extensive testing and vulnerability management systems using mobile device management platforms will reduce the risk of security issues and privacy concerns of the users. Communications to the remote server must be protected by deploying transport layer security and cryptographic algorithms. Sticking to the requirements of security will help create a secure mobile ecosystem capable of handling future challenges as well.

References

Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., … Neumann, P. G. (2015). Keys under doormats: mandating insecurity by requiring government access to all data and communications. *Journal of Cybersecurity*, *1*(1), 69–79.

Downer, K., & Bhattacharya, M. (2015). BYOD security: A new business challenge. In *2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity)* (pp. 1128–1133). IEEE.

Enenkel, M., See, L., Bonifacio, R., Boken, V., Chaney, N., Vinck, P., … Anderson, M. (2015). Drought and food security–Improving decision-support via new technologies and innovative collaboration. *Global Food Security*, *4*, 51–55.

Kotz, D., Gunter, C. A., Kumar, S., & Weiner, J. P. (2016). Privacy and security in mobile health: a research agenda. *Computer*, *49*(6), 22–30.

Serra, L. C., Carvalho, L. P., Ferreira, L. P., Vaz, J. B. S., & Freire, A. P. (2015). Accessibility evaluation of e-government mobile applications in Brazil. *Procedia Computer Science*, *67*, 348–357.