Project 3: Government Mobile Apps Security Assessment

Malintha Liyanage

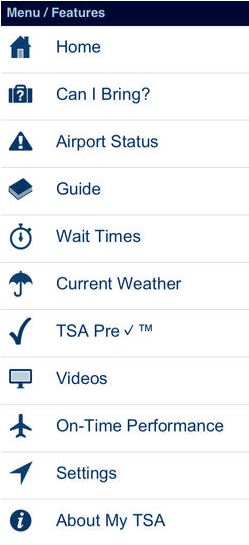
School or Institution Name (University at Place or Town, State)

**Government Mobile Apps Security Assessment**

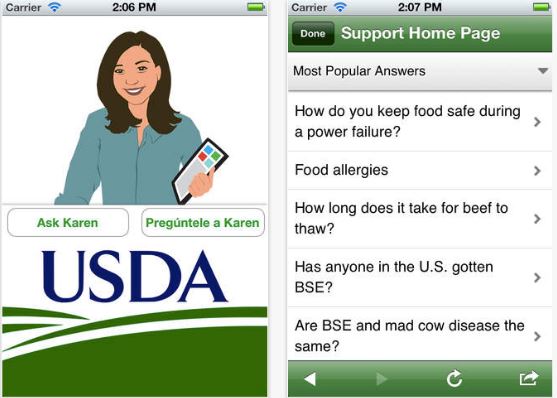
**Introduction and Background:**

Information and communication technologies have brought up the revolution in mobile communications. Mobile phones are now turned into powerful computing devices capable of replacing mainframe computers in typical business environments. Modern mobile devices are equipped with powerful hardware components. They are capable of performing tasks that require massive computing powers. Given the fact that mobile phones and other mobile computing devices are now exponentially penetrated into the daily life of people, governments and businesses are going to be more mobile friendly in their digital services (Shovon, Roy, Sharma, & Whaiduzzaman, 2018). Depending on the requirement for the mobile-friendly digital infrastructure in government institutions a regulation was enforced in 2017 by the federal government of the United States. The regulation is also known as the connected government act that provides initial guidelines for federal and state government agencies to make their websites mobile friendly. They are also required to provide the general public with mobile applications of corresponding digital government services.

As a result of the connected government act of 2017, government agencies are making their digital infrastructure more mobile friendly by developing useful mobile applications. Mobile applications provide similar functionality in an intuitive user interface that provides better user experience to end users. To reduce the gap between the public and their elected representatives, many government institutions have already published their mobile applications (Sharma, Al-Badi, Rana, & Al-Azizi, 2018). Depending on the functionality provided by these mobile applications, there is no need for an individual to visit the physical office of the agency. All of the services can be availed by using the designated application of that particular department. One such application is developed by the federal government known as MyTSA. The application provides useful information about the things that can be included in the air travel luggage. People can get useful information about their favorite items that whether they can be taken to the airport or not. The user interface of the application is shown in the following figure.



To educate people about food safety an amazing application has been developed by the Department of Agriculture known as Ask Karen. The application provides information such as how to check if certain fruits or vegetables are fresh or not. A huge collection of such questions can be answered by the application without any issues. The user interface of the application is shown in the following figure.



Many other useful applications are available to the public by the government such as *“Find a Health Center”* app provides people with an initiative way of finding nearby health centers actively funded by the federal government. FEMA application not only trains citizens for emergency conditions but already affected citizens can register for help from designated government agencies as well. The paradigm shift for moving more and more information to mobile applications and other mobile-friendly information resources will continue to grow in the future as well. Mobile applications that are linked to the information technology infrastructure of the government, usually process personally identifiable information of the users (Matthews, Uzairue, Noma-Osaghae, Enefiok, & Ogukah, 2018). Personally identifiable information collected by such applications may include names, physical addresses, sexual orientation, and social security numbers, etc. Processing of sensitive information and connections to the critical government infrastructure has made mobile applications a potential target of the cyber-criminals. Any possible breach of personal data collected by such applications can bring severe consequences and public reaction for the government. Therefore, it is the sole responsibility of the government to make the mobile application ecosystem secure to provide useful services to the public. The federal government has already issued guidelines for mobile applications developers to create secure applications that can be used with critical information infrastructure.

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

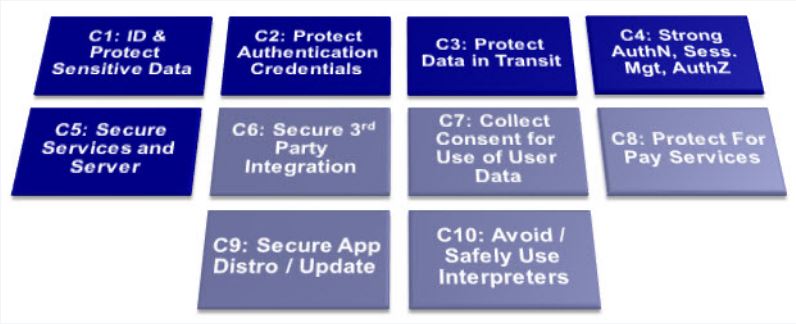
Mobile applications intended to be used in critical information technology infrastructure of the government must be developed with security in mind. The federal government issued comprehensive guidelines for security engineers to ensure that mobile applications for government services are secure enough to be trusted with personal and critical information. Testing an application in real-world environments is a key task in mobile application development. As per the government approved regulations any applications before its general public release must go rigorous testing both in laboratories and in the limited general population as well. Security experts may use authorized penetration testing tools to verify the security code implementation in the application. Cybercriminals use available security holes in applications as an attack vector. Security testing of the applications can ensure that there are no known security holes in the application. Any programmer rushing towards the publication of the application without appropriate testing may invite a disaster for the critical infrastructure of government agencies. Typical testing requirements are shown in the figure below.



It may not be feasible for some critical applications to perform beta testing with limited public exposure of the application. However, to overcome such problems in application development, pre-examined and approved software development kits can be used by the government agencies as a baseline development method for their application (Stickle, Moses, & HOLLAND, 2019). Use of approved development kits will reduce the risk of security loopholes in application algorithms that can otherwise slip through the testing procedure. It is required by the government regulations for the mobile application developers to model threats for the intended application usage as accurately as possible following the testing cycle. Most of the applications require integration of API to connect with backend government infrastructure. The integration must be tested and firmly deployed without any known security holes in the integration of API's. Potential security loopholes can be compromised by the criminals to damage the reputation and information technology infrastructure of the government institutions (Williams, Levi, Burnap, & Gundur, 2018).

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

As compared to government agencies, private business entities are also developing mobile applications. Software engineers working in the industry are well aware of possible security threats to mobile applications. To create mobile ecosystem more secure for end users, industry experts have outlined secure practices for mobile application development as well. OWASP project is a well-known project by the industry that is intended to help mobile application developers with the security standards and requirements (Goldsmith et al., 2018). OWASP and the European Network and Information Security Agency have collaborated and outlined ten essential controls for secure mobile application development. The following figure shows the essential controls required by the industry in mobile application development.



As the threat landscape for mobile applications is evolving consistently, it is required by the industry that the mobile applications must be compliant with CIA triad. CIA triad is ensuring the confidentiality, integrity, and availability of the data either in rest or in transit. Mobile applications must use sophisticated encryption algorithms such as the advanced encryption standard (AES-256-bits) encryption mechanism to comply with CIA triad. Many applications send data and communicate with the server maintained either by the developer itself or any third party (Kartikadarma, Listyorini, & Rahim, 2018). Server and backend connectivity in mobile applications is often governed by integrating various API's into the application. Before implementing a particular API, it is the responsibility of the developers to check for security measures on the server side as well. Cybercriminals can exploit poor API integrations for distributed denial of service attacks. In a distributed denial of service attacks, attackers use a network of infected devices known as the network of bots to create fake traffic targeted at a particular computer. The fake traffic generated by the botnet will block the access of legitimate users to the service due to the congestion on the communication link. Developed applications must have inbuilt security mechanisms to render such cyber-attacks useless.

**Recommendations:**

Most of the time mobile applications transmit sensitive information on wireless networks that pose serious risks to privacy and security of information. Encryption algorithms must be used to encrypt sensitive information before transmitting it over insecure wireless channels such as WiFi networks. Most of the modern mobile devices include a hardware chip known as trusted platform module that is used to generate and store critical cryptographic keys. As any of the encryption systems are as secure as the keys associated with the encryption algorithm. Therefore, mobile applications must be compatible with the trusted platform module. In earlier days of internet a stream cipher known as Rivest Cipher 4 was the most common algorithm of encryption. However, severe security flaws have been discovered in the cryptography algorithm by the RC4NoMore project (Huq, 2015). It must not be used in mobile applications connecting to government services. The algorithm is considered to be flawed in all conditions because it repeats the same key of encryption after every five thousand IP packets. The algorithm can be cracked in just four hours by analyzing sniffed packets from wireless networks. More sophisticated and modern algorithms must be used in application development as required by the industry standards as well.

**Summary:**

Mobile devices have changed the way people perform everyday tasks. Today's population is relying on mobile devices for everything from shopping to driving their cars. Depending on the shift in the computing paradigm, governments across the globe decided to go digital as well (Tripoli & Schmidhuber, 2018). Various government services are being offered by mobile applications developed by government agencies. Such mobile applications provide people with flexibility and ease of use (Yan, 2018). Mobile applications developed by government agencies often process sensitive information. Therefore, secure programming and design guidelines must be followed by the application developers to ensure the security and privacy of sensitive data. Experts in private mobile application industries have also prepared guidelines for developers to create secure applications. Encryption algorithms and secure key management must be used in mobile applications to create the mobile ecosystem more secure.

References

Goldsmith, M. A., Papo, A., LOMBARDI, R. J., Mulaosmanovic, J., Almalki, N., McBride, B. E., & RABINOVITCH, P. M. (2018). *Mobile communications device providing heuristic security authentication features and related methods*. Google Patents.

Huq, N. (2015). Follow the data: Analyzing breaches by industry. *TrendLabs Research Paper*.

Kartikadarma, E., Listyorini, T., & Rahim, R. (2018). An Android mobile RC4 simulation for education. *World Trans. Eng. Technol. Educ*, *16*(1), 75–79.

Matthews, V. O., Uzairue, S. I., Noma-Osaghae, E., Enefiok, M. K., & Ogukah, P. J. (2018). Implementation of a Community Emergency Security Alert System. *Implementation of a Community Emergency Security Alert System*, *3*(6), 475–483.

Sharma, S. K., Al-Badi, A., Rana, N. P., & Al-Azizi, L. (2018). Mobile applications in government services (mG-App) from user’s perspectives: A predictive modelling approach. *Government Information Quarterly*, *35*(4), 557–568.

Shovon, A. R., Roy, S., Sharma, T., & Whaiduzzaman, M. (2018). A restful e-governance application framework for people identity verification in cloud. *International Conference on Cloud Computing*, 281–294. Springer.

Stickle, T. C., Moses, C. J., & HOLLAND, R. C. (2019). *Computer security threat correlation*. Google Patents.

Tripoli, M., & Schmidhuber, J. (2018). Emerging Opportunities for the Application of Blockchain in the Agri-food Industry. *FAO and ICTSD: Rome and Geneva. Licence: CC BY-NC-SA*, *3*.

Williams, M. L., Levi, M., Burnap, P., & Gundur, R. V. (2018). Under the corporate radar: Examining insider business cybercrime victimization through an application of routine activities theory. *Deviant Behavior*, 1–13.

Yan, Z. (2018). Big data and government governance. *2018 International Conference on Information Management and Processing (ICIMP)*, 111–114. IEEE.