Securing Digital Government Services

Malintha Liyanage

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

**Securing Digital Government Services**

**Introduction:**

Government is providing various information services to the general public digitizing the infrastructure of information processing systems. Websites of government services act as the front end presented to the general public to ensure better user experience. Most of the sites operated by government departments provide users an interactive window to interact with the backend server. The server is considered to be the main source of information being offered by the website. Digital technologies have been revolutionized with the advent of web applications and web servers. Government is utilizing these web technologies as well to provide the general public with hassle-free service delivery (Nica, 2015). As most of the time, government-owned digital services host critical information such as personally identifiable information of citizens and information related to national security. This type of information handling at the back end of digital services make them a potential target of cybercriminals. They are always devising new and improved attack methods to compromise such services.

As these services host, critical information assets their protection is the obligation of federal government as well. Increased penetration of internet technologies has changed the war fronts from physical grounds to cyber warfare. Rival states can hire services of criminals for state-sponsored attacks on digital government services such as websites related to defense department or department of homeland security (Carter, Weerakkody, Phillips, & Dwivedi, 2016). Hackers can compromise and take down any website if there are not enough protective layers to protect the critical assets of the nation. The paper describes the threats to digital government services such as data.gov, disasterassistance.gov, and healthcare.gov. The paper provides recommendations to harden the security of such government-owned digital services.

**Information Services Provided by the Websites:**

The government provides many digital services to the general public through designated websites. Three of such websites are reviewed in this paper. Data.gov is the initiative of the federal government that provides researchers access to the data collected by various departments of the government. Website host large data sets in the back end database server operated by the government departments. Data is stored in the back end server and can be accessed by the general public. The website is intended for researchers working in a variety of disciplines. As the website host massive amounts of sensitive data in the back end database server, it is categorized as a high impact website for security and privacy issues. As the critical nature of data being stored in the back end of the website make it an ideal target of cybercriminals. The site is vulnerable to hacking and malware attacks.

Second valuable digital service provided by the government is healthcare.gov providing healthcare professionals, and individuals extended healthcare facilities. The website enables individuals to register for or enroll in healthcare insurance schemes offered by the government. It maintains a record of eligible members as well as all of the new registrations. Users are required to create an account on the website that will serve as a dashboard for their healthcare needs. The account is secured by password-based authentication systems (Abu-Salma et al., 2017). The website is accessible and provides service at the national level and is not confined to a specific territory within the United States. Depending on the information the website is dealing with, it is categorized as a high impact for security and privacy as per the federal information protection standards framework of digital data security. The website can be compromised by phishing or spam campaigns deploying social engineering tactics.

Third valuable digital service offered by the government is disasterassistance.gov that provides assistance and advice in case of a national level disaster experienced by any state in the United States. Website stores historical data and provide access to it using the front end website. It is hosted on servers owned by the government department. The website provides services at the national level; any territory experiencing disaster can benefit from services offered. Based on the valuable data the website is storing, it is rated as a moderate category for security and privacy issues as per federal information protection standards and frameworks.

**Inherent Security Issues of Web Applications:**

As the internet itself was not designed with much security in mind, any service offered as an over the top service on the existing infrastructure of the internet will be inherently insecure. Web services are based on the backbone infrastructure of the internet which is not secure by design. So, all of the web services are inherently insecure. However, there are security solutions that can protect information being shared over the internet. All the websites either owned by the government or individuals are prone to hacking attacks. Although there may be some rigorous security checks in place all of the logical measures can be broken using sophisticated attack methods (Grassi, Garcia, & Fenton, 2017). In digital initiatives like open data provided by the government the basic goal of securing the service is to protect the confidentiality, integrity, availability, and non-repudiation of the data. Confidentiality of the data can be compromised if the website security is breached by the criminals. Such websites are protected with firewall solutions, but these solutions are inherently insecure as a firewall only prevent outside attacks. Any network attack initiating from within the network can bypass firewall defense.

Website providing healthcare services provides username and password facility to authenticate and authorize users to access the records stored by the website. Password-based authentication systems are prone to man in the middle attack. Any attacker can sniff network packets to steal credentials. As the website uses transport layer security and secure sockets layer protocol to transfer information to and from the server such attacks may not be successful. However, a popular attack vector known as phishing can bypass the security seal. An attacker can design a website login page similar to the originals one impersonating valid page and asks for credentials of the user potentially compromising personal health records and insurance information of individuals. Such attacks are on the rise and rapidly changing in their design to obfuscate their presence and avoid detection by phishing filters on host machines.

**Recommendations:**

As it is evident by the above discussion that all of the web resources are prone to sophisticated attacks, there are some best practice based recommendations that can render most of the attacks useless against government’s digital services. Combining the password-based authentication system with certificate-based authentication systems can rule out the potential risk of phishing attacks on such services. Certificate-based authentication systems use public key infrastructure for encryption and decryption of data being transmitted over the network (Bertot, Estevez, & Janowski, 2016). A certificate is essentially a public key having a corresponding private key as an asymmetric encryption algorithm used in public key infrastructure uses different keys for encrypting and decrypting the data. Digital certificates and signatures authenticate any client to the server and vice versa. It also provides integrity of the data being transmitted on top of the confidentiality of the data.

To complement firewall solutions, an intrusion detection system can be implemented as well. The network-based intrusion detection system will monitor the network for any unusual network activity that may be a result of malware attacks on a particular host. Attackers can use code obfuscation or file less exploit to trick intrusion detection systems. The solution is to deploy reverse proxy and segregation of network resources. Segregation will protect the whole network from being compromised in a targeted attack. Reverse proxy will block forged access requests to a protected server such as one hosting the open data provided by the government. Cyber-attacks on web services are constantly evolving not only in number but in complexity as well. There is no single bullet to rule them out. However, the use of preventive technologies can reduce the damages caused by the attack if successful.

**Summary:**

All of the services offered over the backbone infrastructure of the internet are prone to malicious attack by various sources. It is not possible to protect any resource against all types of perceived attacks. However, best practice based recommendations and security solutions can reduce the risk of attack significantly. There is a tradeoff between security and usability of the system in this regard. A more secure system will be less useable by the public. For example, a most secure system will be one buried in concrete under the earth disconnected from everything even the power source as well. But practically that system will be the most useless system as well. So, the best practice is to use a balance between security and usability of the system. Best practice recommendations are based on this security and usability tradeoff.

**References**

Abu-Salma, R., Sasse, M. A., Bonneau, J., Danilova, A., Naiakshina, A., & Smith, M. (2017). Obstacles to the adoption of secure communication tools. In *2017 IEEE Symposium on Security and Privacy (SP)* (pp. 137–153). IEEE.

Bertot, J., Estevez, E., & Janowski, T. (2016). *Universal and contextualized public services: Digital public service innovation framework*. Elsevier.

Carter, L., Weerakkody, V., Phillips, B., & Dwivedi, Y. K. (2016). Citizen adoption of e-government services: Exploring citizen perceptions of online services in the United States and United Kingdom. *Information Systems Management*, *33*(2), 124–140.

Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017). Digital identity guidelines. *NIST Special Publication*, *800*, 63–3.

Nica, E. (2015). Sustainable development and citizen-centric e-government services. *Economics, Management and Financial Markets*, *10*(3), 69.