WHITE PAPER #2

Mobile App Security Assessment & Strategy

DeBora King

CSIA 360 7980

Cybersecurity in Government Organizations (2172)

April 9, 2017

University of Maryland University College – Spring Semester, 2017

INTRODUCTION

In 2012, federal government agencies were charged with creating at least two mobile apps to comply with President Obama's digital government plan (Kamensky and Wedge, 2016). With over 90 percent of Americans owning cell phones (most of which use smart phones), this order is quite fitting for today's society. According to AgileLoad, the majority of Americans spend as many as 2.7 hours a day on mobile apps (AgileLoad, 2013). With this growing demand comes the need for the ultimate "mobile-friendly" user experience – to be easily accessible, easy to navigate, and provides useful information or services that enhances daily life. Delivering these services must be accompanied with ensuring the user's personal identifiable information (PII) is protected and that use of the app is safe and secure. By mobile apps being so prevalent in our society, it gives the Federal Government the opportunity to exercise its Digital Strategy. The three objectives of the Digital Government Strategy is to "1) enable the American people and an increasingly mobile workforce to access high-quality digital government information and service anywhere, anytime, on any device; 2) ensure that as the government adjusts to this new digital world, we seize the opportunity to procure and manage devices, applications, and data in smart, secure and affordable ways; and 3) unlock the power of government data to spur innovation across our Nation and improve the quality of services for the American people" (Digital Government Strategy, 2012).

The objective of this whitepaper is to present a strategy for developing an award winning digital government mobile app for the upcoming Mobi-Gov awards. In order to accomplish this goal, it is beneficial to see examples of mobile apps that excel in user satisfaction (i.e., the best of the best). In addition, this paper will examine the federal government's requirements and recommendations on mobile app security architectures and design recommendations along with industry recommendations for security architectures and risk reduction. Finally, this paper will offer best practices recommendations as a strategy for building security into a new mobile app as a winning product entered into the Mobi-Gov awards contest.

BEST OF THE BEST GOVERNMENT MOBILE APPS

In order to develop an award-winning government app, it is beneficial to see examples of apps that have earned the highest recognition for its design and functionality. These are the type of apps that will be the ones to beat in competition for the Mobi-Gov awards contest. USA.gov names Smart Traveler *(Fig. 1)*, the FEMA app *(Fig. 2)*, IRS2Go *(Fig. 3)*, and Dwellr *(Fig. 4)* among the best government mobile apps of 2016 (USA.Gov, 2016). The chart below is a description of these apps that have been recognized as being innovative for delivering government information and services to mobile devices.

The **Smart Traveler App** offered by the U.S. Department of State can be downloaded on a smartphone, and the user can register for the Smart Traveler Enrollment Program (STEP) directly from the phone. Signing up for STEP through travel.state.gov gives the State Department information about your overseas travel plans. With the user registered, the State Department will have record of their area of travel and is equipped to provide resources in the event of a global crisis in that area, for example, the location of the U.S. Embassy can be at the user's fingertips (Porter, 2016).

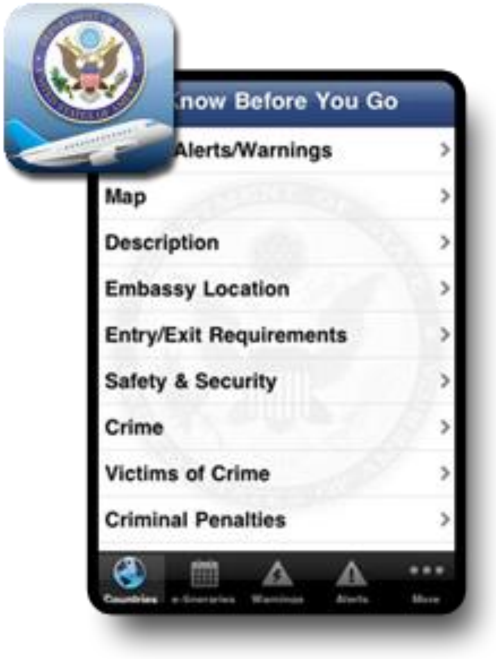


Figure 1. THINKSTOCK. State Department's Smart Traveler App 2013

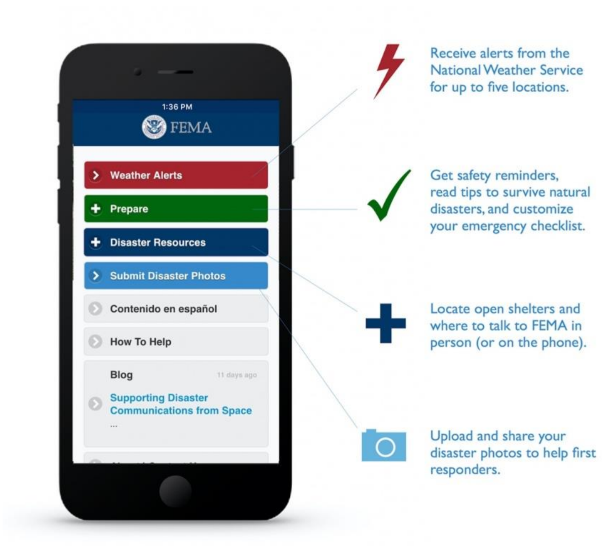

1:36 PM
FEMA
Weather Alerts
Prepare
Disaster Resources
Submit Disaster Photos
Contenido en español
How To Help
Blog
11 days ago
Supporting Disaster Communications from Space
Receive alerts from the National Weather Service for up to five locations.
Get safety reminders, read tips to survive natural disasters, and customize your emergency checklist.
Locate open shelters and where to talk to FEMA in person (or on the phone).
Upload and share your disaster photos to help first responders.

Figure 2. FEMA Mobile App 2017

The **FEMA** app is designed to be used as a constant tool and resource before, during, or after a disaster. Not only that, but this is FEMA's sole application that can also be used offline. For example, if information is stored into the app, such as a fire escape plan or shelter in place plan, user's can access this information even if they do not have WiFi reception. A GPS system is another useful tool in this app, in addition to weather alerts for up to five locations of the user's choice. Tina Adinolfi, FEMA's chief and senior program manager takes pride in the apps simplicity and the fact that there's no confusion (Major, 2016)

In 2011, IRS launched its **IRS2Go** app. It is designed to bring about ease of use in navigating through the tax-filing process. The app has a couple of key tools: 1) if a user owes taxes, they are able to make payments directly from their checking or savings account (or with a debit or credit card); and 2) if a user is due a refund, they are able to find out the status of their refund within 24 hours of filing and submitting an electronic tax return (this feature is the "Where's My Refund" tool). In addition, if a user is searching for tax services, they can conduct a search to find a place that does free tax preparation (Dixon, 2016).

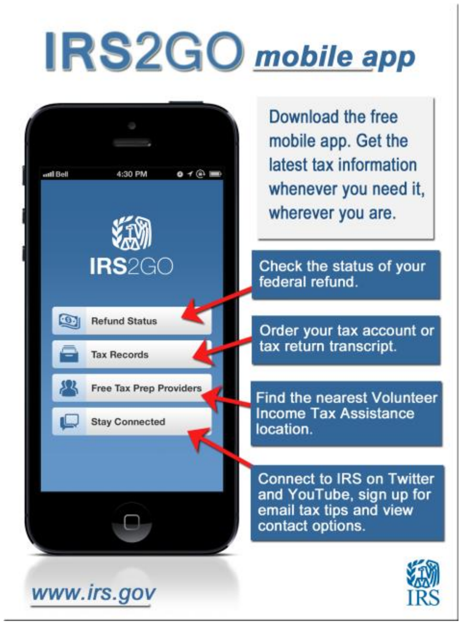
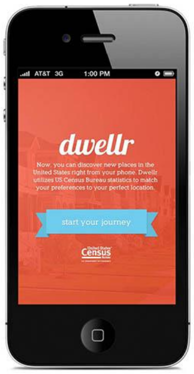

IRS2GO mobile app
Bell
4:30 PM
IRS2GO
Refund Status
Tax Records
Free Tax Prep Providers
Stay Connected
Download the free mobile app. Get the latest tax information whenever you need it, wherever you are.
Check the status of your federal refund.
Order your tax account or tax return transcript.
Find the nearest Volunteer Income Tax Assistance location.
Connect to IRS on Twitter and YouTube, sign up for email tax tips and view contact options.
www.irs.gov
IRS

Figure 3. Internal Revenue Service. Tumblr 2014



Now, you can discover new places in the United States right from your phone. Dwellr utilizes US Census Bureau statistics to match your preferences to your perfect location.

2

Figure 4. Dwellr App for Census Bureau. Jankowski, A. 2014.

The U.S. Census Bureau has released its Dwellr mobile app to bring a vast amount of their statistical data to its citizens. The data includes information collected from the agency's American Community Survey which includes race, ethnicity, economic trends, social characteristics and housing. Users are able to put in information about their gender, city, marital status, dream job, age, and education to get a fit for their ideal location. Americans can find out about demographics, neighborhoods, professions and households (Stiles, 2013).

The apps listed above are just a few outstanding products that support the objective of delivering successful digital government services. The center for Digital Government is an advisory and research entity that focuses on best practices and policy surrounding information technology in local and state government. Each year, the Center for Digital Government awards a government agency with a Digital Government Achievement Award (DGAA) for the most outstanding agency/department apps. The award includes winners from the following seven categories: 1) government-to-business; 2) government-to-citizen (local); 3) government-to-citizen (state and federal); 4) government-to-government; 5) government internal; 6) driving digital government (local); and driving digital government (state government). The 2016 government-to-citizen local government category winner was San Francisco's open source based mobile platform, Open SF (Center for Digital Government, 2016).

MOBILE APP SECURITY DEVELOPMENT

The Federal Trade Commission (FTC) is a consumer protection agency. They suggest aiming for reasonable data security since different apps require a different developer approach. The more complex the app, the more involved the task will be to secure software, data transmission and securing servers. FTC recommends evaluating the following app ecosystem before starting development (FTC, 2013):

- Software development kits (SDKs) supports app developers for timely (not rushed) coding. Developers should be aware of development kits available that best fits the architecture.
- A huge user base requires increased security requirements. A developer must be able to measure delivery of services based on the magnitude of its subscribers.
- A good start to the developer process is to take advantage of ready-made software libraries and cross-platform tool kits. Although these tools are helpful, the developer must be well-versed in the application's infrastructure.
- Features and vulnerabilities must be recognized and balanced. An app's features must be evaluated to measure high stakes against user vulnerabilities, such as insecure Wi-Fi networks, low-tech threats, loss and theft.

MOBILE APP ARCHITECTURES

The Digital Government Strategy (DGS has a deliverable called the Mobile Security Reference Architecture (MSRA). The DGS objective is to securely affordably procure and manage mobile devices, applications, and data in a smart manner. The MRSA guide answers the call to the 2011 Executive Order #13571 to improve quality of service to the American people. From this order, the Digital Government Strategy was created. The department of Homeland

Security (DHS), Department of Defense (DoD) and National Institute of Standards and Technology joined forces providing guidance to agencies to implement mobile security. Key components of a mobile device infrastructure include the following, along with a brief description in laymen's terms (Federal CIO Council, 2013):

- Virtual Private Network (VPN) – ensuring secure connections.
- Mobile Device Management (MDM) – optimal, centralized functionality and security management.
- Mobile Application Management (MAM) – configuration data control.
- Identity and Access Management (IAM) – ensuring a consistent and secure mobile experience across multiple devices.
- Mobile Application Store (MAS) – A bank of available mobile apps; require different user groups and security based on authorization.
- Mobile Application Gateway (MAG) – security designated to mobile app service; network traffic filtering.
- Data Loss Prevention (DLP) – ensuring flow of sensitive information is monitored and traffic blocked when necessary.
- Intrusion Detection System (IDS) – alerts detecting malicious activity.
- Gateway and Security Stack - filters unwanted network traffic.

OWASP Mobile Security Project is designed to equip developers with resources to secure mobile applications. They identify the following mobile risks as their top 10 of 2016 (OWASP, 2016):

- M1 – Improper Platform Usage – incorrect use of platform; not using security controls.
- M2 – Insecure Data Storage – improper data leakage and data storage.

- M3 – Insecure Communication – weak handshaking, wrong SSL versions; insecure protection of sensitive assets via cleartext.
- M4 – Insecure Authentication – insecure authentication; session management.
- M5 – Insecure Authorization – insufficient cryptography to sensitive information.
- M6 – Insecure Authorization – authorization failures.
- M7 – Client Code Quality – catch-all code mishaps.
- M8 – Code Tampering – unauthorized code modification.
- M9 – Reverse Engineering – vulnerabilities to source code and back end servers.
- M10 – Extraneous Functionality – unintended release or reveal of security controls.

GOVERNMENT GUIDELINES

Digital.gov recommends the following guidelines:

Guideline 1: Make sure your content is structured and chunked appropriately for multiple devices (mobile-friendly).

Guideline 2: Follow industry user interface guidelines and government regulations (such as 508) in the development of your mobile product.

Guideline 3: Leverage the device's features for usability and accessibility (crowdsourcing).

Guideline 4: Test at multiple points in the design/development process.

Functionality & Usability

Security & Privacy

Accessibility

Performance

Guideline 5: Collect an duse data (quantitative and qualitative) to determine what content your users want and where.

Guideline 6: Develop security and privacy guidelines with regard to what the app does/how it protects user data and government systems.

The Mobile Application Development Program suggests the following:

Plan: See what other agencies are doing

Check the Federal Mobile Apps Directory (https://www.usa.gov/mobile-apps)

Find out how agencies created mobile products

Check 25 Mobile Gov Case Studies (https://www.digitalgov.gov/tag/mobile-gov-experience/)

Create Statement of work on RFP EZ (https://www.digitalgov.gov/2013/05/06/cracking-the-mobile-contracting-nut/)

Develop: Create mobile enabled websites (https://www.digitalgov.gov/services/sites-usa-gov/)

Reuse mobile code (http://gsa.github.io/Mobile-Code-Catalog/)

RECOMMENDATIONS

The Federal Trade Commission offers the following tips for mobile app security (FTC, 2013):

- Make someone responsibility for security – within the team of people at least one person for each stage of development.
- Take stock of date you collect and retain – exercise data minimalization by not exposing information that is irrelevant.

- Understand differences between mobile platforms – be aware the various applications require different security-related features.
- Don’t rely on a platform alone to protect your users – be well versed in the security features in order to fully protect users.
- Generate credentials securely – appropriate security credentials are necessary for users’ security (i.e. usernames and passwords).
- Use transit encryption for usernames, passwords, and other important data – this will mitigate against vulnerabilities, such as unsecure Wi-Fi access points.
- Use due diligence on libraries and other third-party code – research is most important prior to trusting someone else’s code.
- Consider protecting data you store on a user’s device – when handling PII ensure the app obscures data which will protect the user’s data.
- Protect your servers – software updates on the server is most important, in addition to do research to ensure efficient monitoring for security and protection.
- Don’t store passwords in plaintext – iterated cryptographic has function to has users’ passwords will protect passwords from being exposed.
- Stay aware and communicate with users – once app has moved to production, stay engaged and keep abreast of new or perpetual vulnerabilities. Security updates must be constant.

References:

Kamensky, J. and Wedge, S. (2016, January 13). Government on the go. Government Executive. Retrieved from http://www.govexec.com/excellence/promising-practices/2016/01/government-go/125068/

Agile Support Team. (2013, January 14). Mobile performance testing overall analysis – whitepaper. AgileLoad. Retrieved from http://www.agileload.com/agileload/blog/2013/01/14/mobile-performance-testing-overall-analysis---whitepaper

Digital Government. (2012). Building a 21st century platform to better serve the American people. Retrieved from https://obamawhitehouse.archives.gov/sites/default/files/omb/egov/digital-government/digital-government.html

USA.gov. (2016, March 14). Discover six of the government's best mobile apps. Retrieved from https://www.usa.gov/features/discover-six-of-the-government-s-best-mobile-apps

Porter, D. (2016, August 1). Smart traveler app: US Department of State. The Roaming Boomers. Retrieved from https://www.theroamingboomers.com/smart-traveler-app-u-s-department-of-state/

Major, D. (2016, June 15). FEMA keeps it simple with disaster app. GCN. Retrieved from https://gcn.com/articles/2016/06/15/fema-app.aspx

Dixon, A. (2016, October 26). Reviewing the IRS2Go App. SmartAsset. Retrieved from https://smartasset.com/taxes/reviewing-the-irs2go-app

Stiles, M. (2013, November 26). Census aims to bring statistics home with a new mobile app. NPR. Retrieved from http://www.npr.org/sections/alltechconsidered/2013/11/26/247351451/census-aims-to-bring-statistics-home-with-a-new-mobile-app

Center for Digital Government. (2016, September 1). Best of the web & digital Government achievement awards – 2016 winners announced. Retrieved from http://www.govtech.com/cdg/Best-of-the-Web-Digital-Government-Achievement-Awards-2016-Winners-Announced.html

Digital.gov. n.d. Mobile user experience guidelines and recommendations. Retrieved from https://www.digitalgov.gov/resources/mobile-user-experience-guidelines-and-recommendations/

Federal Trade Commission (2013, February). Mobile apps developers: start with security. Retrieved from https://www.ftc.gov/tips-advice/business-center/guidance/mobile-app-developers-start-security

Federal CIO Council. (2013, May 23). Mobile security reference architecture. Retrieved from https://cio.gov/wp-content/uploads/downloads/2013/05/Mobile-Security-Reference-Architecture.pdf

OWASP.org. (2016). Mobile top 10. Retrieved from https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10

Digital.gov. (n.d.). Mobile Application Development Program. Retrieved from https://www.digitalgov.gov/resources/mobile-application-development-program/

Structure:

Figure 1. THINKSTOCK (2013, July 19). Next.gov. State Department’s smart traveler app. Retrieved from http://www.nextgov.com/mobile/2013/07/state-departments-smart-traveler-app-should-be-left-home/67082/

Figure 2. FEMA. (2017, February 28). Mobile app. Retrieved from https://www.fema.gov/mobile-app

Figure 3. Internal Revenue Service (2014, August 7). Tumblr. Retrieved from http://internalrevenueservice.tumblr.com/post/82198113538/irs2go-mobile-app

Figure 4. Jankowski, A. (2014, September 23). Dwellr App for Census Bureau. B ēhance. Retrieved from https://www.behance.net/gallery/19986987/Dwellr-App-for-Census-Bureau