Chapter 5
Mobile Government and Defense

Jim Jones
Ferris State University, USA

ABSTRACT
The Government, Military, and Intelligence communities of the United States and other countries are adopting mobile technologies almost as quickly as commercial entities, and in some cases are going beyond the applications we see in the commercial space. Government services, such as information access and certain transactions, are rapidly adopting mobile delivery mechanisms. The military is using mobile technology to share static information as well, but is also providing live data feeds and information sharing to support combat operations. Intelligence agencies are using mobile devices as a data collection platform for their own agents, and are also accessing the mobile devices of enemy agents and intelligence targets to collect data surreptitiously. Military operations face unique challenges, given that they are often conducted in regions without existing networks and against an enemy trying to actively disrupt communications. The Government, Defense, and Intelligence communities all face the challenge of securing mobile devices and data in response to regulatory and statutory requirements, as well as a dynamic and evolving threat space of identity thieves, hackers/crackers, hostile military forces, and foreign intelligence services.

INTRODUCTION
This chapter considers applications of mobile technologies in the Government, Defense, and Intelligence communities. Government entities are actively moving services into the mobile domain, as users demand such access and the technology enables it. The Defense community is delivering similar services, but is also actively expanding mobile device services to provide real-time support for combat and other military operations. The Intelligence community, with its unique mission to collect and analyze data from all available sources, is actively exploiting mobile technology...
as both a deliberate and surreptitious collection platform. Military operations often occur in areas without established network infrastructures and in the vicinity of hostile forces, creating a unique challenge to stand up and defend network infrastructures on demand. All of the communities, Government, Defense, and Intelligence, face the challenge of protecting mobile device data in transit and at rest.

GOVERNMENT SERVICES

Description and Mission

Consider the elements of the United States or another government (federal, state, and local) which provide direct services to citizens and residents. With the exception of the profit motive, these organizations function like many commercial enterprises. Specifically, both commercial and government entities need to conduct bidirectional informational and financial transactions with their “customers”. While the two types of entities operate under different sets of laws and regulations, both have requirements to protect information and transaction data, to authenticate users, to provide reliable services, etc. - in short, to protect the confidentiality, integrity, and availability of the information and systems relevant for the services provided. In the examples which follow, we discuss applications of mobile technologies to government services and the relevant assurance criteria, i.e., authentication (none, one, or both parties), transaction security (protected or not), and availability (critical or not). After discussing several current and potential uses of mobile technology for providing government services, the section concludes with a discussion of relevant challenges.

Applications of Mobile Technology

Perhaps the most obvious application of mobile technologies for government services is providing public information such as government office locations, hours of operation, directions, phone numbers, etc. (Harvard, 2003). Such a service does not require strong authentication of either party, nor transmission security, nor high availability. Failure of the service along any of these lines would be inconvenient, but would not violate any legal or regulatory requirements. Most government entities currently provide this information via the web (as well as phone-based 311 services), so the basic service exists if a user simply chooses to use a mobile device browser (or phone) instead of a PC browser (or land line phone). Increasingly, government entities are developing specific mobile applications which provide additional capabilities unique to a mobile device. For example, directions to an office may be directly downloaded to a mobile device navigation app, a phone call can be automatically dialed, or a text message sent with information.

In a similar fashion, government entities which provide online (web-based) transaction processing for things like driver’s license renewal, vehicle tag renewal, and tax payments are increasingly providing mobile device versions of these services. Since private and possibly financial information is involved, such transactions require user authentication and transmission security. Bidirectional authentication may be optional - while the government entity should be strongly authenticated (to prevent phishing and similar attacks), there is limited value in strongly authenticating each user (are you really going to pay someone else’s taxes for malicious purposes?). As with information-only services, high availability is not typically required for these services. A procrastinating user might disagree, but experience with the non-mobile versions of these services has shown that some downtime is acceptable (with the possible exception of the hours leading up to a tax filing
Related Content

Malicious Data Stream Identification to Improve the Resource Elasticity of Handheld Edge Computing System

The iPad in the Classroom: Three Implementation Cases Highlighting Pedagogical Activities, Integration Issues, and Teacher Professional Development Strategies
Nathaniel Ostashewski and Doug Reid (2013). *Pedagogical Applications and Social Effects of Mobile Technology Integration* (pp. 25-41).
[www.igi-global.com/chapter/ipad-classroom-three-implementation-cases/74903?camid=4v1a](www.igi-global.com/chapter/ipad-classroom-three-implementation-cases/74903?camid=4v1a)

The Accuracy of Location Prediction Algorithms Based on Markovian Mobility Models
[www.igi-global.com/article/accuracy-location-prediction-algorithms-based/4066?camid=4v1a](www.igi-global.com/article/accuracy-location-prediction-algorithms-based/4066?camid=4v1a)

Economics of Immediate Gratification in Mobile Commerce
[www.igi-global.com/chapter/economics-immediate-gratification-mobile-commerce/26627?camid=4v1a](www.igi-global.com/chapter/economics-immediate-gratification-mobile-commerce/26627?camid=4v1a)