2013-04-01

Managing Risk in Mobile Applications With Formal Security Policies

Breaux, Travis

Monterey, California. Naval Postgraduate School

NPS-AM-13-C10P06R01-069

EXCERPT FROM THE

PROCEEDINGS

OF THE

TENTH ANNUAL ACQUISITION RESEARCH SYMPOSIUM SOFTWARE ACQUISITION

Managing Risk in Mobile Applications With Formal Security Policies

Travis Breaux and Ashwini Rao
Carnegie Mellon University

Published April 1, 2013

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF BUSINESS & PUBLIC POLICY
NAVAL POSTGRADUATE SCHOOL

The research presented in this report was supported by the Acquisition Research Program of the Graduate School of Business & Public Policy at the Naval Postgraduate School.

To request defense acquisition research, to become a research sponsor, or to print additional copies of reports, please contact any of the staff listed on the Acquisition Research Program website (www.acquisitionresearch.net).

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF BUSINESS & PUBLIC POLICY
NAVAL POSTGRADUATE SCHOOL

Preface & Acknowledgements

Welcome to our Tenth Annual Acquisition Research Symposium! We regret that this year it will be a "paper only" event. The double whammy of sequestration and a continuing resolution, with the attendant restrictions on travel and conferences, created too much uncertainty to properly stage the event. We will miss the dialogue with our acquisition colleagues and the opportunity for all our researchers to present their work. However, we intend to simulate the symposium as best we can, and these *Proceedings* present an opportunity for the papers to be published just as if they had been delivered. In any case, we will have a rich store of papers to draw from for next year's event scheduled for May 14–15, 2014!

Despite these temporary setbacks, our Acquisition Research Program (ARP) here at the Naval Postgraduate School (NPS) continues at a normal pace. Since the ARP's founding in 2003, over 1,200 original research reports have been added to the acquisition body of knowledge. We continue to add to that library, located online at www.acquisitionresearch.net, at a rate of roughly 140 reports per year. This activity has engaged researchers at over 70 universities and other institutions, greatly enhancing the diversity of thought brought to bear on the business activities of the DoD.

We generate this level of activity in three ways. First, we solicit research topics from academia and other institutions through an annual Broad Agency Announcement, sponsored by the USD(AT&L). Second, we issue an annual internal call for proposals to seek NPS faculty research supporting the interests of our program sponsors. Finally, we serve as a "broker" to market specific research topics identified by our sponsors to NPS graduate students. This three-pronged approach provides for a rich and broad diversity of scholarly rigor mixed with a good blend of practitioner experience in the field of acquisition. We are grateful to those of you who have contributed to our research program in the past and encourage your future participation.

Unfortunately, what will be missing this year is the active participation and networking that has been the hallmark of previous symposia. By purposely limiting attendance to 350 people, we encourage just that. This forum remains unique in its effort to bring scholars and practitioners together around acquisition research that is both relevant in application and rigorous in method. It provides the opportunity to interact with many top DoD acquisition officials and acquisition researchers. We encourage dialogue both in the formal panel sessions and in the many opportunities we make available at meals, breaks, and the day-ending socials. Many of our researchers use these occasions to establish new teaming arrangements for future research work. Despite the fact that we will not be gathered together to reap the above-listed benefits, the ARP will endeavor to stimulate this dialogue through various means throughout the year as we interact with our researchers and DoD officials.

Affordability remains a major focus in the DoD acquisition world and will no doubt get even more attention as the sequestration outcomes unfold. It is a central tenet of the DoD's Better Buying Power initiatives, which continue to evolve as the DoD finds which of them work and which do not. This suggests that research with a focus on affordability will be of great interest to the DoD leadership in the year to come. Whether you're a practitioner or scholar, we invite you to participate in that research.

We gratefully acknowledge the ongoing support and leadership of our sponsors, whose foresight and vision have assured the continuing success of the ARP:

- Office of the Under Secretary of Defense (Acquisition, Technology, & Logistics)
- Director, Acquisition Career Management, ASN (RD&A)
- Program Executive Officer, SHIPS
- Commander, Naval Sea Systems Command
- Program Executive Officer, Integrated Warfare Systems
- Army Contracting Command, U.S. Army Materiel Command
- Office of the Assistant Secretary of the Air Force (Acquisition)
- Office of the Assistant Secretary of the Army (Acquisition, Logistics, & Technology)
- Deputy Director, Acquisition Career Management, U.S. Army
- Office of Procurement and Assistance Management Headquarters, Department of Energy
- Director, Defense Security Cooperation Agency
- Deputy Assistant Secretary of the Navy, Research, Development, Test, & Evaluation
- Program Executive Officer, Tactical Aircraft
- Director, Office of Small Business Programs, Department of the Navy
- Director, Office of Acquisition Resources and Analysis (ARA)
- Deputy Assistant Secretary of the Navy, Acquisition & Procurement
- Director of Open Architecture, DASN (RDT&E)
- Program Executive Officer, Littoral Combat Ships

James B. Greene Jr.
Rear Admiral, U.S. Navy (Ret.)

Keith F. Snider, PhD
Associate Professor

Managing Risk in Mobile Applications With Formal Security Policies

Travis Breaux and Ashwini Rao
Carnegie Mellon University

Streamlining the Process of Acquiring Secure Open Architecture Software Systems

Walt Scacchi and Thomas A. Alspaugh
University of California, Irvine

Managing Risk in Mobile Applications With Formal Security Policies

Travis Breaux—Breaux is an assistant professor of computer science in the Institute for Software Research at Carnegie Mellon University (CMU). His research program searches for new methods and tools for developing correct software specifications and ensuring that software systems conform to those specifications in a transparent, reliable, and trustworthy manner. This includes compliance with privacy and security regulations, standards, and policies. Dr. Breaux is Director of the CMU Requirements Engineering Lab, co-founder of the Requirements Engineering and Law Workshop, and has several publications in ACM- and IEEE-sponsored journals and conference proceedings. [breaux@cs.cmu.edu]

Ashwini Rao—Rao is a research assistant enrolled in the software engineering PhD program at Carnegie Mellon University. Her research interests include privacy, security, and regulatory compliance.

Abstract

Department of Defense (DoD) acquisition requires information technology (IT) to undergo the DoD information assurance certification and accreditation process (DIACAP), which makes strong architecture-dependent assumptions. Emerging IT architectures, such as mobile computing platforms, invalidate these assumptions and prevent the DoD from acquiring commercial technologies that are readily available to adversaries. To address this problem, we introduce a preliminary framework in which an application profile is expressed in a formal language and scaled with evolving architectural assumptions. This profile aims to incorporate information assurance (IA) requirements that are commensurate with risk and scalable based on an application's changing external dependencies. Information assurance risk levels that account for changing user identities and IA parameters (confidentiality, integrity, and availability) will result from dynamic recombination of mobile applications during runtime. The language is expressed in first-order logic and includes an evolvable lexicon to describe changing system configurations. We envision that software developers and certification authorities can use these formal profiles with an inference engine to complete the DIACAP and maintain compliance as IT systems evolve over time. The framework has been evaluated using existing DoD acquisition and DIACAP policy and a case study in a popular mobile application ecosystem.

Introduction

Network-centric (net-centric) warfare (NCW) is the "generation of increased combat power by networking sensors, decision makers and shooters" (Alberts, Garstka, & Stein, 1999). The Department of Defense (DoD) adopted NCW as a principle concept of operations as early as the late 1990s. This adoption includes increased efforts to move information from garrisoned to command posted and out to "the edge," or front-line combatants, to reduce the time from decision to action and create a more mobile, agile, and reactive force. During this transition, General Cartwright noted that NCW must decouple the chain-of-information from the chain-of-command (Onley, 2006; Carter, 2010) to enable the right people to gain access to the right information at the right time. Unlike enterprise information systems in garrisons and command posts, computing at the edge must be highly dynamic and responsive to fast-changing situations. This fast-paced environment yields rapidly changing software requirements, evolvable software architectures, and utility computing, which stress the current DoD acquisition system. The DoD acquisition challenge is that edge computing requires mobile applications, which are increasingly software-intensive, developed on shorter timelines, and subject to different cyber security risks (Defense Science Board, 2009).

The short IT development timelines have led commercially available IT to outpace the DoD's ability to rapidly acquire IT solutions. This is concerning when adversaries can acquire and deploy this technology worldwide and with few restrictions. Mobile computing platforms, such as Apple iOS and Google Android, offer a stark contrast to traditional computing paradigms because they enable the rapid development and deployment of commercial software to handheld devices, including tablets and smartphones. This software integrates data from multiple sources and significantly reduces the time from decision to action: New "apps" include software to complete banking transactions by digitally photographing bank checks, to purchasing music based on audio fingerprinting, to integrating mapping, routing, and directory services to locate nearby retailers, all within seconds. In these examples, apps leverage built-in devices, such as cameras, microphones, or geo-location technologies, to create narrowly integrated solutions. However, recent efforts to enable rapid DoD acquisition has focused on non-software-intensive systems (Carter, 2010; Wyatt, 2010).

Mobile computing introduces new IT security risks within a single IT system and collectively across multiple, networked systems. Unlike traditional non–software-intensive systems, IT security vulnerabilities can compromise other systems on a shared network. To reduce cyber security risk, the DoD Chief Information Office (CIO) maintains DoD Directive (DoDD) 8500.1 "Information Assurance" and DoD Instruction 8500.2 "Information Assurance Implementation," which outline policy, responsibilities, and procedures to integrate IT security protections into DoD information systems. Most DoD weapon systems subject to DoDD 5000.1 in the DoD Acquisition System must comply with these CIO policies. These policies are primarily written for enterprise systems, which excludes mobile computing as envisioned at the edge in NCW. The challenges of modernizing the IT acquisition policy have been attributed to a culture of buying large weapon systems, such as aircraft carriers, as opposed to incremental purchases of components that integrate into pervasive, complex systems (Boessenkool, 2009). Moreover, recent calls for modernizing acquisition have called for 80% solutions, which is a departure from complete, service-centric solutions that become outdated before they're completed (Gates, 2009). Mobile applications are exemplars of these modern acquisition challenges.

The U.S. Army has been a leader in the adoption of mobile applications in the DoD. In March 2010, the U.S. Army began the "Apps for the Army" challenge, which sought to test a rapid acquisition process for software applications on mobile devices. The challenge received 53 mobile applications, of which the Army successfully fielded 25 applications through the certification process (Lopez, 2010). In addition, the Army is actively engaged in training mobile application developers in its Mobile Applications Branch at Fort Gordon (Walker, 2011). Finally, the Army is taking steps to increase its mobile device infrastructure: After testing 20–30 smartphones in theater, the Army is now seeking to field 3,500 smartphones for a single brigade (Brewin, 2011). The Relevant ISR to the Edge (RITE) program recently completed testing and seeks to develop technologies to link critical data to soldiers in the field using smartphones, thus further pushing this paradigm forward (Montalbano, 2011). These steps further illustrate the need for adequate solutions to certify mobile applications.

In this paper, we propose a preliminary framework to model app IT-dependencies with the following long-term aims: (1) to reduce IA certification and accreditation time by semi-automatically matching IA assumptions to application profiles; and (2) to extend existing IA policy assumptions to cover emerging mobile applications required in edge computing. This paper is organized as follows. We first review DoD IT acquisition and IA policy environment and present policy gaps that inhibit acquisition of mobile applications;

next, we briefly present our framework, application profile, and language to address this problem; finally, we discuss our evaluation and plans for future work before concluding with related work and our discussion.

DoD Information Technology Policy

The DoD information technology (IT) policy environment is complex and distributed across multiple documents. The leading Department of Defense (DoD) policies for IT acquisition and information assurance (IA) are summarized in Figure 1. The general DoD acquisition policy and responsibilities are detailed in DoD Directive (DoDD) 5000.1, and the DoD-wide IA policy begins in DoDD 8500.1, which is refined by IA controls contained in DoD Instruction 8500.2 and by the process for performing IA certification and accreditation, described in DoDD 8510.1.

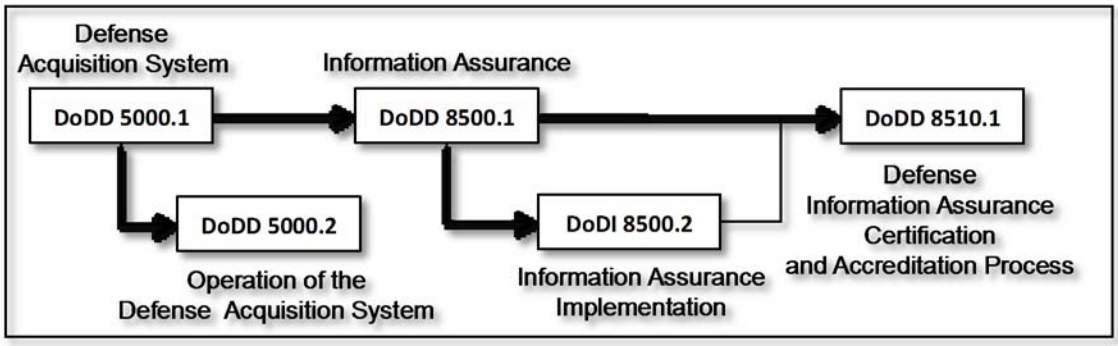

Figure 1. General Overview of the DoD IT Acquisition Environment for Information Assurance

DoDD 8500.1 governs information systems that include mobile computing devices, such as laptops, handhelds, and personal digital assistants (see DoDD 8500.1, § 2.1.2.7) and, in particular, those devices that contain wired or wireless network access to other computing resources. This instruction covers four classes of information system, as follows:

- *Automated Information System (AIS) Applications*, which are products of an acquisition program, such as software applications, or a combination of software and hardware, such as workstations, servers, and mobile computers;
- *Enclaves*, which are a collection of computing environments connected by internal networks, under the control of a single authority and security policy;
- *Outsourced IT-based Processes*, which are business processes supported by private sector information systems; and
- *Platform IT Interconnections*, which are network access points to computer resources that are essential to the mission in real-time.

Figure 2 illustrates an example IS environment, consisting of two enclaves, “A” and “B,” which correspond to a garrison and command post, respectively. These environments contain AIS applications (square boxes) and outsourced IT-based processes (circles), some of which are DoD controlled and appear within the enclave, and others that have shared control and appear outside the enclave. Platform IT Interconnections appear as solid black arrows: When these connections exit an enclave, a demilitarized zone (DMZ) is assumed to exist between the outgoing and incoming network traffic. Mobile computers, such as laptops and handhelds, are a class of AIS application that are capable of moving across enclave

boundaries; in Figure 2, the dotted-line arrows indicate movement of a handheld computer from the battlefield, into a command post, and later into a garrison. To enable this movement, IA controls must be in place to avoid contaminating these DoD controlled environments. For example, DoD 8500.1 defines the Mission Assurance Category (MAC) as the level of integrity and availability required by an information system. Enclaves always assume the highest MAC of their computer resources (AIS applications, outsourced IT-based processes, and platform IT interconnections). When an enclave connects to another enclave that has a lower MAC level, the enclave with the higher MAC level must ensure that this connection does not degrade the integrity and availability of its computer resources. This presents a particular challenge for mobile devices because they could move across enclaves.

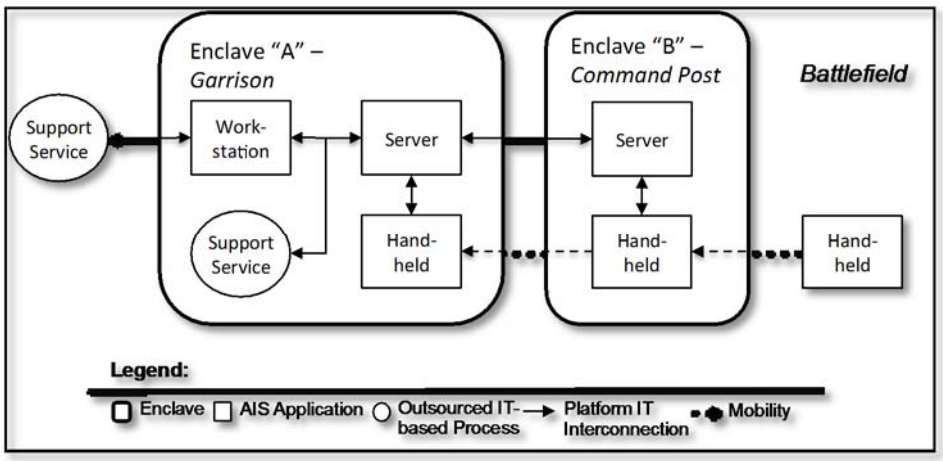

Figure 2. Example Information System Environment to Illustrate System Interactions

Applications for mobile computers, specifically handheld computers, have an operational profile that is situated among several policy gaps in existing IA policy. Under DoDD 8500.1, Designated Approving Authorities (DAAs) are responsible for certifying and accrediting these devices. Policy gaps create challenging certification environments in which the DAA must assume insurmountable risk for an unprecedented DoD information system. The combination of changing users, changing applications, and changing locations is characteristic of these devices. Consequently, a solution is needed whereby configurations can be reviewed dynamically in the field based on explicit IA assumptions that are individually bound to the mobile device hardware and collections of installed mobile applications. Figure 3 illustrates a subset of this complex policy environment: Boxes represent existing DoD IA-related policy; ovals represent IA controls from DoDI 8500.2; and arrows trace policy guidance from DoD8500.2 to IA controls and on to other applicable DoD policies. Using our requirements specification language (Breaux & Gordon, 2013), we extracted a core set of 95 requirements governing DoD IA responsibilities. We now discuss how these policies and IA controls apply to mobile applications, noting relevant shortfalls due to unique characteristics of this technology.

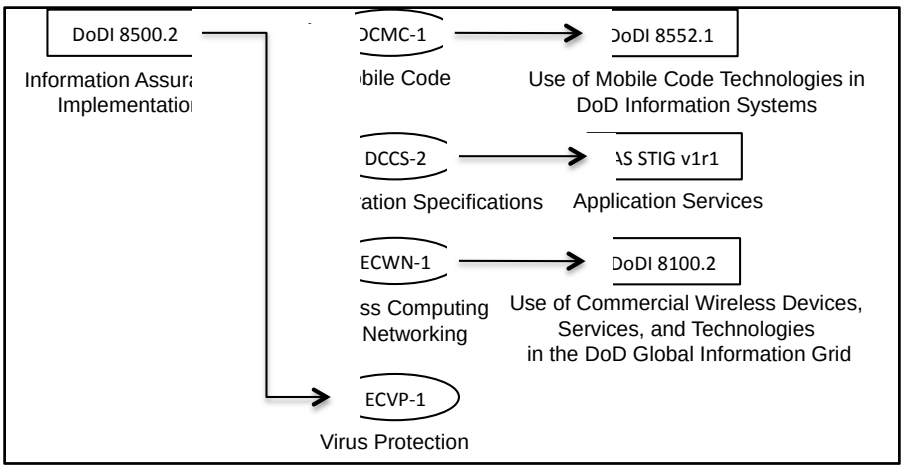

Figure 3. Example DoD Information Assurance Policy Gaps Affecting Mobile Applications

Mobile Code

Mobile code is defined by DoDD 8500.1 to be "software modules obtained from remote systems, transferred across a network, and then downloaded and executed on local systems *without explicit installation or execution by the recipient*." DoDI 8500.2 requires IA control DCMC-1, which requires implementing mobile code policy in DoDI 8552.1. This mobile code policy consists of approval decisions pursuant to one of three mobile code categories, which are differentiated by (a) whether the mobile code is digitally signed by a trusted certificate; and (b) the level of access to operating system resources and networks that is granted to the mobile code. Mobile computing is enriched by mobile applications (code) that can be downloaded and installed remotely to address emerging issues. However, the italicized phrase above in the mobile code definition excludes this policy from covering mobile applications, despite that many of the technical considerations (e.g., the mobile code category differentiators (a) and (b)) are relevant to mobile applications.

Mobility

DoDD 8500.1 defines mobile computing devices to include laptops, handhelds, and personal digital assistants operating in either wired or wireless mode. DoDI 8500.2 states that authorized users may "not relocate or change DoD information system equipment or the network connectivity of equipment without proper IA authorization" (§ 5.12.12), requiring advance IA authorization to move mobile computing devices. To employ compliant mobile computing devices, there is a need to rapidly reauthorize these devices as they move within and across enclaves, recognizing that these devices also contain mobile applications, which may change over time and thus change the device's risk profile.

Application Servers

The Defense Information System Agency (DISA; 2006) defines *application server* as a single computer that, in conjunction with other servers on a network, provides an application service to a user through a web browser. Application servers, such as Apache Tomcat and BEA Weblogic Server, are "containers" that provide application infrastructure while server administrators can remotely deploy applications that are pre-packaged as web application archives (WARs). DoDI 8500.2 contains IA control DCCS-2, which requires compliance with available security technical implementation guides, or STIGs. Only recently were new STIGs developed to cover mobile device operating systems (iOS, Android, or Blackberry OS). Previously, the DISA's STIG governing application servers, which requires responsibility for application server content to be assumed by the sponsoring organization or

activity (DISA, 2006), were the closest approximation of how mobile apps are installed on mobile devices, the main difference being that the STIG assumes that application servers are fixed in an enterprise information system.

Wireless Networking

Wireless computing and networking capability is not required, but it significantly amplifies mobile computing capabilities. DoDI 8500.2 contains IA control ECWN-1, which requires that workstations, mobile computing devices, and other portable electronic devices comply with DoD wireless policy. This policy includes DoDI 8100.2, § 4.3, that states that wireless devices may not be operated in classified environments without approval by the DAA in consultation with CSA CTTA; and § 4.10, which requires a knowledge management process to determine acceptable uses of wireless devices and appropriate mitigation strategies.

Virus Protection

DoDI 8500.2 contains IA controls ECVP-1, which require virus protection for servers, workstations, and mobile computing devices, such as laptops. For general-purpose computers, virus protection includes anti-virus software that recognizes file signatures that correspond to malicious code; this code is downloaded from a remote computer. Mobile devices running restricted operating systems, such as Apple's iOS or Google's Android, however, constrain the environment in which remote code can be executed. In these devices, mobile application infrastructure, including pre-approved applications in a trusted app store, can reduce or eliminate exposure to malicious code for some mobile applications.

Our analysis of the Android 2.2 STIG, Version 1, Release 1, yielded 59 requirements that affect mobile Android devices. Among these, 40 requirements target the operating system, 16 requirements target apps, and three requirements target external actions, such as ensuring that mobile users respect the physical security policy when using the smartphone camera. Requirements WIR-MOS-AND-006-01 and WIR-MOS-AND-006-3 require approval from the DAA or application control board for all non-core apps. This includes an inspection of the app and risk analysis. Although some tools exist to conduct static analysis on source code to identify common vulnerabilities (e.g., buffer overflows), to our knowledge no tools exist to analyze mobile app requirements for the purpose of identifying security risks. As a result, the current guidance is inadequate to support the DAA in evaluating non-core apps. Therefore, we now discuss our framework that aims to begin to address this problem.

Mobile Application Framework

Mobile devices that run pre-approved mobile applications can be viewed as miniature enclaves, in which the user has the authority to reconfigure and recompose new functions from multiple AIS applications (mobile apps) and initiate connections to pre-approved outsourced IT processes using platform IT interconnections. Unlike general-purpose computing enclaves, these applications, processes, and interconnections operate on pre-defined data types in a restricted computing environment. Some mobile applications leverage general-purpose data types, such as e-mail clients or web browsers, but most use restricted data types, such as dates, locations, images, audio, and so forth. Advances in miniaturization may lead to mobile devices that run multiple computing environments in parallel, in which each environment processes different information classes with approved guards for moving unclassified data into classified environments within the same mobile device. For example, recent work has demonstrated the ability to run multiple mobile OSes on the same device using virtualization (Suh et al., 2008). Finally, we envision that mobile devices can be moved between enclaves, which changes the runtime assumptions under

which mobile applications are permitted to operate. Mobile applications approved to handle unclassified data cannot operate in classified physical and cyber environments without approved guards to prevent the unauthorized release of classified data. Similarly, classified applications cannot operate in unclassified environments.

Figure 4 illustrates several challenges to accrediting mobile applications. In Step 1, Figure 4, application (app) developers create an application profile in the EADL for their app based on the mobile application system architecture. In the future, this profile may be generated using code-level analysis to assist in certification (e.g., do network connections use OS SSL libraries, or does file I/O encrypt data in storage?). In Step 2, the DAA certifies the app using the application profile and may accredit the app for deployment to the mobile device under this profile. The certification and accreditation includes a digital signature of the application profile, which the mobile device will use to execute the application only in enclaves that conform to this profile. In Step 3, the signed app is loaded into a DoD app store, authorized users can download the app to their mobile device.

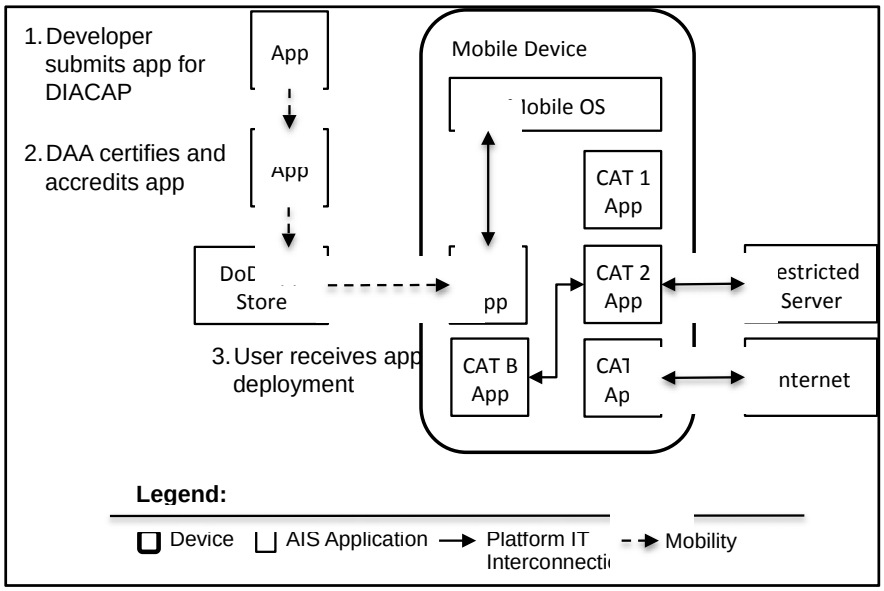

Figure 4. Example Life Cycle for a Mobile Application in a Handheld Device

In our framework, mobile applications are assigned to different categories based on their resource utilization profile. We envision the following categories: CAT 1, 2 or 3, which describe the level of remote connectivity, may be combined with CAT A and B, which describe the type of local interactivity. These categories were validated based on our analysis of DoD IA policy.

- **CAT 1:** *Stand-alone apps* are installed with their complete data set, such as training manuals, calculators, or dictionaries. These apps do not make connections to remote servers or the Internet.
- **CAT 2:** *Restricted apps* periodically make connections to pre-approved servers only. These apps include weather services and route-finding applications that receive updated maps from pre-approved sources.
- **CAT 3:** *Unrestricted apps* may make connections to remote servers that are unsecured or not on a pre-approved list. This includes web browsers.

- **CAT A:** Apps may use specialized operating system resources, such as cameras, microphones, speakers, GPS coordinates, and so forth.
- **CAT B:** Apps may exchange pre-defined data types with other apps.

We examined descriptions of mobile applications in the context of current initiatives in the United States Army. Among the five winners of the Apps for Army Challenge, three Apps could be developed as CAT 1 apps (New Recruit, Physical Readiness Trainer, and Telehealth Mood Tracker): The first two apps provide access to stable knowledge bases that can be updated periodically in new, self-contained versions of the application; these may include hard-coded web pages, training videos, and so forth that reside locally on the mobile device. The remaining two winners, Movement Projection and Disaster Relief Operations, appear to be CAT 2A apps: They rely on map-routing data that can be acquired from an approved source, such as Google Earth and Google Maps. If these connections are not secured, they could leak information to intermediaries who route the data to the map server, which is a CAT 3A app. We envision that these categories can be further subdivided; for example, CAT A can be subdivided to distinguish the use of a mobile camera, versus the use of location-based services and accelerometers. We further envision static analysis tools that can be developed to analyze the source code of these apps to automatically determine which category the app falls within.

Mobile Application Profile and Language Overview

The mobile application profile is described by a set of requirements to express data flows for a single mobile application. These requirements are formalized in the description logic (DL) using the semantic parameterization method (Breaux, Antón, & Doyle, 2008). Based on our mobile application framework, an certification authority may want to prove that, for a given configuration (collection of mobile applications), no CAT 3A apps are operating during field operations that could disclose a soldier's location to an untrusted, third-party server, or that no communications exist between CAT 2B and CAT3B apps that may disclose sensitive data to third parties.

To achieve this aim, we begin by formalizing a subset of data requirements using three Deontic modalities: *Obligations* describe what the app is required to do; *prohibitions* describe what the app is prohibited from doing; and *permissions* describe what the app is permitted to do. Formal requirements analysis is used to identify conflicts between what is permitted and what is prohibited, noting that obligations imply permissions in Deontic Logic (Horty, 1993). In addition, we define a series of roles based on Fillmore's (1968) case frames and Gruber's (1976) thematic roles to encode the actors engaged with the data, the type of data, and the purpose for which the data is used. At present, the restricted set of requirements covers only three specific actions: *Collection*, which is any act to access, assign, collect, import, observe, or receive information from another party, sensor, or device; *transfer*, which is any act to disclose, provide, share, or transfer data to another party; and *use*, which is any action performed on the data by the app for a particular purpose, excluding collections and transfers. The set of data requirements expressed formally constitutes the data flow aspect of the mobile application profile. App developers can formalize these statements using their knowledge of the app's operations, or by using stated natural language requirements, scenarios, or privacy and security policies written specifically for the app. We now illustrate this formalization using an example natural language statement from a written policy.

Figure 5 portrays a statement that has been encoded using the formalism; a more complete description of the formalization and an empirical case study is described in Breaux and Rao's (2013) study. In Step 1, the analyst identifies important keywords that indicate the

action (e.g., import, enter), the modality, and the role fillers: the *object* (e.g., address book contacts) is the data type, and the *purpose* (e.g., locating contacts) for which the data will be used. Because the verbs *import* and *enter* denote the movement of data from the user to the app, these verbs indicate a collection. In Step 2, the keywords are written into a simple SQL-like syntax that encodes a permission, indicated by the language operator P, followed by the action name and the role fillers. The first role filler is the object, followed by the language keyword FOR that precedes the purpose for which the action COLLECT is performed. Using DL, we can express complex hierarchies of data types, actor roles, and purposes. These hierarchies allow us to check whether permissions that broadly allow information sharing of coarsely described information types conflict with prohibitions restricting the sharing of specific types. Conflicts of this type frequently arise due to exceptions in security policies.

Finally, in Step 3, an automated tool parses the language syntax and compiles a DL expression in the Web Ontology Language (OWL). The compiled expression is denoted in Figure 5 by the two axioms for concept p_8: The first axiom defines the concept p_8 as a collection action with the appropriate role fillers; the second axiom defines the concept p_8 to be a subclass of what is permitted. Using a theorem prover, we can check these profiles for internal consistency (i.e., are there any conflicts among the encoded data requirements?). We can also check these mobile application profiles for consistency with external properties by expressing these properties in the formal language, such as prohibiting transfers to third parties of certain data types (e.g., e-mail addresses). Using DL, we reduced data requirements conflict detection to DL satisfiability, which is known to be PSPACE-complete for this family of DL.

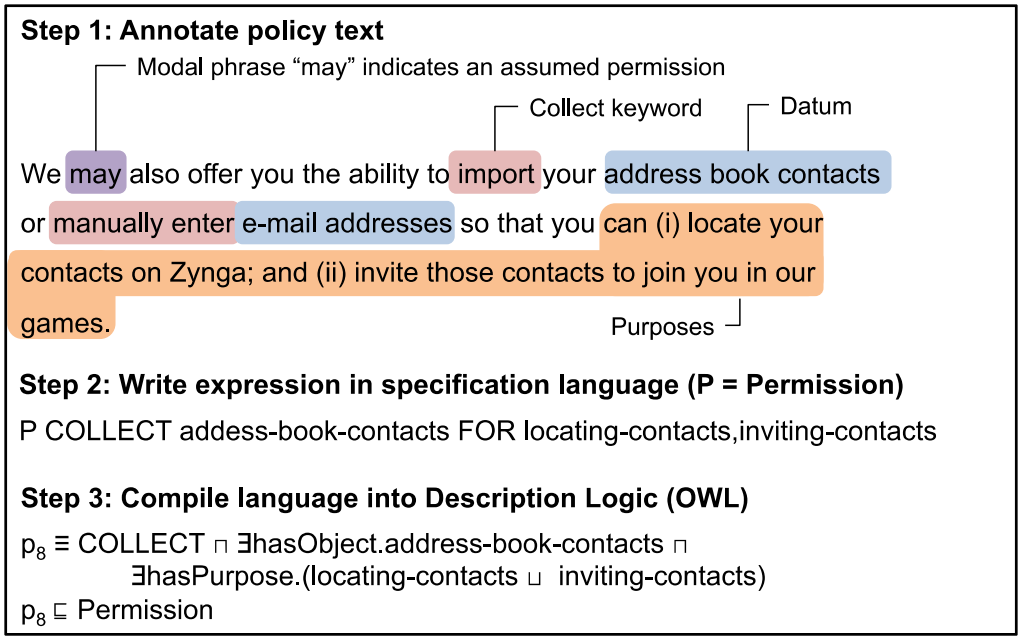

Figure 5. Example Encoding of Data Requirement Into Formal Language

Case Study and Simulation

At present, the language has been developed and validated using information privacy policies that describe privacy and security requirements, such as what information may be collected, used, and transferred, for what purposes, and by whom. These activities architecturally describe an app’s data flows and, based on the providers and recipients of the data described in these policies, these activities frame the app in a larger information ecosystem that consists of the cellular network provider, the mobile phone and operating

system manufacturers and third-party service providers upon whom the app depends. Each of these ecosystem members maintain separate privacy policies that describe what is permitted and prohibited with respect to personal data. In addition, privacy has been viewed as a “subset of security” because these same information-sharing policies also affect confidentiality, integrity, and availability of the system: Companies often aim to increase information availability and integrity to improve their services, while users wish to increase confidentiality of personal information. Best security practices, such as complex passwords, data encrypted in storage and in transfer, and so on, have also been described in these policies. Finally, these policies are increasingly required by regulators and mobile app stores, such as Google Play and iTunes, which makes these policies a pervasive, publicly available, and rich source of security requirements upon which to develop a preliminary data-flow language for assessing our mobile security risk framework.

Our case study to evaluate the language’s formal semantics focused on the analysis of three policies that are linked in an integrated service scenario (Breaux & Rao, 2013). The scenario consists of the Facebook social networking platform, the Zynga game service, and AOL advertising network: Each of these parties has separate policies that govern the user’s interaction with Zynga online games, such as Farmville. Analyzing these three policies yielded 374 statements, of which 144 statements were data security requirements that were expressed in the formal language. Among these, the analysis produced two critical conflicts that we detected with our automated theorem prover: One conflict was between the Zynga policy and the Facebook policy because Zynga reserves the right to share information obtained from Facebook in violation of Facebook’s application developer’s policy.

Finally, we built tools to parse and reason about these policies. Our simulation studies, which are based on these tools, show that identifying conflicts can be performed within a reasonable amount of time (a few minutes) for profiles containing on the order of 100 rules. The simulation evaluated conflict detection using three different DL theorem provers: the Pellet OWL2 Reasoner v2.3.0 developed by Clark and Parsia, the HermIT Reasoner v1.3.4 developed by the Knowledge Representation and Reasoning Group at the University of Oxford, and the Fact++ Reasoner v1.5.2 developed by Dmitry Tsarkov and Ian Horrocks. Conflict detection for HermIT and FaCT++ was shown to be linear and constant, respectively, with respect to the number of rules. The Pellet reasoner was unable to scale beyond four rules in our simulation due to a design decision in this version of Pellet regarding how they handle a certain class of DL expressions. In future work, we aim to optimize conflict detection for larger policies, as needed.

Future Work

In future work, we plan to investigate three extensions to the mobile app framework and language. First, we aim to enhance our technical approach by developing framework extensions to link security specifications among multiple, separate apps. These extensions would allow an analyst to trace data flows across multiple apps and thus check whether security properties are held across these apps and their third-party services. We already have preliminary evidence to demonstrate this extension. Second, we aim to extend our framework to investigate how security policies change as mobile devices move across enclaves. This requires establishing and comparing physical security policies for physical locations with policies for apps that interact with those locations, either through user data entry, location-based services, cameras, or other means. As we discussed with Figure 2, we aim to support graceful degradation to limit the services that become disabled to only those that are not trusted in high security enclaves. Finally, we aim to extend our formal language with additional security properties to describe how data is properly stored, what attributes must be true during collections and transfers, and so forth.

In this paper, we described an overview of the approach and summarized our evaluation based on policy analysis and a runtime simulation. In the future, we seek to study the use of our framework in an experimental setting to answer questions, such as the following: How well can app developers write security specifications for their apps using our framework, and how well can certification authorities use these specifications to assure the app conforms to security best practices? We imagine that new interfaces to our formal methods would be needed and that static and dynamic analysis tools could help authorities verify that app runtimes conform to the stated app security profile.

Related Work

Related work includes enterprise architecture languages, which are used to express relationships between IT resources at a system-wide level, other work to analyze information assurance policy in privacy and security, and work to model information assurance properties in systems. Enterprise architecture (EA) is an informal concept consisting of four layers: business, information, applications, and technology. The layers provide notional constructs for capturing the range of personnel roles, responsibilities, assets, and functional system requirements. The Open Architecture Framework (TOGAF; The Open Group, 2009), Department of Defense Architecture Framework (DODAF; DoD CIO, 2010), and Zachman's Framework (Zachman, 2008) provide business analysts with guidelines and worksheets to capture architectural elements, but none of these frameworks use formal languages to enable model checking to find inconsistencies and conflicts within an architecture. Alternatively, Breaux and Powers (2009) found the Business Process Modeling Notation (BPMN), a declarative language for describing business processes, to be ineffective to express necessary temporal constraints in policy requirements. Ouyang, van der Aalst, Ter Hoftede, and Mendling (2009) asserted that the Business Process Execution Language (BPEL), preferred as the candidate formal semantics for BPMN, only works for limited classes of BPMN models (Ouyang et al., 2009).

Extensive work has been done to model information assurance policies. Breaux developed an early framework to extract privacy and security requirements from regulations (Breaux, Vail, & Antón, 2006), which was later validated in the context of healthcare (Breaux & Antón, 2008). This work led to the development of a requirements-specification language to further automate the encoding process (Breaux & Gordon, 2013). More recently, this work has been formalized using DL to model-check requirements (Breaux et al., 2008) and to trace requirements across mobile application policies (Breaux & Rao, 2013). Breaux has studied the gap between security policy and functional requirements and found a need to express both elements of physical and cyber security architecture in the same language to reason about modern vulnerabilities in distributed systems (Breaux & Baumer, 2011).

Discussion and Summary

In this paper, we presented a mobile application framework that can be used to map existing DoD IA policy onto emerging mobile devices. The aim of the framework is to identify opportunities for new methods and tools to decrease the time required to assure that mobile devices and their applications conform to IA policies. Our approach consists of a taxonomy for classifying mobile apps based on different security risks and an application profile and language for describing data flows within mobile apps that can be used to check for security conflicts. The profile describes what information is collected, used, and transferred, and for what purposes; and the language is used to express the profile formally and to identify conflicts within and between profiles using automated theorem proving. In future work, we plan to extend the framework with extensions to address potential policy conflicts across physical locations as mobile devices traverse different enclaves. In addition, we aim to

experimentally evaluate this approach with mobile app developers and certification authorities responsible for verifying that these apps conform to relevant policy.

References

Alberts, D. S., Garstka, J. J., & Stein, F. P. (1999). *Network centric warfare: Developing and leveraging information superiority* (2nd ed.). DoD C4ISR Cooperative Research Program (CCRP).

Baader, F., Calvenese, D., & McGuiness D. (Eds.). (2003).*The description logic handbook: Theory, implementation and applications*. Cambridge University Press.

Boessenkool, A. (2009, March 4). DoD IT procurement too Slow: Cartwright. *Defense News*.

Breaux, T. D., & Antón, A. I. (2008, January/February). Analyzing regulatory rules for privacy and security requirements. *IEEE Transactions on Software Engineering, Special Issue on Software Engineering for Secure Systems*, *34*(1), 5–20.

Breaux, T. D., Antón, A. I., & Doyle, J. (2008, November). Semantic parameterization: A process for modeling domain descriptions. *ACM Transactions on Software Engineering Methodology, 18*(2), 5.

Breaux, T. D., & Baumer, D. L. (2011). Legally "reasonable" security requirements: A 10-year FTC retrospective. *Computers & Security, 30*(4), 178–193.

Breaux, T. D., & Gordon, D. G. (2013, April). *Regulatory requirements traceability and analysis using semi-formal specifications.* Manuscript accepted to the 19th Working Conference on Requirements Engineering: Foundations for Software Quality (REFSQ'13), Essen, Germany.

Breaux, T. D., & Powers, C. (2009, April). Early studies in acquiring evidentiary, reusable business process models for legal compliance. In *Proceedings of the 6th International Conference on Information Technology: New Generations (ITNG'09)* (pp. 266–272), Las Vegas, NV.

Breaux, T. D., & Rao, A. (2013). *Formal analysis of privacy requirements specifications for multi-tier applications*. Manuscript accepted to the IEEE International Requirements Engineering Conference.

Breaux, T. D., Vail, M. W., & Antón, A. I. (2006). Towards regulatory compliance: Extracting rights and obligations to align requirements with regulations. In *IEEE International Requirements Engineering Conference* (pp. 49–58).

Brewin, B. (2011, March 29). Army confirms battlefield smartphones tests began in December. *Defense News*.

Carter, A. B. (2010, March 11). *Witness testimony from the Under Secretary of Defense for Acquisition, Technology & Logistics before the House Armed Services Committee Panel on Acquisition Reform*.

Defense Information Systems Agency. (2006, January 17). *Application services, security technical implementation guide* (Version 1, Release 1). Defense Information Systems Agency (DISA).

Defense Science Board. (2009, March). *Report on Department of Defense policies and procedures for acquisition information technology*.

DoD CIO. (2010, August). *The Department of Defense Architecture Framework (DODAF) version 2.02*. Retrieved from http://dodcio.defense.gov/dodaf20.aspx

Fillmore, C. J. (1968). The case for case. In E. Bach & R. T. Harms (Eds.), *Universals in linguistic theory*. New York, NY: Holt, Rhinehart and Winston.

Gates, R. M. (2009, April 16). Remarks to the Army War College, Carlisle, PA.

Gruber, J. (1976). *Lexical structure in syntax and semantics*. New York, NY: North Holland.

Horty, J. F. (1993). Deontic logic as founded in non-monotonic logic. *Annals of Mathematics & Artificial Intelligence*, *9*, 69–91.

Lopez, T. (2010, April 5). “Apps for Army” to shape future software acquisition. *Army News Service*.

Montalbano, E. (2011, May 27). DoD tests delivery of data to mobile devices. *Information Week*.

Onley, D. S. (2006, August 23). Untangling the chain of information. *Government Computer News*.

The Open Group. (2009). The Open Group Architecture Framework (TOGAF), version 9. Retrieved from http://www.opengroup.org/architecture/togaf8-doc/arch/toc.html

Ouyang, C., Dumas, M., van der Aalst, W. M. P., Ter Hoftede, A. H. M., & Mendling, J. (2009, August). From business process models to process-oriented software systems. *ACM Transactions on Software Engineering and Methodology, 19*(1), 2.

Suh, S., Heo, S. W., Park, C. J., Ryu, J. M., Park, S., & Kim, C. R. (2008). Xen on ARM: System virtualization using Xen Hypervisor for ARM-based secure mobile phones. In *5th IEEE Consumer Communications and Networking Conference* (pp. 257–261).

Walker, M. (2011, March 21). Army unable to create, distribute the high-level mobile apps they want. *Fierce Government IT*.

Wyatt, E. (2010, April 13). *Rapid fielding: A topic of conversation for winning the current and future fights*. DDR&E/Dir of Rapid Fielding.

Zachman, J. A. (2008). *The Zachman’s framework: A primer for enterprise engineering and manufacture.* Retrieved from http://www.zachmaninternational.com/index.php/ebook

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF BUSINESS & PUBLIC POLICY
NAVAL POSTGRADUATE SCHOOL
555 DYER ROAD, INGERSOLL HALL
MONTEREY, CA 93943

www.acquisitionresearch.net