Security Risk Assessment of Decentralized, Mobile Applications: An Analysis of Location Aware Systems

Amy W. Ray  
*Bentley College*, aray@bentley.edu

Julian J. Ray  
*C2G Logistics, Inc.*, julianray@c2gl.com

Follow this and additional works at: [http://aisel.aisnet.org/amcis2005](http://aisel.aisnet.org/amcis2005)

**Recommended Citation**

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2005 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
Security Risk Assessment of Decentralized, Mobile Applications: An Analysis of Location Aware Systems

Amy W. Ray
Bentley College
aray@bentley.edu

Julian J. Ray
C2G Logistics, Inc.
julianray@c2gl.com

ABSTRACT
Technological improvements, declining costs and mandates to suppliers from large entities such as Wal-Mart and the Department of Defense are driving investments in RFID and other location aware systems (LAS). Expected benefits from LAS investments include improvements in supply chain integration and streamlined operations. However, LAS may introduce a number of new information security vulnerabilities into organizations that must be carefully considered. LAS are highly decentralized and mobile, yet must connect to existing transactional systems to function. Decentralized, mobile applications are especially difficult to secure, and connections between LAS and internal applications can put those systems at risk too. The additional complexity of overall systems architectures also makes identifying security risks more challenging. We assert that current guidelines for information security are increasingly insufficient for organizations with highly decentralized systems and that more attention to how systems are employed is needed. We demonstrate this point with logical process models that illustrate how two different uses of one LAS technology result in different information security risks.

Keywords: Security, Location Aware Systems, RFID.

INTRODUCTION
The number of information system security management challenges facing organizations today is increasing for several reasons. One contributing factor is the growing number of portable devices and mobile technologies being adopted for strategic purposes. Many business and military organization have recently made significant investments in special location aware mobile technologies such as RFID and GPS to enhance business processes and military supplies management. If effectively implemented, information about an asset’s specific location as well as any additional information recorded about the asset on an attached tag or device may be remotely accessed by the organizations implementing the location aware system (LAS). The availability of such information is expected to improve asset management and reduce opportunities for theft while the ability to remotely collect and read data on the device attached to the asset is expected to reduce supply chain management time and errors and ultimately improve profitability.

Most research on decentralized mobile applications has focused on the potential improvements in efficiency and effectiveness that organizations may attain from using mobile systems. However, information security risks associated with their deployment must be addressed before systems are fully trustworthy to their authorized users. Evidence of serious security breaches made possible through poorly secured mobile systems are beginning to emerge (Poulsen, 2005), yet fewer than ten percent of organizations have developed a formal and comprehensive mobile security policy (Firstbrook, 2005).

In this research in progress, we argue that the increasing complexity of systems and the diversity of systems use in highly decentralized and mobile environments requires a more formal approach to security risk assessment than companies have historically used with internally managed systems. Our evolving analysis is designed to illustrate how logical models of systems processes are a useful addition to the security manager’s arsenal. Logical models of organizational and business processes have been used in the past as aids in the analysis and design of complex information systems and by the accounting profession for mapping internal controls and processes within organizations. Many companies, including General Electric, IBM, and NASA, have re-discovered the usefulness of logical modeling techniques to better understand the underlying business and work processes enabled by the variety of systems used (Jacka, et al., 2001; Hunt, 1996; Alter, 2001; Janz et al., 2005). We propose that these logical models may also be useful tools for assessing and managing information systems risk for complex environments such as highly distributed mobile systems environments. Accordingly, we advocate use of the familiar technique of logical modeling, but for analysis of information systems risk, especially where information systems are highly decentralized and mobile, as they are in location aware systems. In the following sections, we discuss information...
security management challenges resulting from increasing decentralization and mobility of systems, the current state of the art in security management guidance and how logical models may be used to fill some of the security guidance gaps, particularly for mobile, decentralized systems.

INFORMATION SECURITY MANAGEMENT CHALLENGES

Some electronic transactions are digitized versions of older processes while other transactions and electronic activities involve completely new processes. Web-based EDI, for example, is one type of Internet transaction that is similar to its predecessor, traditional EDI. Accordingly, appropriate security policies and procedures for traditional EDI can be readily adapted to web-based EDI. Yet, web-based EDI faces additional security challenges associated with use of the Internet as the medium for communication that must also be considered.

Other electronic transactions involve digitization of processes that were previously analog or otherwise in a different electronic format. Face-to-face meetings and telephone calls are now often replaced by e-mail, exchange of electronic working documents, virtual meetings and teleconferencing. Similarly, business processes such as sales and inventory control are increasingly digitized and automated through the combined use of new inter-organizational processes and newer technologies such as RFID tags or other location aware technologies. When mapping out a security management plan, businesses must consider how use of new electronic systems affect security risk while simultaneously considering the security risks inherent to the new technologies.

The volume of electronic business activity, the value of information shared per exchange and society’s reliance on information systems all continue to grow, yet information systems often have little or no security built into their architecture (Power, 2002). A recent survey of information security professionals reveals that IT security budgets appear to be around 6-8% of overall IT budgets in developed countries and lower in other regions (Deloitte Touche Tohmatsu, 2003). Findings from a CIO Magazine survey (2002) are consistent and further found that CIOs surveyed reported an average of seven security breaches a year and 63% of the respondents believe investment in information security at their organization needs to increase.

The challenge for security professionals is to identify a holistic view of the security management issues in an environment where systems complexity and security threats are increasing simultaneously. In the next section, we discuss the current state of the art in security management.

SECURITY MANAGEMENT STATE OF THE ART

Information security guidance for protecting access points, networks, physical devices, data and other systems elements has typically either been strategic-level, top down guidance or bottom up technology specific guidance. Examples of top down guidance include the Information Systems Audit and Control Organization’s Control Objectives for Information and related Technology (COBIT), the International Standards Organization’s ISO17799 and portions of the U.S. Department of Health and Human Service’s Health Insurance Portability and Accountability Act (HIPAA). Examples of bottom up guidance include specific administrative procedures for securing a UNIX platform, appropriate encryption methods for securing the 802.11b wireless network protocol and appropriate password management techniques for a specific end-user application (Hesseldahl, 2004; Keizer, 2003; Power, 2004; Soderborg, 2003; Sullivan, 2005; Zviran, 1999). Information security research focused on theoretical development and further improvement of strategic-level, top down information security guidance continues to progress as well (Nance and Straub, 1988; Straub and Welke, 1998; Sherer and Alter, 2004; Alter and Sherer, 2004; Deshmuhk, 2004).

The bottom up approach to information security management, when used alone, is inefficient because individual technologies continue to evolve and also because organizations may change technologies for a given application or even employ multiple technologies in parallel to perform the same application functions for different users. Using only a bottom up approach to security is also ineffective because the impact of a technology’s interaction with other systems to which it connects and use-related risks are less likely to be visible through a bottom-up lens that focuses primarily on technology-specific characteristics. In fact, to date there has also been little discussion in the academic or professional literatures about the possible interaction between alternative uses of systems and risk. For example, are there different risks associated with a system that processes information by pushing it through the system versus a system that pulls information if both systems use the same hardware, software and networks?

Strategic frameworks such as ISO17799 and COBIT have been a useful starting point for many organizations because the frameworks are implementation-neutral and generalizable across companies and industries. However, there still remains little research or professional guidance on how an organization should go about mapping a strategic framework such as ISO17799 to a unique implementation of systems components for completion of specific organizational processes.

In the next section, we demonstrate the potential usefulness of logical models as a complement to existing strategic frameworks and bottom up methods for assessing information security risk in highly decentralized, mobile environments.
LOGICAL MODEL EXAMPLE: LBS

We use location based systems (LBS) for illustrative purposes because LBS are loosely connected systems with multiple current technological deployments (e.g., GPS, RFID, ActiveBat, Cricket) and because LBS are emerging as popular means for conducting a wide range of business transactions (Mitchell and Whitmore, 2003). The characteristics of technological diversity and immaturity, as well as expected growth in use make LBS an attractive candidate for testing our theoretical approach to security management. The diversity of technologies and applications of LBS are apparent from consideration of just a few emerging sample uses: cell phone applications to help locate the nearest gas and food, transportation management systems for optimizing routes and tracking assets and inventory management of consumer goods as they move from manufacturing to warehousing to retail outlets.

We begin by focusing on the logical process of determining the relative positioning of two or more objects participating in a LBS process. At a fundamental level, all location-based applications aim to determine with reasonable accuracy the relative position of one object, the object being located, to an object collecting the location information or external referencing scheme in order to provide value-added services at the point of the object being located. Example services provided may include anything from simply performing inventory updates within a warehouse, monitoring the movement of assets, and providing specific value-added content back to an object based on location-specific information. We refer to the objects being located as locatable objects, and the objects performing location data collection as location collection objects. A locatable object is any object that can have its location derived using a location collection process. A location collection process is then an interaction between locatable objects and location collection objects and involves the transmission of location data from a locatable object to a location collection object (Figure 1).

Figure 1. Logical Model

The location data that is transmitted during a location process contains two fundamental properties: an object reference and a location reference. Additionally, a temporal reference determining the time for which the location reference is valid can be sent in explicit or implicit form (Rodden, Friday, Muller and Dix, 2002). The object reference is used to denote uniqueness or class membership such as a product code, for the locatable object. In some cases, the object reference might be transmitted as actual data or conversely, implied within the properties of the signal itself (e.g., a specific radio signature). The location reference is defined within the spatial context of the location process and can consist of explicit, derivable, or implied location information. Explicit location references, such as a geographical coordinate, place the locatable object in an external spatial context such as the global coordinate system. A GPS-enabled transponder, for example, can transmit the actual geographic coordinate of the device. Derivable location references require the use of external positioning techniques to determine the location of the locatable object based on the physical properties of the transmission. A cell phone can be located with some degree of accuracy using triangulation methods, for example. Lastly, implied location references place the locatable object in the spatial context of a collection object based on a Boolean result of a collection process, i.e., the object is either there or it is not. The presence of an RFID tag, for example, can only be detected when it is within spatial proximity to a suitable reader.

A location collection process is initiated by a location event. A location event results in location data being transmitted and can originate from either locatable objects or location collection objects. When a locatable object initiates a location event the collection process is defined in this paper as a “Push” system. Conversely, when a location collection object initiates a location event the collection process is defined here as a “Pull” system.

Push Systems

Push systems are characterized by locatable objects which initiate location events (Figure 2).
The transmission of location data in Push systems requires an internally generated signal and power source and the location data is generally broadcast based on a location event initiated by the locatable object. Push technologies have the capability to initiate the dissemination of location data and have little or no control over the number and nature of the collection objects which receive the location data. Technologies in this category include devices such as GPS-enabled transponders, cell phones that can be located via triangulation methods, angle of arrival (AOA), time of arrival (TOA) and radio-beacons such as those used to guide aircraft or locate aircraft black-boxes. Active RFID tags also belong in this category as once activated they can transmit location data without being in proximity to a reader.

**Pull Systems**

In contrast to push systems, location event data in pull systems is transmitted in response to a location process initiated by a location collection object. The location event initiator in this case is a location collection object that queries a locatable object for its location information. During the location process, the location collection object broadcasts a query to one or more locatable objects, which respond with location data (Figure 3).

With pull systems, the location of an object is usually mapped into the location context of the collection object. An RFID scanner inventorying objects passing through a doorway, for example, will retrieve the RFID identifier and instantaneously determine the location of the object relative to the scanner. The location context of the scanner is restricted to the “scan tunnel,” i.e., the concept of location in this example is a Boolean: the object is either present in the “scanned” space or it is not. Applying this concept, we can also place UPCs and bar-scanners in the same framework. The location of the UPC reader sets the location context of locatable objects (i.e. objects with bar codes). The only difference between the UPC and RFID technologies for purposes of this model is that UPCs require line-of-site and therefore have a significantly restricted location context. UPC scanners can also inventory objects one at a time.

**APPLICATION OF SECURITY PRINCIPLES TO LOGICAL DESIGN**

Three information security principles are common to most strategic frameworks: information integrity, confidentiality and availability (Bishop, 2003). Information integrity refers to the trustworthiness of data content and data sources, information confidentiality refers to protection of data from unauthorized users and uses and information availability refers to assurance that data sharing processes are protected from interruption. Table 1 provides examples of general information security threats in each of these three categories of security services. Note that some threats are against multiple security services. Consider further that each threat may be associated with multiple methods of attack. For example, categories of individuals who may attempt to intercept and collect (read) data include employees, former employees, random hackers, competitors or terrorists. Similarly, methods employed for interception and collection of data may include stealing or hacking a password of a
legitimate user, tapping into the communications medium, breaking into the database where desired information is stored, modifying an application program to change routing of information or theft of a computer or device that will allow access to the desired information. While some efforts to expand categorization of security services beyond these three elements exist, not all security professionals and researchers agree on the expanded models, but most will agree to the generalizability and importance of integrity, confidentiality and availability.

<table>
<thead>
<tr>
<th>Integrity</th>
<th>Confidentiality</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intercepting and modifying data</td>
<td>Intercepting and collecting data</td>
<td>Poaching network services</td>
</tr>
<tr>
<td>Poor data quality controls</td>
<td>Intercepting and modifying data</td>
<td>Denial of service</td>
</tr>
<tr>
<td>Destruction of data</td>
<td>Malicious code</td>
<td>Malicious code</td>
</tr>
<tr>
<td>Malicious code</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1. Information Security Services and Security Threats

SAMPLE APPLICATION OF SECURITY PRINCIPLES TO LBS EVENT MODEL

To illustrate a logical design approach to analyzing security issues in location based systems, we apply the three security services described above and the logical model of LBS defined earlier to a simple example from electronic supply chain integration. The problem we analyze requires providing visibility of palletized goods as they move from manufacturer to warehouse. In the first part of the example we look at a push system implementation, which will typically involve either attaching a locatable object to a shipping container containing the pallets or to the vehicle transporting the pallets. We then perform the same analysis for a pull system which will typically involve tagging individual pallets or pallet contents using low-cost RFID tags. Results are shown in Table 2.

Our goal in performing this exercise is to illustrate how important considerations for ensuring information security are more readily apparent when using a logical system design, and to further illustrate how different model designs necessitate different approaches to security management.

<table>
<thead>
<tr>
<th>Push System</th>
<th>Pull System</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Integrity Issues</strong></td>
<td></td>
</tr>
<tr>
<td>Loss or attenuation of signal due to “blind spots”, out-of-range and system black-outs.</td>
<td>Re-coding of RFID tags once they have been attached.</td>
</tr>
<tr>
<td>Spurious location readings due to external effects on signal reception.</td>
<td>Re-location of readers.</td>
</tr>
<tr>
<td>Malicious use of technologies to confuse or jam signals (e.g. GPS jammers).</td>
<td></td>
</tr>
<tr>
<td>Control of network to ensure data received and processed is not altered.</td>
<td></td>
</tr>
<tr>
<td><strong>Confidentiality</strong></td>
<td></td>
</tr>
<tr>
<td>Interception of signal by non-authorized systems.</td>
<td>Controlled access to readers.</td>
</tr>
<tr>
<td>Ability to relate signal to physical object (i.e. the container).</td>
<td>Controlled access to proximity of container within “scan range” of reader.</td>
</tr>
<tr>
<td>Ability to infer container content from signal.</td>
<td>Availability of technical specification of implementation e.g. RFID transmit frequencies, range, etc.</td>
</tr>
<tr>
<td>Ability to track container as it moves from source to destination and predict future location and time.</td>
<td>Reconciliation of pallet contents to RFID tag.</td>
</tr>
<tr>
<td><strong>Availability</strong></td>
<td></td>
</tr>
<tr>
<td>Internal power source.</td>
<td>Access to readers.</td>
</tr>
<tr>
<td>Dependent on availability of network.</td>
<td>Power source for readers.</td>
</tr>
<tr>
<td>Network traffic.</td>
<td>Frequency interference.</td>
</tr>
</tbody>
</table>

Table 2. Application of Push/Pull Model
To illustrate how the logical models can be used for implementation we provide a brief description of implementation details here. Push systems for containers can be readily implemented using radio-transmitting technologies such as cell-phones or short-wave radios possibly coupled with GPS receivers. The device will transmit its location periodically, every 15 minutes for example. Base stations or cell-towers will intercept the transmissions and pass the data onto an application which can use the data to update the location of the container.

Pull systems for pallets can be implemented using passive RFID tags with low-frequency transmitters which can penetrate the walls of the container. The RFID tags are activated when in the presence of a suitable reader which can record the time at which each tag was read by a specific reader and send the data to an application which can update the time at which the container was read by a specific reader. The reader is in a fixed location known a-priori to the application: the exit gate of the manufacturer, an in-transit location or the entrance to a storage facility, for example.

FUTURE RESEARCH

We assert that it is impossible to understand the complexities of mobile, decentralized systems architectures by looking at the physical implementation of a system, one component at a time. We also assert that looking at the holistic system through only a strategic lens misses many of the business process change issues associated with the specific uses of a particular implementation.

We propose that security managers and researchers work together to identify new methods for bridging the gap between strategic security guidelines and implementation specific guidance. This evolving research has demonstrated that using simple diagrams of logical processes will result in identification of a more complete set of security vulnerabilities than using top down, strategic frameworks or bottom up technology specific security controls. To complete this research project, we will develop a fuller discussion of the differences and similarities across different types of LAS, include a more complete description of common risks across LAS and expand our discussion on the value of logical models for assessing risk associated with decentralized, mobile applications.

Much more research is needed in this area. Future research could involve refinement of the logical model presented here, and development of additional logical models for other information systems architectures, as well as mapping of logical models to specific top down frameworks at one end and bottom up technologies at the other end. Additional research is also needed to further develop security frameworks and to identify the applicability of various security frameworks to different domains.

REFERENCES


