A Privacy-Enabled Architecture for an RFID-based Location Monitoring System

James Lee
Faculty of Business and Information Technology
University of Ontario Institute of Technology
Oshawa, Ontario, Canada
James.Lee@uoit.ca

Khalil El-Khatib
Faculty of Business and Information Technology
University of Ontario Institute of Technology
Oshawa, Ontario, Canada
Khalil.El-Khatib@uoit.ca

Abstract—In large hospitals, location discovery and contact discovery presents possibilities to quickly find someone in an emergency, to narrow the epidemiologic scope of an outbreak, and to reinforce good safety practices. An RFID architecture can make the necessary location data available for knowledge extraction. While people can carry RFID tags to help track their location, their location privacy must also be protected from unauthorized surveillance throughout its collection. This paper proposes a privacy-enabled architecture for an RFID-based hospital location tracing system that prevents network eavesdroppers from tracing a person’s location after associating a person to a tag’s identifier.

Keywords: RFID; privacy; location

I. INTRODUCTION

An RFID tag’s static unique identifier, once associated to an individual, acts as a marker for that individual. Every interrogation of the RFID tag marks the associated individual’s location. An adversary able to correlate a person-tag association can compromise the individual’s location privacy. Whether the tag’s unique identifier is encrypted, or is individually serially rotated, the person-tag relationship remains 1:1. The target person-tag association can be easily re-established, offering insufficient location privacy protection. In a crowd of N person-tag associations in which crowd members, when co-located, can trade tag identifiers with each other before dispersing, the person-tag relationship temporarily becomes 1:N. When the target person-tag association is changed, the adversary can no longer trace the true location of the target and the person’s location privacy can be protected.

II. ADAPTING THE CROWDS SYSTEM

The Crowds system, developed by Reiter and Rubin [1], protects senders’ anonymity in the internet by relaying communications through multiple crowd members, obscuring the original source IP address of any communication after the initial relay. Observing a message from one crowd member offers no confidence whether that message originated from that crowd member, or whether it was merely relayed by that member.

Protecting the location privacy of RFID tag-carrying people from a network eavesdropper relies on the difficulty to determine their vectors and a high frequency [2] of change in person-tag associations. A modified crowd system is employed where physical co-located crowds of person-tag associations are formed, in which crowd members may swap their tag identifiers with each another, or other system agents. The formation of the crowd shrouds potential changes to person-tag-vector relationships, increasing the uncertainty of a targeted crowd member’s location based on any previous person-tag-vector association.

Figure 1. Vectors co-located in crowd zone trade RFID tag identifiers.

In figure 1, initial person-tag pairs, denoted by (Px,Ty), enter a Crowd Zone. Tags are scrutinized for trust. Tags meeting trade rules may trade tag identifiers and update system person-tag associations. Here, three real pairs and one system agent pair, (P4T4), are logically dis-associated. Four new person-tag pairs are possible.

In this privacy-enabled architecture, crowds facilitate ongoing, indeterminate and secret reallocation of nearby person-tag associations. Each subsequent Crowd Zone interaction further increases the variability from the original person-tag association. An adversary tracing a person’s location through network interrogations of their RFID tag, over time, can have no confidence of the identity of the person associated to a tag. This strengthened assurance of personal location privacy contributes to user trust and user acceptability of location monitoring systems.
III. SYSTEM ARCHITECTURE

A. Design Components

A referential RFID tag stores only a unique identifier, distinguishing itself from every other trusted tag member known by the system. Using active RFID tags and an adapted crowd system, tag identifiers are rotated among co-located individuals forming an ad-hoc crowd, unlinking the tag carriers from their previous person-tag associations. The Crowd Broker, figure 3, is the architecture’s key component to for location privacy in the network, responsible for rotating co-located person-tag associations.

Supporting domains include Tag Activation, Wireless Network, and Data Repository. The Tag Activation and Wireless Network components focus on system access, person-tag membership, and network access control. The Data Repository component contains the collected user, location, and tag-rotation data which supports knowledge extraction to discover locations, contacts with others, and interactions with equipment.

This architecture works to mitigate privacy perceptions of participants by protecting the location information of tag carriers, i.e. minimize the risk of real-time surveillance, to produce aggregate anonymity in data analysis and to support the provision of situational awareness of individuals in emergency conditions.

B. Tag Activation

Tag carrier privacy begins with RFID tags that have no information other than a unique identifier (UNID) known to the system. Upon arrival on site, the user randomly collects an inactive RFID tag and logs into the wired network.

The tag activation process associates their user ID with an activated tag ID. The UNID is derived from a mathematical hash of the user’s ID concatenated with the initial tag UNID, de-personalizing the tag carrier’s identity to any interrogations of the tag. The data pair is hashed and encrypted during transport through a firewall to the Data Repository domain.

Access controls, data encryption, and audit mechanisms on databases and logs storing data which could be used to correlate an individual to an RFID tag, further minimizes risk to tag carriers’ location privacy.

C. Wireless Network

This domain represents the wireless infrastructure to interrogate RFID tags and to rewrite tag identifiers during the formation of a crowd.

D. Crowd Broker

Location privacy is dependent on the Crowd Broker identifying a logical cloud formation, verifying the members of the crowd, and managing the rotation of tag UNIDs in trusted person-tag associations. The ID Data Triangulation Broker subsystem supports the evaluation of trust and location, determining the RFID tag UNID-reader ID pair to be evaluated when a tag has proximity to more than one reader, then validates incoming tag UNID-reader ID pairs against tag UNIDs recorded during tag activation, and known reader IDs, ignoring rogue tags and readers that may be introduced into the environment. The Crowd Broker is the key component supporting location privacy of RFID tag carriers.

E. Data Repository

This domain manages all the data that could expose a tag wearer’s identity or location, and is assumed to be hardened against unauthorized physical and logical access, and regularly audited for privacy assurance. Several sub-systems are present to deliver post-event business intelligence to management, to provide real-time location awareness for emergency response, to verify access point identities and tag identities, and to strengthen individual location information privacy through crowds.

For audit control and to support future data mining to address non-compliance issues, the ID Switch Tracking Data container also records all tag UNID switching events. This
data, combined with the Raw System Data, facilitates trace back to an initial tag UNID, and its owner, to audit individual compliance. Also, to conserve the lifespan of the active tags, the ID Switch Tracking Data container is queried to determine the elapsed time since members of the tag crowd were reassigned a new UNID. Tags in the crowd which have exceeded a time threshold, swap tag UNIDs with each other, or a tag which has not exceeded the threshold, when there is just one tag which has exceeded the time threshold. After virtually recording the new tag ID associations, the tags are refreshed. Upon acknowledgement from a tag of its new ID, the transaction is committed to disk.

IV. HOSPITAL APPLICATIONS

A. RFID-enabled Environment

In an RFID-enabled environment where all staff carry tags, a medical specialist can be remotely located; an infected nurse’s contacts with others can be traced to help contain spread; and staff interactions with tagged equipment can verified to ensure protocol compliance, e.g. hand wash-gloves-gown-mask.

Figure 4. Typical RFID-enabled patient room.

Figure 4 above shows a typical patient room. The parenthesized figures are representative of relative location co-ordinates. To support policy compliance, in a typical patient room, we have determined the fixed, relative location (x,y) co-ordinates of concerned touch points, such as sinks, antibacterial dispensers, garments, and disposal containers. For example, the location of the gowns and gloves, relative to the room, is the set \{ (2,0), (2,-1), (4,0), (4,-1) \}, representing the cart’s footprint relative to the patient room’s axes.

B. Location Finding

Knowledge of the location of tag-carrying people can be created through data analysis of tag interrogation records and the known locations of fixed tag readers. Several location-finding applications have already been demonstrated in hospital and industrial settings by commercial RFID-location technology vendors[3][4], without location privacy. This privacy-enabled architecture would require an additional synchronization to tag identifier switch records in order to locate specific tag-carrying people. In the sample environment, figure 4, the location of a person-tag pair at one point in time could be denoted by the relative co-ordinates (5,1) which positions the pair just inside the entry of the patient room.

C. Contact Discovery

Staff location data can be used to help identify the epidemiology of hospital-acquired infections [5]. Discovery of possible contact events can contribute to more efficient containment efforts by providing the knowledge which permits a focused response.

D. Protocol Compliance

Defining rules such as a hygiene protocol to follow when entering/exiting a patient room, acceptable co-ordinate sequence patterns expected from tag carriers are defined for the system.

Figure 5. Typical SARS hygiene protocol.

A tag carrier approaching a room stops to follow the expected protocol before entering. The system measures that the relative (x,y) location co-ordinates of the tag carrier outside the room has proximity to the location of gowns and gloves, etc., followed by co-ordinates within the room, followed by a location outside the room, and proximity to the disposal location. Based on the co-ordinate data set and sequence of events, the tag carrier is presumed to have complied with the protocol. Event exceptions to any expected sequence of events could be delivered immediately to a tag carrier for compliance feedback, and be used to measure overall organizational
compliance. Subsequent steps involving care-givers and patients carrying tags, and tags fixed to personal protective equipment, offers the additional granularity to construct views of policy compliance and possible risks. In the sample environment, figure 4, protocol compliance could be inferred by a co-ordinate set in this sequence: \{(4,0), (2,0), (5,0), (12,2), (7,0), (9,0), (4,0)\}. The care-giver’s proximity to the antibacterial dispenser (4,0), followed by the gowns and gloves cart (2.0), the room’s entranceway (5,0), patient bed 4 (12,2), the entranceway (7,0), the waste container (9,0), and the antibacterial dispenser (4,0), suggests a strong propensity for policy compliance.

V. CONCLUSIONS AND FUTURE RESEARCH

Recognizing the ongoing privacy concerns of deploying RFID technologies in healthcare settings remains a barrier to the adoption of RFID technology in healthcare environments. But, if the privacy of individuals can be sufficiently assured, the healthcare sector could achieve similar business value from RFID technologies as in commercial or industrial environments. Crowd anonymity is one possible approach to assure the privacy of tag wearers.

Our future work will focus on building a mathematical model to compute the probabilities of an adversary to maintain true person-tag association knowledge through adapted crowd system. Additionally, the proposed system architecture does not yet consider the possible timing or performance issues with tag interrogation and rewriting IDs over a wide network with hundreds or thousands of tags. Scalability, privacy audit controls, evaluating its economic viability, and constructing a proof-of-concept of the Crowd Broker sub-system, are all possible future research segments.

ACKNOWLEDGMENT

The authors would like to thank Purelink Technology, Inc. for the continuous support on this project. Also, the authors are thankful to Joseph Horobetz for building a simulation of the presented model.

REFERENCES