SAND2012-6335C

Addressing Insider Threat using “Where You Are” as Fourth Factor Authentication

Sung Choi and David Zage

Introduction

For thousands of years, humans have been using authentication methods based on various factors to identifying individuals. These have ranged from simple passphrases given to sentries to be allowed access to a walled city, to special tokens used to gain access to secret meetings, to modern day cryptographic-based public key authentication services to connect to remote computers. In its very basic form, authentication consists of an entity, the user, attempting to prove the user’s identity to a secondary entity called the verifier \cite{Bishop2002}. Authentication is then leveraged to provide access privileges and define the roles and responsibilities associated with the user. For example, a user may use a secret password to authenticate and gain access to a computer system. Once allowed access, the user will have a predefined role, allow certain abilities (e.g., reading a file) while restricting other (e.g., deleting a file).

As can be seen from \reffig{fig:3factor}, the manner in which a user is authenticated typically falls into one of three categories based on the information used in the authentication process:

\begin{itemize}
    \item Knowledge - ``what you know"
    \item Inherence - ``what you are"
    \item Ownership - ``what you have"
\end{itemize}

Figure 1 - Three factors used during authentication

Each of the factors has its own strengths and weaknesses and employing any of them for authentication can improve the security and robustness of the system \cite{O'Gorman2003}. It is also well-known that authentication methods that depend on more than one of these factors are more difficult to compromise than single-factor methods \cite{Council2011}. It should be noted that using two or more of the same factor, such as a password and private information know to an individual, is not considered multi-factor authentication.

While the traditional three factors of authentication (in isolation or combined) can greatly increase the security of a given system, they have deficiencies, particularly in dealing with the insider threat. Typically, once an insider has been authenticated, he or she is given complete and unlimited access for the rest of the time they are using the access controlled resource. This is done to simplify protocols and to avoid annoying end users if they are requested to verify their identity too frequently. Even authentication methods that depend on more than one factor are thus are more difficult to compromise than single-factor methods \cite{Council2011} are often still vulnerable to insider/remote attacks and place a high usability cost on the end-user.

In order to address these identified shortcomings, this paper proposes to utilize ``where you are'' (location) as a fourth authentication factor and shows how it could be used for a robust insider Threat Prevention System (iTPS). iTPS has the potential to radically change the physical protection systems and cybersecurity landscape by providing institutions with the first-of-its-kind tool for real-time threat prevention capabilities.

The contributions of this paper include:
\begin{itemize}
\item Three general rules of authentication that must be satisfied by a system in order to provide security and usability. These rules allow for the analysis and comparison of existing authentication techniques as well as the technologies used to implement the techniques.
\item The use location as a fourth factor and derive authentication attributes based on our generalized rules. Multiple existing indoor positioning technologies were examined as possible candidates and many of the solutions were found to have issues with accuracy, robustness, scalability, or portability.
\item The development of the requirements for a fully functioning iTPS system
\end{itemize}

The rest of the paper is organized as follows: limitations of current authentication techniques and general rules for authentication are proposed in \refsec{sec:limits}, methods for enabling location as a fourth factor for authentication are looked at in \refsec{sec:enabling}, current location technology is reviewed in \refsec{sec:itps}, the iTPS is formalized in \refsec{sec:app} and the paper is concluded in \refsec{sec:conclusion}.

Limitations of Traditional Authentication Techniques and Factors

For well over 2000 years, passwords and passphrases have been the authentication method of choice for identifying an individual. While knowledge-based authentication factors are used as the sole means to provide authorization and access privileges for many systems, they have several limitations which can limit their security and utility. Security guarantees based on known personal information assumes this data is maintained as secret known only to the user and verifier. One of the primary limitations is the simple fact that people have to actually remember the secret information, which limits the potential complexity of the password. In order to make passwords easier to remember, individuals often choose short sequences of characters, which have a low amount of entropy and are thus easy to attack \cite{ Bishop2002}. If the user does choose a strong password \cite{certPassword} which is then forgotten, the user will have to use an out-of-band channel to reset the password. In order to avoid this, one methods many users resort to is writing the password down and leaving it with the computer, thereby invalidating the point of the knowledge-based authentication. These aforementioned problems are only exacerbated by the number of user identities and passwords (potentially shared between multiple authentication mechanisms) that modern users are expected to recall on demand. Finally, when the password is used as the sole authentication means, the authentication mechanism is vulnerable to parallelized password guessing techniques \cite{Rankin2012} and social engineering attacks such as spear phishing \cite{Hong2012}.

The second authentication factor that is used in many modern systems is ``what you are''. Inherence factors, also often referred to as biometrics, can be further divided into physiological characteristics, such as fingerprints, and behavioral patterns, such as typing patters \cite{Jain1999}. While biometrics might seem to be appealing for use in authentication, many users have problems with the psychological acceptability of them due to the invasive nature of their enrollment (creation) and verification. For example, retinal scanning, while accurate, is an unpleasant and invasive technology most users and not willing to accept as part of their authentication paradigm. The biometrics that are more socially acceptable, such as fingerprints, also tend to be vulnerable to compromise and spoofing \cite{Espinoza2011}.

Once users have accepted inherence-based authentication, there are still further issues which complicate the use of biometrics. If a biometrics identifier becomes compromised, whether through accidental disclosure of the saved biometric data or deliberate attempts to forge the data, it is permanently compromised and cannot easily be renewed or revoked \cite{Jain2004}. While it is simple to renew a password, once a user's fingerprints are compromised, the user cannot be issued a new set (without a lot of inconvenience). Also, once the data has been collected, the storage and usage of the data raises privacy concerns as the data could be used in ways unintended by the owner of the biometric \cite{Pfleeger2003}. Not only is there a danger to the system using inherence authentication if a biometric can be compromised, but also the owner of the biometric may in fact be in danger themselves. While extreme, in the past, car thieves have cut off the finger of the car owner to get past sophisticated access control technology \cite{finger}.

The final authentication factor used in securing systems is ownership. This is based on items that the user owns, known as tokens. Typical authentication tokens include items such as an employee photo identification card or a smartcard (e.g., SecurID by RSA). The most prevalent vulnerability to this type of authentication factor is the item can be lost or even worse, stolen. It also places the onus on the user to ensure the token is always available when access is needed, which can often seem as an unnecessary burden by many users \cite{Paul2011}. Finally, if the authentication token is not electronic in nature, it must be verified by human verifier for validity.

While each factor has its own set of unique limitations, they also all share several common ones as well. While not specifically an inherent defect in any feature, the implementation and use of the authentication factors does not allow for easy, continuous mediation of access which is one of the greatest security weaknesses for insider threat. Finally, many cyber security systems are completely agnostic to the domain in which they are employed and do not account for things such as physical laws governing the people using the computing system. For example, while it may be reasonable for a user to access multiple systems in a sequential manner, it may be unwanted/illegitimate to allow simultaneous access by the same user in multiple, distributed locations depending on the application.

Addressing the Limitations of Multi-Factor Authentication

In order to address the discussed limitations of the three factors typically used for authentication, this paper proposes to utilize ``where you are'' (location) as a fourth authentication factor. While location has been previously proposed as a localized access control/authentication system (REFS NEEDED HERE), the necessary technologies capable of providing ubiquitous, continuous, and precise location monitoring of personnel have not been fully explored as a viable insider threat monitoring security tool. One potentially enabling branch of technology is that of Real Time Locating Systems (RTLSs). Typical RTLS system uses targets (sometimes called tags) attached to persons or objects that are being tracked and remote readers which receive remote signals from these tags to determine the location of the racked object \cite{rtls}. A high-level pictorial example of a location system used for providing a fourth authentication factor is displayed in \reffig{fig: 4factor}. Location based on accurate RTLSs has several attractive potential qualities in that the systems can provide continuous target tracking with minimal end-user burden, they can force a once purely virtual threat to maintain a physical presence in order to conduct an attack, and they can be used to address the problem of malicious insiders.

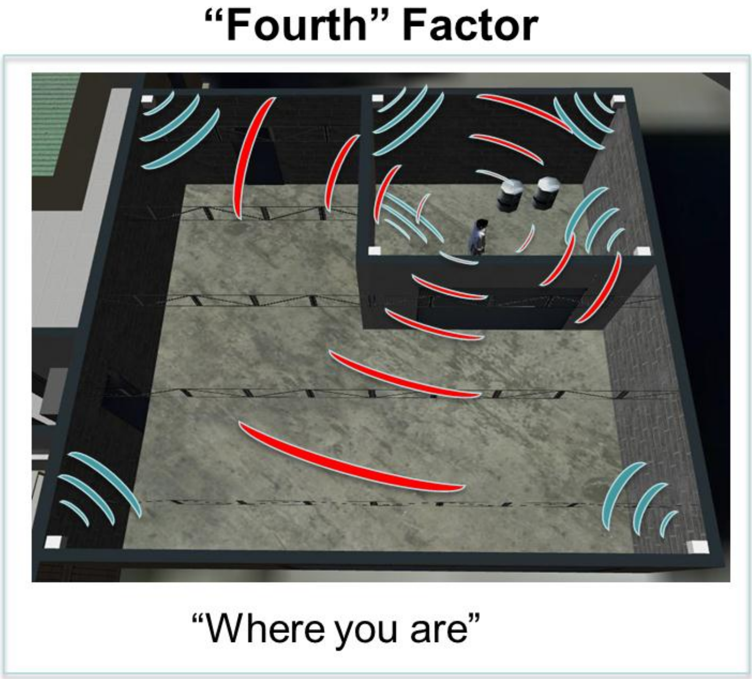

Figure 2

Enabling the Fourth Factor

Currently, there are various RTLS vendors and products available to track devices and personnel (e.g., RFID, IR, Wi-Fi, UWB, ultrasound, sound, MEMS, magnetometer, Inertial Measurement Units (IMUs)) that could potentially be used to create a fourth authentication factor based on location. The primary application of RTLS has been as a local positioning system that can track and identify the location of objects in real time. A comprehensive survey comparing the trade-offs among numerous RTLS technologies and vendor products from the viewpoint of a user for personal tracking was published by Gu et al. \cite{Gu2009}. The survey compares the different solutions based on the evaluation criteria of cost, performance, robustness, and privacy. This paper is not intended to replicate or extend such surveys, but rather focuses on deriving criteria for RTLS technologies that can be used as a fourth authentication factor and leveraged in an iTPS. The precision, frequency, and integrity of RTLS information has not been analysed against the persistent tracking needs of neither security applications nor as navigational or manoeuvring tools.

RTLS technologies can be broken down into measuring four general types of physical phenomenon: 1) electromagnetic waves, 2) sound waves, 3) the Earth’s magnetic field, and 4) IMU-based measurements of velocity, orientation, and gravitational forces. With the exception of IMUs and magnetic fields, location calculations are typically based on measuring one or more of the following attributes of waves (i.e., electromagnetic or sound): received signal strength (RSS), angle of arrival (AOA) and time of arrival (TOA). Furthermore, these technologies are deployed using two distinct methods: self-positioning and infrastructure-based positioning. In the self-positioning system, the targets themselves will gather location information from the surrounding environment or the deployed location infrastructure. For infrastructure positioning, the infrastructure will sense the mobile target and provide the estimation of the target’s location.

By leveraging such RTLS technologies, there is the potential that “where you are” can be used as a fourth factor authentication. This is contingent on the technology and process used with the factor satisfying the 3 rules of the authentication process posited below[1]. The three rules of authentication are as follows:

First Rule: Unless required by established security policies or safety rules, authentication may not hinder operational tasks at hand nor be cost prohibitive.

Second Rule: Unless it violates the First Rule, the integrity of authenticated data must be persistent and available throughout the authenticated state.

Third Rule: Authentication may not violate the laws of physics

A. A person cannot be in two different places at the same time
B. There is a limit to how fast a person can move through space and time
C. A person's identity may not be interchanged

These rules will allow for the generation of the requirements for an operational fourth factor authentication system that will culminate in design of an iTPS system. Additionally, the rules will aid in the evaluation of the applicability of current RTLS technologies in providing a fourth authentication factor.

General Design Traits of a Four Factor Authentication System

This section of the paper looks at applying the Rules of Authentication to define the necessary traits that are needed a viable fourth factor for authentication. The First Rule defines that a RTLS is most likely the best solution that can be used without significantly impacting the end-users with frequent requests for authentication. Most RTLS solutions require the person being tracked carry with them a tag that can act as a receiver or a broadcaster of location information. End-users can remain oblivious of the continuous authentication process simply by carrying RTLS tags that can identify itself on behalf of the end-user. Additionally, the tags cannot be too large, too heavy, too expensive, or require excessive maintenance (e.g., changing batteries every week) as any of these would violate the First Rule; authentication may not hinder operational tasks at hand. The First Rule also states that authentication solution cannot be too costly or goes against the institutionalized security policies or safety rules. If the security solution is too invasive, users will have a strong motivation for bypassing the system. The First Rule of Authentication provides us with the following solution criteria:

- RTLS tags must be portable:
  - small and light form factor
  - long battery life
- RTLS solution must be non-invasive, retaining the respect for and need for privacy (Hall, Edward, The Hidden Dimension, 1966)
  - Personal tracking must have accuracy of less than 1.0 foot

Using the Second Rule (while still considering the First Rule) of Authentication, the RTLS solution architecture (self-positioning versus infrastructure-based positioning) must be scalable. The standard Global Positioning System (GPS) application is the ultimate form of distributed, scalable positioning system that uses self-positioning architecture. Geo-stationary GPS satellites are made to broadcast their identity information down to earth and the GPS receivers listen in on the GPS signal and trilaterate their location based on the TOA. This architecture allows for an unlimited number of GPS receivers with a limited number of positioning beacons. Infrastructure-based architectures rely on infrastructure sensors

[1] Inspiration for the rules was drawn from "Three Laws of Robotics" by Isaac Asimov

to detect the motion of broadcasting tags. As long as the tags are minimal in number and broadcasting attempts, infrastructure sensors will be able to estimate the target location. Since broadcasting tags must continuously announce their ID for sensors to interpret the location information, the portable tags require much more power. Also, each tag signal can be intercepted and rebroadcasted with false information, opening up potential attack vectors for sophisticated adversaries to compromise the integrity of the authenticated data (a violation of the Second Rule). It is important to remember that there is a direct correlation with the number of sensors required and the number of supportable tags. Because of the aforementioned limitations, infrastructure locating architectures are physically un-scalable and potentially insecure for enabling four factor authentication. The following solution criteria can be inferred from the Second Rule of Authentication:

- RTLS Architecture
    - Must be scalable (self-positioning design)
    - Solution must be cost effective
    - Solution must accommodate malicious insider

The Third Rule of Authentication has the most impact on the down selection process among the RTLS technologies with very interesting security and privacy implications. Insiders, by definition, are given the access privileges to a facility because of their trustworthiness. However, a very small percentage of these individuals will intentionally or unintentionally violate the policy by detaching the tags from their body. Malicious insiders may secretly exchange tags with the hope of gaining special privileges. In order to preserve the integrity of an identity, these tags must be designed with some sort of "ephemeral biometrics" technique that can link an identity with an issued RTLS tag. This may be achieved by designing the RTLS tags with wristlock form factor, using impedance/capacitance to continuously monitor for the integrity of tag and identity. In order to enforce the time and space limitations, the RTLS solution must have the capability to check locations every at 2 to 3 second intervals. If a person's location jumps from one building one to another in a matter of seconds, the Third Rule has been violated and security should be notified. RTLS tracking resolution must be less than 1 feet to preserve the tracking of the individual identities. The Third Rule thus yields the following solution criteria:

- RTLS security requirements:
    - Need for ephemeral biometric technology
    - Capable of less than 1 foot location resolution
    - Position checked every 2 to 3 second intervals

iTPS Technology Assessment

As discussed above, RTLS technologies primarily utilize measuring four general types of physical phenomenon: 1) electromagnetic waves, 2) sound, 3) Earth's magnetic field, 4) IMUs. If the location information is to be used as a security tool for monitoring and tracking an individual, technologies must be accurate and robust to malicious insider. There have been several surveys of Indoor Positioning Systems that included common evaluation criteria on performance, robustness, accuracy and cost that are largely consistent \cite{Gu2009,Liu2007}. In this section, this paper utilizes the surveys and technology evaluations to draw conclusions on how certain technologies match up to the technical and design requirements that have been derived out of the Three Rules of Authentication for creating ``where you are'' as a fourth authentication factor. ion.

Magnetometer and IMUs

Although it is important to utilize the technologies that are capable of producing high position accuracy (i.e., under 1 foot), for the position information to be used as the fourth factor authentication, it is just as important to utilize a solution that can retain the integrity of position information throughout the authenticated state (see Second Rule of Authentication). For example, recent advances in Micro-Electro-Mechanical Systems (MEMS), gave rise to magnetometers, electronic gyroscopes, and IMUs that are capable of generating highly accurate positioning systems. Some vendors, like IndoorAtlas, utilizes the built-in magnetometers of smartphones to measure and compare the magnetic field of the Earth with the a priori location fingerprints of the Earth, accurate to a 0.1 meter resolution. Despite this accuracy, magnetic fields are highly susceptible to external variables such as the presence of metal, electronic devices, running motors, piping in the building, necklaces people wear, etc. Malicious insider can easily utilize these external variables to tamper with the field measurements to compromise the integrity of the positioning information.

IMUs, on the other hand, are largely impervious to external influences for tracking motion. This technology is designed to detect changes in the inertia of an object, such as rotation or acceleration of the object, making it appear to be a perfect candidate for addressing the malicious insider threat. However, even when the device is completely stationary, given enough time, an IMU will report drifting from its original position (REFS NEEDED HERE). In other words, it violates the Second Rule of Authentication by self-compromising the integrity of authenticated data. IMUs will also require having individuals follow very precise location initialization procedures which goes against the First Rule of Authentication.

Electromagnetic and Sound Waves

For indoor positioning systems, electromagnetic waves are by far the most abundant and available solution in the market. Many of the mobile electronic devices that people carry around and the communication infrastructure supporting these devices are based on electromagnetic (EM) waves: GPS, RFID, IR, WLAN, Bluetooth, UWB, Cellular based, environmental fingerprinting, etc.

With the exception of environmental fingerprinting, the following trilateration techniques are being utilized for EM waves: Time of Flight / Time of Arrival (TOF/TOA), Time Difference of Arrival (TDOA), Roundtrip Time of Flight (RTOF), Received Signal Strength (RSS), Angle of Arrival (AOA), Phase of Arrival (POA). Although sound waves have not been fully utilized like EM waves and there are a limited number of vendor products specializing in using sound wave for RTLS, it is theoretically possible that sound waves can utilize all the trilateration techniques that EM waves utilize.

Among the surveyed EM wave products, only UWB has the accuracy range satisfying the less than one foot accuracy criteria. Furthermore, technical criteria derived out of the Third Rule of Authentication states that the position information should be checked on 2 to 3 second intervals. This is a demanding system requirement that implies the RTLS will need to function normally even when some signals are not available. Unfortunately, for EM solutions, most require line-of-sight and the indoor propagation is full of obstructions and reflective multipath surfaces. Because of the speed of light, it is extremely difficult to use TOA for trilateration. Both the transmitters and receivers in the system have to be precisely synchronized and a timestamp must be available in the transmitting signal in order for the measuring unit to calculate the distance the EM wave has travelled. In other words, signal processing clock cycle has to be at nanosecond resolution or better to distinguish the TOA for distance calculation. These are some of the technical difficulties that pushed EM wave solutions to rely on estimating position based on RSS techniques. However, because RSS technique does not accommodate dynamic environmental obstructions and reflective multipath issues, the accuracy suffers as clearly shown in \cite{Gu2009,Liu2007}.

The physics of sound waves and EM waves share similar attributes of wave form behaviours. There are three main characteristics of the sound waves that must be considered for RTLS solution: 1) speed of sound is many orders of magnitudes slower than the speed of light, 2) speed of sound will vary depends on the ambient temperature, 3) sound is highly localized. As the speed of sound waves is much slower than EM waves, measuring TOF/TOA is a much easier task then trying to measure the speed of light. The challenges of synchronizing time between sound sources and sinks also becomes a much easier task technically in the sound medium then in light.

For sound, future advances in trilateration techniques should focus on measuring TOF/TOA instead of the RSS techniques that EM wave have been using to estimate the location. The main difference between TOF/TO versus RSS technique is that in TOF/TOA, the measurements are taken as face value to calculate the position information while in RSS technique, because it is design to measure relative amplitude/intensity of wave, the trilateration is going to be best guess estimate. RSS techniques are more susceptible to breaking the Second Rule of Authentication by providing a best estimate instead of the exact calculation based on direct measurements of TOF/TOA. One interesting difference between the sound and EM is that while the speed of light is the more or less the same, the speed of sound varies depending on temperature, pressure, humidity, density of fluid/gas, composition of air molecules \cite{Bohn1988}. While the formula for the speed of sound considering all of these potential variables can get become complex; in most settings, it is simply the following function:

$$Vs = 331.45 * \mathrm{Sqrt}(1+Tc/273.15)$$

where Tc is the temperature of dry air in Celsius.

When measuring TOF/TOA of sound, local ambient temperature must be incorporated into the velocity of sound measurement and adds additional technical difficulties that EM waves does not have to deal with. Sound waves can be broken down into following three ranges for human hearing: infrasound (<20 Hz), hearing range (20 Hz to 20 Khz), ultrasound (> 20Khz). Using sound signals for trilaterate, the ideal frequency range to use is ultrasound since this range is beyond normal human hearing. Sound signals must be inaudible to human ears if the solution is to satisfy the First Rule of Authentication. However, for ultrasound, the signal range becomes a challenge since ultrasound waves are very quickly dissipated in the air due to their high frequencies. Research on the distance ultrasound signals will travel in air is unclear as of yet. SonicNotify, a startup company, has claimed that their ultrasonic signals can be ``heard'' as far as 225ft away by increasing the gain output of piezoelectric ultrasonic speaker. Since ultrasounds are not FCC controlled signal medium, amplitudes of the signal can be determined on a needs basis. Because of high dampening factor of ultrasound, the signals will be highly localized and will not seep through the walls.

RTLS Built on Measuring Multiple Physical Phenomena

As alluded to in the EM and Sound wave discussion, many of the available vendor products utilize single technologies to calibrate location information. For outdoor environment where obstacles are few and sparse (i.e., GPS), using a single signal form factor for trilateration may be sufficient. However, indoor environments are full of challenging dynamic obstacles (including potential malicious insiders) that will break the continuity of location sensing and broadcasting pathways. In addition to solving these very difficult technical challenges, additional technical constraints from Three Rules of Authentication (e.g., high precision, accuracy, high frequency and robustness) must be considered. Because of these reasons, an application of any single layer technology will be insufficient to satisfy iTPS performance requirements. It is possible that by combining multiple sensors, the performance and robustness RTLS capabilities can greatly be enhanced. For example, with a combined RF/ultrasound package, if the sound source becomes unavailable due to unanticipated signal blockage, RF signals can be used as backup to pick up where sound left off. One can also use a combination of ultrasound with that of ambient sound. Ultrasound does not travel around the corners while audible sound does. By digitally hiding audible sounds in the ambient noise (ventilation, or vibrating florescent light bulbs), when ultrasound becomes unavailable, hidden audible sound may be utilized. If the ultrasonic beacons are to be used for trilateration, both the receiver and the beacons must be synchronized to measure the TOA. Since RF signals are instantaneous compared to the sound, RF signals can be used as clocking signal for the TOA.

Application of Fourth Factor Authentication

An insider Threat Prevention System (iTPS) is an application concept designed to address the insider threat through the use of RTLS technologies for tracking materials and personals. Using the continuous surveillance capabilities of RTLS and "where you are" as a fourth factor authentication, a technical solution is proposed to address both the insider threat and the physical-cyber security issues. iTPS can be used not only to monitor the mobility of personnel but it can also be used as access control to buildings, computers and network access. A proper security policies based on location can be incorporated into network and computing resources. iTPS, is a first-of-its-kind technical tool designed to monitor insider movements and critical assets simultaneously. A list of possible iTPS applications is included below:

- Track personnel and high consequence assets in the field
- Enhanced access control based on location (fourth factor authentication tool)
- Provides inspectors with near real-time material and personnel monitoring and accounting capabilities – chain of custody program
- Automate and enforce security policies based on location proximity
- Supplement emergency preparedness and safety
- Deliver automated location/facility guidance system

iTPS scenarios

- Jack has iTPS tag on his wrist. He sits down in front of his computer creating and sending emails. He gets up to get a drink of water without locking his screen. Diablo the prankster then comes in to Jack's office and tries to send email to Jack saying "You have been hacked. Please lock your screen before walking away from your computer." iTPS system will recognize that Jack is not the one trying to send the email and tells Jack's computer not to accept any commands coming from Jack's keyboard.
- Jack, against company policy, downloads PCAnywhere into his company desktop so he can access files and folders from his home. Jack goes home and uses VPN connection to activate PCAnywhere. iTPS will first look for the "physical location" info for Jack, does not find him anywhere in the local facility. Command to activate PCAnywhere is then rejected.
- Jack walks into his office, turns on the computer and the iTPS recognizes that Peter has legitimate privileged access to his computer and automatically enters 250 character password for Jack.
- Jack happens to have his LDRD iPad which have been approved for use in the restricted area. iTPS technologies are integrated into this iPad. iTPS will tell the iPad that it is in the approved/restricted area and allows Jack to use it the instant he pushes the "On" button. Jack takes this iPad to Walmart and leaves iPad visible on the passenger chair. Bad guy breaks in and steals the iPad. He tries to turn on but iPad doesn't get any iTPS signal. It does not allow information access to iPad but it reports its location and potential theft warning to Jack's mobile phone with GPS location information.
- Using iTPS, one can also enforce 2 man rule to access top secrete computers.

- Accounting and tracking employee safety for scenarios such as the routine fire drill practice or emergency evacuation

Conclusion

The traditional factors of authentication whether used in isolation or combinations, have authentication deficiencies, particularly in dealing with insider threats. Three Rules of Authentication have been posited in order to help analyse current authentication systems and the technologies that enable these systems. By utilizing “where you are” as fourth factor for authentication, shortfalls of the traditional three factors (insider threat, remote attack vector, end-user convenience) authentication can have been addressed. Using the Three Rules, attributes of four factor authentication were derived. These attributes were then used to evaluate existing indoor positioning technologies as possible candidate for providing location, with the goal of using them in an iTPS solution. Unfortunately, the existing products all had violations of the Three Rules of Authentication, pointing out the need future work in the RTLS arena. In order for RTLS solution to function as part of a reliable iTPS application, the solution space must be explored by merging multiple location sensing technologies to enhance the accuracy, robustness, and portability of RTLS solution. Once these technical hurdles are overcome, iTPSs have the potential to radically change the physical protection systems and cybersecurity landscape by providing institutions with the first-of-its-kind tool for real-time insider-threat prevention capabilities.