Enhancing the Trust of Location Acquisition Systems for Critical Applications and Location-Based Security Services

[1]Chris Wullems, [2]Oscar Pozzobon, [1]Mark Looi, and [2]Kurt Kubik.

[1]Information Security Research Centre
Queensland University of Technology,
Brisbane, QLD 4000, Australia
Email: {c.wullems, m.looi}@qut.edu.au

[2]School of Information Technology & Electrical Engineering
The University of Queensland,
Brisbane, QLD 4072, Australia
Email: {pozzobon, kubik}@itee.uq.edu.au

ABSTRACT

This paper identifies a number of critical infrastructure applications that are reliant on location services from cooperative location technologies such as GPS and GSM. We show that these location technologies can be represented in a general location model, such that the model components can be used for vulnerability analysis. We perform a vulnerability analysis on these components of GSM and GPS location systems as well as a number of augmentations to these systems.

Keywords: Location, Security, Critical Infrastructure, Vulnerability Analysis, Trust, GPS, GSM, SBAS, GBAS

INTRODUCTION

The requirement for Critical Infrastructure Protection (CIP) has received much attention recently due to many government security initiatives. The national critical infrastructure spans across many sectors of the economy including finance and banking, transportation, telecommunications and information technology, energy, utilities, health, manufacturing, and emergency and other key government services such as defence and law enforcement. The abundance of security vulnerabilities in the national critical infrastructure has become increasingly apparent in recent years, prompting research efforts to investigate these vulnerabilities.

This paper focuses on sectors of the critical infrastructure reliant on location services from cooperative location technologies such as GPS and GSM. Security issues that can affect the survivability and recovery of critical systems from attacks directed at these technologies are identified. This paper is specifically focused at intentional disruption, not unintentional disruption such as those caused by environmental affects. We propose a number of models that generalize location systems for the purpose of identifying the components of these models where security vulnerabilities can occur. These components of a candidate technologies are analysed for vulnerabilities, demonstrating that other location technologies can be analysed using this technique.

This paper will provide a set of building blocks that can be used for assessing and mitigating the risk of using both current and emerging location acquisition technologies in critical applications.

LOCATION SERVICES IN CRITICAL INFORMATION INFRASTRUCTURE

Homeland security initiatives have resulted in many efforts to use GPS and cellular technology for security applications including tracking. In addition, it has become apparent that many existing services are dependent on GPS and cellular networks from both defence and civil sectors. While there are a number of military technologies that significantly improve the robustness and survivability of attacks against these location services, it is not likely that they will be made available to the civil sector. As such, this paper only considers civil uses of location technologies and does not discuss military location technologies or augmentations.

The following non-exhaustive list of location services in critical infrastructure:

- **Vehicle tracking:** Vehicle tracking can be pertinent to critical infrastructure where there is the need track vehicles carrying hazardous substances including chemicals, fuel and radioactive waste, and collection of taxes for tolls;
- **Personal tracking / emergency response:** Particularly relevant to the USA, where the E911 requirements have resulted in cell phones with an imbedded GPS functionality;
- **Electronic Commerce:** An emerging trend can be seen in the use of location for electronic commerce. An example is a small hardware device called a TAD (Transaction Authentication Device) developed by WorldPay (WorldPay, 2001), using an embedded GPS chip to determine the location of where a transaction is initiated. This device is used for identifying the parties involved in large commercial Internet transactions. The integration of GPS receivers in cell phones as part of the E911 requirements will inevitably result in the widespread use of location for identification and security in M-commerce applications.
- **Control applications:** There are many uses of location for control applications including the following transport sector applications identified by (Volpe, 2001):
    1. Railway traffic control and monitoring;
    2. Aviation systems including civil monitoring and landing system augmentations for precision and non-precision approaches; and
    3. Marine systems including harbour approach and constricted waterways control.
- **Access control / auditing:** Location can be used for the enhancement of access control and auditing. There are many applications where location context information can supplement existing security, assuming the location acquired can be trusted; and
- **Time synchronization:** There are numerous critical applications that rely of location technologies such as GPS for time synchronization. Such applications include:
    1. Timing and synchronization of communication networks;
    2. Authentication and access control, e.g. RSA SecureID, Kerberos, etc. using time synchronization protocols such as Network Time Protocol (NTP);
    3. Secure document timestamps (with cryptographic certification);

Because of the widespread use of location for critical services, it is imperative that the location systems provide availability, integrity and trust.

RELATED WORK

Historically, military and civilian development of location technologies has been segregated. While much effort has been focused towards security of location in military applications, there has been little research to date in the development of secure and survivabe location systems and augmentations for use in critical civilian applications.

The first GPS-based location authentication system was developed by (Denning & MacDoran, 1996), the "Cyber Locator", using a patented method of location determination (MacDoran, 1998) to provide assurance of location integrity. This system uses raw GPS signals to derive a location signature, where both the client and server have the same view of satellites. (MacDoran, 1998) states "The security afforded by the invention is actually enhanced by the limitations placed on the broadcast GPS signals known as Selective Availability (SA)…".

Before May 1, 2000 the Selective availability policy was degrading the satellite pseudo ranging signals by dithering the navigation data and introducing an error in the clock (The Epsilon bias component), resulting in an approximate position calculation. For this reason it was improbable to predict the pseudo range and consequently the proposed location signature (LSS). After May 1, 2000 Selective availability was no longer active. The only variation in the signal is due to atmospheric and ionospheric affects that have very few variations and do not change within hundreds kilometres. As such, we do not consider this architecture in this analysis.

There have been numerous proposals for location stacks and frameworks for the use of location data transparently using different technologies with a common coordinate system. Recent proposals, (Hightower, Brumitt, & Borriello, 2002) and (Lara, 2003) do not provide a mechanism for qualifying assurance or trust of acquired location results. As such, existing location frameworks are not suitable for critical or security-based applications.

GENERALIZED MODEL FOR VULNERABILITY ASSESSMENT OF LOCATION SYSTEMS

The crucial elements of location systems, common to all location systems are detailed in terms of a number of generalized models, thus enabling us to focus on the vulnerabilities of these models.

We define a location system to be composed of the following components:

- **Location infrastructure**: The supporting architecture except the mobile device;
- **Location device**: The device whose location is estimated;
- **Signaling:** The signals that the infrastructure or location devices observe for the purpose of calculating location;
- **Observation:** The method utilized to measure the location from the signaling;
- **Calculation:** The computation of the position using the observation measurement;
- **Communication:** The transfer of observations and calculations between the infrastructure and device, and the transfer of location data results to the application; and
- **Application:** The system that will request / receive the location data.

In the following sections, we show that common location technologies can be generalized to the following four location acquisition models. In addition, we apply a general augmentation model to augmentation systems of these location technologies.

LOCATION DEVICE OBSERVED AND CALCULATED MODEL

This model, as illustrated in Figure 1, generalizes location systems where the location is both observed and calculated by the location device. In this model, the location device communicates the calculated location result, or other data such as time, to the location application.

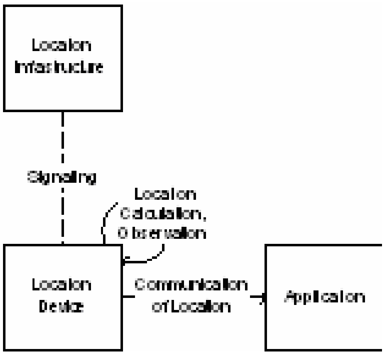

Figure 1: Location device observed and calculated

The following technologies correspond with the location device observed and calculated model.

Global Positioning System (GPS)

GPS corresponds to the Location device observed and calculated model, as illustrated in Figure 1. The GPS Infrastructure consists of 24 satellites that each transmit two bands, the L1 (1575.42 MHz) frequency and the L2 (1227.60 MHz). The signalling is broadcasted on the L1 band in two channels, a narrowband channel occupied by the C/A code and a wideband channel that is intended for precision measurements with the classified P(Y) code. The L2 band contains only the P(Y) codes and serves mainly to act as an ionospheric effects calibrator for the L1 band. (Hoffmann-Wellenhof, B.H.Lichtenegger, & J.Collins, 1994) The GPS receiver (location device) measures its distance from the satellite's by determining the time of arrival (TOA) in the so called "pseudo-range acquisition", from which it calculates its position. The receiver typically communicates the location data to an application though a serial communications interface.

Global System for Mobile Communication (GSM) – Enhanced Observed Time Difference (E-OTD)

GSM is a cellular network technology providing second generation voice and data services. As location is inherent in the operation of GSM signalling, a cell phone's location can be calculated using a number of location methods based on signal timing. There are two types of E-OTD based on different measurements and calculation methods (ETSI, 2000b):

1. **Hyperbolic Type:** This type of calculation requires the MS (Mobile Station) observe the OTD (Observed Time Difference) of signal bursts from different Base Transceiver Stations (BTS). This information is used in combination with the relative synchronization difference of the BTSs to for hyperbolic trilateration of 3 geographically separate BTSs.
2. **Circular Type:** This type of location calculation requires the MS observe the time (MOT) at which signal bursts from BTSs arrive at the MS using its internal clock. Based on the observed time at which the same bursts arrive at a Location Measurement Unit (LMU), the MS clock can be synchronized and hence provide Time of Arrival (TOA) measurements for circular trilateration.

E-OTD can operate in two modes. One of these modes corresponds to the location device observed and calculated model. The MS is able to calculate the location based on assistance data provided by the location infrastructure. Rather than a location request being initiated by an LCS client, the MS performs the calculation and can provide the result to an application via a proprietary interface on the MS and a communications link between the MS and an application.

GSM - Assisted GPS (A-GPS)

There are two methods of GSM assisted GPS. The method corresponding with this model provides assistance data to cell phone-embedded GPS receivers using the GSM infrastructure. In this model, the MS contains a fully functional GPS receiver. The MS location is calculated by the MS, and can be sent to the destination application via a proprietary communications interface.

LOCATION INFRASTRUCTURE OBSERVED AND CALCULATED

This model, as illustrated in Figure 2, generalizes location systems where the location is both observed and calculated by the location infrastructure. In this model, the location infrastructure communicates the calculated location result to the location application.

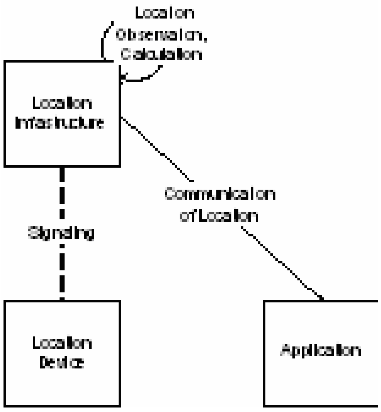

Figure 2: Location infrastructure observed and calculated

The following technologies correspond to the location infrastructure observed and calculated model.

GSM - Timing Advance (TA)

Timing Advance-based location acquisition is specific to GSM, where the round trip propagation delay is measured by the Base Transceiver Station (BTS) as part of the Time Division Multiple Access (TDMA) adaptive frame alignment process for ensuring a Mobile Station (MS) transmits in the correct time slot. The TA is observed by the BTS in the GSM location infrastructure and may be used to calculate the location in the infrastructure or MS. In the method of obtaining the TA that complies with this model, the application (an authorized LCS client) makes a request to the Gateway Mobile Location Centre (GMLC). The cell-ID and TA are obtained by the Serving Mobile Location Centre (SMLC) where the MLC-PCF (Positioning Calculation Function) calculates the position based on knowledge of the serving BTS coordinates.(ETSI, 2000b) The calculated location is returned via the GMLC to the application.

GSM - Time of Arrival (TOA)

The TOA is observed by the GSM location infrastructure and may be used to calculate the MS position in the location infrastructure. The application (an authorized LCS client) makes a location request to the Gateway Mobile Location Centre (GMLC). The cell-ID, TOA values and TOA measurement quality are obtained by the Serving Mobile Location Centre (SMLC), where the Positioning Calculation Function (MLC-PCF) calculates the position of the MS based on knowledge of the Real Time Differences (RTD) and the Location Measurement Unit (LMU) coordinates.(ETSI, 2000b) The calculated location is returned via the GMLC to the application.

LOCATION DEVICE OBSERVED, LOCATION INFRASTRUCTURE CALCULATED MODEL

This model as illustrated in Figure 3, generalizes location systems where the location is observed by the location device, communicated to the location infrastructure, and calculated by the location infrastructure. In this model, the location infrastructure communicates the calculated location result to the location application. The following technologies correspond to this model.

GSM – A-GPS

There are two methods of GSM assisted GPS. In this method, MS-Assisted GPS, only minimal GPS receiver functionality is provided at the Mobile Station (MS) and the majority of the GPS functionality is supported by the network infrastructure in order to save power and reduce computational complexity. As defined in (ETSI, 2000b), the MS (location device) makes GPS measurements aided by assistance data transmitted by the network which facilitate significantly faster GPS acquisition times. The measurements are sent to the network infrastructure, where the Serving Mobile Location Centre (SMLC) calculates the position of the MS.

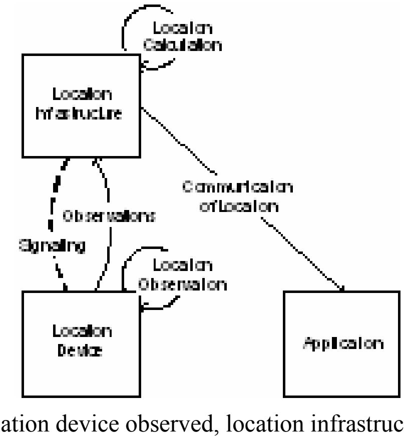

Figure 3: Location device observed, location infrastructure calculated

GSM – E-OTD

There are two methods of E-OTD location acquisition. In this method, the application (an authorized LCS client) makes a location request to the Gateway Mobile Location Centre (GMLC). For hyperbolic calculation, the Serving Mobile Location Centre (SMLC) obtains E-OTD measurements from the MS the where the MLC Positioning Calculation Function (MLC-PCF) calculates the position of the MS using its knowledge of Real Time Differences (RTD) , the BTS coordinates and other supplementary data. For the circular calculation, the SMLC obtains the Mobile Observed Time (MOT) from the MS, the Location Measurement Unit (LMU) TOA measurements and other supplementary data and calculates the position using the MLC-PCF.(ETSI, 2000b) The calculated location if returned via the GMLC to the application.

LOCATION INFRASTRUCTURE OBSERVED, LOCATION DEVICE CALCULATED MODEL

This model as illustrated in Figure 4, generalizes location systems where the location is observed by the location infrastructure, communicated to the location device, and calculated by the location device. In this model, the location device communicates the calculated location result to the location application.

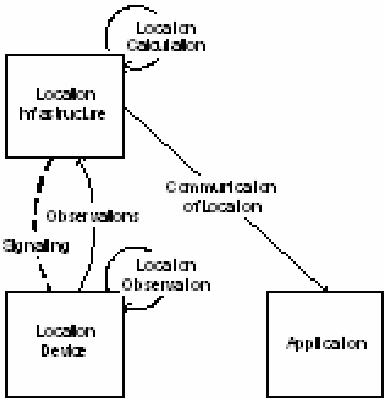

Figure 4: Location infrastructure observed, location device calculated

This model is shown for completeness. While there are no standardized location methods for this model, an example of this model can be shown in GSM. The infrastructure observed measurement of the Timing Advance (TA) is communicated to the MS in layer 3 messages for adaptive frame alignment. The MS could calculate its location based on the coordinates of the BTS of the active cell. The coordinates could conceivably be sent via cell broadcast messages to the MS.

ASSISTANCE DATA AUGMENTATION MODEL

Assistance data can be augmented with basic location devices as shown in Figure 5, to provide better location accuracy. This model generalizes two modes of assistance data augmentation:

- **Mode 1:** Assistance data is communicated to the location infrastructure. In this model, the location infrastructure performs the corrections based on the assistance data received from the 3rd party observer. An example of this mode can be seen in GSM MS-Assisted GPS.
- **Mode 2:** Assistance data is communicated to the location device. In this model the location device performs the corrections based on the assistance data received from the 3rd party observer. It is also feasible that assistance data is communicated through the infrastructure to the location device as in a number of location acquisition methods in GSM. An example of this mode is a GPS receiver that applies corrections received from a satellite-based augmentation system such as EGNOS.

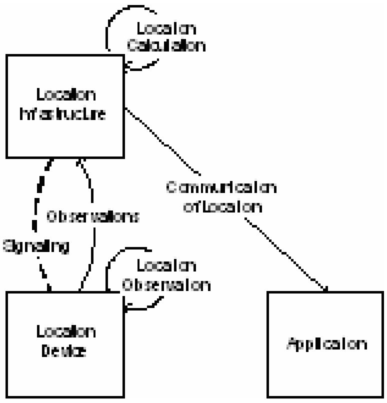

Figure 5: Assistance data model

The following augmentation technologies correspond to this model.

Augmented GPS Positioning

Differential GPS (D-GPS) is a type of GPS augmentation system. D-GPS versions can be shown in terms of this model, where position corrections and integrity information are derived from observations at one or more monitoring stations (3rd party) at known locations. As the 3rd party in this case is another GPS receiver, the 3rd party can be modelled by the location device observed and calculated model. The correction information from the 3rd party is then broadcast to the user location device or an application for improvement of its location calculation. This broadcast corresponds to the (mode-2) communication of assistance data depicted in this model.

Ground and space-based augmentation systems can also be shown in terms of this model. The information from the monitoring stations (3rd parties) is signalled to a master control station (infrastructure), as depicted by the first part of communication of (mode-1) data. The control station pre-processes the information in order to compress data to reduce data rate and to improve data consistency, then signals this processed information to the user location device. The signalling for the various functions may be either ground based (GBAS) or space based (SBAS). The latter usually allows the service to cover wide areas of service and use a standard protocol (RTCA). Examples of these satellite services are the American Wide Area Augmentation Service (WAAS), the European Geostationary Navigation Overlay System (EGNOS), the Japanese Multifunctional Transport Satellite Augmentation Systems (MSAS), the planned Indian GPS and Geostationary Augmented Navigation (GAGAN) and a number of commercial services such as OmniSTAR. Examples of GBASs are the Australian GRAS system as proposed by Air Services Australia(Crosby et al., 2000), the future VICNET of the State of Victoria, and Trimble's virtual base station network.

GSM - Broadcasted Assistance Data

GSM augments its A-GPS and E-OTD location systems using assistance data broadcast to the MS via the Cell Broadcast Channel (CBCH) and Short Message Service Cell Broadcast (SMSCB) (ETSI, 2000b). The Serving Mobile Location Centre (SMLC) creates a LCS broadcast message containing the assistance data to be broadcasted as well as parameters indicating the target BTS and the time at which it is to be broadcasted (ETSI, 2000a). The assistance data is obtained from various sources from within the infrastructure and communicated to the SMLC. This communication can be represented by the first (mode-1) communication from the 3rd party to the infrastructure (SMLC). On receipt of the message, the SMLC sends the message to Cell Broadcast Centre (CBC). The CBC transfers message to BTS, and from the BTS to the MS as detailed in (ETSI, 2000c). This communication can be represented by the second (mode-1) communication from the location infrastructure (CBC/BTS) to the location device (MS).

VULNERABILITIES IN LOCATION SYSTEMS

For the analysis of vulnerabilities, we make use of evaluation levels to assess the ability of location system components to withstand direct attack. All the components derived from the generalized model are assumed to be security critical components, (i.e. those mechanisms whose failure would create a security weakness) and therefore must be assessed for each technology. The strength of each component of a location system shall be rated high risk, medium risk or improbable as follows:

1. **High Risk:** Attacks require few resources and could be performed by knowledgeable attackers;
2. **Medium Risk:** Attacks require moderate resources and could be performed by highly motivated attackers; and
3. **Improbable:** Attacks require significant resources and could be performed by attackers possessing a high level of expertise, where successful attacks are judged to be beyond normal practicality.

If the location system has vulnerabilities in its components, the location system's rating will be based on the component with the lowest rating. The generalized models discussed in section 4 can be reduced into four primitives for the purpose of vulnerability assessment.

1. Location infrastructure;
2. Location devices;
3. Signalling; and
4. Communications.

Observations and calculations are operations that are embedded within location devices or infrastructure. As such, these operations are omitted from the above primitives. This is because vulnerabilities in either location devices or infrastructure result in vulnerable observations and calculations. In addition, applications are not included in these primitives, as applications are assumed to be trusted and this paper is not concerned with the privacy of acquired location. The following subsections outline the vulnerabilities for the location technologies discussed in the generalized models in terms of the above primitives.

Location Infrastructure

The attacks that have been identified as most critical to location infrastructure are:

1. **Physical Disruption:** This includes physical attacks such as removal of power, physical damage, unauthorized access, hacking, theft, etc.; and
2. **Tampering:** This includes attacks on observation and calculation functions performed within the infrastructure, etc.

It is assumed that location infrastructure is managed by telecommunications companies and government, and is physically secure. In addition there can be a higher level of trust placed on the operations performed in the infrastructure due to the increased level of physical security present. Table 1 summarizes the vulnerabilities in the infrastructure.

	Disruption	Tampering
1. GPS	Improbable	Improbable
2. SBAS / GBAS	Medium	Improbable
3. GSM	Medium-High	Improbable

Table 1: Location Infrastructure Vulnerabilities

1. **GPS:** Physical disruption of a Satellite system is improbable due to the difficulty of accessing satellites in space. The GPS ground infrastructure is geographically distributed, making the feasibility of a physical attack on all control stations very improbable. While a physical attack on the satellites is improbable, it is stated in (Adams, 2001) that the US Space Command does not have an operational anti-satellite weapon. As such, it is feasible to attack the satellites using the methods detailed by (Adams, 2001). General Thomas Moorman is cited in (Caton, 1995) as identifying that current launch vehicles and their associated processes do not provide the responsiveness needed to rapidly replace or augment satellites. In addition, he states that the U.S launch infrastructure is vulnerable, inflexible and expensive. Tampering with the GPS infrastructure is also improbable due to the inaccessibility of satellites and the high security of monitoring station installations.

2. **SBAS / GBAS:** Physical disruption of space and ground-based augmentation systems are assumed to be a medium risk. This is because augmentation data is sourced from ground monitoring stations in both technologies. Where ground stations are distributed, an attack on a single ground station would result in a denial of service of augmentation data in the area it observes. Tampering with the SBAS/GBAS infrastructure is also improbable due to the inaccessibility of satellites for SBAS and the assumption that there is high level of security at the monitoring station installations for both SBAS and GBAS.
3. **GSM:** Physical disruption of GSM infrastructure is possible with medium to high risk, depending where the attack is performed. While Base Transceiver Stations (BTS) are quite vulnerable to physical disruption, the benefits of denial of service attacks against individual BTSs is limited due to the number and distributed nature of BTSs. If a Base Station Controller (BSC) is attacked, it will result in denial of service of all BTSs controlled by the BSC. An attack on a Mobile Services Switching Centre (MSC), will result in denial of service to associated BSCs, and intern the BTSs they control. Tampering with the GSM infrastructure depends on the physical security of the sites. The physical security of an MSC is considerably higher than that of a BSC, which typically has better physical security than a BTS. For tampering to be affective, it would require access to a BSC or MSC, presumably with moderate physical security. It is assumed that tampering is improbable; however this assumes adequate physical security in all components of the infrastructure.

The infrastructure of location systems used in critical applications should have a sufficient level of physical security to protect from the threats of tampering and disruption. Vulnerabilities in location infrastructure can be mitigated through the diversification of location acquisition technologies. While it is improbable that physical disruption will occur in satellite-based location infrastructure, diversification of technologies will increase survivability for critical applications reliant on accurate location. For example, the use of GPS-calibrated sensors to monitor location in addition to the standard use of GPS would result in survivability for medium outages of GPS.

Location Device

The attacks that have been identified as most critical to a location device's integrity and operation are:

- **Disassociation**: This is where the location device is physically removed and placed in an alternate location in order to cheat the system;
- **Cloning:** This is where a location device is duplicated undetected, such that an adversary's location is seen to be in the location of the device that was cloned;
- **Mafia Fraud:** This is where the device acts as a "Mafia agent" and relays all information between the participants in a communication exchange, causing misidentification for example. This attack requires the location device be compromised;
- **Disruption:** This includes attacks such as removal of power, blockage of antenna, physical damage, etc.; and
- **Tampering:** This type of attack could be performed on the device hardware or firmware causing the device to behave improperly.

It is assumed that a location device is not trusted, and as such operations performed in the device cannot be trusted. Table 2 summarizes the vulnerabilities in the location device.

	Disassociation	Cloning	Mafia Fraud	Disruption	Tampering
1. GPS Receiver	High	Not Relevant	Medium	High	High
2. SBAS / GBAS Receiver	High	Not Relevant	Medium	High	High
3. GSM MS	High	Medium	Improbable - Medium	High	High

Table 2: Location Device Vulnerabilities

1. **GPS Receiver:** Disassociation is a high risk, as the removal of the receiver from a ship for example, cannot easily be detected. The risk of cloning is found to be irrelevant, as GPS receivers do not have any methods of authenticating themselves to an application, and as such, cloning would not be beneficial. If the GPS receiver was uniquely identifiable, the risk of

cloning would be classified as high risk unless mitigated with some form of tamper-resistant module (e.g. smartcard), where cloning of the receiver's identity would be intractable. Mafia fraud attacks are medium risk, as a receiver must be compromised and must cooperate with another device with a communications path that can be intercepted. There is a potentially high risk for disruption of GPS devices by removing the power supply or physically damaging the unit. An attack based on tampering with the receiver is also high risk, as the device is not typically physically secure, and there are no standardized mechanisms to authenticate the firmware integrity to an application.

2. **SBAS / GBAS Receiver:** An SBAS / GBAS receiver is typically integrated into or attached to a GPS receiver. The vulnerabilities of an SBAS/ GBAS receiver are same as the GPS receiver as detailed above.
3. **GSM MS:** Disassociation is a high risk, as the GSM Mobile Station (MS) can be removed or separated from the associated subject. This risk can be reduced to a medium risk using the association protocol proposed in (Wullems, Looi, & Clark, 2003). The risk of cloning is high due to the vulnerabilities of the COMP128 authentication algorithm and the ability to recover the secret key in approximately 8 hours (Briceno & Goldberg, 1998). There is improbable risk of mafia fraud for infrastructure observed / calculated location, as the infrastructure must be compromised. For location where observations or calculations are performed on the MS, there is medium risk as it requires the MS to be compromised and another MS to cooperate. There is a high risk of disruption by the removal of the power supply or physical destruction. An attack based on tampering with the receiver is also high risk, as the device is typically not physically secure, and there are no standardized mechanisms to authenticate the firmware integrity to an application.

Where location devices are used in critical applications, it is imperative that the device can be trusted if it performs any observation or calculation functions. The use of tamper-resistance and trusted computing methods could facilitate a higher assurance of trust in location devices. In addition, the problems of disassociation may be remedied through the use of tamper-resistant mountings that protect the location device from disassociation.

Signaling

The attacks that have been identified as most critical to signalling are:

- **Spoofing:** This involves interception, alteration and/or retransmission of a signal or data in such a way as to mislead the recipient;
- **Jamming:** This is the deliberate radiation or reradiation of electromagnetic energy for the purpose of disrupting electronic devices and causing denial of service; and
- **Meaconing:** This involves receiving radio signals and rebroadcasting them on the same frequency to confuse navigation.

Table 3 summarizes the vulnerabilities in the signaling used to derive location.

	Spoofing	Jamming	Meaconing
1. GPS (C/A)	Improbable – Medium	High	Improbable
2. GSM (E-OTD)	Improbable	High	Improbable
3. GSM (TOA)	Improbable	High	Improbable
4. GSM (TA)	Improbable	High	Improbable

Table 3: Signaling

1. **GPS (C/A):** Spoofing of GPS signaling is considered improbable to medium risk, depending on the nature of the application. This is because the C/A code of GPS is based on a pseudorandom number which is not cryptographically protected. GPS signal simulators are expensive but readily available. These simulators can reproduce GPS signals and navigation data, allowing the GPS signal to be easily spoofed. However, the simulation equipment required for a spoofing attack is expensive, and as such the attack is improbable. For applications such as banking transaction authentication, an expensive attack such as this may be viable, and as such could be considered medium Risk. The risk of a jamming attack is

considered very high, as the C/A code transmitted on the L1 frequency is very weak (typically –130dBm at the antenna) and as such, easy to jam. GPS jammers generate noise on the L1 band and corrupt the original signal, making location estimation (and time synchronization) impossible, causing denial of service. (DOD, 1993) states that current GPS receivers are vulnerable to jamming in acquisition mode at very long ranges from low-power jammers and will loose moderate range for reasonable jammer threats. This risk is quantified in (Adams, 2001) to the effect that a 100-watt jammer can affect a standard GPS receiver as far away as 600 miles (960 km) during initial GPS acquisition. In addition, it is stated that even when a GPS receiver has acquired the GPS signal and is using it for tracking, tracking could be interrupted within 28 miles (44.8 km) of the jammer. A 1-watt (cellular phone-size) jammer than can be built from schematics that are readily available on the Internet, and can prevent a good quality civilian receiver from acquiring the C/A code from 37.5 miles (60 km). This is a significant threat for critical applications reliant on GPS. A meaconing attack, while potentially feasible, is considered to be improbable, as there is little evidence of successful low-cost technologies to perform the attack. The GPS signals can theoretically be captured and retransmitted in the same way an indoor GPS system does, with the exception that the signal is buffered, specific time delays on certain channels introduced, and the new signals are retransmitted confusing the GPS receiver.

2. **GSM (E-OTD):** Spoofing of signaling used to measure the E-OTD is considered improbable, as the OTD value is calculated from the time difference of the arrival of signal bursts from neighboring BTSs. An attack would require simulating the signals for at least one fake BTS in proximity of the MS. To spoof a significant distance would require the simulation of at least three neighboring BTSs. Jamming is considered high risk, as it is possible to jam a MS or BTS as shown in (Stahlberg, 2000). In addition, GSM jammers have become readily and cheaply available for purposes such as denying service to MSs in cinemas, hospitals, etc. Meaconing is considered improbable, as the signals would have to be buffered and retransmitted for at least one neighboring BTSs, such that the signals were delayed when received at the MS antenna. This would require the attacker be in proximity of the MS. Meaconing in general would have a poor affect on spoofing location, as the location area of the MS is at greatest the intersection of the effective circular areas of the neighboring BTSs.
3. **GSM (TOA):** Spoofing of signaling is considered improbable, as a single signal burst from an MS is used to measure TOA at 3 geographically separate BTSs. Spoofing the signal would have little or no affect on the location. Jamming is considered a high threat for the same reasons detailed in GSM (E-OTD). Meaconing is considered improbable for similar reasons to those detailed in GSM E-OTD. The affect meaconing would have on the MS location would be minimal.
4. **GSM (TA):** Spoofing the signaling is considered improbable, as the signals would have to be simulated from a fake BTS, posing the problem of returning the TA measurement to the SMLC. Jamming is considered a high threat for the same reasons detailed in GSM (E-OTD). Meaconing the signaling is considered improbable, as the TA measurement is critical for TDMA adaptive frame alignment processes, and is calculated in the BTS. Any value other than that representing the MS' propagation distance may result in a collision of signal bursts with an adjacent slot. As a result, it is very improbable that TA location obtained from the GSM infrastructure could be spoofed.

Communications

The attacks that have been identified as most critical to communications are:

- **Repudiation:** This is the denial of an action having occurred;
- **Sniffing:** This is the unauthorized monitoring of information over a communications link;
- **Spoofing:** This involves interception, alteration and/or retransmission of a signal or data in such a way as to mislead the recipient; and

- **Denial of Service:** This is where a malicious attack results in partial or total deprivation of a service.

Table 4 summarizes the communications vulnerabilities:

	Repudiation	**Sniffing**	**Spoofing**	**Denial of Service**
1. GPS (NMEA 0183)	High	High	High	Medium
2. GPS (RTCM-104)	High	High	High	Medium
3. SBAS (RTCA)	High	High	High	Medium
4. GSM (MS-BTS(Um))	Improbable	Improbable	Improbable	Medium
5. GSM (Assistance Data Broadcasts)	Improbable	Improbable	Improbable	Medium
6. GSM (BTS-BSC (Abis))	Improbable	Medium	Improbable	Medium
7. GSM (A / Lb / Lc / Le / Lg / Lh / Lp / Ls)	Improbable	Improbable	Improbable	Improbable

Table 4: Communications Vulnerabilities

1. **GPS (NMEA 0183):** This is the defacto standard for marine navigation data communication. The NMEA 0183 Interface Standard(NMEA, 1997) defines electrical signal requirements, data transmission protocol and time, and specific sentence formats for a 4800-baud serial data bus, without providing any message integrity or encryption. As a result, there is a high risk of repudiation, as there is no mechanism in NMEA to support non-repudiation. There is a high risk of sniffing and spoofing, as there is no integrity or encryption. Spoofing can also be easily achieved through the use of simulator software available on the Internet. Denial of service is considered as a medium risk, but this depends on how the data is communicated to an application. The risk of denial of service for wireless transmission is high compared with the risk of denial of service on a cable, where a remote attack would not be possible. While denial of service at the communications layer is possible, it is easier to perform jamming on the signalling used for location acquisition to achieve the same result.
2. **GPS (RTCM-104):** This is the defacto standard for marine navigation correction for the transmission of D-GPS data (RTCM, 1998). This protocol does not make use of message encryption or integrity, and as such is vulnerable to the same attacks as NMEA. The affects of a spoofing attack on a GPS receiver's reported position depends on the rejection characteristics of the GPS receiver. Inevitably some GPS receivers will accept virtually any correction data, regardless of how erroneous it is.
3. **SBAS (RTCA):** Satellite Based Augmentation systems such as WAAS use the standard protocol RTCA for communications of D-GPS data via satellite. This is a standard protocol that integrates WAAS, EGNOS and MSAS. This protocol does not provide message integrity or encryption, and as such is vulnerable to the same attacks as NMEA. Similarly to RTCM, depending on the GPS receiver, it may be possible to spoof location though the spoofing of RTCA correction data.
4. **GSM (MS-BTS(Um)):** The risk of sniffing transmissions is high due to encryption using the A5 cipher. (Barkan, Biham, & Keller, 2003) propose a method of obtaining the A5 key in a few milliseconds, after which the transmissions can be sniffed. There is a medium risk of denial of service by jamming the MS or BTS based on methods detailed in (Stahlberg, 2000).
5. **GSM (Assistance Data Broadcasts):** Where the non-mandatory enciphering option is used, sniffing and spoofing of the location data and or assistance data is improbable. The assistance data broadcasts are vulnerable to the other vulnerabilities of GSM (MS-BTS(Um)) transmissions.
6. **GSM (BTS-BSC(Abis interface)):** There is a medium risk of sniffing where link-level encryption is not implemented over this link. In GSM there is no requirement for the use of encryption for communications between the BTS and BSC, and as such it may be possible to sniff data. The risk of a denial of service attack is deemed as medium, as it is possible to jam the microwave links when the BTS-BSC links are not cabled, to prevent transmission of location and assistance data.
7. **GSM (A/Lb/Lc/Le/Lg/Lh/Lp/Ls interfaces):** These communications occur within the infrastructure over the A/Lb/Lc/Le/Lg/Lh/Lp/Ls interfaces (ETSI, 2000b). It is assumed that these interfaces link systems that are within physically secured locations, and are physically

secure themselves. It is therefore considered improbable that any of the attacks occur due to the lack of accessibility.

Secure communication of both location data and augmentation data are critical to the security and reliability of critical applications. There is need for research into secure protocols to replace the currently insecure NMEA, RTCA and RTCM protocols. Critical applications can utilize existing technologies such as GSM A-GPS for its security services such as encryption of the D-GPS corrections, providing a workable solution to the absence of a secure augmentation data service. The other GSM location mechanisms can provide a redundant location backup should there be a GPS outage.

EMERGING TECHNOLOGY

GALILEO constellation is under development and will be operative from 2008. It will be composed of 27 active satellites + 3 spare satellites in Medium Earth Orbit. It has been projected "service oriented" on 6 bands: the E5a (1176,45MHz, the GPS L5) and E5b(1207,14MHz, the Glonass L3),the band E6 (1278,75MHz) and the GPS L1 (1575,42MHz) 8 MHz wider (extension E2 and E1) as detailed in (Hein & al, 2002). The interoperability with GPS is realized by having two common frequencies in E5a/L5 and L1.

As Galileo is still under development there are not detailed specification on signals and cryptography. There few technical descriptions from the European Space Agency (ESA) documents, as detailed in (ESA, 2001) and (ESA, 2003). Galileo will broadcast different services of which some utilize cryptography. The Open service will be broadcasted in 2 signals with no cryptography.

The Galileo Safety of Life (SOL) service will have cryptographic integrity check broadcasted with the signal. The commercial service provides 3 signals for navigations and data, one of which will be encrypted (ESA, 2001). We are currently exploring the Galileo proposals and intend to submit in a future paper how these new services can be used in critical applications.

In addition to the Galileo project, Europe is testing a Satellite based augmentation system, EGNOS, which will provide integrity and coarse location acquisition services as well as GPS/Galileo correction data. The system is expected to be fully operational by 2005, providing redundancy through a course location acquisition not dependant on GPS. This will be beneficial for critical applications that currently rely solely on GPS.

Australia relies on GPS without a service agreement from the United States of America. The proposed GRAS augmentation system does not provide redundancy or integrity services, and as such, GPS-based critical applications in Australia require the augmentation of other location / timing technologies to supplement a critical system in case of a GPS outage.

CONCLUSION

In this paper, we have proposed a generalized model for the vulnerability assessment of active location technologies with cooperative infrastructure, grouping the characteristics of GSM, GPS and various augmentations to these location systems. The model reduced the technologies to the fundamental characteristics of Infrastructure, Devices, Signaling and communications. Based on these characteristics, we have performed a vulnerability assessment of these technologies, and demonstrated how other cooperative location technologies can be applied to this model.

The significance of this generalized model and of the related vulnerability assessment is to create an instrument to build trusted location services for Critical Infrastructure. Any active location technology with a cooperative infrastructure can be modelled using this method.

REFERENCES

Adams, T. K. (2001). GPS Vulnerabilities. *Military Review*, 10-16.

Barkan, E., Biham, E., & Keller, N. (2003). *Instant Ciphertex-Only Cryptanalysis of GSM Encrypted Communication*. Haifa Israel: Technion Computer Science Department.

Briceno, M., & Goldberg, I. (1998, April). *GSM Cloning*, 2003, from http://www.isaac.cs.berkley.edu/isaac/gsm-faq.html

Caton, J. L. (1995). *We Can Reduce Satellite Vulnerability.* Paper presented at the U.S. Naval Institute.

Crosby, G. K., Ely, W. S., McPherson, K. W., Stewart, J. M., Kraus, D. K., Cashin, T. P., et al. (2000). *A Ground-based Regional Augmentation System (GRAS) - The Australian Proposal.* Paper presented at the ION GPS2000, Salt Lake City UT.

Denning, D. E., & MacDoran, P. F. (1996). Location-based Authentication: Grounding Cyberspace for Better Security. *Computer Fraud and Security*, 167-174.

DOD. (1993). *Report of the Defense Science Board Task Force on Tactical Air Warfare*. Washington D.C.: Department of Defense, United States of America.

ESA. (2001). Galileo - Mission High Level Definition: European Space Agency.

ESA. (2003). Galileo: The European Programme for Global Navigation Service: European Space Agency.

ETSI. (2000a). *Digital cellular telecommunications system (Phase 2+) (GSM); Location Services (LCS); Broadcast Network Assistance for Enhanced Observed Time Difference (E-OTD) and Global Positioning System (GPS) Positioning Methods*: European Telecommunications Standards Institute.

ETSI. (2000b). *Digital cellular telecommunications system (Phase 2+); Location Services (LCS); (Functional description) - Stage 2*: European Telecommunications Standards Institute.

ETSI. (2000c). *Digital cellular telecommunications system (Phase 2+); Technical realization of Cell Broadcast Service (CBS)*: European Telecommunications Standards Institute.

Hein, G. W., & al, e. (2002). Status of Galileo Frequency and Signal Design. Brussels.

Hightower, J., Brumitt, B., & Borriello, G. (2002). *The location stack: a layered model for location in ubiquitous computing.* Paper presented at the Fourth IEEE Workshop on Mobile Computing Systems and Applications.

Hoffmann-Wellenhof, B.H.Lichtenegger, & J.Collins. (1994). *GPS: Theory and Practice* (3rd ed.). New York: Springer-Verlag.

Lara, W. (2003). *Universal Location Framework: A New Wireless Building Block.*

MacDoran, P. F. (1998). Method and Apparatus for Authenticating the Location of Remote Users of Networked Computing Systems. United States Patent 5757916.

NMEA. (1997). NMEA 0183 Standard for Interfacing Marine Electronic Devices: National Marine Electronics Association.

RTCM. (1998). *RTCM Recommended Standards for Differential Navstar GPS Service, Version 2.2, RTCM Special Committee No. 104*: Radio Technical Commission for Maritime Services.

Stahlberg, M. (2000). Radio Jamming Attacks Against Two Popular Mobile Networks.

Volpe, J. A. (2001). *Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System*.

WorldPay. (2001). *WorldPay deploy GPS technology to deliver pinpoint security for Business to Business transactions and launch WorldPay Genesis*. Retrieved September, 2003, from http://www.worldpay.co.kr/kr/news/2001/news_genesis.shtml

Wullems, C., Looi, M., & Clark, A. (2003, July). *Enhancing the Security of Internet Applications using Location: A New Model for Tamper-resistant GSM Location.* Paper presented at the Proceedings of the Eighth IEEE Symposium on Computers and Communications (ISCC 2003).

COPYRIGHT