A Location Based Encryption Technique and Some of Its Applications

Logan Scott, *GeoCodex LLC, LS Consulting*
Dorothy E. Denning, *GeoCodex LLC, Naval Postgraduate School*

BIOGRAPHY

Logan Scott is a consultant specializing in radio frequency signal processing and waveform design for communications, navigation, radar, and emitter location. He has more than 24 years of military GPS systems engineering experience. As a senior member of the technical staff at Texas Instruments, he pioneered approaches for building high-performance, jamming-resistant digital receivers using large-scale application-specific integrated circuit (ASIC) technologies. He has developed gain and frequency plans, non-uniform analog/digital conversion techniques, fast acquisition architectures, Baseband signal processing algorithms and adaptive array approaches. He is currently involved in projects to provide location based encryption and authentication. He holds 27 US patents.

Dr. Dorothy E. Denning is a founding partner in GeoCodex and a professor in the Department of Defense Analysis at the Naval Postgraduate School. Her current work encompasses the areas of cybercrime and cyberterrorism, information warfare and security, and cryptography. She has published 120 articles and four books, her most recent being Information Warfare and Security. She is an ACM Fellow and recipient of several awards, including the Augusta Ada Lovelace Award and the National Computer Systems Security Award. In November 2001, she was named a Time magazine innovator. Dr. Denning received the B.A. and M.A. degrees in mathematics from the University of Michigan and the Ph.D. degree in computer science from Purdue University. She has previously worked at Georgetown University, Digital Equipment Corporation, SRI International, and Purdue University. She holds 1 US patent.

ABSTRACT

Location based encryption enhances security by integrating position and time into encryption and decryption processes. We find that from a security perspective, it is not enough to simply enable or disable decryption based on location and time; these aspects must be integrated into the key construction process. Furthermore, keys or files in transit should not reveal anything regarding their locations/times of applicability. After reviewing the objectives of location-based encryption, this paper introduces a specific approach called geo-encryption.

The described geo-encryption approach builds on established cryptographic algorithms and protocols in a way that provides an additional layer of security beyond that provided by conventional cryptography. It allows data to be encrypted for a specific location(s) or for specific area(s), e.g. a corporation's campus area. Constraints in time as well as location can also be enforced. Geo-encryption can be used with both fixed and mobile applications and supports a wide range of data sharing and distribution policies.

We then discuss a process of applying successive geo-encryptions at the originating node to enforce specific geographic routings for transmission to the final destination node. With each intervening node removing one layer of encryption, unless the file has gone through the proper sequence of nodes, decryption will fail. Using a similar process, messages can be location authenticated by applying one layer of encryption at each intervening node.

Next, we discuss some specific applications. In the civilian sector, there has been a great deal of interest in providing location-based security for digital cinema distribution and forensic analysis in cases of piracy. In this application, the same, large (25 to 190 Gbyte), encrypted media file might be used at multiple theatre locations but with distinct GeoLocked keys specific to the

intended recipient location and exhibition license. This provides a secure and efficient point to multipoint distribution model applicable to distributions via satellite or DVD. At the exhibition hall, robust watermarking/steganographic techniques can introduce location, time and exhibition license information into the exhibition for subsequent use in piracy investigations.

For the military GPS user, we show how individual waypoints can be uniquely encrypted so as to be accessible only when the set is physically within the route parameters; both location and time wise. An intact, captured set would not reveal mission parameters.

INTRODUCTION

On September 17, 2000, Qualcomm CEO and Chairman Irwin Jacob's IBM Thinkpad computer was stolen while he stood a few feet from it.

> *"…was startled to find his laptop missing from the podium after he wrapped up questions from the Society of American Business Editors and Writers in Irvine, Calif."* Forbes Magazine

Fortunately, his hard drive was password protected.

> *"… at one of the largest technology companies, where policy required that passwords exceed 8 characters, mix cases, and include numbers or symbols...*
>
> - *L0phtCrack obtained 18% of the passwords in 10 minutes*
> - *90% of the passwords were recovered within 48 hours on a Pentium II/300*
> - *The Administrator and most Domain Admin passwords were cracked"*
>
> @stake website advertising their LC4 password audit and recovery product

Government people know better.

> *"The Pentagon is investigating whether ultrasecret "black programs" were compromised by former CIA Director John Deutch after he put details about some of the Defense Department's most sensitive activities on his home computers."* Washington Times, 17 February 2000.

People tend to be the weakest link in security.

> On the subject of computer security: *"…the mathematics are impeccable, the computers are vincible, the networks are lousy, and the people are abysmal."* Bruce Schneier, "Secrets & Lies, Digital Security in a Networked World

Network and computer security is rarely breeched using a brute force attack against cryptographic elements; the algorithms are simply too strong. Instead, attackers rely on myriad techniques that take advantage of operating systems features, attack protocols, use insider access, exploit human weaknesses, or obtain information through social engineering.

Geo-encryption builds on established cryptographic algorithms and protocols in a way that provides an additional layer of security beyond that provided by conventional cryptography. It allows data to be encrypted for a specific place or broad geographic area, and supports constraints in time as well as space. It can be used with both fixed and mobile applications and supports a range of data sharing and distribution policies. It provides full protection against attempts to bypass the location feature. Depending on the implementation, it can also provide strong protection against location spoofing.

GEOENCRYPTION

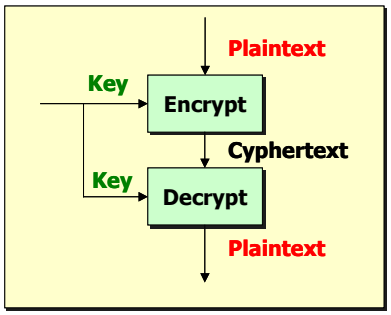
The term "location-based encryption" is used here to refer to any method of encryption wherein the cipher text can only be decrypted at a specified location. If an attempt is made to decrypt the data at another location, the decryption process fails and reveals no information about the plaintext. The device performing the decryption determines its location using some sort of location sensor, for example, a GPS receiver or some other satellite or radio frequency positioning system.

Location-based encryption can be used to ensure that data cannot be decrypted outside a particular facility, for example, the headquarters of a government agency or corporation, or an individual's office or home. Alternatively, it may be used to confine access to a broad geographic region. Time as well as space constraints may be placed on the decryption location.

A Short Tutorial On Encryption Algorithms

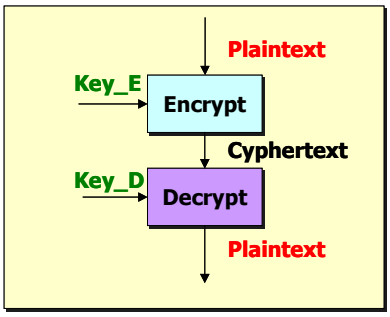
Broadly speaking; encryption algorithms can be divided into two categories; symmetric algorithms and asymmetric algorithms. Referring to figure 1, symmetric algorithms use the same key for encrypting and decrypting plaintext. Numerous, very fast symmetric algorithms are in widespread use including: DES & Triple-DES as described in [1] and the newly released Advanced Encryption Standard (AES) described in [2]. Keeping the key private is essential to maintaining security and therein lays the key question; how to share keys securely. Numerous techniques have been developed and the interested reader is directed to [3] for further discussion.

Figure 1: Symmetric Algorithm



Asymmetric algorithms are comparatively new on the scene with the first published description [4] in 1976. Also known as Public Key algorithms, these algorithms have distinct keys for encryption and decryption as is shown in figure 2. Here, Key_E can be used to encipher the plaintext but not to decipher it. A separate key (Key_D) is needed to perform this function.

Figure 2: Asymmetric Algorithm



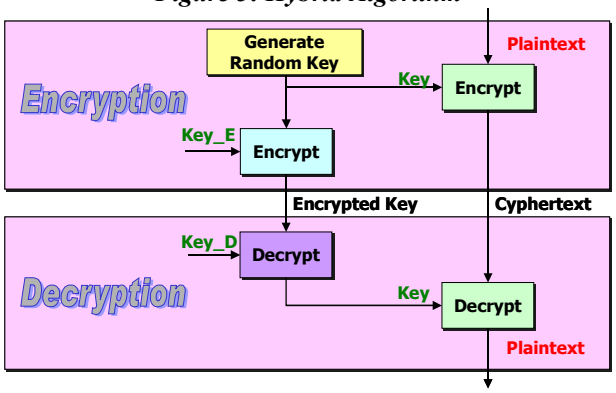
In principle, to securely convey the plaintext, the intended recipient could generate a key pair (Key_E, Key_D) and send Key_E, the public key, to the originator via unsecured channels. This would allow the originator (or anyone else) to encrypt plaintext for transmittal to the recipient who uses Key_D, the private key, to decrypt the plaintext.

RSA, named after its creators Rivest, Shamir & Adleman is perhaps the most popular asymmetric algorithm in use today. Its security is based on the difficulty of factoring large prime numbers.

One major drawback with asymmetric algorithms is that their computational speed is typically orders of magnitude (~1,000) slower than comparable symmetric algorithms. This has led to the notion of hybrid algorithms such as the one shown in figure 3.

Here, a random key, sometimes called the session key, is generated by the originator and sent to the recipient using an asymmetric algorithm. This session key is then used by

Figure 3: Hybrid Algorithm



both parties to communicate securely using a much faster symmetric algorithm. The hybrid approach has found wide application, most notably on the Internet where it forms the basis for secure browsers (Secure Socket Layer (SSL)) and secure e-mail.

The GeoEncryption Algorithm

In principle, one could cryptographically bind (attach) a set of location and time specifications to the cyphertext file and build devices that would decrypt the file only when within the specified location & time constraints. There are several potential problems with such an approach:

- The resultant file reveals the physical location of the intended recipient. The military frowns on this sort of thing, at least for their own forces. Furthermore, it provides vital information to someone who wants to spoof the device.

- If the device is vulnerable to tampering, it may be possible to modify it so as to completely bypass the location check. The modified device would decrypt all received data without acquiring its location and verifying that it is correct. Alternatively, an adversary might compromise the keys and build a modified decryption device without the location check. Either way, the modified device could be used anywhere and location would be irrelevant

As another possibility, one might consider using location itself as the cryptographic key to an otherwise strong encryption algorithm like AES. This is ill advised in that location is unlikely to have sufficient entropy (uncertainty) to provide strong protection. Even if an adversary does not know the precise location, there may be enough information to enable a rapid brute force attack analogous to a dictionary attack. For example, suppose that location is coded as a latitude-longitude pair at the precision of 1 centimeter, and that an adversary is able to

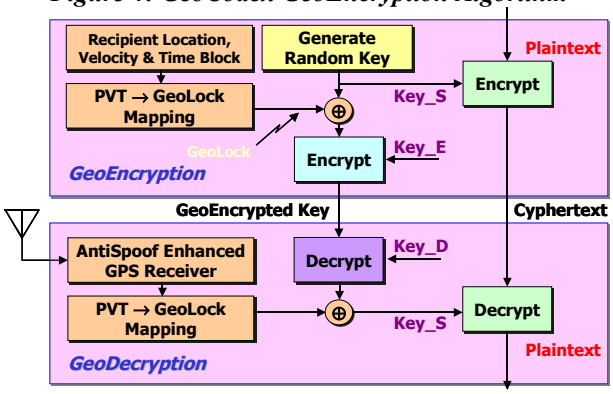
narrow down the latitude and longitude to within a kilometer. Then there are only 100,000 possible values for each of latitude and longitude, or 10 billion possible pairs (keys). Testing each of these would be easy.

Applying an obfuscation function to the location value before using it as a key could strengthen this approach; however, the function would have to be kept secret in order to prevent the adversary from doing the same. In general, security by obscurity is scoffed at, because once the secret method is exposed, it becomes useless. The entire security system collapses like a house of cards.

A guiding principle behind the development of cryptographic systems has been that security should not depend on keeping the algorithms secret, only the keys. This does not mean that the algorithms must be made public, only that they be designed to withstand attack under the assumption that the adversary knows them. Security is then achieved by encoding the secrets in the keys, designing the algorithm so that the best attack requires an exhaustive search of the key space, and using sufficiently long keys that exhaustive search is infeasible.

GeoCodex's GeoEncryption algorithm addresses these issues by building on established security algorithms and protocols. Referring to figure 4, our approach modifies the previously discussed Hybrid algorithm to include a GeoLock.

Figure 4: GeoCodex GeoEncryption Algorithm

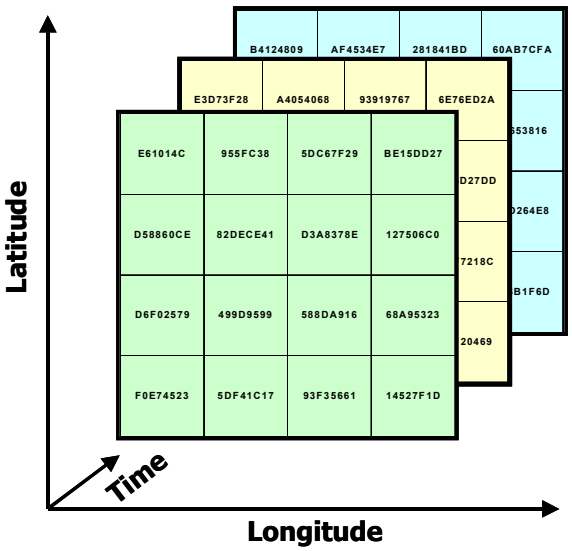


On the originating (encrypting) side, a GeoLock is computed based on the intended recipient's Position, Velocity, and Time (PVT) block. The PVT block defines where the recipient needs to be in terms of position, velocity & time for decryption to be successful. The GeoLock is then XORed with the session key (Key_S) to form a GeoLocked session key. The resultant is then encrypted using an asymmetric algorithm and conveyed to the recipient, much like we saw in the Hybrid algorithm of figure 3. On the recipient (decryption) side, GeoLocks are computed using an AntiSpoof GPS receiver for PVT input into the PVT→GeoLock mapping function. If the PVT values are correct, then the resultant GeoLock will XOR with the GeoLocked key to provide the correct session key (Key_S).

PVT→GeoLock mapping function

Sidestepping the issue of what constitutes an AntiSpoof receiver for the moment, we now address how GeoLocks are formed. Figure 5 shows a notional diagram of a PVT→GeoLock mapping function where latitude, longitude and time constitute the inputs. Here, a regular grid of latitude, longitude and time values has been created, each with an associated GeoLock value.

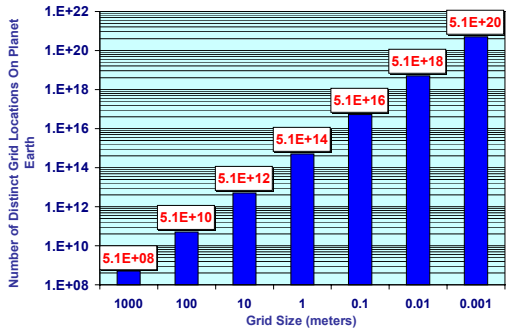
Figure 5: PVT→GeoLock Mapping Function



Grid spacing must take into account the accuracy of the GPS receiver at the decrypting site; otherwise erroneous GeoLock values may result. It makes no sense to have 1cm grid spacing if using a standalone GPS receiver. Conversely, if using an RTK style receiver capable of 2cm accuracy, 10-meter grid spacing is overly conservative. Grid spacing may also be wider in the vertical direction to account for poorer vertical positioning accuracy typical in most sets because of satellite geometries [5].

Figure 6 shows the number of possible grid points on the planet as a function of grid spacing, ignoring altitude, time and velocity.

Figure 6: Number of Distinct Grid Locations



A more complete PVT→GeoLock mapping function could actually have eight inputs:

- Position (East, North, Up)
- Velocity (East, North, Up)
- Time
- Coordinate System Parameters

The velocity inputs might actually map into a minimum speed requirement so as to ensure that the recipient is actually underway. Including coordinate system parameters in the PVT→GeoLock mapping function provides support for non-stationary reference frames. This feature might be used, for example, in communicating with a satellite.

The grid could just as well been based on a Military Grid Reference System (MGRS) or it's close cousin UTM. In fact, any arbitrary shapes could have been used; for example the shape of the Disneyland theme park could map to a single GeoLock value so as to permit successful decryption when located in the theme park but not when outside.

Finally, we note that the PVT→GeoLock mapping function itself may incorporate a hash function or one-way function with cryptographic aspects in order to hinder using the GeoLock to obtain PVT block values. Similarly, the algorithm may be deliberately slow and difficult; perhaps based on solving a difficult problem.

A Few Quick Observations On AntiSpoof Receivers

Most civilian receivers are trivially simple to spoof; simply hook up one of the many excellent signal simulators available and the receiver will buy into whatever PVT values you want [6]. This is why military receivers use Y-code; an encrypted version of P-code. Unless the spoofer has access to the correct cryptographic keys and knows how to generate Y-code from P-code, it can't spoof the military set. He may be able to jam it, but not spoof it.

Civilian sets can be made difficult to spoof through a series of hardening measures. These include a variety of signal's checks:

- Use J/N meter to check for above normal energy levels
- Monitor C/No meter for Consistency/ Unexpected C/No given J/N
- Monitor Phase Difference Between Antenna Elements (All signals shouldn't come from the same direction)
- Deep Acquisition to Look for Weak, Real Signals

Numerous navigation checks can also be instituted:

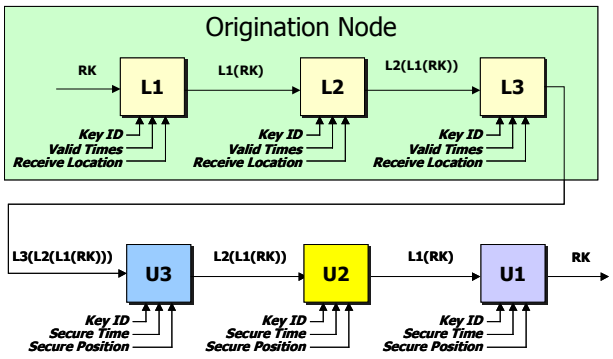
- Compare "Watch Time" with "Signals Time" (Most signal generators can't synchronize with GPS time)
- Continuity Checks in Time and Position (There is no hyperspace button in real life)
- Consistency with other Navigation Sensors
- Large Residuals, Particularly in Differential Correction Channel(s)
- RAIM Type Functions

With careful attention to detail, civilian sets do not have to be as vulnerable to spoofing as most of them are.

Relay Encryption to Force a Particular Routing & For Authentication

Successive Geo-encryption can be used to force data and/or keys to follow a specific geographical path before it can be decrypted. This is achieved by applying multiple geo-locks at the origination node prior to transmittal using a procedure such as the one shown in figure 7. As each required node is traversed, one layer of GeoLocking is removed, thus ensuring the desired path has been followed.

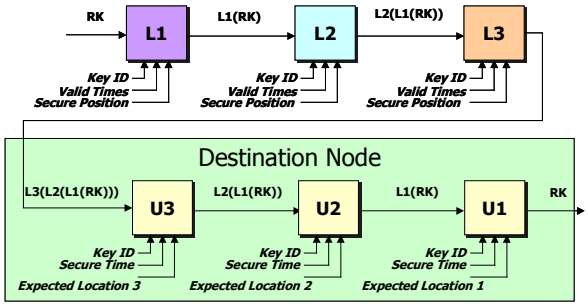
Figure 7: Successive GeoLocking to Force A Particular Routing



Relay encryption might be useful for applications that employ regional distribution centers for the distribution of data supplied by producers. For example, in subscription television, the producers could be the television networks, while the distributors are cable or satellite television providers. A producer could lock a key initially to a geographic region covered by one of the distributors using a key known only to the subscribers, and then to the precise location of the distributor using the distributor's key. The distributor would unlock its geo-lock before broadcasting the programming to subscribers, who would then unlock the regional geo-lock and decrypt the cyphertext.

In some applications, it may be desirable to know that a message has followed a particular route. Figure 8 depicts a process similar to the Route Forcing technique for achieving this, where each traversed node in effect stamps the message with its PVT values.

Figure 8: Route Authentication By Successive GeoEncryption



APPLICATIONS EXAMPLES

To show how GeoEncryption can be applied to real world problems, we discuss two examples: digital cinema distribution, and, GPS receiver waypoint GeoEncryption.

Digital Cinema Distribution

"Today, the film studios spend over $1 billion each year to duplicate, distribute, rejuvenate, redistribute and ultimately destroy the thousands of film reels required to bring the close to 500 films released each year to audiences across the U.S." Booz Allen Hamilton: DIGITAL CINEMA: BREAKING THE LOGJAM

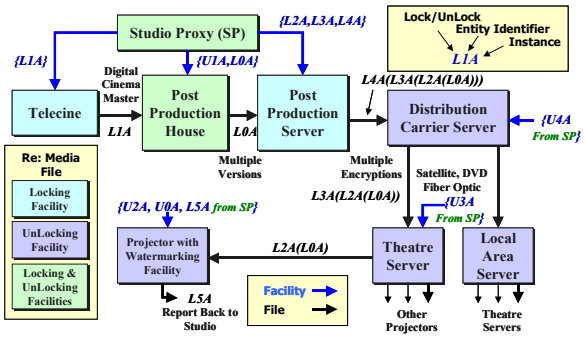
SATCOM links provide for a very efficient and cost effective digital cinema distribution model but piracy is a major concern; SATCOM links are easy to intercept. The experience with Direct Satellite Services (DSS) has not been encouraging. There are an estimated 3 million unauthorized users using cloned versions of the tamper resistant smart cards that seek to prevent this. Furthermore, cinema stakeholders are risk adverse towards piracy based on the music industry's experience with Napsterization. Music sales are down 8% and company valuations are down 40%, largely because of piracy.

As a consequence, there has been significant interest in providing location-based security for digital cinema distribution and forensic analysis in cases of piracy. GeoCodex has been working with Digital Cinema Ventures (DCV) to develop security techniques specific to this industry.

In this application, the same, large (25 to 190 Gbyte), encrypted media file might be used at multiple theatre locations nationwide but with distinct GeoLocked keys specific to the intended recipient location and its exhibition license. This provides a secure and efficient point to multipoint distribution model applicable to distributions via satellite or DVD. At the exhibition hall, robust watermarking/steganographic techniques can introduce location, time and exhibition license information into the exhibition for subsequent use in piracy investigations.

Figure 9 depicts a media distribution reference model wherein a Studio Control policy is maintained. In this model, we start with the Telecine, which produces the Digital Cinema Master, an uncompressed, highest resolution digital version taken from the film masters. The

Figure 9: Media Distribution Reference Model (Studio Control Version)



postproduction house assembles and converts the DC master into multiple versions, possibly for presentation and exhibition on a variety of media (e.g. Theatre, DVD, Cable TV). A postproduction server then provides multiple encryptions of the multiple versions for distribution. Individual distributors are expected (but not required) to have their own servers to source their own facilities. Theatres receive copies of the media file in non-real-time; storing a copy on their local server. The Theatre server then provides the still encrypted media file to an authorized, tamper resistant projector, which contains

sufficient buffering to source the real-time decryption and exhibition of the media file.

Placing four successive locks on the random key (ala. Figure 7), the studio proxy can force the key to traverse the distribution carrier's server which takes off its lock (U4A), the Theatre server which takes off its lock (U3A) and finally, the projector which takes off its lock (U2A) and the studio's lock (U0A). Only the projector and the studio proxy can access the random key needed to decrypt the media file. Intervening stages of distribution are critically involved in key transmittal and partial decryption, but they have no access to the plaintext media.

Waypoint GeoLocking for Improved Mission Security

To navigate with GPS, users typically follow a route consisting of an ordered series of waypoints. In its simplest form, a waypoint is nothing more than a position but in airborne applications it may contain velocity expectations and time of transit expectations as well. In military applications, velocity & time of transit specifications are used in launching coordinated attacks where diverse force elements converge on target(s) simultaneously. Ground forces routinely use GPS to place, and then traverse mine fields via safe routes.

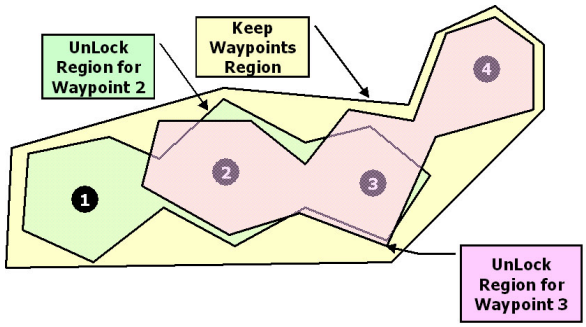
Extended waypoint/regional information can include:

- Radio Contact Parameters
  - Frequency
  - IFF Parameters
- Weapons Parameters/Restrictions
- Crypto variables

In short, for the military user, the waypoints and associated routes comprise some of the most sensitive data in the military GPS set and should be protected accordingly. GeoEncryption can provide an additional layer of security by restricting access to waypoint data based on location, time & velocity.

Figure 10 depicts a notional mission profile consisting of a series of waypoints where we have defined regions of access for waypoints 2 & 3. There is no particular requirement that the PVT→GeoLock mapping function be based on a regular grid and here; we have chosen polygonal shapes based on mission needs. Also, note that GeoLock regions can overlap; they do not have to be geographically disjoint from one another. Time & velocity window requirements could also have been imposed.
As an added refinement, we could also define a "keep waypoints" region (shown in yellow). If the set exits this area, perhaps due to capture, it can destroy its waypoints. Alternatively, it might display a different set of waypoints

Figure 10: Waypoint GeoEncryption to Secure Mission Information



and routes, maybe with misleading descriptions. For example, it might display a route titled "Safe Route Through Minefield" that in fact really leads over the mines. The set could also be configured to display erroneous position when outside of its authorized area. Integrated into weapons systems, they may refuse to fire (or worse) when outside of their authorized areas. The possibilities are limited only by the creativity of the mission planner.

CONCLUSIONS

Geo-encryption is an approach to location-based encryption that builds on established cryptographic algorithms and protocols. It allows data to be encrypted for a specific place or broad geographic area, and supports constraints in time as well as space. It can support both fixed and mobile applications, and a variety of data sharing and distribution policies. It provides full protection against location bypass. Depending on the implementation, it also can provide strong protection against location spoofing.

ACKNOWLEDGMENTS

The authors would like to acknowledge the helpful commentary and discussions with our other GeoCodex partners: Mark Seiler, Barry Glick and Ron Karpf.

REFERENCES

[1] FIPS 46-3
[2] FIPS 197
[3] Bruce Schneier, "Applied Cryptography, 2nd ed."
[4] Diffie & Hellman, "New Directions in Cryptography" IEEE Transactions on Information Theory, Nov 1976
[5] SEP discussions at: http://home.earthlink.net/~loganscott53/Circular_Error_Probable.htm
[6] Logan Scott, Navtech Seminars course: "GPS Interference & Jamming Issues for Civil & Military Users"