Innovation

Using GPS to Enhance Data Security

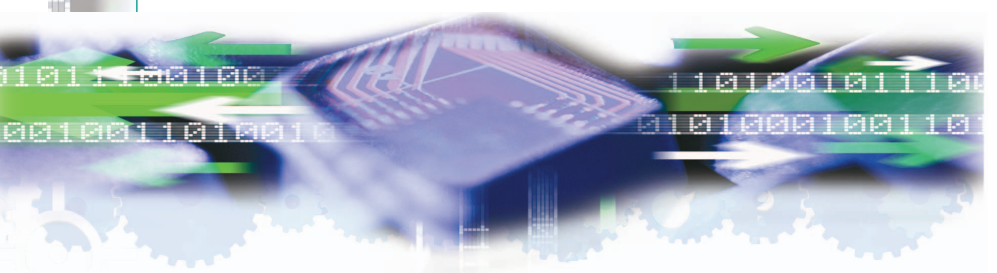
Geo-Encryption

Logan Scott and Dorothy E. Denning

Generals, diplomats, and lovers have used cryptography for thousands of years to encode messages and other documents so that only the intended recipient would be able to read them. Julius Caesar, for example, is reported to have used a substitution encryption scheme or cipher to exchange messages with his generals. Each letter in an original message was substituted with another letter obtained by shifting a fixed number of letters further along in the alphabet. So, *a* would be replaced by, say, *c; b* would become *d;* and so on. The codes of such simple substitution ciphers are easily broken by noting the frequencies of the letters in the encoded messages. In English words, for example, the letter *e* occurs most often – it is 56 times more common than *q*, the least common letter. And more English words begin with the letter *s* than with any other letter. So over the years, cryptologists have devised ever more sophisticated and complex encryption schemes to provide greater security to encoded information.

In this month's column, Logan Scott and Dorothy Denning discuss an innovative encryption scheme that integrates position and time into the encryption and decryption processes. Their 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 one or more specific locations or areas such as 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 such as providing location-based security for digital cinema distribution and forensic analysis in cases of piracy. For the military GPS user, the authors illustrate how individual waypoints can be uniquely encrypted so as to be accessible only when the receiver is physically within the route parameters, both in terms of location and time.

— R.B.L.



On September 17, 2000, Qualcomm CEO and Chairman Irwin Jacob's IBM Thinkpad computer was stolen while he stood a few meters from it. He "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, California" *(Forbes Magazine)*. Fortunately, his hard drive was password protected.

"At one of the largest technology companies where policy required that passwords exceed eight characters, mix cases, and include numbers or symbols ... [the program] L0phtCrack obtained 18 percent of the passwords in 10 minutes. Ninety percent of the passwords were recovered within 48 hours on a Pentium II/300. The Administrator and most Domain Admin passwords were cracked" *(@stake Web site advertising their LC4 password audit and recovery product)*.

Government personnel should know better. However, that is not always the case: "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, February 17, 2000)*.

People tend to be the weakest link in security. On the subject of computer security, security technologist and author Bruce Schneier comments that "the mathematics are impeccable, the computers are vincible, the networks are lousy, and the people are abysmal" *(Secrets and Lies: Digital Security in a Networked World)*.

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

Geo-Encryption

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.

The terms *location-based encryption* or *geo-encryption* are used in this article to refer to any method of encryption in which the encrypted information, called *ciphertext*, can be decrypted only at a specified location. If someone

Logan Scott is a consultant specializing in radio frequency signal processing and waveform design for communications, navigation, radar, and emitter location. He is a partner in GeoCodex, LLC, Arlington, Virginia. With a B.S.E.E. degree from Columbia University, he has more than 24 years of military GPS systems engineering experience and is currently involved in projects to provide location-based encryption and authentication. He holds 28 U.S. patents.

Dorothy E. Denning, Ph.D., is a founding partner in GeoCodex and a professor in the Department of Defense Analysis at the Naval Postgraduate School in Monterey, California. Her current work encompasses the areas of cybercrime and cyberterrorism, information warfare and security, and cryptography. She received B.A. and M.A. degrees in mathematics from the University of Michigan and a Ph.D. in computer science from Purdue University. She has previously worked at Georgetown University, Digital Equipment Corporation, SRI International, and Purdue University. She co-holds a U.S. patent for geo-encryption.

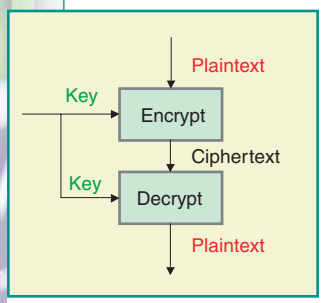


FIGURE 1 Symmetric or single-key algorithms use the same key to encrypt the plaintext and to decrypt the ciphertext. The key must be kept secret.

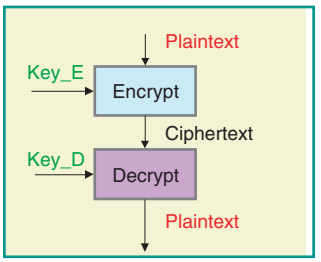


FIGURE 2 Asymmetric or two-key algorithms use one key for encrypting the plaintext and another key for decrypting the ciphertext. Also known as *public-key algorithms*, a public key, Key_E, is used for encryption and a distinct private key, Key_D, is used for decryption.

attempts to decrypt the data at another location, the decryption process fails and reveals no details about the original *plaintext* information. The device performing the decryption determines its location using some sort of location sensor such as a GPS receiver or 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 can be placed on the decryption location.

Encryption Algorithms. Broadly speaking, encryption algorithms or ciphers can be divided into two categories: symmetric algorithms and asymmetric algorithms. As shown in **Figure 1**, symmetric algorithms use the same key (i.e., a specific digital code or bit pattern used with the algorithm) for encrypting (i.e., locking) plaintext and decrypting (i.e., unlocking) ciphertext. Numerous, very fast symmetric algorithms are in widespread use, including the Data Encryption Standard (DES) and Triple-DES and the newly released Advanced Encryption Standard (AES). Keeping the key private is essential to maintaining security. Therein lies the crucial question: How should keys be shared securely? Several techniques have been developed; the interested reader is directed to the "Further Reading" sidebar for more information.

Asymmetric algorithms are comparatively new on the scene — the first description was published 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 encrypt the plaintext but not to decrypt the ciphertext. A separate key, Key_D, is needed to perform this function. 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 by means of unsecured channels. This action 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 ciphertext. RSA, named after its creators Rivest, Shamir, and 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 to asymmetric algorithms is that their computational speed is typically orders of magnitude (~1,000) slower than are comparable symmetric algorithms. This problem 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 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 (e.g., Secure Socket Layer) and secure e-mail.

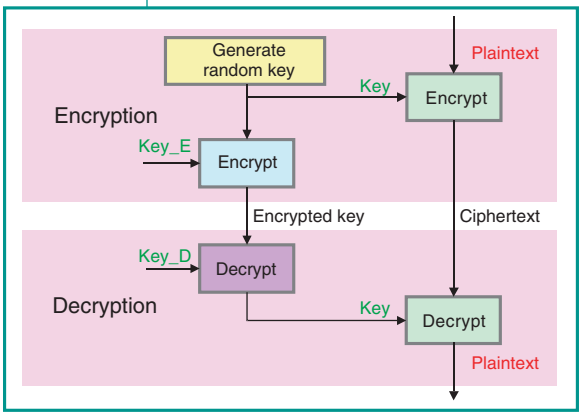


FIGURE 3 In hybrid encryption algorithms, a randomly generated key is used to symmetrically encrypt and decrypt a message, file, or data stream, and the key itself is encrypted using a public-key algorithm. Such a procedure is more efficient than using the two-key approach to encrypt the whole message.

The Geo-Encryption Algorithm. In principle, one could cryptographically bind or attach a set of location and time specifications to the ciphertext file and build devices that would decrypt the file only when the user is within the specified location and time constraints. However, this approach presents potential problems: 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 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 could use location itself as the cryptographic key to an otherwise strong encryption algorithm such as AES. This is ill advised in that location is unlikely to have sufficient entropy (i.e., uncertainty) to provide strong protection. Even if an adversary does not know the precise location, enough information may be available 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 one centimeter and that an adversary is able to narrow the latitude and longitude to within a kilometer. Then there are only 100,000 possible values each for latitude and for longitude, or 10 billion possible pairs (i.e., keys). Testing each of these pairs 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

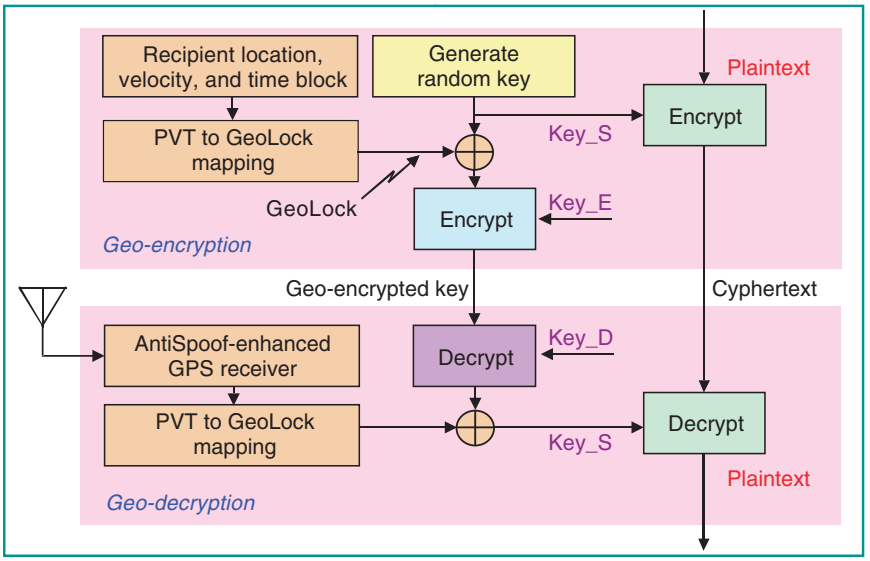


FIGURE 4 A geo-encryption algorithm uses a GPS receiver to decrypt a key that has been encrypted with position, velocity, and time values. If successfully recovered, the key can then be used to decrypt the accompanying cyphertext.

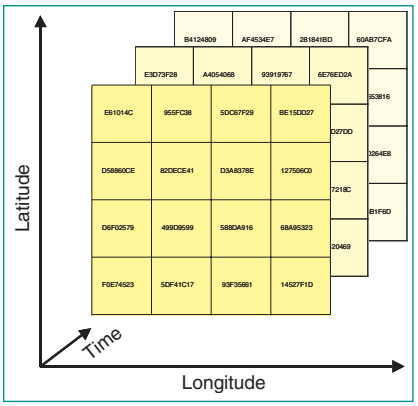


FIGURE 5 Our geo-encryption process uses a position-velocity-time to GeoLock mapping function to generate a code or GeoLock to lock and unlock the session key.

secret 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 is that security should not depend on keeping the algorithms secret, only the keys. This does not mean that the algorithms must be made public, but 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 geo-encryption algorithm addresses these issues by building on established security algorithms and protocols. As shown in **Figure 4**, our approach modifies the previously discussed hybrid algorithm to include a "GeoLock."

On the originating (i.e., encrypting) side, a GeoLock is computed on the basis of the intended recipient's position, velocity, and time (PVT) block. The PVT block defines where the recipient must be in terms of position, velocity, and time for decryption to be successful. The GeoLock is then added bit by bit — an *exclusive or* (XOR) logical operation — with the session key (i.e., Key_S) to form a GeoLocked session key. The result is then encrypted using an asymmetric algorithm and conveyed to the recipient, much like that in the hybrid algorithm of Figure 3. On the recipient (i.e., decryption) side, GeoLocks are computed using a spoof-resistant GPS receiver for PVT input into the PVT-to-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 (i.e., Key_S).

PVT-to-GeoLock Mapping Function. Sidestepping for now the question of what constitutes an antispoof receiver, we will address how GeoLocks are formed. **Figure 5** shows a notional diagram of a PVT-to-GeoLock mapping function in which 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.

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 one-centimeter grid spacing if a standalone GPS receiver is being used. Conversely, if one is using an RTK-style receiver capable of two-centimeter 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. **Figure 6** shows the number of possible grid points on the planet as a function of grid spacing, ignoring altitude, time, and velocity.

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

- position (east, north, up components)
- velocity (east, north, up components)
- time
- coordinate system parameters.

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

The grid could just as well be based on the Military Grid Reference System or its close cousin, the Universal Transverse Mercator system. In fact, instead of a point, an area with any arbitrary shape could have been used. For example, the shape of the Disneyland theme park could map to a single GeoLock value to permit successful decryption when the user is located in the theme park but not when outside.

Finally, the PVT-to-GeoLock mapping function itself may incorporate a hash function — a one-way encryption function (which cannot be reversed) — with cryptographic aspects 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.

Antispoof Receivers. Most civil or nonmilitary GPS receivers are trivially easy to spoof or fool into determining erroneous positions: Simply hook up one of the many excellent signal simulators available, and the receiver will buy into whatever PVT values you want. This characteristic is why military receivers use

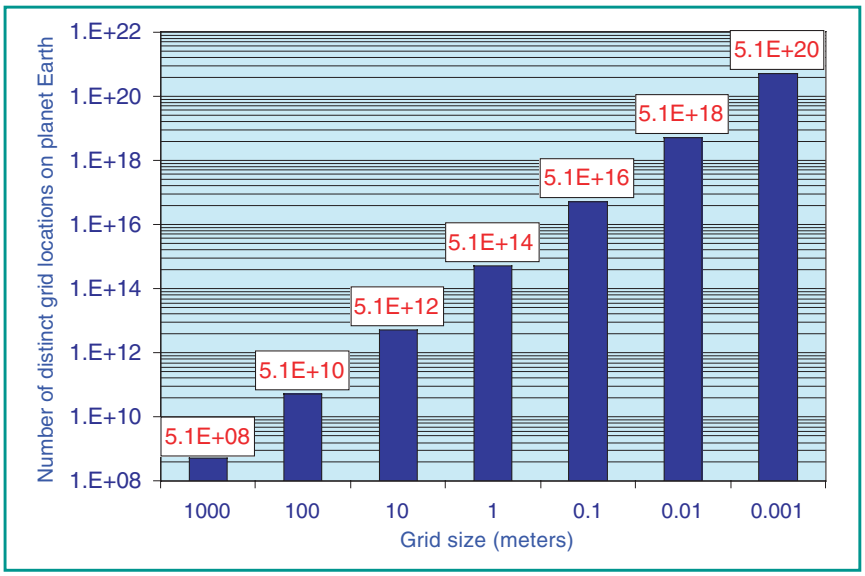


FIGURE 6 The number of distinct grid locations covering the earth's surface depends on the grid spacing.

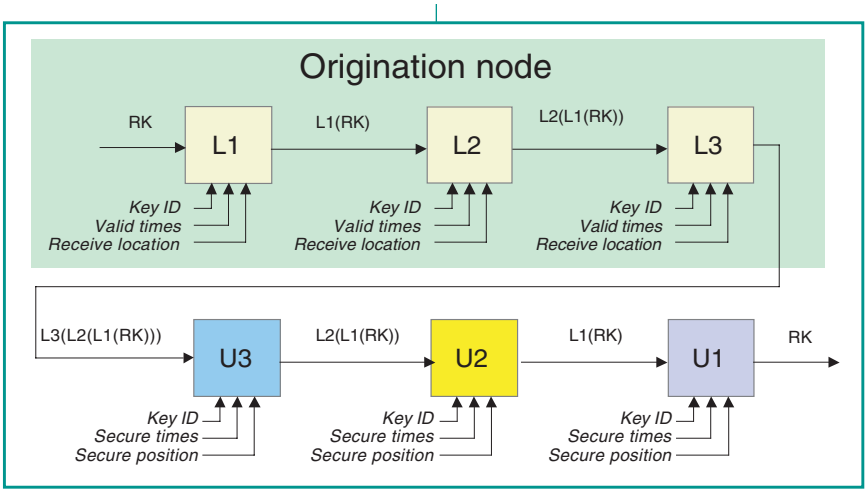


FIGURE 7 Successive geo-encryptions can force data to follow a specific geographic path.

the Y-code, which is an encrypted version of the P-code. Unless spoofers have access to the correct cryptographic keys and know how to generate Y-code from P-code, they can't spoof the military set. They may be able to jam it, but not spoof it.

Civil sets can be made difficult to spoof through a series of hardening measures. These include a variety of signals checks:

- Use a jamming-to-noise power ratio (J/N) meter to check for above-normal energy levels.
- Monitor carrier-to-noise-density ratio (C/N_0) for consistency or unexpected C/N_0 given J/N.
- Monitor the phase difference between antenna elements (all signals shouldn't come from the same direction).
- Use "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).
- Conduct continuity checks in time and position.
- Conduct consistency checks with other navigation sensors.
- Check for large residual errors, particularly in differential correction channel(s).
- Use receiver-autonomous integrity monitoring (RAIM)–type functions.

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

Relay Encryption. Successive geo-encryption can be used to force data and/or keys to follow a specific geographical path before they can be decrypted. This strategy is achieved by applying multiple GeoLocks 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.

Relay encryption might be useful for applications that use regional distribution centers for the distribution of data supplied by producers. For example, in subscription television the producers could be the television networks, and the distributors are cable or satellite television providers. A producer could first lock a key 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 GeoLock before broadcasting the programming to subscribers, who would then unlock the regional GeoLock and decrypt the ciphertext.

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 in which each traversed node in effect stamps the message with its PVT values.

Applications

To show how geo-encryption can be applied to real-world problems, we present two examples: digital cinema distribution and GPS receiver waypoint geo-encryption.

Digital Cinema Distribution. "Today, 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.," management consulting firm Booz Allen Hamilton reports in *Digital Cinema: Breaking the Logjam*. Although satellite-communications (SatCom) links provide a very efficient and cost-effective digital cinema distribution alternative, piracy is a major concern. SatCom links are easy to intercept. Direct Satellite Services satellite-to-home broadcasting is a good example. An estimated three million unauthorized users are reaping benefits from cloned versions of the tamper resistant smart cards that seek to prevent piracy. Furthermore, cinema stakeholders are risk adverse toward piracy on the basis of the music industry's

That is used with restrictive clauses, as I see “use regional distribution centers...” to be (the sentence wouldn’t mean the same without it).

When earth is preceded by “the,” no cap on earth.

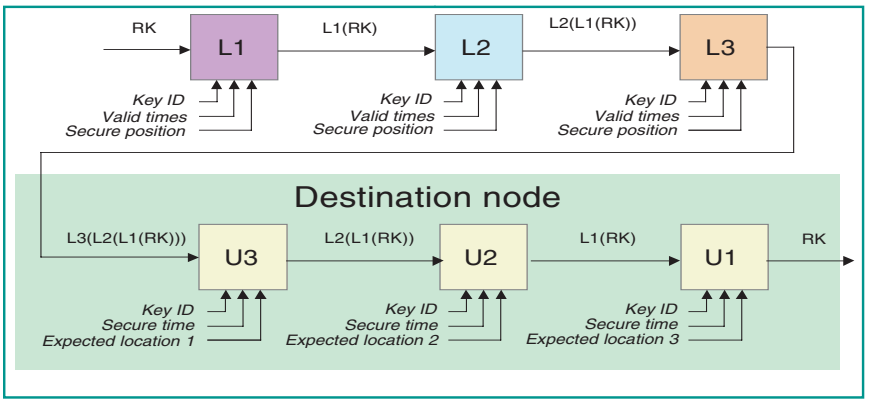


FIGURE 8 If it is important that a message follow a specific route from origin to destination, then at each node along the route, the message could be stamped with position, velocity, and time values.

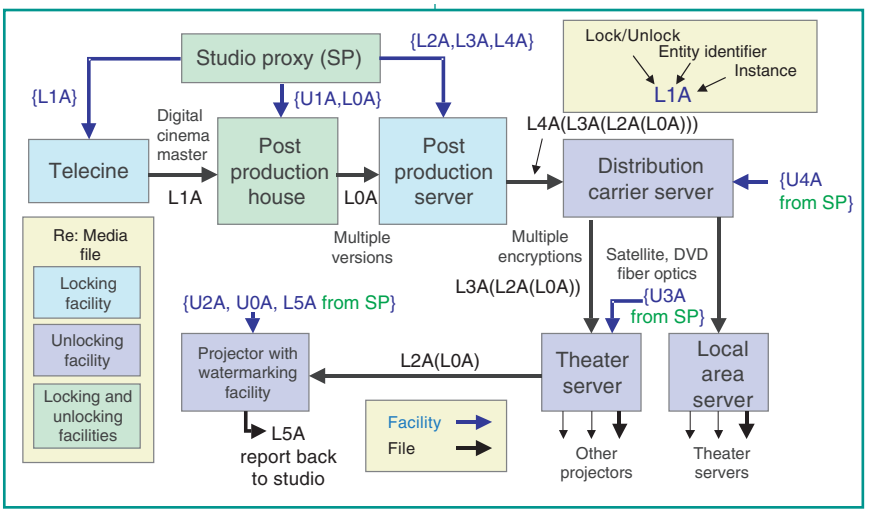


FIGURE 9 Geo-encryption can be used to enforce a studio control policy to ensure that only designated theater projectors at a specified location will be able to screen a film.

experience with "Napsterization." Music sales are down 8 percent, and company valuations are down 40 percent, largely because of piracy.

As a consequence, the cinema industry has shown 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 to develop security techniques specific to this industry.

In this application, the same large (i.e., 25 to 190 gigabytes) encrypted media file might be used at multiple theater locations nationwide but would have distinct GeoLocked keys specific to the intended recipient location and its exhibition license. This approach provides a secure and efficient point-to-multipoint distribution model applicable to distributions by means of satellite or DVD (formerly known as *Digital Video/Versatile Disk*). 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 in which a studio control policy is maintained. In this model, we start with the telecine, which produces the digital cinema (DC) master, an uncompressed, highest-resolution digital version taken from the film masters. The postproduction house assembles and converts the DC master into multiple versions, possibly for presentation and exhibition on a variety of media (e.g., theater, DVD, cable TV). A postproduction server then provides multiple encryptions of the various versions for distribution. Individual distributors are expected, but not required, to have their own servers to source their own facilities. Theaters receive copies of the media file in non–real time and store a copy on their local servers. The theater server then provides the still-encrypted media file to an authorized, tamper-resistant projector that contains sufficient buffering to source the real-time decryption and exhibition of the media file.

Placing four successive locks on the random key similar to those shown in Figure 7, the studio proxy can force the key to traverse the distribution carrier's server, which takes off its lock (U4A); the theater 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. 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 as well as time-of-transit expectations. In military applications, velocity and time-of-transit specifications are used for launching coordinated attacks in which 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
  - identification-friend-or-foe (IFF) parameters
- weapons parameters/restrictions
- crypto variables.

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

Figure 10 depicts a notional mission profile consisting of a series of waypoints for which we have defined regions of access for waypoints 2 and 3. There is no particular requirement that the PVT-to-GeoLock mapping function be based on a regular grid; in our example we have chosen polygonal shapes based on mission needs. Also, note that GeoLock regions can overlap; they do not have to be geographically disjointed from one another. Time and velocity window

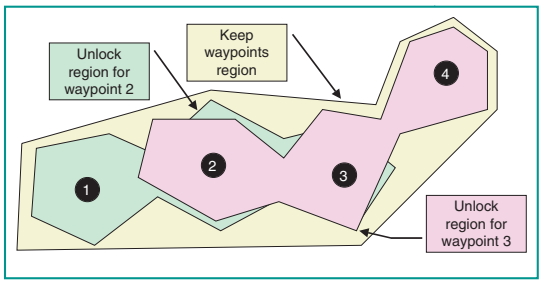


FIGURE 10 GPS waypoints can be geo-encrypted to secure mission information.

requirements could also have been imposed.

As an added refinement, we could also define a "keep waypoints" region, shown in yellow in Figure 10. If the set exits this area, perhaps due to capture, it can destroy its waypoints. Alternatively, it might display a different set of waypoints and routes, possibly with misleading descriptions. For example, it might display a route titled "Safe Route Through Minefield" that in fact leads over the mines. The set could also be configured to display an erroneous position when outside of its authorized area. Weapons systems with integrated GeoLock capability may refuse to fire — or worse — when outside of their authorized areas. The possibilities are limited only by the creativity of the mission planner.

Conclusion

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 in space. The system 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 individual implementations, it also can provide strong protection against location spoofing.

Acknowledgments

The authors would like to acknowledge the helpful commentary and discussions with our GeoCodex partners Mark Seiler, Barry Glick, and Ron Karpf. This article is based on a paper presented at The Institute of Navigation's National Technical Meeting held in Anaheim, California, January 22–24, 2003.

Further Reading

For a practical introduction to modern cryptography, see

- *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd ed., by B. Schneier (John Wiley & Sons, New York, 1996).

For an online introduction to cryptography, see

- *RSA Laboratories' Frequently Asked Questions About Today's Cryptography*, <http://www.rsasecurity.com/rsalabs/faq/index.html>.

For the seminal work on asymmetric encryption algorithms, see

- "New Directions in Cryptography," by W. Diffie and M.E. Hellman, *IEEE Transactions on Information Theory*, Vol. IT-22, November 1976, pp. 644–654.

For details of the Data Encryption Standard, see

- *Data Encryption Standard (DES)*, Federal Information Processing Standards Publication 46-3, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, Maryland, 1999. An online version is available at <http://www.itl.nist.gov/fipspubs/>.

For details on the Advanced Encryption Standard, see

- *Advanced Encryption Standard (AES)*, Federal Information Processing Standards Publication 197, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, Maryland, 2001. An online version is available at <http://www.itl.nist.gov/fipspubs/>.

"Innovation" is a regular column featuring discussions about recent advances in GPS technology and its applications as well as the fundamentals of GPS positioning. The column is coordinated by Richard Langley of the Department of Geodesy and Geomatics Engineering at the University of New Brunswick, who appreciates receiving your comments and topic suggestions. To contact him, see the "Columnists" section on page 2 of this issue.