Location-Based Authentication: Grounding Cyberspace for Better Security

Dorothy E. Denning and Peter F. MacDoran

Cyberspace is often characterized as a virtual world that transcends space. People log into computers and transact business electronically without regard to their own geographic location or the locations of the systems they use. A consequence of this lack of grounding in the physical world is that actions can take place over modems and computer networks without anyone knowing exactly where they originated.

Although this has not adversely affected many activities, it has caused numerous problems. It has been difficult to prevent unauthorized access to computer systems and to restrict access to privileged accounts and sensitive information. Finding the perpetrator of a computer intrusion or any crime in cyberspace has been extremely difficult and often impossible, especially when the perpetrator has looped through numerous machines throughout the world to get to a target. It is not unusual to read a news story such as the following, which appeared on 4 July 1995:

> SEATTLE (AP) — An Internet provider with about 3000 subscribers shut down after a computer hacker defeated security measures on the system. The electronic intruder entered the system through an Internet link in North Dakota, but his actual location is unknown...

This article shows how computer and network security can be substantially improved through a new form of authentication based on geodetic location. Location-based authentication has the effect of grounding cyberspace in the physical world so that the physical locations of network entities can be reliably determined. With location-based controls, a hacker in Russia would be unable to log into a funds transfer system in the United States while pretending to come from a bank in Argentina.

Location signatures

In grounded cyberspace, the physical location of a particular user or network node at any instant in time is uniquely characterized by a *location signature*. This signature is created by a *location signature sensor* (LSS) from the microwave signals transmitted by the 24 satellite constellation of the Global Positioning System (GPS). It can be used by an independent device to determine the geodetic location (latitude, longitude and height in a precisely defined geocentric coordinate reference system) of the LSS to an accuracy of a few metres or better. For reasons described later, the signature and its derived location are virtually impossible to forge. An entity in cyberspace will be unable to pretend to be anywhere other than where its LSS is actually situated.

A powerful security tool

Information security fundamentally depends on the ability to authenticate users and control access to resources. Existing user authentication mechanisms are based on information the user knows (e.g. password or PIN), possession of a device (e.g. access token or crypto-card), or information derived from a personal characteristic (biometrics). None of these methods are foolproof. Passwords and PINs are often vulnerable to guessing, interception, or brute force search.

Devices can be stolen. Cryptographic systems and one-time password schemes can fail even when the algorithms are strong. Typically, their security reduces to that of PINs or passwords, which are used to control access to keys stored in files or activation of hardware tokens. Biometrics can be vulnerable to interception and replay.

Geodetic location, as calculated from a location signature, adds a fourth and new dimension to user authentication and access control. It can be used to determine whether a person is attempting to log in from an approved location, e.g. a user's office building or home. If a user is mobile, then the set of authorized locations could be a broad geographic region (e.g. city, state, country). In that case, the login location serves to identify the place of login as well as to authenticate it. If unauthorized activity is detected, it will facilitate finding the individual responsible for that activity.

Authentication through geodetic location has many benefits. It can be performed continuously so that a connection cannot be hijacked, for example, if a user forgets to logout or leaves the premises without logging out. It can be transparent to the user. Unlike most other types of authentication information, a user's location can serve as a common authenticator for all systems the user accesses. These features make location-based authentication a good technique to use in conjunction with single sign-on. A further benefit of geodetic-derived location signatures is that they provide a mechanism for implementing an electronic notary function. The notary could attach a location signature to a document as proof that the document existed at a particular location and instant in time.

Unlike other authentication devices, a user's location signature sensor cannot be stolen and used elsewhere to gain unauthorized entry. The LSS will simply create a signature for the thief's location. In addition, intercepting the location signature transmitted during login does not allow an intruder to replay that data from some other place in order to the spoof the location and gain unauthorized entry. Further, location-based authentication does not require any secret information to protect at either the host or user end.

Geodetic location can be used to ensure that users can perform sensitive operations (e.g. switch to root, modify system files, or initiate electronic funds transfers) or access valuable information (e.g. company proprietary information, bank accounts, or medical information) only from approved physical locations (e.g. within a particular office building or set of buildings). It could be extremely valuable for authenticating financial transactions and remote control of critical systems. It could be used to prevent corporate secrets from being downloaded into employee homes or hotel rooms.

The use of geodetic location can supplement or complement other methods of authentication, which are still useful when users at the same site have separate accounts and privileges. Its value added is a high level of assurance against intrusion from any unapproved location regardless of whether the other methods have been compromised. In critical environments, for example, military command and control, telephone switching, air traffic control and banking, this extra assurance could be extremely important in order to avoid a potential catastrophe with reverberations far beyond the individual system cracked. In work environments where the principal threat is outsiders, the use of geodetic location combined with simple, fixed passwords might be sufficient.

"Information security fundamentally depends on the ability to authenticate users"

Geodetic location can be useful for locating the perpetrators of cyber crimes. One of the biggest obstacles to investigating computer intrusions is tracing an intruder back to a physical location so that an arrest can be made. If the intruder has looped through several hosts, it is necessary to get the cooperation of the system administrators operating each host in addition to the cooperation of the telecommunications carriers. With knowledge of the precise geodetic location of anyone logged in, the problem is readily solved.

In many cases, an intruder could be located and apprehended during a first attack, making it unnecessary to allow an intruder back into the system several times in order to conduct a trace. Knowledge of geodetic location can be used in other types of cases as well, for example, to find the originator of a fraudulent transaction, a libellous or harassing message, or a death threat. Moreover, the requirement to reveal physical location would itself be a deterrent to the commission of cyber crime because of the loss of anonymity. In addition, each of the sites through which a user passes

could add its own location signature so that the complete physical path is readily discernable.

Location information can provide evidence not only for the purpose of conviction, but also to absolve innocent persons. If illegal activity is conducted from a particular account by someone who has gained unauthorized access to that account, then the legitimate owner of the account may be able to prove that they could not have been present in the location where the activity originated.

A major threat to network security is spoofing of host computers. Location signatures can be used to prevent such spoofing and limit execution of certain protocols (e.g. for file transfer or program execution) to machines that are inside a security perimeter (e.g. a building or set of sites inside a network firewall). Location information effectively transforms any logical security perimeter defined by a set of host identifiers into a physical one defined by a set of geodetic locations. Even if a host name can be spoofed, its location cannot.

Enforcing export controls on software that is posted on a server is nearly impossible today because of the lack of reliable information about location. With location signatures, it would be possible to restrict access to persons within national borders. Similarly, it would be possible to control access to other information that is subject to national or regional controls, or to enforce site licences.

There are numerous defence and civil applications of GPS, including navigation (planes, boats, cars, missiles, etc.), fleet monitoring and surveying. Many of these applications depend upon computer networks, where they become vulnerable to spoofing and network intrusions. They will require a grounded cyberspace for security and safety and can be designed so that their use of GPS supports that goal. As described later, GPS receivers used for navigational purposes are not suitable for grounding cyberspace as they are readily spoofed.

The technology

International Series Research Inc. of Boulder, Colorado, USA has developed a GPS-based technology, called CyberLocator, for achieving location-based authentication (see *Figure 1*). An LSS, connected to a small antenna, computes the location signature from

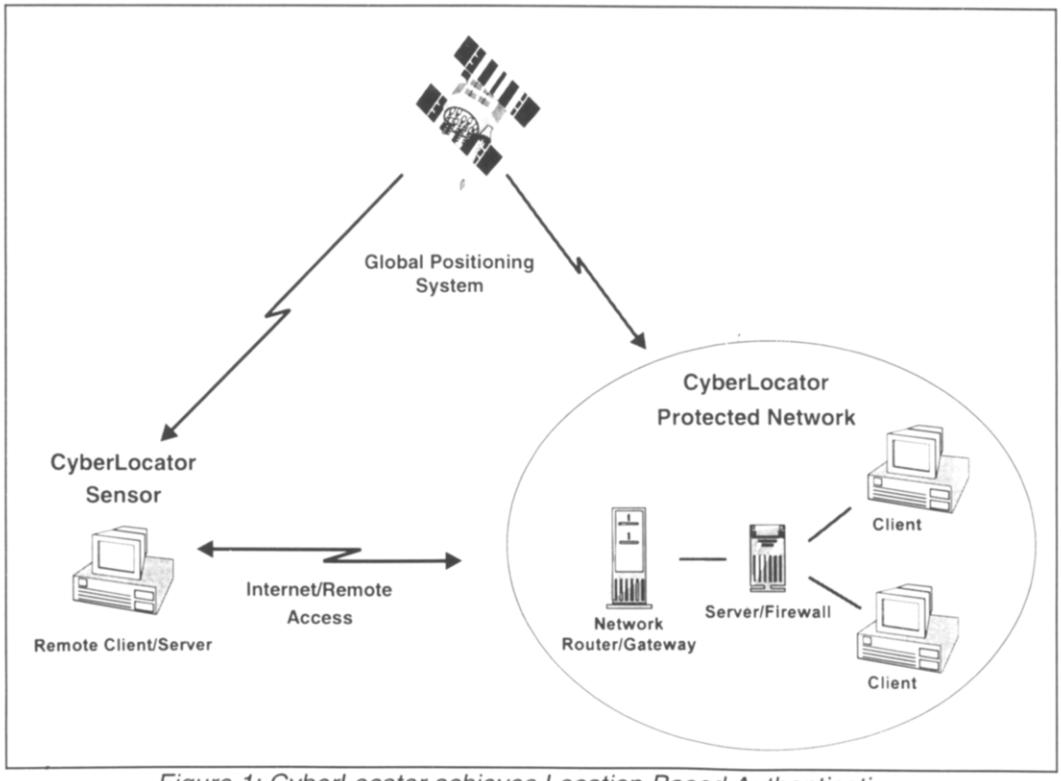

Figure 1: CyberLocator achieves Location-Based Authentication.

bandwidth compressed raw observations of all the GPS satellites in view (perhaps as many as 12 satellites). Because the signals are everywhere unique and constantly changing with the orbital motion of the satellites, they can be used to create a location signature that is unique to a particular place and time. As currently implemented, the location signature changes every five milliseconds. However, there are options to create a new signature every few microseconds.

When attempting to gain access to a host server, the remote client is challenged to supply its current location signature. The signature is then configured into packets and transferred to the host. The host, which is also equipped with an LSS, processes the client signature and its own simultaneously acquired satellite signals to verify the client's location to within an acceptable threshold (a few metres to centimetres, if required). For two-way authentication, the reverse process would be performed. In the current implementation, location signatures are 20 000 bytes. For continuous authentication, an additional 20 bytes per second are transferred. Re-authorization can be performed every few seconds or longer.

The location signature is virtually impossible to forge at the required accuracy. This is because the GPS observations at any given time are essentially unpredictable to high precision due to subtle satellite orbit perturbations, which are unknowable in real-time, and intentional signal instabilities (dithering) imposed by the US Department of Defense selective availability (SA) security policy. Further, because a signature is invalid after five milliseconds, the attacker cannot spoof the location by replaying an intercepted signature, particularly when it is bound to the message (e.g. through a checksum or digital signature). Continuous authentication provides further protection against such attacks.

Conventional (code correlating and differential) GPS receivers are not suitable for location authentication because they compute latitude, longitude and height directly from the GPS signals. Thus, anyone can report an arbitrary set of coordinates, and there is no way of knowing if the coordinates were actually calculated by a GPS receiver at that location. A hacker could intercept the coordinates transmitted by a legitimate user, and then replay those coordinates in order to gain entry. Typical code correlating receivers, available to civilian users, are also limited to 100 metre accuracy. The CyberLocator sensors achieve metre (or better) accuracy by employing differential GPS (DGPS) techniques at the host, which has access to its own GPS signals as well as those of the client. DGPS methods attenuate the satellite orbit errors and cancel SA dithering effects.

Application environments

Location-based authentication is ideal for protecting fixed sites. If a company operates separate facilities, it could be used to restrict access or sensitive transactions to clients located at those sites. For example, a small (7 cm x 7 cm) GPS antenna might be placed on the rooftop of each facility and connected by cable to a location signature sensor within the building. The sensor, which would be connected to the site's local area network, would authenticate the location of all users attempting to enter the protected network. Whenever a user ventured outside the network, the sensor would supply the site's location signature. Alternatively, rather than using a single sensor, each user could be given a separate device, programmed to provide a unique signature for that user.

"A major threat to network security is spoofing of host computers"

Location-based authentication could facilitate telecommuting by countering the vulnerabilities associated with remote access over dial-in lines and Internet connections. All that would be needed is a reasonably unobstructed view of the sky at the employee's home or remote office. Related application environments include home banking, remote medical diagnosis, and remote process control.

Although it is desirable for an antenna to be positioned with full view of the sky, this is not always necessary. If the location and environment are known in advance, then the antenna can be placed on a window with only a limited view of the sky. The environment

would be taken into account when the signals are processed at the host.

For remote authentication to succeed, the client and host must be within 2000 to 3000 kilometres of each other so that their GPS sensors pick up signals from some of the same satellites. By utilizing a few regionally deployed LSS devices, this reach can be extended to a global basis. For example, suppose that a bank in Munich needs to conduct a transaction with a bank in New York and that a London-based LSS provides a bridge into Europe. Upon receiving the location signatures from London and Munich, the New York bank can verify the location of the Munich bank relative to the London LSS and the London LSS relative to its own location in New York.

The technology is also applicable to mobile computing. In many situations, it would be possible to know the general vicinity where an employee is expected to be present and to use that information as a basis for authentication. Even if the location cannot be known in advance, the mere fact that remote users make their locations available will substantially enhance their authenticity. In his new book, *The Road Ahead*, Bill Gates predicts that wallet PCS, networked to the information highway, will have built-in GPS receivers as navigational assistants. With the CyberLocator technology, these PC receivers can also perform authentication while being a factor of 10 less expensive than conventional code correlating receivers (most of the processing is executed in the host rather than the remote units), which only achieve 100 metre accuracy, and a factor of a 100 less expensive than conventional DGPS receivers.

Privacy considerations

The use of location signatures has the potential for being used to track the physical locations of individuals. To protect their legitimate privacy interests, access to and the dissemination of geodetic information that has been collected for some purpose (e.g. login authentication) should be strictly limited. In fact, existing laws already control government access to such information. Government agencies must obtain subpoenas to get subscriber information (name, address, phone number, etc.) and court orders to get online transactional records (e.g. the addresses on electronic mail messages). Access in the private sector can be controlled through contracts and other commercial agreements or, if needed, through additional regulations.

Privacy can also be protected by using and retaining only that information which is needed for a particular application. Even though a geodetic location can be known at the metre level, for many applications, the location could be 'rounded', for example to a country level for the purpose of controlling transborder data flows.

A third safeguard would be to give users some control over the release of their geodetic locations, analogous to capabilities for 'opt-out' and caller-ID blocking. Such blocking could protect against misuse by persons who have no need for such information. Providing one's geodetic location could be voluntary, although some actions might be prohibited if location is not supplied (e.g. access to a particular system or transaction).

Summary

Location-based authentication is a powerful new tool that can provide a new dimension of network security never before possible. It can be used to control access to sensitive systems, transactions, or information. It would be a strong deterrent to many potential intruders, who now hide behind the anonymity afforded by their remote locations and fraudulent use of conventional authentication methods.

If the fraudulent actors were required to reveal their location in order to gain access, their anonymity would be significantly eroded and their chances of getting caught would increase. The CyberLocator technology is currently available in a portable concept demonstration.

Dorothy E. Denning is professor of computer science at Georgetown University, Washington, DC, and consultant to ISR. She can be reached on +1 202-687-5703 or denning@cs.georgetown.edu. Peter F. MacDoran is president and CEO of International Series Research Inc., Boulder, CO, USA. He can be reached on +1 303-447-0300 or pmacdorn@isrinc.com.