LA-UR- 97-2854

Approved for public release; distribution is unlimited.

Title: REMOTE MONITORING USING TECHNOLOGIES FROM THE INTERNET AND WORLD WIDE WEB

CONF-970744--

Author(s): JOHN M. PUCKETT
LENARD BURCZYK

Submitted to: 38th Annual Meeting of the Institute of Nuclear Materials Management, Phoenix, July 20-24, 1997

Los Alamos
NATIONAL LABORATORY

DISCLAIMER

REMOTE MONITORING USING TECHNOLOGIES FROM THE INTERNET AND WORLD WIDE WEB

John M. Puckett and Leonard Burczyk
Los Alamos National Laboratory, Los Alamos, New Mexico 87545 USA

Abstract

Recent developments in Internet technologies are changing and enhancing how we process and exchange information. These developments include software and hardware in support of multimedia applications on the World Wide Web. In this paper we describe these technologies as we have applied them to remote monitoring and show how they will allow the International Atomic Energy Agency to efficiently review and analyze remote monitoring data for verification of material movements. We have developed demonstration software that illustrates several safeguards data systems using the resources of the Internet and Web to access and review data. This Web demo allows the user to directly observe sensor data, to analyze simulated safeguards data, and to view simulated on-line inventory data. Future activities include addressing the technical and security issues associated with using the Web to interface with existing and planned monitoring systems at nuclear facilities. Some of these issues are authentication, encryption, transmission of large quantities of data, and data compression.

Introduction

> *We are on the verge of a revolution that is just as profound as the change in the economy that came with the industrial revolution. Soon electronic networks will allow people to transcend the barriers of time and distance and take advantage of global markets and business opportunities not even imaginable today, opening up a new world of economic possibility and progress.*
>
> *Vice President Albert Gore, Jr.*

On Tuesday, July 1, 1997, President Clinton and Vice President Al Gore announced a major blueprint for electronic commerce they are hoping will ensure the growth of worldwide Internet commerce. This plan, "A Framework for Global Electronic Commerce" (www.iitf.nist.gov/eleccomm/ecomm.htm), is the result of 15 months of work by an interagency task force and industry leaders. The plan addresses a wide range of issues including copyright protection, tariffs, trade, encryption, and content regulation. The potential for secure electronic commerce is indeed very large; in 1995, electronic commerce on the Internet was approximately two hundred million dollars (US). By 2010, it is estimated that electronic commerce will reach one trillion dollars. As this plan is incrementally implemented, it will further facilitate the already exponential growth of those industries that provide technology and services to the Internet infrastructure.

To the casual user, the World Wide Web and the Internet provide a useful, but often frustrating, experience. The explosive growth of the Internet over the past few years, with more than 50 million users accessing it a some level each week, leads many novice users to believe there must be a better, faster way to find the information they typically look for. The growth of the Internet is fueling an expansion of the telecommunications industry and many related service sectors and technologies. This telecommunications industry growth will result in a significantly better, faster, and more secure Web in the next few years. It is an interesting fact that two-thirds of commercial space launches planned for the next five years are related to telecommunications; a high percentage of these launches are related directly to extending the existing Internet infrastructure into space. The Internet and Web are a tremendous business opportunity for those participating in its development and growth; there is perhaps not a single industry that is not actively involved in using more technology of the Internet and Web for both private, corporate intranet and public Internet applications.

During the past several years Los Alamos has been closely following the wealth of technologies and standards emerging as a result of the dramatic growth of the Internet and its most popular application, the World Wide Web (WWW). Many of these technologies appear to be suitable candidates as building blocks for a standardized, secure safeguards remote monitoring architecture. Under the sponsorship of the International Safeguards Division (ISD) in DOE and working with Sandia National Laboratories, Aquila Technology Group[1] and other commercial vendors, Los Alamos developed a prototyping environment to merge data acquisition technology with the Internet and WWW technologies. The result is an

open web site that demonstrates how data can be collected, indexed, and made available to authorized individuals on a remote basis from any location in real-time. Using the WWW as a model, the data collection applications automatically build a set of indexed web pages using simple templates as a guide. Just as humans manually build pages for Web sites with authoring tools on their desktops, the data collection system automatically generates the same type of pages. The result is a working prototype (http://remo.lanl.gov) that provides an actual example of what is possible today with the application of these new technologies. It is anticipated that this web site will continue to be a test bed for other new technology and ideas and therefore will receive periodic updates for anyone to observe and operate. As we have demonstrated and discussed the new automated site over the past year, a number of frequently asked questions helped us to develop our focus. Four of these common questions are addressed in this paper.

In this paper we discuss how, when assembled carefully and applied systematically, a set of these key technologies can provide a secure, standardized method for remote monitoring in the area of nuclear safeguards. Connectivity remains the central issue in the design of a remote monitoring standard. We will provide an end-to-end example of how secure "quick-look" access methods can provide an almost instant connection for authorized users to any nuclear safeguards data system on a global basis. The intention of this design is not to replace the complete transfer of all data required for formal reconciliation (as it is done today) but rather to provide a quick, simple remote method to "look in" on a data system for reasons now required locally by an on-site facility officer. This type of approach provides a host of possible benefits for the security of a facility; safeguards system developers can look in from a distant location to observe how the system they have fielded is performing, including a look at state-of-health data. When a potential problem arises at the facility, the developer often can be very useful to an on-site facility officer if he can remotely access the system in question. In those cases of an alarm condition, a facility officer may need to be automatically notified when he is at home or away from the facility. A notification method is more useful if in includes a concise summary of questionable data. Both local (within several hundred miles) and remote (several thousand miles) systems can be automated to perform the quick-look authorized access in the same manner and based on the same set of standards and technologies from the Internet and WWW. Today at Los Alamos we are developing prototypes of the "Internet-in-the-Pocket" method for accessing our data systems remotely. The design is based on the integration of a number of technologies from the Internet and a key standard upon which the Internet is based: TCP/IP networking. Imagine having a small device in your shirt pocket that you can remove, turn on, press one button, and make an authorized connection to a safeguards data system anywhere on the planet in a manner of seconds. A very useful application of this type of connection arises during system testing, when the developers and users are located at some distance from the system under test. Remote connection serves a useful purpose for connecting to systems remotely during all the typical stages of development and testing that occur prior to final acceptance and installation, when connectivity may become more restricted but could also be implemented with the same standard TCP/IP network connection used during development and testing. The technologies for making this type of Internet-in-the-Pocket connection are becoming available today because of the continuing growth of the digital cellular telecommunications industry and the evolution of the Internet and WWW standards and technologies.

One of the real advantages of using WWW and Internet technologies and tools for remote access of safeguards data systems is that system functionality can be developed today for a terrestrial Internet; as Internet connectivity extends to space in the near future, the same technology can be used to reach locations not yet served by the terrestrial Internet infrastructure. TCP/IP protocol of the Internet will remain as the basic mechanism for data packet transfer. Prototyping a system that uses a digital cellular connection today will be easily extended to use the two-way space-based communications systems that will be available in the next several years. We are proposing to prototype, build, and test today with a standard phone line using PPP (Point-to-Point Protocol) for TCP/IP networks, and then deploy in near future by using the cellular satellite infrastructure extension of the Internet.

As we have implemented Internet-based data collections systems at Los Alamos over the past year we have heard questions that relate to the common concerns of our potential users. We will paraphrase four of these frequently asked questions and answer each one by relating it to a key area of technology used in our systems.

1. How will I obtain secure, remote access to safeguards systems in locations where the Internet access is not yet available, and secondly, how do I obtain better performance on access to those sites that are already connected to the Internet?

Space-based Internet technology

Geostationary satellites have provided commercial space-based telecommunications since the 1960s, primarily to interconnect economically developed urban areas. Today there are about 200 high-altitude telecommunications satellites. The geostationary satellite has inherent limitations for two-way communications, however, because of the significant signal delay caused by their high altitude (22,000 nautical miles). This distance, and the resulting transmission delay, means that a large number of applications, including interactive Internet applications such as the WWW, simply do not work over geostationary satellites. Because of their high altitude, geostationary satellites cannot provide fiber-like delays to be compatible with fiber-based networks on the ground.

High-altitude satellite constellations

The benefits of satellite constellation technology can be illustrated by describing a well known existing system. A high-altitude (11,000 nm) satellite constellation known as the Navstar Global Positioning Satellite (GPS) was developed by the US defense industry as a means of providing global navigation, mapping, and position information to the military. Public access to much of the GPS data has now been made possible by the US Government. GPS consists of 24 active satellites orbiting the earth every 12 hours. Four satellites are located in each of six orbits. With coverage of the entire globe, this system has essentially provided a unique "address" for every square meter on the planet. GPS receivers have been miniaturized to just a few integrated circuits making the technology accessible to virtually everyone. Today, using advanced features of GPS, measurements can be made to within a centimeter.

Low-earth-orbit satellite constellations

Low-earth-orbit (LEO) satellite systems orbit at a significantly lower altitude (typically about 400 nm) than the geostationary telecommunications systems and the GPS system. At this low altitude they can provide global access to the telecommunications infrastructure currently available in advanced urban areas of the developed world. Space-based networks are evolving from centralized networks relying on a single geostationary satellite, to distributed networks of smaller interconnected LEO satellites. Their low altitude eliminates the delay associated with geostationary satellites; these networks can provide communications that are compatible with existing terrestrial fiber-based standards such as the Internet.

Over the past few years, LEO systems have evolved from small systems that will provide the satellite equivalent of paging to those that will provide the satellite equivalent of Internet service. The next generation of these broadband LEO systems holds the potential to emulate and extend the Internet, providing the type of Internet "many-to-many" access, but as broadband communications that allow real-time capability and location-insensitive access. Because a constellation of LEO satellites moves in relation to the Earth, they can provide continuous coverage of any point on Earth. In order to provide service to the advanced markets, the same quality and quantity of capacity must be provided to the developing markets, including those areas to which no one would provide that kind of capacity for its own sake.

LEO satellite systems represent a technology that promises to radically transform the economics of the telecommunications infrastructure to enable universal global access to the Information Age beyond developed urban areas. Three LEO systems are particularly worth noting because they all have received Federal Communications Commission approval and are currently in various stages of financing and development.

IRIDIUM constellation: global wireless communications (www.iridium.com).

The IRIDIUM project has established global participation for what will be the first global cellular telecommunications satellite constellation. The IRIDIUM project is an international consortium of telecommunications and industrial companies financing the development of the IRIDIUM satellite system (see Fig.1).

Sponsors of IRIDIUM include Iridium Africa Corporation, Iridium Canada, Inc., Iridium China (Hong Kong), Ltd., Iridium India Telecom Limited, Iridium Middle East Corporation, Iridium SudAmerica Corporation, Khrunichev State Research and Production Space Center of the Russian Federation, Korea Mobile Telecommunications of Korea, Lockheed Martin and Motorola of the US, Nippon Iridium Corporation of Japan, o.tel.o communications bH of Germany, Pacific Electric Wire and Cable Co., Ltd. of Taiwan, Raytheon Company of the US, Sprint Corporation of the US, STET Group, Societa Finanziara Telefonica per Azioni of Italy, and Thai Satellite Telecommunications Co., Ltd. of Thailand.

IRIDIUM is a LEO constellation of 66 satellites being developed by Motorola at the Motorola Satellite Communication facility in Chandler, Arizona. IRIDIUM will be a global wireless personal telecommunications network designed to provide any type of telephone transmission, voice, data, fax, and paging to reach its destination anywhere in the world at anytime. A total of 17 IRIDIUM satellites have been launched successfully so far this year—five in May, seven in June, and five in July. These satellites are currently undergoing in-orbit testing. IRIDIUM services will be available to the public on a worldwide basis next year (1998). In undeveloped areas where even traditional telephone systems do not exist, IRIDIUM will provide governments and telecommunications providers with an economical alternative. The IRIDIUM connections will be symmetric, i.e., users will be able to send files back and forth quickly to and from any point on the planet. Cost of the IRIDIUM satellite constellation is estimated at $12.9 billion dollars. Motorola told the FCC that a comparable terrestrial network would cost more than one trillion dollars.

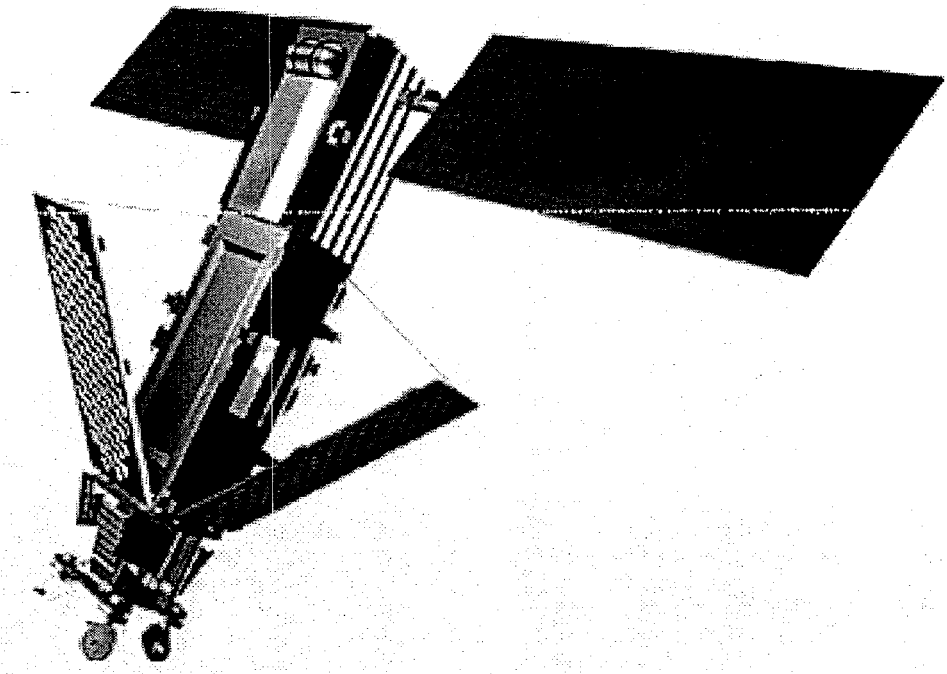

Fig. 1. The IRIDIUM satellite.

Teledesic: Internet-in-the-sky (www.teledesic.com).

The Teledesic Corporation has joined with Boeing Aerospace to undertake a venture several times larger than that of the IRIDIUM project. It is backed by two key individuals, Craig McCaw, the telecommunications pioneer who became a billionaire when he sold McCaw Cellular Communications to AT&T several years ago, and William Gates III, who is well known for the company he founded called Microsoft. The Teledesic Network will consist of a LEO constellation of several hundred small satellites being built for Teledesic by the Boeing Corporation. The Teledesic constellation will orbit the earth 50 times closer than the traditional geostationary satellites described earlier. This low orbit will eliminate the long signal delay normally experienced in satellite communications and enables the use of small, low-power antennas about the size of direct broadcast satellite dishes found on many residences today.

2. How do we enable safeguards instrumentation for remote access with standardized Internet protocols such as HTTP (HyperText Transfer Protocol) when a dedicated instrument such as a digital video camera may use only a very small (embedded) computer and not have the resources of a complete personal computer?

Embedded Internet device technology

Todays "information appliance" is the personal computer (PC). It often provides (serves) information to the WWW and allows access (browsing) as well. It is usually based on mainstream technology such as Microsoft's Windows NT®. This same information appliance for the WWW is many times found in today's nuclear safeguards systems as well; in fact, it is becoming a "de facto standard" technology for application in safeguards.

Manufacturers of the next generation of electronic devices of all types are motivated to connect their products to the Internet to take advantage of the wealth of information available on-line. The computer resources available on this next generation of devices vary widely across productivity products, consumer electronics, and industrial and manufacturing products and include products as diverse as pagers, handheld computers, industrial controls, gas pumps, and automobiles. Many of these non-PC devices are very limited in resources, including power, and are often created for a very specific purpose.

Web server technology is rapidly gaining acceptance of the preferred means of gaining access to a wide variety of products, including those types with small embedded computers, as mentioned above. Manufacturers of all types of devices are provided with a standardized means to access the device both in terms of the protocol used and the client-side

browser application. Small electronic devices that once could be accessed remotely only with some degree of difficulty and specialized software can now be accessed in a standard manner using Web server technology. This is due to the emergence of a new embedded class of Web server software products designed for very small, resource-limited devices.

Several Companies, including Spyglass (www.spyglass.com), have to date embedded web server software technology in a few hundred very small, specialized electronic devices. This is device-independent software that permits publishing and accessing information on the Internet using HTTP and HTML (HyperText Markup Language) in the form of a collection of lightweight portable ANSI C language components. The Spyglass MicroServer product provides a small footprint Web server with features necessary to support management and control of devices such as copiers, printers, hubs/routers, manufacturing equipment, and instrumentation. The server can serve multiple concurrent remote connections using as little as 36 KB of memory.

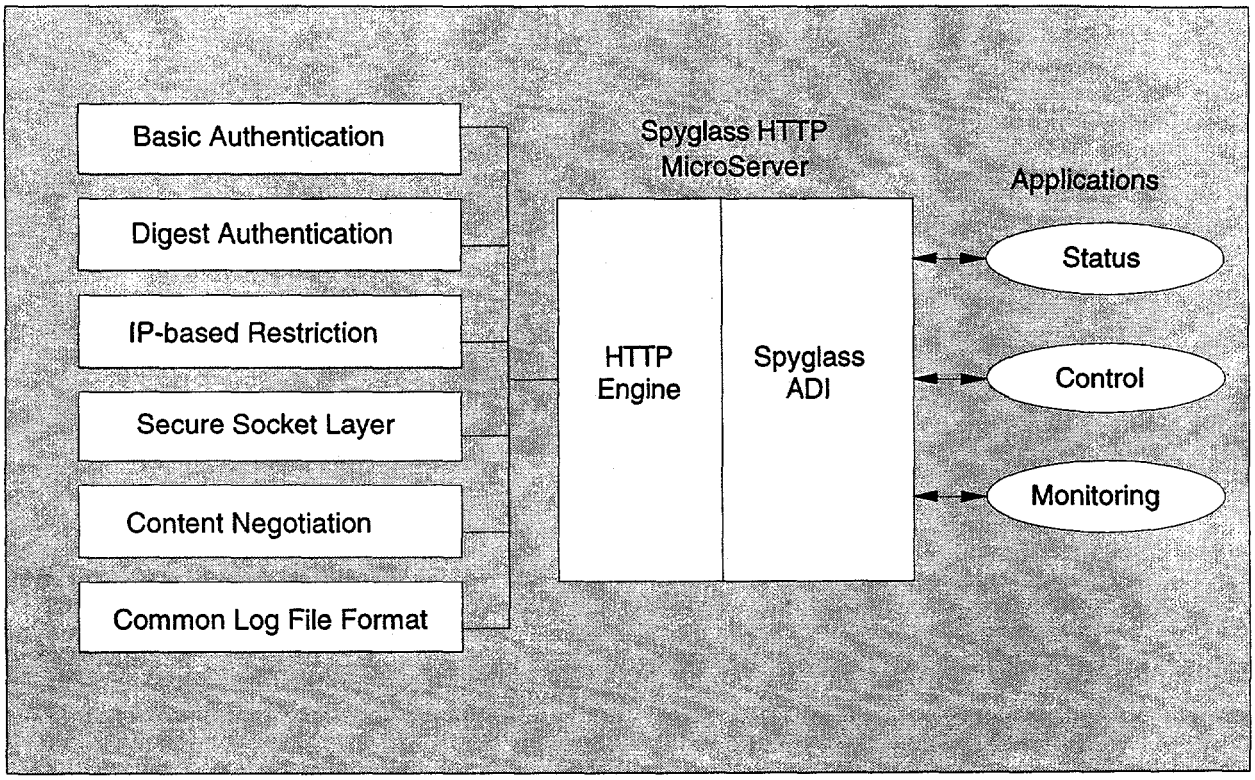

Fig. 2. Spyglass HTTP MicroServer Technology.

This same type of portable Web sever software could be embedded in all new and many existing safeguards instruments as a standardized software front-end for remote access. New instruments can be designed to take advantage of these emerging server technologies and by doing so can eliminate a more haphazard approach that results from the relative lack of connectivity standards that currently exists in the safeguards instrumentation community. Authorized, direct instrument access provides a wealth of benefits to the safeguards community including the timely access of data, shorter latency to correct malfunctions, and reduced development costs.

3. How do I obtain mobile, 24-hour authorized access to a specific safeguards instrument or data system when I am away from my office and do not have access to a personal computer?

The US Robotics (www.usr.com) PalmPilot™ organizer (see Fig. 3) is an Internet-ready handheld extension of the PC, rather than a miniaturized PC running a stripped-down version of a PC-type operating system. It has been designed to leverage the capabilities already found on the standard desktop PC, without forcing you to split information between a handheld device and the full-sized PC. With a TCP/IP protocol stack integrated into Palm OS, PalmPilot can support a variety networking applications. Applications may be added to the protocol stack by means of BSD UNIX Berkeley Sockets. Use of the standard socket mechanism allows reliable bidirectional transfer of data to take place. An authorized user cannot only observe the status of a remote data collection system but can also make adjustments to its controls, such as by adjusting a trigger level. PalmPilot supports a standard C language software development kit (SDK) from

Metrowerks (www.metrowerks.com) for adding custom data-collection applications like those being developed at Los Alamos. Running an operating system optimized for handheld devices, PalmPilot offers instant one-button access to data-collection applications. The PalmPilot handheld device and a data-collection computer are always synchronized with each other. PalmPilot Network HotSync™ technology automatically synchronizes information with a Windows NT® or Macintosh® PC at the touch of a button. You can synchronize your PalmPilot and data-collection PC from a remote location, using a dial-up link or a digital cellular data packet connection to the Internet or a wide area facility intranet.

Fig. 3. Internet-ready handheld PalmPilot™ for remote data system access.

This close coupling of a handheld organizer and a data-collection PC allows the two devices to work in tandem, with the PC taking on the processing and storage chores while the PalmPilot does the lighter weight remote viewing tasks. PalmPilot is a nonintrusive standards-based device that appears to be very powerful and flexible, yet requires minimal support. Optional "conduit" software allows PalmPilot to exchange information seamlessly with Windows NT® data-collection applications such as those being developed at Los Alamos. On Windows 95 or Windows NT development platforms, new conduits may be developed using Microsoft's Visual C++ programming environment and Microsoft Foundation Class libraries. The PalmPilot OS Conduit SDK contains all the Windows libraries and source files necessary to build Windows conduits, which run as Windows DLLs. Optional software also lets the user connect to their facility network, send and receive e-mail, and synchronize data remotely.

A Handheld Device Markup Language (HDML) specification, which is an extension of the HTML (HyperText Markup Language) used for Web applications, has been submitted to the World Wide Web Consortium for approval. Web browsers for handheld devices such as the Pilot are already in development by third-party developers. In just a few months, as the handheld browsers begin to appear, accessing a data system remotely using these handheld tools will be very similar to accessing a Web site using the Netscape or Microsoft Browsers on a PC.

PalmPilot features an intuitive graphical interface and a very simple and accurate text input system called Graffiti®. Using the PalmPilot's stylus, you can enter alphanumeric information if an application uses remote input. Or you can use PalmPilot's on-screen keyboard or the keyboard on your PC to enter data. Remote access data-collection and data-viewing applications at Los Alamos are being developed with a point-and-tap, menu-driven approach.

Developers can write new applications for PalmPilot that are launched from icons, or they can reprogram the control buttons on the PalmPilot by having new applications override the default functions. This customization capability makes PalmPilot attractive for remote-data-system access applications.

Internet access and remote access links are becoming increasingly important for handheld devices as facility networks add mobile communications support for their users. The infrastructure will soon be in place to provide a broad base of users with reliable, cost-effective services.

4. If a remote monitoring model for nuclear safeguards is based on technologies derived from the Internet and WWW, how do we provide the level of security required to guarantee only authorized remote access to sensitive nuclear safeguards data?

Digital Certificate (X.509) Server Technology (www.netscape.com).

On the Internet, information that is sent from one computer to another can pass through numerous other computers before it reaches its destination. Normally, the users of these intermediary computers do not monitor the Internet traffic routed through them, but someone who is determined can intercept and eavesdrop on any data, even conversations we consider private or, potentially more damaging, transmissions such as credit card exchanges. Even worse, they might replace our information with their own and send it back on its way. Because of the architecture of the Internet and intranets, there are ways for unscrupulous people to intercept and replace data in transit. Without security precautions, users may encounter security problems when sending information over the public Internet or a private intranet.

One major security problem is impersonation, where information passes to or from a person who poses as the intended recipient or as the sender of the message. The chances of impersonation can be reduced if people are required to authenticate (or verify their identities) before communicating information. On the Internet and intranets, commercial digital certificate technology is now being used to ensure that users or computers are really who they say they are. In this way, a certificate acts as a digital ID (like a badge or passport). When two machines try to establish a connection using the standard secure socket mechanism, they use their digital certificates as their identification for authentication. This is termed as a secure socket layer (SSL).To understand how digital certificates and the SSL work, we need to understand the concepts of public-key cryptography and digital signatures.

Public-key cryptography

Encryption is the process of using a mathematical algorithm to transform information into a format that cannot be read (this format is called ciphertext). Decryption is the process of using another algorithm to transform encrypted information back into a readable format (this format is called plain text). In order to ensure that other users cannot decrypt an encrypted message, we use a unique key to encrypt the message. Each unique key produces a different result when used to encrypt or decrypt a message. Unless others know the key that we used to encrypt the message, they cannot decrypt the message correctly.

Public keys and private keys

A public-key cryptosystem is a cryptographic system that uses a pair of unique keys (a public key and a private key). Each individual is assigned a pair of these keys to encrypt and decrypt information. A message encrypted by one of these keys can only be decrypted by the other key in the pair.

The public key is available to others for use when encrypting information that will be sent to an individual. For example, people can use a person's public key to encrypt information they want to send to that person. Similarly, people can use the user's public key to decrypt information sent by that person. The private key is accessible only to the individual. The individual can use the private key to decrypt any messages encrypted with the public key. Similarly, the individual can use the private key to encrypt messages, so that the messages can only be decrypted with the corresponding public key. Once the keys are assigned their use is transparent to the user. Figure 4 shows how the keys work.

RSA is the most widely used public-key cryptographic algorithm. Developed by RSA Laboratories (www.rsa.com), RSA provides methods for encrypting data using public and private keys. The current export restrictions imposed by the United States limit the exported versions of Internet software to support public keys to no longer than 512 bits (64 bytes). Within the US, Internet software will support up to 1024-bit (128-byte) keys. For testing Netscape software across national borders, we are currently limited to keys that are 512 bits long.

Digital Signature. The previous section describes a simplified example of how public keys can be used to verify that a specific person or organization sent the data. Digital signatures work in a similar way. Digital signatures provide the means to verify that the message was sent by the person who claims to have sent it and that the message was not altered between the time it was sent and the time it was received.

Digital Certificate. Because public keys are used for verifying digital signatures, it is important to make sure that a public key actually belongs to the specific individual or organization. We need to make sure that the key does not belong to someone impersonating the sender. A certificate is a digital document that validates that a public key and its corresponding private key are used in a transaction. The certificate belongs to a particular individual or organization. Certificates are issued by authorities who can vouch for the individual's or organization's identity and ownership of the public key. These authorities are called certificate authorities.

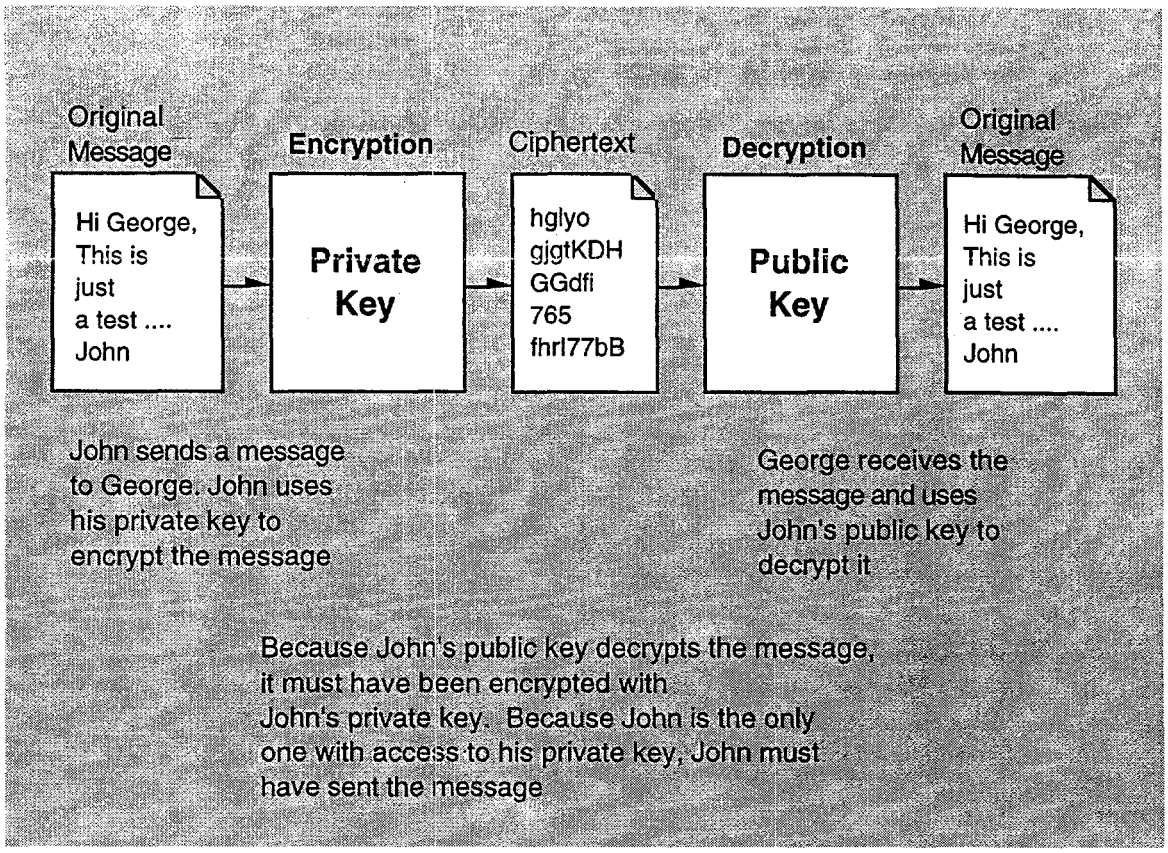

Fig. 4. Public-key cryptography.

Secure Sockets Layer. SSL is an industry-standard protocol that makes substantial use of public-key technology. SSL is widely deployed on private corporate intranets as well as on the public Internet in the form of SSL-capable servers and clients from vendors such as Netscape. SSL provides three fundamental security services, all of which use public-key techniques, as shown below.

Service	Underlying Technology	Protection Against
Message privacy	Encryption	Eavesdroppers
Message integrity	Message authentication codes (keyed hash functions)	Vandals
Mutual authentication	X.509 certificates	Imposters

The Netscape Certificate Server.

The Netscape Certificate Server (see Fig. 5) allows one to create, sign, and manage public-key certificates using a fully automated process. These digital documents certify an entity's ownership of a public key. Certificates issued by the Netscape Certificate Server comply with the X.509 standard. Figure 5 illustrates the different components of the certificate server and the different types of users who interact with it.

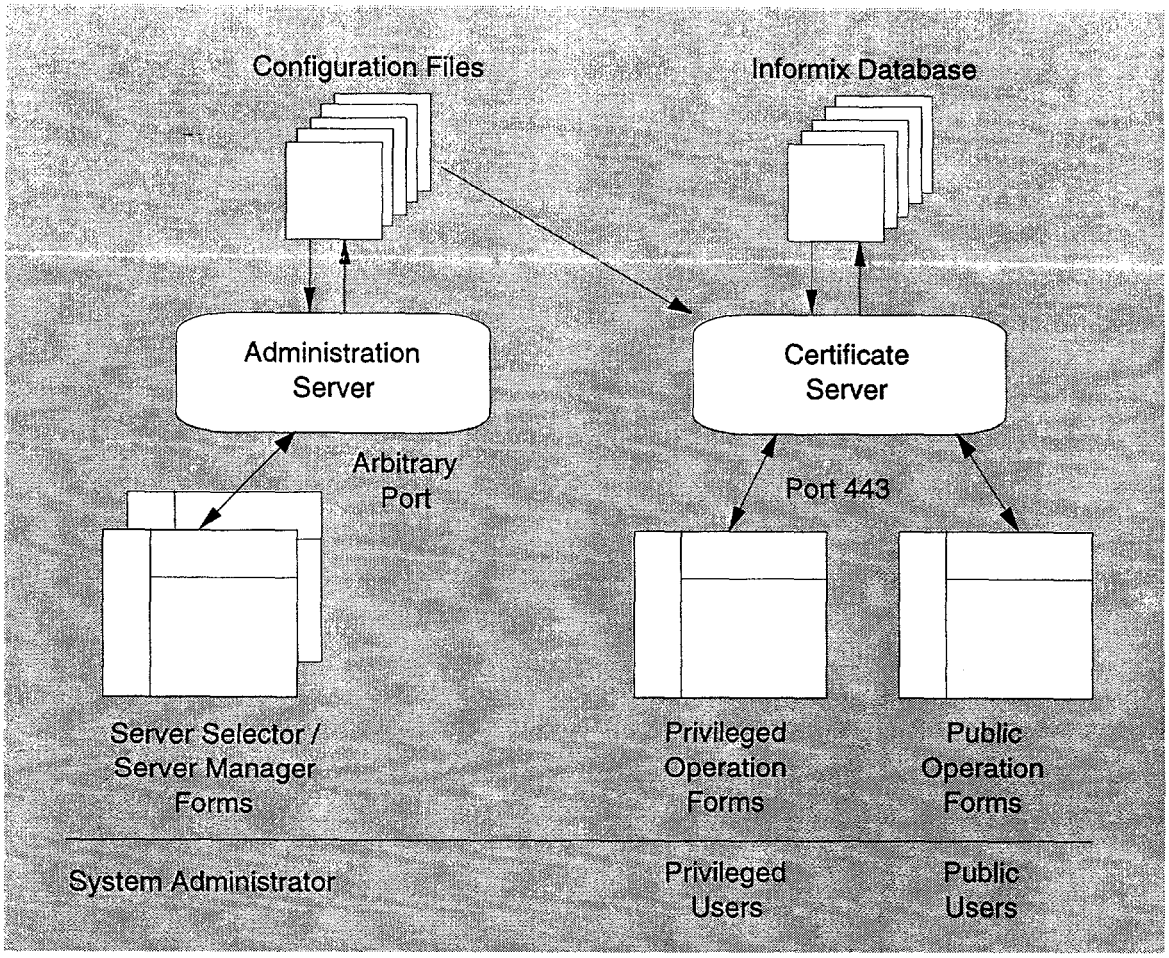

Fig. 5. The Netscape X.509 Certificate Server.

Summary

The continued geometric growth of the Internet and WWW, especially in the area of electronic commerce, is resulting in a wealth of new technologies that can be applied directly to remote monitoring for nuclear safeguards in a cost-effective manner. Four technologies in particular have been outlined in this paper as suitable candidates to facilitate the development of prototype components of a remote monitoring system: digital cellular connections to the existing Internet infrastructure, embedded HTTP software (e.g., SpyGlass MicroServer technology) for Internet-enabling of new and existing safeguards instrumentation, secure HTML browser-enabled handheld computing devices (e.g., the US Robotics PalmPilot™) that will permit Internet connectivity to be carried in one's pocket or briefcase and provide the ability to readily access any authorized safeguards data system on the planet, and X.509 digital certificate technology (e.g., the Netscape Certificate Server) that will automate security for remote connections. As space-based extensions to the Internet begin to appear in the next few years, the reach of a remote monitoring system based on the type of technologies discussed in this paper will offer a standardized, secure candidate method for remote access not yet available in nuclear safeguards.

Reference

1. Steven P. Kadner, et al., "A Remote Monitoring Testbed Facility," in this proceedings of the 38th annual INMM Meeting.