Unit IV

Information warfare

Information warfare is the tactical and strategic use of information to gain an advantage. It includes multiple types of operations and has been pursued in radically different ways during different eras.

Information warfare is also known as cyberwarfare, electronic warfare and cyberattack.

Types of information warfare include:

- Using viruses or malware for cyberattacks
- Exploiting holes in a network
- Stealing information through various types of unauthorized access

Information warfare (IW), or sneak electronic assaults, could easily crash power grids, financial networks, transportation systems, and telecommunications, among other vital services. The National Security Agency (NSA) traces the macro threat from hostile or potentially hostile governments as well as drug lords, criminal cartels, and increasingly computer-savvy guerrilla groups. Some of these rogue organizations are doing reconnaissance today on U.S. networks, mapping them, and looking for vulnerabilities.

The NSA is reportedly studying a rather imaginative arsenal of "info-weapons." Among the current possible offensive weapons are:

- ✓ Computer viruses, which could be fed into an enemy's computers either remotely or by "mercenary" technicians
- ✓ Logic bombs, another type of virus that can lie dormant for years, until, upon receiving a particular signal, it would wake up and begin attacking the host system
- ✓ Worms, whose purpose is to self-replicate ad infinitum, thus eating up a system's resources
- ✓ Trojan horses, malevolent code inserted into legitimate programming to perform a disguised function
- ✓ Back doors and trap doors, a mechanism built into a system by the designer to give the manufacturer or others the ability to sneak back into the system at a later date by circumventing the need for access privileges

Weapons of the future

Body count: 796. Cause: midair collision. The air traffic control system was "cybotaged." News reports indicate that FAA personnel complained that their radar screens were freezing and were switching data tags (such as aircraft altitude data) between close-flying

> planes, causing a series of near-misses in skies throughout the country— and one head-on collision between passenger jets in a thunderstorm over New York, resulting in the deaths of all aboard. It's suspected that the automated route and altitude management program's collision-avoidance algorithm was damaged.

Body count: 1,807. Cause: midair collision with a structure. The navigation system of another passenger jet was taken over by hackers, leaving the pilots helpless as the jet nose-dived into the Sears Tower in Chicago. No reports yet on how the hackers got in.

The Electromagnetic Bomb (E-bombs):

A Weapon of Electrical Mass Destruction Perhaps the most dangerous of all of defensive and offensive weapons in the IW arsenal of the future is the electromagnetic bomb. High-power EMP (electromagnetic pulse) generation techniques and high-power microwave (HPM) technology have matured to the point where practical E-bombs (electromagnetic bombs) are becoming technically feasible, with new applications in both strategic and tactical information warfare.

The development of conventional E-bomb devices allows their use in nonnuclear confrontations. This section discusses aspects of the technology base and weapon delivery techniques and proposes a foundation for the use of such devices in warhead and bomb applications.

The Technology Base for Conventional Electromagnetic Bombs

The technology base that may be applied to the design of electromagnetic bombs is both diverse and in many areas quite mature. Key technologies that are extant in the area are explosively pumped flux compression generators (FCGs), explosive or propellant driven magneto-hydrodynamic (MHD) generators, and a range of HPM devices, the foremost of which is the virtual cathode oscillator.

The Lethality of Electromagnetic Warheads:

The issue of electromagnetic weapon lethality is complex. Equipment that has been intentionally shielded and hardened against electromagnetic attack will withstand greater orders of magnitude and field strengths than standard commercially rated equipment.

Targeting Electromagnetic Bombs:

The task of identifying targets for attack with electromagnetic bombs can be complex. Certain categories of target will be very easy to identify and engage. Buildings housing government offices and thus computer equipment, production facilities, military bases, and known radar sites and communications nodes are all targets that can be readily identified through conventional photographic, satellite, imaging radar, electronic reconnaissance, and human operations. These targets are typically geographically fixed and thus may be attacked, providing that the aircraft can penetrate to weapon release range. With the accuracy inherent in global positioning system

(GPS)/ inertially guided weapons, the electromagnetic bomb can be programmed to detonate at the optimal position to inflict a maximum of electrical damage.

Mobile and relocatable air defense equipment, mobile communications nodes , and naval vessels are all good examples of this category of target.

The Delivery of Conventional Electromagnetic Bombs:

With explosive warheads, electromagnetic warheads will occupy a volume of physical space and will also have some given mass (weight) determined by the density of the internal hardware. Like explosive warheads, electromagnetic warheads may be fitted to a range of delivery vehicles.

An electromagnetic bomb delivered by a conventional aircraft can offer a much better ratio of electromagnetic device mass to total bomb mass, as most of the bomb mass can be dedicated to the electromagnetic-device installation itself.

Defense against Electromagnetic Bombs

The most effective defense against electromagnetic bombs is to prevent their delivery by destroying the launch platform or delivery vehicle, as is the case with nuclear weapons.

Limitations of Electromagnetic Bombs

The limitations of electromagnetic weapons are determined by weapon implementation and means of delivery. Weapon implementation will determine the electromagnetic field strength achievable at a given radius and its spectral distribution. Means of delivery will constrain the accuracy with which the weapon can be positioned in relation to the intended target.

The EMP (electromagnetic pulse) Effect:

EMP stands for electromagnetic pulse. The source can be a nuclear or a nonnuclear detonation. It can be used by Special Forces teams who infiltrate the enemy's territory and detonate a device near their electronic devices. It destroys the electronics of all computer and communication systems in a quite large area. The EMP bomb can be smaller than a HERF (High Energy Radio Frequency) gun to cause a similar amount of damage and is typically used to damage not a single target (not aiming in one direction) but to damage all equipment near the bomb.

The EMP effect was first observed during the early testing of high-altitude airburst nuclear weapons. The effect is characterized by the production of a very short (hundreds of nanoseconds) but intense EMP, which propagates away from its source with ever-diminishing intensity, governed by the theory of electromagnetism. The EMP is, in effect, an electromagnetic shock wave.

This pulse of energy produces a powerful electromagnetic field, particularly within the vicinity of the weapon burst. The field can be sufficiently strong to produce shortlived transient voltages of thousands of volts (kiloVolts) on exposed electrical conductors, such as wires, or conductive tracks on printed circuit boards, where exposed.

It is this aspect of the EMP effect that is of military significance, as it can result in irreversible damage to a wide range of electrical and electronic equipment, particularly computers and radio or radar receivers. Subject to the electromagnetic hardness of the electronics, a measure of the equipment's resilience to this effect, and the intensity of the field produced by the weapon, the equipment can be irreversibly damaged or, in effect, electrically destroyed.

The damage inflicted is not unlike that experienced through exposure to close proximity lightning strikes and may require complete replacement of the equipment, or at least substantial portions thereof.

Commercial computer equipment is particularly vulnerable to EMP effects, as it is largely built up of high-density metal oxide semiconductor (MOS) devices, which are very sensitive to exposure to high-voltage transients.

Computers used in data processing systems; communications systems; displays; industrial control applications, including road and rail signaling; and those embedded in military equipment, such as signal processors, electronic flight controls, and digital engine control systems, are all potentially vulnerable to the EMP effect.

Other electronic devices and electrical equipment may also be destroyed by the EMP effect. Telecommunications equipment can be highly vulnerable, because of the presence of lengthy copper cables between devices.

Snoop, sniff and snuff tools

Snoop and sniff tools

similr to wireshrk

A sniffer is a software or hardware tool that allows the user to "sniff" or monitor your internet traffic in real time, capturing all the data flowing to and from your computer.

Snoop is a tool that can be used for debugging and various trouble shooting purposes.

Sniffit is a kind of a network packet sniffer and snooper. Packet sniffers are rather intriguingly named pieces of software that monitor network traffic. Under many networking protocols, data that you transmit gets split into small segments, or packets, and the Internet protocol (IP) address of the destination computer is written into the header of each packet. These packets then get passed around by routers and eventually make their way to the network segment that contains the destination computer.

As each packet travels around that destination segment, the network card on each computer on the segment examines the address in the header. If the destination address on the packet is the same as the IP address of the computer, the network card grabs the packet and passes it on to its host computer.

Promiscuous Network Cards:

Packet sniffers work slightly differently. Instead of just picking up the packets that are addressed to them, they set their network cards to what's known as "promiscuous mode" and grab a copy of every packet that goes past. This lets the packet sniffers see all data traffic on the network segment to which they're attached—if they're fast enough to be able to process all that mass of data, that is. This network traffic often contains very interesting information for an attacker, such as user identification numbers and passwords and confidential data.

This data is also useful for other purposes. Network engineers use packet sniffers to diagnose network faults, for example, and those in security use packet sniffers for their intrusion detection software. That last application is a real case of turning the tables on the attackers: hackers use packet sniffers to check for confidential data; companies use packet sniffers to check for hacker activity. That has a certain elegant simplicity to it.

Snuff

As hackers obtain ever more dangerous and easy-to-use tools, they are being countered by novel defense strategies.

Deception Network

This so-called deception network is envisioned as more than just a single server set up to be a "honeypot," where hackers may break in, find a dead-end, and have their activities recorded with an eye toward prosecution.

Experts debate whether such nets will be worth the effort, but agree they can be a way to slow hackers long enough to sort the curious from the truly destructive "snuff." A group calling itself the Honeynet Project has quietly begun testing decoy networks on the Internet.

It is possible to create a deception network that has the same IP network address as your real network. Deception nets carry obvious administrative burdens, such as the need to generate realistic traffic to fool a hacker and maintain a network no one really uses.

Email Wiretaps

As part of its ongoing research, the Privacy Foundation (see sidebar, "The Privacy Foundation") found that a simple, hidden JavaScript code segment in HTMLformatted email messages can effectively allow someone to monitor all succeeding messages that are forwarded with the original message included. Clearly, this can cause confidential internal communications to be compromised. Here's a look at how to identify wiretaps and protect you from them.

The privacy foundation

The Privacy Foundation at the University of Denver conducts research into communications technologies and provides the public with tools to maintain privacy in the Information Age. You can read the Foundation's report and commentary on email wiretaps. The report cites the following possible uses for this security breach:

The wiretaps can provide the ability to monitor the path of a confidential email message and the written comments attached.

In a business negotiation conducted via email, one side can learn inside information from the other side as the proposal is discussed through the recipient company's internal email system.

A bugged email message can capture thousands of email addresses as the forwarded message is sent around the world.

Commercial entities, particularly those based offshore, may seek to offer email wiretapping as a service.

This security problem is a particularly dangerous one for organizations that conduct conversations containing sensitive internal information via email. The usual scenario for such communication is that a message from an outside source is forwarded from executive to executive within a company and it includes each person's comments.

If there's an email wiretap on the original external document, each time someone forwards the message to someone else, a copy of their message is automatically and invisibly emailed to the original sender of the external message (or someone designated by him). This problem affects only HTML-enabled email readers that have JavaScript turned on by default, such as Microsoft Outlook, Outlook Express, and Netscape Communicator.

Eudora and AOL are not affected, nor are Web mail services such as Yahoo and Hotmail.

Spy Dust Balls

Thousands of gossipy particles, each a tiny bundle of electronic brains, laser communications system, power supply, sensors, and even a propulsion system, could lurk all around, almost undetectable.

Scientists recently set up a network of small, wireless sensors called motes that detect birds as well as measure temperature, humidity, and barometric pressure. The battery-powered devices transmit their data by radio link to a solar-powered base station and then to the Internet. You can literally be anywhere in the world and know what's going on.

Tracking Tots

Cheap, dispersed sensors may tell farmers the exact condition of their acreage; manufacturers, the precise humidity and temperature history of their raw materials; parents, the locations and conditions of their small children all the time.

Climate-control systems in buildings would know exactly where it is too cold, humid, hot, or drafty. In five years, smart dust could be linked by satellite. Eventually, you could log on to readings from smart dust almost anywhere.

Poppy Seeds

Pister coined the label smart dust in 1996 and produced the first complete smartdust particle in mid-2002, about 1 millimeter on a side, or roughly between a poppy seed and a grape seed in size.

If a smart dust particle detects a tank going by, it could hop up and hitch a ride like a little spy. Some smart dust may be equipped with solar cells for power. Others might alight on vibrating machinery to soak up energy from the motion or charge batteries off electromagnetic pulsations leaking from power lines.

Sensors, at first, would be simple (such as for temperature, humidity, a few targeted chemicals, etc.), but eventually microphones and camera systems should be possible.

Mechanical Dragonflies

The military calls it "situational awareness": the ability to detect how many hostile tanks wait in the next valley or if bombed-out buildings are filled with snipers. It is an advantage that has proved difficult to attain: spies, satellites, and U-2s have all failed to keep commanders from blundering into ambushes and mismatches. The worst thing does just not know where the enemy is. It's having the sense that somebody's out there trying to get you but having no idea of where the enemy might be.

The researchers envision tomorrow's soldiers coming to a hill, halting, and reaching into their packs for cigar-shaped tubes. From every tube emerges a robotic spider, or a robotic dragonfly, each no longer than 3 inches.

Equipped with cameras or acoustic sensors, the mechanical insects range forward and provide data on the hazards that lie in wait on the other side: the number of machine gun nests and the position of artillery.

Recently, the researchers built their first crawling bug prototypes, and they aim to perfect the design within two years. Insect-shaped "micro aerial vehicles" are next on the slate.

In most robotic systems today, people think that if you want to move one joint, then you need to attach a motor at that joint. That makes for large, bulky, energyhog robots. It also reduces robots to the ranks of expensive toys.

Motors are only about 80% efficient in turning electrical power into movement, so, although robots may impress with their futuristic looks, most motor-driven devices have ranges limited to only a few dozen yards, rendering them useless for practical applications.

Nano Technology

Nanotech takes its name from the nanometer, a unit of measurement just one billionth of a meter long. Nano-bombs are molecular-size droplets, roughly 1/5,000 the head of a pin, designed to blow up various microscopic enemies of mankind, including the spores containing the deadly biological warfare agent anthrax.

Since 1999, a series of breakthroughs have transformed nanotech from sci-fi fantasy into a real-world applied science and, in the process, inspired huge investments by business, academia, and government. In industries as diverse as health care, computers, chemicals, and aerospace, nanotech is overhauling production techniques, resulting in new and improved products—some of which may already be in your home or workplace.

Silicon Fingers

Meanwhile, nearly every week, corporate and academic labs report advances in nanotech with broad commercial and medical implications. In 2000, for example, IBM announced it had figured out a way to use DNA to power a primitive robot with working silicon fingers 1/50 as thick as human hair. Within a decade or so, such devices may be able to track down and destroy cancer cells.

At Cornell University, researchers have developed a molecule-sized motor, built out of a combination of organic and inorganic components. Because of nanotech, all of us will see more change in our civilization in the next 30 years than we did during all of the 20th century.

Shrinking all the information housed at the Library of Congress into a device the size of a sugar cube or detecting cancerous tumors when they are only a few cells in size.

To build such objects, engineers employ a wide range of techniques, borrowed from bioengineering, chemistry, and molecular engineering. Such feats include imitating the workings of the body, where DNA not only programs cells to replicate themselves but also instructs them how to assemble individual molecules into new materials such as hair.

Atom by Atom

Starting in the Stone Age, all human technology, from sharpening arrowheads to etching silicon chips, has involved whittling or fusing billions of atoms at a time into useful forms.

In 2000, the chief scientist at Sun Microsystems created a stir when he warned that in the wrong hands, nanotech could be more destructive than nuclear weapons.

Using a tool known as a molecular beam epitaxy, scientists have learned to create ultrafine films of specialized crystals, built up one molecular layer at a time. This is the technology used today to build read-head components for computer hard drives.

Natural Motion:

The next stage in the development of nanotechnology borrows a page from nature. Building a supercomputer not bigger than a speck of dust might seem an impossible task, until one realizes that evolution solved such problems more than a billion years ago. Living cells contain all sorts of nanoscale motors made of proteins that perform myriad mechanical and chemical functions, from muscle contraction to photosynthesis. In some instances, such motors may be re-engineered, or imitated, to produce products and processes useful to humans.

Animals such as the abalone, for example, have cellular motors that combine the crumbly substance found in schoolroom chalk with a "mortar" of proteins and carbohydrates to create elaborate, nano-structured shells so strong they can't be shattered by a hammer. Using a combination of biotechnology and molecular engineering, humans are now on the verge of being able to replicate or adapt such motors to suit their own purposes.

Future Phenomena:

Where will it all end? Many futurists have speculated that nanotech will fundamentally change the human condition over the next generation. Swarms of programmable particles, sometimes referred to as "utility fog," will assemble themselves on command.. Meanwhile, new, superstrong, lightweight nanomaterials could make space travel cheap and easy as some scientists predict, nanotech can be used to create an Earth-like atmosphere on Mars.

Space colonization could well be necessary if the new science of "nanomedicine" extends life indefinitely, manufacturing new cells, molecule by molecule, whenever old cells wear out. It all seems hard to imagine, yet nanotech has already produced enough small wonders to make such big ideas seem believable, if not alarming at least to the high priests of science and the IW military strategists.

Surveillance tools for Information warfare in future

Wireless systems capable of monitoring vehicles and people all over the planet are leaving businesses and the military aglow with new possibilities and some privacy advocates deeply concerned. Companies seeking to tap the commercial potential of these technologies are installing wireless location systems in vehicles, hand-held computers, cellphones—even watchbands. Scientists have developed a chip that can be inserted beneath the skin, so that a person's location can be pinpointed anywhere.

For example, the owner of a small company in Dallas that installs automobile alarms uses a wireless tracking service to monitor his fleet of six Dodge Dakota pickup trucks, and the equipment alerted him recently when one of his trucks turned up in the parking lot of the Million Dollar Saloon, a strip club. When he signed up for this service, he told his guys, “Big Brother’s keeping an eye on you, and I’m Big Brother.” After he fired that one fellow, you bet they all believed him. These technologies have become one of the fastest-growing areas of the wireless communications industry.

Monitoring Everything

A federal effort to make it easier to pinpoint the location of people making emergency 911 calls from mobile phones means that cell phones sold in the United States are now equipped with advanced wireless tracking technology.

Although satellite-based global positioning system (GPS) technology has been commercially available for some time for airplanes, boats, cars, and hikers, companies have only recently begun manufacturing GPS chips that can be embedded in wireless communications devices. GPS uses satellite signals to determine geographic coordinates that indicate where the person with the receiving device is situated.

Real-life improvements in the technology have come largely from research initiatives by start-up companies in the United States, Canada, and Europe as well as from large companies like IBM, which recently formed a “pervasive computing” division to focus on wireless technologies such as location-based services.

Cyber footprint and criminal tracking

At 10:00 A.M. one morning in 1999, an elderly woman in Osaka, Japan, became alarmed. Her 74-year-old husband, who suffers from dementia, had left four hours Surveillance Tools for earlier and had not yet returned. She did not panic, but contacted the provider of her personal locator service, Life Service Center.

Within a minute, the provider found him on the second floor of a department store, simply by paging a miniature locator device secured to the man’s clothes. Forty minutes later, when the man’s son arrived at the department store, his father had already left. Fortunately, the service provider continued tracking the elderly man and was able to direct the son to the fourth floor of an Osaka hotel.

At 1:10 P.M., the two were reunited. Locus Corp. provided the system that made this possible.

The belief that it should be easy to find anyone, anywhere, at any time with a few pushes of a button has caught on with the advent of the GPS. People imagine a miniature device, attached to one’s person that reports one’s whereabouts almost instantaneously. Add the highly practical need to find missing persons promptly, and the personal locator system (PLS) industry is born.

Systems of this nature, whether based on the GPS or some other technology, are being tested throughout the world. Some are already being deployed in Japan.

The service alone can be sold by cellular companies, which base it on their wireless infrastructure. Several companies looking into the technology options plan to offer a broad array of services to the public and to businesses.

In Japan, location services are now commercially available to 74% of the nation's population, including Tokyo, Osaka, Kyoto, Yokohama, Nagasaki, and Hiroshima. Initially designed to support the mentally handicapped, personal locator services have expanded to serve children, the elderly, tourist groups, and security patrols, as well.

They may also be used to track valuables and recover stolen vehicles. Not surprisingly, service areas coincide with wireless infrastructure deployments, which personal locators have exploited since their beginning in 1998.

In the United States, two further factors encourage the adoption of these geolocation systems. One is the need to effectively monitor offenders on parole and probation. Tagging offenders with locator devices would tighten their supervision and enhance public safety and could even reduce the prison population. The other is the wish to provide wireless callers with enhanced 911 (E-911) emergency services. For land-line telephony, the location of a phone from which a 911 call is made appears automatically on the 911 operator's computer screen. Callers using cellular phones could be anywhere and unlocatable, unless location technology were applied to the wireless telephone system.

One PLS Architecture

A PLS is likely to involve a service provider, a location center, and a wireless network. In this setting, three scenarios, each involving a different operating mode, are possible. The person bearing a locator device is either being sought by a subscriber to the service, is seeking help from the subscriber, or, as in the case of a parolee, is having his or her whereabouts monitored continuously.

Consider again the introductory example, but from a system architecture perspective. It is representative of the first scenario, based on the paging mode, wherein the person with the locator device is sought. In this instance, the subscriber calls the service provider, giving the operator there a password and the "wanted" person's identification (user) number (ID). The operator enters the ID into a computer, which transmits it to another computer at the location center. That machine calls the locator device, in effect paging it to establish communication through the PHPS (personal handy phone systems) wireless telephone switching office. Immediately the office forwards the call to the wireless base station nearest the locator.

Once communication is established between the center and the device, the center asks the device for the signal strength data and IDs of any base stations in its vicinity. The locator replies, and from those inputs, plus RF database information on the base stations, the center computes the locator's coordinates.

These coordinates are transmitted to the service provider's computer, which displays the missing person's position on a street map for the service operator to report to the subscriber. The user's location is continuously updated on the service provider's map as long as the location center maintains its call connection to the locator device.

In a second scenario, involving the emergency mode, the user of the locator is lost or in dire straits of one sort or another and presses the device's panic button. The locator calls the location center, which computes the user's position and alerts the service provider, which in turn alerts the subscriber to the user's situation.

The system can employ either packet data or voice channel communications. If a data channel is used, the service takes about 8 seconds to obtain a geolocation fix. If a voice channel is used, the wait could last up to 33 seconds because of processing differences between the two channel types.

Six Technologies

A PLS (personal locator system) could use any of several technologies. Among the most common methods are angle and time difference of the signal's arrival, GPS and the more recent assisted GPS, enhanced signal strength, and location fingerprinting.

Signal Direction

The simplest technology is based on measuring the direction of a signal received from an RF transmitter at a single point. This can be done by pointing a directional antenna along the line of maximum signal strength. Alternatively, signal direction can be determined from the difference in time of arrival of the incoming signals at different elements of the antenna. A two-element antenna is typically used to cover angles of ±60 degrees. To achieve 360-degree coverage, a six-element antenna can be used.

Signal Times of Arrival

Similarly, the time difference of arrival (TDOA) between signals received at the geographically disparate antennas can be used to determine position. Given the speed of light and known transmit and receive times, the distance between the mobile locator and receiver antenna can be calculated.

Global Positioning System

As previously explained, a GPS relies on a constellation of 24 satellites. It, too, employs signal timing to determine position, but the mobile locator is a receiver and the orbiting satellites are transmitters. The satellites transmit spread-spectrum signals on two frequency bands denoted L1 (1575.42 MHz) and L2 (1223.6 MHz). The signals are modulated by two pseudorandom noise codes, the precision (P) code, and coarse/acquisition (C/A) code. The GPS signal is further modulated with a data message known as the GPS navigation message.

To acquire the satellites' signals, the GPS receiver generates a replica of the satellites' pseudorandom noise codes. The GPS navigation message can be demodulated only if the replica can be matched and synchronized with the pseudorandom noise codes received. If the receiver cannot match and synchronize its replica, the GPS signal appears to the receiver as noise. Matching the pseudorandom noise codes and using the satellites' navigation message also enables the receiver to calculate the signal transmit time as well as the coordinates of the satellites.

Server-Assisted GPS

To combat the shortcomings of GPS, an innovative technique known as "serverassisted GPS" was introduced in 1998. The idea is to place stationary servers throughout the area of coverage to assist mobile receivers to acquire the GPS signals. In effect, the servers are stationary GPS receivers that enhance the mobile GPS receiver's capabilities by helping to carry their weak signals from satellites to locator. The server includes a radio interface for communicating with the mobile GPS receiver and its own stationary GPS receiver, whose antenna has full view of the sky and monitors signals continuously from all the satellites within view.

Enhanced Signal Strength

If no obstructions are present, computing the position of a mobile locator is straightforward for both the signal timing and signal strength methods. When timing is used, the speed of light multiplied by the time signal takes to propagate between the two points gives the distance between them.

For the signal strength method, the distance between two points can be determined from the signal attenuation between the points. However, direct line contact seldom exists inside buildings, where signal attenuation is usually unknown and many indirect paths between transmitter and receiver are likely.

Location Fingerprinting

To determine the position of a mobile transmitter, the RadioCamera system matches the transmitter's signal signature to an entry in the database. Multipoint signal reception is not required, although it is highly desirable. The system can use data from only a single point to determine location. Moving traffic, including vehicles, animals, and people and changes in foliage or weather do not affect the system's capabilities.

Implications of cookies and integrated platforms

Cookies have benefits and drawbacks. Used properly, they can enhance a visitor's experience of a Web site. Used carelessly, they can poison a user's impression of a site and even prompt some users to stay away forever.

All Web site integrated platform designers will eventually face the question of whether and how to use cookies. Often, designers find themselves ill-equipped to make this decision and so they employ cookies haphazardly or without regard for user acceptance or data privacy.

A Cookie in a Nutshell

When a visitor views a Web page, the server can assign that visitor a unique customer ID, known as a cookie. The server asks the visitor's browser program to "accept" the cookie—to save the ID number on the visitor's computer. Then the browser sends the cookie back to the Web server each time the visitor returns to that page, or in some cases, to any page on the Web site. The ID number tells the server that the visitor has visited the site in the past. The server can use the ID number as a key to store any information the visitor has provided in past visits, or any details it has observed about the visitor's preferences or browsing behavior. The ID number can save a visitor from having to repeatedly log-in to a members-only site on each visit.

Why Cookies Provoke Controversy

Cookies (like any powerful data-gathering tool) can be abused. Many users fear, sometimes justifiably, that a cookie they accept may allow unscrupulous Web site operators to gather information about them and then use that data in an unauthorized manner. These users set their browser software to warn them of each incoming cookie—and many users reject every cookie, without exception.

Poor Support of Cookies in Browsers

Part of the climate of mistrust surrounding cookies stems from the poor cookie interface provided by current Web browser software. Both Netscape and Microsoft browsers can consult users before accepting a cookie, and many users choose to browse with this preference turned on. Currently, a visitor who rejects a cookie on a Web site integrated platform but continues to browse experiences a relentless barrage of cookie requests. Often, even visitors who accept a cookie are still bombarded by offers of more cookies from the same site. On many sites, this badgering can include multiple cookies per page, cookies that change gratuitously even once accepted, and cookies on pages that don't even require cookies for any apparent reason. As feedback from users reaches the designers of browser software, look for browsers to add the following features to help users cope with this overuse of cookies.

1. Reject all cookies option
2. Better choices when asked
3. Cookie management tools

Reject All Cookies Option

Today, browsers present only the annoying false choice between “Accept all cookies without asking” and “Ask about each cookie.” Users should expect to see these choices expanded to include a third “Reject all cookies without asking” option.

Better Choices When Asked

For users who choose notification, browsers should offer a more flexible set of choices regarding what happens after a cookie has been accepted or rejected. Specifically, the user should be able to say “I want to accept/reject this cookie, and then don’t ask me again...”

- About this particular cookie on this Web site integrated platform
- About any cookie on this Web site integrated platform
- About any cookie on this page

Cookie Management Tools

Finally, expect to see browsers offer a mechanism that lets users view and manage the set of cookies they’ve collected. Certain browsers, such as the most recent release of Microsoft Internet Explorer, have begun to add these or similar cookie management features. Until a majority of common browsers have incorporated these options, integrated platform designers should plan to minimize the number and type of cookies a visitor encounters on a site.