

Wireless LAN Links Ammo Outpost To Base

Federal Computer Week
By Dan Caterinicchia
April 2, 2003

CAMP ARIFJAN, Kuwait — Within the past week, Army logistics specialists have connected an ammunition outpost more than two miles away via a secure, wireless local-area network that enables basic Internet access and the automatic downloading of critical information back to the base.

The Combat Service Support Automated Information System Interface (CAISI) is a wireless LAN that provides "last-mile connectivity" between combat service support computers and the base network.

Jose Ilarraza, a logistics management specialist here from the Combined Arms Support Command, Fort Lee, Va., said the remote ammunition outpost had no communications capabilities prior to the March 26 establishment of CAISI. The self-healing network uses an 11-megabit "pipe" FTP for transferring data, and has omnidirectional antenna and encryption at both ends.

"Because we're dealing with ammo, the importance of this information increases" up the chain of command, Ilarraza said.

Staff Sgt. Daniel Peters, stock control noncommissioned officer in charge of the theater storage area, said before the CAISI hook-up, his staff had to save the ammunition data on a disk and then drive about 30 minutes to hand-deliver it to the required location on base.

"The disk creates errors, but now we can do everything automatically" on the Standard Army Ammunition System-Modernization (SAAS-Mod), Peters said. "It's like using the regular Internet. And we can use the 'net' to look up more updated [ammunition] information, because most of the books are outdated."

SAAS-Mod feeds the Integrated Logistics Analysis Program — the data repository portion of the Logistics Common Operating Picture — that Army logisticians here have been developing for the past few months, Ilarraza said.

The wireless LAN is also being used to transmit data collected by radio frequency identification tags and scanners that are used to track the movement and location of ammunition, Peters said.

CAISI uses mostly commercial off-the-shelf products housed in a rugged, military casing, said Maj. Carter Corsello, support operations officer for the logistics automation office. Among the vendors contributing to the CAISI program are Fortress Technologies with its AirFortress wireless security suite, as well as overall information technology support from Technical and Management Services Corp.

The wireless connectivity enables work to be done in minutes that normally takes hours to complete, and if the ammunition outpost had to wait for the "wire dogs" to run fiber lines out there, the rough terrain and constant splicing would quickly degrade the network, Corsello said.

He added that the war effort has produced many unplanned problems that are empowering innovative thinking and technological solutions. which would normally take much longer to get

approved. "We're doing things here we couldn't do normally because of the situation," Corsello said. "We just try not to take too much advantage."

The use of CAISI at the ammunition outpost is the second one in southwest Asia. The first one, set up at another outpost located about four miles outside Camp Arifjan, was completely unplanned. To install it, the automated logistics assistance team described the set-up process to users on the other end via cellular phones, Corsello said.

802.11's in the Army Now

Wi-Fi Planet (formerly 802.11 Planet)

By Gerry Blackwell

March 29, 2002

How secure does your enterprise wireless LAN have to be? We're guessing that if it was as secure a U.S. Army battlefield network, you'd be satisfied. Are we right?

The Army has decided that 802.11b networks are secure enough to carry Sensitive But Unclassified (SUB) data - if they're protected by add-on security technology that passes the National Institute of Standards and Technology (NIST) FIPS 140-1 cryptography certification process.

The Army's Program Executive Office, Enterprise Information Systems (PEO EIS) is in fact currently implementing FIPS 140-1-compliant technology from Oldsmar FL-based Fortress Technologies Inc. (www.fortresstech.com) to beef up security on new 802.11b-based portable field network systems which it will deploy worldwide.

The Fortress technology uses 128-bit AES (Advanced Encryption Standard) to encrypt all data passing over the air, including in the subnet authentication process. The amazing thing about the Fortress technology is that before it encrypts the data it first compresses it, with the result that it actually increases throughput over standard Wi-Fi radios.

With the Combat Service Support Automated Information System Interface Project (CAISI) the Army will link small, otherwise stand-alone wired LANs in the field in a Wi-Fi "last-mile" network, and ultimately connect them into the military's wide area mobile radio network.

The Army has committed to buying 6,000 of Fortress's Wireless Security Gateway devices and thousands of copies of its Secure Client software. The two products are part of the company's AirFortress security suite.

"We'll start deploying within 60 days," PEO EIS chief information officer (CIO) Pete Johnson told us. "I can't talk about specifically where it will be deployed initially, but it will be used by all of the army eventually."

The CAISI project, minus the Fortress protection, was close to going live last November when the Army suddenly woke up to fairly serious security flaws in the 802.11b protocol. It banned all use of Wi-Fi - unless networks were protected by add-on security products such as those from Fortress.

The CAISI networks are used to track maintenance of vehicles and weapons in the field and to manage field supply systems. Johnson says, "Imagine those World War II movies with guys sitting at tables in tents with clipboards and typewriters. Well, now they sit at laptop or desktop computers."

The CAISI network architecture is interesting to say the least. In each combat unit, there will be a small network of PCs connected by CAT-5 cabling to a standard Ethernet hub.

Why not wireless for the local area? Because this way the Army doesn't have to retrofit all its field PCs at great expense with Wi-Fi cards. Also, in some cases, the PCs are old enough that Wi-Fi card drivers may not be readily available for them, Johnson says.

Traffic destined for other field units or for any other destination outside the local unit will pass through the hub to the Fortress box where it's encrypted, then to a standard off-the-shelf Cisco Wi-Fi access point and router.

This Wi-Fi "last mile" network is also bridged to the Army's much lower bandwidth mobile radio data network for wide area communication.

Johnson sees two key vulnerabilities in an unprotected - or WEP-protected (which is about the same thing) - Wi-Fi network.

Using readily available hacking tools, an enemy could intercept data passed over the wireless network as part of its intelligence gathering. More importantly, the enemy could infiltrate the Army's larger network by posing as a trusted user on a Wi-Fi subnet.

The Fortress technology eliminates those vulnerabilities.

The information passed over the CAISI network is not classified. It's not military orders or data about field strength, but it is sensitive. If the enemy learned, for example, that helicopters were due for maintenance the next day during a certain period, they might deduce that the helicopters would be out of action and plan military operations accordingly.

This may be a somewhat farfetched scenario, Johnson concedes. Still, just on general principle, "you don't want anyone unauthorized reading any military information."

He won't say anything about what it is costing the army to deploy the Fortress technology, but Fortress itself is more than happy to provide commercial pricing. (We're assuming the Army is paying significantly less than the going rate - but you never know.)

The Wireless Security Gateway - the hardware component - sells for \$1,995, the Secure Client software for \$49 per user. The catch is that every client in the wireless subnet must run the software.

Because of the data compression used, each gateway can handle a full 11 Mbps of throughput. Fortress vice president of marketing and corporate development John Dow estimates that standard Wi-Fi access points actually only squeeze through about 4.8 to 5.2 Mbps.

So in a high-traffic wireless LAN, you need about one gateway per two access points. A less heavily used network could make do with fewer gateways. And then there's the client software.

The Army contract is a "marquee win" for Fortress, says Dow. But there are other significant vertical markets for the AirFortress product, including health care, manufacturing and retail.

The company's primary competition in these markets is from traditional VPN vendors. Dow argues that while VPN technology is good for remote access, it's not really

appropriate for securing wireless LANs.

In the past, industrial strength security for any wireless network - and the AirFortress solution is protocol agnostic, working in 900MHz, 802.11x and 802.16 networks - tended to be expensive and complex, or was perceived to be.

The crucial competitive advantage for the Fortress products, Dow says, is that they're dead simple to set up and use. The Army's Johnson confirms this. Ease of set-up was critical for the Army given that the systems it's deploying will have to be constantly re-configured as units move around.

"Fortress was the only [vendor we considered] that offered the kind of ease of configuration we needed," he says.

Can you make a Wi-Fi network secure enough to satisfy one of the most security conscious organizations in the world? Yep. And if it's good enough for the Army, we're thinking it's good enough for most enterprises.

U.S. Army Enlists Fortress Technologies' Wireless Local Area Network Security Solution

(Press release from Fortress Technologies)

TAMPA, MARCH 12, 2002 — Fortress Technologies, a leading global provider of infrastructure security solutions for 802.11 wireless networks, today announced a major enterprise win for its AirFortress Security Solution. The WLAN security offering will be deployed by the U.S. Army to secure mission critical business systems across its Combat Service Support Automated Information System Interface Project (CAISI).

CAISI is a multi-year WLAN deployment that will provide commercial and tactical network connections for approximately 85,000 Combat Service Support users. The AirFortress system will enable the CAISI program to provide secure wireless connectivity to support IT for supply chain management, maintenance and other Army business systems.

The AirFortress solution was selected after extensive testing and evaluation by The Program Executive Office, Enterprise Information Systems (PEO EIS). PEO EIS, which provides IT acquisition, implementation and training for the Army, evaluated security solutions based on comprehensive criteria including level of security, ease of use, network performance, mobility and total cost of ownership.

Upon the completion of CAISI, the Fortress security system will secure a wireless infrastructure totaling approximately 11,000 Cisco access points and workgroup bridges, according to Pete Johnson, CIO, PEO EIS. Fortress Technologies expects to deploy in excess of 6,000 AirFortress Wireless Security Gateways.

Mr. Johnson said the CAISI project presented a complex network environment with significant technical challenges. "Because of the highly mobile nature of these networks and a non-technical user base, ease of installation and transparency of operation were critical requirements," he explained. "These were key aspects in which the AirFortress solution differentiated itself."

"We're excited to be a strategic partner in a project that revolutionizes the Army's communication methods, enabling them to increase efficiencies and improve operations," said Willard Thomas, senior vice president of sales, Fortress Technologies.

AirFortress is a suite of infrastructure security products that eliminates the security risks and re-establishes confidence in WLAN communications, comprised of:

- **Wireless Security Gateways**, which are full-featured security appliances that enforce network access rights and encrypt/decrypt communication across the WLAN, while increasing performance.
- **Secure Client**, a software client that encrypts/decrypts communication across WLANs and protects the wireless devices against attacks. The client supports bar scanners, PDAs, laptops and integrated wireless devices, across various operating systems.
- **Access Control Server (ACS)**, a software application database designed to monitor and manage the authentication and access control of wireless clients.

About Fortress Technologies

Fortress Technologies (<http://www.fortresstech.com>) is a leading global provider of security products that address the largely ignored vulnerabilities of Wireless Local Area Networks and Fixed Wireless Networks. Fortress provides the missing element for today's 802.11 networks with the AirFortress Security Gateway, which shields against privacy invasions and unauthorized

network access. Founded in 1995, the Tampa Florida-based company uses open industry standards as the foundation of its proven and validated Security Architecture. Privately held, Fortress offers the first security product to have been granted the required certifications from the National Institute of Standards and Technologies and the Department of Defense for addressing the security risks inherent in communicating over wireless data networks.

Army Ready To Go Wireless With Combat Support

Government Computer News
By William Jackson
April 15, 2002

The Army this spring will start beaming IEEE 802.11b wireless LAN connectivity to support troops in the field. The Combat Service Support Automated Information System Interface will cross the proverbial last mile to the Defense Department's wired networks for maintenance, logistics and supply chain management systems.

"CAISI is a tactical wireless LAN," said Pete Johnson, CIO for the Army's Program Executive Office, Enterprise Information Systems. "It will provide wide area connectivity between the end users and the networks."

The first batch of 11,000 CAISI gateways, using wireless access points and workgroup bridges from Cisco Systems Inc. of San Jose, Calif., is set to roll out in May.

"It's a multiyear effort," Johnson said. "We still have a couple more years of buying to do." Deployment will keep pace with the schedules of the combat support units being equipped.

PEO-EIS buys and integrates commercial components to make turnkey enterprise systems with standard documentation, training and support. The office ruggedizes off-the-shelf products when necessary.

CAISI will secure the wireless links with encryption and access control technology from Fortress Technologies Inc. of Tampa, Fla. The program was held up last year because of security exposures found in IEEE 802.11b networks' Wired Equivalent Privacy protocol.

The wireless Ethernet standard uses the 2.4-GHz band at data rates up to 11 Mbps. Under WEP, all users of an 802.11b access point share one encryption key, and its weak encryption makes it easy to decipher. Also, wireless access depends on a user device's media access control layer address, which is easy to discover and spoof.

Those weaknesses could have compromised both network access and networked data. So the Army called a moratorium on wireless LAN use last year and in November issued a directive requiring Federal Information Processing Standard security on top of any Army 802.11b network.

"We had a small delay while we put in the security," Johnson said. "The level of traffic we are carrying is sensitive but unclassified, but securing the data as well as the network is of the utmost importance."

PEO-EIS could find no FIPS-certified products that met CAISI requirements for simplicity, scalability and throughput.

Then Fortress in December announced its proprietary Wireless Link Layer Security architecture as a replacement for WEP. The company's AirFortress Security Solution combines encryption, hashing for authentication and compression.

AirFortress met CAISI requirements, said John Dow, Fortress vice president for business development, and the company committed itself to earning FIPS certification. The WLLS architecture is undergoing independent laboratory testing, and if it passes will move on to the National Institute of Standards and Technology for certification.

"Basically, it's a bulk encryptor," Johnson said of AirFortress. Virtual private networks would not

have worked for CAISI, he said, because VPN users must authenticate themselves when roaming from one server to another. That complicates configuration and mobility.

AirFortress consists of a secure client, which handles access control and encryption-decryption across the wireless LAN, plus a gateway between the wireless access point and the wired network.

The gateway can support multiple access points and acts as a firewall as well as supplying encryption-decryption services between clients and other gateways.

Not one network

CAISI will use the Triple Data Encryption Standard with AirFortress. The product also can employ the newer Advanced Encryption Standard, and CAISI could change to AES after its FIPS testing is completed.

CAISI will serve thousands of notebook and handheld computers, personal digital assistants and bar-code scanners, but its planned 11,000 access points will not form a single network. "Think of them as end points hanging off a very large network," Johnson said.

A final cost for the CAISI project is unavailable, but "it's fairly inexpensive on a piece-by-piece basis" because of the off-the-shelf components, Johnson said.

Business Case Excerpt from CISCO Website

Cisco Aironet Wireless Bridges Help Army Communicate with Deployed Units

Regardless of their locations, forward-deployed units of the United States Army can communicate quickly and reliably through a wireless network that employs Cisco® Aironet® wireless bridges and wireless workgroup bridges. Following field-testing in Afghanistan, the Army has authorized procurement of approximately 11,000 Cisco Aironet wireless bridges.

Background

To operate effectively, the U.S. Army must be organized, trained, and equipped primarily for prompt and sustained combat associated with operations on land.

To accomplish its mission, especially in the combat service support (CSS) arena, the Army relies heavily on its Standard Army Management Information Systems (STAMIS). The Combat Service Support Automation Office (CSSAMO) provides customer assistance for the Army's STAMIS systems, including software, limited hardware and technical support.

The CSSAMO also plays an essential role in distributing new STAMIS equipment to the field and, with guidance from the New Equipment Training teams, the CSSAMO will usually spearhead new equipment fielding.

Challenge

Following Operation Desert Storm, the Army issued a directive to eliminate "sneaker net," the process of hand-carrying floppy diskettes across the battlefield in a deployed support area. Instead, the organization wanted to provide STAMIS with automated access to the Army's tactical packet network. This prompted development of the Combat Service Support Automated Information System Interface (CAISI). CAISI will be the backbone element for the Sensitive but Unclassified (SBU) network supporting the CSS community on the battlefield.

Subsequently, the Army authorized testing of an upgraded version of CAISI, which would incorporate standard commercial off-the-shelf (COTS) wireless technology with a Federal Information Processing Standard (FIPS) 140-1-approved in-line encryption. CAISI would thus integrate COTS equipment into modules designed specifically for military use. The goal was to revolutionize CSS communications in deployed support areas.

Solution

The US Army Information Systems Engineering Command (ISEC) of Ft. Huachuca, Arizona, designed the CAISI solution, which has been specially adapted to work in rugged conditions. The ISEC design includes CAISI bridge modules (CBM), and CAISI client modules (CCM). The CBM uses a Cisco Aironet 350 Series wireless bridge as its radio, while the CCM uses the Cisco Aironet 350 Series workgroup bridge. Both the CBMs and the CCMs have an inline encryption device and Ethernet hub(s).

Cisco Aironet 350 Series wireless bridges and wireless workgroup bridges use IEEE 802.11b standard in the 2.4 GHz band, with an 11 Mbps data rate. These bridges combine with the CAISI

"ruggedized" antennas and reach up to four miles with clear line of sight. CAISI is designed to provide encrypted wireless connectivity for the unclassified logistics systems in a deployed seven-square-kilometer brigade support area. Logistics computers use their regular network interface card to connect to the hub in the CAISI bridge module.

The Fortress Technologies AF-1100 has been validated for FIPS 140-1 to provide inline encryption, and is approved for SBU government data. A CAISI module and antenna is deployed into each tent, van, or shelter that has logistics computers. A single CAISI module includes up to 30 CCMs and nine CBMs. One CBM at each field site is designated as the central, or "root," node. This node controls the LAN for that field site, sets parameters for, and directs traffic among, other radios in the network. The root node normally links the CAISI LAN to an unclassified but sensitive Internet protocol router network (NIPRNET) port through the long-haul connections provided by Mobile Subscriber Equipment (MSE) or the newer Brigade Subscriber Node (BSN).

Results

Following a four-year development, testing, and procurement process that ensured selected products conformed to Department of Defense frequency regulations, security policies, and legacy application compatibilities, the Army started officially fielding CAISI equipment in June 2002. CAISI is now being used extensively in Army deployments in southwest Asia.

CAISI systems engineers from ISEC were sent to Afghanistan in October 2002 to train and assist in the deployment of CAISI modules in a brigade support area. Some trees and buildings were obstructing line-of-sight between the bridges, but after carefully positioning and configuring three of the modules to act as relays for the others, the network was operational.

CSSAMO personnel soon became confident with their new equipment and installed CAISI modules in 15 remote locations supporting approximately 50 users. CAISI is used for a number of applications, including supply chain management and maintenance.

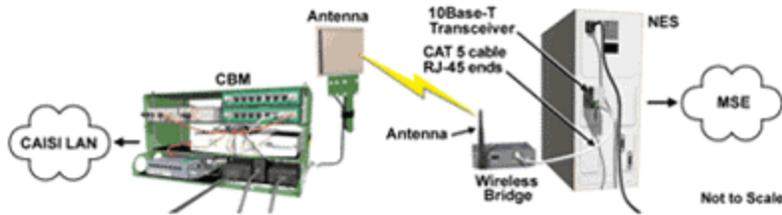
Additionally, in a deployed environment, NIPRNET and e-mail service is often limited to a few terminals near the headquarters. While the primary purpose of CAISI is to provide network connectivity between logistic systems within the brigade support area, the soldiers who are located in the CAISI remote sites now have access to a local e-mail server, resulting in a significant boost in moral.

Next Steps

The CAISI effort is addressing ongoing deployment requirements as quickly as possible. All brigade and rear logistics units throughout the Army are scheduled to receive CAISI equipment within the next three years. During that period, the Army will purchase approximately 11,000 Cisco Aironet 350 Series wireless bridges and wireless workgroups.

Excerpted from William R. Wiley Environmental Molecular Sciences Laboratory website located on the campus of the Pacific Northwest National Laboratory.

Combat Service Support Automated Information Systems Interface (CAISI)



Combat Service Support Automated Information Systems Interface (CAISI) Dr. Frank Greitzer Project Manager

CAISI provides commercial and tactical network connections for Combat Service Support Standard Army Management Information System (STAMIS) users. The tactical connectivity capability extends from the Theater level to the Brigade Support Area. The CAISI training course familiarizes personnel with the CAISI hardware and teaches them how to set up and maintain it. The training is designed to provide the necessary development for physical connectivity to the hardware in an operational (tactical/commercial) network environment. The multimedia material that PNNL has developed for the web-based CAISI training is also being used to support classroom training developed and delivered by the US Army CAISI Project Office.

From the William R. Wiley Environmental Molecular Sciences Laboratory is located on the campus of the Pacific Northwest National Laboratory in Richland, Washington.

CAISI Comes To Bat For Coalition Warfighters In Iraq

The Monmouth Message

By Stephen Larsen

April 18, 2003

PEO EIS

When you have forces conducting 21st century mobile warfare, with supply chains stretching hundreds of miles as war-fighters thunder forward – as is now happening in Iraq – how do you keep the war-fighters supplied with everything they need, from bullets to butter?

One way is with CAISI, the Combat Service Support (CSS) Automated Information Systems Interface, a secure, wireless local area network (LAN) that provides "last-mile" connectivity between combat service support computers and their logistics base networks.

CAISI, with 11Mb wireless line of sight (LOS) transmission, encryption on all wireless LAN links and 2Mb Digital Subscriber Line backup capability for non-LOS requirements within a four mile distance, extends tactical connectivity capability from the Theater level to the Brigade Support Area, and is providing traditionally-lacking communications for combat service support missions such as supply chain management, maintenance and business systems.

In support of Operation Iraqi Freedom in Southwest Asia, CAISI is connecting logisticians at a remote ammunition outpost to their base two miles away, allowing them basic Internet access and to automatically download critical information back to the base - helping ensure that troops get ammunition when they need it.

Before CAISI? According to Jose Ilarraza, a logistics management specialist from the Combined Arms Support Command, Fort Lee, Va., who is deployed in Southwest Asia as part of the Automated Logistics Assistance Team, previously the remote ammunition outpost had to rely on "sneaker net" - saving the data on a disk and then walking or driving to hand-deliver the disk to the required location on base.

Now, they can do it with a few keystrokes and use the power of the net to ensure they have the latest, updated information.

In another location, CAISI allowed coalition forces to wirelessly connect logisticians to a facility 3.5 miles away, according to Maj. Forrest Burke, chief, logistics automation with the Coalition Forces Land Component Command (CFLCC) in Kuwait, saving four weeks installation time, \$40,000 in installation costs and the need to obtain host nation property clearances.

"CAISI is a tremendous value, in terms of less labor, reduced environmental impact of digging in wire and cost of lost wire," said Burke. "Plus, CAISI is allowing us to be much more flexible in where we position units, both in tactical and garrison facilities."

Accelerated fielding

According to Maj. Sal Fiorella, Assistant Project Manager, CAISI with the Project Manager Defense Communications and Army Transmission Systems here, his team got the call from CFLCC in October, 2002 to provide a wireless CAISI solution for coalition forces in Southwest Asia.

He said they coordinated with units that had priority due to deployment schedules to provide new equipment training, then started fielding in December, completing the fielding in mid-March.

"I have a great team," said Fiorella. "My team was able to adjust fire and be responsive to the customer. We're not only meeting the requirements of the Coalition Forces Land Component Command, but we're working with the Automated Logistics Assistance Team to ensure connectivity for all standard Army management information systems (STAMIS) in Theater."

Burke echoed that thought. "Connectivity issues here are the same as we went through in the Balkans and before," said Burke. "A distinct network for STAMIS is necessary."

Col. Lee Price, the project manager Defense Communications and Army Transmission Systems (PM DCATS), is proud of the way Fiorella and his team have fielded CAISI.

"Combat service support people traditionally haven't gotten much in the way of communications when a battle is ongoing because they don't move fast and they have a big footprint," said Price. "Now they have a tool."

Next, said Price, will be satellite connectivity for CAISI, which is right in line with the April 3 decision of Kevin Carroll, the Program Executive Officer for Enterprise Information Systems (PEO EIS), to make PM DCATS responsible for the acquisition of the proof of concept and end-state satellite communications for all future PEO EIS system satellite connectivity requirements.

"We believe this is the beginning of the synergies Lt. Gen. Cuviallo (Army Chief Information Officer) aims to achieve by placing the emerging satellite requirements with PM DCATS," said Price. The field is equally excited, according to Burke. "Division Support Commands and Corps Support Commands are clamoring for CAISI-SAT and are excited about what it will do for their customers in reduced customer wait time and flexibility in the battle space," said Burke. "It's coming," said Fiorella. "It is next on our agenda."

Army Securing Wireless LAN

Federal Computer Week (FCW)
By Dan Caterinicchia
March 12, 2002

The Army this week announced that it has selected a security solution to protect the mission-critical business systems of the Combat Service Support Automated Information System Interface (CAISI) project, a wireless local-area network with about 85,000 users.

The Army has awarded Fortress Technologies a three-year "multimillion-dollar" contract for its AirFortress wireless security suite, said Janet Kumpu, chief operating officer of the firm.

"CAISI is a multiyear, wireless LAN program that will provide 'last mile' connectivity between the combat service support computers on the tactical battlefield and the wireless LAN that the Army provides," said Peter Johnson, chief information officer in the Army's Program Executive Office for Enterprise Information Systems (PEO EIS).

PEO EIS, which provides IT acquisition, implementation and training for the Army, evaluated several security solutions based on criteria that included level of security, ease of use, network performance, mobility and total cost of ownership.

CAISI will most benefit areas that lack Internet or LAN connectivity -- such as motor pools and supply rooms -- by "giving them that level of connectivity," Johnson said. "The real value is in the computers we're connecting."

The AirFortress system will enable CAISI to provide secure wireless connectivity to support information technology for supply chain management, maintenance and other Army business systems, Johnson said, adding that deployment will begin within 60 days.

The AirFortress suite, designed for networks based on the 802.11b standard, has three components:

Wireless Security Gateways - appliances that enforce network access rights and encrypt and decrypt communication across a wireless LAN.

Secure Client - a software client that encrypts and decrypts communication across wireless LANs and protects wireless devices against attacks.

Access Control Server - a software application database that monitors and manages the authentication and access control of wireless clients.

Defense Department policy prohibits agencies from operating wireless LANs without certified strong security, so "without our solution, they couldn't deploy the [CAISI] program," Kumpu said. "They haven't been able to use wireless at all [and] had to go back to wired [communications] until they solved the security issues."

The company already has shipped the first units to the Army for staging and testing, and an initial field launch is scheduled for next month. The original agreement called for 6,000 of the Wireless Security Gateways, deploying 2,000 units per year for three years, but the Army may accelerate that, Kumpu said.

The Army formally selected the AirFortress solution in January, said John Dow, Fortress' vice president of marketing and corporate development. He said the technology can be integrated into the Army's already-designed wireless LAN infrastructure within an hour, but because multiple modules and rollouts have to meet the service's "diligent" staging and testing processes, full deployment will take about one month.

In related news, Northrop Grumman Information Technology has awarded General Dynamics Decision Systems a contract to provide the Army Program Manager, Warfighter Information Network-Tactical (PM, WIN-T) with wireless secure LAN capabilities.

The program includes options that would bring the total value to \$83.4 million, with General Dynamics' portion valued at \$64.9 million, according to the company. Of the total initial award, valued at \$8.9 million, General Dynamics' portion is \$4 million.

Security Solutions Ride Wi-Fi Wave

Making wireless networks more secure is critical to growth of federal and commercial use.

©SIGNAL Magazine 2003

By Michael A. Robinson, Jr.

August 2003

One of the key factors inhibiting the growth of the wireless fidelity market is security. The attractive wireless technology that offers a wide range of applications also is generating a wave of uncertainty about the fidelity of its connectivity.

Security concerns limit growth of the enterprise wireless fidelity (Wi-Fi) market for two primary reasons. Companies and government agencies want to make sure neither hackers nor unauthorized users gain access to sensitive data such as social security numbers, bank and stock account balances and transfers, tax returns, medical records and human resources files. At the same time, many large corporations still must contend with tight budgets for any type of information technology purchase, even one that can replace wired local area networks (LANs) with gear that is easy to install and maintain and that also can knock two-thirds off the cost when compared to its wired counterpart. Citing security concerns gives information technology managers another reason to delay wireless deployment, industry observers say.

"We are out there talking to clients all the time, and the number one concern they cite is security," says Eric Carr, an analyst with Incode Telecom, a wireless consultancy in San Diego. "They've all heard stories about how some hacker using a Pringles can for an antenna hacked into the company system. When you start looking at financial services and government, they are much more security-oriented. It's much more of an issue for them. They have a lot of sensitive data to protect."

One company, a privately held startup located on the outskirts of Tampa, Florida, focuses on security as a prime gateway into the enterprise Wi-Fi market. Fortress Technologies may have found the industry's sweet spot. Following a company restructuring and fresh infusion of cash last year, company executives decided to focus on establishing secure links for federal agencies that need a wireless LAN.

Analysts say it could be a highly lucrative niche as hundreds of government agencies gear up for broadband access without all those cumbersome cables. No one seems to have solid estimates for the size of the government market, but the overall Wi-Fi sector had sales last year approaching \$2 billion, a figure that could skyrocket to \$8 billion by the end of 2007, industry analysts say.

So far, Fortress is ahead in the game. The company already ranks as the leading supplier of wireless security solutions for the U.S. government, backed by recent contracts with the U.S. Department of Veterans Affairs (VA) and the U.S. Army, which deployed Fortress technology in operation Iraqi Freedom.

In this market, government certification is paramount, and when Fortress Technologies introduced its AirFortress product at the end of 2001, according to the company the secure Wi-Fi link became the first to meet the wireless security network standards set by the National Institute of Standards and Technology and the U.S. Defense Department. Although the company does not disclose exact sales figures, Fortress' chief operating officer, Janet Kumpu, says she expects sales this year to reach roughly \$10 million. The company had zero wireless sales just two years ago.

"Fortress has been fortunate to be in the right place at the right time," Kumpu says. "We found that in the government circle, lack of security was a major inhibitor to Wi-Fi. Departments actually sent out policy changes that prohibited the use of Wi-Fi until they could address the security issue. We have traditionally focused on selling into the federal government, which is contrary to a lot of our competition. We've had a first-to-market advantage and have tried to capitalize on that. I think the government has been very creative in its implementations of wireless."

Although Wi-Fi has generated far more interest among consumers and those businesses ready-made for the technology--for example, warehouses and transit hubs--industry analysts say the enterprise market could take off soon. Many state, local and federal agencies, Global 2000 companies, medical centers and financial services firms would love to roll out Wi-Fi networks and replace wired systems. Industry observers say the technology could have as profound an impact on communication and productivity as the Internet itself. That is quite an accomplishment for a technology that is formally known as 802.11.

Within three years, experts say, nearly every mobile professional will have Wi-Fi cards in their laptops and an increasing number of personal computers used in business will be shipped Wi-Fi ready. Many tech-savvy professionals who use laptops, cellular telephones and personal digital assistants already have Wi-Fi access at home as well as in airports and hotels.

"Originally, we thought the enterprise market was going to drive the use of Wi-Fi equipment because people would see it at work and want it at home," says a spokesperson for the Wi-Fi Alliance, an industry trade group that promotes the technology. "What has happened though is that Wi-Fi has taken off in retail, then people got it at home and said, 'Hey, I want this at work, too.'"

And that is what worries so many information technology managers of large, distributed organizations like multinational corporations and government agencies. Without wireless security protections, technology officials potentially face a small army of unauthorized users looking for rogue access points.

Chris Kozup, a wireless analyst with the META Group, a Stamford, Connecticut market research and consulting firm, says many information technology managers have not taken the Wi-Fi plunge because they have yet to develop broad policy guidelines that can be applied throughout their organizations. He says he frequently receives calls from government clients concerned about security who are attempting to write wireless policies and procedures. This helps explain why sales for the enterprise market remain essentially flat. Standing pat for now is a safe decision because most enterprise networks using traditional wired technology are highly secure.

"I don't believe 2003 will be a huge year for enterprise wireless LAN," Kozup says. "But within 2004, as you see a lot of issues around security being resolved, you will start to see broader government adoption. And, you have a lot of Global 2000 companies that are planning complete deployment of Wi-Fi within their buildings."

Either way, Kozup says, Wi-Fi will never completely displace wired networks. The two will coexist indefinitely with wireless LANs serving as an alternative means of cost-effective broadband access as Wi-Fi networks become ubiquitous throughout the United States.

For her part, Kumpu says Fortress stumbled into the wireless security market almost by accident a little more than two years ago. At the time, Fortress was invested almost exclusively in the wired market with a device that provided security for a virtual private network (VPN). As Fortress executives recall, U.S. Navy officials began using the Fortress wired VPN technology to protect a

wireless system on the USS Coronado based in San Diego. Back at Fortress' headquarters, company executives made an intuitive leap that pushed the company in a new direction.

"We said, 'You know, what a great application. It's really going to take off,'" Kumpu recalls. "The need for wireless is going to grow significantly. So, we took some of the intellectual property that we had developed, and we basically designed a wireless-specific solution."

In essence, Fortress bet the company on the new strategy. At the end of 2001, the company launched the AirFortress product line that includes a gateway for secure wireless LANs, a client-side utility for laptops, personal digital assistants and bar code readers, and a control server for managing a system's back end.

By August 2002, Fortress officials restarted the company as a wireless outfit, complete with \$13 million in new funding. As a result, an investor group led by Liberty Partners received 51 percent control of the company. Now the contracts are rolling in.

In March 2002, one deal really made Fortress' reputation within the Defense Department, when the Army chose Fortress for secure, mission-critical business systems across its Combat Service Support Automated Information System Interface Project (CAISI). CAISI is a multiyear wireless LAN deployment that will provide commercial and tactical network connections for approximately 85,000 combat service support users.

The AirFortress system will enable the CAISI program to provide secure wireless connectivity to support information technology for supply chain management, maintenance and other Army business systems. Company officials say they have shipped the service some 6,000 AirFortress gateways, adding that their technology recently was deployed in Kuwait in support of operation Iraqi Freedom.

In early April of this year, Fortress Technologies announced that the VA is deploying the AirFortress in the agency's bar-code-based medication administration program. Fortress will ensure patients' privacy at VA medical centers by protecting the wireless data transmission of patient information at 167 hospitals and centers.

The program is important because more than 7,000 Americans die each year from medication-dispensing errors, according to a study by the National Academies' Institute of Medicine in Washington, D.C. To eliminate such errors, the VA developed a wireless system used for real-time retrieval of medical information from bar codes on patients' wristbands. The system prevents errors by electronically alerting health care providers to any potential problems or inconsistencies before medication is given.

In late May, Fortress won a contract to provide wireless security for the U.S. Defense Commissary Agency, which provides groceries and household goods to military personnel, retirees and their families through a worldwide chain of nearly 280 stores. Fortress partnered with Psion Teklogix, which had provided the commissary agency's wireless system.

Now, Fortress executives expect to extend their reach within the federal government market as more agencies go wireless. That in turn, says Kumpu, could lead to corporate sales. "The nice thing from our standpoint is that these success stories also translate into commercial applications," she concludes. "With an appropriate security solution, logistics, transportation, retail, health care are all viable markets for wireless. Many of those markets look to the government for leadership on how to address security. Security is a key component of any solution offered today. It's a must-have. It's in the check box that everybody looks at."

Army Secures 'Last Mile' In Its Supply Chain

InternetWeek

By Tom Smith

Mar 22, 2002 (11:32 AM)

The military's equivalent of a corporate supply chain is a critical link in getting soldiers the materials they need to wage war.

That's why it's especially noteworthy that the U.S. Army plans a major rollout of highly secure wireless LAN equipment that will be used by soldiers charged with maintenance, replenishment, and repair of equipment and other materials used in combat.

If a tank or truck breaks down on the battlefield, the wireless LAN gear would be used in ordering the necessary parts through wireless connectivity with Army systems.

Wireless connections could also be used to check and update maintenance records on ground vehicles and aircraft, for example.

"There's basically a warehouse on the battlefield, and that's where certain supplies are stored," said Pete Johnson, CIO in the Army's Program Executive Office for Enterprise Information Systems (PEO EIS), Fort Belvoir, Va. "If a unit orders supplies that aren't locally stored, they're shipped to the local warehouse."

The relevant IT systems that wireless LANs will communicate with -- developed internally by the Army -- control warehouses and inventory, such as helicopter and airplane parts for aviation units. Those systems, of course, have connectivity back to central Army systems, which in turn have connections to Army suppliers, such as those that make or distribute spare parts.

The Army's internally developed supply chain systems apply the Army's business rules related to maintenance, such as keeping up-to-date information on the combat readiness of a vehicle. "If you pull a tank from an engine, it's no longer battle-ready, so readiness data is compiled and sent back up to the national level so the Army as a whole can see the status of assets," Johnson said.

All this means that the wireless LANs the Army will begin implementing in the next 60 days will ultimately serve as the last-mile connection in the its supply-chain network.

The types of data being transmitted in such applications are called "secure but unclassified," which means the Army didn't need "super-duper encryption" when it first considered deploying wireless LANs.

As part of the Army's Combat Service Support Automated Information System Interface Project (CAISI), Johnson had already planned to roll out wireless LANs when a major security hole was discovered in wired equivalent privacy (WEP) last year.

"If you had a wireless LAN card, a [hacker] could sniff into your network, read your data and become a member of that network," Johnson said.

That prompted the Army to issue a wireless LAN policy stating it was not permitted to use 802.11 natively, or without additional encryption safeguards, and that whatever supplemental encryption was used must satisfy Federal Information Processing Standards (FIPS) requirements.

That requirement, in turn, prompted PEO EIS to begin investigating products that would supply additional encryption.

Its choice: wireless LAN security products from Fortress Technologies. Fortress is currently working on FIPS certification for its AirFortress product, but it has other products that have already achieved FIPS certification, Johnson said, which gave him confidence the company's products would meet the federal government security standards.

Fortress' products were also selected because they had an advantage over those that use virtual private network (VPN) technology. Such products build secure tunnels inside the network over which they operate, and require network nodes to alert other nodes of their IP address and other relevant information. The shortcoming with that approach, Johnson explained, is that it doesn't work very well in a highly mobile environment. "You set the VPN up, and tell each VPN device on your network where all the other ones are, and that works until things change. In an environment with soldiers on the battlefield, that becomes very cumbersome."

With AirFortress, each gateway and client share an Access ID that creates a closed architecture in which gateways and clients only pass encrypted traffic between AirFortress devices, giving more flexibility for roaming than the VPN approach.

The Army's introduction of new WLAN security requirements delayed the rollout of some WLAN equipment. Johnson said PEO EIS had planned to double its WLAN systems to 4,000 this year, but has had to delay 2,000 new purchases in order to buy the AirFortress security system. He declined to cite the Army's overall investment in the wireless and security technology. AirFortress gateways start at \$1,995.

Once it's operational -- and the plan is to begin CAISI wireless deployment in the next 60 days at the Fort Bragg, N.C., Army base -- Johnson said he expects PEO EIS will use triple DES encryption on the AirFortress product, with 168-bit keys. AirFortress offers multiple encryption options. That encryption will supplement the encryption that's available in the wireless LAN radios.

The total CAISI deployment, which will involve 11,000 wireless clients, will take about four years and involve Cisco Systems and other off-the-shelf wireless equipment, Johnson said.

Meantime, Johnson thinks the Army has put in place a secure method of providing last-mile connectivity in its supply chain.

Army ready to go wireless with combat support

From Mobile Access Solutions Web Site

Author Unknown

April 03, 2003

The Army this spring will start beaming IEEE 802.11b wireless LAN connectivity to support troops in the field. The Combat Service Support Automated Information System Interface will cross the pro

CAISI will cross the proverbial last mile from the battlefield to the Defense Department's wired networks. verbal last mile to the Defense Department's wired networks for maintenance, logistics and supply chain management systems.

"CAISI is a tactical wireless LAN," said Pete Johnson, CIO for the Army's Program Executive Office, Enterprise Information Systems. "It will provide wide area connectivity between the end users and the networks."

The first batch of 11,000 CAISI gateways, using wireless access points and workgroup bridges from Cisco Systems Inc. of San Jose, Calif., is set to roll out in May.

"It's a multiyear effort," Johnson said. "We still have a couple more years of buying to do." Deployment will keep pace with the schedules of the combat support units being equipped.

PEO-EIS buys and integrates commercial components to make turnkey enterprise systems with standard documentation, training and support. The office ruggedizes off-the-shelf products when necessary.

CAISI will secure the wireless links with encryption and access control technology from Fortress Technologies Inc. of Tampa, Fla. The program was held up last year because of security exposures found in IEEE 802.11b networks' Wired Equivalent Privacy protocol.

The wireless Ethernet standard uses the 2.4-GHz band at data rates up to 11 Mbps. Under WEP, all users of an 802.11b access point share one encryption key, and its weak encryption makes it easy to decipher. Also, wireless access depends on a user device's media access control layer address, which is easy to discover and spoof.

Those weaknesses could have compromised both network access and networked data. So the Army called a moratorium on wireless LAN use last year and in November issued a directive requiring Federal Information Processing Standard security on top of any Army 802.11b network.

"We had a small delay while we put in the security," Johnson said. "The level of traffic we are carrying is sensitive but unclassified, but securing the data as well as the network is of the utmost importance."

PEO-EIS could find no FIPS-certified products that met CAISI requirements for simplicity, scalability and throughput.

Then Fortress in December announced its proprietary Wireless Link Layer Security architecture as a replacement for WEP. The company's AirFortress Security Solution combines encryption, hashing for authentication and compression.

AirFortress met CAISI requirements, said John Dow, Fortress vice president for business development, and the company committed itself to earning FIPS certification. The WLLS architecture is undergoing independent laboratory testing, and if it passes will move on to the National Institute of Standards and Technology for certification.

"Basically, it's a bulk encryptor," Johnson said of AirFortress. Virtual private networks would not have worked for CAISI, he said, because VPN users must authenticate themselves when roaming from one server to another. That complicates configuration and mobility.

AirFortress consists of a secure client, which handles access control and encryption-decryption across the wireless LAN, plus a gateway between the wireless access point and the wired network.

The gateway can support multiple access points and acts as a firewall as well as supplying encryption-decryption services between clients and other gateways.

Not one network

CAISI will use the Triple Data Encryption Standard with AirFortress. The product also can employ the newer Advanced Encryption Standard, and CAISI could change to AES after its FIPS testing is completed.

CAISI will serve thousands of notebook and handheld computers, personal digital assistants and bar-code scanners, but its planned 11,000 access points will not form a single network. "Think of them as end points hanging off a very large network," Johnson said.

A final cost for the CAISI project is unavailable, but "it's fairly inexpensive on a piece-by-piece basis" because of the off-the-shelf components, Johnson said.

Vision Excel Testimonial

From Vision Excel Website

1. The **US Army** project was presented as a quick technical reference to be utilized in classroom training. The thrust was to ensure that all participants learned the same steps in deploying combat hubs. The major challenge in this particular project involved an ambiguity in the actual objective. While documentation of the steps involved proved fairly straightforward, the approach to teaching and measuring the learning response levels was cloudy at the onset. VisionExcel employed its DSP approach to ensure a clear pre-project launch. Once on a specific task timeline, the project rolled smoothly and effectively. The final output was both classroom course books and CBT format.

"Documenting the CAISI system and providing the training efforts resulted in a standardized transfer of knowledge. This immediately produced efficiencies in performance in that repeat training was eliminated and the same methods were employed throughout each combat unit. The integrity of this company (VisionExcel) was critical to the success of this project."

Mary McCarthy, Project Manager
U.S. Army CAISI Project

CSS STAMIS Telecommunications on the Battlefield

Quartermaster Professional Bulletin
By CPT Charles P. Downie
Summer 2001

Quartermasters who understand the telecommunication systems available for combat service support (CSS) on the battlefield will better influence the outcome of battle. Logisticians can use the transfer of data in the Standard Army Management Information System (STAMIS) over long distances as a combat multiplier.

Mobile Subscriber Equipment (MSE) provides the architecture for STAMIS conductivity. MSE, a voice and digital communication system, is arrayed to cover a geographical area in a tactical field environment. MSE components consist of the following: Digital Nonsecure Voice Telephone (DNVT), Digital Secure Voice Telephone (DSVT), Single Subscriber Terminal (SST), Mobile Subscriber Radio Terminal (MSRT), and facsimile equipment (TACFAX or BLACKJACK). The MSE network is the backbone of all CSS telecommunications assistance described in the following paragraphs.

Electronic Technical Manual-Interface

The Electronic Technical Manual-Interface (ETM-I) system works with the automated Unit Level Logistics System-Ground (ULLS-G) and the Standard Army Maintenance System (SAMS). The ETM-I uses these forms of data transmission to import or export electronic data: wire, radio frequency, Personal Computer Memory Card International Association (PCMCIA) or 3.5-inch magnetic floppy disks. The benefits of the ETM-I are profound in reducing paperwork for reporting orders and installing Class IX (repair parts). In fact, soldiers can complete Preventive Maintenance Checks and Services (PMCS) by using a hand-held computer. This PMCS information is transmitted to an ETM-I module on the ULLS-G system and the SAMS REHOST. The ETM-I system provides logisticians with "near real-time" status of combat power, faults/deadlines, and Class IX requirements. The ETM-I will eliminate filling out official forms on paper such as the DA Form 2404 (Equipment Inspection and Maintenance Worksheet), expedite identifying and recording maintenance faults, and electronically record PMCS completion. The ETM-I is currently fielded at Fort Bragg, NC, and Fort Hood, TX.

Wireless STAMIS Modem

A wireless STAMIS modem interfaces with STAMIS hardware to communicate supply and maintenance transactions via high frequency antenna over distances of three to five kilometers. This technology reduces the need for customer units to bring floppy disks ("Sneakernet") to the brigade support area (BSA). The wireless STAMIS modem not only enhances the direct support (DS) unit's ability to requisition repair parts and supplies, but also provides the customer units with the immediate status of their requisitions. This removes guesswork from the supply system for the customer, thus increasing confidence in the logistics system. The ULLS is targeted for the wireless STAMIS modem. The ability to transmit data over longer distances directly to the next higher STAMIS greatly reduces processing times. It is important to note that the wireless STAMIS modem interface with STAMIS hardware is self-sufficient because it does not use existing signal assets. This system is integral to the Force XXI initiative for shared information.

Tactical Terminal Adapter

The Tactical Terminal Adapter (TTA) is a field telephone with modem capabilities. The TTA allows computers to connect with a circuit switch. The TTA uses MSE to receive and transmit data.

The TTA is hard-wired into a Small Equipment Node (SEN) using a communications landline. The positioning of both the SEN and the using STAMIS is a planning consideration. Ideally, the SEN will be centrally placed between the STAMIS's location and the tactical operations center (TOC) to make maximum use of dedicated signal assets. This positioning allows transmitting data point-to-point over the MSE network or allows linking into a concentrator that will convert data into a format to send over a tactical network. The TTA should be used sparingly because it uses voice lines that can congest the MSE voice system.

Combat Service Support Automated Information Systems Interface

The Combat Service Support Automated Information Systems Interface (CAISI) provides tactical network connections for CSS units. The CAISI translates various types of signal formats. The CAISI allows all existing STAMIS systems to interface with each other by using the tactical network. One CAISI can support up to 32 users. It is important to note that all data transmission takes place over the Tactical Packet Network (TPN), a system embedded in the MSE architecture. Each location of MSE on the battlefield also has a packet network switch to route all the traffic from the CAISI systems located throughout the geographical area.

Army systems that already exist can greatly increase the logisticians' ability to communicate throughout the battlefield. However, soldiers need extensive training to master these communications systems, and most systems need the type of communications architecture found in a brigade-level exercise involving all slice elements. Knowing about these tools is the most important step in developing both a CSS unit's standing operating procedures for communications and a training plan at home station. Understanding the interrelationship of these systems is critical in the transition to the Force XXI concept and the digitization of the Army.

WLANs, the Army way

Infoworld Magazine
By Ephraim Schwartz
March 08, 2002

WE LIVE IN a democracy, a fact that is evident even in the corporate world which, during the past decade or so, has tried at least to build consensus. But sometimes it is hard not to admire swift, autocratic decisions made from the top.

In late 2001, researchers revealed how to break the backbone of IEEE 802.11 security based on a so-called static WEP (Wired Equivalent Privacy) key. Although corporate execs waffled on what to do while reassuring one another that the risk was small, the U.S. Army handled things its own way.

"The Army said anybody using WLANs [wireless LANs] had to shut them down. They issued a directive that you cannot run a wireless LAN ... unless you were running the [NIST FIPS (National Institute Standards Technology Federal Information Processing)] standard on top of that," said Pete Johnson, CIO of the Army's Program Executive Office of Enterprise Information Systems in Virginia.

What that meant was anybody who had 802.11b hardware was out of luck.

I relate this not just because it is a good story, but because after much searching, the Army found a level of security with which it could live. Now the Army is firing up its WLANs again, and next month it will launch project CAISI (Combat Service Support Automated Information System Interface), which will roll out 11,000 access points with 85,000 users for battlefield logistics support. The project had been postponed due to the potential for breach of 802.11 security.

Johnson says he saw a lot of "quick fixes" to the potential breach, such as rapid rekeying for WEP as ratified by the IEEE 802.11 committee, but he was not satisfied. "We don't know what the performance hit is with rapid rekeying," he said.

As a matter of fact, neither do its proponents. I spoke with Dennis Eaton, chairman of Wireless Ethernet Compatibility Alliance, and he said performance will depend on the processor in the access point.

The Army turned to Fortress Technologies, in Tampa, Fla., for its solution: AirFortress, a stand-alone appliance and software that can process NIST FIPS high-level security.

According to Dick Hibbard, vice president of engineering at Fortress, another difference between Fortress and everybody else is that it encrypts the entire IP packet at Layer 2.

"All the other vendors encrypt at Layer 3. All of the IP header is exposed at Layer 3, source, and destination address," Hibbard said.

But I did speak with John Pescatore, a security analyst at Gartner, in Stamford, Conn., and a former member of the National Security Agency and the FBI. Although Pescatore says Fortress offers more than most companies probably need, he also said this: "For classified information -- and in the military where it can be a matter of life or death -- a solution like the one Fortress offers is the way to go. It's tamperproof."

And that, folks, is the Army way.

Fast-tracking WLAN security

Infoworld Magazine
By Ephraim Schwartz
March 08, 2002

LIKE AN ALARM bell sounding in the firehouse, the WLAN (wireless LAN) industry scrambled when the Fluher, Mantin, and Shamir paper "Weaknesses in the Key Scheduling Algorithm of RC4" revealed how easy it was to crack IEEE 802.11 wireless Ethernet (WLAN) security.

A lot was at stake for WLAN vendors: Any legitimate threat to the integrity of the network could put a major hold on its growing corporate and government business.

In fact, the U.S. Army halted its CAISI (Combat Service Support Automated Information System Interface) project, which was about to deploy 11,000 access points with 85,000 users for battlefield logistics support. When the news emerged about the WEP (Wired Equivalent Privacy) key being broken, the Army had no choice but to issue a directive, says Pete Johnson, CIO of the Program Executive Office of Enterprise Information Systems in Virginia.

"Last November we became aware that WEP had been exploited. The Army issued a policy that said anybody using WLANs had to shut them down," Johnson explains.

Because of 802.11 WLAN vulnerabilities, several recommendations and specifications for greater security from Task Force I, the IEEE's 802.11 subcommittee comprised of vendors, cryptographers, and security organizations, were put on the fast-track to ratification.

The first recommendation is 802.1x, ratified by the full committee in July. It takes authentication out of a less robust AP (access point) and places it in the authentication server, such as Radius or Kerberos, on the back end. The 802.1x standard allows for the use of dynamically generated WEP keys on a per-session, per-user basis in place of a static WEP key placed in the AP.

Unfortunately, hardware vendors began building to the 802.1x spec before it was ratified, which will likely lead to product interoperability problems because each vendor interprets the spec differently. The products will be useful, but early adopters of 802.1x will be tied to a single vendor, says John Pescatore, research director of Internet security at Gartner in Stamford, Conn.

On the software side, Windows XP is the only major OS vendor supporting 802.1x. The Microsoft version uses EA-TLS protocol, which requires a PKI (public key infrastructure) and does not support directory services for password-level security.

Pescatore favors the use of PKI as a long-term solution; however, he notes that the requirement to create a certificate authority rather than using directory services for authentication might be a problem, especially for smaller companies.

Task Force I's next task is replacing WEP with the TKIP (Temporal Key Integrity Protocol). TKIP is backward compatible with current APs and wireless cards and requires only a software upgrade. But because it is based on rapid rekeying and generates a new encryption key every 10,000 packets, there are some latency issues.

"[TKIP] performance is vendor-dependent. If you have a small ARM processor in the access point, there may be some [performance] hit," says Dennis Eaton, chairman of the Wireless Ethernet Compatibility Alliance based in Mountain View, Calif. AES (Advanced Encryption Standard) completes the current IEEE 802.11 road map.

AES is recommended and used by the federal government's National Institute of Standards -- it has a far-better underlying cipher, according to Eaton.

The major issue with AES is its incompatibility with current hardware, requiring that processing be off-loaded to a separate chip.

"You can't have a WEP client that talks to AES access point," Eaton says.

But what do companies do while waiting almost two years for AES availability? Johnson examined the situation carefully before making a decision. "AES is in the future. I need something now," he says.

Johnson went with Fortress Technologies, a company offering its own hardware appliance and software solution. AirFortress is compatible with the Army directive barring WLANs unless they use the National Institute of Standards Technology Federal Information Processing (NIST FIP) security standards on top.

Gartner's Pescatore believes solutions such as AirFortress do offer the highest level of WLAN security. But it is more costly than software-only security, and network security can still be compromised if companies keep only software-level security for Internet access to their VPN.

For now, Pescatore recommends that companies put the AP outside the firewall and use a VPN to get in.

"If you have public exposure to your signal or people wandering around with wireless NICs, then use VPN. It is the most secure approach," Pescatore says.

Army Deploys WLAN Security System

InterWeek Web Site

By Tom Smith

March 12, 2002

The U.S. Army on Tuesday said it is deploying Fortress Technologies' AirFortress Security Solution products to secure wireless LAN communications.

The Combat Service Support Automated Information System Interface Project (CAISI) is a WLAN deployment that will give wireless connectivity to 85,000 Combat Service Support users for applications including supply chain management and maintenance.

The WLAN will total approximately 11,000 Cisco wireless access points and workgroup bridges, according to Army officials. Fortress Technologies said it expects to deploy more than 6,000 of its AirFortress Wireless Security Gateways.

The gateways are just one component of the AirFortress system. They enforce network access rights and encrypt data traversing 802.11 WLANs, which use airborne radio communications that are often considered susceptible to interception. With the AirFortress system, enterprises are able to select the level of encryption they use, whether it's 56 bits, 128 bits, or 168 bits.

Other components of the AirFortress product are the Secure Client, which encrypts and decrypts data. It runs on PDAs and laptops. The product line also includes an Access Control Server, which monitors and manages authentication and access control of wireless clients.

The Army project announcement comes one day after another WLAN security product, from SMC Networks, was announced.

From Parrot Systems Website

Parrot Systems is proud of the track record we have developed with our clients. We realize the importance of our clients and the impact they have on our success as a company. Some of our clients include:

AKO

The Army Knowledge Online (AKO) portal is the official online knowledge management tool for the U.S. Army, providing a single access point to numerous information and services for Army personnel. Parrot Systems assisted in the content auto-categorization process which involved integrating AKO's existing Verity K2 search engine with Entrieva's Semio Tagger content categorization software.

Entrieva

Entrieva is an information discovery and categorization software company which provides real-time solutions for information mining and notification. Parrot Systems provides solutions that incorporate Entrieva's indexing and categorization capabilities and integrates those solutions into third party applications.

KPMG

KPMG is a global leading provider of assurance, tax, legal and financial advisory services. Parrot Systems assists KPMG's Tax Knowledge Management group in architecting and implementing information management solutions ranging from search & retrieval to portal and content management.

PEO EIS / U.S. Army

PEO EIS (Program Executive Officer, Enterprise Information Systems) is a joint Army service organization responsible for developing, acquiring and deploying tactical and non-tactical Information Technology systems and communications for the Army. Parrot Systems develops custom software for PEO EIS which greatly simplifies deployment and management of their mobile network equipment (CAISI) while ensuring compatibility with legacy systems.

Phoenix Consulting Group

Phoenix Consulting Group is a public affairs and communications firm which provides strategic planning, relations, business advocacy and event planning services. Parrot Systems was consulted to evaluate a custom training software application, provide development roadmaps and cost analysis, and prepare demonstration media.

SAIC

SAIC (Science Applications International Corporation) is a Fortune 500 research and engineering company which offers technology and system development, analysis, integration and technical support services. SAIC contacted Parrot Systems for assistance with porting a legacy UNIX network routing and communications system to Windows NT/2000 for the Army.

Verity

Verity is a market leader in search, content organization and information solutions. Parrot Systems specializes in Verity technology with years of experience and has implemented solutions for many of Verity's largest customers.

AirFortress Gets Government Certification

Wi-Fi Planet (formerly 802.11 Planet)

By Eric Griffith

July 15, 2002

The Army has been testing out Tampa, FL-based Fortress Technologies' AirFortress for a while now, but as of this week, the product finally meets the government standards for cryptography of non-classified information. AirFortress is now FIPS 140-1 certified.

FIPS is short for Federal Information Processing Standards; the 140-1 cryptographic standard was created by the National Institute of Standards and Technology (NIST). The standard has four levels of security - Level 1, Level 2, Level 3, and Level 4 -- that increase in quality as they go up. They are suitable for a wide array of areas in which cryptographic modules could be used.

Companies that need FIPS certification contract with outside labs that are partners with the federal government. The labs, which go through some rigorous accreditation by the government, perform tests to see if products and services meet the FIPS requirements.

"[FIPS certification] allows the government to put on their stamp of approval," says Shawn Hughes, President and CEO of Fortress Technologies. "To sell secure solutions to the federal government, it has to have FIPS approval, especially post 9-11."

Even before testing and certification was done, the Army had committed to purchasing thousands of Wireless Security Gateways (\$1,995 commercially). Fortress expects to deploy 2,000 gateways and eventually have 85,000 users in the Army. The government had confidence in Fortress that certification would happen, since the company has been through FIPS tests before. However, Hughes noted, had AirFortress not received FIPS certification, the entire deployment would have ended right there.

With FIPS certification complete, Fortress looks forward to developing relationships with other branches of the Armed Services and the federal government.

"We expect as much as half our business to be from the government and military this year," says Hughes, but he feels the certification is also a "really strong validation for commercial customers looking for authentication. While not all can make sure it works, the government did it for them."

The gateways, together with clients and the free access control server software, help form the complete AirFortress security solution, which uses Layer 2 Wireless Link Layer Security (WLLS) to compress -- which increases throughput -- and 128-bit AES (Advanced Encryption Standard) to encrypt all wireless data.

The Army, however, is not using the full AirFortress setup: "The solution they're using is only the gateways to secure communications coming in," says Hughes.

The Army is rolling out AirFortress gateways within its Combat Service Support Automated Information System Interface (CAISI) Project, which tracks field supplies, weapons and vehicles, as well as their maintenance. The project almost went live last year but the Army stopped all use of 802.11b wireless LANs when security issues when using wired equivalent privacy (WEP) encryption in 802.11b networks were revealed.

Wireless Gets Down to Business

Excerpted from Computerworld Magazine

By Stacy Collet

May 5, 2003

Defense & Military

Wireless on the Front Lines

On the battlefields of Iraq, Afghanistan and Southwest Asia, Army troops have replaced the sneakernet used to requisition supplies and maintenance during the 1991 Persian Gulf War with wireless technology that can save time, money and maybe even lives.

Now, instead of loading a floppy disk with logistics information, supply chain reorder forms, mechanical parts orders and requisitions for vehicle maintenance and then carrying it to base camp for processing, troops are using CAISI (pronounced "Casey"), the Army's Combat Service Support Automated Information Systems Interface. The technology went into the field in October 2002 and is now used by four of the Army's 10 divisions.

"It used to take a week or so to get these supplies commissioned and back to the troops," explains Maj. Salvatore Fiorella, assistant product manager. "CAISI increases the capability to order supplies by getting the wheels turning immediately, as soon as the transmission is made."

In one instance, CAISI saved a unit in Southwest Asia \$40,000 in hardware costs, the two weeks it would have taken to run wire, and hours of negotiations with the host country to get approval for laying down extra wire.

The system can transmit data about three to four miles, which has limited its use once troops venture deeper into enemy territory. But "with satellites linked to CAISI, that just brings it to the battlefield," Fiorella adds.

The wireless system consists entirely of off-the-shelf hardware and software. Laptop computers in the field are physically connected to wireless modules, which are triple-encrypted using software from Fortress Technologies Inc. in Oldsmar, Fla., even though CAISI's use is restricted to "sensitive but unclassified" information.

CAISI is just one of the Army's efforts to have 802.11b wireless devices deployed in the field between 2008 and 2010, once all security issues have been addressed. "We have to worry about encryption, we have to worry about firewalls, we have to worry about nonworking communication lines," says George Knizewski, lead engineer and contractor at the U.S. Army Program Executive Office, Enterprise Information Systems (PEO, EIS), at Fort Belvoir, Va. "We don't want to be on the bleeding edge of technology."

Today, government agencies require wireless technology to meet the Federal Information Processing Standards (FIPS). "Unless it's up to that level of security, government agencies can't deploy them," says Frost & Sullivan's Lee. CAISI is one of the first Army systems to be FIPS-compliant, which opens the door to many future uses.

"I see wireless bringing better assistance to the [troops] that are deployed, providing rapid information so they can see what's available on the battlefield, which will help leaders to determine what combat units are equipped to go forward," Fiorella says.

Collett is a freelance writer. Bob Brewin and Tom Hoffman also contributed to this report.

Excepted from the **TechNet Solutions - A Division of TechNet Training Centers & More Inc.** website

AF2100

The AirFortress Model **AF2100**'s small, sleek, yet versatile design makes this solution perfect for deployment at the edge of any network. Its durable, fan-less design made this product the choice for the U.S. Army's Combat Service Support Automated Information System Interface (CAISI) project. Even if your requirements are less demanding, your network deserves the same level of robust security. The AF2100 can reliably provide secure service for several 802.11b access points simultaneously.

Operation Iraqi Freedom - From Sunset to Sunrise at Bashur, Northern Iraq

Quartermaster Professional Bulletin
By CW3 Angel M. Matos
Summer 2003

Downloading Cargo Aircraft

On 26 Mar 03, more than 950 paratroopers from the 173d Airborne Brigade jumped into Bashur, Iraq, to set the stage for a northern front. Two days later, the first soldier from the 501st Forward Support Company, 173d Airborne Brigade, Supply Support Activity (SSA) arrived at Bashur Airfield. Within hours of landing on the ground, this specialist issued one day of supplies of Meals, Ready To Eat (MREs) along with bottled water to more than 2,000 service members from the 173d Airborne Brigade, the 201st Forward Support Battalion, 250th Field Surgical Team, 86th Air Force Contingency Response Group (CRG), US Marine units, and Joint Special Operations Task Force-North (JSOTF-N).

On 29 Mar 03, the remaining SSA personnel departed Aviano Air Force Base, Italy, on two C-17 Globemasters. These SSA personnel were the accountable officer, noncommissioned officer in charge (NCOIC), two stock control NCOs, a receiving/turn-ins NCO, a storage/shipping NCO and two automated logistics specialists. The giant cargo aircraft transported five mobile containers (ISU90s) containing 720 lines of Class IX (repair parts) on the Authorized Stockage List (ASL) stored in cabinetry, one M280/E shelter, a 10,000-kilowatt Tactical Quiet Generator (TQG), two M10A forklifts with 10,000-pound (10K) load capacity, and one M105 trailer jam-packed with SSA office supplies and equipment.

On 30 Mar 03, the SSA personnel posted their "Logistics Warriors" sign made of duct tape letters on brown cardboard from ration boxes. This signified their readiness to support customers - no matter who they were. By 1005 hours, the Standard Army Retail Supply System-Level 1 (SARSS-1) was operational. The "Logistics Warriors" SSA could use SARSS-1 to securely send supply requisitions with File Transfer Protocol (FTP) connectivity to the Corps Theater Automated Service Center (CTASC), 19th Materiel Management Center (MMC), Wiesbaden, Germany. At sunset, the Iraqis sent a not-so-friendly greeting when they lobbed a mortar round at Bashur airfield. It missed with some distance to spare, but served as a reminder that Quartermasters were in harm's way.

To provide wireless, responsive and efficient support to the combat operation, SSA personnel used the Combat Service Support Automated Information System Interface (CAISI). The CAISI wireless Local Area Network (LAN) connected the SARSS-1 system through bridge modules to a Small Extension Node (SEN) switch operating in the brigade support area (BSA). The SEN switch communication equipment is in an S250/E shelter mounted on a high mobility multipurpose wheeled vehicle (HMMWV).

The CAISI wireless solution enabled the SARSS-1 system to transfer batches of logistical information via line-of-sight radio to CTASC in Germany, reduced the set-up time, covered a broader area, and enhanced the supported Standard Army Management Information Systems (STAMIS) users with data speeds high enough for web-based logistics. The CAISI wireless technology placed the logistics community at Bashur Airfield on the path to providing real-time logistics data, enabling faster requisitions. During the first day of SSA operations at Bashur, the SARSS-1 system received 32 batches of logistics updated data from the MMC, filled 136 Materiel Release Orders (MROs) from the ASL and processed 295 requisitions.

During the first week, the Army and Air Force handled 84 flights (US Air Force C-17 Globemasters and C-130 Hercules aircraft) that brought in about 4,000 troops and 6 million

pounds of cargo. After less than a week on the ground, the nine-soldier SSA section - based in Vicenza, Italy, and accustomed to running a small direct support (DS) Class IX warehouse - faced new challenges. Missions now included supporting the 1/63D Armor Battalion (a heavy tank unit based in Vilseck, Germany) and becoming an area support redistribution point in charge of processing, storing, receiving and issuing all classes of supply. This small SSA section had become the central receiving point (CRP) and supply redistribution point (SDP) for northern Iraq almost overnight.

During the next two weeks at Bashur Airfield, all supplies arrived via the air lines of communication (ALOC) on C-17s and C-130s from Ramstein Air Force Base through Constanza Air Force Base in Romania. During an average 24-hour day of operations, more than 40 Air Force 463L ALOC pallets would arrive. Each pallet then had to be downloaded from the plane, transported to the SSA, processed and finally issued either to storage or to customers.

The radio frequency identification (RFID) system was vital for the SSA in collecting data for all incoming shipments. The RFID system uses state-of-the-art wireless technology to monitor, track and locate assets, enhancing support operations. The system consists of tags, readers, radio frequency (RF) links, and a standalone computer with installed RF identification management software. The system's RF tags can store, transmit and receive RF data from the readers within a 350-foot radius. The system's readers immediately collected manifest information from RF tags attached to ALOC pallets as the airplanes were downloaded. This technology helped in forecasting demands, expedited the processing of incoming supplies, and allowed the SSA personnel to identify those ALOC pallets "where the right stuff was" in minutes. (See the Summer 2003 article, Commentary - Radio Frequency Identification (RFID) Technologies: Potential for the Department of Defense.)

Transporting ALOC Pallets

When the ground lines of communication (GLOC) finally opened, the SSA started to receive trucks carrying boxes of MREs, bottled water, and subsistence from Turkey. The aircraft were still arriving at the same rate. The numbers of personnel, equipment and units to support continued to rise. The SSA was increasing in size daily and the 720 ASL increased to 1,100 lines. Stockpiles increased dramatically within a week. Battling the drastic changes in weather from heavy wind, rain and dust, the outdoor warehouse had its fair share of challenges.

In addition to the two organic M10A rough terrain forklifts, SSA personnel relied heavily on the Air Force's Tanker Air Lift Control Element (TALCE) 10K forklifts to transport the high volumes of pallets from the flight landing strip to the SSA "warehouse" pallet-holding yard. The mud and unimproved road conditions were a challenge for soldiers who had no choice but to adapt and overcome.

Another challenge was the increase in the number of customers from 8 to 42. As SSA personnel discovered new units on the ground in Northern Iraq, they adapted by adding new customers into the SSA system and filling the growing demands. The "Logistics Warriors" SSA knew the customers were relying on them and refused to turn anyone away.

Between 28 Mar 03 and 11 Apr 03, the 501st Forward Support Company processed 2,305 requisitions; issued 30 463L Air Force pallets of Class IV (construction and barrier materiel); issued 574 MROs from the ASL; received and processed 120 shipments of bottled water and MREs from Turkey; received and processed 210 463L ALOC pallets containing Class II (general supplies), packaged Class III (petroleum, oil and lubricants), Class IV, Class IX, bottled water and MREs from Ramstein Air Force Base in Germany; and issued more than 20,000 cases of MREs and more than 30,000 liters of bottled water.

On 11 Apr 03, the 501st Forward Support Company SSA received marching orders to move 120 miles south to city of Kirkuk, Iraq, controlled by the Kurdish and US coalition forces. The SSA began operating in an old Iraqi Air Force base hangar to continue its mission of providing reliable logistics support to the 173d Airborne Brigade and units across Northern Iraq.

Stock Control in M280 Shelter

The greatest challenges have been the GLOC from Turkey with the Harbor Gate Turkish border convoys, Arrival/Departure Airfield Control Group (A\DACG) downloading and transporting ALOC pallets on rough terrain to ensure the landing strip was cleared within an hour of an airplane's arrival, light communication package firewall rules and restrictions, familiarization by the SEN communications personnel on SARSS-1, personnel shortages (augmentation requirements), maintenance of materials handling equipment organic to the SSA section while airplanes are still arriving, increase in customers from 8 to 42, and support of joint forces (US Air Force personnel and US Marines). Deploying with the following items will improve the SSA's sustainment capability in the future: great quantities of computer diskettes, great quantities of MRO paper, printer ribbons and laser printer cartridges; an additional SARSS-1 server (a "float"); and 120-volt (V) and 220V transformers and adapters. Two recommended actions before future SSA deployments are Combat Service Support Automation Management Office (CSSAMO) functional training and also training for communications personnel on SARSS-1 protocols.

Editor's Note: LT Kyle Upshaw, who also deployed in March 2003 to Basur, Northern Iraq, during Operation Iraqi Freedom, contributed to the accuracy of this article.

Army Taps 128-bit Encryption For Battlefield Wireless LANs

Computerworld Magazine

By Bob Brewin

May 20, 2002

Last November, when the glaring weaknesses in wireless LAN security became apparent, the U.S. Army decided it needed to beef up the security of a battlefield wireless LAN system it was about to deploy.

Major Hieu Tran, project officer for the Army's Combat Service Support Automated Information System Interface (CAISI) project, said top Army commanders ruled out relying solely on the Wired Equivalent Privacy protocol for encryption on an 802.11b wireless LAN that the Fort Belvoir, Va.-based unit planned to deploy to support battlefield logistics systems.

Looking for an encryption system as close to bulletproof as possible, Tran said, CAISI decided it needed to use the newly approved federal Advanced Encryption Standard (AES) endorsed by the National Institute of Standards and Technology (NIST).

CAISI then selected Tampa, Fla.-based Fortress Technologies Inc. to supply an encryption system that incorporates 128-bit AES into a device that can be attached to Army battlefield networks, Tran said.

Janet Kumpu, chief operating officer at Fortress, said the company's AirFortress Wireless Security Gateway encrypts "everything from the data layer up" in a wireless LAN, including holes routinely exploited by hackers such as IP addresses. Kumpu said that by encrypting IPs, AirFortress can help defeat spoofing attacks with algorithms so strong the NIST estimates they would take trillions of years to break.

Tran said the Army has bought roughly 40 of the AirFortress Gateway products, which sell for \$1,995 each, and it has an immediate need for another 300, which will be fielded to units at Fort Lewis, Wash.

The Army has an open-ended contract with Fortress pegged at 2,000 AirFortress Gateway products per year for the next three years, Tran said. Any federal agency, including the Defense Information Systems Agency, can buy off the contact. "We'd like to help," Tran said.

From the AirFortress Website



The **AirFortress Model AF1100**'s small, sleek, yet versatile design makes this solution perfect for deployment at the edge of any network. Its durable, fan-less design made this product the choice for the U.S. Army's Combat Service Support Automated Information System Interface (CAISI) project. Even if your requirements are less demanding, your network deserves the same level of robust security. The AF1100 can reliably provide secure service for several 802.11b access points simultaneously.

The CAISI Connection: A Wireless Solution for the Digitized Battlefield

Army Logistician (PB 700-01-6), Volume 33, Issue 6
By Captain Joseph M. Colacicco
November-December 2001

The Army's move toward a digitized force is giving warfighters increased situational awareness and better tools for planning and executing operations. For logisticians, this creates a greater need for real-time information, faster reporting, and a smaller logistics footprint. All three of these requirements involve improved connectivity to the Standard Army Management Information Systems (STAMIS) used to provide logistics support to our soldiers. The logistics community has reached another significant step in accessing information with the development of the wireless Combat Service Support Automated Information System Interface (CAISI).

Some people undoubtedly will ask, "Why do we need this new technology? Our information flow is just fine in garrison." The answer is twofold. First, the information flow in garrison typically uses the garrison local area network (LAN) and is radically different from the information flow in a field environment. The second reason we need the CAISI is that systems in the field need a network architecture in order to interact with each other and pass information. Unfortunately, no practical solution has been found to replicate the garrison capability in a field environment—until now.

The Road to CAISI

The Army first realized its need for a network solution while reviewing lessons learned from Operation Desert Storm. There, connectivity was provided by soldiers carrying disks from one computer to another. Though effective, this method obviously was not the most efficient. The Army began to look at newly developed technologies and rapidly evolving network systems for a new way to connect its logistics systems.

In 1992, the Army demonstrated one connectivity solution in the 1st Corps Support Command at Fort Bragg, North Carolina. It was called "near-term fix" (NTF), and it eliminated the need to transfer disks. The NTF consisted of Sun computer workstations that consolidated the data transferred from STAMIS and used the "send mail" function to send it over the tactical network.

This solution had several flaws. The biggest problem was that a concentrator was required at each end of all network communications links among various STAMIS, even if one of those systems was network capable. Another problem was the sheer size of the NTF. The Sun workstation consisted of 17 separate components and associated cables and connectors, which made it difficult to move quickly in a high operating tempo environment. The NTF also had a complex user interface, but there was no formal training available on its use in Army Training and Doctrine Command schools. The final problem was that the "store and forward" e-mail function did not support the real-time data communications required by the Objective Supply Capability, Total Asset Visibility, and Total Distribution System programs.

Technology Moves Forward

In 1995, the CAISI Mid-Term (CAISI-MT) replaced the NTF. CAISI-MT allowed users to make direct file transfers instead of having to use "send mail," thus providing a great first step toward creating a functional logistics field network. CAISI-MT provided LAN technology to units in the field, enabling continuous network connections without using modems. It consisted of a ruggedized transit case containing a Cabletron MMAC-8 modular hub (eight-slot chassis), a terminal server, and a management module. The keyboard and monitor were separate. Although this system was effective, STAMIS users considered it bulky and extremely heavy at over 148 pounds. It was demonstrated successfully at Fort Bragg, but a better model—a smaller Cabletron

MMAC-3 modular hub (three-slot chassis)—was developed before its actual fielding. The MMAC-3 weighed only 84 pounds and used a laptop computer that could connect 82 users.

The Cabletron MMAC-3 modular hub represented a huge leap forward in network technology for the Army. Fielding of the CAISI-MT began in October 1996, and the 46th Corps Support Group (CSG) (Airborne) at Fort Bragg, North Carolina, used it with great success during a field training exercise in early 1997. It enabled the supply support activities to transmit data between the field site and the 2d Corps Materiel Management Center (CMMC) in the garrison. This proved the ability of CAISI-MT to facilitate data transmission over the tactical network to a garrison. The 46th CSG could send data to the CMMC as well as "telnet" to various sites at Fort Campbell, Kentucky, and to the CAISI-MT contractor in Fairfax, Virginia. The CAISI-MT went on to have operational successes in Haiti and Bosnia.

A supplement to the introduction of CAISI-MT was the development of Transmission Control Protocol/Internet Protocol (TCP/IP) technology. CAISI-MT, coupled with TCP/IP, enabled logisticians to pass information to multiple users anywhere in the world in a matter of seconds by taking advantage of the Internet. This was the beginning of web-based logistics.

Tethered Technology

CAISI-MT provided new capabilities to the logistics world, but it was limited to the capabilities of its thin coaxial cable. This meant it had to be located within a 185-meter radius of a mobile subscriber equipment small extension node switch. STAMIS users beyond that distance connected to the system with field wire that weighed 95 pounds for every mile and transmitted data at extremely slow speeds.

Although CAISI-MT was easier to transport than the NTF, its dependence on coaxial cable and field wire made it extremely difficult to jump locations without abandoning the cable and wire. The wire had to be reconnected every time the system was moved to a new location, which added considerable time to set-up operations. Therefore, CAISI-MT served as a functional system for units that remained in one location. Units that moved continuously found its wire requirements and set-up times prohibitive. As a result, CAISI-MT was ignored in training environments.

Connectivity Gone Wrong

The difficulty of setting up and operating CAISI-MT caused units to find other ways to pass data in the field. For example, STAMIS users in a brigade participating in a rotation at the Combat Maneuver Training Center at Hohenfels, Germany, had to connect to the data network to pass requisitions and receive status information. However, the existing phone lines in the brigade support area (BSA) were substandard and could not support large transfers without losing data. The solution to the problem seemed obvious: the brigade would write its data to disks. With that decision, the brigade immediately fell back to the system that had proven cumbersome during Desert Storm in 1991.

Here's how the information flowed in that brigade using the Unit Level Logistics System-Ground (ULLS-G). Units prepared their requisitions and maintenance updates once a day and wrote those files to disks. This took two disks per company—one for requisitions, which went to the warehouse, and one for maintenance updates, which went to the maintenance shop office. The shop office input the information on the maintenance disks into the Standard Army Maintenance System-Level 1 (SAMS-1), and those files were stored on a consolidated maintenance disk. The requisition disks were passed to the supply organization to input the information into the Standard Army Retail Supply System-Level 1 (SARSS-1). Unfortunately, if the SARSS-1 was located in the garrison because of field connectivity difficulties, the consolidated maintenance disk had to be sent to garrison for input into the SAMS-2 and transmission to the division support command. A truck driver returning to home station would carry the disks in a

"weatherproof container" (Ziploc® bag) to the warehouse and to the support operations representative in garrison. The data then would be loaded into the respective STAMIS. For status information to flow back down to the customer, the new disks then had to be placed into the same weatherproof containers and sent back to the field with the next day's deliveries for distribution to the customers.

The Wireless Solution

This clearly was not an effective way to use our logistics technologies. The Army needed a way to replicate garrison networks in the field. Enter the wireless CAISI. The CAISI project engineers took full advantage of available technologies and developed a wireless CAISI. The new system is flexible, easy to use, and connects an entire brigade's STAMIS without wires. It transports easily and links unclassified logistics systems together through a wireless network.

CAISI consists of commercial, off-the-shelf technologies in a modular system, which permits components to be replaced without difficulty and will allow easy upgrades in the future. The system can function in garrison to extend the LAN to units without connectivity and to tactical environments without changing network addresses. The same system is used in the field and in garrison without changing anything. In a forward support battalion, the CAISI can establish a wireless LAN that can connect up to 294 systems that are widely dispersed throughout a support area and rapidly transmit the information through the tactical network.

The CAISI for division and below consists of a service support representative kit, 9 CAISI bridge modules, and 30 CAISI client modules. A CAISI will be assigned to each support battalion headquarters and will be used to set up wireless combat service support LANs from the brigade, through the division and corps, to the echelons above corps. It will connect all logistics STAMIS, including those used by maneuver units. The CAISI will provide industry-standard connectivity for all computer users in the BSA. This means that any unit in the BSA will be able to use the Internet or any other network system to support its operations.

The client module, which weighs only 9 pounds, is the actual user level of CAISI. It consists of a base unit that can connect seven computers and allow them to transfer information via line-of-sight radio to the bridge module. The actual user interface with the client module is simple to operate: plug a computer into it, set up the antenna, and turn on the switch. The system can transmit information securely up to 2 kilometers with a data transfer rate of 11 million bytes per second.

The bridge module serves as a relay station for the client module. This component weighs 25 pounds, including the antenna. It can transmit data at speeds of 11 million bytes per second to a distance of 6 kilometers. In addition to relaying signals from client modules, it can support up to 14 computers wired directly into it. The bridge module is maintained by the support battalion S6 (automation officer) and monitored by the STAMIS user. One bridge module is located with the signal section in the BSA. There, CAISI interfaces with the network encryption system and enters data into the tactical packet network (TPN). The data move through the TPN to other LAN locations and systems, providing a theater logistics network. This permits real-time data transfer and assists with meeting the Army's goals for Velocity Management, Total Asset Visibility, and just-in-time logistics. This digital network upgrade increases transmission speeds and enables the use of web-based logistics.

The Brigade Revisited

Here's how information would flow in that same brigade at Hohenfels using CAISI. The ULLS-G computer would connect to a client module located in the BSA. When the operator ran the requisition and maintenance processes, the signal would transmit data to the bridge module. The information for the maintenance update would travel through the BSA to the SAMS-1 computer

and enter the system. The supply data would move through the base bridge module, through the signal node, and into the TPN, where it would connect with the SARSS-1 computer at home station. The SAMS-1 computer would conduct a maintenance update, and its data then would be transmitted to the SAMS-2 computer at home station. The updates would pass back through the TPN to the ULLS-G system in the BSA. The entire process would take just a few minutes, and no one would have to get up from his chair!

Other Benefits and Limitations

CAISI also supports garrison logistics operations. The system can be used to transmit data without using the Directorate of Information Management's LAN. This will greatly enhance capabilities in areas like Germany, where many installations do not have networks and still use modems to interact. A major benefit of CAISI is that the network addresses used in garrison remain the same when the unit goes to the field or deploys. This prevents blackout periods while the systems are reconfigured or wire is put in place.

The new CAISI does have some limitations. The first is that it is a line-of-sight transmission system. This means that transmission distances are dependent on terrain features and manmade obstacles. Increasing the number of bridge modules in the support areas minimizes this problem. However, each bridge module can relay the signal of any client or bridge module; there is no one path for a client module to reach the root bridge module. Instead, the signal automatically follows the quickest path from the client module to the root bridge module into the mobile subscriber equipment network.

Another limitation is supporting bridge modules that do not have a small extension node (SEN) switch operating in the area. (An SEN switch consists of an S-250/E shelter mounted on a high-mobility, multipurpose, wheeled vehicle. The SEN switch contains switching, multiplexing, and communications security equipment that supports the secure digital communications of a command post.) This problem can be alleviated somewhat by limiting the distance from the bridge module to the forward support area and eventually will be overcome by more advanced signal technologies.

The wireless CAISI fills a critical role in logistics support and advancement. By providing wireless communications, CAISI reduces set-up and tear-down time, covers a broader area, and supports more users in a given area with data speeds high enough to support web-based logistics. It puts the logistics community on the path to providing real-time logistics data and enabling faster requisitions. This makes CAISI an important tool in providing responsive and efficient support to our combat operations. ALOG

Captain Joseph M. Colacicco is the Supply and Services Officer in the office of the XVIII Airborne Corps Artillery G4 at Fort Bragg, North Carolina. He is a graduate of the Quartermaster Officer Basic Course, the Combined Logistics Captains Career Course, Airborne School, the Aerial Delivery Materiel Officer Course, and the Petroleum Officer Course.

Excepted from the Team C4IEWEWS, comprised of the US Army Communications-Electronics Command (CECOM) Contributions website

Why could CENTCOM always count on both secure and non-secure communications getting through?

A: CECOM deployed systems engineers to optimize voice and data systems for CENTCOM in advance of Operation Iraqi Freedom, significantly increasing command and control capabilities during the campaign. In addition, system engineers assisted PM Tactical Message System in the training of deploying units; and teamed on an accelerated schedule with the Army Network Command to upgrade the CENTCOM (Forward) Command Center in Qatar. The Combat Service Support Automation Information Systems Interface (CAISI) managed by the PEO EIS enabled a secure wireless local area network for Combat Service Support units in theater—connecting facilities that previously had no communications.



Cisco Aironet Wireless Bridges Help Army Communicate with Deployed Units

Regardless of their locations, forward-deployed units of the United States Army can communicate quickly and reliably through a wireless network that employs Cisco® Aironet® wireless bridges and wireless workgroup bridges. Following field-testing in Afghanistan, the Army has authorized procurement of approximately 11,000 Cisco Aironet wireless bridges.

Background

To operate effectively, the U.S. Army must be organized, trained, and equipped primarily for prompt and sustained combat associated with operations on land.

To accomplish its mission, especially in the combat service support (CSS) arena, the Army relies heavily on its Standard Army Management Information Systems (STAMIS). The Combat Service Support Automation Office (CSSAMO) provides customer assistance for the Army's STAMIS systems, including software, limited hardware and technical support.

The CSSAMO also plays an essential role in distributing new STAMIS equipment to the field and, with guidance from the New Equipment Training teams, the CSSAMO will usually spearhead new equipment fielding.

Challenge

Following Operation Desert Storm, the Army issued a directive to eliminate "sneaker net," the process of hand-carrying floppy diskettes across the battlefield in a deployed support area. Instead, the organization wanted to provide STAMIS with automated access to the Army's tactical packet network. This prompted development of the Combat Service Support Automated Information System Interface (CAISI). CAISI will be the backbone element for the Sensitive but Unclassified (SBU) network supporting the CSS community on the battlefield.

Subsequently, the Army authorized testing of an upgraded version of CAISI, which would incorporate standard commercial off-the-shelf (COTS) wireless technology with a Federal Information Processing Standard (FIPS) 140-1-approved in-line encryption. CAISI would thus integrate COTS equipment into modules designed specifically for military use. The goal was to revolutionize CSS communications in deployed support areas.



Solution

The US Army Information Systems Engineering Command (ISEC) of Ft. Huachuca, Arizona, designed the CAISI solution, which has been specially adapted to work in rugged conditions. The ISEC design includes CAISI bridge modules (CBM), and CAISI client modules (CCM). The CBM uses a Cisco Aironet 350 Series wireless bridge as its radio, while the CCM uses the Cisco Aironet 350 Series workgroup bridge. Both the CBMs and the CCMs have an inline encryption device and Ethernet hub(s).

Cisco Aironet 350 Series wireless bridges and wireless workgroup bridges use IEEE 802.11b standard in the 2.4 GHz band, with an 11 Mbps data rate. These bridges combine with the CAISI “ruggedized” antennas and reach up to four miles with clear line of sight. CAISI is designed to provide encrypted wireless connectivity for the unclassified logistics systems in a deployed seven-square-kilometer brigade support area. Logistics computers use their regular network interface card to connect to the hub in the CAISI bridge module.

The Fortress Technologies AF-1100 has been validated for FIPS 140-1 to provide inline encryption, and is approved for SBU government data. A CAISI module and antenna is deployed into each tent, van, or shelter that has logistics computers. A single CAISI module includes up to 30 CCMs and nine CBMs. One CBM at each field site is designated as the central, or “root,” node. This node controls the LAN for that field site, sets parameters for, and directs traffic among, other radios in the network. The root node normally links the CAISI LAN to an unclassified but sensitive Internet protocol router network (NIPRNET) port through the long-haul connections provided by Mobile Subscriber Equipment (MSE) or the newer Brigade Subscriber Node (BSN).

Results

Following a four-year development, testing, and procurement process that ensured selected products conformed to Department of Defense frequency regulations, security policies, and legacy application compatibilities, the Army started officially fielding CAISI equipment in June 2002. CAISI is now being used extensively in Army deployments in southwest Asia.

CAISI systems engineers from ISEC were sent to Afghanistan in October 2002 to train and assist in the deployment of CAISI modules in a brigade support area. Some trees and buildings were obstructing line-of-sight between the bridges, but after carefully positioning and configuring three of the modules to act as relays for the others, the network was operational.

CSSAMO personnel soon became confident with their new equipment and installed CAISI modules in 15 remote locations supporting approximately 50 users. CAISI is used for a number of applications, including supply chain management and maintenance.

Additionally, in a deployed environment, NIPRNET and e-mail service is often limited to a few terminals near the headquarters. While the primary purpose of CAISI is to provide network connectivity between logistic systems within the brigade support area, the soldiers who are located in the CAISI remote sites now have access to a local e-mail server, resulting in a significant boost in moral.

Next Steps

The CAISI effort is addressing ongoing deployment requirements as quickly as possible. All brigade and rear logistics units throughout the Army are scheduled to receive CAISI equipment within the next three years. During that period, the Army will purchase approximately 11,000 Cisco Aironet 350 Series wireless bridges and wireless workgroups.



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the
Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992-2003 Cisco Systems, Inc. All rights reserved. Aironet, Catalyst, Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)