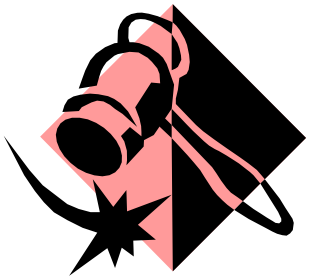
INFORMATION RESOURCES MANAGEMENT COLLEGE

Summer 2005
Volume 10, No. 3



# Info Tech Talk

Focusing on Enabling Information Technologies by the IRMC Organizational Transformation & Technology Department

## *From Horses to Coffins: Internet Auctions and Government Business*

**By LTC John S. Holwick, U.S. Army**
**ICAF and IRMC's Information Highway Student**

Inside this issue:



*Internet auctions have started a revolution in the way that the government both sells its excess property and streamlines its complex acquisition process.*

### E-Auctions - Leveraging a Worldwide Market

Internet auctions have entered the mainstream eBusiness since eBay started out as a means to bring collectors of cheap PEZ brand candy dispensers together. Today eBay is an auction powerhouse and shares the Internet with many competitors from Sotheby's, for fine collectibles, to Manions, for the military antique connoisseurs. The virtual gavel is now closing sales across the Internet everyday. Sellers can now reach a worldwide market, and buyers are finding access to an unheard number of products. The Bush Administration has embraced eCommerce as a means to streamline the government's acquisition and disposal process. [1] Now many government agencies, from the Department of Agriculture to the Small Business Administration, have opened on-line auction venues. The Department of Defense (DoD) was one of the first to recognize the potential savings from using this new tool. Internet auctions have started a revolution in the way that the government both sells its excess property and streamlines its complex acquisition process.

### Forward Auctioning - Cleaning Out the Garage

The traditional Internet-based forward auction process provides the government an efficient means to dispose of its excess items. Internet sales have given various agencies an avenue to dispose of over 4,000 foreclosed homes and market more than $175 billion in loans to the public in a single year while increasing efficiencies and reducing costs.[2] Real-time online bidding (E-Cry) permits the government to reach a wide market without incurring the added expense of having to set up central "war rooms" for the bidders. The Defense Reutilization and Marketing Service (DRMS) is using the Internet to leverage an international audience for its surplus items. Utilizing an outside firm, Government Liquidation LLC, the Defense Department has sold everything from aircraft parts to coffins to big screen television sets.[3]

In one Internet auction, Fort Hood's DRMS auctioned two retired military horses for $500 to an individual whose father had served in the cavalry. With this broad Internet audience, the government is able to leverage a fair price for its goods but the buyer can no longer expect to purchase the $1 yacht from traditional federal property auction.[4] Despite his new eCommerce competition, the buyer will always have the incentive of getting a good deal to draw him back each time. One bidder managed to purchase 2,000 ammunition cans for 15 cents each and resold them for $4 a can. With just a $300 investment, this buyer managed to net an $8,000 profit on the transaction. [5] Through numerous outside contractors, to include www.govliquidation.com, www.fedbid.com, www.bid4assets.com and www.firstgov.gov, the government is able to leverage an Internet audience to achieve the best return for the disposal of its excess property.

*(Continued on page 2)*

# From Horses to Coffins (cont.)

*(Continued from page 1)*

**The Reverse Auction - Getting the Most Bang for the Taxpayers' Buck**

The traditional forward auction only allows the government to recover a portion of the money it has already spent. The reverse auction, in which numerous bidders vie to win a buyer's business, is an eBusiness forum that has the potential to truly leverage the best deal for each acquisition dollar. For several years, reverse auctions have revolutionized procurement in the business-to-business (B2B) community. Defense contractors, from United Technologies to Raytheon, have used this forum to secure necessary components at often 20% savings over traditional buying methods. [6] Individuals have also embraced this Internet process as a means to garner the lowest prices on items from automobiles to hotel rooms on such sites as Price.com. The Acquisition Directions Advisory, best describes the reverse auction as "a fierce [event] where bidders don't just get one shot at getting the business, they keep re-bidding and lowering their price, depending on their competition, until they are successful or unwilling to go any lower to continue in the process. The government clearly reaps a benefit." [7]

Prior to 1997, Federal Acquisition regulations prohibited any agency from using auctions to procure products or services. Because of civilian sector savings in the 22-28% range, the General Services Administration surrendered to the changing times. As the Army's Deputy Associate Administrator for Acquisition Policy admitted, "Today, we know that reverse auctions are a good tool in certain types of acquisitions and in certain situations."[8] This type of auction is best suited for buying off-the-shelf technology, from computers to auto parts, and negotiating the best deals on services. The Army Corps of Engineers found that reverse auctions did not result in a significant savings over the sealed bid process for construction projects, but acquisition experts still expect an overall savings of more than 10% throughout DoD each year. [9]

These eCommerce reverse auctions are streamlining the acquisition process by getting products and services to the warfighter faster and at a more competitive price. The reverse auction process works as follows: [10]

◊ An agency posts the items or services it wishes to purchase on a website.

◊ At the designed time, registered pre-screened contractors in the Central Contractor Registration System submit their bids online at the secure website.

◊ During the auction period, the submitted bids become progressively lower.

◊ Bids are accepted until a designated deadline.

◊ If a bid is received within the 60 seconds of the deadline, the auction is extended for an additional five minutes.

◊ Upon the conclusion of the bidding, the agency announces the winner who has agreed to meet its requirements for the lowest cost.

While the forward auction seller seeks out the highest bid for his product, the reverse auction buyer strives to secure the lowest price for something he needs. The Army's Communications-Electronics Command was able to purchase notebook computers, and secure fax machines, at reverse auction for a 37% savings over traditional procurement methods. In another auction, this same agency watched bids for Patriot missile connectors fall from $1,080 to $780 in a matter of minutes. [11] Internet reverse auctions continue to save the government billions of dollars each year. At the same time, this process opens up a venue for small businesses to compete outside of the normal Byzantine bureaucratic acquisition process.

**We're Not in Kansas Anymore: The Challenges of Ecommerce**

While Internet auctions are revolutionizing the way business is done today, it is not without its challenges. The traditional forward auction process provides an open forum for a wide range of illegal activities. Aside from the normal occurrences of bidders failing to complete their transactions, the Internet is plagued with individuals attempting to sell illicitly gained products. The Air Force's Office of Special Investigations found an antiques dealer attempting to sell sensitive aircraft communications components online with eBay and the Federal Bureau of Investigations continually monitors Internet auction sites for sellers trying to pass off stolen items. [12] The established Internet auction sites attempt to counter fraud through mandatory registration of participants, monitoring of items on the site, and establishing escrow ac-

*(Continued on page 3)*

*(Continued from page 2)*
counts for transactions through such brokers as PayPal.

Reverse auctions are not without their own risks. Aside from the common areas of fraud that occur during forward auctions, reverse transactions have their own challenges. There are incidents in which vendors either default on the promised contract, or substitute an inferior item to cover their losses, when they realize they have bid too low. The General Services Administration is concerned that the reverse auction process lends itself to the lowest bidders ending up operating on too thin a margin, and damaging the civilian business market in the long run. [13] The acquisition community continues to fine-tune the auction process for such improvements as electronic bid protests (E-protests). Still, the vast majority of vendors who participate in these auctions feel they are fair. Even the losing bidders report that the overall process is inclusive. [14]

**Leveraging the Marketplace through eCommerce Auctions**

Internet auctions are providing government agencies an effective means to leverage a worldwide audience for disposing of surplus items while guaranteeing a competitive market for its own product and services procurement requirements. The Internet is revolutionizing the acquisition process in a time of constrained budgets. The virtual gavel is now closing sales across the Internet allowing sellers to reach a worldwide market, while giving buyers access to an unheard number of products. If we continue to refine this venue, the government can realize savings for common products and services of more than $6 billion a year.

**References**

[1] Saffir, Barbara J. U.S. Auctions Offer Coffins, Horses Online, The Washington Post, Washington, D.C., 3 September 2002. p. A-15.

[2] Sisk, Michael. Uncle Sam's New Market is Virtually Impossible to Ignore" U.S. Banker, Volume 112, Issue 9, Online, September 2002, (http://search.epnet.com/login.aspx?direct=true&db=bsh&an=7305051)

[3] Saffir. p. A-15.

[4] Ibid. p. A-15.

[5] Schwartz, Karen. Government Auctions Grow Up; In the Mood for a Bargain? Check Out the Auction on Auction Sites Specializing in Government Surplus Property, Information Week, 22 December 2003, p. 1.

[6] Elgart, Edward G. Army Reverse Auctions: An ECommerce Acquisition Tool, The Public Manager, Volume 30, Spring 2001, p. 13.

[7] Ashley, Patti. Who's Afraid of Reverse Auctions?, National Contract Management Association, June 2002.

[8] Schwartz, Karen D. Reversal of Fortune, Government Executive, Volume 36, Issue 1, January 2004, p. 58, Online, http://search.epnet.com/login.aspx?direct=true&db=mth&an=12183185

[9] Wyld, David C. After September 11th: Reverse Auctions in Government Procurement, Editorial, National Contract Management Association, February 2002.

[10] Dollase, Steve. Reverse or Forward…Auctions Save Dollars, The Navy Supply Corps Newsletter, January/February 2003, Online, http://www.navsup.navy.mil/npi/lintest/jf03/Pages/reverse.htm

[11] Elgart, Edward G. Army Reverse Auctions: An ECommerce Acquisition Tool, The Public Manager, Volume 30, Spring 2001, p. 13.

[12] Caram, Ed. A Hot Deal on Spy Gear, Newsweek, Volume 139, Issue 21, 10 June 2002, p. 18

[13] Alert: Government Regulations/Government Contracts, Federal ECommerce: Reverse Auctions, Shaw Pittman, Washington D.C., Number 1, September 2000, Online, www.shawpittman.com

[14] O'Hara, Colleen. Feds Buy In to Reverse Auctions, Federal Computer Week, Falls Church, VA, Volume 14, Issue 28. 14 August 2000, p. 50.

# *IT Security Trends and Solutions*

**By Professors Paul Flanagan, James Kasprzak and Les Pang**

The Gartner IT Security Summit 2005 was held in early June and numerous security managers, practitioners, and experts participated in the conference. Attended by several IRMC professors, here is a list of their observations of the security landscape as presented by the IT security community including Gartner analysts.

A Gartner survey revealed that the first priority among organizations is addressing budget and cost constraints while the second priority is security issues and concerns. Considering both priorities, demonstrating value for security has become a key concern among managers.

In terms of funding and legislation, Congress has placed cyber-security behind physical security. Many of the IT security experts are arguing that cyber-security is closely linked with physical security.

**"...demonstrating value for security has become a key concern among managers."**

California's law that requires companies to tell citizens about security breaches has made a profound effect on the public awareness of identify theft particularly after the disclosures made by ChoicePoint and LexisNexus. The point was made by several analysts that changes in laws will have profound impacts on an organization's future security and privacy policies.

Security experts recommend that government agencies have security "built-in" as part of the procurement process. Also, government should consolidate and leverage its significant buying power to help reduce its security costs. Furthermore, government needs to improve its own act when it comes to security as shown by the low FISMA scores.

Emerging security threats involve the newer technologies including RFID, wireless LANs, VoIP, Bluetooth and service-oriented architectures. "Ransomware" was mentioned as a way that a hacker can "lock up" a key electronic document and holding it for ransom.

Spyware and its solution, anti-spyware programs, were significant topics. One of the more dangerous variants of spyware is the keystroke logger programs. These programs are able to record every key punched at a computer and offer a significant threat particularly in terms of capturing user information for use in spreading spyware. One consultant indicated that as many as 40 percent of all machines attached to Internet have spyware. About 3-4% of these have some malware attached. To prevent spyware from getting on a system, one should avoid downloading freeware, consider using an open source browser, install and run anti-spyware software, and use the MAC operating system or the latest version of the Windows operating system with the most recent patches loaded.

Anti-spyware is becoming more of a necessity. There are some freeware products such as Lavasoft Ad-Aware and Spybot Search and Destroy. There are some standalone vendor solutions for enterprises -- Spy Sweeper and Spy Catcher are two examples. (No endorsement of these products is implied or expressed.) Many well-known anti-virus vendors are blending anti-spyware into their current product offerings.

Public key infrastructure (PKI) is being morphed to a concept called public key operations (PKO). Although still important for e-government, PKI has had implementation problems related to user acceptance, system complexity and too many players involved. PKO promises user transparency since PKI features will be embedded in applications and PKO will be used selectively -- as opposed to an enterprise-wide application characteristic of PKI.

Secure sockets layer (SSL) has become the standard for securing electronic transactions on the Internet including providing most of the security requirements for web services. Transport layer security (TLS) is being pushed by standards bodies such as IETF to be the successor to SSL.

Best practices in IT security can often be found in the Code of Practice for Information Security Management (ISO 17799) as well as National Institute of Standards and Technology (NIST), IT Infrastructure Library (ITIL), Control Objectives for Information and Related Technology (COBIT) and Committee of Sponsoring Organizations of the Treadway Commission (COSO) publications.

When it comes to IT security, an expert suggested following the time-honored mantra: "Think globally…act locally."

# What's WiMAX and Why You Should Care

## By Professor Russell Mattern

Worldwide Interoperability for Microwave Access (WiMAX) may be one of the most disruptive technologies to emerge according to a number of recent articles. (Mannion, 2005; Rivituso, 2005 and TechwebNews, 2005) This article explores WiMAX's superb capabilities, compares it to current broadband technologies and discusses what must happen to assure its proliferation. As with any new technology, security issues and projected cost must be considered. Finally, possible uses within the Department of Defense (DoD) are explored.

WiMAX is an emerging wireless technology that offers users bandwidth capabilities equal to or greater than Wireless Fidelity (WiFi) with ranges that far exceed WiFi's 300-foot limit. (WiMAX Forum) WiMAX claims ranges up to 30 miles in rural, unobstructed areas. In urban or obstructed areas, range can drop to 2-5 miles. (Intel, 2004 and Diaz and Takahashi, 2004) As a point of reference, WiMAX and the IEEE 802.16 standard, Wireless Metropolitan Area Network (MAN), tend to be used interchangeably in the literature. (WiMAX Forum, 2004) In its original form, WiMAX was to use frequencies from 10 to 66 GHz but later evolved to include non-line-of-sight, licensed and unlicensed sub-11GHz frequencies all the way down to 2 GHz. (WiMAX Forum, 2004 & NetworkWorldFusion, 2004) One company, Aloha Partners, has received Federal Communications Commission (FCC) permission to conduct tests in the 700MHz range. (Mannion, 2005)

WiFi hot spots have been with us for some time now. Patrons of Starbucks and other businesses can ride the wireless signal to the Internet while sipping espresso or eating a Danish. Many homeowners have set up wireless access points in their homes to share computing power and peripherals. This technology produces useful ranges of 70-150 feet. While WiFi, with its IEEE 802.11a/b/g standards, and frequencies of 5.0 and 2.4GHz may have solved the local premises connectivity problem, WiMAX is viewed as a "last mile" solution. (Intel, 2004)

The last mile problem is associated with bringing broadband capabilities to the masses. Currently, home and small business users must obtain their primary broadband capability using cable modems, satellite dishes, or Asymmetric Digital Subscriber Lines (ADSL, usually abbreviated to DSL). Even WiFi users must obtain their ultimate broadband connection to the Internet via the same modalities. The advent of WiMAX offers a very elegant solution to this 'back haul' problem of how to make the broadband connection to the Internet and is why WiMAX has the potential to be so disruptive. (WiMAX Forum, 2004)

Consider the case of Verizon in the DC metropolitan area. They offer DSL via your phone line with download capabilities theoretically as high as 8 Mbps. Since 8 Mbps cannot always be delivered, we generally see advertised speeds of 1.5 Mbps with upload speeds of 640 kbps under perfect conditions down to 64 kbps when conditions are poor. The reason that actual performance is lower than the theoretical is based on signal attenuation due to distance from the central telephone office to your home or office. This attenuation limits DSL to a distance of 18,000 feet. Voice coils used to amplify voice signals over phone lines become a showstopper for DSL by cutting off the broadband signal entirely thus limiting overall reach and usefulness. (Franklin, 2004)

Therefore, in a contiguous town or neighborhood, some potential DSL users will be beyond the range of the central office and/or have voice coils blocking their access to service, creating broadband 'haves' and 'have-nots.' While DSL has its own technical limitations, so does broadband via cable.

Cable-based broadband enjoys more customers than DSL due to its significant penetration into the home television entertainment sector. Current cable TV customers can quickly add a cable modem to access broadband capabilities. Cable, however, has its own issues. One is that service can vary from neighborhood-to-neighborhood. A cable circuit must be fully installed before customers can gain broadband access. Thus in neighborhoods under construction, access must await build-out. Further, cable modem users share the line's capacity. If usage is high, upload and downloads speeds suffer -- never reaching their 30 Mbps potential. In fact, during periods of peak usage, DSL users' up- and download speeds can exceed cable modem users. (Mitchell, 2004)

**What's the Alternative to DSL and Cable?**

Enter WiMAX. Consider that all neighborhoods and businesses can have immediate access to broadband with performance of up to 54 Mbps. No need to lay coaxial cable, fiber, or phone lines—no huge capital outlays before the first revenues are realized. Next consider that WiMAX is not only a solution to broadband connectivity to the Internet, it can also be the solution for Voice Over Internet Protocol (VOIP) phone capability thus truly making your home phone and cell phone one and the same. The possibilities do not end here; WiMAX could also replace your cable or satellite television programming and eliminate XM satellite and Sirius satellite radio. WiMAX offers the possibility of achieving true convergence. Homes and businesses that have already installed WiFi networks can still use WiMAX for their back-haul needs without significant outlays.

**What Stands In The Way Of WiMAX Rollout?**

Standards and standard chip sets! The current IEEE standard for WiMAX is IEEE 802.16d. It will offer 300 Kbps to 2 Mbps speeds while the 802.16e standard will address mobile computing. The three most popular bands appear to be 2.5, 3.2 and 5.8GHz. The 5.8GHz frequency is licensed in many parts of the world

*(Continued on page 10)*

# Cutting Edge Technologies for Homeland Security

Asa Hutchinson

Asa Hutchinson, former Undersecretary for Border and Transportation Security in the Department of Homeland Security, spoke at a recent breakfast meeting sponsored by Government Executive magazine (no endorsement implied or expressed). Among the items he discussed was the topic of technologies used by Homeland Security to secure the United States from terrorist attacks. These included the following:

**Unmanned aerial vehicles (UAVs)** - U.S. Customs and Border Protection now use UAVs as part of their Arizona Border Control Initiative. These vehicles permit better border coverage and faster response times in rugged, desolate areas of the southwest border. As the first non-military use of UAVs for border protection, they supplement ground security efforts with a live video feed of potential illegal smuggling as it occurs.

**Ground sensors** – One example is the use of thermal exposure sensor technology to increase the safety of fire fighters and other first responders.

**Surveillance cameras** – For example, an infrared camera system at the port of Valdez can reveal objects crossing Prince William Sound in rain, fog, snow and darkness. This maritime surveillance system supplements the present extensive maritime and land-based homeland security measures.

**Software** – Software applications help to sort out the data gathered from surveillance initiatives and identify terrorist threats.

**Radiological screening equipment** – This equipment will prevent terrorist attack involving the use of penetrating radiation.

**Biometrics** – This is defined as the use of a measurable physical characteristic or personal behavioral trait used to recognize the identity or verify the claimed identity of an individual. Among the features that can be measured are face, fingerscans, hand geometry, handwriting, iris, retina, vein and voice. As part of the entry and exit process for aliens, Homeland Security's US-VISIT program has the capability to capture biometrics (initially, digital fingerscans and photographs) at airports and seaports.

Mr. Hutchinson stated the need for continued investment for technology as well as a priority requirement for agencies to share information. Relevant performance metrics are also needed to measure and ensure program success. He pointed out that integration is possible without merging agency divisions which may result in a large, dysfunctional body.

Reference: Dept. of Homeland Security web site

Unmanned aerial vehicle.

Thermal exposure sensors are embedded in these firefighting devices.


Finger scan instructions used in DHS's US-VISIT program.

# *Technology Briefing: Biometrics for the Enterprise*

By Will Cladd, Michael Cuccio, Patrick Lee, Patricia Quinn and Ron Tyler
"Changing World of the CIO" Students

The most popular method of authenticating users in the enterprise consists of them entering a login ID and password to gain access to various resources on the network. Depending upon the resource (local network services, databases, websites, etc.), users may often be required to remember several passwords. This can result in users forgetting their passwords, users creating passwords that are easily guessed or users writing passwords down that can be compromised, all of which expose the enterprise to security breaches. Passwords have been utilized since the 1960s as a technique for authenticating users to computer systems—only to become the most popular way to intrude into those systems. The use of biometrics will not only simplify the method in which users gain access to enterprise resources, but will also result in tighter security and less calls to the help desk when one forgets a password.

"Biometrics" is a general term for the verification of individuals using unique biological characteristics. It is an identifier that measures a person's unique physical characteristics or behavior and compares it to a stored digital template to authenticate identity. Biometrics can be *physiological* based (something you are born with--i.e., iris, fingers, hand, face, etc.) or *behavioral* based (i.e. signature, gait, voice, etc.). Biometrics is who you are and what you are. It cannot be lost, stolen or duplicated unless one is willing to take extreme measures, say for example, to severe someone's finger to gain access. Also, unlike traditional methods involving passwords or PIN numbers, biometrics require the person desiring access to be physically present. The benefits of biometrics are increased security, increased convenience, decreased costs, and freezing/fixing identity. Since each individual is unique, biometrics can greatly reduce the risk of identity theft, an ever-increasing problem in society. Additionally, people will not have to worry about carrying numerous forms of identification which can be lost or stolen.

**This essay on biometrics is an example of the results of one assignment during the 12-week distributed learning Changing World of the CIO Course.**

**Last quarter's Info Tech Talk included an article on Voice Over Internet Protocol (VOIP) which was created as an exercise during the Information Technology Trends and Assessments lesson of the Changing World of the CIO course. Throughout this interactive course, students complete a mix of individual and group assignments. A few of the other assignments include developing best practice articles, debating whether IT matters, and case study role-playing. Consider adding an IRM College Distributed Learning course to your repertoire of accomplishments.**

***- Dr. Kathleen Schulin, Course Leader, Changing World of the CIO***

## Potential Issues and Challenges

Biometrics is not a new technology but is quickly becoming very technologically advanced. The more complicated it gets, the more expensive it gets. The technology is not fully developed and will take years and great expense for it to be developed to a point where it is truly secure. There are still concerns with the accuracy of the technology because biometric indicators may produce false positives and false negatives.

Other issues are legal challenges related to privacy and data protection. Many view biometrics as creating something akin to an Orwellian society. Concerns exist about people having information on them compromised especially upon enrollment in a biometric system. Fall-back procedures are another issue in the event of failure of biometrics equipment. Lastly, there are cultural and social issues such as religious concerns with certain biometric techniques and fears of retinal scanning and other perceived intrusive approaches.

*(Continued on page 8)*

# Biometrics (Cont.)

*(Continued from page 7)*

**Military and Government Applications**

Biometrics are used in today's military mainly through fingerprint identification in the Common Access Card. The index fingerprint is recorded but the use of fingerprints for verification is not commonly used. Although biometrics are not largely used by the military at this time, the Department of Defense is elbow-deep in biometric development and has created a Biometric Management Office. The military can use biometrics to verify in a timely manner the identity of people seeking access to military facilities, enhance force protection measures, and have an audit trail of people accessing certain spaces.

Face recognition biometrics have been used for homeland security, fingerprint biometrics for authenticating cargo truck drivers at Chicago's O'Hare airport and biometric-based e-passports at the State Department. Biometrics are also widely used in forensics such as criminal identification and prison security.

**Measuring Success**

Performance metrics are necessary to determine the strengths and weaknesses of technologies under consideration for a given application. Key performance metrics are listed in the table below.

These metrics can be measured with regard to numbers of false acceptance/rejects, numbers of impostor verification attempts, etc.

In addition to the above *quantitative* metrics, a *qualitative* assessment should be conducted to measure user satisfaction. This can be performed by collecting customer survey data. Further indicators of success would be a decrease in the number of help desk calls relating to user access.

**Future Outlook**

Biometrics technology will be used much more frequently in the future. In today's global environment, the need for identity assurance is driven by our network centric infrastructure. Methods of biometrics will become more and more technologically advanced and more secure. As the war on terror intensifies, many countries have begun or are considering the use of biometrics for border control and national ID cards. Recent developments include the use of body odor and DNA as biometric indicators.

**Conclusion**

The introduction of this new technology should be conducted in phases -- starting with a small population of the enterprise. Consideration should also be given to the current enterprise architecture to determine the best method for integrating the technology into the enterprise infrastructure. Gradually the effort should expand to the entire enterprise and become a part of the daily way of doing business.

References

http://www.informationweek.com/story/showArticle.jhtml?articleID=159401600&tid=5978

http://www.washingtontechnology.com/news/1_1/daily_news/25771-1.html

http://www.macnewsworld.com/story/33554.html

http://www.publictechnology.net/modules.php?op=modload&name=News&file=article&sid=304

| Metric | Description |
|---|---|
| Failure to Enroll Rate (FTE) | Where the potential user is unable to enroll due to an insufficiently distinctive biometric sample (i.e. amputee). |
| False Accept Rate (FAR) | Incorrect identification of an individual |
| False Reject Rate (FRR) | Failure to identify an enrollee |
| Failure to Acquire Rate (FAR) | Biometric system is unable to capture a sample of sufficient quality |
| Crossover Rate | Crossover is where the FAR and FRR would be equal |

# Words from an RFID Guru: Bill Nuti, CEO, Symbol Technologies

We are moving from wired to wireless, from batch to real-time, from fixed to portable and from client server to "client-net." Next is the age of mobility which provides organizations the potential for increased efficiencies and improved customer relations.

The following are examples of where government has the potential in transitioning to this new mobile era:

The Federal Drug Administration uses RFID technology to reduce the high rate of deaths in hospitals due to administrate the wrong drug, at the wrong time or at the wrong dosage. There is a "ludicrous" span of control among nurses – 13-15 patients per nurse. They need all of the capture technologies they can get to manage patient care data.

Using mobile devices in hospitals, the Veteran's Administration can offer better services, improved control and reduced costs – all of this will help in reducing taxes.

The Department of Defense offers numerous storefronts. The agency should follow Wal-Mart's data capture and wireless strategies to integrate and better access these storefronts.

Other opportunities for improvement include the increased efficiency of passenger flow, secure cargo shipments, and an architecture that leverages mobile devices for the soldier, postal worker, nurse and others.

Government needs to leverage the commercial sector to identify applications that meet their needs. This is particularly relevant now that there are less research and development dollars available in government.

Capture technologies started with laser bar code scanners at grocery checkouts and have expanded to include voice, imagers, biometrics, sensors and RFID.

UHF-based RFID tags now support extended read ranges of 20 feet. Now costing 30 to 50 cents each, passive tags are expected to drop in price dramatically in the near future. The read rate has improved to 97 percent. The technology has reduced inventory to help increase revenue. The technology has ensured that the right goods are provided at the right time, i.e., products are replenished at the correct time. The technology also helps to drive down shrinkage (undocumented losses).

To make the system work, partners are needed to support data processing at the back end and to provide system integration.

There is considerable misinformation out now on RFID. There are privacy concerns, but tags contain no personal information – it is basically a "talking" bar code. Passports with embedded tags cannot be read when they are closed and the read range for this application is in inches.

Requirements for mobile devices include:

- Device convergence – a single platform that supports PDA's, cell phones, MPEG players, instant messaging, etc.
- Durable – able to withstand short drops on the floor and adverse environmental conditions
- Compact – needed for portability
- Long battery life - the biggest drain is due to the radio and screen functions
- Manageable – downloadable patches, secure platform

Applications need to support asset management, e-mail, ERP systems, Homeland security, mobile CRM, point of service (e.g., DMV, passport service), scheduling, and others.

Technologies supporting the different network types include:

- Body area network – RFID
- Personal area network – UWB and Bluetooth
- Local area network – WiFi
- Metropolitan area network – WiMax
- Wide area network – 3G

Security issues with wireless networks are exaggerated. Eighty-four percent of those surveyed have not experienced any security breach to their wireless local area network according to Jupiter Research. Recent technologies have improved wireless security.

Where is it all going?

- Convergence of existing and new mobile technologies
- Seamless wireless access across the LAN, WAN and PAN
- Embedded and invisible mobile technologies
- RFID market to hit $8.3 billion by 2008
- Fully functional virtual office
- An "on-demand" world

Examples of the potential for connectivity include the following:

- Mobile pacemaker units which tell in real-time when vital signs are bad
- Mobile-based soda machine – sales will be notified when the machine needs servicing
- Cars with Bluetooth
- Smart appliances
- Mobile devices that is always with you (dock the device at work and at home to maintain constant connectivity)

# What's WiMAX and Why You Should Care (Cont.)

*(Continued from page 5)*

while 3.5GHz is not available in North America. The 2.5GHz frequency is licensed in the U.S. and many of the Americas. (NetworkWorldFusion, 2004)

With regard to the manufacturing side of the house, Intel is busy trying to produce chips that support the technology. Standard, easily reproducible chip sets are needed to lower the costs of implementation of this technology. (Rethinkresearch, 2004) Because there are several frequencies WiMAX will operate on worldwide, we will see a variety of chip set solutions and Customer Premises Equipment (CPE).

Further, there will be competition from 3G cell providers. WiMAX will certainly challenge the lower data rates offered by cellular 3G providers and may eventually lure customers away. Consider the ability to stream video to cell phones. Verizon currently offers downloading of video clips in this region. The better data rates of WiMAX may adversely impact 3G's growth. (NetworkWorldFusion, 2004)

**Are There Any Security Issues with WiMAX?**

WiMAX is susceptible as any wireless system to security issues. Compromises of the present WiFi systems abound. Consider the case of two hackers who tapped into a Lowes Home Improvement store via a network of wireless bar-code readers and collected credit card information as shoppers checked out. In another case, a hospital computer technician, who was testing new security software, detected an intruder and traced it to a medical supplier salesman sitting in the cafeteria and scanning emails headed for the purchasing department. One website posted a simple way to break into Cisco Systems products by publishing the default password -- apparently Cisco encourages its users to change the password but many do not. Scarier still is a product called QueTec 4-in-1. It allows any laptop to become a wireless transmitter and access point. The targets are unsuspecting users in airport lounges or any other location where laptop users congregate. Users unwittingly hop onto the signal to use the Internet while the hacker collects password and credit card data as it streams in. (Bulkeley, 2004)

User names and passwords help to protect wireless systems but they are not enough. Encryption is also needed. Some say we need to move from 128-bit to 256-bit encryption but that may not be enough. Roles-based rules can help. Some proprietary security systems using this approach are being used in the market place. For instance, the Aruba Wireless Network authenticates users and limits their access based upon roles. Additionally, they use integrated 'user-aware' firewalls. (Aruba, 2004)

An interesting 'black paper' on wireless security reviewed most of the available wireless security measures and then articulated the vulnerabilities of each. Using the 802.11b standard as a basis, each security method is discussed followed by how it can be defeated or compromised. It begins with the setting of the Service Set Identifier (SSID). For Linksys systems its factory setting for the SSID is 'linksys' and for Cisco, it is 'tsunami.' Both venders recommend you rename the SSID using the same principles used to generate strong password protection to reduce vulnerability. (ARS Technica, 2004)

Next discussed is use of Wired Equivalent Privacy (WEP). It can be attacked by ciphering the Initialization Vector (IV) which is only 24-bits long. It is just a matter of trial and error to discover it and break the WEP key. A second available attack is based on 'weak IVs.' Using this route, a determined attacker must accumulate massive numbers of packets and in doing so can decipher the WEP key. Finally, WEP key management is problematic. Each device on the network must have the proper WEP key entered into it. This is easier to do at system rollout but as employees leave and devices change, WEP key management becomes more difficult. Worse, if someone gives out the key, the administrator must change it for all devices or lose all security. (ARS Technica, 2004)

The paper then addresses Lucent Technology's attempt to secure wireless by turning off the SSID signal in their Orinoco WaveLAN product. They claim this makes their LAN a 'closed network' but it turns out that a determined attacker can still detect it. Other techniques involve 128-bit encryption, broadcast key rotation and Media Access Control (MAC) address filtering -- all provide increased security but they have vulnerabilities. Next addressed is the use of Virtual Private Networks (VPN) which in the wireless world have their vulnerabilities. The paper concludes with a discussion of Extensible Authentication Protocols (EAP). Several variants include EAP-MD5 based on the MD5 hash of the user name and password, Cisco uses EAP-Cisco Wireless (also called LEAP), Microsoft uses EAP-TLS and finally EAP-TTLS was developed by Funk Software. (ARS Technica, 2004)

A few conclusions from this article:

- ◊ The problems of securing 802.11b wireless will be very similar to those encountered securing WiMAX systems.
- ◊ All forms of wireless security may ultimately be vulnerable.
- ◊ Increasingly robust wireless security methods create increased management and usability difficulties.
- ◊ A layered security approach should be imperative.
- ◊ WiMAX will have to solve the security problem if it to achieve its full potential.

*(Continued on page 11)*

*(Continued from page 10)*

**What are the Projected Costs of WiMAX Implementations?**

One cost comparison estimated that up to 85 million homes could be served by WiMAX for $2B versus 18 million homes served by high capacity fiber for a cost of $4B. (Rivituso, 2005)

For residential customers, the Average Revenue Per Unit (ARPU) would be $30/month for WiMAX broadband service. VOIP's ARPU would be $20/month. Figure in $10/month for equipment lease and a one-time $50 activation fee. Similar rates are postulated for small to medium-sized businesses in this paper. The analysis makes monthly rates appear to be competitive with existing broadband services. We know that infrastructure build out will be significantly cheaper than that for cable or DSL. That would mean that rural communities would be good targets of opportunity for this technology as well as suburban and exurban areas that are under- or spottily-served by cable or DSL providers. (WiMAX Forum, 2004)

**WiMAX and the NetCentric Warfare -- What's the Future Look Like?**

Quickly deployable and redundantly backed-up WiMAX will give the warfighter a tremendous advantage on the battlefield. Bandwidth limitations were one of the shortfalls in the last two major conflicts in the Middle East. Once designed and fully tested, ruggedized versions of WiMAX could be deployed quickly and moved about the battlefield expeditiously as needed. WiMAX could fulfill the expectations of the 'digital battlefield' enabling the display of troop and vehicle locations to commanders and personnel taking part in operations. High quality video could be downloaded directly from Unmanned Aerial Vehicles (UAVs) to the troops who need the information. Battlefield commanders can make more informed decisions based upon more accurate information from the front. This technology also promises to improve communications across the battlefield -- it may obviate the need for certain types of radio systems currently under development.

WiMAX can also help win the peace. Take for example the telecom infrastructure situation in Iraq right after Saddam Hussein was defeated. At best it was poor to non-existent. Communications or the lack of contributed to the chaos reported. Immediate installation of WiMAX cell capabilities and the issuance of cell phones may have helped quell the chaos by allowing civilians to communicate with one another. Small as it may seem, the ability to communicate with the 'outside' greatly reduces anxiety and could have helped lead to a more rapid stabilization. Any place that flexible and high bandwidth operations are used within DoD should consider the use of WiMAX technology.

**Conclusion**

WiMAX's range and excellent data rates threaten the way broadband services are delivered today—it might in fact be the technology that brings broadband to the masses by solving the last mile problem. Its effects on broadband access however may pale in comparison to the impact it will have on the telephone, cable and satellite industries. We may see some of these industries literally disappear or morph into something not seen before. The recent round of mergers and acquisitions in the telecom world may be just the beginning of more changes to come. For the warfighter, it will change the way information is shared across the battlefield and greatly influence how battles are fought and won. WiMAX holds tremendous possibilities for the future--it will be very interesting to see where it is five years from now.

References

1. Aruba Wireless Networks Delivers Sharp Healthcare Painless WiFi. (Jul 19, 2004). Arubanetworks.com. Retrieved Mar 3, 2005 from http://www.arubanetworks.com/news/releases/viewrelease.php?d=20040717
2. Bulkeley, W. (Dec, 2004). Wireless Mischief—Cautionary Tales. The Wall Street Journal. Retrieved Mar 3, 2005 from http://www.ncl.ac.uk/iss/wireless/wirelessmischief.html
3. Business Case Models for Fixed Broadband Wireless Access based on WiMAX Technology and the 802.16 Standard (2004). WiMAX Forum. Retrieved 22 Feb 05, from http://www.wimaxforum.org/news/downloads/WiMAX-The_Business_Case-Rev3.pdf
4. Chen, E. and Cimino, J. (Nov-Dec, 2002). Use of Wireless Technology for Reducing Medical Errors. Journal of the American Medical Informatics Association. Retrieved Mar 3, 2005 from http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=410419
5. Diaz and Takahashi (2004). Taking WiFi to the Max: SiliconValley.com. Retrieved 22 Feb 05 from http://www.siliconvalley.com/mld/siliconvalley/business/technology/personal_technology/9831069.htm
6. Franklin, C. (2004). How DSL Works. HowStuffWorks.com. Retrieved 23 Feb 2005 from http://computer.howstuffworks.com/dsl3.htm
7. Fitton, L. (Feb, 2005). OneNote EMR Toolkit is for Physicians with a Tablet Computer. Medicaltabletpc.com. Retrieved Mar 3, 2005 from http://medicaltabletpc.com
8. Intel and Clearwire Forge WiMAX Alliance (Oct 29, 2004). Rethinkresearch.com. Retrieved Feb 9, 2005 from http://www.theregister.co.uk/2004/10/29/intel_clearwire_wimax/print.html
9. Koprowski, G. (Apr 30, 2004). Wireless World: WiFi Comes To Hospitals. United Press International. Retrieved Mar 3, 2005 from http://www.upi.com/view.cfm?StoryID=20040429-101218-5859r
10. Lawson, S. (Jul 6, 2004). WiMAX starting to make its move. NetworkWorldFusion.com. Retrieved 7 Feb 05 from http://www.nwfusion.com/news/2004/0607wimax.html
11. Mannion, P. (Mar 14, 2005). Can WiMAX Become A Disruptive Technology? EE Times. Retrieved 22 Jun 2005 from http://informationweek.smallbizpipeline.com/159402686
12. Mitchell, B. (2004). DSL vs. Cable Modem Comparison. About.com. Retrieved 23 Feb 2005 from http://compnetworking.about.com/od/dslvscablemodem/l/aa111200a.htm
13. Renden, J. (Feb 10, 2003). Medical School Heals Wireless LAN Vulnerability. SearchNetworking.com. Retrieved 3 Mar 2005 from http://searchnetworking.techtarget.com/originalContent/0,289142,sid7_gci879556,00.html
14. Rivituso, M. (Apr 5, 2005). The Next Disruptive Technology. SmartMoney.com. Retrieved 22 Jun 05 from http://yahoo.smartmoney.com/Techsmart/index.cfm?story=20050405&afl=yahoo
15. To Err is Human: Building a Safer Health System. (Nov, 1999). Institutes of Medicine. Retrieved Mar 7, 2005 from http://www.iom.edu/Object.File/Master/4/117/0.pdf
16. Understanding WiFi and WiMAX as Metro-Access solutions (2004). Intel White Paper. Retrieved 22 Feb 05, from http://www.intel.com/netcomms/technologies/wimax/304471.pdf
17. WiMAX to Challenge DSL, Cable Broadband. (Feb 2, 2005). Techweb-News.com. Retrieved Mar 3, 2005 from http://www.techweb.com/wire/networking/59200152
18. Wireless Security Blackpaper. (2004). ARS Technica.com. Retrieved Mar 4, from http://arstechnica.com/articles/paedia/security.ars/1

# A Manager's Look at Spyware

## By Professor Paul Flanagan

According to the on-line encyclopedia Wikipedia, spyware is "a broad category of malicious software intended to intercept or take partial control of a computer's operation without the user's informed consent." Beyond this definition there are three main points to grasp:

The first point is that *"spyware" or "adware" is something you should not ignore.* Some have described spyware as a minor nuisance but increasingly the purpose of spyware is for major illegal financial dealings. For example, on May 29, 2005, Israeli police took action in a case of spyware that was developed and used for industrial espionage (Litan, Girard, and Pescatore 2005). Other spyware episodes include keystroke loggers and password grabbing programs developed to steal money.

The second point is that *spyware may lurk on your computer.* Other types of malicious code, such as worms and viruses, reveal themselves as intended by the hacker. When these type of programs infest your computer, you know it. Spyware may have some tell-tale signs of infestation like slower initial boot-up, but it is more likely that it will not. The program can and will lurk on your computer, capturing your sensitive data and sending it out over the Internet without your knowledge. Organizations that scan for spyware are often dismayed at the amount and extent of spyware infestation.

The final point about spyware is *you can do something about it.* Effective anti-spyware products are currently available. There are some reputable freeware and shareware products available for download from the Internet and there are standalone vendors that have interesting technology solutions. Finally, the major anti-virus vendors have developed some anti-spyware solutions. Anti-spyware is currently an emerging market but the long-term future of this market is not clear. What is clear is that organizations and end-users need to educate themselves about spyware and take their appropriate steps to ameliorate the threat posed by this class of malicious software.

Reference

Litan, A., Girard, J., and Pescatore, J., (2 June 2005) Israeli Attack Represents a Dangerous New Breed of Spyware, Stamford CT: Gartner Research



**Here's Our Web Address!!!**

http://www.ndu.edu/irmc/elearning/infotech.html

***CHECK OUT OUR PREVIOUS ISSUES!***

INFORMATION RESOURCES MANAGEMENT COLLEGE

**The World Leader in Information Resources Management Education**

300 5th Avenue Marshall Hall (Building 62)
Fort Lesley J. McNair, DC 20319
(202) 685-2096
http://www.ndu.edu/irmc/

**Director: Dr. Robert Childs**

**Dean of Faculty & Academic Programs: Dr. Elizabeth McDaniel**

**Chair, Organizational Transformation & Technology Department : Dr. Judith Carr**

**Newsletter Editor: Dr. Les Pang**