RuBee (IEEE 1902.1) – The Physics Behind, Real-Time, High Security Wireless Asset Visibility Networks in Harsh Environments.

John Stevens, Ph.D., Craig Weich, Rod GilChrist

Visible Assets, Inc.195 Bunker Hill Ave. Stratham, NH 03885
Phone: 603-418-8800 info@rubee.com

ABSTRACT

RuBee (IEEE 1902.1), an active, long wavelength (131khz), packet based, on-demand, protocol was designed for real-time asset visibility networks in harsh environments. RuBee tags have a 5-10 year battery life, optional sensors, a range of 1 to 50 feet, can be 1” x 1” to credit card size and 2 mm thick. RuBee tags work near steel and water, typically produce about 50 milli-gauss of magnetic signal (H) and almost no measurable electric field (E = 0.4 nano-watts). RuBee has no known human safety or intrinsic safety risks. The voltage for RuBee magnetic fields drop $1/R^3$ and the voltage for conventional wireless RF electric fields drop 1/R. That means, unlike wireless RF systems, RuBee can provide a controlled Physical Security Layer with no eavesdropping, tempest or target risk. RuBee tags also provide a Packet Security Layer using AES, or public private key authentication, and several other optional encryption protocols.

Index Terms: Asset Visibility, RFID, RuBee, Security

1. INTRODUCTION

Real-Time asset visibility and high security have some conflicting objectives. On the one-hand the end-user wants real-time reports of the asset’s status and physical location, inventory usually from a wireless asset tag, but on the other hand the same end-user wants to keep all of that information secret and confidential. Additionally, to save costs the end-user wants the visibility side of the equation to be free of any new processes or changes in current processes that might require expensive training or lead to human generated errors. We review in this paper what we have learned over the last five years providing RuBee based (IEEE 1902.1) high security asset visibility networks for mission critical assets that do meet both the security and asset visibility requirement. We explain the physics behind RuBee’s ability to provide high security visibility networks.

1.1. RuBee IEEE 1902.1 Background

RuBee [1] is a long wavelength (131kHz), active, inductive, peer-to-peer wireless protocol with a range of 1 to 50 feet. The RuBee standard was created by an industry wide workgroup to provide secure, mission critical asset visibility networks in harsh, high security environments. Because RuBee uses magnetic signals with virtually no detectable RF energy, it works on and near steel and water has no affect. RuBee tags use low clock frequencies so have 5-10 years battery life using coin size Lithium batteries. RuBee tags have several memory and processing options: Option 1, RuBee tags can have a simple fixed function read only ID with no memory; Option 2, a fixed function masked four bit CPU with read/write memory of 500 bytes to 1K bytes of sRam; Option 3, a field programmable, RISC based CPU, programmable in high-level languages, with read/write sRAM of 500 bytes to 5K bytes. RuBee tags can have optional sensors for vibration, shock temperature and humidity. A typical RuBee tag can send and receive a full data packet 6-8 times a second.

RuBee is in use by the US Department of Energy (DoE) in its own high security areas [2,3]. In July 2006, the FDA classified IEEE 1902.1 as a Non-Significant Risk (NSR) Class 1 device in medical visibility applications. In May 2007, a peer-reviewed study was published by the Mayo Clinic (4,5) showing that RuBee has no effect on pacemakers or ICDs. A second independent Mayo Clinic [6] study has shown RuBee has no EMI or EMC in the operating room for 32 tested medical devices. The company has tags that meet MIL-STD-810G and NEBS interference tests, using independent laboratories, and has initiated independent laboratory tests and expects its RuBee tags to meet the Intrinsically Safe ANSI 913-88 standard, and ATEX in a Zone 0 or Zone 1 explosive atmosphere as well as the US DoD HERO standards.

1.2. Security and Asset Visibility Essentials

Many asset visibility end-users assume data security is limited to how data packets are encrypted. In most wireless systems, data is encrypted using one of the standard symmetric or asymmetric encoding schemes. Symmetric encoding requires an initial secure exchange of two keys, (e.g. the US government approved Advanced Encryption Standard, AES) while an asymmetric encoded system (RSA, public/ private key) uses one undisclosed private key for encoding and second public key for decoding [see 7,8,9,10]. The end-user local IT experts responsible for maintaining local security systems assume that any cloud based, public internet encryption system, and all wireless based data transfer systems are not secure.

We have all read stories about data thieves sitting in the parking lot. In 2007, a US$17B company, TJX, lost 40 million credit and debit card numbers though eavesdropping on a WEP encrypted WiFi network [11]. Each year it has become common for the Computer Science departments at major academic institutions around the world to report they have cracked yet another 128 bit or 256 bit encryption algorithm [12,13]. The US Federal Bureau of Investigation set up a demonstration a number of years ago where they were able to crack any WiFi WAP secure network in a matter of a few minutes [14)].

We find the standard "high security site" assumption worldwide is that anyone who can eavesdrop on a message can probably crack the encryption scheme. It is assumed that a skilled hacker, or a government with unlimited computational and financial resources can crack anything that is encrypted. We agree with this assumption. Data packet layer encryption alone does not guarantee security in a wireless visibility network. Most high security site end-users simply do not allow wireless data systems on-site or within a secure area. Banning any wireless use is the simplest way to eliminate or reduce all security risks.

The facts are that while data packet security is important, and while elimination of wireless systems does eliminate risks, the other side of the equation is elimination of asset visibility and any system to provide asset location and status also enhances security risks. Risks of loss, or stolen mission critical or top secret assets increases without automated asset visibility networks.

RuBee is unique in that it provides a secure physical communication layer, but also provides a highly flexible asset flow layer that can enhance security and provide high quality asset visibility. RuBee provides both asset visibility, with secure asset flow and high asset security that does not rely solely on data encryption. We review details below.

1.3. The Four Important Security Layers

To create a secure wireless RuBee visibility network that provides maximum asset security, with maximum control of high-value items, we analyze four separate security layers. Each of these layers is important, and must be carefully considered if secure wireless asset visibility within a high security site is to be delivered.

1. **Asset Flow Layer** - How mission critical assets are managed, stored, inventoried, checked in and out, detected and identified on exit and entry. The security/ alarm rules for exits and entrances.

2. **Physical Asset Layer** - How the asset is securely identified, labeled, or tagged. If it is tagged how does the tag know it is on the correct asset, and how can that be authenticated. We also call this asset authentication.

3. **Packet Data Layer** - How the data in a packet is encrypted, and protected. We want impenetrable barriers to any casual data theft, and make covert, intentional, well-financed data theft insurmountably difficult.

4. **Physical Communication Layer** - How data is securely transferred from one node to another node within a visibility network, making eavesdropping difficult or impossible, with no tempest or target risk. Hardwired data can be transferred using TCP/IP over a secure Cat 5E cable with known and identified routes, or a fiber optic cable again with identified routing. RuBee uses magnetic data communication to eliminate the risks associated with other wireless technologies.

We review each of these layers and discuss issues below.

2. THE FLOW LAYER

The asset flow layer is how mission critical assets flow though normal daily or weekly use. We see three important steps in this layer that have to be considered in any final asset flow design for maximal security:

A. Real-Time Asset Inventory
B. Asset Checkin/Checkout
C. Asset Entry/Exit Management

2.1. Real-Time Asset Inventory

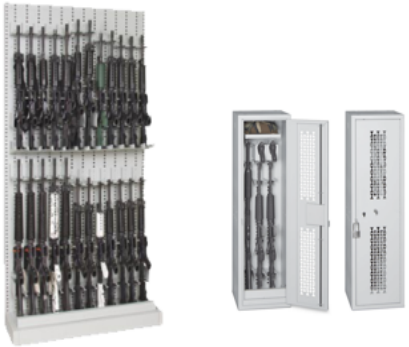

Figure 1 - Example smart rack that provide real-time inventory.

Real-time asset inventory is the foundation of any visibility network. That usually means the asset is on a specialized "RuBee Smart" rack (see Figure 1) or Smart Shelf and a RuBee wireless visibility network system embedded that can read all tags on each asset in real time. The visibility system reports the full physical inventory as a "bed check" in real-time. Software systems can set time and frequency to verify the physical presence of all mission critical assets, for example, every ten minutes, once an hour or once a day. This provides the highest possible security. An end-user can verify status and presence of any mission critical asset in storage or in active use. It is possible to combine the smart storage rack with a keypad and door lock. That system can be used to enable automatic physical inventory, and also makes it possible to checkout or checkin an asset with minimal process change and complete user authentication.

Smart Rack systems also provide unchallengeable audit trails that include the date and time an asset is removed or replaced, with ID of the user and asset. Tags on mission critical assets often also have sensors to monitor how an asset is used (e.g. number of rounds fired, temperature). The automatic inventory software can be configured to recommend important maintenance steps, as well as normal preventative maintenance based on use

2.2. Asset Checkin/Checkout

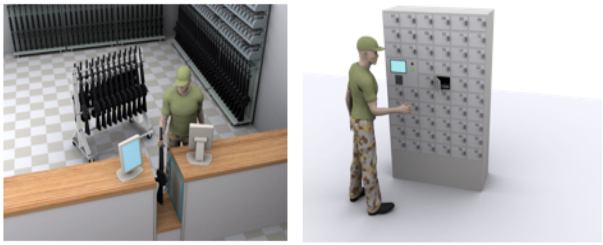

Figure 2 - Counter based, face to face issuance, on left and vending auto issuance on right.

Asset Checkin/ Checkout, also known as asset dispensing or asset issuance, can be a complex process. In some cases because of security it must be a face-to-face transaction between a “storekeeper” and a “guard”. The transactions typically take place across a counter and can go from totally manual processes to fully automated counter based processes. In general the more automated, the higher the security and the lower the transaction costs. The more manual based the process, for example if the storekeeper is required to read a serial number, the greater the likelihood of errors with reduced security. Full issuance automation typically means the storekeeper and guard both have long range, RuBee visibility ID tags that can be read in a wallet or on a neck lanyard, and the mission critical assets also have long range (10-20 feet) visibility tags that can also be read and verified as they cross the counter.

A second method for asset issuance and storage is a vending system, or smart locker with multiple lockers, and automatic electronic locks. A user (usually guard) enters in a PIN number of a keypad, often on a touch panel. The smart locker reads the users visibility ID card, confirms the users identity and automatically opens the locker with required mission critical assets. The lockers may contain a scale, and the stored assets may also have a wireless tag system. This again provides the ID who removed what items as well as who and when they were replaced.

In some cases we have found an asset is issued to a specific individual, and its use is also limited to a specific area. The users often request that if the asset is removed from that area an alarm event should be issued. The methods for any logic associated with the hierarchal managing of asset tags and ID’s in and out of specific areas can become very complex, but are always possible.

Cost is always a consideration that balances any security consideration. But the important metric is always Return on Investment (ROI). Full automation in these issuance systems do provide the highest security and also typically provide the highest ROI. Often 100’s of people are waiting in some facilities for the next shift to be issued assets. Even a 10-20% improvement in people flow reduces costs that can pay for an entire Visibility Network in a brief period. Issuance is a choke point for both security and costs. The US Department of Energy has published ROI figures for visibility networks in armories, and the ROI for even a small armory is attractive [2].

2.3. Asset Exit/Entry Management

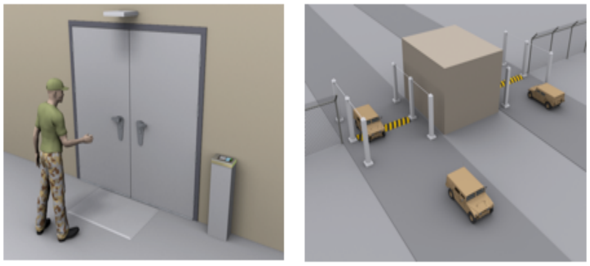

Figure 3 - Exit entry data logging provides automatic ID reads and asset reads for individuals and groups in vehicles.

The final requirement for any high security visibility network is exit/entry asset management. At the lowest level, simple detection to prevent exit of assets that have been improperly issued or not issued at all. At the high end is verification of a user’s ID as well as all allowed assets on exit or entry is possible. It also often a requirement that identity detection be possible through a door or person gate, as well as in a moving vehicle. Again both are possible and in use, with very high reliability with a properly designed RuBee visibility network.

We provide many flexible advanced RuBee exit/ entry systems designed to maximize security. DoorGuard® can be configured to read both asset tags and ID’s as an individual passes through a single door, double door or wide person gate. ID cards may be carried in a wallet or on a neck lanyard. GateGuard® can be configured for 9-18 foot wide roads and reads ID tags and asset tags in a vehicle as it passes by a guard gate at 5 km/hr. In a recent independent test GateGuard was able to discover 5 ID tags inside a vehicle moving at 5 km/hr, and detect all legal assets, and detect any hidden illegal assets 100% of the time [15]. In one tests a weapon was wrapped in Aluminum foil and placed inside a steel briefcase under the wheel well and GateGuard detected the presence of an illegal weapon 100% of the time [15]. These systems are able to provide high sensitivity and high security on high security site exits and entrances.

In theory it should be possible to infer where an asset is if you see it going by a DoorGuard or GateGuard portal, but there are always exceptions. Someone may leave the asset on a table and it does not go back into inventory, or there may be intentional asset mishandling, designed to remove an asset and it appear in inventory. Many unexpected advantages appear with a well thought out asset flow design that includes all three flow steps A, B, and C. Our experience is if we always have the real-time asset inventory on a rack with, issuances records, ID’s, dates and times, as well as exit entry statistics, it is always possible to discover undesired events in near real-time and most importantly take steps (sound alarms, signal guards, etc.) to safeguard the operation.

3. THE ASSET LAYER

Security in any visibility network is only as good as tag attachment.

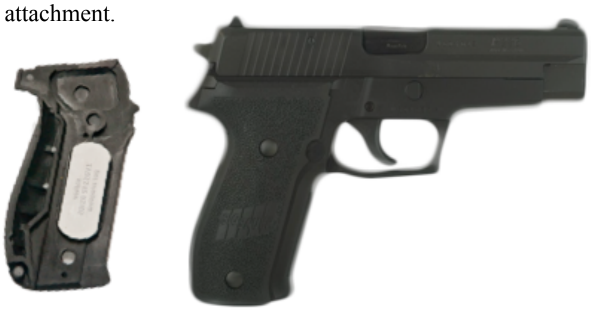

Figure 4 - Asset tags should be securely attached. In this case the tag is placed in the grip of a Sig Sauer P226 and the grip is attached with tamper resistant security screws.

For high security applications, the RuBee tag can be built into the asset in such a way that it can only be removed with special tools, or by destroying or damaging the tag, so we minimize any risk of a false positive, spoofs, or clones on a smart rack. For example, the Sig Sauer P226 pistol has a thin tag placed in the grip, and the grip is attached using security screws. The tag is tuned so it actually uses the weapon as the antenna. In most cases we custom design RuBee tags to not only fit a specific identified asset, we also design the antenna so the asset itself becomes a magnetic radiator. This often enhances detection sensitivity. It is always possible to attach a tag with adhesives stuck on the side, but that compromises the security of the other three layers

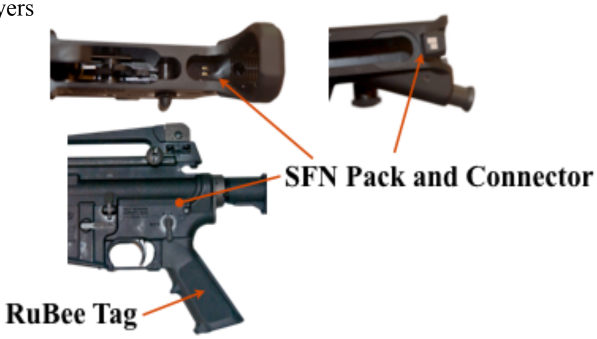

Figure 5 - Tag authentication and part identity is possible with SFN packs, EEPROM 32 bit ID's. The RuBee tag is placed on the lower receiver in the grip, and an SFN tag is placed on the upper receiver and barrel assembly.

In high security applications, where asset authentication is critical we often to move to one higher level, and place an EEPROM package (called an SFN pack) attached directly to the asset. The RuBee tag has electrical contact to the EEPROM. The EEPROM contains a unique 32 bit serial number. That makes it possible to authenticate individual parts as well as fact that the tag is actually to the asset and it is the correct asset. SFN packs can be force fit mounted on any steel item so that it can only be destructively removed.

For example, in Figure 5 we have placed an SFN pack on the upper receiver of an M4, and a RuBee tag with shot counting in the lower receiver on the grip. The tag can detect it is attached to an M4 and identify that it has upper receiver with a specific serial number or ID. That means maintenance can be planned for all components (barrel assembly, upper receiver, and lower receiver) based on actual use. It also means we have high security authentication of the asset, and components.

4. THE PACKET LAYER

Two way AES is preferred standard encryption in RuBee tags, when encryption is required. Additional options include AES keys that are altered by a clock, so a new key is generated daily or weekly. RSA public private key authentication is also an option in the RISC version of a tag. RSA can be slow and is not recommended for real time detection through doors or gates. To be clear, we do not rely on encryption for our systems security, rather we optimize the flow and we optimize the Physical Layer below, and include encryption when necessary.

Additional packet-related issues often appear in high security sites. In some cases asset visibility is important within the facility, but dangerous outside the facility. For example, weapons may be issued to covert personnel where detection in the field could put the operator at risk. The requirement is that the RuBee tags inside a facility provide visibility but on exit become silent. We have developed an advanced protocol known as Zero Field Detection (ZFD) where upon leaving the facility the tag goes into “stealth mode” and does not respond to any inquiry. It can only come out of stealth mode if it receives an encrypted site key several times over a predefined period of time. We have many ZFD variations that make impossible for anyone to detect or activate a tag once it is in stealth mode.

5. THE PHYSICAL LAYER

Security officers of any secure facility have three major physical layer concerns (16) with any wireless system:

1.**Tempest Threat** - The ability for an attacker to place a listening device or other data collection device into a wireless transmitter and send data to a remote data collection site. Any signal that leaves a secure site is a potential tempest threat.

2.**Eavesdropping Threat** - The ability for an attacker to listen and monitor data and packets that might enable them to obtain classified or secure information about mission critical assets and asset status.

3.**Target Threat** - The ability for an attacker to use a signal emanating from a wireless system or systems component as a reference or target .

Conventional higher radio frequency (RF) tag networks can be designed as short range systems, but what is often forgotten is the RF signal can propagate many miles and can be monitored using expensive specialized equipment. That possibility opens the risks for all three concerns listed above for any wireless system.

Two classic laws of physics are important to understand these risks and issues. The first is Planck's law - energy contained in a radio signal is directly proportional to the frequency (E = h*V). That means as you go up in frequency the signals have more energy and the ability to propagate a much greater distance. The second law is contained in Maxwell's equations (see reference 1 for summary). RuBee has a wavelength of 7,511 feet, but we use RuBee only within a 10-20 foot range. That means RuBee works in the ultra-near-field, 1/375 of a wavelength. As a result does not produce any significant RF field (E in Maxwell's equations), and only produces a magnetic field (H in Maxwell's equations). RF signals when measured as voltage on an antenna drops off at 1/R. If you use power (voltage x current) on the antenna it is $1/R^{2.}$. In contrast magnetic signals when measured as voltage drops off $1/R^3$ (see Figure 6). as measured as the voltage on an antenna (power on the antenna is $1/R^6$)

So RuBee does not require a lot of E or H power thanks to Max Planck, and RuBee does not produce much of E power anyway thanks to James Clerk Maxwell

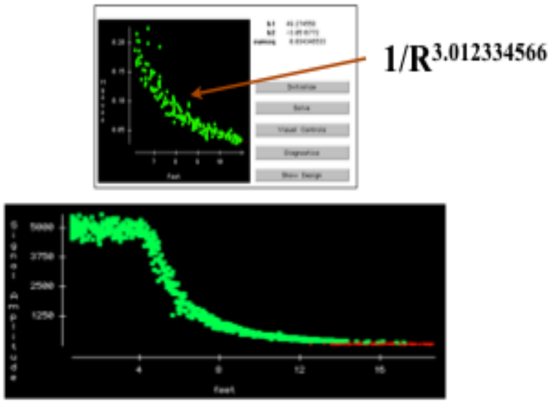

Figure 6 - Actual measurement of voltage vs. distance on a RuBee magnetic tag. Both plots are antenna signal vs distance. Best curve fit shows it drops off $1/R^3$ as expected.

The rapid drop in signal turns out to be a security officer's gift from physics. It means the range of a RuBee magnetic signal can be controlled and limited. Planck's law and the fact that RuBee operates in the ultra-near-field also means that same RuBee signal produces no significant RF power. A typical RuBee system can read and write to tags 20 feet away, with about 600 milli-gauss of magnetic power from a base station. That same RuBee antenna produces only about 40 nano-watts (10^{-9}) of RF power. That RF signal drops to undetectable levels at about 25-30 feet away. In other words the RuBee wireless signal range can be safely contained and managed, while even low powered data systems at higher frequencies can be monitored many miles away. With RuBee, any possible eavesdropper is within view, and no detectable signals leave the secure facility.

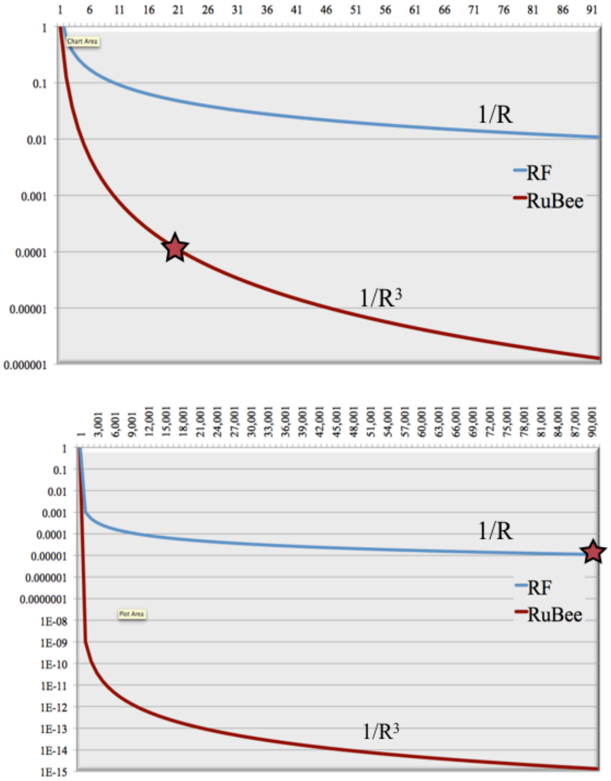

Figure 7 - Two graphs illustrate differences between 1/R drop off for RF signals (E) and $1/R^3$ for magnetic signals (H). Both plots have logarithmic Y axis as the signal, and assume a signal at zero of 1.000. The top plot has a distance X axis 1-91 feet, lower plot is 1- 90,000 feet. Star is point where signal drops to .0001 for both.

We illustrate the differences between 1/R and $1/R^3$ in Figure 7 with two simplified graphs seen above. Assume we have designed an amplifier in a tag that can detect a 0.1 millivolt signal (0.0001 Volts) on an antenna. And assume we have a transmission signal voltage of 1 for both a 1/R RF system and a $1/R^3$ RuBee magnetic system. The RuBee system can read a tag out to about 20 feet (see figure below) with that amplifier where the signal drops below .0001 volts, see star on upper graph with range of 1-91 feet. The 1/R RF system can be read at about 17 miles (90,000 feet), see star in second lower grape at the same voltage level on the antenna. This is an over simplification, since many other things like noise background must be taken into account. However, it illustrates the dramatic differences between a 1/R and $1R^3$ drop in any signal.

6. CONCLUSIONS

Security and Visibility together at the same site is never simple. However we have reviewed here the four important security layers to consider in the design of any visibility network at a high security site, and have provided references and data. We have shown that taken together, it is possible to have the both Asset Visibility and Date Security so that site and asset security is maximally enhanced.

7. REFERENCES

[1] C. Weich, R. Gilchrist, J. Stevens, “RuBee Web Information Site www.rubee.com” Visible Assets, Inc. Aug 2010.

[2] Michelle V. Rafter, “Gunning for Change- Sig Sauer, a leading handgun manufacturer, is offering customers the ability to track weapons with a RuBee based inventory management system.”, RFID Journal, Inc., Sep 29, 2008

[3] B.J. Stinson, J.R. Younkin, C.A. Pickett, G.D. Richardson, “Application for Automated Inventory Management of Weapons and Related Assets.”, Oak Ridge National Laboratory, Department of Energy, UT-Battelle, LLC, White Paper, Feb. 3, 2009

[4] D.L. Hayes MD, G. Eisinger, L. Hyberger RN, J.K. Stevens, PhD, “Electromagnetic interference (EMI) and electromagnetic compatibility (EMC) of an active kHz radio tag (Rubee IEEE P1901.1) with pacemakers (PM) and ICDs.” *Heart Rhythm* 2007;4:S398 (Supplement).

[5] D.L. Hayes, MD, G. Eisinger, L. Hyberger, RN, John K. Stevens, PhD, “Electromagnetic Interference (EMI) and Compatibility (EMC) of an active 131 KHz radio tag (RuBee IEEE P1902.1) with pacemakers and ICDs: A Preliminary Safety Study of a RuBee Enabled Operating Room Visibility Network.” Department of Medicine, Mayo Clinic, Rochester, MN USA, White Paper, Jan 26, 2007.

[6] S. Kapa, MD, T. Pierce, D.L. Hayes, MD, D.R. Holmes, Jr., MD, S.J. Asirvatham, MD, “Electromagnetic Interference from Auto Identification Systems May Be Diminished Using IEEE 1902.1, A Low Frequency, Magnetic Field Based Protocol, in Healthcare Settings”, Department of Medicine, Mayo Clinic, Rochester, MN USA, White Paper, (To be published) March 7th 2009

[7] J. Schwartz, "U.S. Selects a New Encryption Technique". *New York Times*, October 3, 2000.

[8] B. Schneier, “*Applied Cryptography”*, John Wiley & Sons, 1994. ISBN 0-471-59756-2

[9] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, Chris Hall, Niels Ferguson, Tadayoshi Kohno, Mike Stay "The Twofish Team’s Final Comments on AES Selection". White Paper, May 2000.

[10] Wikipedia , “Public Key Encryption”, Aug 2010

[11] Larry Greenemeier, “T.J. Maxx Parent Company Data Theft Is The Worst Ever” , *InformationWeek,* March 29, 2007

[12] Robert McMillan, “Once thought safe, WPA Wi-Fi encryption is cracked”, *Computerworld*, November 6, 2008.

[13] Dan Raywood, WiFi is no longer a viable secure connection *Secure Business Intelligence,* October 10, 2008

[14] T.J. Troy, “FBI Teaches Lesson In How To Break Into Wi-Fi Networks Network Computing, April 8, 2005

[15] T. Pierce, M. Norton, “Indepedent Gateguard Acceptance Test Results” Visible Assets, Inc., White Paper, Aug 2, 2010

[16] Wikipedia, “Tempest Threat Summary” Aug 2010.