Intro

This paper has been written at the request of the Booz Allen Hamilton Technical Advisory Committee to support the current placement of Secure File Interchange in their Cyber Security Demonstrator. This application shows the deployment of dynamic identity verification and authentication (DIVA) in dynamic distributed key infrastructures (DDKI).

These technologies will be augmented in the new Booz Allen Hamilton Cyber Security Demonstrator in McLean's, Virginia with iris optical scanners, both a large scale system for high population traffic areas like airports, and a mobile android based optical scanning utility.

Combining iris authentication with DIVA identity management keys binds organic identity to the use of digital keys and satisfies international standards for Level 3 and Level 4 Identity Proofing.

The responses to the questions posed by Booz Allen Hamilton Technical Advisory Committee will be as direct as the questions themselves. Each answer will contain links for references, specific email addresses to experts for due diligence, background to explain the context of the sciences, and the players and their actions as these sciences advanced.

André Brisson - January 28, 2012

(Mr. Brisson is co-inventor of Whitenoise, DIVA, DDKI and founder of Whitenoise Laboratories Canada Inc.)

1. What are the technical details to back up: 1 framework – 1 protocol for complete network security?

Dynamic Distributed Key Infrastructures are point-to-point and peer-to-peer distributed software frameworks that are scalable, interoperable, and extremely economical. They can be used for great security effect and identity management in any digital context. They are compatible with any existing security techniques, protocols and frameworks currently in place.

When used with existing network security systems like asymmetric public key systems, they address the flaws and vulnerabilities attendant with these systems at little-to-no cost and without the necessity for the direct integration into these systems. They are incredibly simple and accurate identity management technologies to deploy both for human use and non-person entity systems like electrical grids etc.

Just running DDKI and DIVA in parallel with these systems creates a large, distributed authentication platform that imposes identity on all components and on all network use. Their presence eliminates any possibility of man-in-the-middle and side-channel attack classes. These technologies can be provisioned by Level 3 and Level 4 Identity Proofing or by electronic/digital secure key distribution (1-time.) Key distribution can occur in manufacturing with the addition of secure chips in a clean environment (or the addition of firmware to these chips) or by two channel authentication and key distribution over the Internet and through telecommunications providers. See addendums in:

http://docbox.etsi.org/Workshop/2012/201201_SECURITYWORKSHOP/3_INTERNATIONAL_STANDARDIZATION/BRISSON_WHITENOISELABS.pdf

and

http://www.wnlabs.com/Presentations/Bringing_in_Legacy_Appliances_to_Secure_Networks.pps

DIVA is a protocol that is possible because of the extraordinary length of key streams that are generated by the Whitenoise algorithm, a singularly unique deterministic random number generator. As a state-based algorithm, it can create completely random, deterministic key streams of any size. Generally key streams of only **10 to the 60th power** bytes in length with a variable inherent key strength of **250,000 bits** are used commercially. Because it is state-based (i.e. mechanical versus mathematical) Whitenoise can easily generate key streams larger than the number of atoms in the universe and use them more quickly than 128-bit keys.

DIVA, a commercially protectable and globally patented proposition, manages the offsets and eliminates key transfer in use. The use of keys is the only 100% accurate identity management process. As many different key segments as desired can be used at any one-time to ensure digital provenance. Different segments of the same key can be used for any requisite network and data security need without compromising or exhausting the key. These keys can provide intrusion detection, authentication, authorization, revocation, signature etc.

These unique keys and resultant protocol naturally led to dynamic distributed key infrastructure software frameworks for the easy creation, management and distribution of keys in all communications and digital contexts.

As such, just DIVA and DDKI are sufficient for identity management and data controls in the majority of secure commercial communications or lower-level security contexts.

HOWEVER, ***WE RECOGNIZE AT NATIONAL SECURITY LEVEL MILITARY AND GOVERNMENT USE THAT LAYERED, REDUNDANT, MULTIPLY-HARDENED SYSTEMS ARE A REQUIREMENT AND ARE MANDATED. WE ADVOCATE THE PROPER USE OF THESE TECHNOLOGIES WITH PKI SYSTEMS, AS WELL AS BIOMETRICS AND QUANTUM TECHNIQUES; THIS CREATES TWO-CHANNEL (ASYMMETRIC AND SYMMETRIC) DISTRIBUTED, MULTI-FACTOR IDENTITY BASED SYSTEMS TO FURTHER HARDEN CRITICAL DEFENSES.***

DIVA AND DDKI ARE PERFECTLY COMPLIMENTARY WITH ALL EXISTING SYSTEMS AND WITHOUT DIRECT INTEGRATION. THEY SIMPLY RUN IN PARALLEL.

This protocol and framework have been recognized by Export Controls (and permitted), national and international standards groups like the International Telecommunications Union, the International Standards Organization, the European Telecommunications Standards Institute and the White House Office of Science and Technology Policy.

The well-planned use and integration of DIVA and DDKI is needed now more than ever. Just empirically it is fair (and scientifically responsible) to ask why after 40 years of public key infrastructures that only about 10% of large enterprises use these system and why their proper (in the best sense possible) implementation is even smaller.

2. What is innovative about Whitenoise, Dynamic Identity Verification and Authentication (DIVA) and Dynamic Distributed Key Infrastructures?

Whitenoise, DIVA and DDKI are innovative in many ways. What follows is not a complete list. However, it is important to point out many factors, particularly scientific ones that were heretofore thought to be impossible. The results will be presented and it behooves you to conduct your own additional testing (simple) to determine the veracity of my statements.

- **Whitenoise is random.**

  The University of Victoria tested the randomness of Whitenoise keys against the accepted NIST test suite. Normally, this test suite allows for one statistical failure for every 100 rounds on an encryption or key technology. The test suite was hardened to only allow 1 statistical failure for every 1000 rounds. Over the entire duration of the testing against a super-computer array there was not a statistical failure – period!
  http://www.wnlabs.com/pdf/UVIC_Performance_Analysis.pdf

- **Whitenoise is more random than radio-active decay.**

  Any sample of emitted particles in radio-active decay has been considered to be the most random event in nature. Whitenoise tests more random than this phenomenon. Take any of our posted demonstration software and test the encrypted output at http://www.fourmilab.ch/hotbits/ At this Swiss site, in a couple of minutes, you can perform six tests to see that Whitenoise cipher text or a key is orders of magnitude more random than radioactive decay.

- **It is easier to process Whitenoise encrypted data than it is to process untreated data.**

  This has been an unexpected result in internal testing. We suspect it is because WN data is order one and processed bit by bit and that this result is because it is more efficient than the processes (i.e. caching and use of memory) available on commercially available operating systems. We have a radio frequency ID tag application to demonstrate this protocol in the lowest energy context available at that time.

- **Whitenoise keys cannot be factored.**

  Whitenoise keys are created by using a variable number of prime number sub-key lengths, populated with Whitenoise random data. Corresponding values between sub-keys are then X/Or'd together. Sub-key values are not multiplied together and therefore there is no factoring technique that can be utilized to attack the key and there are NO mathematical shortcuts.
  http://www.wnlabs.com/pdf/WhitenoiseAlgorithmVisualLook.pdf

- **Whitenoise keys cannot be broken.** (They can be reconstituted.)
  In the cryptanalytic game there are three pieces of data: the key, the plain-text and the cipher text. In cryptanalytic attacks, two of the three pieces must be available in

sufficient quantity (ignoring the dynamic reality for the moment.) There is NO key transfer during use. Using offsets eliminates this, and when tokens (particular key segments) are used it is not sufficient in size because at least 50% of the key would need to be captured and then rapidly processed. There are NO mathematical shortcuts.
http://www.wnlabs.com/pdf/Wagner_Security_Analysis.pdf

In our game we always reduce the only option to attacking a Whitenoise key to brute force or trying every single possible combination. There is never enough material for a hacker to work with. The keys are simply too large to try every combination – even more so because the system is dynamic and constantly changing. Additionally, these keys will be secure even with the arrival of quantum computing because every variable is variable. There are no fixed key sizes as there are in current systems or constants as there are in mathematical functions. Even though physical manifestations can be captured when one attempts side channel attacks, every process after key load is order 1 which means there are no patterns (it is a flat line of output.) Side Channel attacks cannot form “cribs” and therefore are reduced to ineffective brute force attacks as well.

For law enforcement and national security reasons it is requisite that keys can be recovered in contexts with proper authority and authorization. All keys, even when internally created without oversight are subsets of master keys and so by definition, with effort, can be reconstituted and recovered.

- **Whitenoise, DIVA and DDKI networks can be instantly hardened on the fly.**

  Whitenoise Identity Management keys are distributed securely one-time and both the endpoint and the server have a copy and the starting offset of the pre-authenticated, pre-distributed key for a unique client, device or entity. Generally, about 20 sub-key lengths are utilized in key creation. In the event of a critical national security event it would be simple and fast to electronically provision all endpoints with additional sub-keys. The additional sub-keys to be used in key creation would perturb the keys already distributed in a predictable and instantly usable fashion. The result is that the key strength and key lengths could be automatically increased exponentially in a national security response.

- **Whitenoise keys and dynamic offsets can be deployed from a single-endpoint to control the life of data.**

  Because WN is a deterministic random number generator and because we are controlling and manipulating the use of dynamic offsets, it is possible to have a key reside at only one endpoint and to securely embed (encrypted) the offset in a packet header etc. Using this technique would allow the endpoint to randomize the offset on demand and make the system non-synchronous. This would ensure that data residing on the device or in a cloud in an encrypted state cannot be used. The protected data associated with the device or upload remains in an encrypted state that prevents use or access. Any access to data by a bad player would then require that they resort to brute force techniques. It is easy to envision this technique to be used to decommission the electronics on lost or stolen assets like weapons and possibly nuclear ordinance.

- **The innovative critical differentiator is inherent, identity-based intrusion detection.**

  This capacity makes all other network self-protecting processes possible. http://www.wnlabs.com/Papers/WCSF_2006_brochure.pdf

- **It is simple to deploy.**

  A device requires minimal storage or memory and connectivity. A server requires a minimal amount of space to have DIVA supervise login and network access.

- **A key can never be exhausted (in practicality)**

  A device or person would need thousands and thousands of lives to ever use a key enough times to cause a repeat. See WN A visual look at key construction – a key would be perfectly secure until the seams of all the sub-keys line up perfectly.

Additional innovative characteristics

- **Easily configurable** – one offset controls life of data – multiple keys – any context etc.
- **Dynamic symmetric systems**
- **Implements in minutes**
- **Lowest real cost** – all manufacturing except when there is provision of a self contained key vault server is virtual. No security systems can come close to competing on “real” cost of deployment.
- **We can use existing PKI structures for key exchange (SSL)** although it is not necessary because of intrusion/spoof detection. This creates more “peace of mind” and exploits layered, redundancy.

3. Clarify the criticisms about Public Key Infrastructures and how properly implemented systems are vulnerable to man-in-the-middle and side channel attacks.

The use of the word criticism for many carries a negative connotation. In science, that is not the case.

PKI is in-depth and layered and this is deemed critical. It is deemed critical because it has been proven to be necessary to harden defenses.

Scientifically, at minimum theoretically:

Man-in-the-Middle attacks are possible and happen when there is session key exchange.

Scientifically, at minimum theoretically:

> Side Channel attacks are possible and happen when the processing is not all order one. This begins to create patterns. All of our digital distribution components, as well as the physical backbones for energy distribution leak some form of physical information.

The use of in-depth and layered defenses would not be deemed necessary if this wasn't the case. These systems would already be secure.

Empirically, we just need to assess what is happening around us. Note these breaks and articles:

- Booz Allen Hamilton compromised? http://news.cnet.com/8301-27080_3-20078498-245/hackers-claim-they-exposed-booz-allen-hamilton-data/

- RIM – Saudi Arabia announcing that they will just set up companies to break their communications. http://www.ifex.org/international/2011/10/14/rim_cooperation/

- Communications for drone aircraft being broken with software available over the internet. http://rt.com/usa/news/iran-drone-hack-stealth-943/

- One million counterfeit microprocessors in US Defence assets: http://www.wnlabs.com/news/papers/What_happened_to_you.pdf

Science is a spectrum and public key systems **were and are** a brilliant adjunct to our security and advancement of cryptographic sciences – they just are not the final answer in isolation.

In fact, WNL and our sciences have received a great deal of support and assistance from iconic persons from this field like Brian O'Higgins, the founder of Entrust Technologies, which spun out of NORTEL in the most profitable day in NORTEL history.

We have also received assistance from Dr. Andrew Csinger who advanced PKI systems and sold his company to RSA.

Again, I emphasize that Whitenoise, DIVA, and DDKI are a complimentary and powerful adjunct to existing digital security sciences.

The fallback position on this line of discussion always comes back to "properly implemented" systems which seem to place the blame solely on humans and not the limitations of science. It is not a productive discussion because vast systems with too many working parts are never (or rarely at best) properly implemented and like all existing security is subject to human failings and malfeasance. It is another form of the question: "who guards the guards?" or the NSA final question of "How do you know the proper person is accessing the system or whether they have a gun against their head?" (BTW – we believe there is an answer to that question with creative use of biometrics.)

4. PKI is multi-layered and distributed. How is DIVA and DDKI different?

Whitenoise is an identity-based symmetric key cipher. Symmetric key ciphers are inherently at least 10 times stronger than block ciphers.

These systems have no public key to attack.

There are NO cryptanalytic attacks because of the way keys are constructed and because they are state-based (sub-keys are not multiplied together etc.)

DIVA and DDKI prevent the attacks to which current networks are vulnerable.

DIVA and DDKI are EASILY scalable, interoperable and configurable.

DIVA and DDKI can be learned and implemented in minutes, without implementation errors, at a tiny fraction of the cost of PKI systems.

Everything we currently treasure is protected by PKI systems. DIVA and DDKI address the problems: the sum of the whole is greater than the sum of the parts. It is absolutely imperative that there is NO RISK with the deployment of additional security protocols or the transitioning towards next generation secure networks.

DDKI and DIVA are simple technologies to deploy at “virtually” no cost. When deployed from chip sets, manufacturers simply switch out to a different generation of chip set. They are already set up for manufacturing and already buy chip sets without these capabilities. With electronic provisioning there is no hard manufacturing costs.

5. Have we had the algorithm vetted publicly like at EuroCrypt or BlackHat?

http://www.wnlabs.com/news/challenge.php

To properly answer this question, I will provide the actual history and context of Whitenoise sciences. I will also refer you to the proper government resources where complete documentation of these sciences and their efficacy exist.

First, I politely would point out that Booz Allen Hamilton qualified employees are already members of the public vetting bodies like EuroCrypt and Black Hat.

Although RSA stopped doing factoring contests long ago because their keys were always broken with freely available sieve utilities, I encourage Booz to download these utilities or use any other at your disposal to try to break a Whitenoise key and to vet it for yourselves.

There is a constant tension in science when new and dramatic developments occur. Scientific method, even from "world experts", seems to be thrown under the bus of expediency, self-interest, politics, profit and other unrelated personal realities.

When Whitenoise was invented we proceeded down the traditional path. We first posted specifications for a deployment of Whitenoise in an application called Tinnitus. This posting was made on e-Print, the electronic archive for the International Association for Cryptographic Research in Switzerland. The specifications posted were in their simplest form for easy understanding and peer review. The only element left out was a delinearization utility to further ensure the characteristic of a one-way function for the resultant key stream because that utility was already freely available through the Sandia Labs in New Mexico.

Within days of the posting of the Tinnitus specification, a man named Wu from Singapore (we were told Singapore Naval Intelligence by a responsible Canadian government figure) posted a "supposed" break of Whitenoise. We complained to the IACR about the lack of scientific integrity, particularly since we had been in contact with Wu and in discussion had actually incorporated a suggestion he gave for a delinearization technique and for which he was credited: see ePrint or a visual look at DIVA.

The IACR said they would not "get involved" in such scientific disagreement which is odd since it is a scientific archive. We would be allowed to post a change to the specification to make it clearer but they would not allow the subsequent filing so that it would be posted at a date later than Wu's questionable paper. Any scientists searching the archive would first arrive at the fraudulent break paper and would never precede any further to do accurate research and their own testing. Those results would be taken as fact.

Subsequently we found out that it appeared Wu had been affiliated with, either as a student or colleague, with Dr. David Wagner of the University of California, Berkeley who studied Whitenoise and Tinnitus extensively and published that there were no mathematical breaks or short-cuts. This relationship seemed odd.
http://www.wnlabs.com/pdf/Wagner_Security_Analysis.pdf

Following scientific method, we worked with a Communications Security Establishment crypto-mathematician for four months, to write a proof and rebuttal to the false claim made on e-Print. Although, they were not playing fair, we had to take the claim at face value for scientific integrity. The IACR refused to publish this rebuttal when presented.
http://www.wnlabs.com/pdf/Response.pdf

At the same time, there were other events that happened that raised potential questions about the integrity or motivations of "experts" in this field.

Bruce Schneier, publisher of Cryptogram, principal of CounterPane, published a blurb in the electronic "DogHouse" section of his blog. In discussions with Bruce Schneier it was obvious he had a different agenda and he would not allow any rebuttal to claims that he made without performing any research and ignoring the published results of his own colleague David Wagner.

Additionally, he tried to intimidate us and warned us "against trying to form any cryptosystems. This is already being done by MIT…"

Further investigation showed another strange relationship in that David Wagner was a principal person to help try to fix Blow Fish, a Bruce Schneier algorithm that was kicked out of the AES competition. When Blow Fish added a round and became Two Fish it was a bit more secure but slower. We found it strange to discover the tangled overlap between Wu, Schneier and Wagner. We are not in any position to speculate on motivations.

We also had an advisor, Dr. Andrew Csinger, a notable Canadian cryptographer, who sold his company to RSA. As an advisor to Whitenoise Laboratories (Canada) Inc. Dr. Csinger authored the paper Critical Insights and Differentiators of Whitenoise but would **not** allow us to publish his name with the paper even though he was an advisor at that point. This raised questions of conflict of interests in my mind.

We concluded that there was a plethora of competing motives in this field not driven by scientific accuracy so we took matters into our own hands.

There is a saying: **Where do you hide an elephant**? Answer: **In a herd of elephant**s.

On our web site is a link that says Whitenoise is STILL Not Broken. It provides the history of these events and a very public challenge to the very best that were in the field of cryptography.

http://www.wnlabs.com/WhitenoiseSecurityChallenge/

http://www.wnlabs.com/Papers/Chronological_%20History_of_Whitenoise_redacted_for_marketing.pdf

We purchased a $100,000 insurance policy and created a contest to break a Whitenoise key. Although I am not proud of the tactic, Wu was baited over the internet and correspondence into trying to prove his claim. Where he published the claim that only 80,000 bytes of key stream were needed to do his break, we gave him a million bytes of key stream information. He was told that he could use any resources etc.

If one reads the correspondence and closely looks at all the people that were cc'd in the correspondence, you will find among the myriad of names who watched this challenge unfold all the experts and key government persons we knew of in this field. Included in the correspondence, and watching this all unfold (not a complete list) were: Brian O'Higgins, Carlisle Adams (creator of CAST), Bruce Schneier, David Wagner, Dr. Csinger, Mark Fabro (world expert and advisor), Daniel Sherrange (joint chiefs adjunct), Dr. Price Kagey (Lockheed Martin), CTO of Lockheed, members of Communications Security Establishment, members of CSIS, professors from major universities, Directors of major labs in Canada and the US, and on and on. To his chagrin and embarrassment, Mr. Wu behaved miserably and childishly and could not back his claim. He admitted that he couldn't break Whitenoise. Mr. Wu appears to have tried to make a career of breaking encryption algorithms, which he never backs up by actually doing it, while peddling his own cipher. These people were all included in the correspondence because we were soliciting input on documenting an accurate history of Whitenoise and this was the bait.

http://www.wnlabs.com/Papers/History_of_Whitenoise_WN_Can't_be_broken.pdf

All this information remains on our web site, as it has for years. We would be more than happy to purchase another insurance policy so that any Booz employees or colleagues can have a motive to try their own hand at it. The key, cipher text and process all remain posted.

Given the lack of honest scientific method that we have encountered, we continue to rely on the government and persons within formal institutions and not on "the popular science cryptographers" that most people are familiar with. Government seconded experts like Mark Fabro and Brian O'Higgins and committed government workers without public recognition just simply are better and operate with a higher level of integrity because it is national security at stake and not fame or fortune.

I would refer you to CSIS and Communications Security Establishment (Daniel Wevrick) and to Richard Marshal (former director of DHS) and Dr. Celluci (former CTO of DHS.) These persons can point persons with proper clearance to the appropriate validation resources and results contained within their offices or affiliated ones like NSA and NIST.

Richard Marshall – Former Director of DHS – Richard.Marshall@tritonfsi.com
Thomas Cellucci – Former CTO of DHS tcellucci@ics-nett.com
Dr. Abbie Barbir – Director Kantara, OASIS, ITU 17 abarbir@live.ca
Mark Fabro – Lofty Perch fabro@loftyperch.com
George Sebek – Orange/International Telecommunications Union bgsebek@orange.com
Dr. Carmine Rizzo – European Telecommunications Standards Carmine.Rizzo@etsi.org

I will be happy to provide more references upon request.

6. There are no characteristics of a one-time pad. Is it an OTP?

A one-time pad refers to key technologies when they are used for encryption. When Whitenoise is used for encryption it is a one-time pad (as well as the strongest encryption in history.) One time pads are the only mathematically provable unbreakable encryption and they always have three characteristics:

i. The key is random
ii. The key is larger than the data encrypted
iii. The key (token) is only used once

Whitenoise when used for encryption is a one time pad. We have not shouted out this fact too often because ironically the idea of encryption makes the field of crypto crazy. Also, we don't care what kind of encryption process is used because even though other keys are fallible, they can not be broken and used without being detected when DIVA is present.

In contexts where Whitenoise keys are used for dynamic identity verification and authentication, there are still characteristics of a one time pad that are inherent as well as additional functionality, like intrusion detection, that wasn't available before. So, if a process is using a fallible encryption technique like DES, 3DES, Blowfish etc. the Whitenoise key that is performing DIVA still retains the following qualities while it performs its authentication, authorization, signature, intrusion detection and revocation:

iv. The key is random
v. The key is only used once
vi. (you can make the authentication key larger than data- arbitrary)

7. Can it be used in RuBee chips with 16 words memory or 128-bits of memory?

Yes, Whitenoise can be easily deployed in RuBee chips with sixteen words of memory. Reviewing the RuBee background addendum below, you will see that although most RuBee tags are 128 bits, which is fine for WN/DIVA/DDKI, they do go up to 5 mgs of memory. The larger tags, particularly on high grade or nuclear ordinance could be very useful as an additional means for the deactivation of electronics on lost or stolen weaponry. This would be a critical addition to provide security beyond the perimeter of effectiveness of quantum and give visibility in vast area contexts with secure communications.

Deployment of DIVA would be a critical element to deploy to protect still existing problems that are attendant with quantum key distribution. Review of the following paper presented at ETSI on the same panel as ours shows that Side Channel Attacks and Man-in-the-Middle attacks still need to be considered.

Rarely if ever does one hear how quantum key distribution can be protected against denial of service attacks. Quantum by definition is highly unstable and just looking at subatomic particles changes their nature. In a war situation, it would be just as effective for the enemy to prevent secure communication as to know what the communication is. If it is communication controlling the deployment of a nuclear weapon, they have a pretty good idea.

http://docbox.etsi.org/Workshop/2012/201201_SECURITYWORKSHOP/3_INTERNATIONAL_STANDARDIZATION/QuantumKeyDistrib_AIT_LAENGER.pdf

http://docbox.etsi.org/Workshop/2012/201201_SECURITYWORKSHOP/3_INTERNATIONAL_STANDARDIZATION

The standard granted for RuBee was for protecting ordinance in a Safe Separation Distance (SSD) of zero. However, in doing theoretical "war games" it is not hard to envision a scenario where all personnel have been killed and the systems are left without human oversight.

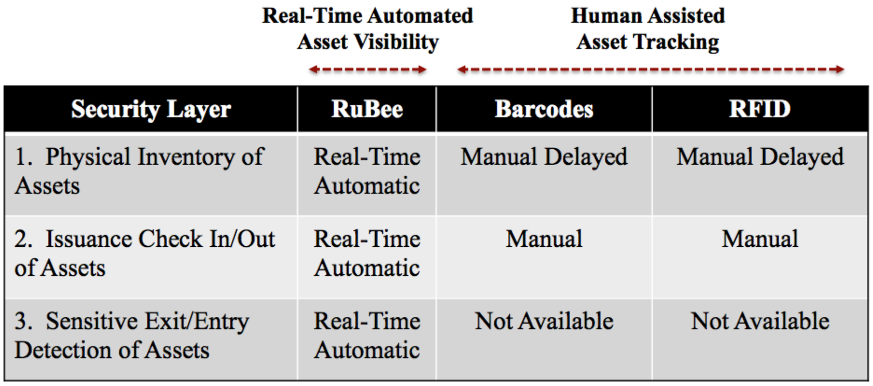
Quantum is used for key distribution and is very effective in a controlled, line of sight context. Its obvious advantage is being able to see through metal and other materials that may be used to try to hide controlled materials. Whitenoise can be used for high level key creation before distribution and Dynamic Identity Verification and Authentication can provide the additional identity based functionalities to protect these systems. The DDKI architecture provides a very simple and economical framework to provide the machine-to-machine communications in harsh, remote, and limited energy contexts where these systems are found.

The example in the addendum examines quantum tagging and the issuance of rifles. However, there is always the human element which should be controlled. Also, these assets are leaving bases and the protected perimeter for use in the field. If a soldier falls, it is possible for those weapons to be retrieved by the enemy. It would be extremely beneficial to add a component that was long range and not simply line-of-sight that could render these weapons useless.

Whitenoise was a sponsor of the BCIT Smart Grid run by Dr. Hassan Farhanghi, Director of British Columbia Technology Institute GAIT Labs. He is a member of IEEE and had approached us for standardization work with ZigBee protocols for substations and other electrical grid critical points.

http://www.bcit.ca/microgrid/sponsors.shtml - Hassan_Farhangi@bcit.ca[1]

Both ZigBee and RuBee tags are used in these environments and the use of WN/DIVA/DDKI would provide a significantly higher level of security in these critical infrastructures.



Real-Time Automated Asset Visibility

Human Assisted Asset Tracking

Security Layer	RuBee	Barcodes	RFID
1. Physical Inventory of Assets	Real-Time Automatic	Manual Delayed	Manual Delayed
2. Issuance Check In/Out of Assets	Real-Time Automatic	Manual	Manual
3. Sensitive Exit/Entry Detection of Assets	Real-Time Automatic	Not Available	Not Available

Finally, looking at the above chart DIVA and Whitenoise could be deployed with both barcodes and RFID (application available) to provide detection of assets and make both automatic. Barcodes could deploy sensitive inks for easy reading.

8. Are we selling code breaking services with the factorial utility to US defense or intelligence agencies?

The factorial utility was created after we invented Whitenoise, DIVA and DDKI simply to make the point and demonstrate that existing network security was vulnerable. We were showing that a couple of creative guys could demonstrate that fact with creative thinking.

After we invented Whitenoise the first people we contacted were CSIS (the Canadian CIA equivalent) and Communications Security Establishment (the Canadian NSA equivalent.)

A representative from CSIS spent a day with us getting demonstrations and explanations of our discoveries and various deployments. The only warning he gave me at the end of the day was, “You will never give that utility away will you? !!!”

Our point was proven, and it was recognized that any use of such a utility outside of government and law enforcement authorization would be illegal. We stopped pursuing this line of research at that time.

We always knew that we would sell this utility, or service, one time to the proper organization. We would only do so with the direct blessing and permission of the Canadian government.

We would be happy to sell this utility, or to form a joint venture with an approved intelligence agency or company. To that end, this paper and that statement is being forwarded to the Canadian US Embassy in Washington DC. Internally, I am quite sure they will be able to identify the proper persons within the Canadian military, CSIS, CSE or export controls to determine whether this permission would be granted and under what contexts, oversight or partnership.

We believe that this utility has extraordinary value but we would never use it directly ourselves and would never provide it to anyone except Canada or the United States and to whichever company or agency they select.

Addendum RuBee tags/chips

From Wikipedia

RuBee (IEEE standard 1902.1) is a two way, active wireless protocol designed for harsh environment, high security asset visibility applications. RuBee utilizes Long Wave (LW) magnetic signals to send and receive short (128 byte) data packets in a local regional network. The protocol is similar to the IEEE 802 protocols in that RuBee is networked by using on-demand, peer-to-peer, active radiating transceivers. RuBee is different in that it uses a low frequency (131 kHz) carrier. One result is that RuBee is slow (1,200 baud) compared to other packet based network data standards (WiFi). 131 kHz as an operating frequency provides RuBee with the advantages of ultra low power consumption (battery life measured in many years), and normal operation near steel and/or water. These features make it easy to deploy sensors, controls, or even actuators and indicators. Because RuBee uses long wavelengths and works in the near field (under 50 feet) it is possible to simultaneously transmit and receive from many adjacent antennas, without interference providing the signals are synchronized. That makes it possible to enhance bandwidth and remove any angle sensitivity normally seen with other RF systems.

RuBee has no reflections and is not blocked by steel or liquids and therefore is volumetric (not line-of-sight). That makes RuBee robust in harsh environment visibility and security applications. It also means RuBee has no TEMPEST target or eavesdropping risks in secure facilities. RuBee is the only wireless technology to ever be approved for use in secure facilities by the U.S. Department of Energy (DoE). RuBee has also been approved by DoE for use in high explosive areas with a Safe Separation Distance (SSD) of zero. RuBee is also only wireless technology to ever be approved by DoE with an intrinsic safety zero SSD. RuBee tags may be detected with high sensitivity through doors, even if the asset is hidden in steel brief case, as well as in vehicles though gates using antennas buried in a road.

RuBee is often confused with RFID Radio Frequency Identification. It does not work like passive or active RFID, and has a protocol more in common with WiFi and Zigbee. All passive and active RFID protocols use what is known as backscattered transmission mode. Passive and active RFID tags act like a mirror, and work as reflective transponders. In contrast RuBee, similar to WiFi and Zigbee in that it is peer-to-peer, is a networked transceiver that actually transmits a data signal on demand, but is much slower (6-8 two way packets per second). The main difference between RuBee and WiFi or Zigbee is that RuBee works in the long wavelength band using the magnetic field, whereas WiFi, Bluetooth, Delta7, and Zigbee work in the VHF, UHF or SHF bands and with the electric field. The 1902.1 standard has been approved by the IEEE.[1] RuBee received the Technology of the year award from Frost & Sullivan in 2007.[2]

Contents

[hide]

The IEEE 1902.1 protocol details

1902.1 is the "physical layer" workgroup with 17 corporate members. The Workgroup was formed in late 2006. The final specification was issued as an IEEE standard in March 2009. The standard includes such things as packet encoding and addressing specifications. The protocol has already been in commercial use by several companies, in asset visibility systems and networks (see www.rubee.com). However, IEEE 1902.1 will be used in many sensor network applications, requiring this physical layer standard in order to establish interoperability between manufacturers. A second standard has been drafted 1902.2 for higher level data functions required in Visibility networks. Visibility networks provide the real-time status, pedigree and location of people, livestock, medical supplies or other high-value assets within a local network. The second standard will address the data-link layers based on existing uses of the RuBee protocol. This standard, which will be essential for the widespread use of RuBee in visibility application's, will support interoperability of RuBee tags, RuBee chips, RuBee network routers and other RuBee equipment at the data-link layer.

RuBee tag details

A typical RuBee radio tag, about 1.5 x .75 by 0.07 inches. It has a 4 bit CPU, 1 to 5 kB of sRAM A typical RuBee Radio Tag has: a 4 bit CPU, 1 kB sRam, crystal, and lithium battery with expected life of five years. , a clock. It could optionally have sensors, displays and buttons

RuBee is bidirectional, on-demand, and peer-to-peer. It can operate at other frequencies (e.g. 450 kHz) but 131 kHz is optimal. RuBee tags can have sensors (temperature, humidity, jog), optional displays and may have a full 4 bit microprocessor with static memory. The RuBee protocol uses an IP Address (Internet Protocol Address). A tag may hold data in its own memory (instead or in addition to having data stored on a server). Some tags have as much as 5 kB of memory. RuBee functions successfully in harsh environments, with networks of many thousands of tags, and has a range of 1 to 30 m (3 to 100 ft) depending on the antenna configuration. By 'harsh environment' we mean situations in which one or both ends of the communication is near steel or water. RuBee radio tags function in environments where other radio tags and RFID may have problems. RuBee networks are in use in many visibility applications, including: exit entry detection in high security government facilities, weapons and small arms in high security armories, mission critical specialized tools, smart shelves and racks for high-value assets; smart entry/exit portals.

How RuBee works

IEEE 1902.1 RuBee uses magnetic waves also often called inductive communication. James Clerk Maxwell presented his now famous set of equations (Maxwell's Equations) to the Royal Society in 1864. These equations describe what happens when an electron travels along a conductive wire. Two fields are created, the Electric Field, labeled **E**, and the Magnetic Field, labeled **H**. These electric and magnetic fields travel through the aether, (i.e. outer space or the far field), at the speed of light with an assumed impedance of 377 Ω. **E**, the electric field, may be given in newtons per coulomb or volts per meter, and **H**, the magnetic field, may be given in gauss or amperes per meter. The two fields are tied together with the aether to form simple electric circuit capable of transferring power. However, when these two fields are measured in what is called the near field (much less than the wavelength of the signal) very strange things happen. (Also see Capps "Near Field or Far Field"). E and H are no longer connected in a simple predictable manner. The value of *c* (speed of light) and the resistance of the aether are altered and it is possible to produce large **H** values with low **E** values. It is as if the aether impedance has been reduced to only a few ohms.

Virtually all of the energy radiated by a RuBee base station or a RuBee radio tag is contained in the magnetic field (**H**), not the electric (**E**) field. This stems from the fact that the RuBee antennas are short relative to the wavelength (about a mile and half or 2½ km at 131 kHz), and RuBee operates in the near field. A typical emitted **E** from a RuBee base station is about 40-50 nanowatts, and **H** is about 900 milligauss (90 µT). Finally, RuBee is a packet based protocol in which only one end of the communication at a time generates fields, that is, a RuBee tag is a radiating transceiver.

Environmental factors

RF is based on physics, and can be reliably modeled with prediction tools and tuned models (see RF Microwaves, and Migraines, Electro Magnetics Explained). RF is not always predictable because the active environment (people, steel shelves, floors, cabinets, doors) are all part of the same tuned circuit, and change with time. For example, a cell phone call to a phone in a building is modified by steel in the building. Reception may be improved by moving the phone near a window, or pointing the antenna in a particular direction. Radio waves are affected by just about everything around us. Many environmental factors influence performance. The more significant ones include steel and water, but people and electrical noise sources are also high on the list.

Magnetic waves can pass through almost anything, even rock. That same rock blocks RF after only a few feet. An RF signal falls off as 1/*r*, whereas the strength of a magnetic wave falls off far faster at the rate of $1/r^3$. This means that the magnetic signal will not travel nearly as far as the RF signal.

This rack likes to vibrate (resonate) at the RuBee frequency

At first glance this difference in fall-off rate may appear as a negative for the range of a tag using magnetic signaling, but, as explained below, it turns out to be quite a plus in a local visibility network. Secondly, an unexpected advantage is that the noise RuBee sees is also magnetic, so it too falls off $1/r^3$. Noise and interference sources must be much more local to have significant strength, and tend to be easy to locate and minimize in an IEEE 1902.1 network.

RuBee is 99.99% magnetic waves it therefore is not affected at all by people or animals, mud or water. Steel can alter performance, but steel can actually enhance a magnetic signal. A high frequency (over 1 MHz) RF antenna on or near a steel shelf has three problems: 1. The steel detunes the antenna; 2. RF nulls will appear on the shelf with no signal at all (Swiss cheese field) this is because steel blocks radio waves; and 3. Steel also reflects the radio waves (E in Maxwell's equations) contributing to communication errors and shelf nulls.

In contrast Long Wavelength magnetic transmissions (below 1 MHz) is not blocked or reflected by steel so nulls do not occur. The loop antennas may be detuned by the steel, just like higher frequencies. But, unlike higher frequencies, magnetic loop antennas may be re-tuned with external capacitors, and, in many cases, circuits can be created that dynamically pick the optimal external capacitor for the antenna. Thus the de-tuning issue can vanish in a RuBee network. But the tuning has to be set to the right frequency by adjusting the capacitor to match the tuning curve with steel in place.

Parasitic inductance and capacitance (see Self-resonant frequency) of the antenna wire and the shelf steel limit the range of tuned frequency of any antenna circuit. A simple loop of speaker wire about 100 ft (30 m) in diameter maybe tuned to resonate at 131 kHz with a simple external capacitor. A loop of only a 1 inch (25 mm) may be also tuned to resonate at 131 kHz. At 30 MHz, however, you might be able to tune the 1 inch (25 mm) antenna, but not the 100 ft (30 m) antenna, and not the shelf.

File:Gate Guard 20 (Type X mat) transparent 01 2.png
RuBee antennas maybe 100 x 100 ft (30 x 30 m) and buried. These large antennas can be placed in roads and can read a RuBee tag anywhere within the loop, including asset tags and ID tags in a moving vehicle

At 30 MHz the largest tunable loop is about 1-foot (30 cm). RuBee's frequency is low on purpose so that it can nearly always re-tune to compensate for the parasitic inductance and capacitance despite use in harsh environments like steel shelves (see Roche et al. 2007). Back to the shelf example—the RuBee installation actually tunes the steel in the shelf, and the shelf itself becomes the antenna - the shelf becomes part of the resonate circuit and the **H** signal gets stronger near the shelf. For frequencies over 1 MHz it's not possible to incorporate most things you find in a warehouse, office building or factory as part of the antenna.

RuBee works well in harsh environments because most steel items resonate well at the RuBee frequency of 131 kHz. As the frequency goes up over 1 MHz fewer steel items resonate. At a frequency of 10 MHz for example, nothing large made of steel can be tuned to resonance.

How big can a RuBee loop antenna be? As the antennas get larger and larger noise becomes the gate keeper. A 100 ft (30 m) diameter loop can detect lighting storms hundreds of miles away. The biggest source of noise is deep space kilometric noise. While it is possible build a second antenna and do differential subtraction, a 10,000 sq ft (1,000 m^2) limit of a RuBee network is adequate for most practical visibility applications. RuBee antennas may also use ferrite rods with wire coils and get same range but without large loops.

RuBee disadvantages and advantages

The major disadvantage RuBee has over other protocols is speed and packet size. The RuBee protocol is limited to 1,200 baud in existing applications. The IEEE 1902.1 specifies 1,200 baud. The protocol could go to 9,600 baud with some loss of range. However, most visibility applications work well at 1,200 baud. Packet size is limited tens to hundreds of bytes. RuBee's design forgoes high bandwidth, high speed communication because most visibility applications do not require them.

The use of LW magnetic energy brings about a number of advantages:

- **Long battery life** – Because of the use of low frequencies and data rates the chips and detectors can run at low speed. Using (lowest cost) 4 micrometre CMOS chip technology, this leads to extremely low power consumption. LW magnetic wave tag systems can and have achieved 15 year lives using low-cost lithium batteries. This is also the expected battery shelf life.

- **Tag data travels with the asset** – Because data is stored in the tag, IT (Information Technology) costs are reduced. This means that with a low-cost handheld reader one can simply read a RuBee tag and learn about the asset — manufacturing data, expiry date, lot number, etc. — without having to go to an IT system to look it up. In addition, the distance between the reader and the asset is not critical. RuBee can also write to a tag at the same range as it can read it. RFID, on the other hand, uses EEPROM memory, and writing to the tag is awkward. (In the case of RFID, range is limited, more power is required and write times are long.)

- **Human Safe** – A RuBee base station produces only nanowatts of radio energy. RuBee's LW magnetic waves are not absorbed by biological tissues and are not even regulated by OSHA. In fact, RuBee produces less power and lower field strengths than the metal detectors in airports and the anti-theft detectors in retail stores operating at similar frequencies — by a factor of about 10 to 100. Recently published studies show that RuBee has no effect on pacemakers or other implantable devices (Hayes et al., 2007).

- **Intrinsically Safe** – A RuBee base station and tag produces low energy magnetic energy simply not capable of heating explosives or creating a spark. In independent studies carried out by the Department of Energy RuBee was given a Safe Separation Distance (SSD) of zero, and is the only wireless technology to have that rating. That means tags and base stations can be placed directly on high explosives with no risk of accidental ignition or any heating.

- **High security and privacy** RuBee tags have many unique advantages in high security applications. The Eavesdropping range (the range at which a person with unlimited funds can listen to tag conversations) is the same as tag range. That means if someone is listening, they must be close enough for you to be able to see them. This is not true for RFID or 802 protocols (see Wall Street Journal May 4 Credit Card Data). That means no one can secretly listen to tag/base station conversations. In addition, since RuBee tags have a battery, a crystal and sRAM memory, they can use strong encryption with nearly uncrackable one time keys, or totally uncrackable one time pads. RuBee is in use today in many high security applications for these reasons. RuBee is the only wireless technology approved for use in secure US government sites.

- **Controlled volumetric range** – RuBee has a maximum volumetric range of approximately 10,000 square feet (900 m²), using volumetric loop antennas — From even a small volumetric antenna of 1 sq ft (900 cm²), RuBee can read a tag within an egg-shaped (ellipsoid) volume of about 10 x 10 x 15 ft (3 x 3 x 5 m). A special feature of IEEE P1902.1 known as Clip makes it possible to place many adjacent loop antennas in an antenna farm, and read from tens to hundreds of base-stations simultaneously.

- **Cost effective** - With RuBee, relatively simple base stations and routers can be employed, which means receivers and card readers can be reasonably priced as compared to higher frequency transceivers. In addition, the tags often include a single chip, a battery, a crystal and an antenna, and can be priced competitively with respect to active RFID tags (those including a battery).

- **Less noise** – Because ambient noise in a region falls off as $1/r^3$, RuBee exhibits reduced susceptibility to extraneous noise. The major limit to antenna size is deep space noise.

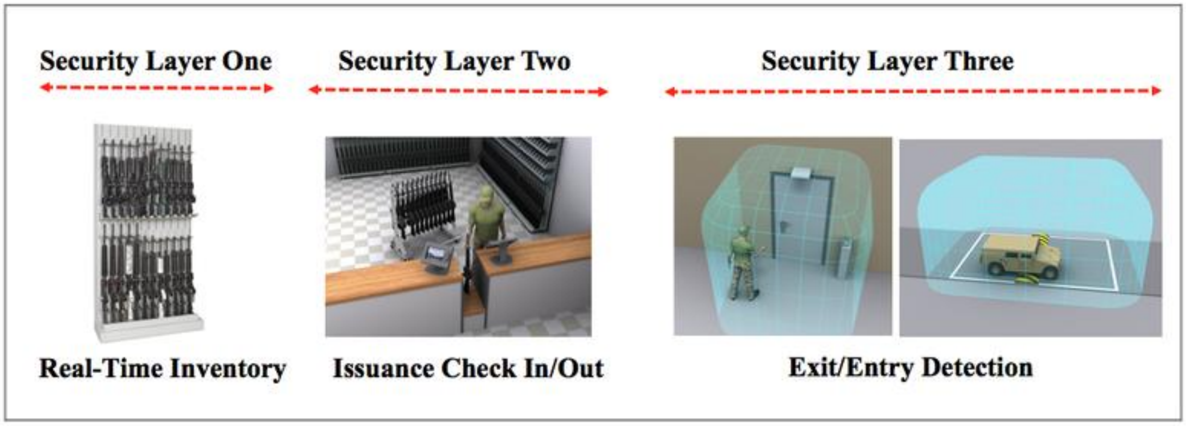
Unique RuBee application example: mission critical asset availability and security

Because RuBee is secure and magnetic it can provide real-time automated visibility, and the highest possible security of Mission Critical Assets—Mission Critical Assets (MCA) are assets that simply can not be lost or stolen, worth far more on the street or in hands of terrorists than the cost to replace. Visible Assets, Inc., Dasco Date, Inc., SMi Ltd, and Laser Device Inc. provide RuBee based automated MCA visibility and security using three important security layers:

- **Security Layer 1:** Real-Time, Storage Physical Inventory. Assets in storage in a warehouse on racks, shelves or weapons in armory racks or other secure facility have RuBee wireless tags embedded or attached. RuBee enabled smart racks and smart shelves turn the steel in these racks into an antenna, and Visible software applications do daily or hourly audit trails of each item and report inventory and asset status.

- **Security Layer 2:** Issuance Check Out/In. When an asset is removed from inventory, we know it has been removed from shelf, but ownership has to be transferred from a “storekeeper” to a new owner, a soldier or guard or asset guardian. This is done using ruggedized Apple iPads known as gRaps® that have a RuBee embedded reader. Tags are read as the asset is passed across the check out counter.

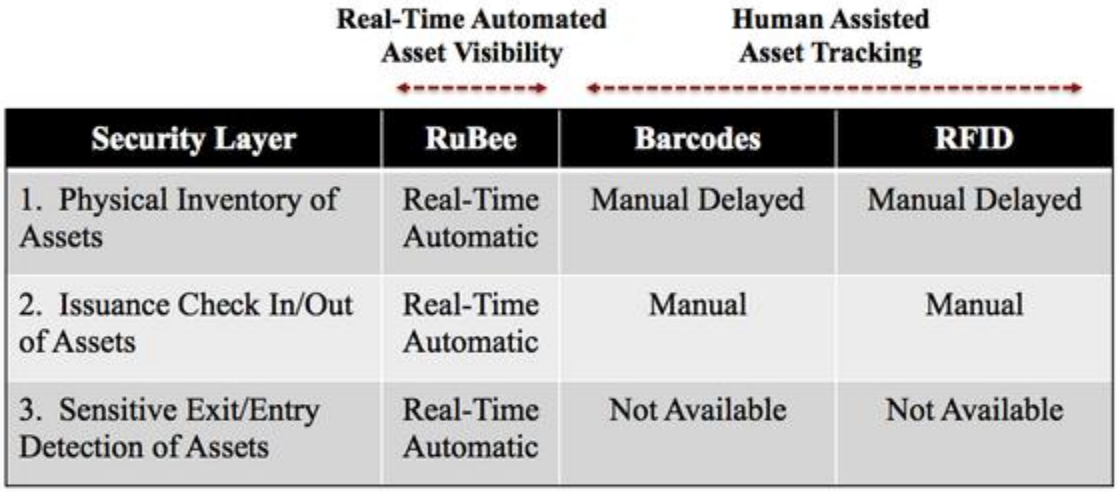
- **Seurity Layer 3:** Exit/Entry Detection. When the asset leaves the facility RuBee portal platforms provide identification detection and alarms using DoorGuard® and GateGuard®. Both detect RuBee enabled assets and IDs as a person passes though a door or gate, on foot or in a vehicle. These systems have passed many objective User Acceptance Tests (UAT) with 100% detection of assets even if hidden inside a steel case or vehicle.



RuBee Three-Layer Security

Three-Layer Security provides process free security for mission critical assets on racks with real-time inventiry, on check in/out, and with sensitive exit entry detection of people and assets. Because RuBee is not blocked by people or by steel tags are read automatically without human assistance

Security becomes far more reliant on human trust with loss of any layer. RuBee reduces that human trust reliance with full “process free” automation in all three layers. For example, if something is removed from inventory off the racks, but does not get checked out an alarm is issued. If an asset exits facility but is not checked out, an alarm is issued etc. RFID and barcode systems are blocked by steel and the human body. As a result security is based on new human processes focused only on Layer 2. Both become human assisted asset tracking systems, not real-time automated security systems. Visible has repeatedly proven that RuBee is the wireless technology that can provide fully integrated, visibility with three security layer automation.



	Real-Time Automated Asset Visibility	Human Assisted Asset Tracking	
Security Layer	**RuBee**	**Barcodes**	**RFID**
1. Physical Inventory of Assets	Real-Time Automatic	Manual Delayed	Manual Delayed
2. Issuance Check In/Out of Assets	Real-Time Automatic	Manual	Manual
3. Sensitive Exit/Entry Detection of Assets	Real-Time Automatic	Not Available	Not Available

Three-Layer RuBee Security compared to tracking technologies like bar codes and RFID. Bar codes and RFID become line-of-sight in harsh environments, blocked by people and by steel, and therefore require human assisted tag reads. In contrast RuBee visibility is not line-of-sight in harsh environments and provides process free security for mission critical assets because it is not blocked by steel or water

RFID and barcode systems are blocked by steel and the human body. As a result security is based on new human processes focused only on Security Layer 2. Both become human assisted asset tracking systems, not real-time automated security systems. Many in-use secure sites provide, process-free, fully automated, RuBee visibility with three-layer security.