Visible Assets, Inc.

High Security Government and Healthcare
IEEE P1902.1 (RuBee) Applications

The Elimination of Eavesdropping, Tempest
and Target Risk in Wireless Networks.

March 2008

John K. Stevens Ph.D.
CEO, Chairman
Visible Assets, Inc.
617-395-7601
john@rubee.com
IEEE P1902.1 RuBee Licensees

- Seiko/Epson Electronics – Full Chip Set 09
- Sig Sauer Inc. – Weapons Visibility Networks
- US Air Force – Tool Visibility Networks
- Trimble Inc. - Mobile Visibility (Vans, Trucks)
- Visible Assets – Healthcare, Livestock, HV Assets
- CERT, Abu Dhabi (UAE) - Healthcare
- MidTown Technologies - Construction
- 2 Fortune 100’s, 1 Fortune 500, many SmallCo’s
The Problem

Healthcare:
+ Patient Visibility Reduces Cost by $168/ Patient –
- HIPAA Patient Privacy Requirement

DoE:
+ Asset Visibility Essential
- Evil Dark Spies With Unlimited Capital in Bushes
- Visibility in facilities with highest security requirement in the world.

DoD:
+ Weapons Visibility Pedigree Essential + Safety
- The Enemy Looking for RF Targets
The Problem

The Wireless System is Not Working as Well as We Would Like

Base Station

0.5 Watts
The Problem

So Let’s Increase The Base Station Power
And Get Longer Range, More Reliable Performance

But we also ……..

✅ Create New Human Safety Issues

✅ Create New SecurityIssues
The Problem
Our Focus Today is on Four Key Security Issues

1. Clone-ability
2. Eavesdropping
   (Tempest)
   (Target)
3. Authentication
4. Packet Security
All forms of solid state memory leave, detectable traces for a 0 and a 1. These traces may be reverse engineered at low cost even months after removal of power. With access to modest cost equipment, this makes it easy for any attacker to clone or spoof any tag. Any RFID tag may be reversed engineered for $5,000 to maximum of $50,000 from multiple sources in the US, Canada, EU, and Asia.
The Security Problem
Tempest, Eavesdropping Target
Because RF voltage decays at a rate of 1/R (R is distance in meters) from the source, most RF signals may be, monitored (listened to) many miles away. Eavesdropping is the major security risk in any RF wireless network. The eavesdropper may require expensive specialized equipment, but as shown in next slides this not always true.

Note: Voltage across a coil from an RF source drops off 1/R. Power or Voltage \times Current through a coil drops off 1/R^2. All comparisons in this document are based on simple voltage measured across a coil.
The Security Problem
Tempest, Eavesdropping Target

Again, because RF decays $1/R$ it may also be used to transmit unauthorized information a distance from a site. For example, an attacker could secretly design a microphone into a RFID base-station, and transmit everything said in the room without the knowledge of the owner. It would look like RFID data but actually represents major security risk. This is known as the Tempest threat.

Signal decays $1/R$
(R is meters from source)
The Security Problem
Eavesdropping Tempest Case Study – 20 mile radius 13.56 Mhz

Case Study: A conventional 13.56 MHz RFID system was accidently left “Power On” for two months (2 months). A poorly installed cable connector twenty one feet away picked up the signal and injected into the entire Comcast cable network.
The Security Problem
Case Study – 20 mile radius 13.56 Mhz

The injected 13.56 Mhz signal was detectable in the cable network for a 20 mile radius, disrupted pay-per-view and lowered internet bandwidth for two months. It took Comcast two months to track down the source. It is easy to eavesdrop and the tempest threat is real.
“Compromising Emanations”
Detection From Space

An attacker with a budget (any government), may monitor RF signals using line of sight satellites in outer space. Cell phone traffic (under 1 watt power), is routinely monitored around the world from strategically placed satellites. These are known in the government as “compromising emanations”.
“Compromising Emanations”
Source becomes Target

The key outcome: an attacker can use the RF source as a target. This is known as the RF Target risk.
The Security Problem
Packet Security is and Always will be Weak.

2007: TJX or TJMax/ Marshalls 200 million identities

2007: RSA Conference 32 Evil Twin Attacks

2005: FBI cracked WEP 128 encryption under 3 minutes

Free On-Line Programs: aircracker-rig, weplab, WEPCrack, airsnort, cracks WEP, WPA and WPA2.
RuBee
Technology Summary
Maxwell's Equations

\[ \nabla \cdot \vec{E} = \frac{\rho}{\varepsilon_0} \quad \text{(Gauss' Law - electrostatics)} \]

\[ \nabla \cdot \vec{B} = 0 \quad \text{(Gauss' Law - magnetostatics)} \]

\[ \nabla \times \vec{E} = -\frac{\partial \vec{B}}{\partial t} \quad \text{(Faraday's Law)} \]

\[ \nabla \times \vec{B} = \mu_0 \vec{J} + \mu_0 \varepsilon_0 \frac{\partial \vec{E}}{\partial t} \quad \text{(Ampère-Maxwell Law)} \]
RuBee

Is a Transceiver Mode Active Radiating Protocol

131 KHz Battery + Crystal + \(\nabla \cdot \vec{B}\)

RuBee is Magnetic (Inductive)
Water Immune
Steel Friendly
Human Safe
Low frequency means low power consumption. 20 year life has been achieved in the field Li coin size batteries.
RuBee
Long Open Tag Range

25-35 Feet Volumetric Air Tag Range

Because RuBee is in Transceiver Mode
RuBee
Long Range and Undetectable E Power

RuBee Wireless Does not Transmit using RF, “it has no detectable RF power”

10^-9 Watts of E Power
40 Nanowatts

Base Station

17 Feet (34 volume feet)
RuBee

RuBee is Low Power B (magnetic energy)

RuBee wireless uses 1/5 to 1/30th the magnetic power found in many consumer exposed sites. Examples: airport metal detectors, and anti-theft protection systems in retail stores are all 5-10 times the power found in RuBee.

600 mGauss B power from Base
50 mGauss B power from Tag

17 Feet (34 volume feet)
RuBee
Range and Low Power H 600 mGauss

RuBee signals (voltage across a coil) drop off at 1/R^3 not 1/R with 17’ range. RuBee power actually drops off much faster at 1/R^6.
RuBee
Range and Power

Water has little or no affect

Signal $1/R^3$

Base Station

Tag 23

16.5 Feet (33 volume feet)
RuBee
Range and Power

Still works in steel
reduced range

Base Station

Signal 1/R³

Tag 23

5 Feet (10 volume feet)
RuBee
Range and Power

Still works on steel
Range enhanced if tuned

Base Station

12.5 Feet (25 volume feet)
RuBee
Tag Range Limited by Constant Deep Space Noise

0.06 to 0.006 mGauss
Deep space background noise
24 hours/day, 7 days/week Deep Space Noise

Deep Space

Local Transient Spikes (Lightening )
The Security Problem
How has RuBee Addressed Each Item?

1. Clone-ability
2. Eavesdropping (Tempest) (Target)
3. Authentication
4. Packet Security
RuBee Tags
Form Factors

RuBee t-Tags
2mm - 0.78mm thick

iDots™
RuBee Tags
Form Factors

Small t-Tags
Cell Phones

Large t-Tags
For Heavy Steel
The RuBee Tags

Form Factors

ID Tag – 3.2” x 2.4” x 2mm thick.

2T Wallet Tag – 3.2” x 2.4” x 1mm thick on edge and 2mm on top. 2T cards work in your wallet.
RuBee Security
The Data is in The Tag

MCU  4 – 32 Bit
500 Byte – 7KBytes
10K-25K bytes EE

<table>
<thead>
<tr>
<th>Tag IP</th>
<th>11.11.11.00</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tag Subnet</td>
<td>11.11.11.1</td>
</tr>
<tr>
<td>MAC:</td>
<td>77-AC-D8-9A-99-AC</td>
</tr>
<tr>
<td>Object Name</td>
<td>Hip 23678</td>
</tr>
<tr>
<td>Size</td>
<td>23mm x 18mm</td>
</tr>
<tr>
<td>Birthdate</td>
<td>11/23/2004</td>
</tr>
<tr>
<td>Expirydate</td>
<td>11/2007</td>
</tr>
<tr>
<td>Serial Number</td>
<td>6778895</td>
</tr>
<tr>
<td>Lot Number</td>
<td>7878789905</td>
</tr>
<tr>
<td>Manf. Site</td>
<td>Ireland</td>
</tr>
<tr>
<td>Manufacture</td>
<td>Medco</td>
</tr>
<tr>
<td>CRC</td>
<td>34567</td>
</tr>
</tbody>
</table>
### RuBee Security

Data is Stored in SRAM Memory

#### Memory map v. 07D

<table>
<thead>
<tr>
<th>Hi/Lo</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Buffer</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>32 bit ID</td>
<td></td>
<td></td>
<td></td>
<td>32 bit master ID</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>32 bit group ID</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>32 bit clock counter</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Preset LED timer</td>
<td></td>
<td>Read Temp. Time</td>
<td></td>
<td>Temp. Offset</td>
<td>LED masks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Red Line</td>
<td></td>
<td>Blue Line</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Display data RAM reserved for Temperature only, not shown in V05</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Display data RAM, scrollable from B0h to C0h, default page, set MSB to scroll</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Display data RAM, scrollable from C0h to D0h</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Display data RAM, scrollable from D0h to E0h</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Display data RAM, scrollable from E0h to F0h</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Display data RAM, scrollable from F0h to B0h</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Several key items are stored in memory.
The tags IP address, master ID, subnet (group) asset data.
RuBee Security
Safe SRAM Data Storage

RuBee uses static memory (SRAM) and can therefore also use optional advance bit swap keys/data algorithms, to rewrite a secure word once every 10 minutes. This guarantees no one can reverse engineer a RuBee tag or clone a Rubee tags’ pedigree. Bit swapping is near impossible with EEPROM, due to long write times, high power considerations, and limited read/write life.
RuBee Security
Safe SRAM Data Storage

“A RuBee Tag’s hardware can be reversed engineered (same as any electronic device), but critical tag content remains secure, minimizing clone-ability risk”
RuBee Tags can use Real-Time AES Encryption Similar to TLS protocol. We have strong packet layer authentication security.
RuBee Tags can use Real-Time AES Encryption

Base Range 17 ft

Hey it is Visa Calling

I only talk to Visa at 1 foot

Tag Range 17 ft
RuBee Tags use Real-Time AES Encryption, But we also have strong physical layer security.

![Diagram showing Base and Tag interaction with ranges and commands]
RuBee Real-Time Range Management Makes eavesdropping impossible

Base Range 1 ft

Tag Range 1 ft

No Detectable RuBee Signal @ 2ft
All eavesdropping blocked by deep space kilometric noise
RuBee
Tag Range Limited by Constant Deep Space Noise

“An attacker with a near unlimited budget can provide only a few feet of additional listen range, beyond the tag range obtained with the lowest possible cost RuBee Tag and lowest possible cost RuBee base station range.”
RuBee Security
The Data can be Private and Secure

Visible™

<table>
<thead>
<tr>
<th>Tag IP</th>
<th>11.11.11.00</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tag Subnet</td>
<td>11.11.11.1</td>
</tr>
<tr>
<td>MAC:</td>
<td>Locked</td>
</tr>
<tr>
<td>Object Name</td>
<td>Hip 23678</td>
</tr>
<tr>
<td>Size</td>
<td>23mm x 18mm</td>
</tr>
<tr>
<td>Birthdate</td>
<td>Encrypted</td>
</tr>
<tr>
<td>Expirydate</td>
<td>11/2007</td>
</tr>
<tr>
<td>Serial Number</td>
<td>6778895</td>
</tr>
<tr>
<td>Lot Number</td>
<td>7878789905</td>
</tr>
<tr>
<td>Manf. Site</td>
<td>Ireland</td>
</tr>
<tr>
<td>Manufacture</td>
<td>Medco</td>
</tr>
<tr>
<td>CRC</td>
<td>34567</td>
</tr>
</tbody>
</table>
RuBee Packet Security
Selective Optional Encrypted Security with Keys

Rijndael (AES), LZW, Eliptic, PGP, TWOFISH, BLOWISH, CAST, MARS, TEA

Because RuBee tags have a clock they can optionally use single Keys or OTP
RuBee Packet Security
Selective Optional Encrypted Security with Keys

“Because RuBee Tags have a CPU, SRAM memory, high content mask ROM, a date and time (clock) – RuBee can employ the most advanced, authentication and Packet security possible, including One Time Pads”
The Security Problem

RuBee has addressed each item on the list

- Clone-ability
- Eavesdropping (Tempest) (Target)
- Authentication
- Packet Security
“A RuBee Tag may be one of the most secure wireless devices on the planet”
Application Examples
Procedure Room
Medical device implants today…

Hospital hall storage and the inventory is $5 billion/year…
Transforming The Procedure Area
Medical Device Smart Shelf
The RuBee Smart Cart is in use now with four multiplexed antennas that can read a RuBee tag anywhere in the operating room. Precise times for patient entry, product entry and product identity, Physician, Nurse identity and data logs are all captured with no change in process, and total safety.
Transforming The Procedure Area
Smart Cart

**Step 1:** Sponge + Pharmaceutical Dispensary + Blood Products + RuBee Access Control.

**Step 2:** Sponge + Pharmaceutical + RuBee Access Control + RuBee Sponge Tag and Count + RuBee Drug Tags, Blood Product Tags and Part11 Data Log.
Application Examples
Security Portals
Visibility Portal
RuBee Mats and RuBee Appliances

In The Wallet 2T-Tag
Cell Phones Wrapped in Aluminum Foil

Cell Phones 1-4 were wrapped with one layer of .001 inch Al foil and sealed. Tests in front breast pocket were repeated.
Test Portal Antennas

Cell phone test detection inside an aluminum brief case.
Cell Phones in Aluminum Brief Case

Cell Phone 1

Cell Phone 2

Cell Phone 3

Cell Phone 4
RuBee Security Issues
Security Plans Approved

• Los Alamos
• Sandia
• Pantex
• Savannah River
• Oak Ridge
• Idaho National Labs
• Lawrence Livermore
Application Examples

Weapons Visibility Rack

Sig Sauer
RuBee Enabled Weapons
Enhanced Safety Security

ATF Serial Number
Make Model
Manufactured Date
Number of Rounds Fired
Mean Round Kinetics (MRK)
A weapon is removed from storage, the serial number turns to red and the date time event is stored the Part11 audit trail log.
Firearms maybe stored on shelves with full physical inventory, check in check out and use records. Firearms maybe stored in original boxes or on specialized shelf.
Firearms and employees may be detected and identified by existing standard DOE Industrial Visibility portals now used for cell phones.
Firearms and employees maybe detected and identified by existing standard DOE Industrial Visibility portals now used for cell phones.
Application Examples
Tool Visibility
US Air Force
RuBee Family of Tools
Shadow Board

Smart Mat

Long Ranger Portal

RuBee TVN
Confidential

Visible™
Other Application Examples

Cervid Visibility
USDA NY CO
NASA Space Habitat
RuBee has Redefined Wireless Security

Thanks for your time