

Visible Assets, Inc.

High Security IEEE P1902.1 (RuBee) Applications and Issues For the Internet of Things

The Elimination of Clone-ability, Eavesdropping, Tempest and Target Risk in A Secure Wireless AIT Network.

John K. Stevens Ph.D.

CEO, Chairman

Visible Assets, Inc.

617-395-7601

john@rube.com

The Problem

Healthcare:

- + Patient Visibility Reduces Cost by \$168/ Patient –**
- HIPAA Patient Privacy Requirement**

DoE:

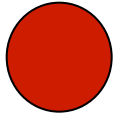
- + Asset Visibility Essential**
- Spies With Unlimited Capital in Bushes**
- Visibility in facilities with highest security requirement in the world.**

DoD:

- + Asset Visibility Pedigree Essential + Safety**
- Visibility in facilities with highest security requirement in the world.**

The Problem

Base Station



0.5 Watts



Transceiver

Active



Passive

Transponder

**The Wireless System is
NOT Working as Well as
We Would Like**

The Problem

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

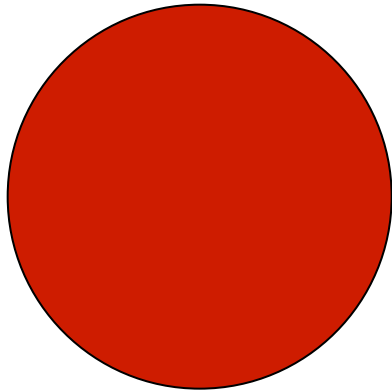


But we also

- ✓ **Create New Human Safety Issues**
- ✓ **Create New Security Issues**

The Problem

Our Focus Today is on Four Key Security Issues

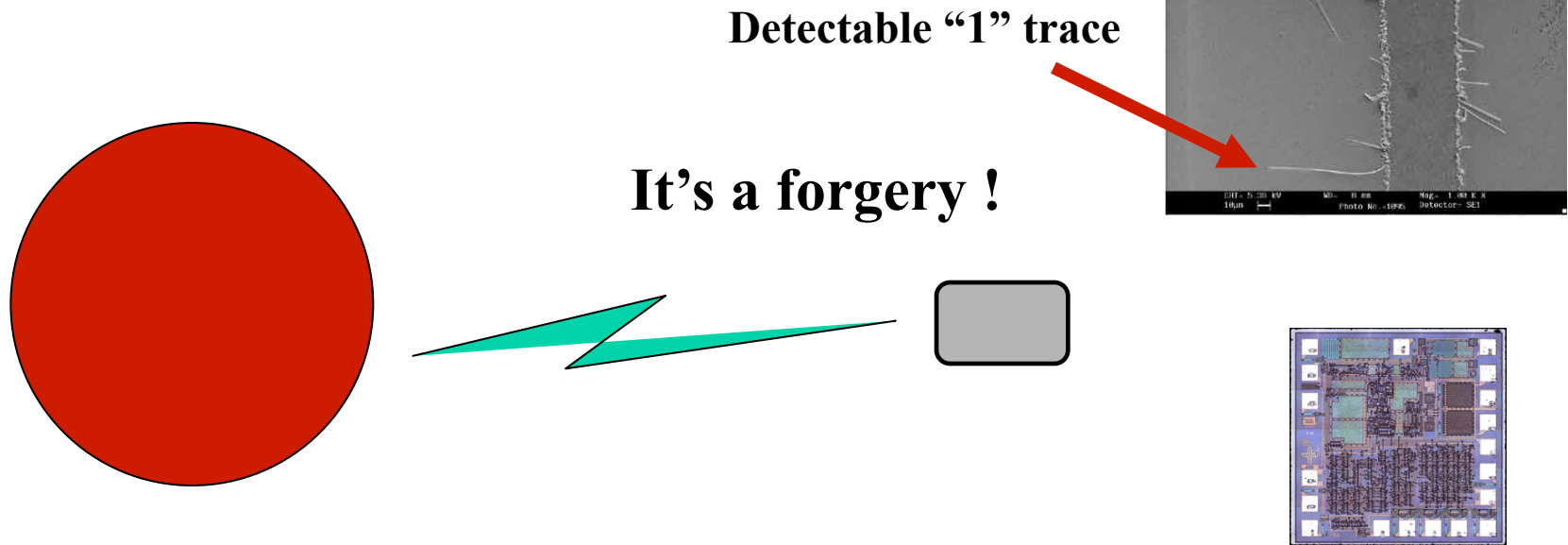


- 1. Clone-ability**
- 2. Eavesdropping**
(Tempest)
(Target)
- 3. Authentication**
- 4. Packet Security**



The Security Problem

Clone-ability

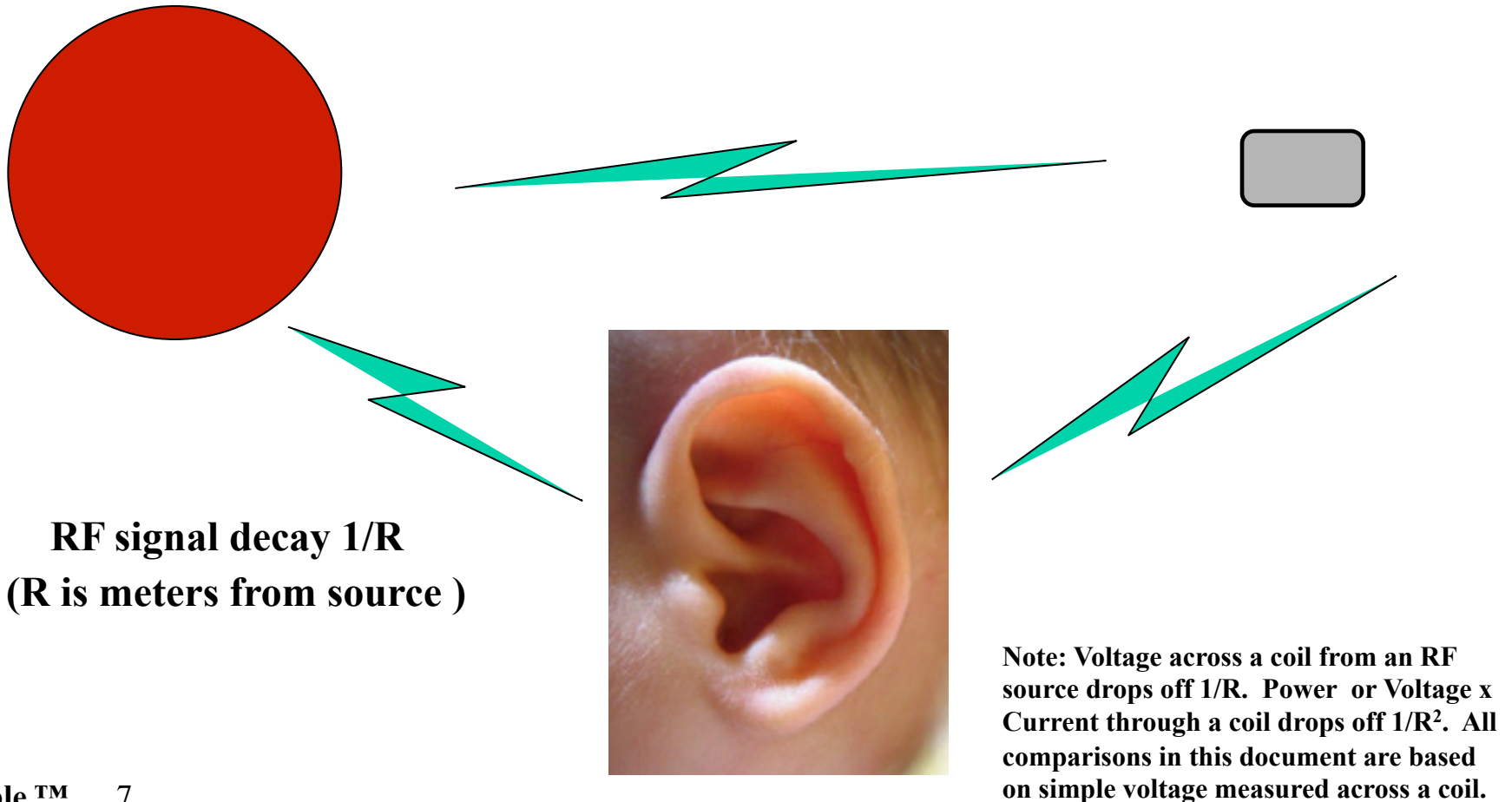


All forms of solid state memory leave, detectable traces for a 0 and a 1. These traces may be reverse engineered at low cost even months after removal of power. With access to modest cost equipment, this makes it easy for any attacker to clone or spoof any tag. Any RFID tag maybe reversed engineered for \$5,000 to maximum of \$50,000 from multiple sources in the US, Canada, EU, and Asia.

The Security Problem

Tempest, Eavesdropping Target

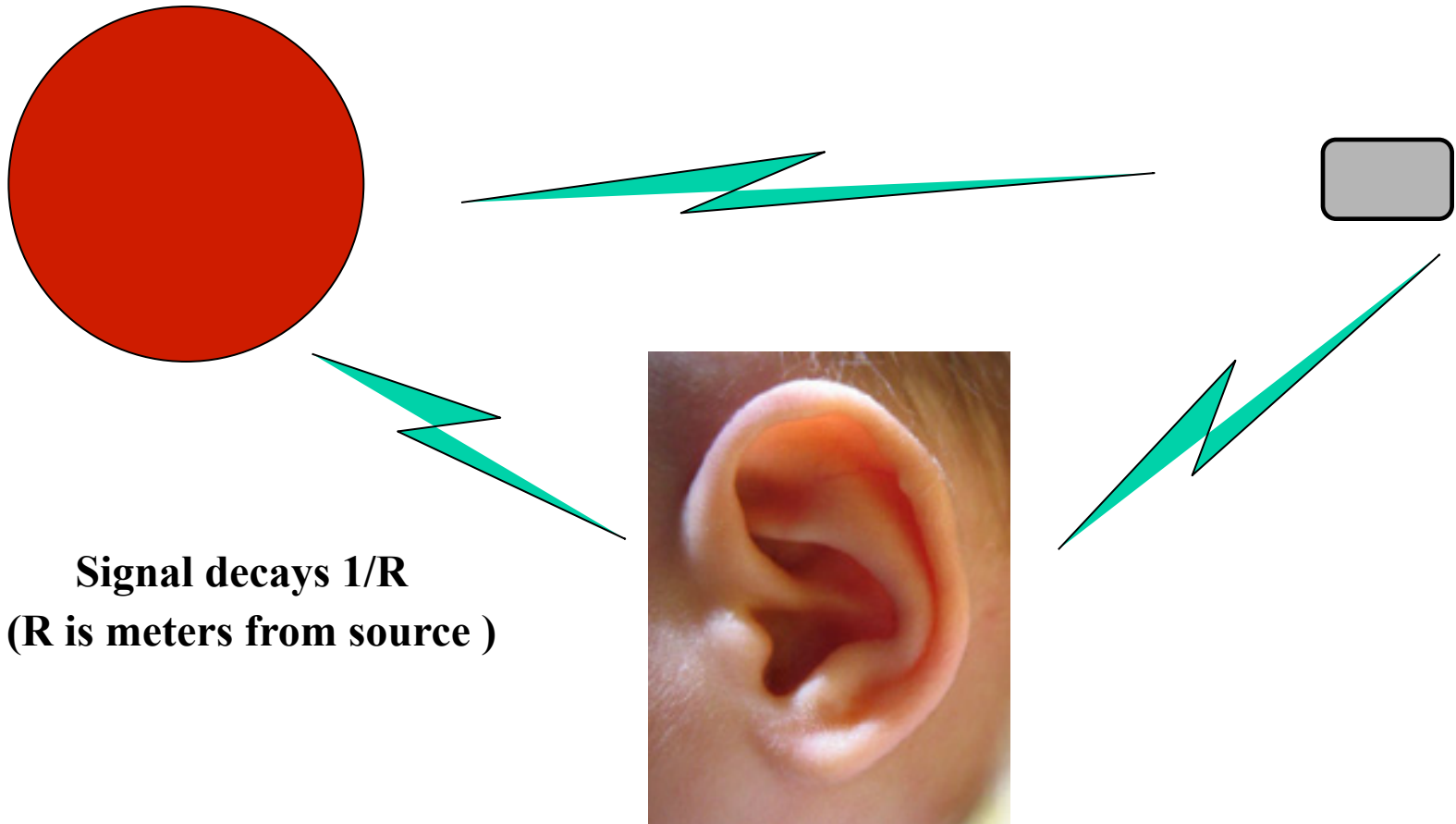
Because RF voltage decays at a rate of $1/R$ (R is distance in meters) from the source, most RF signals may be, monitored (listened to) many miles away. Eavesdropping is the major security risk in any RF wireless network. The eavesdropper may require expensive specialized equipment, but as shown in next slides this not always true.



The Security Problem

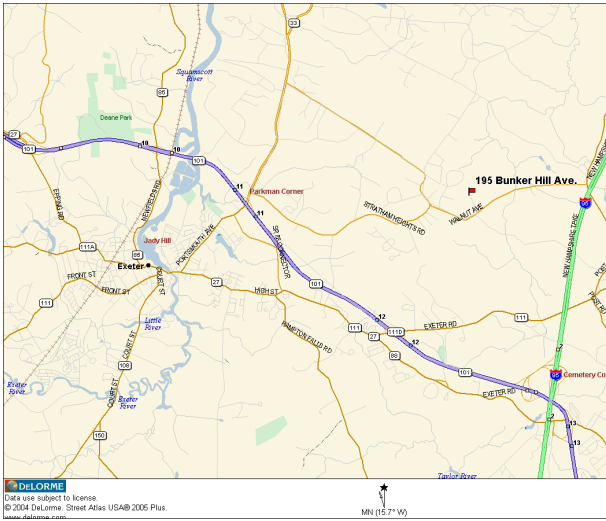
Tempest, Eavesdropping Target

Again, because RF decays $1/R$ it may also can be used 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 a The Tempest threat

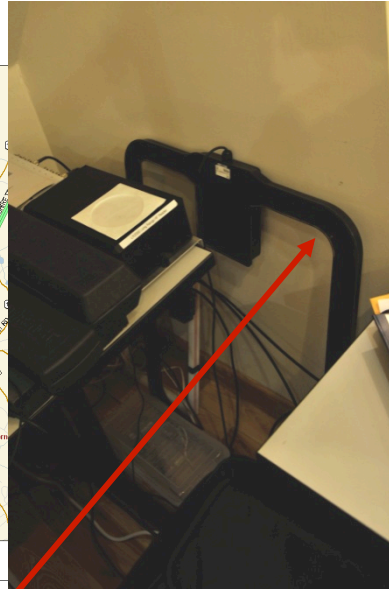


The Security Problem

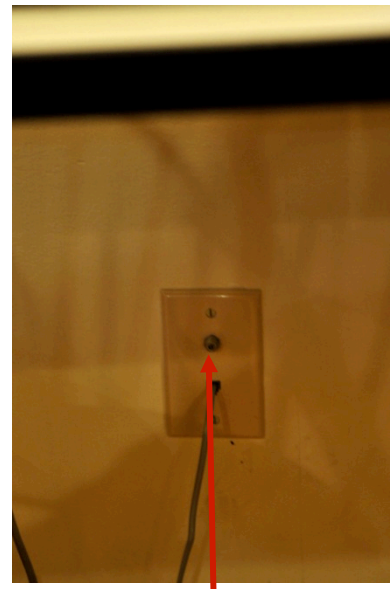
Eavesdropping Tempest Case Study – 20 mile radius 13.56 Mhz



13.56 System



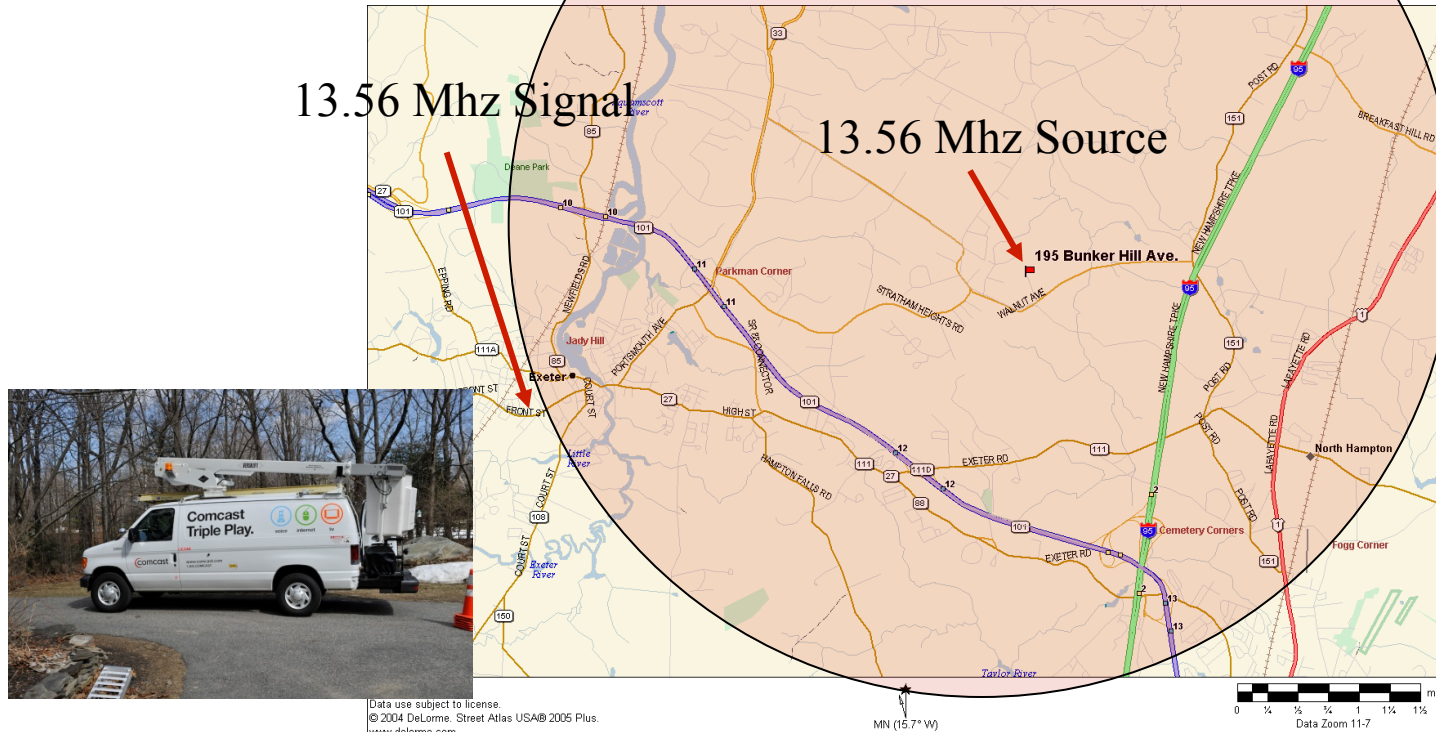
Poorly installed cable connector 21' feet away



Case Study: A conventional 13.56 MHz RFID system was accidentally 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

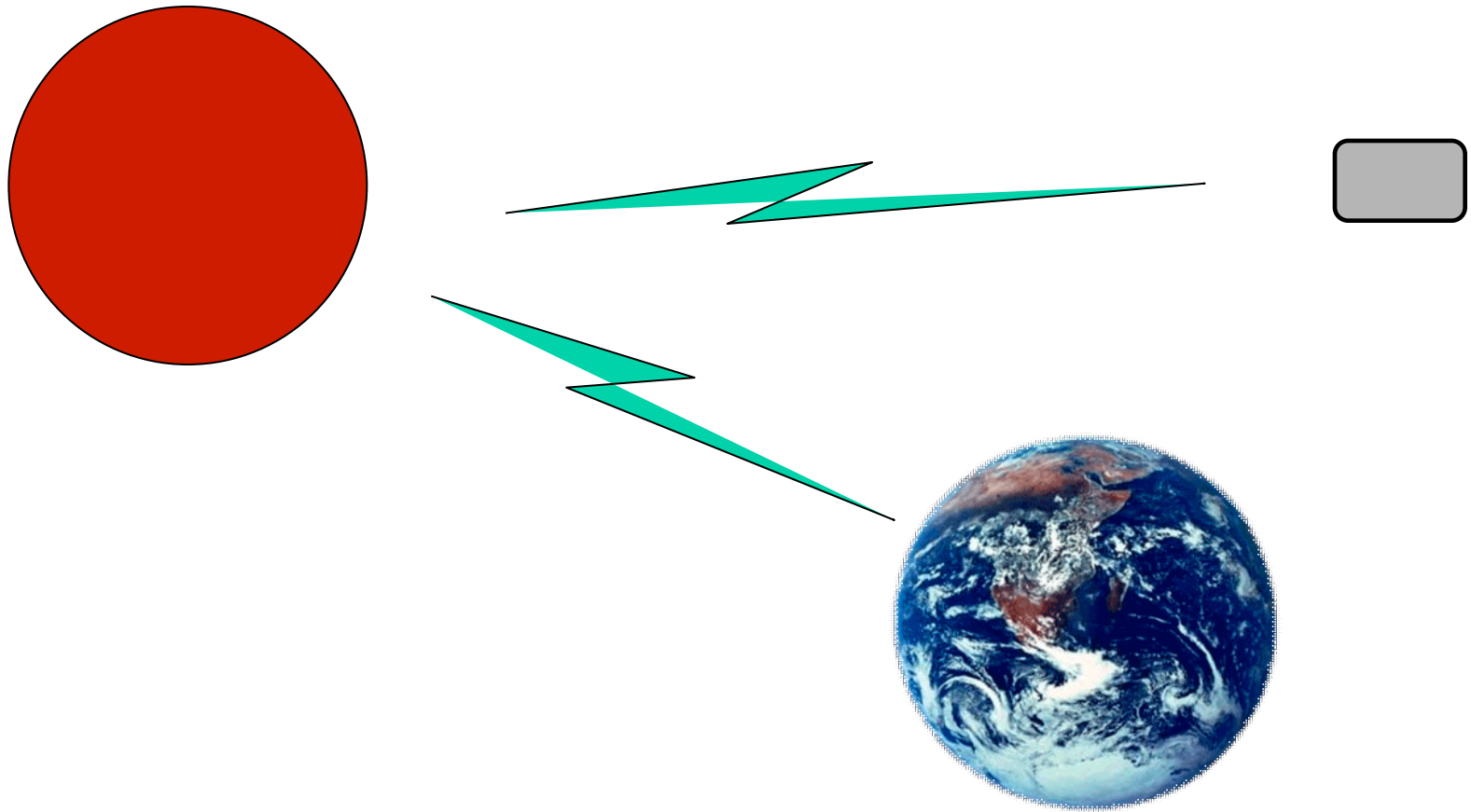
Case Study – 20 mile radius 13.56 Mhz



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.

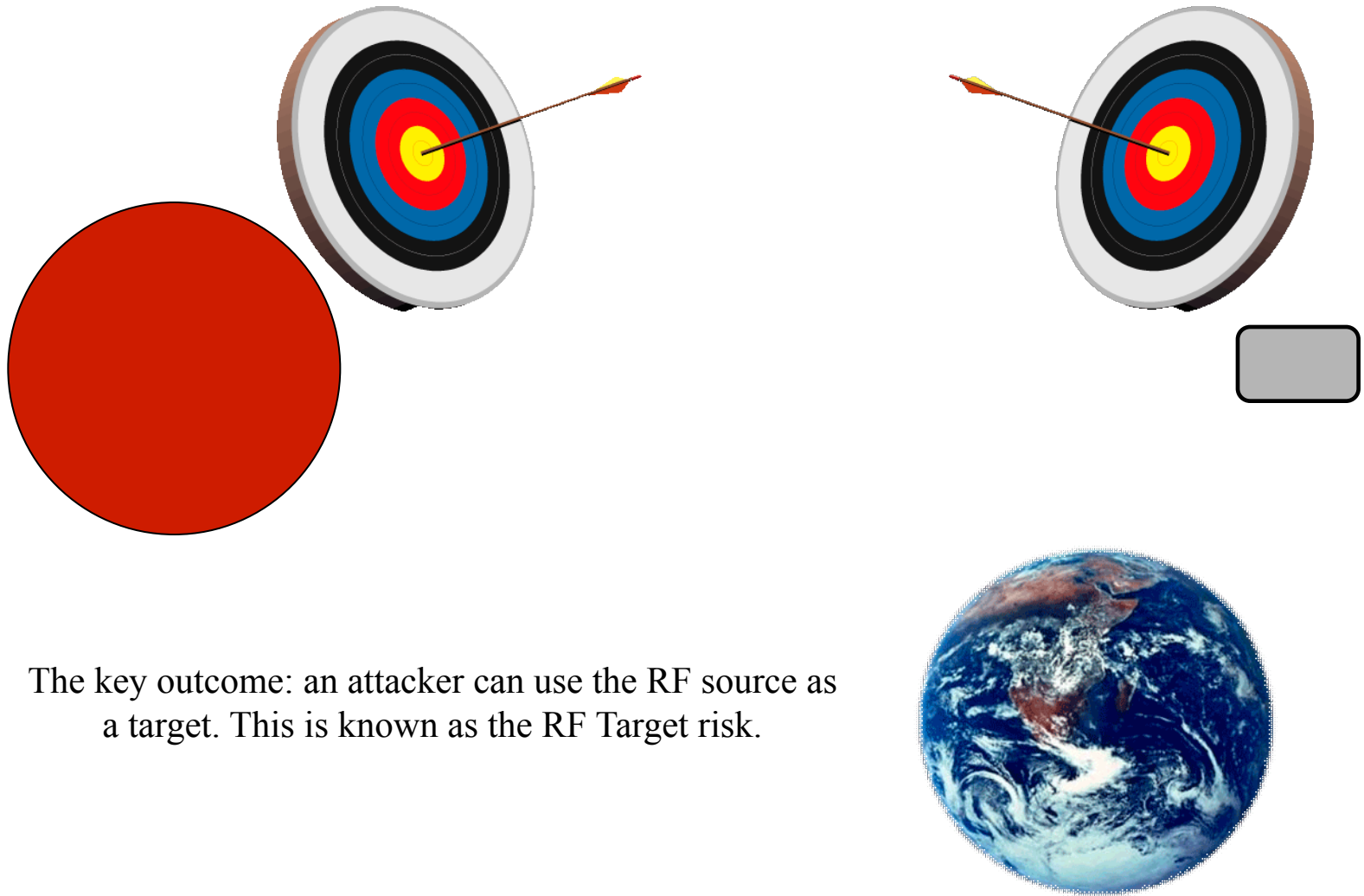
“Compromising Emanations” Detection From Space

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, airtsnort, cracks WEP, WPA and WPA2.**

RuBee

Technology Summary



Maxwell's Equations

$$\nabla \cdot \vec{E} = \frac{\rho}{\epsilon_0} \text{ (Gauss' Law - electrostatics)}$$

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

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

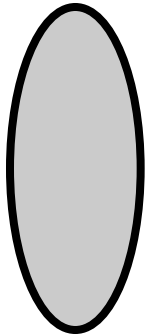
$$\nabla \times \vec{B} = \mu_0 \vec{J} + \mu_0 \epsilon_0 \frac{\partial \vec{E}}{\partial t} \text{ (Ampère-Maxwell Law)}$$

RuBee

Is a Transceiver Mode Active Radiating Protocol

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

Base Station



Transmit TX

Hello 23

Receive RX

Tag

**Tag
23**

RuBee is Magnetic (Inductive)

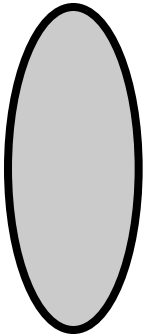
Water Immune

Steel Friendly

Human Safe

RuBee

Low frequency means low power consumption. 20 year life has been achieved in the field Li coin size batteries



Assumes 280 mA-hr Li Battery			
Freq.	Power (uA/hr)	Predicted Life	Units
128kHz	1	31.00	Years
13.56 MHz	102	3.78	Months
915 MHz	7,031	1.66	Days

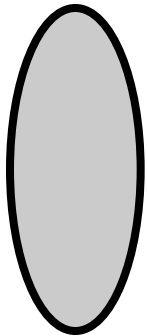
**Tag
23**

RuBee

Long Open Tag Range

25-35 Feet Volumetric Air Tag Range

Base Station



Receive RX

Transmit TX

**Tag
23**

Because RuBee is in Transceiver Mode

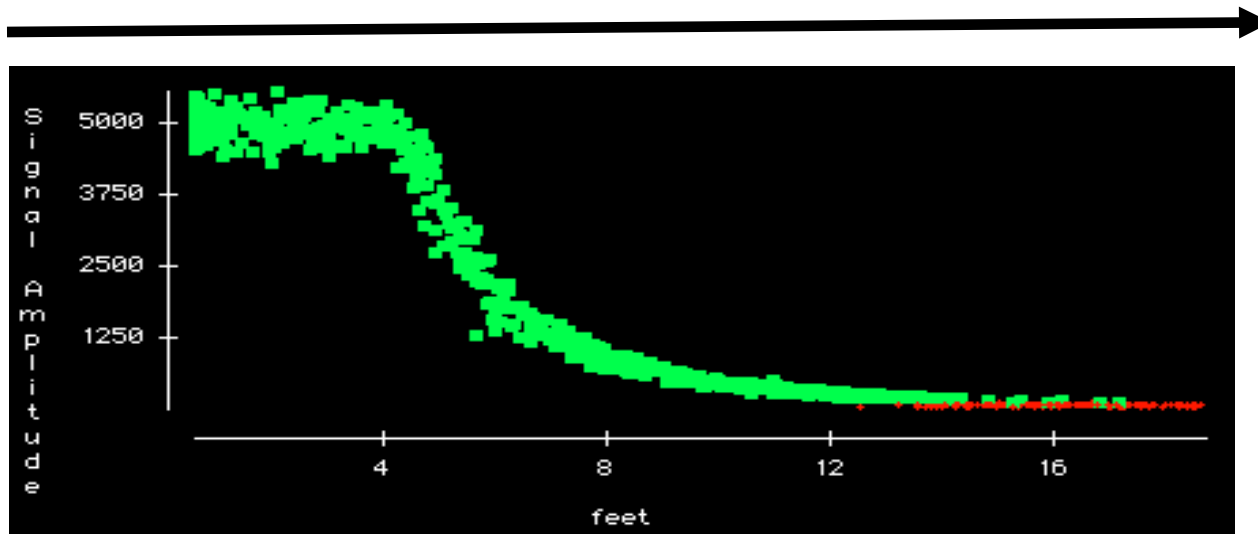
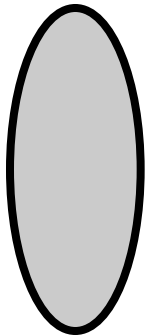
RuBee

Long Range and Undetectable E Power

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

Base Station

10^{-9} Watts of E Power
40 Nanowatts



Tag
23

17 Feet (34 volume feet)

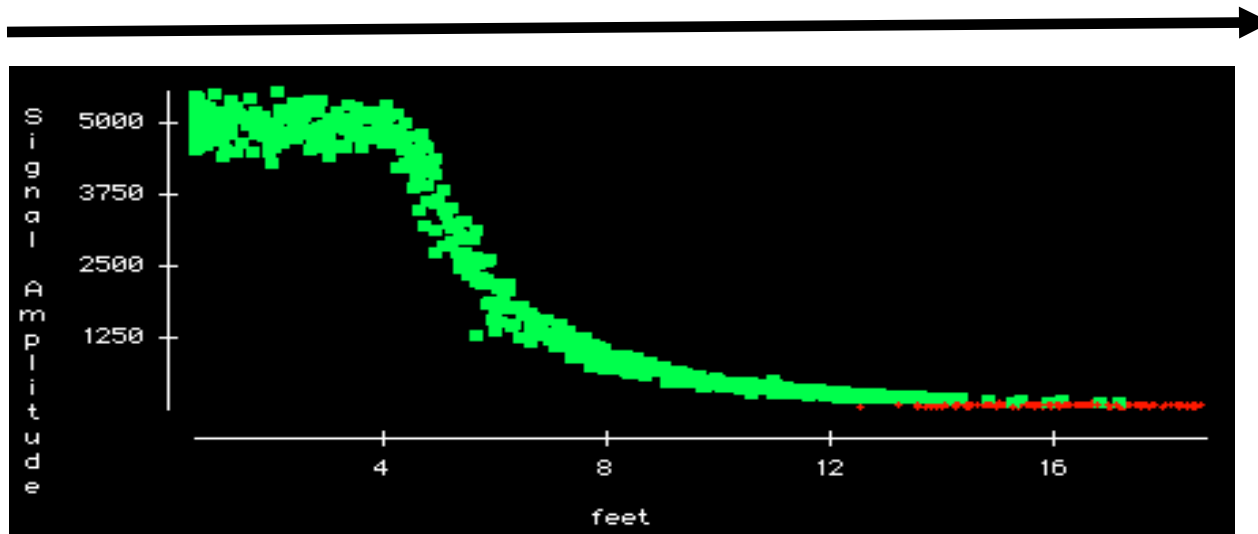
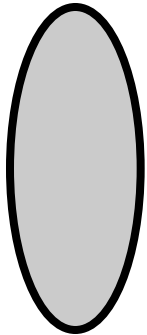
RuBee

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.

Base Station

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



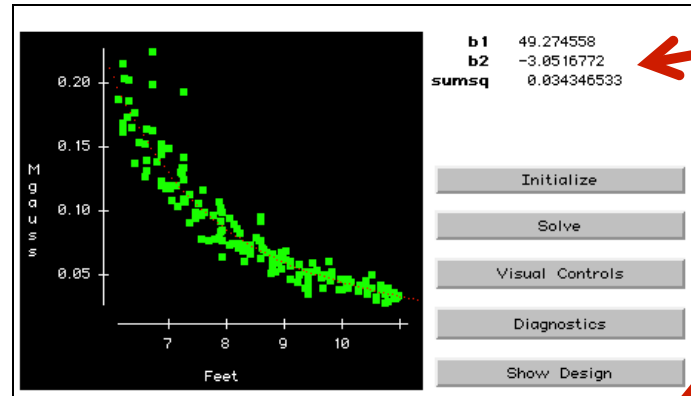
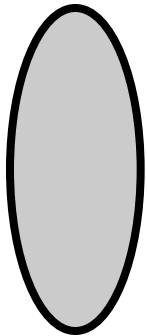
Tag
23

17 Feet (34 volume feet)

RuBee

Range and Low Power H 600 mGauss

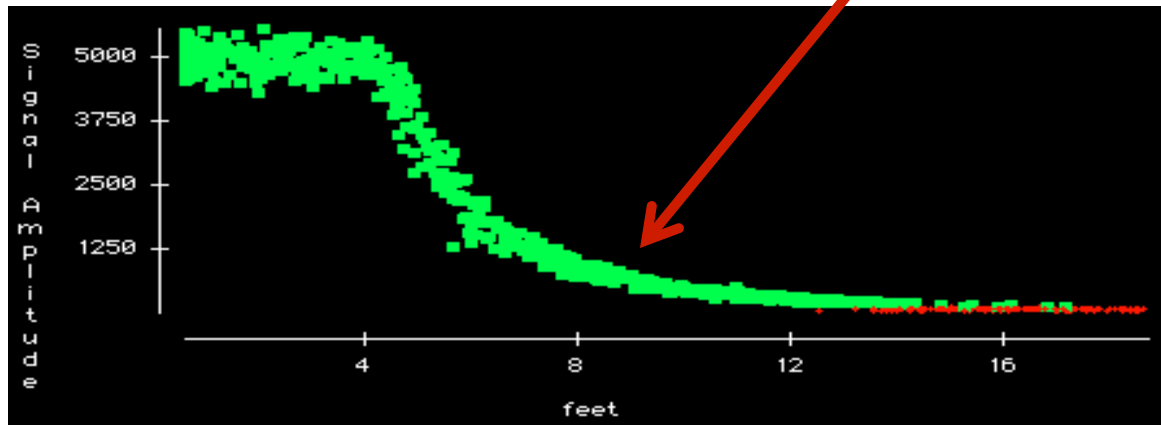
Base Station



3.0516772 best fit exp

Signal $1/R^3$

Tag
23

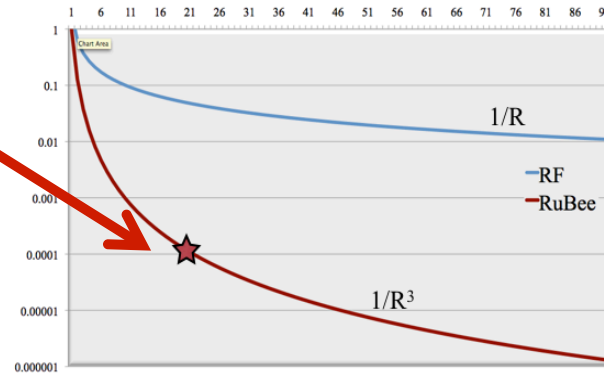


RuBee signals (voltage across a coil) drop off at $1/R^3$ not $1/R$ with 17' range.
RuBee power actually drops off much faster at $1/R^6$.

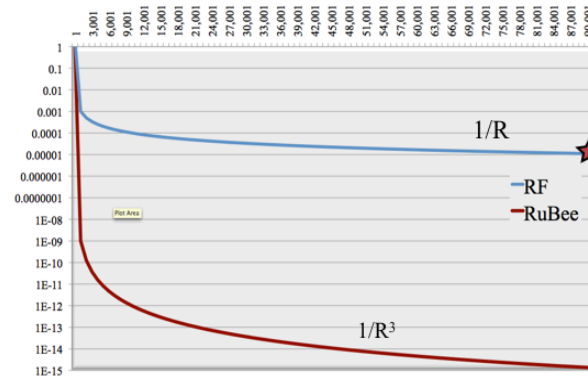
RuBee

Detection distance RF vs RuBee

RuBee
Signal $1/R^3$
DETECTION
17 FEET



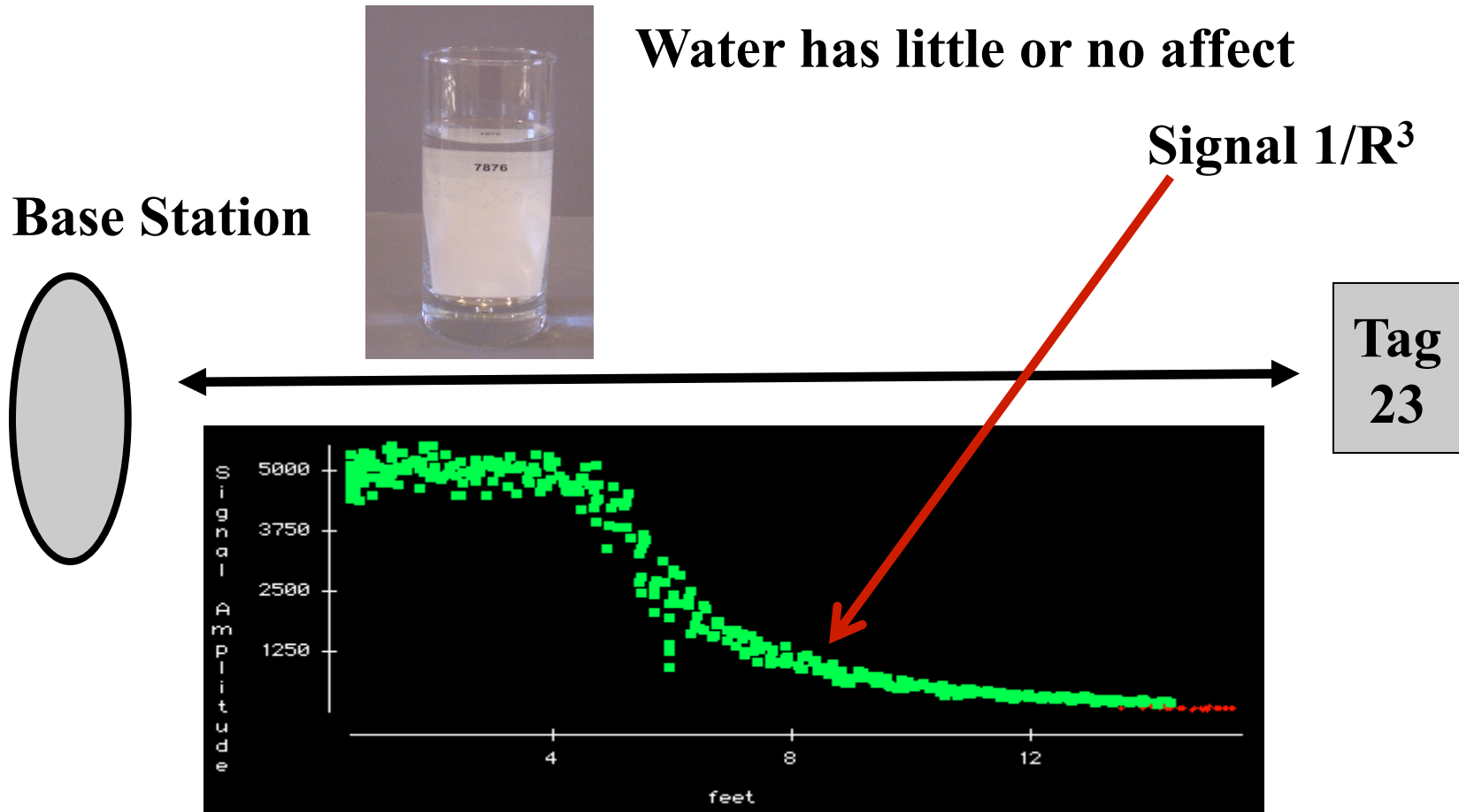
RF RFID
Signal $1/R$
DETECTION
17 MILES



Two graphs illustrate differences between $1/R$ drop for voltage across loop antenna for RF signals (E) and $1/R^3$ for magnetic signals (H) drop. 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. Note if we measure power H is $1/R^6$ and E is $1/R^2$

RuBee

Range and Power



16.5 Feet (33 volume feet)

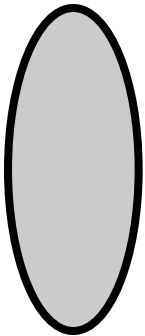
RuBee

Range and Power



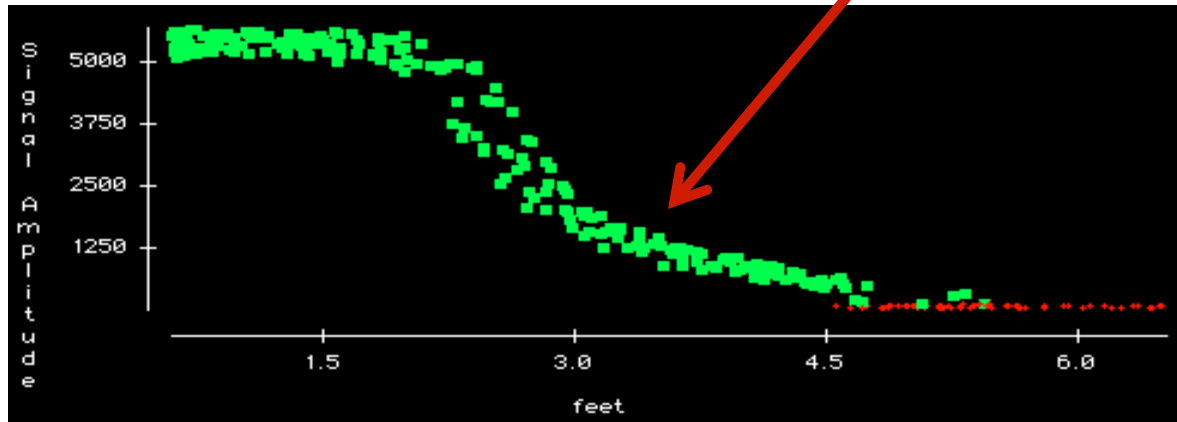
Still works in steel
reduced range

Base Station



Signal $1/R^3$

Tag
23



5 Feet (10 volume feet)

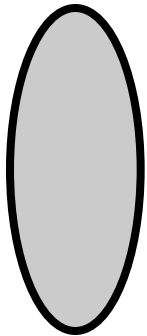
RuBee

Range and Power

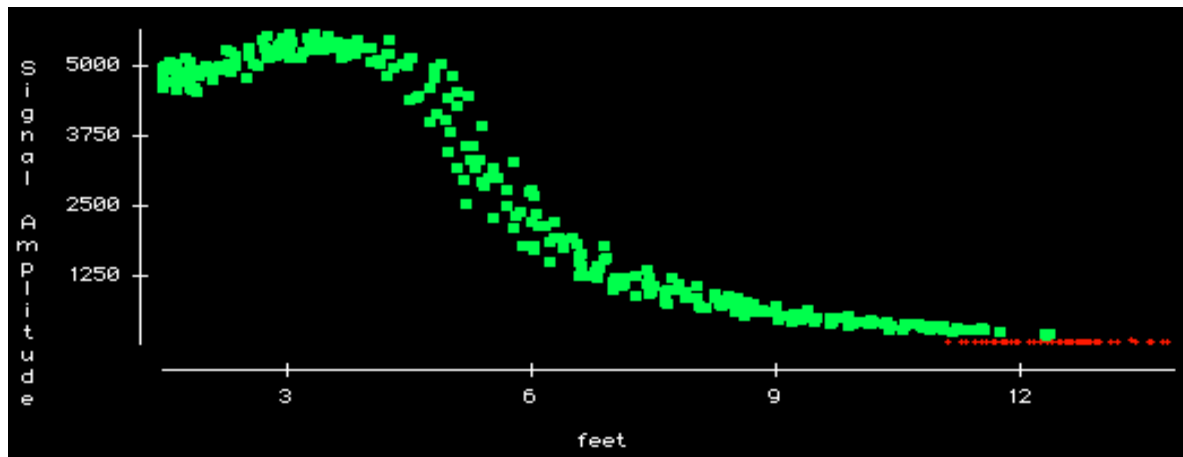


Still works on steel
Range enhanced if tuned

Base Station



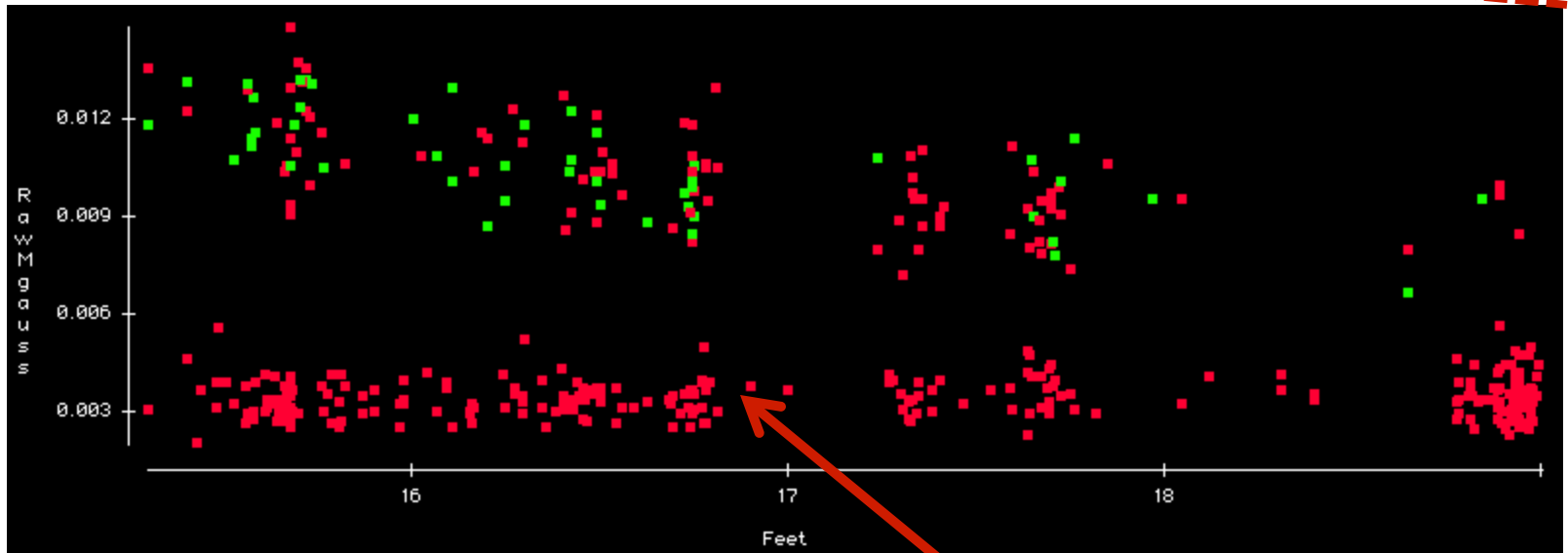
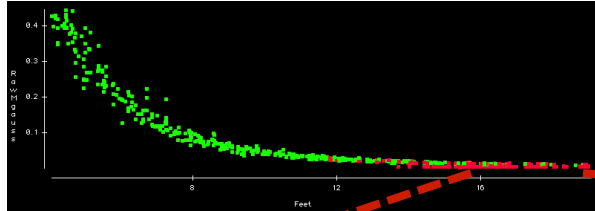
Tag
23



12.5 Feet (25 volume feet)

RuBee

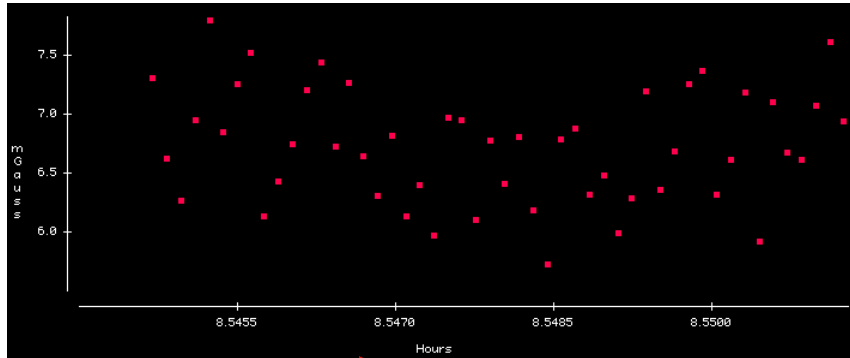
Tag Range Limited by Constant Deep Space Noise



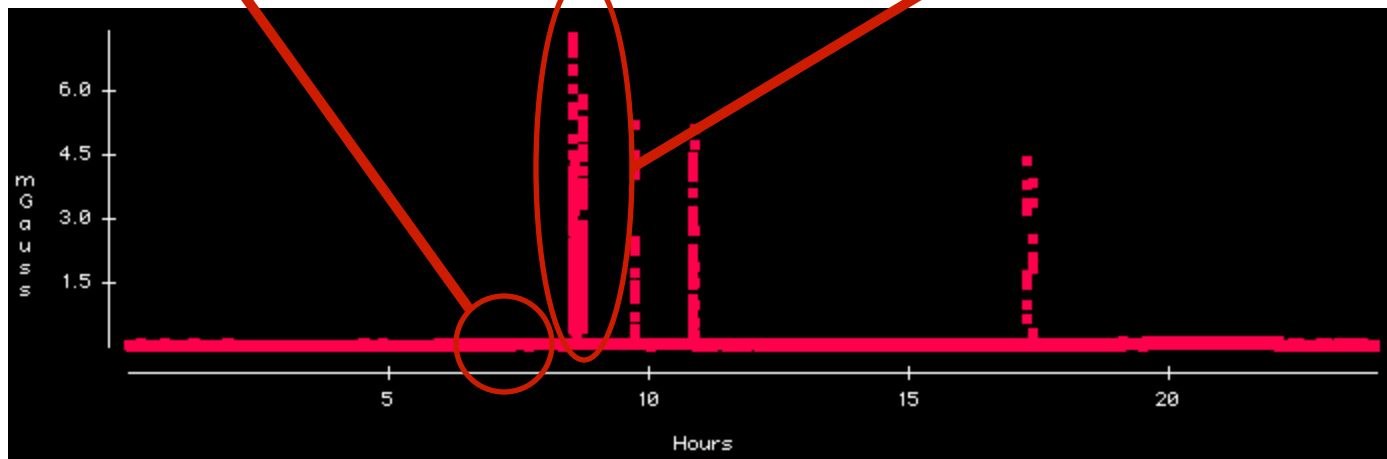
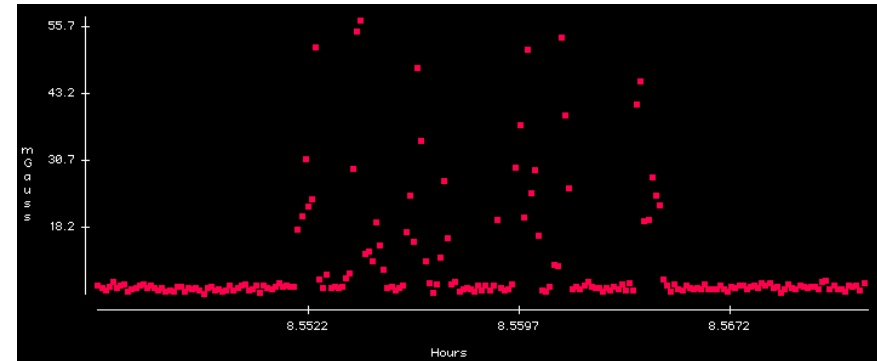
**0.06 to 0.006 mGauss
Deep space background noise**

24 hours/day, 7 days/week Deep Space Noise

Deep Space

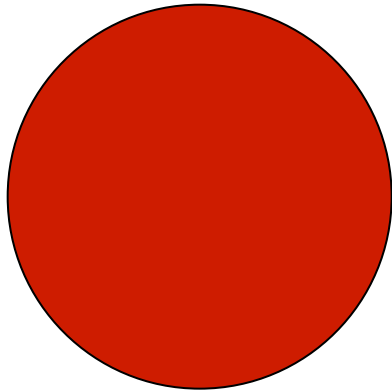


Local Transient Spikes (Lightening)



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

Small t-Tags Cell Phones



Large t-Tags For Heavy Steel

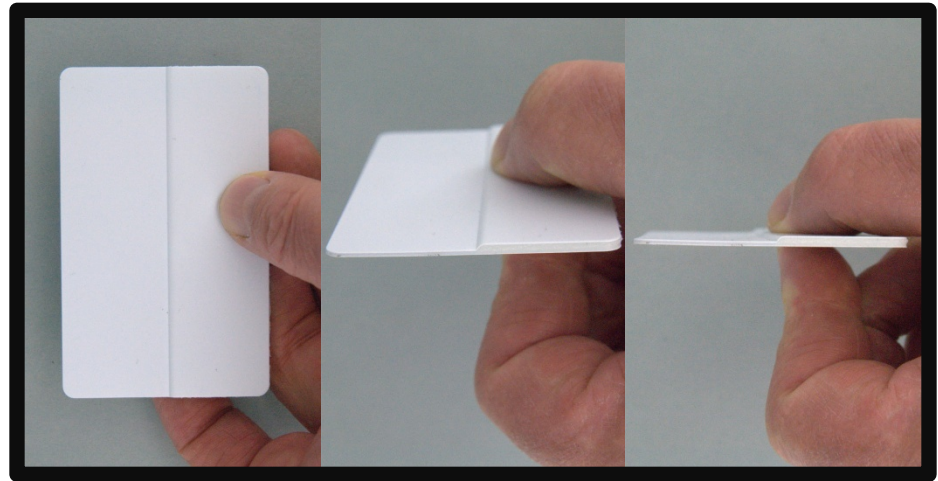


The RuBee Tags

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



Tag IP	11.11.11.00
Tag Subnet	11.11.11.1
MAC:	77-AC-D8-9A-99-AC
Object Name	Hip 23678
Size	23mm x 18mm
Birthdate	11/23/2004
Expirydate	11/2007
Serial Number	6778895
Lot Number	7878789905
Manf. Site	Ireland
Manufacture	Medco
CRC	34567

RuBee Security

Data is Stored in SRAM Memory



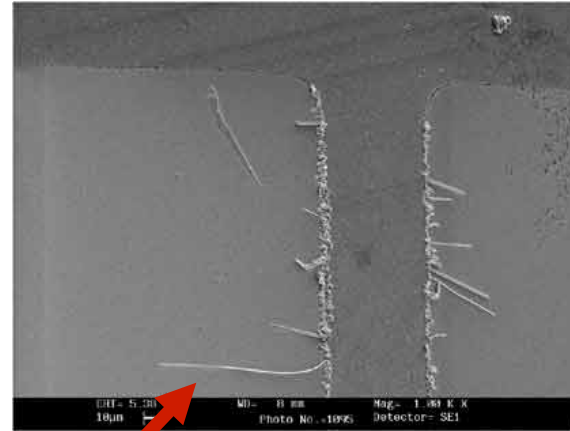
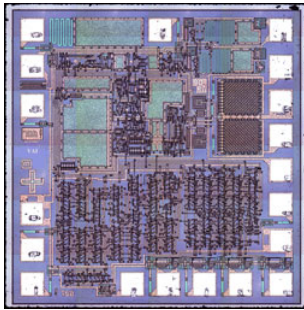
Memory map v. 07D

Lo Hi	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	Buffer															
1	32 bit ID								32 bit master ID							
2	32 bit group ID															
3	Current Temp.				Highest Temp.				Lowest Temp.				Read temp. cntr		Page Reg.	MSI 75 Cnt
4	32 bit clock counter								Temp mask	Red LED Counter	DSP pointer	Version	ID mask	Group Mask		Status flags
5	Preset LED timer				Read Temp. Time		Temp. Offset		LED masks		Grn LED counter			Red LED counter		
6	Red Line				Blue Line				Red Line Counter		Blue line Counter		Last RAM address			
7	Stack															
8	RAM															
9	RAM															
A	Display data RAM reserved for Temperature only, not shown in V05															
B	Display data RAM, scrollable from B0h to C0h, default page, set MSB to scroll															
C	Display data RAM, scrollable from C0h to D0h															
D	Display data RAM, scrollable from D0h to E0h															
E	Display data RAM, scrollable from E0h to F0h															
F	Display data RAM, scrollable from F0h to B0h															

Several key items are stored in memory.
The tags IP address, master ID, subnet (group) asset data.

RuBee Security

Safe SRAM Data Storage

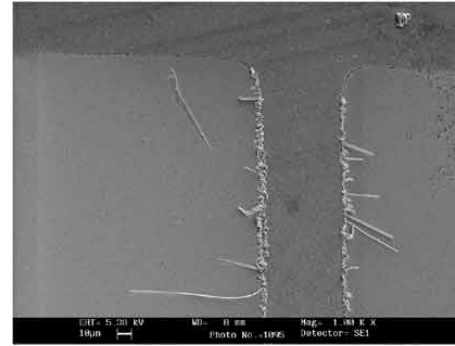
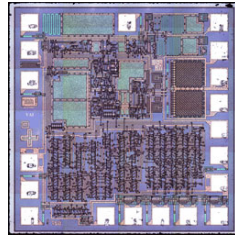


Bit swapping removes

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

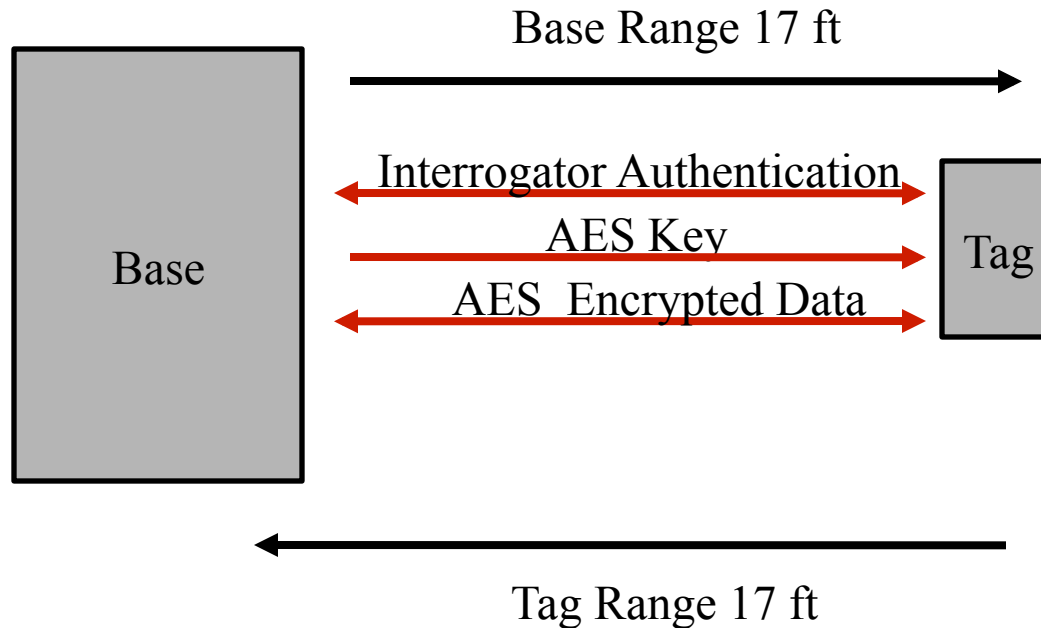
Safe SRAM Data Storage



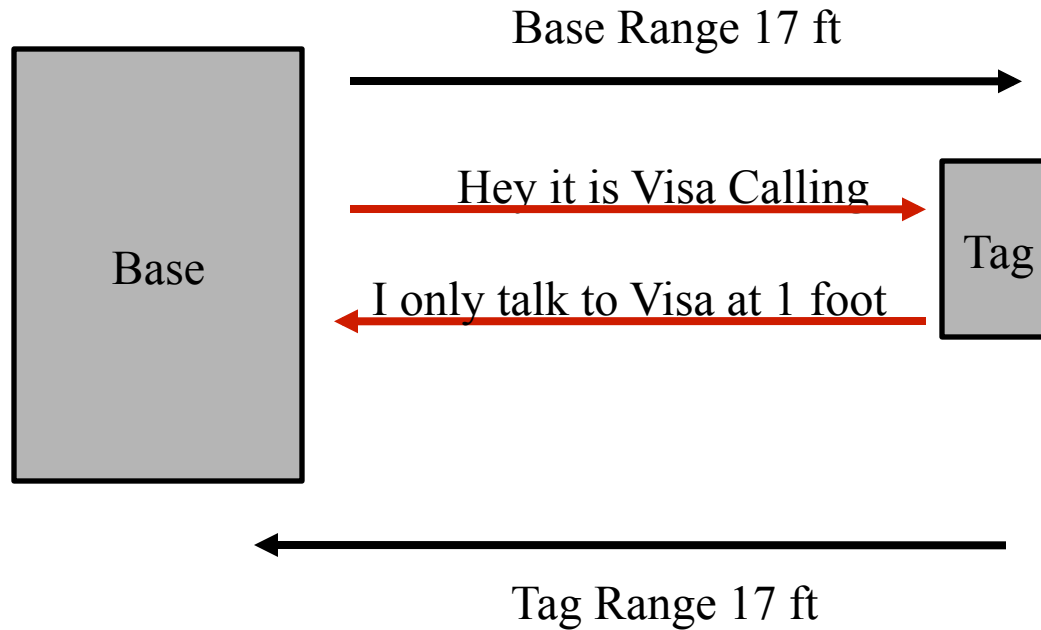
“A RuBee Tag’s hardware can be reversed engineered (same as any electronic device), but critical tag content remains secure, minimizing clone-ability risk”

RuBee Tags can use Real-Time AES Encryption Similar to TLS protocol.

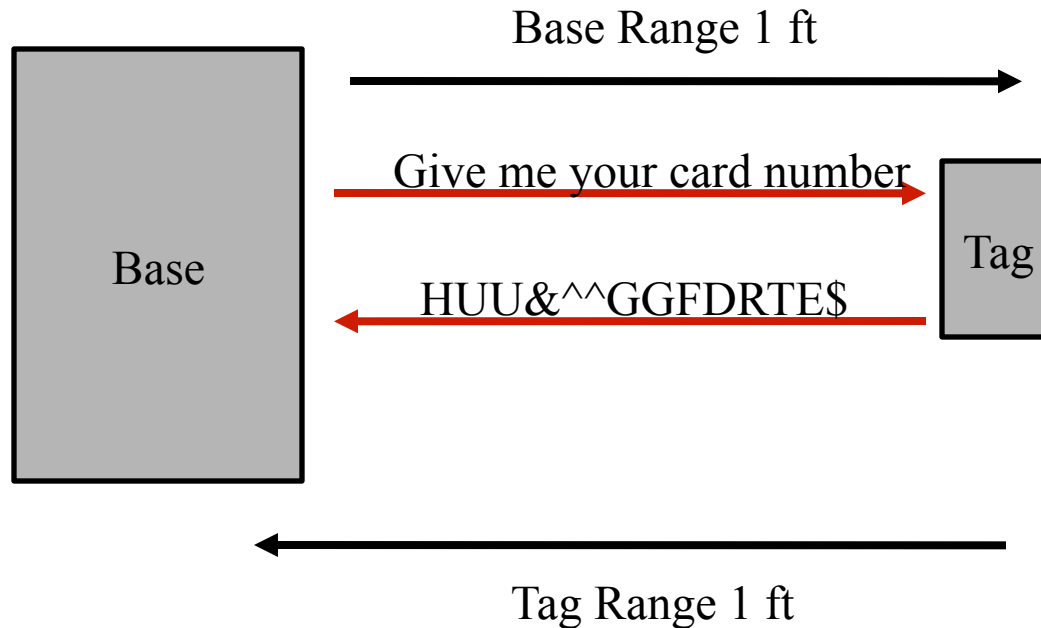
We have strong packet layer authentication security.



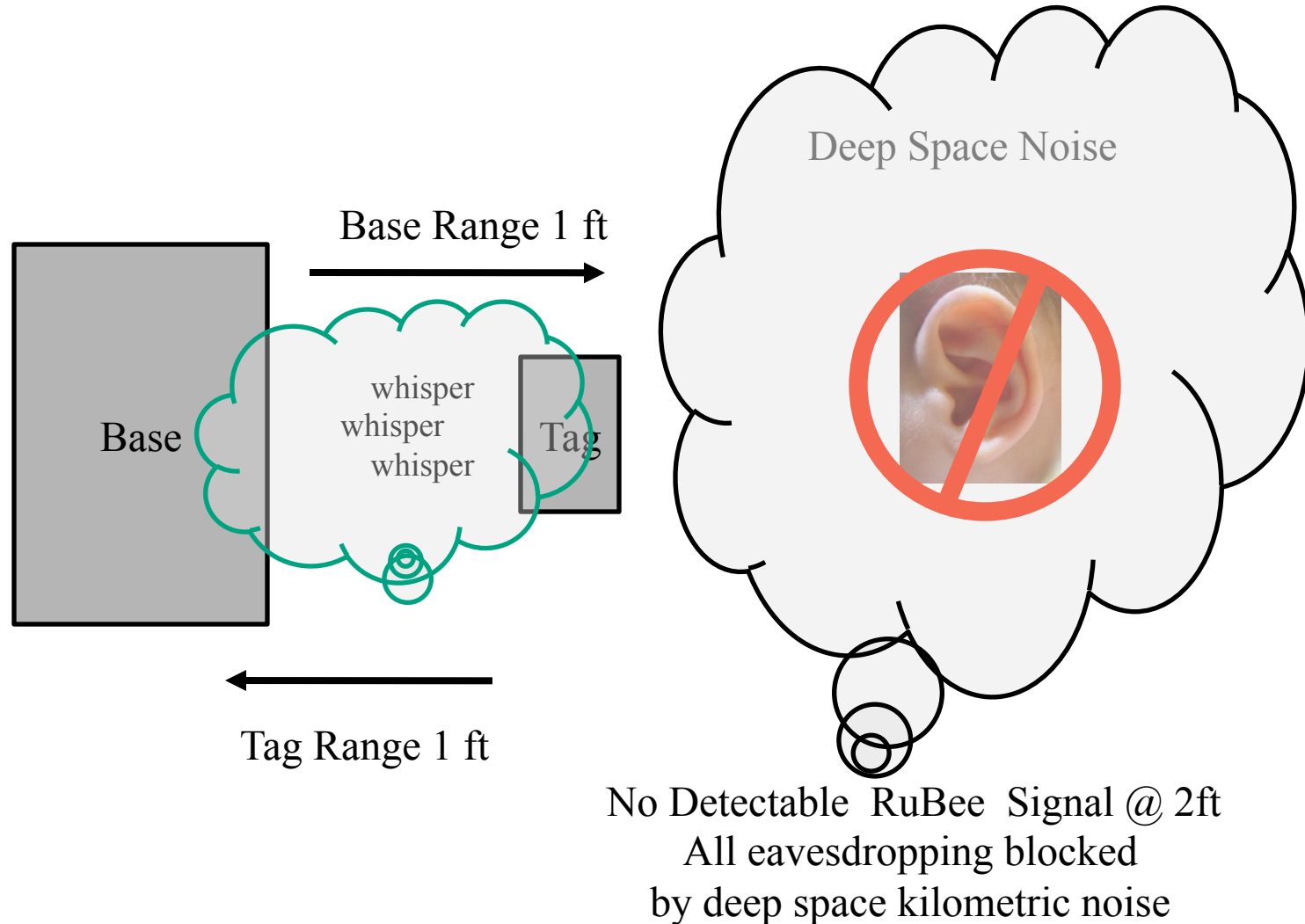
RuBee Tags can use Real-Time AES Encryption



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

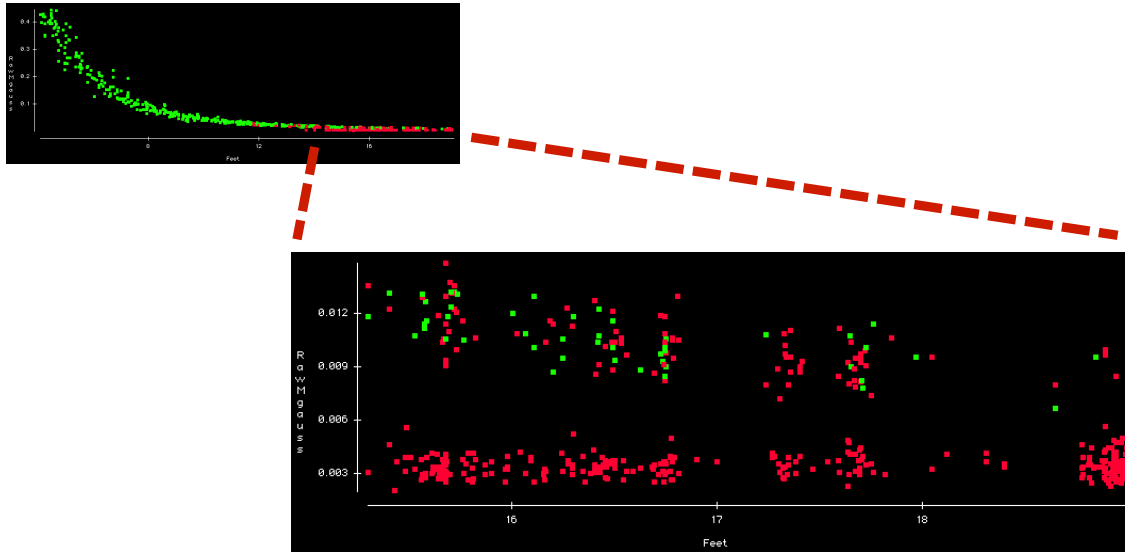


RuBee Real-Time Range Management Makes eavesdropping impossible



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



Tag IP	11.11.11.00
Tag Subnet	11.11.11.1
MAC:	Locked
Object Name	Hip 23678
Size	23mm x 18mm
Birthdate	Encrypted
Expirydate	11/2007
Serial Number	6778895
Lot Number	<u>7878789905</u>
Manf. Site	Ireland
Manufacture	Medco
CRC	34567

RuBee Packet Security

Selective Optional Encrypted Security with Keys

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



←	kapn	←	John
→	Jsg h	→	John
→	Agtd	→	John
→	Htua	→	John

Because RuBee tags have a clock they can optionally use single Keys or OTP

RuBee Packet Security

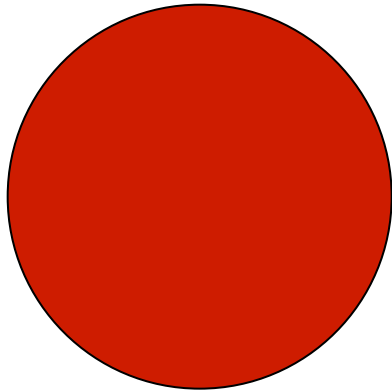
Selective Optional Encrypted Security with Keys



“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 OPAL - One Time Pads that are uncrackable”

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”***

***RuBee has Redefined
Wireless Security***

Thanks for your time