



BlackHat®

USA • EUROPE • ASIA

digital self defense

Passive RFID Security

Kevin Mahaffey, Flexilis
July 2005

If you know the enemy and know yourself, you need not fear the result of a hundred battles.

If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.

If you know neither the enemy nor yourself, you will succumb in every battle.

-Sun Tzu, *The Art of War: Attack by Stratagem*, Lionel Giles trans.

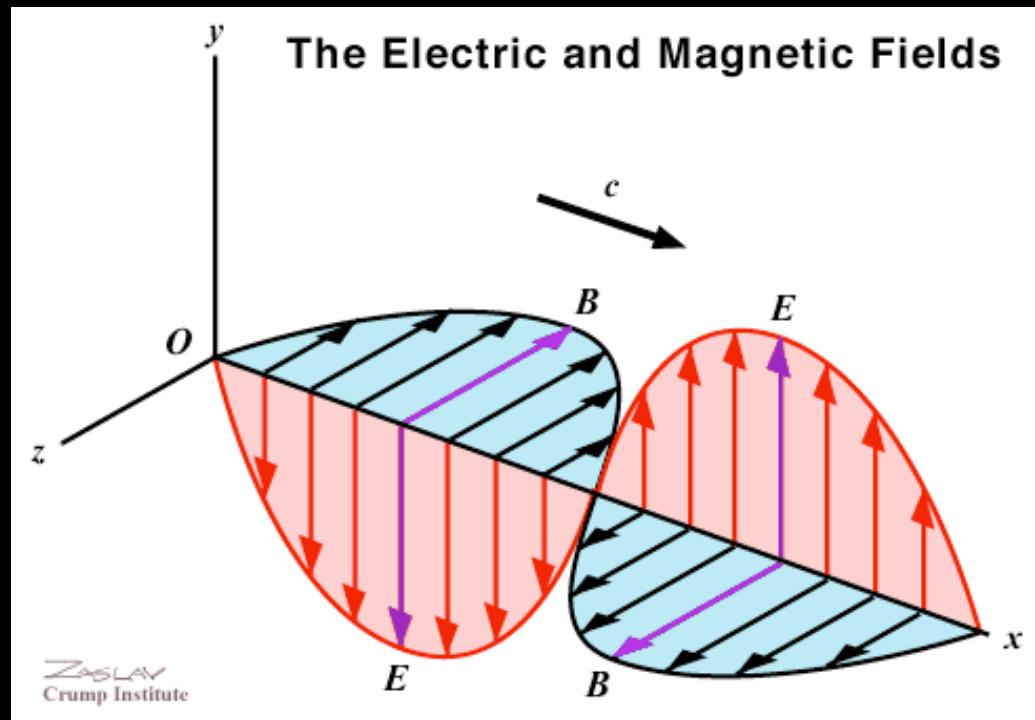
Physics/Technology

- Inductive Coupling

- Magnetic Field

- Capacitative Coupling

- Electric Field



Inductive Coupling (Magnetic Field)

- 13.56 MHz, 134.2 KHz RFID use near field coupling
 - In the near field, the signal is basically an alternating magnetic field
- Near field power received drops as r^{-6} , relatively safe with regards to direct over the air sniffing.
 - DHS has reported ~10 feet max range in sniffing HF RFID.
 - Possible disturbances in far-field radiation due to near-field modulation: may be possible to sniff HF RFID from far away.
- Inductive coupling is like a free-air transformer, with the tag's contribution to the mutual inductance being varied in order to transmit data back to the reader.

Inductive Critical Range

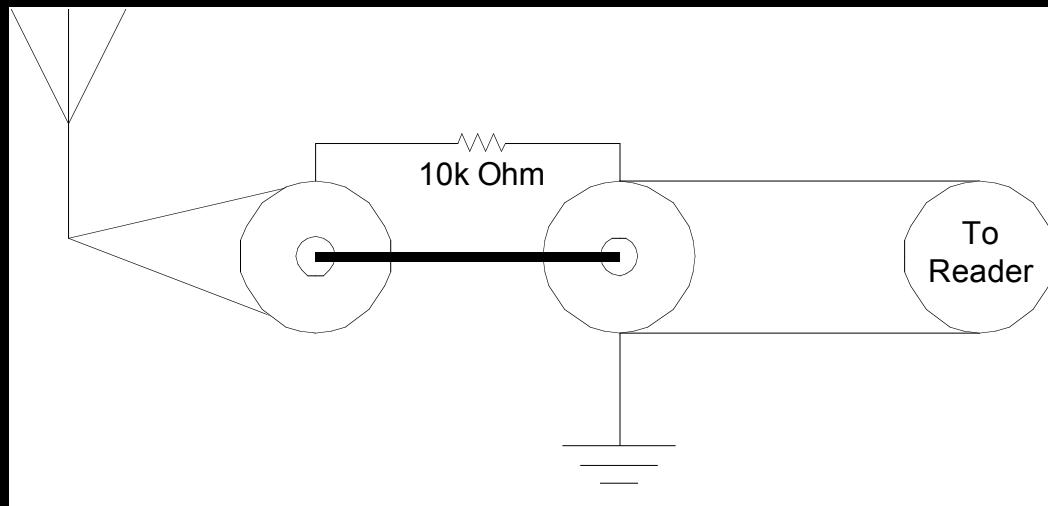
- The range of a given inductive RFID system is relative to its ability to propagate magnetic field lines to the tag.
 - There are many clever techniques for changing magnetic field patterns such as antenna size, antenna composition, etc.
- Power is important, but antenna design/implementation are more so.
- There are physical limits to range gained by feats of engineering and massive amounts of power.
- View the magnetic field lines as conservative, oscillating back and forth to the maximum distance of the near field.
 - At a given frequency of oscillation, the further the field lines travel in a given period, the faster they have to travel. Thus, the maximum theoretical range of the near field alternating magnetic field is limited by the speed of light.
 - Unless we can utilize tachyons, 3×10^8 m/sec is the fastest anything in the universe can travel.
- For our purposes, the near field ends at $\lambda/2\pi = 3.5$ meters at 13.56 MHz.
 - When coupled with the minimum power needed to energize a tag, the effective range of HF RFID becomes much shorter under realistic power limitations.

Capacitative Coupling (Electric Field)

- ~900 MHz or 2.4 GHz
 - 900 MHz is not precise because of regulatory limitations
- Power drops as r^{-2}
- The tag transfers data through “backscatter,” altering its radar cross section to modulate a signal.
- Realistic range limiting factor is not SNR at demodulation circuitry, but power supplied to the tag.
 - With a larger SNR than required, sniffing can take place further than the maximum read range.

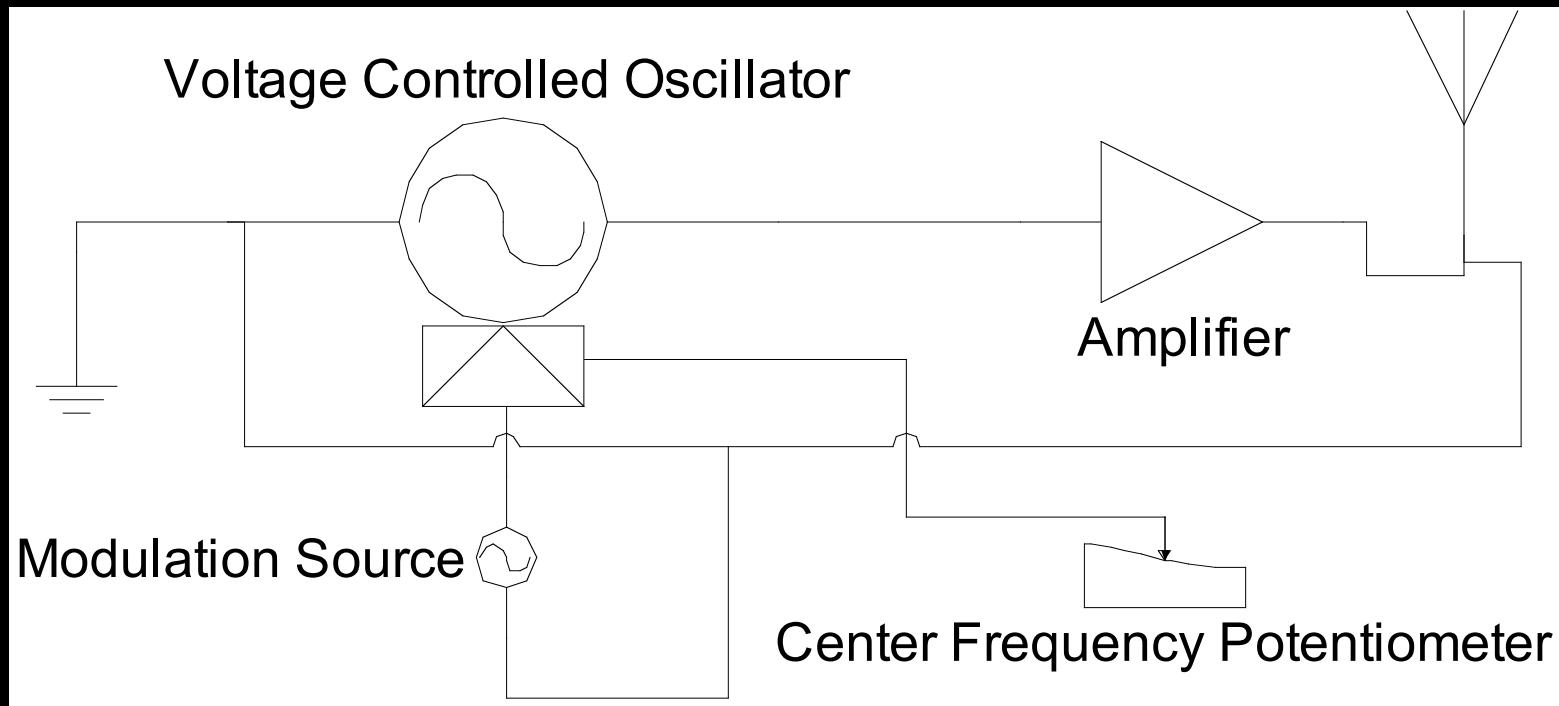
Long Range UHF RFID

- Long Range UHF RFID demonstration
 - High Gain, Directional Antennae for both Tx and Rx
 - Radiative Impedance Matching
 - DC Impedance Matching dependant on antenna detection method
- Tx antenna retrofit for this demo



UHF RFID DoS

- UHF RFID DoS demonstration
 - Continuous Wave, Frequency Modulation 7000Hz
 - This system uses FSK, so we can hit the center freq, or either of the subcarriers to disrupt proper reading.



Privacy and Security

- Differentiate privacy and security:
 - Neither are mutually inclusive nor mutually exclusive, but individually determined by the specific protocol/implementation.
- Privacy centers upon the ability for any rogue device to read unique session-invariant data from a tag, regardless of meaningfulness of that data.
 - Many secure systems are not private; however, many private systems are secure because they implement some form of access control.
- Standards provide a framework to create security and privacy.
- RFID is neither categorically secure nor insecure. It is highly implementation dependant.
 - Most RFID standards provide room for interpretation because of the varying demands of the technology. There is no turnkey solution. One vendor's system may be more secure than another.
- Security is a factor of authoritative identification
 - None, Passkeys, Symmetric Key, Public Key
- Transport-Over the Air Encryption to prevent sniffing
 - Range is determined by physics/frequency, is basically protocol-invariant and can be a baseline access control mechanism

Authoritative Identification

- Authoritative tag identification is perhaps the most important factor in RFID security
- Privacy is an issue if any unique invariant information is publicly readable.
- If invariant data is used for tag identification, the tag needs to establish reader authority to prevent the possibility of skimming and tag cloning.
 - If tags can be cloned, a tag's identification is not authoritative and security is compromised.
- Next, We're going to analyze authority establishment mechanisms in the context of RFID then apply them to specific implementations.

Authority: No Authentication

- Typically implemented on read only tags which have an ID and/or a userdata payload.
- No privacy consideration: tag data is uniquely linked to the tag and can serve as a tracking tool.
- Vulnerable to Skimming/Cloning: any appropriate reader can dump (and replicate) tag data.
 - Tag id/userdata determines tag identity, but not authoritatively due to the possibility of tag cloning.
- No reader authority assertion.
- No over the air encryption.

EPC Non-Authenticating (Gen 1 Class 0)

- Big Endian communications interface
- Stored data: EPC code 96-bit (variable), Kill Code 24-bit, User Data n-bit
- Very easy to clone because the only identification data is public.
- Meaningful data is usually carried on the tag->reader channel which is much lower power than reader-> tag.
 - Harder to sniff traffic on the tag->reader channel because lower power transmission does not propagate as far.

Gen 1 Class 0 Spec vs. Implementation

- Spec is somewhat ambiguous and leaves many security decisions up to manufacturers
 - EPC Gen 1 took proprietary standards from Matrics (now Symbol) and Alien Technology to form Class 0 and Class 1, respectively.
- EPC spec documents have some reference to security, but very little.
- "Telling secrets in a noisy room."
- Kill codes are transmitted on the high-power reader->tag channel
 - Transmitted verbatim over the air
- No rate-limiting for kill codes, and are manufacturer coded for class 0 tags.
 - 1/0 Acknowledgement of successful code. 24-bit binary brute force: 16.7 million combinations.

Gen 1 Class 0 Implementation

- Safe implementations of kill coding require on-line readers and tag-specific passkeys.
 - Problems if non-trusted devices/vendors or off-line readers need to access to kill codes.
- Retailer using kill codes to protect privacy of customers upon checkout.
 - Killcode databasing adds cost and time to checkout.
 - Possible single killcode for entire RFID deployment.
 - Simple id->killcode algorithm.

Authority: Passkeys

- Privacy is a problem if there is no access control to any unique data stored on the tag.
- Typically implemented on R and RW tags to limit access to specific portions of memory and allow access to specific commands.
- The level of authoritative tag identification depends on what factor is used for tag identification. If only a public tag id is used for identification, this mechanism is as insecure as unauthenticated tags.
 - Ideally, systems should use private userdata on the tag in conjunction with a public tag id to establish tag authority.
- Safe implementations of Passkey authentication require on-line readers and tag-specific passkeys.
 - This presents problems if non-trusted devices/vendors or off-line readers need to access protected tag data/functions.
- No data encryption, although sometimes protocol-dependant passkey obfuscation.

EPC Gen 2 Passkey Support

- 4 Memory Banks: EPC, TID, Reserved, User
- TID contains tag specifications
 - 0x00-0x07 ISO 15963 Identifier (Standard)
 - 0x08-0x13 Tag Capability Identifier (Assigned by EPC)
 - 0x14-0x1F Tag Model Number (Assigned by manufacturer)
- EPC contains the EPC tag id code (should be tag unique) and protocol level controls
 - 0x00-0x0F CRC-16
 - 0x10-0x1F Protocol Controls
 - 0x20-... EPC Tag id
- Reserved contains access and kill passwords
 - 0x00-0x1F Kill Password
 - 0x20-0x3F Access Password
- Multi-factor authentication can help prevent “superficial” cloning done by regular (read: non-L33T) users.
 - Store tag specifications (TID data) as an identification parameter

(EPC Gen 2 > Gen 1) && (Gen 2 <= Secure)

- Tags are referenced by 16-bit pseudo-random handles generated during interrogation.
- Passkeys are 32-bit (P_0 - P_{31}). Current handle is designated as H0.
 - Reader sends (P_0 - P_{15}) XOR (H0) to tag.
 - Tag generates new 16-bit pseudo-random H1, sends to reader.
 - Reader sends (P_{16} - P_{31}) XOR (H1) to tag.
 - Tag confirms authentication, reader uses H1 as handle to communicate with Tag.
- Passkey transport not plain text, but the handles are transmitted in plain text on the reader->tag channel on initial tag interrogation (for H0) and for subsequent transactions (for H1).
 - Reader-> tag channel more powerful, more conducive to sniffing.
- Memory can be written to without a passcode if it is not locked, but, if locked requires a passcode.
- In order to change lock status, a passcode is always required. Also, lock status can be locked (makes a read only tag).
 - Many users will simply lock their tags, but not lock-lock them, creating a vulnerability if weak passcodes are used.
- The gen 2 spec recommends, but does not require, that kill/access codes be tag unique (would require an online reader population).

Authority: Symmetric Key

- Privacy is a problem if there is unique invariant data available to readers without any sort of authoritative reader requirement.
- Symmetric Key Encryption relies on a "shared secret" between the tag and the reader so that tag authority can be established to the reader.
- If a Challenge-Response system is used, a correct tag response to the reader's challenge ensures tag authority.
- Like a passkey, safe implementation requires on-line readers with tag-specific passkeys.
 - Similar problems to passkey if non-trusted devices/vendors need to read tag data/functions.
- Transport data is encrypted, but may be analyzed to determine shared secret.
- Weak algorithms lead to weak authority.

Texas Instruments DST

- ❑ Implements a 40-bit iterative cipher on a shared secret key to authenticate its user id.
- ❑ Has a publicly available unique id.
 - ❑ No privacy consideration
- ❑ Challenge response symmetric key architecture.
- ❑ Weak, proprietary algorithm invented in the early 1990s.
- ❑ Using pre-selected challenges can ascertain the key via brute force or via Time-Memory tradeoff table within minutes (offline attack).

Authority: Public Key

- ❑ Privacy is a problem if the tag issues unique invariant information to any reader.
- ❑ Tag validates reader's public key (using pre-stored criteria) and encrypts data with that reader's public key.
- ❑ Very sniff-safe.
- ❑ Does not require on-line readers. Encrypted data.
- ❑ Very highly authoritative, but expensive often using proprietary hardware.

Hong Kong Octopus Card - Sony FeliCa

- Huge distributed payment card: taxis, busses, restaurants, subways, apartment complex access, etc.
- Readers can be offline
 - Utilizing a store and forward mechanism that validates small transactions using PKI, but does not perform an exact balance check until synced with an online system.
- Other readers have offline authentication using PKI and online balance check.
- Eliminate the need to share secret keys or have database access between all system devices.

Practicality

- Tag cost, size, power requirements inversely proportional to better security and privacy.
- "Security does not exist in a vacuum"
 - Applications only implement adequate, rather than ideal security.
- Possibility vs. Feasibility: simply because the equipment is expensive today doesn't mean that it will continue to be out of reach tomorrow.
 - Don't make security decisions based on data obscurity.

Workarounds

- Workarounds do not make the protocol itself more secure, but can maximize the security of a given application.
- Dynamic Recoding
 - Each tag read rewrites part of a tag's user data. Requires online readers to detect if cloning has occurred.
- RFID Odometer
 - Performed by the tag manufacturer, incredibly effective fraud mitigation.
- Passkey protected validation data.
 - Easy implementation in production tags.
 - Does not increase privacy, but does increase security significantly if used with online readers and variable passkeys.

Vulnerabilities: Tree Trimming

- Exploits the tree-walking protocol to ascertain unique ids of a tag population for tags that use preset, unique identifiers to singulate tags.
 - Ineffective against EPC gen. 2 which uses ALOHA singulation, a random time interval instead of tree-walking to singulate tags.
- EPC gen 1 class 0 has multiple singulation criteria: the reader decides which to use.
 - epc code + crc16
 - semi-static identifier
 - pseudo random number generated on demand
- The spec recommends that readers use of the semi-static identifier
 - 64 bits of data + 16 parity bits generated from the epc's crc16 data or stored by the tag manufacturer (manufacturer's choice).
 - This never changes if manufacturer coded or, if based on crc16, changes only when the tag's epc changes.
- 2 of the 3 singulation criteria contain unique data that can link reader broadcasting to a specific tag.
- The reader chooses which to use (often hard coded by the reader manufacturer), creating an implementation dependant security issue.

Skimming and Cloning

- Skimming
 - Surreptitiously reading tags
- Cloning
 - Class 0 tags considered manufacturer unique and have no protection against counterfeiting.
- Generation 2 EPC tags have several manufacturer and user fields that can be used for multi-factor identification.

Sniffing

- ❑ Capacitatively coupled RFID tags more vulnerable than inductively coupled tags because of signal propagation range.
- ❑ Tag to reader channel is much harder to sniff than reader to tag due to the substantially higher power on the tag to reader channel.
- ❑ Obfuscation is better than plain text, but not by much, so don't trust it.

"Real Time Reader Emulation"

- Bypass high-security tags in an access-control application.
- One reader emulator (R_E) and one tag emulator (T_E) linked via a backhaul.
- The legitimate tag (T_R) needs to be within range of the reader emulator and the tag emulator within range of the legitimate infrastructure reader (R_R).
 - T_E records the modulations from R_R as an arbitrary waveform and sends them via the backhaul to R_E .
 - R_E transmits the sniffed modulations to T_R and listens for a response and records it as an arbitrary waveform.
 - T_E transmits the recorded tag response to R_R .
 - Repeat cycle until a full exchange has taken place in the frame of reference of R_R .
- Nobody likes to bruteforce.
 - "The rule is, not to besiege walled cities if it can possibly be avoided."
-Sun Tzu, *The Art of War: Attack by Stratagem*

Implementation: Industry

- RFID deployment is driven by various industries.
 - Greatly pushes adoption, but causes fragmented standards and wildly different implementations.
 - Most RFID integrators have weeks of experience according to recent industry studies. Many don't have any infosec or engineering training.
- Integrators and manufacturers determine what is implemented, not a standard.
- Future Problems
 - Buggy tag implementations could lead to local privilege escalation
 - Undocumented diagnostic functions on tags
 - No way to update tags because of hard wired ICs.

RFID Passports

- 13.56 MHz
- Passport will contain PKI encrypted data for verification.
- ICAO (U.N. air transportation governing organization) has a large list of security mechanisms that are optional.
- The baseline implementation has no access control mechanism and will allow anyone to uniquely identify individual passports.
 - Also allows skimming and cloning.

Passport BAC

- Basic Access Control (BAC) is likely going to be the highest security implemented in U.S. passports.
- Requires an optical scan of a passport to read data physically printed on the cover.
- The cover data is hashed and used to authoritatively identify the reader and establish an encrypted session.
- The set of data to be hashed is constant for the life of the passport, thus, if someone reads the passport data once, they will be able to read it forever.
- Lack of entropy in hashed data set: birth date, passport expiration date, passport number, and several check digits.
 - According to a recent article published by the International Association for Cryptologic Research, there are only 52 bits of entropy in the 64 bit BAC access key.
- Passive sniffing of a BAC exchange would give a challenge response pair that would allow an offline brute force attack and give the attacker the passport number, birth date, and passport expiration date.

Other Passport Vulnerabilities

- Depending on how the actual tags are manufactured, the passport may be vulnerable to a “tree-trimming” attack if they do not implement silent tree-walking or ALOHA in their anti-collision system.
- Even if you can't read data from a passport, you can tell if someone is carrying a passport from ~2 ft under reasonable constraints.

Passport Physical Security: Eddy Currents, Ferrite, and Tinfoil Hats, Oh My!

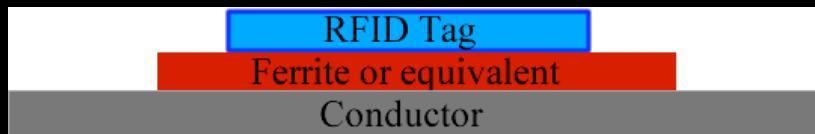
- With Capacitive RFID (EPC 900 MHz, etc.), preventing a transponder from transmitting would be as simple as surrounding it with a conducting surface or conducting mesh with holes much smaller than the wavelength.
 - Conductive materials, when surrounding an object, create a “faraday cage,” effectively stopping any part of the electric field from powering up the given transponder.
- Inductive RFID (13.56 MHz), the kind used in passports, uses a magnetic field to power itself, not the electric field.
- A static (DC) magnetic field is unaffected by a conductor (specifically in the binding of the passport).
- As the alternation frequency of the magnetic field increases, eddy currents form in the conductor, creating local opposing magnetic fields to the global magnetic field, effectively canceling the net field seen by the tag.
 - This is the same phenomenon that makes generators work: any conductor opposes a change in magnetic flux by creating a current that induces a flux opposite the direction of change.
- It's easy to create conductor around a RFID transponder to render it useless, but much more difficult to make it work only when read from a specific direction.

Flux Pipes

- We have developed a configuration that allows single direction reading of an open passport and chip isolation for a closed passport.
 - Partially open passports will nominally allow reading, but not realistically due to the magnetic flux seen by the tag at any given time being proportional to $\sin(\theta)$ on the interval $0-\pi/2$ where θ is the angle of the passport opening.
- We need to mitigate the eddy currents in the conductor, but cannot elevate the RFID chip substantially using dielectric separation.
- Essentially we need a “flux pipe” to allow field lines to pass through the RFID transponder’s inductor, but not enter the conductor and create eddy currents.
 - We cannot use normal metals to do this because they would generate their own eddy currents.
 - We need a flexible material that has an extremely high resistivity as well as a high magnetic permeability.

Ferrite!

- Ferrite powder is perfect and is widely used in producing magnetic tapes (VHS, audio, etc.) and can be layered under the RFID transponder in manufacturing or by using a prefabricated label design.
- This system can also be used to protect library RFID systems from abuse by requiring the medium being scanned to be in an open state to be read.
- Below-left is a manufactured passport inlay that provides integral protection.
- Below-right is a retrofit inlay to create an access control system in any opening and closing medium (i.e. library books)



Panel Discussion

- Mark McGovern, Security Lead, In-Q-Tel
- Paul Simmonds, CSO, ICI
- Jon Callas, CTO, PGP Corp.