Is NFC a Better Option Instead of EPC Gen-2 in Safe Medication of Inpatients

Mehmet H. ÖZCANHAN,
Gökhan DALKILIÇ,
Semih UKTU

Dokuz Eylul University
Department of Computer Engineering

Outline

- Medication Error
- Types of Medication Error
- Related Work
- Case Study I (Yen's Proposal)
- Case Study II (Wu Scheme)
- Suitable Technology for Patient Safety: NFC
- Conclusion

Medication Error

A MEDICATION ERROR is defined as the administering of a wrong medicine or dosage to a patient that ends up harming the patient [4, 5].

Adverse Drug Events (ADEs): An ADE is the next broadest term. It refers to any injury caused by a medicine. An ADE refers to all ADRs, including allergic or idiosyncratic reactions, as well as medication errors that result in harm to a patient.

Medication errors can occur anywhere

Prescribing

Repackaging

Dispensing

Administration

Monitoring

Types of Medication Error

Prescribing Error

Incorrect drug selection (based on indications, contraindications, known allergies, existing medication therapy, and other factors), dose, dosage form, quantity, route, concentration, rate of administration, or instructions for use of a medication product ordered or authorized by Physician

Omission Error

The failure to administer
an ordered dose to a patient
before the next scheduled dose, if any.

Types of Medication Error Cont'd

Wrong Time Error

Administration of medication outside a pre-defined time interval from its scheduled administration time.

Improper Dose Error

Administration to the patient of a dose that is greater than or less than the amount ordered by the prescriber or administration of duplicate doses to the patient.

Example: one or more dosage units in addition to those that were ordered.

Types of Medication Error Cont'd

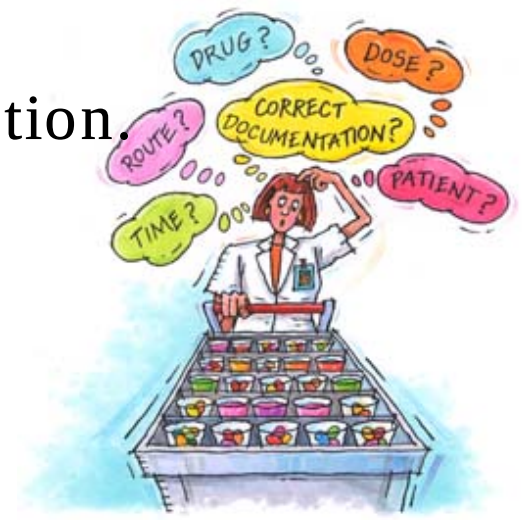
Wrong Medication - Preparation Error

Medication product incorrectly formulated or manipulated before administration.

Wrong Administration Technique Error

Inappropriate procedure or improper technique in the administration of a medication.

Example: wrong route/site or rate of administration



Recommendations to Prevent Medication Errors

- Adopt a system-oriented approach to medication error reduction such as: (time-out, & technology confirmation).

Use technology effectively such as:

- Implement Computerized Physician Order Entry (CPOE).
- Use of Automated Dispensing Cabinets.
- Use of Pharmacy Dispensing Robotics.
- Use of Barcoding/RFID/NFC in medication and patient identification.
- Implement a unit dose system.

UHF RFID Tags

- A passive UHF tag can be read from a few meters away
- Hundreds of tags can be read per second
- The ISO 18000-6 and EPC Global Class 1 Generation 2 (EPC Gen-2) standards govern the UHF tags

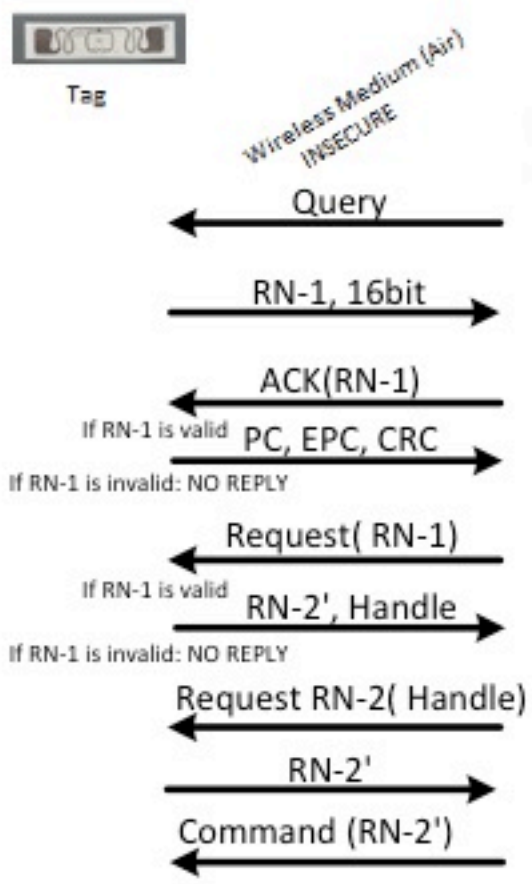
- the UHF tags contain no encryption or hashing capabilities;

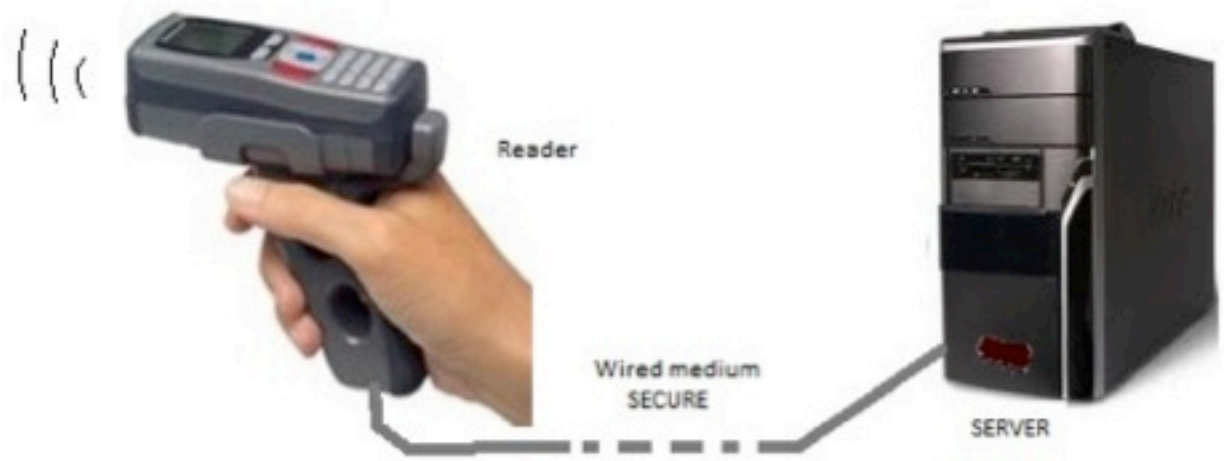
but only;

- a 16 bit pseudo random number generator (PRNG),
- a cyclic redundancy check (CRC)
- an XOR function for obscuring message exchanges.

To overcome the known weaknesses, various grouping protocols have been proposed. But, each protocol has some deficiencies.

A typical UHF RFID tag reading scenario.





The server has all the information:
personal information,
the unique identification number (ID) of the inpatient's wristband tag,
the ID of the tag on the inpatient's medicine pack and
the pre-shared secrets used for authentication

Related Work

- The origins of using RFID tags in groups for the identification of objects go back to the work of Juels et al. [8]
- One of the first proposals to use RFID tags in patient medication is by Wu et al. [11]
- Sun et al. proposed the use of RFID tags for identifying patients and barcodes for unit dose medication [12].
- A proposal where both the inpatient and the medicine are identified by low-cost RFID tags conforming to EPC Class-1 Generation-2 (EPC Gen-2) standard was made by Huang and Ku [14].

Related Work

The security problems arise because the requirement of strong mutual authentication is not obeyed

- in this study, the two recent works, analyzed
- they try to rectify previous vulnerable schemes, but fail because, they do not consider the algebraic attacks.

Our assumptions

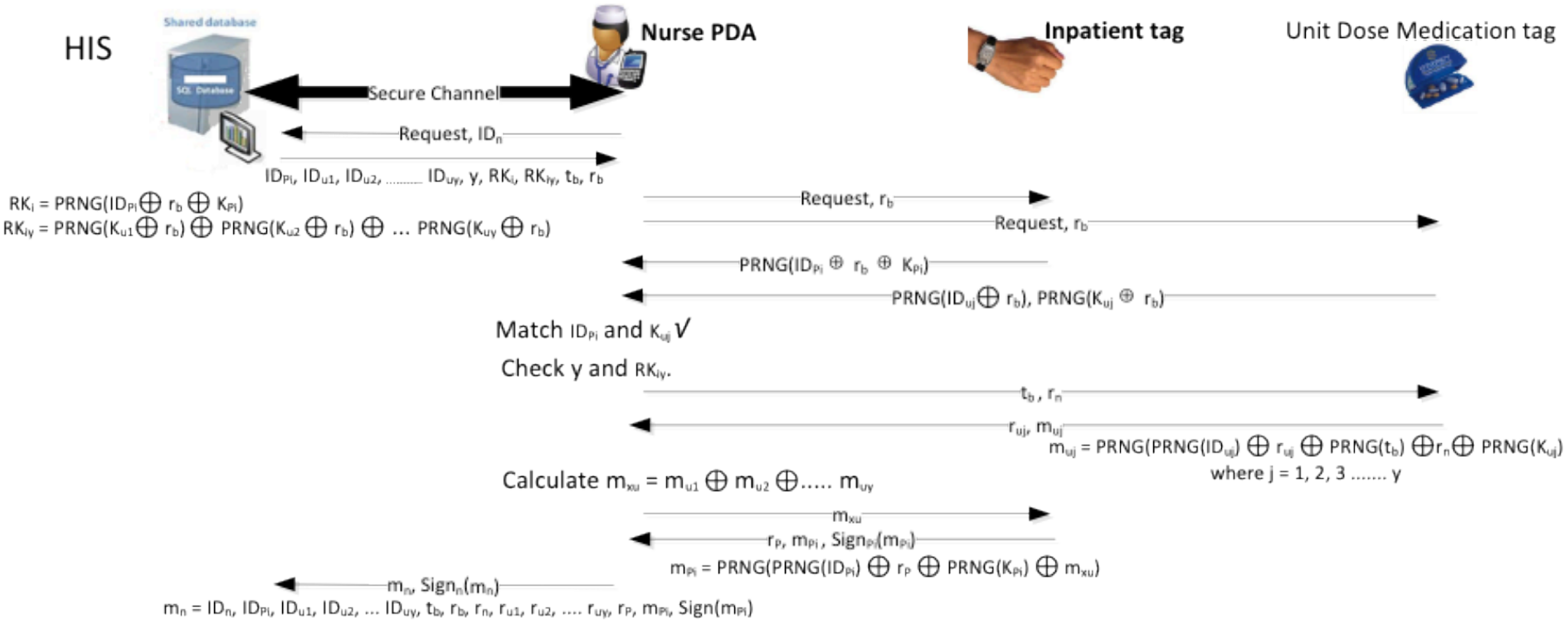
- While the reader and the server communicate over a secure channel, the tag and the reader's channel is insecure.
- The tag has limited resources but the reader has unlimited resources. Therefore, the reader is assumed to support cryptographic algorithms but the tag cannot.
- The reader is not trusted and a counterfeit reader can be used in the system.
- Our attacker can listen to the messages between the tag and the reader over the air.
- The final assumption is the attacker has only passive attack abilities.

Case Study I

- The work by Yen et al. analyses some weaknesses of a previous work [16]. The analyzed proposal is the Inpatient Safety RFID System (IS-RFID) of Peris et al. [18].

- Yen's proposed rectified scheme is shown in Figure

Yen's proposed offline scheme



in the online version, the inpatient's tag is authenticated online by the server

ID_n, ID_{Pi}	ID of a nurse and the tag ID on i^{th} inpatient wristband.
ID_{ui}	Tag ID on a unit dose medicine pack of i^{th} inpatient.
ID_{uj}	Tag ID multiple unit dose medicine packs, j=1,2 ..y.
K_{Pi}, K_{ui}	Tag key of i^{th} inpatient wristband and i^{th} inpatient's unit dose pack.
K_{uj}	Tag key of multiple unit dose medicine packs, j=1,..y.
t_b	Timestamp generated by server.
r_b, r_n, r_p, r_{uj}	Random number generated by server, nurse PDA, inpatient's tag, and j^{th} unit dose, respectively.
PRNG()	16-bit pseudo-random number generation function.
y	Number of unit doses for i^{th} inpatient.
Rk_i	Key validation value for i^{th} inpatient.
Rk_{iy}	Key validation value for i^{th} inpatient's unit doses.
e_i	Evidence generated by a nurse for i^{th} inpatient.
m_{uj}	Partial evidence generated by unit-dose tag j, j=1,2..y.
m_{Pi}	Partial evidence generated by i^{th} inpatient's tag.
m_n	Medication evidence generated by a nurse.
$Sign_n(m_n)$	Signature function of nurse, that signs evidence m_n.
$Sign_{Pi}(m_{Pi})$	Signature function of i^{th} inpatient, that signs evidence m_{Pi}.

Ambiguities of Yen's Scheme

- Neither the inpatient's tag nor the nurse PDA digital signature functions are explained.
- The assumption of inpatient's tag having the computational ability of generating digital signatures is way out of the ISO 18000-6 and UHF Gen-2 standards

A Typical Pre-calculated Table

INPUT = input	Output = PRNG(input)
0000 0000 0000 0000	0000 0010 0000 0000
0000 0000 0000 0001	0010 0110 0000 0010
....	....
1111 1111 1111 1111	0100 0111 1100 0110

Disclosure Attack Scenario on Yen's Protocol

- The 16 bit PRNG function of the Gen-2 tags is public and available [19].
- According to Yen, any PRNG(x) is calculated for a given input x;

e.g. using $(ID_{Pi} \oplus r_b \oplus K_{Pi})$ as input, a deterministic output $PRNG(ID_{Pi} \oplus r_b \oplus K_{Pi})$ is obtained and matched with R_i.

Therefore, a table of 2^{16} (65,536) possible inputs against calculated outputs can be prepared beforehand, as in Table

The rogue reader sends a request

{request, r_a } to the conveyer,

where r_a is the attacker's constant nonce.

The tag answers with $PRNG(ID_{Pi} \oplus r_a \oplus K_{Pi})$.

The output column of Table is searched to find the value of $PRNG(ID_{Pi} \oplus r_a \oplus K_{Pi})$.

When found, the corresponding *input* is read.

Thus, $input = (ID_{Pi} \oplus r_a \oplus K_{Pi})$.

If $(ID_{Pi} \oplus r_a \oplus K_{Pi})$ is an XOR operation then,

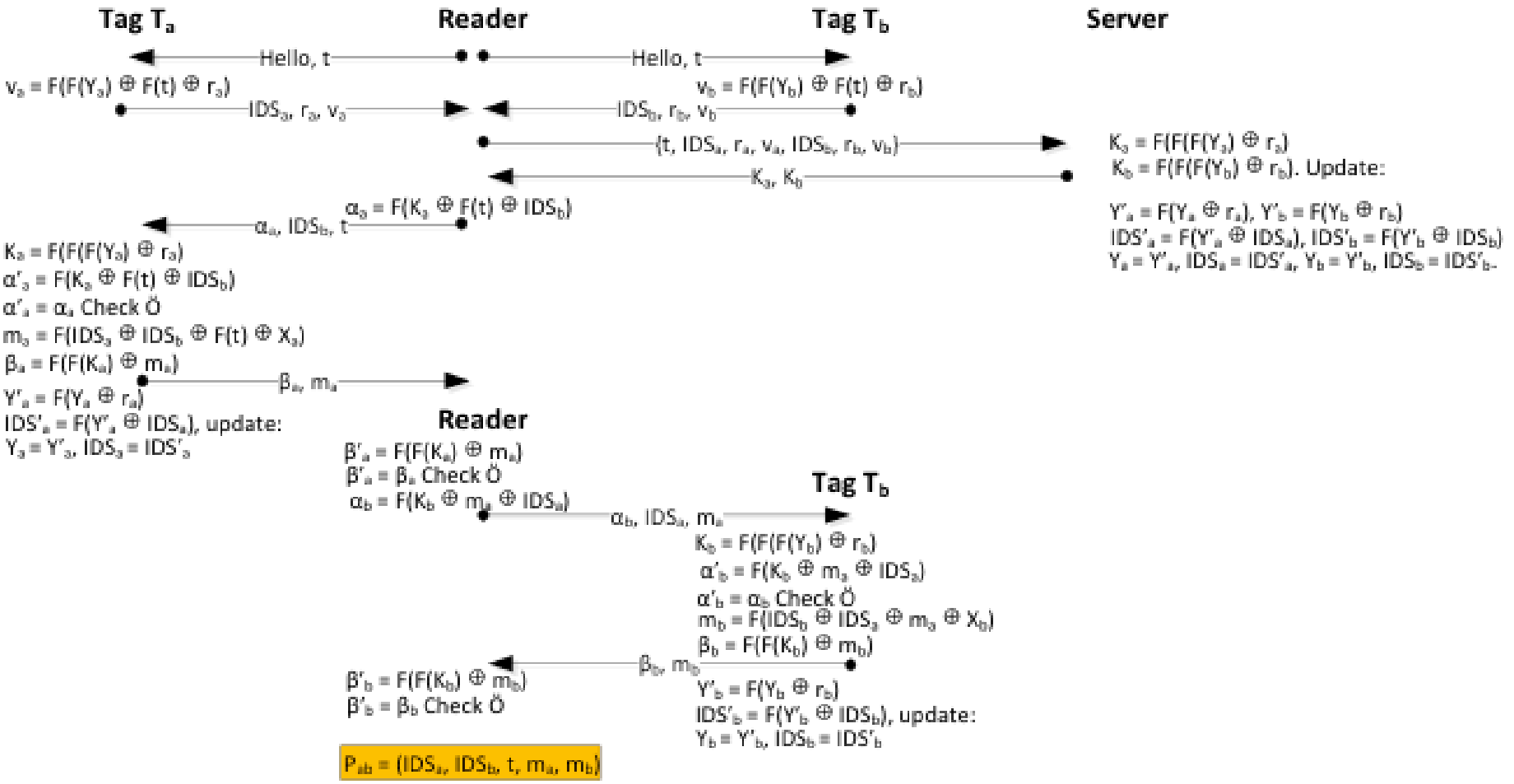
$$(ID_{Pi} \oplus K_{Pi}) = input \oplus r_a$$

with Table and XORing each $\{PRNG(ID_{uj} \oplus r_a), PRNG(K_{uj} \oplus r_a)\}$ with r_a, all values of ID_{uj} and K_{uj} are exposed,

Case Study II

- A second work uses Gen-2 RFID tags is by Wu et al. [22]
- The proposal also uses the 16-bit PRNG function of Gen-2 tags to form authenticators and prove the simultaneous existence of two tags, in the same electromagnetic field.

The scheme of work



- Wu uses a random permutation function F while calculating the authenticators and partial evidences.
- Wu claims F to be a one way function that uses only the PRNG and XOR operation available in a Gen-2 tag.

Since F is a public function, for any known input, F(x) can be calculated. Therefore, a table similar to "PRE-CALCULATED TABLE" can be prepared.

Attacks on Wu's Scheme

- Exposure Attack: The exposure attack on the protocol is similar to the attack in "Yen's Protocol". The adversary challenges the tags, with a bogus timestamp t. In the replies of tags, the IDS and nonce values are recorded, then the authenticators v_a and v_b, are analyzed.

The attacker loads the captured values into two rogue tags, switching the identities of the *target* and *conveyor*.

Attacks on Wu's Scheme

- **De-synchronization Attack**: De-synchronization happens when one of the partners of the message exchange update some shared terms to new values, while the other does not. If the old values are not stored, then there is no way for mutual authentication to take place, with mismatched values.

Computational Load of Wu's Scheme on Gen-2 tags

- Every F function involves 16 PRNG and 12 XOR operations. Hence, T_a makes 144 PRNG and 115 XOR operations.
- In total, T_a spends 27,475 (144x190+115) clock cycles in computations.
- This is around 26 times more than an 8-bit AES implementation
- Wu's proposal cannot meet the limits, as it exceeds 220 clock cycles [26].

Discussions

- The Yen's and Wu's fail to meet their goal of enhancing inpatient medication safety, because our full-disclosure attack can harm a patient.
- Work [19] reveals the general properties of the CRC function and shows how its use introduces weaknesses into a number of protocols.
- CRC or the PRNG of an EPC Gen-2 tag is not safe [13, 14, 16, 19].
- But, CRC and PRNG are the only available functions, in the EPC Gen-2 tags. For confidentiality of critical data, alternatives which contain true encryption algorithms are necessary.

Ambiguities of Yen's Proposal

- PRNG as an encryption algorithm as in PRNG($ID_{Pi} \oplus r_b \oplus K_{Pi}$) , which is not clear; because in regular EPC Gen 2 tags PRNG function doesn't have any input parameters.
- Another unexplained assumption is the digital signing ability of the tags.
- UHF tags are read in numbers from a few meters away. Thus, it is not possible to identify which inpatient's tag is read, if there are many in a room.
- If a complication occurs during the medication of a patient, the responsibility of the results of remaining medication by a second nurse is ambiguous.

Disadvantages of Yen's Proposal

- UHF technology used (Unintended inpatient tags in a room can also be read)
- A second disadvantage is dedicating a PDA for every nurse, which is neither widely available nor cheap
- unavailability of cheap UHF readers in the form of PDAs
- the lack of consideration of HL7 standard

Suitable Technology for Patient Safety: NFC

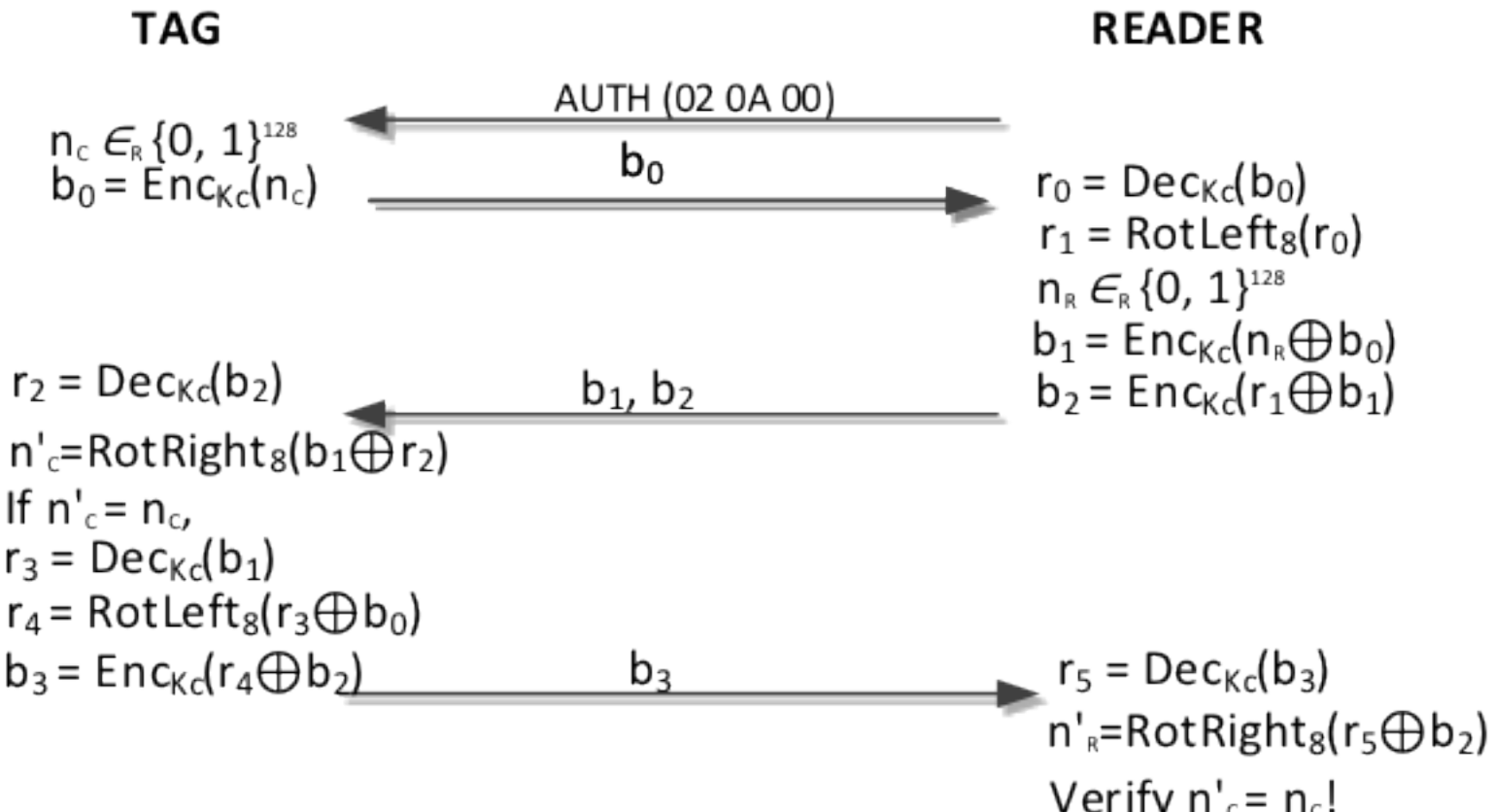
- A viable alternative technology is the near field communication (NFC) tags, because they possess the desired characteristics and cryptographic primitives.
- Mifare DesFire version EV1 (EV1) tag has a built in AES engine [29]
- Another important characteristic that would have prevented our attacks is the operating distance. EV1 is read from a distance of 20-100 mm

Comparison Of EPC Gen-2 Tage and DesFire EV1

Property		
	8000-6	ISO/IEC 14443A

DesFire EV1 Authentication

- Another important parameter of the EV1 is its 3-way mutual authentication



Conclusion

- Physical requirement removes the danger of reading a rogue tag and eavesdropping of an adversary from meters away.

- Dropping costs of alternative tag types and readers (Near Field Communication (NFC) enabled tablet (Google Nexus 7) make their initial investment increasingly compatible to UHF tags.

- Smarter tags with shorter operating distance, longer key size and better cryptographic primitives are needed.

Conclusion Cont'd

- The NFC tag prices are higher than the UHF tags, but the total cost for a complete solution is not.
- There is a need for tags with cryptographic primitives, intentional tag reading characteristics and longer key sizes. State of the art NFC tags are a viable alternative.

Conclusion Cont'd

- Bit size of PRNG can be extended to 64 or more bits to increase the search space of the unknowns given as input to the PRNG which makes creating a table and searching through the table unaffordable.
- Even more, PRNG function can be replaced by a better cryptographic function. But these extensions mean to change the EPC Gen2 standard.

Thanks for Listening

Any Questions?