

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

Mehmet Hilal Özcanhan, Gökhan Dalkılıç^(✉), and Semih Utku

Department of Computer Engineering, Dokuz Eylul University,
Izmir, Turkey

{hozcanhan, dalkilic, semih}@cs.deu.edu.tr

Abstract. Wrong medication is an important problem of the citizens of many countries. Using contemporary technologies like UHF Gen-2 RFID tags helps decreasing the medication errors, experienced by many. As UHF Gen-2 tags have limited capacity, cryptographic algorithms cannot be accommodated. The only available functions PRNG and CRC cannot be used instead of cryptographic algorithms. To overcome the known weaknesses, various grouping protocols have been proposed. But, each protocol has some deficiencies. Two of those protocols are covered in this study. Some of their common deficiencies are studied and solutions are suggested.

Keywords: Patient safety · Medication error · RFID · UHF tag · EPC Gen 2 · NFC · ISO 18000-6 · Authentication · Group proofing protocol

1 Introduction

It is reported that 78% of the participants in the Eurobarometer survey, on the perception of medical errors, have voted wrong medication as an important problem, in their country [1]. The poll indicates that 23% of the participants have been directly or indirectly affected, by a medical error. 18% reported that they experienced a serious medical error, in a hospital. This contradicts the major patient safety goal of avoiding harm caused, during medical care [2]. The need for better patient safety is stated in many works [3,4].

The medication error definition is given as errors in drug ordering, transcribing, dispensing, administering, or monitoring [2]. This work is concerned with correct drug administering of an inpatient, at the correct time; i.e. drug administration free of human errors due to patient-drug pack mismatch. Many technologies are used in hospital automation systems, from high-end servers, to personal digital assistants (PDA), tablets, automatic medicine dispensers (AMD) and recently radio frequency identification (RFID) tags. Doctors and nurses are the users of these technologies and they have tablets, which they know how to use. Some of these tablets even have an integrated tag reader. On the other hand, the patients are the subjects who need to be tracked, correctly. RFID tags are one of the best tools available for identification and tracking of subjects. For



Fig. 1. A typical UHF RFID tag reading scenario

example, one of the biggest chain stores of U.S.A., the Walmart, started using RFID tags on its goods, in 2005 [5]. Walmart has gradually replaced traditional paper barcodes with RFID tags. Recently, passive UHF RFID tags have been proposed in inpatient medication. Passive tags are named as such because; they have no battery but are energized by the reader that approaches to read the ID inside the tag. These tags are used as bracelets for inpatients and as tags on medicine packs. Passive UHF tags are preferred because of their low cost and long reading distance, but they have limited resources and lack security primitives. A specific type of passive UHF tag can be read from a few meters. As many as hundreds of tags, can be read per second. According to ISO 18000-6 and EPC Global Class 1 Generation 2 (Gen-2) standards written for UHF tags, they contain only a 16 bit pseudo random number generator (PRNG), a CRC and an XOR function to obscure their messages [6,7]. Therefore, the capture of the Electronic Product Code (EPC), i.e. the ID of the tag, is not difficult.

A typical RFID set up used in patient identification consists of a back-end database server (server), a reader and a tag (Fig. 1). The server has all the information about a subject: 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 (also stored in the tags).

In the rest of this paper, Sect. 2 summarizes previous work. Sections 3 and 4 demonstrates weaknesses of two latest proposals. Section 5 questions the use of Gen-2 tags and, proposes another type of tag that is better suited for health-care. Some critical capabilities and characteristics of the two tag types are also compared, in Sect. 5. Section 6 concludes and has the future work.

2 Related Work

Juels et al.'s work [8] is one of the first in identification of a group of objects, using RFID tags. In this work, a grouping proof is defined as the simultaneous reading of two tags at a given timestamp. Other grouping proofs have also been

proposed for tags [9]. The weaknesses and recommended security enhancements for grouping proofs in general can be found in [10].

Two of the first proposals to use RFID tags in patient medication were made by Wu et al. and Sun et al. [11, 12]. These pioneering work in inpatient medicine administration, lacked detailed description and advocated the use of personal computers as mobile devices and paper barcodes. Barcodes have limited capabilities and there are disadvantages of their use in patient safety [13].

A proposal where both the inpatient and the medicine are identified by low-cost RFID tags conforming to Gen-2 standard was made by Huang and Ku [14]. The inpatient is assumed to have a wristband with an embedded RFID tag. The inpatient's medicine container is also marked with a Gen-2 tag. Unfortunately, the security flaws in the grouping proof are demonstrated by Chien et al. [15]; whom suggested an alternative protocol, which is shown to be also vulnerable [16]. The grouping proof protocol schemes, suggest evidence to be generated after the administration of medicine. The evidence is verified later, in the HIS server. False evidence generation, interference with evidence generation procedure, exposure of critical information during evidence creation are some of the problems encountered. The issues arise, because the unsecured messages through the air are eavesdropped by adversaries.

Apart from the above, we demonstrate further weaknesses in two recent works, in Sects. 3 and 4. The two works are specifically chosen because, their authors try to rectify previous vulnerable schemes, but fail because, they do not consider the algebraic attacks outlined in previous works due to non-availability of security primitives, in Gen-2 tags. The works fail because, they do not consider the enhancements neither in [10], nor the algebraic attacks outlined in [17].

3 Case Study I

Our assumptions for both case studies are as follows. 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. Another assumption is that 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.

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]. Skipping the details, the Safe Drug Administration Procedure (SDAP) and the Evidence Generation Procedure (EGP) are analyzed. The inexistence of the pre-shared secrets in the SDAP is criticized, but no attack is demonstrated. The EGP is also criticized for not being signed by the inpatient, which allows the hospital to re-generate false evidence without inpatient's awareness. Yen's proposed rectified scheme is shown in Fig. 2. We demonstrate a disclosure attack on Yen's rectified scheme, which also succeeds in IS-RFID. The attack will show

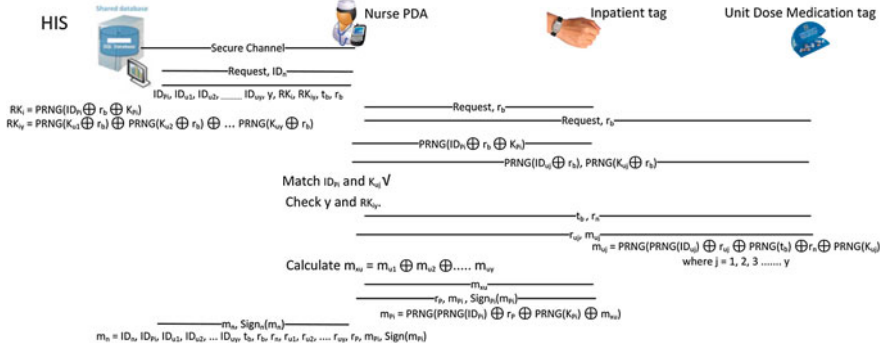


Fig. 2. Yen's proposed offline scheme [16]

that all protocols based on obscuring the ID of a tag by the use of the PRNG of a Gen-2 tag are vulnerable.

Yen proposes one offline and one online solution. Two schemes are the same, except in the online version, the inpatient's tag is authenticated online by the server, via the nurse PDA. The notation used in Fig. 2 is explained below:

$\text{ID}_n, \text{ID}_{Pi}$	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, $j=1, 2, \dots, y$.
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, $j=1, \dots, y$.
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.
$\text{PRNG}()$	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 , $j=1, 2, \dots, y$.
m_{Pi}	Partial evidence generated by i th inpatient's tag.
m_n	Medication evidence generated by a nurse.
$\text{Sign}_n(m_n)$	Signature function of nurse, that signs evidence m_n .
$\text{Sign}_{Pi}(m_{Pi})$	Signature function of i th inpatient, that signs evidence m_{Pi} .

Before starting the round, the nurse makes a request with her ID and downloads all inpatient records from the HIS. The daT_a also include the timestamp t_b to supervise the time of drug administration. Validation values RK_i and RK_{iy} are formed by using the pre-shared key of the inpatient's tag and the corresponding unit-dose key, respectively. The nurse starts the round and sends the same request both to the inpatient and the unit-dose tags, with a reader equipped

PDA. Using the HIS nonce r_b , the inpatient tag replies with $\text{PRNG}(\text{ID}_{P_i} \oplus r_b \oplus K_{P_i})$ and every unit-dose tag replies with $\{\text{PRNG}(\text{ID}_{uj} \oplus r_b), \text{PRNG}(K_{uj} \oplus r_b)\}$, where $j=1,2, \dots, y$. Upon receiving the replies, the PDA matches the inpatient tag's reply with RK_i to identify and authenticate the inpatient. Next, the PDA uses the RK_{ij} to identify and authenticate the unit-dose packs. If all matching is good, the PDA generates its own nonce r_n and sends it with the timestamp of the HIS to every unit-dose pack. The unit-dose packs generate their own nonce and use it together with nurse PDA's nonce to prepare a partial medication evidence $m_{uj} = \text{PRNG}[\text{PRNG}(\text{ID}_{uj}) \oplus r_{uj} \oplus \text{PRNG}(t_b) \oplus r_n \oplus \text{PRNG}(K_{uj})]$, where $j=1, 2, \dots, y$. Each unit-dose sends back its reply to the nurse PDA. The PDA stores every nonce r_{uj} sent and calculates m_{xu} , by XORing every m_{uj} . The value m_{xu} is sent to inpatient's tag. The inpatient's tag prepares its partial evidence $m_{P_i} = \text{PRNG}(\text{PRNG}(\text{ID}_{P_i}) \oplus r_P \oplus \text{PRNG}(K_{P_i}) \oplus m_{xu})$, after generating a nonce reply r_P . Finally the inpatient tag signs its evidence $\text{Sign}_{P_i}(m_{P_i})$ and sends the tuple $\{r_P, m_{P_i}, \text{Sign}_{P_i}(m_{P_i})\}$ to the nurse PDA. Upon receiving the final partial evidence, the nurse PDA prepares a final medication evidence m_n . The evidence is signed and saved in the PDA, as $m_n, \text{Sign}_n(m_n)$. At the end of the round, the nurse returns to the nurse station and uploads all of the drug administration evidence to the HIS. It is the duty of HIS to check and find if there have been any medication errors.

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 Gen-2 standards [6,7]. But, even this assumption cannot save the scheme.

3.1 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 $\text{PRNG}(x)$ is calculated for a given input x ; e.g. using $(\text{ID}_{P_i} \oplus r_b \oplus K_{P_i})$ as input, a deterministic output $\text{PRNG}(\text{ID}_{P_i} \oplus r_b \oplus K_{P_i})$ 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 1. Looking at the table, the corresponding output of an input or the corresponding input of an output can be found, easily. PRNG may produce the same output for the distinct values, but this shows the weakness of the PRNG which is not a desirable property. In that case much more trial and errors are needed.

The inpatient desired to be administered wrong medication is the "target". Another inpatient whose identity is going to be illegally given to the target is

Table 1. A typical pre-calculated table

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

called the “conveyor”. The goal is to cause repeated switch of medicine administrations of the target and conveyor, without getting detected. After exposing the $(ID_{Pi} \oplus K_{Pi})$ of the conveyor and the target; the identities are switched and detection is avoided.

An adversary/attacker acts as a visitor and goes near the conveyor with a rogue reader. Rogue or untrusted readers are assumed to be always present in open environments [16, 18]. The attacker sends a request request, r_a , 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 the table is searched and the corresponding input; e.g. $input1$, is found: $input1 = (ID_{Pi} \oplus r_a \oplus K_{Pi})$. Then, $(ID_{Pi} \oplus K_{Pi}) = input1 \oplus r_a$. $(ID_{Pi} \oplus K_{Pi})$ is constant for any given inpatient; therefore any inpatient is uniquely identified. Using the replies of the unit-dose packs with Table 1 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 for $j = 1, 2, \dots, y$. The same attack is repeated at the target. At the end, both the target and conveyor’s $(ID_{Pi} \oplus K_{Pi})$, ID_{uj} and K_{uj} are captured.

Next, the evidence generation procedure of the target and conveyor are eavesdropped for just one round. The messages $\{r_{uj}, m_{uj}\}$ of the unit-dose packs in Fig. 2 are recorded, by the attacker. The value of m_{xu} , sent to the conveyor is also recorded. The final reply $\{r_P, m_{Pi}, Sign_{Pi}(m_{Pi})\}$ of the conveyor is analyzed next. The values not known in $m_{Pi} = PRNG(PRNG(ID_{Pi}) \oplus r_P \oplus PRNG(K_{Pi}) \oplus m_{xu})$ are $PRNG(ID_{Pi})$ and $PRNG(K_{Pi})$. But the value $[PRNG(ID_{Pi}) \oplus PRNG(K_{Pi})]$ is constant and can be exposed. Looking at the output column of Table 1, a match for the value of m_{Pi} is found, e.g. $output1$. Using $output1$, $[PRNG(ID_{Pi}) \oplus PRNG(K_{Pi})] = output1 \oplus r_P \oplus m_{xu}$ is obtained. The only unknown left is $Sign_{Pi}(m_{Pi})$. The available functions in a Gen-2 tag are PRNG, CRC and XOR operation. Therefore, the assumed out-of-standard, digital signature is most likely to be a deterministic function that has its own 65,536 (216) entry table. Whatever it is, it has to be public and readily available to all tags. Either we have the function and we can construct $Sign_{Pi}(m_{Pi})$ out of m_{Pi} or the attacker records the $m_{Pi}, Sign_{Pi}(m_{Pi})$ pairs, as a table called Table X. Therefore, the attacker has the $m_{Pi}, Sign_{Pi}(m_{Pi})$ pair. The same is repeated near the target.

The attacker takes the exposed values $(ID_{Pi} \oplus K_{Pi})$, $[PRNG(ID_{Pi}) \oplus PRNG(K_{Pi})]$, $Sign_{Pi}()$ function or Table X, for the target and conveyor and writes them into two different tag emulators, at a private location. Such a hardware device emulating an RFID tag is the Chameleon [20]. We do not intend to implement any, but there are works on RFID tag emulators [21]. The difference from the real tag is that the emulator uses the XORed $(ID_{Pi} \oplus K_{Pi})$, $[PRNG(ID_{Pi}) \oplus PRNG(K_{Pi})]$ values instead of individual values to form its replies.

In the final step of the attack, the tag emulator of the target is placed next to the conveyor and the emulator of the conveyor is placed next to the target. Hence, the switch of the identities is completed. The nurse cannot notice the presence of the switch, because she does not come close to the UHF tags. When

the nurse follows normal procedure, the rogue tags generate correct RK_i , $RK_{i,y}$ and partial evidences. The nurse administers wrong medicine to both patients, signs the evidence and sends them to the HIS. The HIS cannot detect the switch and wrong medication is repeated until the target and impatient show diverse symptoms.

Yen's protocol has another weakness, as well. Blocking $\{t_b, r_n\}$ or m_{xu} , and sending bogus instead stop the medication procedure. The medication in a clinic can be disrupted with a strong, bogus transmission.

4 Case Study II

A second work criticizing a previous proposal which uses Gen-2 RFID tags is by Wu et al. [22]. Wu criticizes Yu et al.'s proposal for being based on a fully analyzed protocol [23]. We leave the study of Yu's proposal outside the scope of this work, because we would like to concentrate on Wu's rectified protocol. Wu's proposal is summarized in Fig. 3. 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.

At the beginning the server pre-shares secrets X_a and X_b with tags T_a and T_b , respectively. Typically, the reader challenges both the inpatient and unit-dose tag with the same timestamp, t . Both tags reply with their index-pseudonym (IDS), a nonce and a tag authenticator; $\{IDS_a, r_a, v_a\}$ and $\{IDS_b, r_b, v_b\}$ respectively. The index-pseudonym is a pseudo ID of the tag that is an updated version of constant ID, every round. The reader is online with the back-end server and sends the tag replies together with the timestamp to the server. If verification is good, the server sends two keys K_a, K_b to the reader. Without waiting for a reply, the server immediately updates IDS_a and IDS_b . Using the key K_a , the reader calculates its authenticator α_a and sends $\{\alpha_a, IDS_b, t\}$ to tag T_a . T_a calculates its own α'_a and matches it with the received α_a . If they are a match, T_a prepares β_a and partial evidence ma and sends them to the reader. Then, T_a updates. The reader verifies β_a and then prepares its authenticator α_b and sends $\{\alpha_b, IDS_a, m_a\}$ to tag T_b . Using its own key, T_b verifies α_b ; then, computes its second authenticator β_b , partial evidence mb and sends them to the reader. Then, T_b updates its IDS_b . Upon receiving $\{\beta_b, mb\}$, the reader verifies β_b and then concludes that T_a and T_b exist in the field, simultaneously. Finally, the reader accumulates $\{IDS_a, IDS_b, t, m_a, m_b\}$ in a tuple, as a proof and, sends it to the back-end server. Notice that the reader does not update, at the end.

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. The implementation of F function is shown by an example. Let $M = (m_0, m_1, m_2, m_3)$, $C = (c_0, c_1, c_2, c_3)$, $D = (d_0, d_1, d_2, d_3)$, $E = (e_0, e_1, e_2, e_3)$, where m_i, c_i, d_i, e_i and γ are all 16-bit numbers. Function $\gamma = P(E) = \text{PRNG}(\text{PRNG}(\text{PRNG}(\text{PRNG}(e_0) \oplus e_1) \oplus e_2) \oplus e_3)$. For $C = F(M)$; $c_0 = P(m_0, m_1, m_2, m_3)$, $c_1 = P(m_1, m_2, m_3, m_0)$, $c_2 = P(m_2, m_3, m_0, m_1)$, $c_3 = P(m_3, m_0, m_1, m_2)$. In brief, $F(M)$ is a total of 16 nested

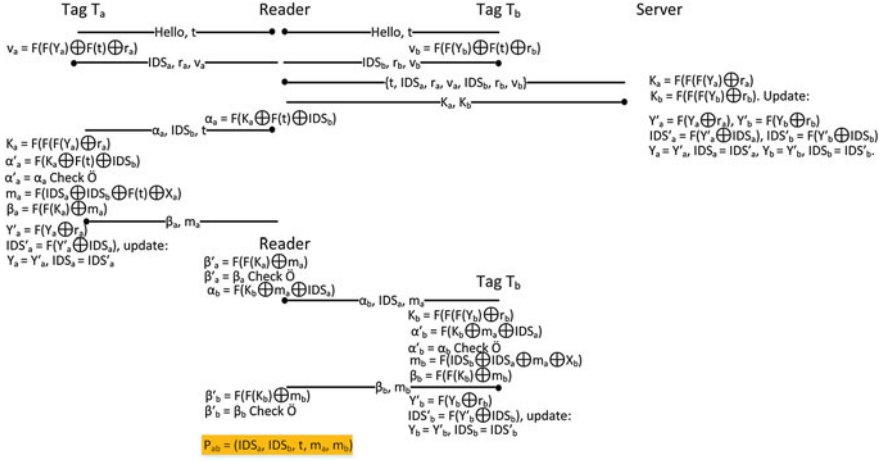


Fig. 3. The scheme of work [22]

PRNG and 12 XOR operations. Since F is a public function, for any known input, $F(x)$ can be calculated. Therefore, a table similar to that of Table 1 in Sect. 3.1 can be prepared. Only the preparation of the table -called Table X- is computationally more intensive than the preparation of Table 1, but it will have 216 (65,536) possible inputs and corresponding outputs as Table 1. Referring to the input and output columns of Table X is no different than that of Table 1 and takes very short time. Additionally, $F(F(x))$ is the application of F function on the result of $F(x)$, i.e. 32 PRNG and 24 XOR operations.

4.1 Attacks on Wu's Scheme

Exposure Attack. The exposure attack on the protocol is similar to the attack in Sect. 3.1. 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.

Referring to the hypothetical Table X, the value of v_a is used as an output and the corresponding input -called $input_{va}$ - is read. From Fig. 3:

$$input_{va} = F(Y_a) \oplus F(t) \oplus r_a \quad (1)$$

$$F(Y_a) = input_{va} \oplus F(t) \oplus r_a \quad (2)$$

The nonces r_a , r_b , IDS_a , IDS_b and the timestamp t are in clear text and the value of $F(t)$ is found from the output column of Table X. Hence, by XORing the found $input_{va}$ with the known values $F(Y_a)$ is exposed (Eq. 2). Using the exposed $F(Y_a)$ in the output column of Table X, the value in the input column gives Y_a . Following the same steps Y_b is also exposed. The keys K_a , K_b are calculated

using the newly exposed Y_a and Y_b , the nonces r_a and r_b . Next, the updated values of Y_a and Y_b are also exposed. The updated values of IDS_a and IDS_b depend on the current values and the updated values of Y_a and Y_b , exposed in the previous step. Thus, the adversary also obtains the updated values of IDS_a , IDS_b . Without eavesdropping any message exchanges the adversary captures Y_a , Y_b , K_a , K_b and updated values of Y_a , Y_b , IDS_a , IDS_b .

The attack continues by eavesdropping one complete round. When the reader sends $\{\alpha_a, IDS_b, t\}$ to T_a , the attacker waits for the reply $\{\beta_a, m_a\}$. Using the value of m_a in the output column, a corresponding input – call it input m_a – is read:

$$input_{m_a} = IDS_a \oplus IDS_b \oplus F(t) \oplus X_a \quad (3)$$

$$X_a = input_{m_a} \oplus IDS_a \oplus IDS_b \oplus F(t) \quad (4)$$

Hence, the pre-shared secret X_a is captured (Eq. 4). The message $\{\alpha_b, IDS_a, m_a\}$ is of no importance because its terms are captured values. The reply $\{\beta_b, m_b\}$ of T_b gives away the pre-shared secret X_b , after a similar analysis of m_b , as in m_a . Hence, the adversary has the shared secrets X_a and X_b , necessary for the creation of rogue tags. The rest of the attack is the same as in Sect. 3.1. The attacker loads the captured values into two rogue tags, switching the identities of the target and conveyor. The result is wrong medication of a targeted inpatient, possibly causing deadly conditions.

De-synchronization Attack. The protocol of Fig. 3 is also vulnerable to de-synchronization attack, at many points. 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. For example, consider the moment when the reader sends the messages $\{IDS_a, r_a, v_a\}$ and $\{IDS_b, r_b, v_b\}$, to the server. After calculating and sending the keys, the server updates. If the reader does not get the keys (loss of power), or cannot continue communication with the tags, then the server is de-synchronized with the tags; because the tags have not been updated. During the retry, the reader obtains and sends the old $\{IDS_a, r_a, v_a\}$ and $\{IDS_b, r_b, v_b\}$. The server never finds the old values in its database to verify the tags. In total, there are four instances that can cause de-synchronization: the reply of the server to the reader, the message exchange between the reader and T_a , the message of reader to T_b . Extra care is necessary in protocols that use updating, because de-synchronization halts medication.

4.2 Computational Load of Wu's Scheme on Gen-2 Tags

Looking at Fig. 3, the most intensive computations in tags take place, after receiving authenticator (α_a, α_b) of the reader. Counting the number of F function and XOR operations from the instant of computing K_a until sending $\{\beta_a, m_a\}$

(assuming update can take place after sending $\{\beta_a, m_a\}$); Ta has a larger computational load with nine F function and seven XOR operations. Every F function involves sixteen PRNG and twelve XOR operations. Hence, Ta makes 144 PRNG and 115 XOR operations. A PRNG consumes around 190 clock cycles to produce a random number [24]. Assuming a 16-bit architecture, each XOR operation takes one clock. In total, Ta spends 27,475 ($144 \times 190 + 115$) clock cycles in computations. This is around 26 times more than an 8-bit AES implementation, which consumes 1032 clock cycles [25]. In other words, Wu's proposal cannot meet the limits, as it exceeds 220 clock cycles [26].

5 Discussions

As demonstrated, Yen's and Wu's schemes are as vulnerable as their predecessors, which contradict the major safety goals [2, 4]. Wu's scheme cannot fit in a Gen-2 tag, is vulnerable and has the same characteristics of Wu's and Yen's protocols; therefore, it will not be discussed any further. The reason of the disclosure of critical data by our attacks is a result of using the only available function PRNG, as an encryption function. To the best of our knowledge there is no formal proof of using a PRNG as an encryption or hashing algorithm [19]. For patient safety, confidentiality of critical data has to be provided by true encryption. In other words, an alternative with stronger cryptographic primitives is necessary, instead of the 16-bit PRNG function of ISO 18000-6 or EPC Gen-2 tags, which are used for commercial goods in supply chains. 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.

5.1 Ambiguities and Disadvantages of Yen's Proposal

Yen's proposal carries over the ambiguities of the work it criticizes. Even if PRNG is accepted as the only viable option, a special tag is required to calculate values like $\text{PRNG}(\text{ID}_{P_i} \oplus r_b \oplus K_{P_i})$, 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. This assumption is highly questionable as the only available option is a PRNG and suggesting its use in digital signing is totally unacceptable. An unconsidered but possible scenario is the presence of more than one inpatient, in the same room. 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. With equal distance from two inpatients, a nurse can give the other patient's medicine to the intended patient. The aftermath of a complication at an inpatient is not considered, either. The medication responsibility of other inpatients, while a previous inpatient is going through a complication, is ambiguous. The continuation of medication with the

same PDA, by a second nurse is not good. If a wrong medication is detected, the first nurse is falsely blamed. Using a second nurse PDA causes a discontinuation of the inpatient tuples and requires server intervention; since every nurse downloads inpatient data with her own PDA/password.

In their security analysis, Yen et al. claim that data confidentiality of their protocol is guaranteed. However, the identities and keys of the inpatients are exposed after our full disclosure attack, even though they are not transferred in plaintext.

Not only that, Yen's system has disadvantages, as well. A disadvantage is dedicating a PDA for every nurse, which is neither widely available nor cheap. UHF readers in the form of PDAs are uncommon and expensive. This increases the overall cost in hospitals, where there are many clinics and many shifts. Finally, the lack of consideration of Health Level 7 (HL7) standards is another disadvantage, because any noncompliant solution is unlikely to be endorsed [27]. Not paying attention to HL7 standards is partly the reason of vulnerabilities; especially the mutual authentication requirement. Various attacks on ISO 18000-6 RFID are explained in detail [10, 17, 28]. In brief, there are four types of attacks: Interception, interruption, modification and fabrication attacks. Each attack has some counter measures, but they are not enough to guarantee patient safety, simply because of the limited resources of the tags, in question.

5.2 Security Vulnerabilities of Wu's Scheme

In their security evaluation, Wu et al. [22] defends that impersonation, ID-Theft and clone attacks cannot be launched against their protocol. Contrarily, our full disclosure attack exposes the secret keys, which opens the avenue to generating false grouping proof evidence. Not only that, our attack demonstrates how a fake tag (clone) can be devised to alter the identity of an impatient. Therefore, their clone attack evaluation is also unsatisfactory. Besides the successful impersonation and clone attacks, a de-synchronization attack is demonstrated above, an attack type they fail to evaluate in their analysis.

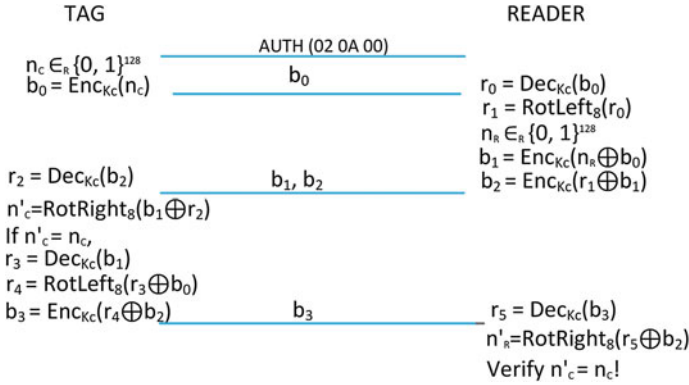
5.3 Suitable Technology for Patient Safety: NFC

A viable alternative technology is the near field communication (NFC) tags, because they possess the desired characteristics and cryptographic primitives. For example, Mifare DesFire version EV1 (EV1) tag has a built in AES engine [29]. If this feature existed in ISO 18000-6 tags, both of our PRNG table attacks would have been ineffective. Definitely, the existence of an AES engine provides better patient data safety. Another important characteristic that would have prevented our attacks is the operating distance. EV1 is read from a distance of 20–100 mm, therefore the nurse has to approach intentionally very close to an inpatient. Such a physical requirement removes the danger of eavesdropping by an adversary from meters away and the danger of reading a rogue tag.

The characteristics of EPC Gen-2 and EV1 tags that impact medicine administration are compared, in Table 2. Apart from the encryption and reading

Table 2. Comparison of EPC Gen-2 Tag and DesFire EV1

Property	EPC Gen-2 Tag	DesFire EV1
Authentication	\oplus	AES
Supply energy	No battery	No battery
Operating distance	Up to 7 m	20–100 mm
Tags read	1000 tags/s	1 tag/s
Data integrity	16 bit CRC, framing	16/32 bit CRC, parity, bit coding, bit counting
Memory capacity	512 bit on chip	2, 4, 8 kB NV-memory
Standard	ISO 18000-6	ISO/IEC 14443A

**Fig. 4.** DesFire EV1 authentication

distance advantages, the NFC tags have other advantages over the EPC Gen-2 tags. Data integrity of the exchanged messages is an important security characteristic. Any multiple changes in the transmitted messages should be detected. As observed from the table, EV1 provides better data integrity algorithms. But, a property where EPC Gen-2 technology performs better is the number of tags read per second. A nurse can read only maximum one NFC tag/s, because physically she has to approach and momentarily touch the tag. But, this does not provide an advantage over NFC tags because; there is no hurry to read many inpatient tags. The memory capacity of EV1 tags surpasses the EPC Gen-2 tags. This is important because future protocols and schemes have a better chance to be accommodated on a spacious EV1 tag. User developed security applications or extended secrets can be stored in EV1. The ISO standards of the two technologies are different. But, the ISO 14443A standard is meant for the smartcards, clearly a higher class technology than the ISO 18000-6 standard.

Another important parameter of the EV1 is its 3-way mutual authentication. As given in Fig. 4, a new session key is created for each session through a pre-shared key. Simply, the authentication is based on the verification of the exchanged encrypted nonces.

The use of strong cryptographic primitives instead of a simple 16-bit PRNG function increases the security level but also leads to other hardware requirements. Therefore, one would expect to see a considerably more expensive cost for the higher NFC technology solution. But, this is not the case. The NFC tag prices are higher than the UHF tags, but the total cost for a complete solution is not. In his cost analysis, Peris et al. calculate a total cost for a floor with 5000 inpatients/year, 3 unit-dose/day, 3 nurses on each floor and an average hospital with 8 floors [18]. The cost of the HIS and AMD are excluded, because those are included in the overall cost of the hospital. The cost of an EPC Gen-2 tag is given as \$0.5/tag, including the plastic package of each unit-dose. Every nurse is equipped with a PDA, astonishingly priced at \$300. The total number of tags used for the inpatients and the unit doses is 20,000/year; mistakenly taken as 15,000/year by Peris et al. In the end, Peris et al. conclude with a cost of \$70,000/year, for his proposal. An NFC tag costs \$0.421 to \$0.825, depending on the size of the order. Hence, the NFC tags are more expensive than EPC Gen-2 tags, as expected. But, to the best of our knowledge, a mobile UHF Gen-2 reader is around \$1027. On the other hand, a popular NFC enabled tablet (Google Nexus 7) costs around \$199. Therefore, there is a 5:1 price ratio, in favor of NFC readers. Obviously, even with the most expensive NFC tag, our solution (\$21,300) is less expensive than that of Peris et al.'s.

6 Conclusion

The weaknesses of ISO-18000-6 or Gen-2 tags in safe drug administration are obvious, following the various attacks presented in this and previous work. As demonstrated the analyzed protocols fail their data confidentiality claims. The use of PRNG as an encryption algorithm is a major drawback. On the other hand, those proposals that try to provide stronger encryption by nested PRNG operations, cannot meet the time limits of RFID tags. With so many weaknesses and disadvantages, EPC Gen-2 type tags cannot increase inpatient medication safety.

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. The previous works suggest the use of non-standard operations and special equipment. The contemporary, less expensive and widely available NFC enabled tablets are better suited for the job. The comparison of EPC Gen-2 and NFC tag technologies indicate that NFC is a better viability. Currently, a proposal using the NFC technology and strong security is underway, in our lab. An authentication based on EV1 mutual authentication structure will be the future work. Another alternative to increase the security is using public-key cryptography as indicated in [30], but the huge clock cycle (66,048) of using that alternative affects usability of the system.

References

1. Eurobarometer 2006 survey on medical errors. Technical Report, October 2005 (2006)
2. Kaushal, R., Bates, D.W., Landrigan, C., McKenna, K.J., Clapp, M.D., Federico, F., Goldmann, D.A.: Medication errors and adverse drug events in pediatric inpatients. *JAMA* **285**(16), 2114–2120 (2001)
3. Reporting, E., Meaders, S., Hickner, J., Kuo, G.M., Fagnan, L.J., Forjuoh, S.N., Stevens, B.K., Pace, W.D., Hamlin, B.N., Scherer, H., Hudson, B.L., Oppenheimer, C.C.: Field test results of a new ambulatory care medication error and adverse drug. *Ann. Family Med.* **8**, 517–525 (2010)
4. 2010 National Patient Safety Goals (NPSGs) (2010)
5. Wal-Mart details its RFID journey. http://www.computerworld.com/s/article/109132/Wal-Mart_details_its_RFID_journey
6. Information technology - Radio frequency identification for item management - Part 6: Parameters for air interface communications at 860 MHz to 960 MHz. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=46149
7. Prop, E.I.: EPC Global Class1 Gen2 RFID Specifications, December 2005 (2006)
8. Juels, A.: Yoking-proofs for RFID tags. In: Second IEEE Annual Conference on Pervasive Computing and Communications Workshops, pp. 14–17, 138–143. IEEE Press, New York (2004)
9. Saito, J., Sakurai, K.: Grouping proof for RFID tags. In: Conference on Advanced Information Networking and Applications, pp. 621–624. Taichung (2005)
10. Peris-Lopez, P., Orfila, A., Hernandez-Castro, J.C., van der Lubbe, J.C.: Flaws on RFID grouping-proofs. Guidelines for future sound protocols. *J. Netw. Comput. Appl.* **34**(3), 833–845 (2011)
11. Wu, F., Kuo, F., Liu, L.W.: The application of RFID on drug safety of inpatient nursing healthcare. In: 7th International Conference on Electronic Commerce, pp. 85–92, New York (2005)
12. Sun, P.R., Wang, B.H., Wu, F.: A new method to guard inpatient medication safety by the implementation of RFID. *J. Med. Sys.* **32**, 327–332 (2008)
13. Chen, C.-L., Wu, C.-Y.: Using RFID yoking proof protocol to enhance inpatient medication safety. *J. Med. Sys.* **36**, 2849–2864 (2012)
14. Huang, H.H., Ku, C.Y.: A RFID grouping proof protocol for medication safety of inpatient. *J. Med. Sys.* **33**(6), 467–474 (2008)
15. Chien, H.Y., Yang, C.C., Wu, T.C., Lee, C.F.: Two RFID-based solutions to enhance inpatient medication safety. *J. Med. Sys.* **35**(3), 369–375 (2011)
16. Yen, Y.C., Lo, N.W., Wu, T.C.: Two RFID-based solutions for secure inpatient medication administration. *J. Med. Sys.* **36**(5), 2769–2778 (2012)
17. van Deursen, T., Radomirović, S.: Algebraic attacks on RFID protocols. In: Markowitch, O., Bilas, A., Hoepman, J.-H., Mitchell, C.J., Quisquater, J.-J. (eds.) WISTP 2009. LNCS, vol. 5746, pp. 38–51. Springer, Heidelberg (2009)
18. Peris-Lopez, P., Orfila, A., Mitrokovtsa, A., van der Lubbe, J.C.A.: A comprehensive RFID solution to enhance inpatient medication safety. *Int. J. Med. Inform.* **80**, 13–24 (2011)
19. Wickboldt, A.K., Piramuthu, S.: Patient safety through RFID: vulnerabilities in recently proposed grouping protocols. *J. Med. Sys.* **36**(2), 431–435 (2012)
20. Kasper, T., von Maurich, I., Oswald, D., Paar, C.: Chameleon: a versatile emulator for contactless smartcards. In: Rhee, K.-H., Nyang, D. (eds.) ICISC 2010. LNCS, vol. 6829, pp. 189–206. Springer, Heidelberg (2011)

21. Redemske, R., Fletcher, R.: Design of UHF RFID emulators with applications to RFID testing and data transport. In: Fourth IEEE Workshop on Automatic Identification Advanced Technologies (AutoID 2005), pp. 193–198 (2005)
22. Wu, S., Chen, K., Zhu, Y.: A secure lightweight RFID binding proof protocol for medication errors and patient safety. *J. Med. Sys.* **36**(5), 2743–2749 (2012)
23. Yu, Y.C., Hou, T.W., Chiang, T.C.: Low cost RFID real lightweight binding proof protocol for medication errors and patient safety. *J. Med. Sys.* **36**(2), 823–828 (2012)
24. Peris-Lopez, P., Hernandez-Castro, J.C., Estevez-Tapiador, J.M., Ribagorda, A.: LAMED—A PRNG for EPC Class-1 Generation-2 RFID specification. *Comput. Stand. Interfaces* **31**(1), 88–97 (2009)
25. Feldhofer, M., Wolkstorfer, J.: Hardware implementation of symmetric algorithms for RFID security. In: Kitsos, P., Zhang, Y. (eds.) *RFID Security*, pp. 373–415. Springer, New York (2009)
26. Martín, H., Millán, E.S., Entrena, L., César, J., Castro, H.: AKARI-X: a pseudo-random number generator for secure lightweight systems. In: 17th IEEE IOLTS, pp. 228–233 (2011)
27. Health Level Seven International. <http://www.hl7.org/implement/standards/index.cfm?ref=nav>
28. Hawrylak, P.J., Schimke, N., Hale, J., Papa, M.: Security risks associated with radio frequency identification in medical environments. *J. Med. Sys.* **536**(6), 3491–3505 (2012)
29. Mifare DesFire EV1 Leaflet. http://www.nxp.com/products/identification_and_security/smart_card_ics/mifare_smart_card_ics/mifare_desfire/
30. Oren, Y., Box, P.O.: A low-resource public-key identification scheme for RFID tags and sensor nodes a brief description of the protocol. In: *WiSec 2009*, pp. 59–68 (2009)

Radio Frequency Identification: Security and Privacy
Issues

Security and Privacy Issues 9th International Workshop,
RFIDsec 2013, Graz, Austria, July 9-11, 2013, Revised
Selected Papers

Hutter, M.; Schmidt, J.-M. (Eds.)

2013, XIV, 177 p. 59 illus., Softcover

ISBN: 978-3-642-41331-5