Serialized TID Numbers – A Headache or a Blessing for RFID Crackers?

Mikko Lehtonen*, Antti Ruhanen† Florian Michahelles*, and Elgar Fleisch*‡
*Information Management, ETH Zürich, 8092 Zürich, Switzerland, {mikkol,fmichahelles}@ethz.ch
†Confidex Oy, 33230 Tampere, Finland, antti.ruhanen@confidex.fi
‡University of St.Gallen, Institute of Technology Management, 9000 St. Gallen, Switzerland, elgar.fleisch@unisg.ch

***Abstract*—Though transponder ID (TID) numbers of RFID tags were originally introduced to identify the chip model, serialized TID numbers are currently advertised as security features of UHF chips. Serialized TID numbers do not provide any cryptographic protection, but they do introduce a practical hurdle against adversaries who want to clone RFID tags today. Furthermore, serialized TID numbers are important for end-users who want to protect their current UHF tags from cloning since cryptographic tags are not yet commercially available in that frequency range. In this overview paper, we analyze the suitability of serialized TID numbers for security applications by evaluating the effort to bypass the TID check based on known vulnerabilities and we compare this effort to the needed level of protection in an example of anti-counterfeiting in the tobacco industry. The analysis illustrates that the practical hurdle of TID checks is not high enough for industrial-scale security applications and that it can completely diminish due to commodification of the RFID technology. However, end-users of security applications can still benefit from the increased tag cloning resistance that serialized TID numbers provide before migrating to more secure solutions.**

I. Introduction

Radio frequency identification (RFID) tags store Transponder ID (TID) numbers that identify the chip's model and manufacturer. These numbers are written on the chips during fabrication and they are protected against rewriting. A TID number can optionally include a serial part that identifies also the unique chip. These serialized TID numbers are written on some existing EPC Class-1 Generation-2 (in short: Gen-2) chips and they are expected to become a common feature of Gen-2 chips in the future.

On the one hand, serialized TID numbers can be a big headache for RFID crackers who want to clone tags. While a tag's object ID number, such as the Electronic Product Code (EPC), can be easily changed, changing the write-protected TID number is considerably harder. As a result, chip manufacturers advertise the serialized TID numbers as security features of Gen-2 chips. On the other hand, the use of serialized TID numbers as security features represents a big opportunity for RFID crackers. In contrast to cryptographic tags, serialized TID numbers do not provide any real security against tag cloning. For instance, there is nothing that prevents an adversary from reading the serialized TID number of a tag and transmitting this number to a reader to impersonate the tag. In addition, if chips with programmable TID numbers became commercially available, cloning serialized TID numbers would become as easy as cloning EPC numbers.

Despite these obvious vulnerabilities of the TID scheme, it would nevertheless be incorrect to claim that serialized TID numbers do not provide *any* protection against tag cloning and impersonation; since RFID tags with programmable TID numbers are not available in the market today, it is currently not easy for an adversary to obtain a passive RFID tag with a wanted serialized TID number. Because of this dilemma, end-users have a reason to be confused about the usefulness of serialized TID numbers in security applications such as access control, ticketing and anti-counterfeiting. In addition, there are dangerous misconceptions about the level of protection that serialized TID numbers can provide. For instance, the United States Department of Homeland Security posits in its Privacy Impact Assessment on the Passport Card [1] that "*...there is a powerful tool that can be used to remove the risk of cloning. This tool is the Tag Identifier, or TID. The TID is available on all Gen 2 RFID tags*" [2]. First, given the aforementioned vulnerabilities, it is hardly appropriate to call TID a powerful tool, at least in the long term. Second, as our survey of major Gen-2 chip manufacturers shows, only some Gen-2 tags have *serialized* TID numbers.

These misconceptions contribute to the creation of a dangerous illusion of strong security, upon which end-users should not rely. As an attempt to clarify the misconceptions, this paper tries to draw a clearer picture of the capabilities and limitations of serialized TID numbers in security applications. This paper is especially important for applications operating on UHF tags, since passive cryptographic tags are not yet commercially available in that frequency range.

This paper is organized as follows. We first provide a technical primer to TID numbers in Section II. We then evaluate how the TID checks can be broken or bypassed through all known vulnerabilities in Sections III and IV, and we compare this effort to the needed level of protection in an example of anti-counterfeiting in Section V. In Section VI we discuss and derive guidelines for using serialized TID numbers in security applications for end-user companies.

II. Technical background of TID numbers

This section provides a detailed technical primer that is needed for the detailed evaluation of vulnerabilities presented in Sections III and IV.

A. TID Standards

The purpose of the TID numbers of EPC tags is to identify the chip type and the possible custom commands and optional features the chip supports. This can be done without unique identification of the chip and thus the EPC TID number format does not require serialization of the TID numbers. When the TID number is appended with a unique serial number, such as in the ISO TID format, it also identifies the unique chip.

TID numbers begin with an 8-bit ISO/IEC 15963 Allocation-Class (AC) identifier [11]. The ISO/IEC 15963 standard describes the mechanism to guarantee uniqueness of the TID numbers and presently four organizations have been assigned an AC identifier [10]. The allocation-class identifier for EPCglobal is $11100010_2 = E2_h$.[1] For tags whose AC identifier is $E2_h$, the EPC Gen-2 standard requires that the TID memory be comprised of a 12-bit Tag Mask-Designer Identifier (Tag MDID) and a 12-bit Tag Model Number. According to the Gen-2 air interface specification [11], the TID memory may also contain tag and vendor-specific data such as the serial number. The content of the TID memory bank defined by the EPC standards is shown in Fig. 1.

TID MEM BANK BIT ADDRESS	BIT ADDRESS (In Hex)															
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
10_h-$1F_h$	TAG MDID (last 4-bits)				TAG MODEL NUMBER (12-bits)											
00_h-$0F_h$	11100010_2=E2$_h$								TAG MDID (first 8-bits)							

Fig. 1. TID memory structure in the current EPC standards [12]

For tags whose AC identifier is $E0_h$, the ISO/IEC 15963 requires that the TID memory comprise of an 8-bit tag manufacturer ID and a 48-bit tag serial number. Furthermore, the standard requires that the TID memory be permalocked. The ISO TID structure is illustrated in Fig. 2.

TID MEM BANK BIT ADDRESS	BIT ADDRESS (In Hex)															
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
30_h-$3F_h$	TAG SERIAL NUMBER (48-bits)															
20_h-$2F_h$																
10_h-$1F_h$																
00_h-$0F_h$	11100000_2=E0$_h$								TAG MANUFACTURER ID (8-bits)							

Fig. 2. TID memory structure in the ISO standards [12]

The upcoming EPC Tag Data Standard is likely to make locking the TID numbers mandatory and define a way to specify serialized TID numbers. This is likely to be done with an extended tag identification number (XTID) that extends the current EPC TID format with an 48-bit (or more) serial number and information about key features implemented by the tag. Though chip manufacturers can still opt for a non-serialized version of the TID within this scheme, the new standard is presumed to foster the adoption of serialized TID numbers.

B. Tag manufacturing and memory

To understand the chip manufacturer's arguments about the security of TID checks, this subsection provides an overview to tag manufacturing and memory. A typical RFID tag manufacturing process starts with the design of the integrated circuit (IC), the chip. Outcome of the design project is a chip mask, based on which a semi-conductor foundry can produce the silicon chips. The chip production process is characterized by the manufacturing precision of the semi-conductor manufacturing plant. Currently 120-140 nanometers is considered state of the art for RFID chips. Building a modern semi-conductor manufacturing plant is a billion-dollar investment, but older manufacturing technology is much less expensive. The semi-conductor foundry produces wafers that contain several thousands of chips. While chips are on the wafer, they are in an open test state and can be contacted through direct connectors instead of the radio frequency interface. After testing and programming, the chips are cut from the wafer and attached to antennas [16].

A tag's non-volatile memory consists of Read Only Memory (ROM) and Electrically Erasable Programmable Read Only Memory (EEPROM). Pure ROM is implemented during the wafer production as arrays of transistors on the silicon chip. Because data is fully incorporated in the chip's physical structure, it can neither be erased nor replaced (cf. subsection III-A for exceptions). ROM is defined by the chip mask and all chips that are manufactured with the same chip mask have identical ROM content. Therefore ROM can only be used to store non-serialized ID numbers.

Rewritable non-volatile memory is typically implemented as EEPROM. Implementing one bit in EEPROM is more expensive than using ROM but it gives the chip manufacturer the possibility to rewrite the data. A conventional EEPROM memory cell structure is illustrated in Fig. 3. The memory cell employs two transistors in series: the storage transistor and the access (or select) transistor. The storage transistor has an additional floating gate, located between the channel and the upper gate known as the control gate. The stored memory state of any cell depends upon whether or not electronic charge is present on its floating gate [7].

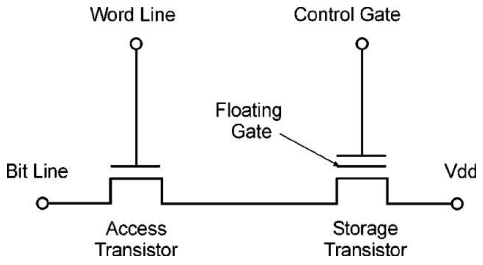

Fig. 3. Circuit schematic of EEPROM memory cell [7]

EEPROM can be protected from rewriting by implementing a *permalock* command. This can be done in different ways. For example, the chip's write command might work only while the chip is on the wafer in the test state, and once the the chip is physically altered to end the test state (e.g. by breaking a connector, by burning a fuse etc.), the write commands are no longer executed by the chip's internal logic. These ways can be used only by the chip manufacturer. Another way is to

[1]Subscripts 2 and h stand for binary and base-16 (*hexadecimal*) number formats, respectively

make use of a lock-bit that can only be flipped once. All write commands to a certain part of the memory first check whether the corresponding lock-bit is flipped and get executed only if the memory is still unlocked. This permalock command can be activated at any time during the chip's lifetime.

III. Vulnerabilities in TID-based authentication

This section analyzes the known vulnerabilities of TID checks. We evaluate the effort to execute different attacks in monetary terms or other resources as far as it makes sense and can be done under general assumptions. The vulnerability of buying unprogrammed chips is addressed in a review of major UHF chip manufacturers in Section IV. The attack tree against TID checks is illustrated in Fig. 4.

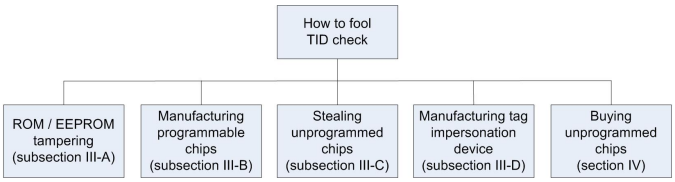

Fig. 4. Attack tree against TID checks

A. EEPROM and ROM tampering

One way to clone the serialized TID numbers, in theory, is to purchase standard tags and to manipulate the content of their TID memory. Even though standard tags' TID memory is write-protected (cf. subsection II-B), there are ways to bypass this. In section II we described how TID memory can be written using EEPROM and ROM (for the non-serialized parts). Both these memories are vulnerable to physical tampering if suitable equipment and knowledge are available.

Tampering of EEPROM and ROM has been discussed in the field of smart card security. The general rule is that the more sophisticated the chip structure is (e.g. higher manufacturing precision), the more expensive the equipment needed to tamper with it. The difficulty in these techniques is that the adversary needs to know or find out which parts of the physical chip (e.g. transistors) to tamper with, and the attacks can also damage nearby portions of the integrated circuit.

According to expert interviews, the cost of equipment to manipulate ROM memory starts from tens of thousands of dollars. Specialized failure analysis laboratories can provide pieces of the necessary physical analytical services at rates around USD 400 per hour [4]. For example, an electron beam of a conventional scanning electron microscope can be used to read, and possibly write, individual bits in ROM and EEPROM. To do this, the surface of the chip must be first exposed, usually via chemical machining [5]. Single bits in a ROM can be overwritten using a laser cutter microscope and EEPROM can be altered using two microprobing needles [6].

Focused Ion Beam (FIB) is perhaps the most powerful equipment to analyze and tamper with the structure of integrated circuits. FIB tools are scientific instruments that resemble a scanning electron microscope and they are used, for example, to locate failure sites within EEPROM memory microcircuits [7]. FIB can be used to modify the hardware circuitry in different ways: it can change a hardwired ROM cell and in principle it can also modify an EEPROM cell. This technique corrupts the EEPROM cell forever, i.e. rewriting is no longer possible, but that is not a problem in the case of TID. In some cases, FIB can also restore test circuitry in smart cards by restoring a fuse that has been blown to physically prevent access to the test state [9]. According to Koemmerling [8], using laser interferometer stages, a FIB operator can navigate on a chip surface with 0.15 μm precision. Using laser-interferometer navigation or infrared laser imaging it is possible to locate individual transistors. Modern FIB workstations cost less than half a million USD and are available in over hundred organizations [8].

B. Manufacturing programmable chips

If any existing chip manufacturer would sell UHF chips with programmable (unlocked) TID memory, the practical hurdle of TID checks would be completely undermined; an adversary could simply buy an empty chip and write the wanted TID number on it. Current EPC standards do not require permanently locked TID memory banks, but according to the best of the authors' knowledge all available EPC chips have their TID memory locked (cf. Section IV). Chips with programmable TID numbers would cause discontent among companies who use TID as a security feature and it appears that the current UHF chip manufacturers recognize their responsibility in securing the TID scheme. However, nothing really prevents companies from manufacturing and selling programmable chips.

In addition to the current chip manufacturers, also a new entrant could start producing programmable chips. According to expert interviews, the biggest effort in manufacturing such chips is in the IC design that includes both an analog radio-frequency part and a digital part. The IC design projects of modern Gen-2 chips cost several millions of dollars and can last 2-3 years. However, these projects include many activities that would not be necessary for a manufacturer of programmable chips, most importantly optimization of the chip size and price. According to expert estimates, the minimum effort to make an IC design is in the range of hundreds of thousands of dollars and there are at least tens of semi-conductor foundries who could produce the chips.

We derive a rough estimate of what programmable chips could cost in small quantities. According to tag manufacturers, chip manufacturers sell modern Gen-2 chips around EUR 0.05 - 0.07 apiece today and the total price of the resulting RFID label would be around EUR 0.15 - 0.20 (in volumes of tens of thousands). This chip price includes the chip manufacturer's variable manufacturing cost per chip, fraction of the fixed costs like IC design (depreciation), and the chip manufacturer's profit. When manufacturing programmable chips in smaller quantities, the fixed costs (e.g. IC design and configuring wafer production line) are divided by a much smaller number of chips. In addition, assuming a less optimized IC design, the price per chip could be 10 to 100 times bigger than that of the

most popular UHF chips, and the resulting price of a single programmable RFID label would be around EUR 0.60 - 7.15.

C. Stealing unprogrammed chips

In theory, a wafer could be stolen early enough in the manufacturing process by an adversary who wants to write his own TID numbers on the chips. However, also this would require an investment in infrastructure to write the chips. Therefore this approach does not seem to be scalable. Furthermore, wafers are high-value articles that are tracked and traced both inside and outside the factories and therefore stealing them would neither be easy nor go unnoticed.

D. Tag impersonation devices

One option to bypass the TID check is to build a device that effectively emulates or imitates an RFID tag, without the need for IC manufacturing. This kind of device could fool the inspections if the tag is not seen during the check. This could be done in practice, for example, when pallets or cases of goods are verified by distributors or customs and the impersonation device is hidden inside the package. In addition, in case when the tag is not a label but a hard tag (encapsulated tag), the spoofing device could be built inside it (cf. figure 6). These kinds of encapsulated tags are used in applications requiring longer tag life cycle or tolerance for harsh conditions.

Achieving adequate functionality and performance for such a device is possible even with moderate effort and costs and without special equipment. The effort can be further decreased by using a UHF-tag hardware and software developer platform such as the WISP[2]. To illustrate the feasibility of an attack based on a tag impersonating device, we present our implementation and evaluate the implementation effort. A generic block diagram of such a device is illustrated in Fig. 5. The hardware blocks are described below.

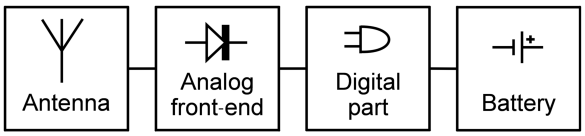

Fig. 5. Block diagram of semi-passive impersonation device

The antenna can be a simple half-wave dipole. It can be easily fabricated by anyone.

The analog front-end should be capable to detect the reader signal and to create backscatter modulation during reply. As the receiver does not need to be very sensitive or frequency selective, fairly unsophisticated structures can be used. A simple rectifier, envelope detector, and a comparator are enough [17]. More complex and better performing front-end designs can be found in the literature (e.g. [18]). Backscatter modulation can be done with a single transistor.

The digital part implements the actual communication protocol. The protocol description is publicly and easily available and protocol emulation can be implemented by using a microcontroller or a Field Programmable Gate Array (FPGA). This is the most challenging part and will be discussed later. The chip used for protocol emulation is also the most expensive component of such impersonation device.

The battery provides operating power for the digital part and the battery voltage can also be utilized to make the front-end more sensitive.

Implementing the protocol without prior knowledge naturally requires a serious effort. However, the communication protocol is open and standardized which makes it easily available for anyone and, demonstrably, the protocol emulation can be done (e.g. it is done in [17], [19], [20]). For example, the authors have successfully implemented the Gen-2 protocol in a microcontroller as a part of research in the BRIDGE project[3]. The used microcontroller is a very lightweight and inexpensive controller with a 8MHz clock rate. Due to the slow clock rate, all mandatory data rates are not supported by the prototype. The cost of the microcontroller is only few euros and the total bill of materials (BOM) is less than EUR 10. The prototype is shown in Fig. 6. Implementation of the protocol with supporting functions is mainly done in the C language. The total amount of source lines of code (SLOC) within the protocol implementation is around 2300. By using a basic COCOMO-model (*The COnstructive COst MOdel* [21]) with embedded project coefficients, the estimated man month (MM) effort for the implementation is around 10MM. These numbers roughly reflect the required effort for software based protocol implementation with a microcontroller.

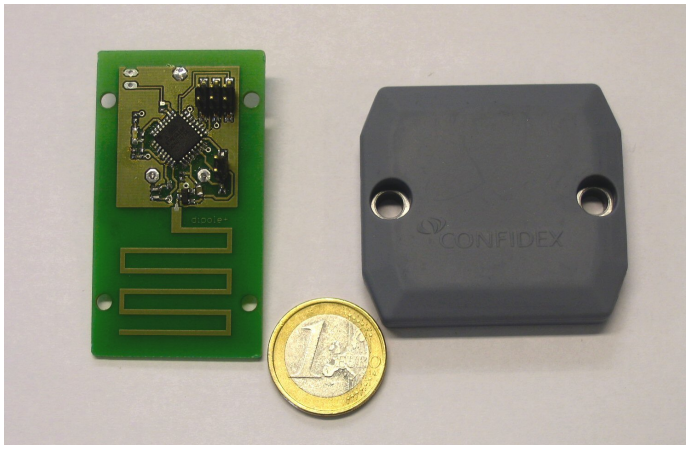

Fig. 6. Programmable semi-passive tag prototype (left) and a commercial encapsulated tag (right)

To achieve total conformance with the Gen-2 protocol, a faster and more expensive microcontroller should be used. The problem is to meet the timing requirements of the physical layer with higher communication data rates. However, a tag impersonation device does not necessarily need absolute com-

[2]http://www.seattle.intel-research.net/WISP/

[3]http://bridge-project.eu/

pliance with the standard since all features of the protocol are not likely to be needed in a basic TID check.

A tag impersonation device can also be implemented based on a Field Programmable Gate Array (FPGA) instead of a microcontroller. FPGA implementation is closer to a real hardware implementation and in general requires more effort with Register Transfer Level (RTL) code than a similar task in the C language and a microcontroller. Since the physical design can be omitted, it is still significantly less than a real application-specific integrated circuit (ASIC) design effort (cf. subsection III-B). The required speed should be easy to achieve with an FPGA so, in contrast to a microcontroller, higher data rates should not be a problem. Present Gen-2 chips include roughly 40000 transistors [22] which indicates that even a low-cost FPGA is sufficient to implement the same functionality. Prices of such FPGA chips start from ten euros. Also other "fixed" non-recurring engineering (NRE) costs are comparable to microcontroller implementation and are only a fraction compared to ASIC design NRE costs.

IV. Review of Gen-2 chip manufacturers

This section evaluates the possibility of buying Gen-2 chips with writable, not locked, TID memory by reviewing practices of major Gen-2 chip manufacturers. If buying such unprogrammed chips was possible, copying a serialized TID number would be as easy as copying an EPC number, and the cost to break would be the market price of such chip. The presented information is collected from interviews with the chip manufacturers and from public product catalogs, and the results are summarized in Table 1.

NXP: The currently available UHF chips from NXP include UCODE G2XM, UCODE G2XL, SL3 ICS1001, SL3 ICS3101, and SL3 ICS3001. All these chips have serialized write-protected transponder ID numbers already today. The tag identifier in the UCODE chips is 64-bit long and includes a 32-bit unique serial number. These TID numbers are written in the TID memory bank of the Gen-2 tags. NXP uses a 140 nanometer manufacturing process. The non-serial part of the TID numbers is not defined by the chip mask but it is programmed to the tag as well. The TID memory is locked by destroying bridges, that is connectors on the surface of the chips, after the TID numbers are written and the tags are tested on the wafer. This happens before cutting the chips from the wafer. After these bridges are destroyed, the TID write command no longer works and even the manufacturer cannot change the TID values. According to the company, NXP would not sell chips with programmable TID numbers to the market since it has been a reliable supplier for security products for years and has a reputation and a brand to maintain.

Impinj: The currently available UHF RFID chips from Impinj comprise Monza, Monza/ID, and Monza/64. Of these chips Monza/ID has a serialized 64 bit transponder ID that is factory-programmed and the other chips have only short, non-serialized TID numbers. The serial part of Monza/ID chip's TID memory is written in the user memory. The non-serial part is defined in the chip-mask and written as hard-wired ROM (cf. subsection II-B), and the serial part is permalocked using a lock-bit. Locking is done before cutting the chips from the wafer. In the near future, all UHF chips from Impinj will have serialized TID numbers.

Alien: The current UHF RFID chip ICs of Alien Technology include Higgs-2 (H2) and Higgs-3 (H3). H2 has a 32-bit non-serial TID written in ROM and an optional factory-programmed 32-bit serial number that is written on the chips if needed. Vast majority of the H2 chips in the market do not have serialized TID numbers because the market has only recently started to demand them. H3 chips have the serialized TID number as a standard feature and the company predicts that in two years all UHF chips they sell will have serialized TID numbers. The serialized TID numbers are written during the inlay production process and protected in a *foundry protect* process that disables the chip's internal commands for rewriting the TID memory. Alien uses a 160 nanometer manufacturing process.

TI: UHF Gen2 STRAP contains 32-Bit TID Memory (Factory Programmed and Locked). In HF products, TI has chips with 64-bit Factory Programmed Read Only Numbers. According to official documentation, the TID bank is permanently locked. TI uses a 130 nanometer manufacturing process.

ST Microelectronics: The current UHF RFID chip IC of ST Microelectronics is XRAG2. It has TID memory bank which can be programmed to store either the serialized 64-bit ISO TID number or the non-serialized 32-bit EPC TID number (cf. Fig. 1 and Fig. 2). To allow writing the TID numbers in both ISO and EPC formats, none of the TID memory is implemented as hard-wired ROM but it can be programmed by the chip manufacturer. The TID numbers are programmed and protected from rewriting while the chips are on the wafer. XRAG2 is manufactured using a 180 nanometer process.

This review suggests that all Gen-2 chips of the reviewed major chip manufacturers have permanently locked TID numbers. Moreover, the authors are also not aware of other companies selling unprogrammed chips. As a result, to the best of the authors' knowledge, it is not possible to buy chips with unprogrammed TID numbers today.

V. How much security is needed?

In this section we illustrate the financial incentives of counterfeiters in the tobacco industry so as to evaluate how much security (cost to break) is needed from a technical security feature. Cigarettes are the world's most widely smuggled legal products and accounted more than half of the 126 million counterfeit and pirated products that were seized by the European customs in 2006 [15]. To illustrate the vast size of the illicit tobacco market, the smuggler's market share is estimated to account for 15 percent [13] of the total USD 20 billion tobacco market in the UK [14]. More than half of the illicit cigarettes in the UK are counterfeits and the rest are diverted genuine products [13]. Assuming that illicit actors make their profit by not paying the taxes and duties that

TABLE I
SUMMARY OF AVAILABLE GEN-2 CHIPS AND THEIR TID NUMBERS

Chip	Company	Chip Model ID	Serial TID	TID Lock
Higgs-2	Alien	ROM	Optional	Yes
Higgs-3	Alien	ROM	Standard	Yes
Monza	Impinj	ROM	No	Yes
Monza/ID	Impinj	ROM	Standard	Yes
Monza/64	Impinj	ROM	No	Yes
UCODE G2XM	NXP	EEPROM	Standard	Yes
UCODE G2XL	NXP	EEPROM	Standard	Yes
SL3 ICS1001	NXP	EEPROM	Standard	Yes
SL3 ICS3101	NXP	EEPROM	Standard	Yes
SL3 ICS3001	NXP	EEPROM	Standard	Yes
UHF Gen2 STRAP	TI	ROM	No	Yes
XRAG2	ST M.	EEPROM	Optional	Yes
QR2233	Quanray	EEPROM	Standard	Yes

account for ca. 80% of cigarettes' sales price in the UK and given a sales price of USD 10 per pack, the illicit profit per pack would be around USD 8.

If single packs of cigarettes were tagged and the authenticity of a pack was verified by checking that the RFID tag has a correct serialized TID number, illicit actors would have a big financial motivation to buy or even to produce programmable RFID tags. The illicit actors' budget per one cloned tag could be several dollars and even more assuming that tagging would take place in higher aggregation levels such as for cartons of 10 packs. Carton level tagging could also introduce more opportunities for using tag impersonation devices (cf. subsection III-D). Furthermore, because of the vast size of the illicit market, also the investment that is needed in design and manufacturing of programmable chips (cf. subsection III-B) could be absorbed as a mere cost of doing business by the counterfeiters. The break-even from the initial investment in IC design could come after some hundreds of thousands of sold counterfeit packs. As a result, relying on TID checks does not appear to be secure enough as a long-term solution for the tobacco industry.

VI. DISCUSSION

End-users of Gen-2 tags need to understand that a serialized TID number is not a security feature – even though it can be used like one. The fact that serialized TID numbers provide a practical hurdle against chip cloning today is mostly based on the fact that programmable passive Gen-2 chips are not currently available. But there are no guarantees that this will be the case in the long term. The looming threat is that end-users will put too much confidence on TID checks, which would create potentially a major RFID security breach. Owing to the high level of automation that RFID provides, compromising the authenticity checks could lead to a wide scale exploitation – and an urgent market need for strong security features. However, we still believe that serialized TID numbers can be used in a smaller scale, as a partial and temporary solution against chip cloning when certain guidelines are respected.

As a result, the status-quo resembles a prisoner's dilemma (e.g. [30]) where the optimal strategy for all actors is to use the TID checks to benefit from the practical hurdle it provides, while hoping that nobody else makes use of it so that the incentive to produce programmable chips remains low. Hypothetically speaking, if TID checks will be used as a security feature by too many and in too many applications, the incentive to produce programmable chips for illicit purposes will grow so high that someone will do it, which will completely undermine for everybody the practical hurdle that TID checks provide.

The overview to current Gen-2 tags revealed that the serialized TID numbers of UHF chips are currently written in different memory banks and have varying lengths due to a lack of standards. This complicates applications that need to support different types of UHF chips since the reader does not know which kind of TID number is written on the chip, how long the TID number is, and where it is written in the chip's memory. As a result, an application that must read serialized TID numbers of different types of chips might need up to three read cycles to do it (identification of the AC identifier, identification of the Tag MDID / the Tag manufacturer ID, and identification of the tag serial number / serialized model number), increasing the read time. The upcoming EPC Tag Data Standard will ease the situation by specifying the serial number format, but it will probably take years until most tags on the market will conform to a unified format.

A. Analogy with MAC addresses

We can learn about the security of TID numbers also by drawing an analogy with the MAC (Medium Access Control) addresses of network cards. The MAC address is a serialized 48-bit integer that identifies all network cards. Hardware manufacturers purchase blocks of addresses from the IEEE Registration Authority and assign unique addresses to their cards. Every company is responsible for ensuring that every manufactured unit gets a unique address [3]. Various motivations to rewrite MAC addresses exist, for example, bypassing a mechanism that limits the use of software to authorized network cards, bypassing a restriction of Internet service providers that limit the use of a connection to one computer, and falsification of the source of Internet traffic.

Most network cards store the MAC address in a separate EEPROM chip that can be removed and reprogrammed using

off-the-shelf EEPROM programmer kits. There also exist software-based solutions to rewrite the MAC addresses of network cards [3]. In addition, it is possible to buy network cards with fully programmable MAC addresses[4]. Furthermore, in some cases it is enough to change the MAC address in higher levels of communication protocols.

From a technical point of view, changing the MAC address of a network card appears to be easier than changing the TID number of an RFID tag. First, reprogramming the memory where the MAC address is stored is substantially easier than tampering with the memory on RFID tags IC (cf. subsection III-A), when the MAC address is stored in a separate EEPROM chip that can be connected to a programming kit. Second, there are ways to program MAC addresses based on software, whereas there should be no mechanisms to rewrite the TID number after TID memory is permalocked. Third, compared to manufacturing passive RFID tags with programmable TID numbers (cf. subsection III-B), manufacturing network cards with programmable MAC addresses seems easier since it can be done using standard components.

B. Guidelines

This subsection consolidates the findings of this overview paper by proposing guidelines for the use of TID numbers in security applications.

1) Verify that the chips you intend to use have *serialized* TID numbers.
2) If your application needs to support for different chip models, reserve more time for the TID check. Since the serialized TID numbers of UHF chips (ISO or EPC) are currently written in different memory banks and have varying lengths, they must be read in multiple read cycles if the chip type is not known beforehand.
3) Do not create an illusion of perfect security. Serialized TID numbers are no real security feature and the protected items need also other security features.
4) Do not rely on TID in high value items. The higher the financial motivation for breaking the feature, the faster it will be done. In theory, if TID checks are only moderately used, the lifetime of TID as a security feature will be prolonged. Relying only on TID checks would create a lucrative opportunity for RFID crackers to produce fully programmable passive tags.
5) Avoid using TID checks when the tags cannot be physically inspected. An important part of protection is based on the fact that the TID number is written on an off-the-shelf passive RFID tag.
6) Have a serious migration plan to more secure measures (e.g. cryptographic tags, PUFs, and clone detection measures) and be ready to adopt them once TID checks are compromised. Since the authenticity checks are automated, security breaches can cause a great deal of harm before organizations have time to react.

[4]e.g. from http://www.sdadapters.com

VII. Related work

This section reviews related work. An up-to-date bibliography can be found from [24].

Koscher *et al.* [2] analyzed the weaknesses of TID-based tag authentication by discussing the threat of emulating of genuine tags with publicly available devices. Similar to this work, the authors concluded that the security of the serialized TID-scheme is overly optimistic in the long term. This work complements the analysis of Koscher *et al.* by quantifying the cost and effort to construct a tag imitation device, by analyzing all known vulnerabilities against the TID-scheme and by reviewing the status quo of both TID standards and the practices of the major Gen-2 chip manufacturers. In addition, we recognize that nothing prevents current and future chip manufacturers from selling chips with fully programmable TID numbers.

Serialized TID numbers are not the only way how low-cost RFID tags can be protected against cloning. Juels proposed ad-hoc techniques for authenticating Gen-2 tags based on two existing PIN-based commands, KILL and ACCESS [23]. The KILL protocol bases on the fact that even though the EPC of a tag can be maliciously scanned, the KILL-password remains secret. Cloned tags can be found by testing, but without killing the tag due to low reader power, if a tag's KILL password matches the one stored in a database. Koscher *et al.* [2] demonstrated that implementation of this technique is indeed feasible in deployed tags, but presents some delicate technical challenges.

Several tag-to-reader authentication protocols have been proposed in the literature, usually based on cryptographic primitives like bitwise operations and pseudo-random numbers (e.g. [25]) or hash-functions (e.g. [26]). Also different symmetric encryption-based tag authentication protocols exist, for example based on AES algorithm (e.g. [27]). Asymmetric encryption is currently very challenging on RFID tags but due to advances in elliptic curve cryptography (ECC) it is becoming feasible [28]. These approaches cannot be employed without hardware support from the chips and they might decrease the tag performance in terms of reading time and range. Another promising way to authenticate an RFID tag is to use a Physical Unclonable Function (PUF) [29] that is a one way function implemented using minimalistic hardware overhead.

VIII. Conclusions

This paper evaluates how serialized TID numbers of RFID tags can be used in security applications. Our findings confirm that serialized TID numbers currently provide a practical hurdle against cloning of Gen-2 chips since Gen-2 chips with programmable TID memory, to the best of the authors' knowledge, are not commercially available today. However, our working prototype demonstrates that a tag impersonation device can be built from less than ten euros worth of standard components to fool TID checks. As a result, we encourage end-users to make use of serialized TID numbers in applications where the tagged items can be physically

inspected as a temporal and complementary solution. Having said that, we discourage end-users to completely rely on TID checks because it could create a lucrative opportunity for manufacturing programmable chips that would completely undermine the practical hurdle that the TID scheme provides today. Overall, the biggest threat against this scheme relates to the commodification of RFID technology which is desired and somewhat inevitable. Therefore, serialized TID numbers do not appear to provide any sustainable long-term solution for tag cloning, but only a temporary solution before stronger tag authentication techniques.

ACKNOWLEDGMENT

This work is partly funded by the Auto-ID Labs and by the European Commission within the Sixth Framework Programme (2002-2006) projects BRIDGE (Building Radiofrequency IDentification solutions for the Global Environment), IP Nr. IST-FP6-033546, and SToP (Stop Tampering of Products), Nr. IST-FP6-034144. The authors would like to thank the anonymous reviewers and the following experts for their contribution: Manfred Aigner, Bill Brown, Matthew Brown, Srdjan Capkun, Ali Dada, Kalle Holma, Christophe Mani, Chris Segura, Mario Steiner, and Marc Witteman.

REFERENCES

[1] United States Department of Homeland Security: Privacy impact assessment for the use of radio frequency identification (RFID) technology for border crossings. http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_rfid.pdf (2008). Accessed 15 November 2008

[2] Koscher, K., Juels, A., Kohno, T., Brajkovic, V.: EPC RFID Tags in Security Applications: Passport Cards, Enhanced Drivers Licenses, and Beyond. Manuscript, RSA Laboratories, 2008.

[3] Grand, K.: MAC Address Cloning. http://www.netsourceasia.net/resources/mac_address_cloning.pdf (1998). Accessed 5 December 2008

[4] Asanghanwa, E.: Product Counterfeiting Made Easy. And Why it's so Difficult to Prevent. Atmel White Pape. http://www.rsaconference.com/uploadedFiles/RSA365/Security_Topics /Deployment_Strategies/White_Papers/Atmel/doc5280.pdf (2008). Accessed 15 November 2008

[5] Weingart, S.: Physical Security Devices for Computer Subsystems: A Survey of Attacks and Defense. In Cetin Kaya Koc and Christof Paar, editors, Proceedings of Cryptographic Hardware and Embedded Systems CHES 2000, volume 1965 of Lecture Notes in Computer Science, 302–317. Springer-Verlag (2000)

[6] Anderson, R. and Kuhn, M.: Low cost attacks on tamper resistant devices. IWSP: International Workshop on Security Protocols, LNCS (1997)

[7] Haythornthwaite, R., Nxumalo, J. and Phaneuf, M.: Use of the focused ion beam to locate failure sites within electrically erasable read only memory microcircuits. J. Vac. Sci. Technol. A 22.3., May/Jun (2004)

[8] Koemmerling, O. and Kuhn, M.: Design Principles for Tamper-Resistant Smartcard Processors. Proceedings of the USENIX Workshop on Smartcard Technology (Smartcard '99), Chicago, Illinois, USA, May 10-11, USENIX Association, 9–20 (1999)

[9] Poll, E: Smartcard attacks: invasive attacks. http://www.cs.ru.nl/ẽrikpoll/hw/slides/smartcards_invasive_attacks.pdf (2007). Accessed 5 December 2008

[10] Frmling, K., Tossavainen, T. and van Blommestein, F.: Comparison of the ID@URI (TraSer) approach with other systems. TraSer-Project White Paper (2007)

[11] EPCglobal: Class-1 Generation-2 UHF RFID Conformance Requirements. Version 1.0.2.

[12] EPCglobal: Class-1 Generation-2 UHF RFID Protocol for Communcation at 860 MHZ - 960 MHz. Version 1.1.0.

[13] HM Customs and Excise: Annual report 2003-2004. The Commissioners of HM Customs and Excise, London. (2004)

[14] Action on Smoking and Health: ASH Factsheet No:18 - The UK tobacco industry. http://old.ash.org.uk/html/factsheets/html/fact18.html (2007). Accessed 5 December 2008

[15] European Commission Taxation and Customs Union: Summary of Community Customs Activities on Counterfeit and Piracy. Results at the European Border 2006. http://ec.europa.eu/taxation_customs/customs/customs_controls/counterfeit_piracy/statistics/index_en.htm (2006). Accessed 5 December 2008

[16] Finkenzeller, K.: RFID Handbuck. 4th Edition. Carl Hanser Verlag (2006)

[17] Aigner, M., Plos, T., Feldhofer, M., Tutsch, C., Ruhanen, A., Na, Y., Coluccini, S., and Tavilampi, M.: D4.2.1 - Report on first part of the security WP: Tag security. BRIDGE project, no. 033546 (2008)

[18] Barnett, R., Balachandran, G., Lazar, S., Kramer, B., Konnail, G., Rajasekhar, S. and Drobny, V.: A Passive UHF RFID Transponder for EPC Gen 2 with -14dBm Sensitivity in 0.13m CMOS. Solid-State Circuits Conference 2007, ISSCC 2007. Digest of Technical Papers. IEEE International. 11-15 Feb., 582–623 (2007)

[19] Mitsugi, J.: Multipurpose sensor RFID tag. In APMC 2006 workshop on Emerging Technologies and Applications of RFID, WS04-4, 143–148 (2006)

[20] SecureRF Corporation: LIME Tag. www.securerf.com/pdf/-SecureRF_LIME_Tag_product_sheet.pdf (2008). Accessed 15 November 2008

[21] Center for Systems and Software Engineering: Basic COCOMO-model. http://sunset.usc.edu/csse/research/COCOMOII/cocomo81.htm (2008). Accessed 5 December 2008

[22] Roberti, M.: The Price of EPC Gen 2. RFID Journal. http://www.rfidjournal.com/article/articleview/1609/1/2/ (2005). Accessed 5 December 2008

[23] Juels, A.: Strengthening EPC Tags Against Cloning. In M. Jakobsson and R. Poovendran, eds., ACM Workshop on Wireless Security (WiSe), 67–76 (2005)

[24] Avoine, G.: Online bibliography: Security and privacy in RFID systems. http://www.avoine.net/rfid (2008). Accessed 5 December 2008

[25] Juels, A.: Minimalist cryptography for low-cost RFID tag. In: Blundo, C., Cimato, S. (eds.) International Conference on Security in Communication Networks SCN 2004. LNCS, Vol. 3352, 149–164, Springer, Heidelberg (2004)

[26] Avoine, G., Oechslin, P.: A scalable and provably secure hash based RFID protocol. In: IEEE International Workshop on Pervasive Computing and Communication Security, 110–114 (2005)

[27] Feldhofer, M., Aigner, M., Dominikus, S.: An Application of RFID Tags using Secure Symmetric Authentication. In: 1st International Workshop on Privacy and Trust in Pervasive and Ubiquitous Computing, 43–49 (2005)

[28] Hein, D., Wolkerstorfer, J., Felber, N.: ECC is Ready for RFID - A Proof in Silicon. Workshop on RFID Security (RFIDSec'08), Hungary, Budapest, July (2008)

[29] Devadas, S., Suh, E., Paral, S., Sowell, R., Ziola, T., Khandelwal, V.: Design and Implementation of PUF-Based "Unclonable" RFID ICs for Anti-Counterfeiting and Security Applications. In: IEEE International Conference on RFID 2008, 58–64 (2008)

[30] Axelrod, R.: Effective Choice in the Prisoner's Dilemma. The Journal of Conflict Resolution, Vol. 24, No. 1, 3–25 (1980)