# The Evolution of RFID Security

*As RFID technology progresses, security and privacy threats also evolve. By examining RFID's history, we can learn from past mistakes, rediscover successful solutions, and inspire future research.*

**Melanie R. Rieback, Bruno Crispo, and Andrew S. Tanenbaum**
*Vrije Universiteit Amsterdam*

Since its invention in the 1940s, RFID has been an obvious target for abuse. Wireless identification is a powerful capability, and RFID reveals both a physical object's nature and location. Anyone can easily gain unauthorized access to RFID data because they don't need a line of sight to gather it. For example, in the original RFID-based application—Identification Friend or Foe (IFF) systems—security breaches resulted in Allied planes being shot down.

A casual observer might think that the situation hasn't improved because despite concerns that RFID systems are open to abuse, it is now achieving wide deployment. RFID functions as a medium for numerous tasks including managing supply chains, tracking livestock, preventing counterfeiting, controlling building access, supporting automated checkout, developing smart home appliances, locating children, and even foiling grave robbers (www.rfidbuzz.com/news/2005/rest_in_peace.html). Pundits and activists warn that modern RFID systems could be used for a wide range of activities, from corporate security breaches to behavioral profiling to universal surveillance. Although this is true, it's important to remember that problems tend to inspire daring solutions. RFID and information security have been historically intertwined in a serendipitous marriage of technological progress. Attacks against original IFF systems provided the backdrop for the development of both classical and modern security techniques, ranging from signal jamming to challenge-response identification. It's also likely that RFID will continue to inspire progress in security and privacy research, as it has done for decades.

## RFID

To understand RFID technology's implications, you need a sense of where it came from and where it's going.

### Historical perspective

RFID's primary prerequisite was the advent of radio technology. Since Guglielmo Marconi first transmitted radio signals across the Atlantic in 1901, radio waves have been an important way to send messages—from Morse code to the first voice broadcast in 1906. Scientists also discovered that they could use radio waves for more than just message transmission.[1] In 1935, Alexander Watson-Watt showed how his new invention, radar, could use radio waves to locate physical objects.[2] Radar found its first big application during World War II, where it detected incoming aircraft by sending out pulses of radio energy and detecting the echoes that came back.[3] Radar energy's reradiation was a form of on-off modulation that indicated an aircraft's presence or absence.

However, radar operators still had no way to identify their own forces, presenting a major military weakness. (Some people hypothesize that the US could have prevented the attack on Pearl Harbor if its radar had been able to identify as well as detect. A Diamond Head, Hawaii, radar station


Published by the IEEE CS and IEEE ComSoc ■ 1536-1268/06/$20.00 © 2006 IEEE

allegedly spotted the incoming airplanes but dismissed them as American aircraft arriving from the mainland.[3])

The Germans attempted to solve the identification problem by simultaneously rolling their aircraft in response to a signal from the ground radar station. This would change the radar reflection's polarization, creating a distinctive blip on the radars. This crude system was the first demonstration of active RFID using electromagnetic backscatter.[3] The British responded by creating IFF, where long-range transponders actively modulated the reradiated ground radar signal so the aircraft itself didn't have to.[2] Parallel to these developments, Harry Stockman of the US Air Force Materiel Command published "Communications by Means of Reflected Power," the first public description of RFID technology.[4]

## Modern perspective

A half-century later, RFID systems hardly seem recognizable. Modern RFID tags, like other pervasive technologies (such as sensor motes), represent a culmination of the evolution toward wireless infrastructure and low-cost embedded computers. RFID tags are now the size of a grain of rice and have built-in logic (microchip or state machine), a coupling element (analog front-end with antenna), and memory (pre-masked or electrically erasable-programmable read-only memory) (see figure 1). Passive and semiactive tags use RFID readers' power to communicate, while active tags use battery power for greater range. You can typically read low-frequency tags (125–135 kHz) up to 30 cm away, high-frequency tags (13.56 MHz) up to 1 m away, ultra high-frequency tags (2.45 GHz) up to 7 m away, and active tags 100 m away or more.

Despite these modern features, RFID hasn't changed as suddenly as we think. Many of today's familiar RFID applications have roots deep in the past.

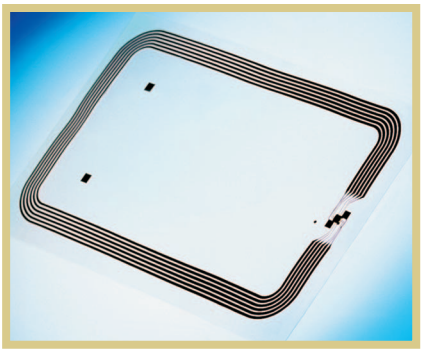
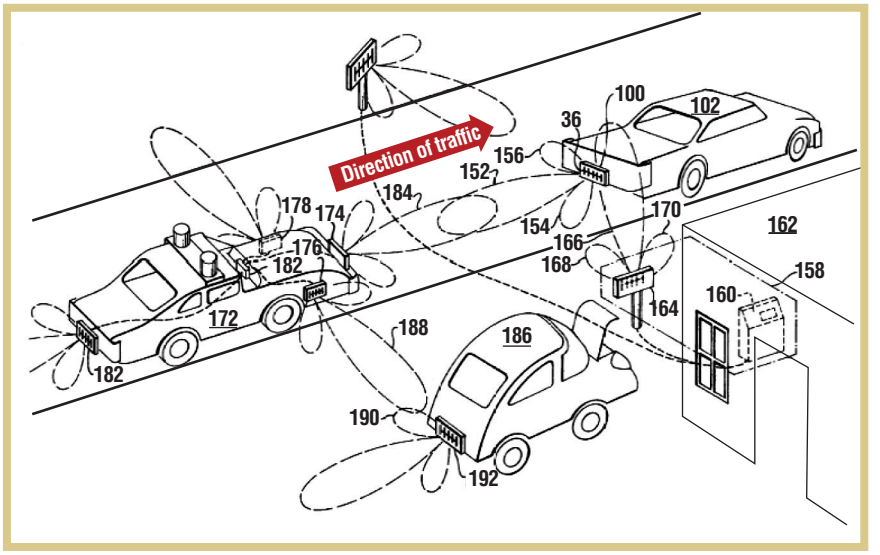


Figure 1. A Philips I.Code RFID tag. (figure courtesy of Philips Semiconductors)

***Supply chain management.*** Stores and libraries have used *electronic article surveillance*, a 1-bit form of RFID for theft control, since the 1960s. EAS tags indicate whether an item has been bought or properly checked out; a clerk will usually deactivate the tag at checkout. By extension, RFID tags are basically EAS tags augmented with additional data storage and processing. Low-cost RFID tags promise to expedite supply-chain processes, from moving goods through loading docks to managing the terabytes of data collected from these goods. The US Department of Defense and various retailers are already conducting RFID trials at the pallet, case, and item levels. Wal-Mart even issued a mandate requiring its top 600 suppliers to adopt pallet-level RFID tagging by January 2007 (www.rfidjournal.com/article/articleview/1930/1/9).

***Automatic payment.*** Automatic payment is another popular RFID application. Various industry sectors have conducted trials of RFID-enhanced cashless payment technology, from RFID-augmented credit cards and public transportation tickets to RFID-like Near Field Communication in consumer devices. Electronic toll collection using E-ZPass is widespread. The active E-ZPass transponder attaches to a car's windshield or front license plate; as the car drives over a toll road, the transponder sends account information to equipment in the toll collection lanes. The toll then automatically deducts from a prepaid account. Although customers consider the E-ZPass hip and modern, the technology was patented in 1977 (see figure 2) and has been deployed since the 1980s.

Figure 2. Car tracking with RFID-tagged license plates. (courtesy Fred Sterzer, US Patent 4001822)



***Access control.*** Contactless access control with RFID is popular for securing physical locations, such as office buildings and university campuses. Charles Walton first invented an RFID-based access control system in 1973. It involved an electronic lock that opened with an RFID key card. The passively powered key card, which Schlage sold for US$1.25, was a 36-square-inch circuit board loaded with chips and analog components. Today, RFID-based access cards are the size of a credit card and assist with policing border access. The US Department of Homeland Security and the International Civil Aviation Organization also plan to use passive RFID to police airport access. By 2015, the ICAO wants to replace all passports—approximately 1 billion—with digital passports that store encrypted biometric data on an RFID chip. The DHS also wants to use passive RFID to record who is entering or leaving the US across land routes.

***Animal tracking.*** RFID-tagged animals are already common. Applications vary from identifying runaway pets to tracking cattle from pastures to the grocer's freezer. Cows and chips first met in the 1970s in American microwave-based systems and European inductively powered systems (see figure 3). Since then, various parties have used RFID-based animal tracking to monitor cows, pigs, cats, dogs, and even fish to control outbreaks of animal diseases such as avian influenza ("bird flu") or bovine spongiform encephalopathy ("mad cow disease").

RFID has also been used to track people. Manufacturers have created wearable RFID wristbands, backpacks, and clothing to track prisoners, schoolchildren, and even the elderly. Applied Digital created an injectable RFID tag called the Verichip. This subdermal RFID chip stores personal data that can be read at venues as varied as nightclubs and hospitals.

Figure 3. Injecting a cow with an RFID tag, circa 1978. (photo courtesy of Matt Lezin)

***Other applications.*** RFID tagging lets physical objects be represented in cyberspace and entered into databases. Candidates include clothes (to be queried by smart washing machines), packaged foods (to be queried by smart refrigerators), medicine bottles (to be queried by smart medicine cabinets), rental cars, airline baggage, library books, banknotes, driver's licenses, employee badges, and even surgical patients (to avoid mix-ups). Both the opportunities and the threats are enormous.

### The evolution

Despite modern RFID's gradual evolution, comparing older RFID systems with modern RFID systems reveals several trends.

***RFID tag characteristics.*** RFID tags are both shrinking and multiplying. They're smaller, and there are more of them, especially in the supply chain. The proportion between active and passive tags is also changing; IFF and early RFID systems used mostly active tags, while most modern applications use passive RFID tags.

***Application characteristics.*** Today, RFID is used for much more than just identification. RFID tags have been reinvented as data-bearing devices. Accordingly, modern applications require network connectivity to permit the exchange of data with back-end management systems (which then necessitates the development of industry-wide standards for air interfaces and on-tag data formats). Another modern twist is that the desired RFID application functionality might change within a tag's lifetime. When an RFID tag changes hands, the new owner might consider the old function undesirable or even an attack—for example, tracking supply-chain RFID tags after a customer buys the tagged item.

***System perimeters.*** Modern RFID systems have no clear system perimeters. The users aren't well-defined, and RFID tag ownership has become less clear. With IFF, the military was always the owner. However, with modern RFID, an individual could own an RFID tag but a separate third party could own the tag's data (for example, the issuing government could retain sovereignty over the data on a digital passport).

## Security and privacy threats

Despite—or perhaps on account of—their myriad uses, RFID chips scare many people. Tags that optimize supply chains can also violate a person's privacy by tracking the tagged item's owner. Muggers with RFID readers could scan crowds for high-value banknotes. Terrorists could scan digital passports to target specific nationalities. And police could abuse a convenient new method of cradle-to-grave surveillance. As futuristic as these threats sound, they have precedent.

### Historical perspective

IFF has always been an attractive military target. Attacks against IFF systems can be classified into several categories.

***Sniffing and tracking.*** Analysts can examine IFF devices' operating characteristics using tools such as search receivers, pulse analyzers, and panoramic adapters.[5] This analysis allows the localization and tracking of airplanes using signals sent by their IFF transponders. In one incident during World War II, British Royal Air Force bomber crews mistakenly

Figure 4. Dispersing chaff from an airplane in WWII.

believed that their IFF systems had a jamming effect against the German Wurzburg-Riese radar system. Some bomber crews deliberately left their IFF turned on. The German air force then deployed the Freya Flamme system, which covertly interrogated the IFF transponders, to get range bearing and identification information for several RAF bombers at once.

***Spoofing.*** American and British military forces simulated enemy aircraft by dispersing large quantities of reflecting material into the sky. The most efficient material for this purpose was aluminum foil cut into strips of one-half the enemy radar frequency's wavelength. The British called these strips *window*, and the Americans called them *chaff*. Allied aircraft dispensed thousands of these foil dipoles on every flight over enemy territory. Additionally, the Allies sometimes sent up balloons towing strips of chaff (see figure 4).[5] (The German countryside became littered with chaff, which people used to decorate their Christmas trees.)

***Replay attacks.*** Friendly aircraft have been simulated by the use of decoy IFF transponders. Enemies would either steal authentic IFF transponders or program enemy transponders to imitate the characteristics of legitimate IFF identification signals. The Germans conducted a specialized spoofing attack where they recorded legitimate Allied IFF responses and played them back whenever the Allies challenged them.[6]

***Denial of service.*** IFF was affectionately nicknamed "reply or die" because radar operators considered an airplane an enemy if it couldn't send back correct IFF responses. To exploit that design decision, developers created counter-IFF jamming radars (such as the Jadwiga-4) that performed denial of service (DoS) attacks on IFF systems. These attacks were effective because they degraded pilots' ability to discriminate friendly from enemy aircraft, possibly causing friendly fire or hesitation to shoot down enemy aircraft.

## Modern perspective

In contrast to the high-budget military campaigns against early RFID systems, modern ones face less expensive attacks. As RFID is adopted for more applications, vandalism and other attacks against RFID will likely occur, stemming from temptation, dishonesty, civil disobedience, and a perverse sense of humor. But despite these differences, modern RFID security and privacy threats can still be grouped into familiar categories.

***Sniffing.*** RFID tags are indiscriminate—they're designed to be readable by any compliant reader. Unfortunately, this lets unauthorized readers scan tagged items unbeknownst to the bearer, often from great distances. People can also collect RFID data by eavesdropping on the wireless RFID channel. Unrestricted access to tag data can have serious implications; collected tag data might reveal information such as medical predispositions or unusual personal inclinations, which could cause denial of insurance coverage or employment for an individual.

***Tracking.*** RFID technology facilitates clandestine monitoring of individuals' whereabouts and actions. RFID readers placed in strategic locations (such as doorways) can record RFID tags' unique responses, which can then be persistently associated with a person's identity. RFID tags without unique identifiers can also facilitate tracking by forming *constellations*, recurring groups of tags that are associated with an individual. RFID technology also enables monitoring entire groups of people. UK workers' union GMB recently called on the European Commission to ban the RFID tagging of employees in the workplace. GMB accused employers of "dehumanizing" warehouse staff by forcing them to wear computers that track how long it takes to complete tasks with RFID tagged objects.[7] Civil liberties groups also warn that governments could monitor individuals' movements, eliminating anonymity in public places.

***Spoofing.*** Attackers can mimic authentic RFID tags by writing appropriately formatted data on blank RFID tags. For example, thieves could retag items in a supermarket identifying them as similar, but cheaper, products. Tag cloning is another kind of spoofing attack, which

produces unauthorized copies of legitimate RFID tags. Researchers from Johns Hopkins University recently cloned a cryptographically-protected Texas Instruments digital signature transponder, which they used to buy gasoline and unlock a DST-based car immobilization system.[8]

***Replay attacks.*** At least three researchers (Ziv Kfir, Jonathan Westhues, and Gerhard Hancke) have independently described or implemented RFID relay devices. Relay devices can intercept and retransmit RFID queries, which offenders can use to abuse various RFID applications. England's new RFID-enabled license plates, *e-Plates*, are one example of a modern RFID system that's susceptible to attack by a relay device. The active e-Plate tags contain an encrypted ID code that is stored in the UK Ministry of Transport's vehicle database. An attacker can record the encrypted identifier when another car's license plate is scanned and replay it later (perhaps to avoid paying the Congestion Charge when driving into central London).

***Denial of service.*** RFID systems only work when RFID tags and back-end databases are available. Thieves can exploit this to steal RFID-tagged items by removing tags from the items completely or by putting them in a foil-lined *booster bag* (that is, a Faraday cage) that blocks RFID readers' query signals and temporarily deactivates the items. (In 2001, the Colorado State Legislature made it a misdemeanor to make or wear aluminum underwear or to conceal its use to fool stores' theft-protection devices.) Another attack takes the opposite approach—flood an RFID system with more data than it can handle. Anti-RFID activists could remove RFID tags and plant them on other items, causing RFID systems to record useless data, discrediting and devaluing RFID technology.

### The evolution

Despite the similar threats facing IFF and RFID systems, modern RFID has acquired some unique qualities that influence security and privacy requirements.

***Attacker model.*** In the original military RFID systems, there was a clear delineation between attackers and defenders. Both were highly motivated and highly skilled, had abundant resources, and acted rationally to achieve a well-defined goal. With modern RFID systems, the delineation between attackers and defenders is fuzzy, and attackers are often opportunistic, unskilled, poorly financed, and even irrational. It's also difficult to answer the question, "Who is the enemy?" The definition of an attack against modern RFID systems isn't constant, given that the desired RFID tag functionality changes over time. Of course, classification difficulties in modern RFID systems also parallel the difficulties facing much of computer security today.

***Physical security.*** In the old days, airplanes (and their IFF devices) were largely physically secure. Planes fell into enemy hands only in the most extreme cases. In contrast, modern RFID tags are often "in enemy hands." (We can take this phrase literally when discussing subdermal RFID chips. Amal Graafstra, author of *RFID Toys*, implanted an RFID chip in his hand that automatically unlocks his front door). Consequently, most modern RFID applications can't achieve physical security because the chip owners are also the potential attackers—for example, the owner of a contactless smart card could try to increase the amount of money on the card.

***Security versus privacy.*** The military cares about security matters, such as the confidentiality of its intelligence, weapons, and logistics information. However, privacy is a nonissue; worse yet, surveillance and privacy loss are inherent to participation in the armed forces. In contrast, modern RFID tags suffer primarily from privacy threats. Security concerns haven't gone away—companies deploying RFID still must defend against security breaches. However, privacy violations have more far-reaching implications for consumers.

***Back-end infrastructure.*** The original IFF systems were stand-alone, so attacks usually affected only one airplane. In contrast, modern RFID transponders import all of RFID's weaknesses into a back-end digital infrastructure (such as databases and distributed middleware). This infrastructure necessitates using a cost-benefit analysis. As opposed to the militaristic view of "security at all costs," modern security analysts must now weigh the value of RFID return on investment against the cost (both monetary and reputation) of security and privacy violations.

***Social considerations.*** The controversy surrounding modern RFID introduces a social dimension that defines threats based on stakeholder perspectives. In World War II, soldiers died conducting or preventing DoS attacks on radar and IFF systems. With modern RFID, DoS isn't always considered an attack—sometimes it's a social defense. This perspective causes anti-RFID activists to place random RFID tags on objects throughout the city.

## Security and privacy solutions

World War II's electronic front was called the *Wizard War* for good reason. IFF-related security problems forced uniformed heroes to devise groundbreaking technological countermeasures. Modern RFID security solutions have partially evolved from this work. However, modern RFID poses special problems and constraints that will require academic

and industry researchers to show the same ingenuity as their predecessors.

## Historical perspective

We can classify IFF-related countermeasures into the following categories:

***Cryptography.*** The US Air Force drafted skilled cryptographers into the war effort, including Horst Feistel (best known for his work on the Lucifer and DES block ciphers). Feistel developed secure IFF devices during the 1940s and 1950s, including a system that mitigated German replay attacks. The system works as follows:

- IFF interrogators send a radio signal containing a random challenge to unidentified aircraft.
- Friendly planes encrypt the challenge and send the result back to the interrogator.
- The interrogator decrypts and validates the response.

Enemy planes can't replay recorded responses because subsequent encounters use a different challenge.[9]

Since the 1950s, Feistel's two-pass challenge-response scheme has withstood the test of time and has found numerous practical uses. The scheme also still distinguishes friendly from hostile aircraft in MK XII IFF systems today.[6]

***Detection and evasion.*** During World War II, both sides tried to locate enemy radars and jamming devices to take evasive or retaliatory action. Allied aircraft used *radar prediction devices*, relief maps of enemy territory that showed suspected radar locations. The RPD indicated weak detection or blind spots in the enemy radar beam, helping Allied aircraft escape detection.[5]

***Temporary deactivation.*** RAF bomber pilots in World War II learned the hard way that German attackers could track aircraft by their IFF transponders. But the solution was simple, according to US Colonel Walker "Bud" Mahurin. During the Korean War, he carried out attacks in Chinese airspace. One day, Mahurin was summoned to the Fifth Air Force Headquarters, where the commanding general reprimanded him for violating the China-Korea demarcation line. The general threatened him with a court martial—then quietly warned, "If you're gonna cross the Yalu, for god's sake, turn off your identification friend or foe system, because we can track you on radar."[10]

***Other techniques.*** The Allies used numerous other techniques to protect IFF devices against attacks. Frequency-hopping spread spectrum was a method to combat eavesdropping and signal jamming. Invented in 1942 by actress Hedy Lamarr and composer George Antheil, FHSS is a method of transmitting signals by rapidly switching a carrier among several frequency channels using a pseudo-random sequence both the transmitter and receiver know. Additionally, IFF equipment designers combated IFF transponder spoofing by giving IFF transponders a secret code; enemy forces couldn't use stolen IFF interrogation equipment without periodically entering this code.

## Modern perspective

In contrast to IFF systems, modern RFID imposes physical limitations for on-tag security mechanisms. Fifteen microAmps of power and 5,000 gates are typical for a 0.35-micrometer complementary metal-oxide semiconductor process.[11] To cope with these limitations, researchers have devised ultra lightweight cryptographic and procedural solutions, which we have categorized similar to the IFF-based solutions.

***Cryptography.*** Researchers have developed lightweight versions of symmetric key[11] and public key cryptography. RFID-specific authentication schemes have also sprouted up, some of which are lightweight, using techniques such as minimalist cryptography[12] and human-computer authentication.[13] Other schemes offload complexity to a back-end database, such as hash locks[14] and EPCglobal's proposed authentication servers (www.epcglobalinc.org/standards_technology/Final-epcglobal-arch20050701.pdf). One of the first RFID-specific authentication schemes to be widely deployed is the public-key-based Basic Access Control for digital passports.

***Detection and evasion.*** Consumers able to detect unauthorized RFID activity can also take their own evasive maneuvers. *C't* magazine's RFID Detektor (http://tinyurl.com/blfx4) and FoeBuD's Data Privatizer (https://shop.foebud.org/product_info.php/products_id/88) help users detect nearby RFID activity. Other devices, such as the RFID Guardian (www.rfidguardian.org), will interpret RFID scans and log their meaning. Customers can also perform more active RFID evasion by RFID blocking in either a distributed[15] or centralized[16] fashion.

***Temporary deactivation.*** Just as fighter pilots deactivated their IFF devices to escape detection, consumers can sometimes deactivate their RFID tags to avoid most modern-day threats. One temporary tag-deactivation method is using a Faraday cage, such as the RF-deflecting metallic sleeves that will be issued with digital passports. Researchers have also created on-tag mechanisms for tag deactivation. EPCglobal tags come with a password-protected kill function that permanently deactivates tags, and some more expensive tags might offer a password-protected sleep/wake function, which temporarily deactivates and then reactivates RFID tags.

***Other techniques.*** Numerous other techniques protect RFID devices from attacks. Similar to FHSS, periodically modifying RFID tag identifiers' appearance and data can prevent unauthorized tag access. RFID tags' pseudonyms consist of names that are periodically refreshed, either by trusted RFID readers[12] or an on-tag pseudorandom number generator. A mixnet of RFID readers can also periodically reencrypt tag data.[17]

### The evolution

Despite the similarities between IFF and RFID security solutions, some modern RFID characteristics can influence these solutions' feasibility.

***Application considerations.*** Cost and implementation size were never issues for IFF devices, but these factors now prevent our standard cryptographic tools from working. The difficulty defining enemies and attacks also complicates RFID security protocols' design, which always starts by establishing principles, assumptions, and goals. Also, modern RFID devices rarely have physical tamper resistance and tamper evidence; such qualities are expensive, and it's easier for attackers to use the wireless channel.

***On-tag cryptography.*** During World War II, the Allies used every technology possible against their enemy, including cryptography on IFF transponders. With modern-day RFID, cryptography's desirability is situation dependent. On-tag cryptography is generally desirable when replay, man-in-the-middle, and tracking attacks are a problem. For the rest, off-tag cryptography is usually sufficient for most data-privacy needs. Furthermore, on-tag cryptography is prohibitive when cryptography violates application requirements, such as power or cost constraints.

***Key revocation.*** In the early days, if someone stole an airplane, the army revoked the IFF key. Fortunately, this wasn't normal, so compromised keys were both infrequent and obvious. With modern RFID, it's difficult to know when RFID tag information has been compromised. Additionally, offline RFID use makes it difficult to communicate that information back to a centralized location, which can then pass the revocation information to other RFID deployments.

***Legislation.*** Legislation or self-regulatory guidelines wouldn't have helped prevent attacks against IFF systems during World War II. This stems from the fact that laws aren't respected much during wartime (not even the Geneva Convention). Modern RFID, however, requires a modest amount of legislation or industry guidelines to succeed. Without a regulatory mechanism, both lawmakers and the general public are likely to resist and reject RFID technology.

***Standardization.*** What ultimately prevented the Germans from deploying IFF systems was astoundingly low-tech—lack of standardization. Nazi technology policies were inconsistent and disorganized, resulting in inadequate unified standards. German engineers worked on IFF throughout the war but were unable to pool their efforts. They never developed an IFF transponder capable of being carried on an aircraft (www.vectorsite.net/ttwiz8.html#m2). With modern RFID standardization, ISO and EPCglobal have taken a leadership role. Other radio-specific issues also need to be coordinated nowadays, including radio spectrum allocation and preventing RFID-induced airwave congestion (the FCC/ETSI regulates the airwaves).

Revolutionary as it might seem, RFID technology is relatively old. Examining RFID and its threats historically lets us learn from past experiences and reuse old solutions. More important, looking back inspires us to devise new solutions to lead information security research into the future. P

## ACKNOWLEDGMENTS

The Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO) supported this work as project #600.065.120.03N17.

## REFERENCES

1. J. Landt, "Shrouds of Time: The History of RFID," 1 Oct. 2001; www.aimglobal.org/technologies/rfid/resources/shrouds_of_time.pdf.
2. "The History of RFID Technology," *RFID J.*, 20 Dec. 2005; www.rfidjournal.com/article/articleview/1338/1/129.
3. "Identification Friend or Foe IFF Systems: IFF Questions & Answers," *Dean Boys*, 20 Dec. 2005; www.dean-boys.com/extras/iff/iffqa.html.
4. H. Stockman, "Communication by Means of Reflected Power," *Proc. IRE*, Oct. 1948, pp. 1196–1204.
5. Dept. of Ordnance and Gunnery, US Naval Academy, "Chapter 16: Radar and Optics," *Naval Ordnance and Gunnery, Vol. 2, Fire Control*, 1958; www.eugeneleeslover.com/USNAVY/CHAPTER-16-A.html.
6. W. Diffie, "The First Ten Years of Public-Key Cryptography," *Proc. IEEE*, vol. 76, no. 5, 1988, pp. 560–577.
7. A. McCue, "Union Calls for European Ban on Staff-Tracking RFID," *silicon.com*, 19 Jul. 2005; http://hardware.silicon.com/servers/0,39024647,39150564,00.htm.
8. S. Bono et al., "Security Analysis of a Cryptographically-Enabled RFID Device," *Proc. 14th Usenix Security Symp.*, Usenix, 2005, pp. 1–15; http://spar.isi.jhu.edu/~mgreen/DSTbreak.pdf.
9. S. Levy, *Crypto: How the Code Rebels Beat the Government—Saving Privacy in the Digital Age*, Viking, 2001.

10. W. Mahurin, "Interview with Col. Walker 'Bud' Mahurin," 1997; www.acepilots.com/korea_mahurin.html.

11. M. Feldhofer, S. Dominikus, and J.Wolkerstorfer, "Strong Authentication for RFID Systems Using the AES Algorithm," *Cryptographic Hardware and Embedded Systems—CHES 2004—6th Int'l Workshop*, LNCS 3156, Springer, 2004, pp. 357–370.

12. A. Juels, "Minimalist Cryptography for Low-Cost RFID Tags," *Security in Communication Networks—Proc. 4th Int'l Conf.*, LNCS 3352, Springer, 2004, pp. 149–164.

13. A. Juels and S. Weis, "Authenticating Pervasive Devices with Human Protocols," *Advances in Cryptology—CRYPTO 2005—25th Ann. Int'l Cryptology Conf.*, LNCS 3621, Springer, 2005, pp. 293–308.

14. S. Sarma, S. Weis, and D. Engels, "RFID Systems and Security and Privacy Implications," *Cryptographic Hardware and Embedded Systems—CHES 2002—4th Int'l Workshop*, LNCS 2523, Springer 2002, pp. 454–469.

15. A. Juels, R.L. Rivest, and M. Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy," *Proc. 10th ACM Conf. Computer and Comm. Security*, ACM Press, 2003, pp. 103–111.

16. M.R. Rieback, B. Crispo, and A.S. Tanenbaum, "Keep on Blockin' in the Free World: Personal Access Control for Low-Cost RFID Tags," to be published in *Proc. 13th Int'l Workshop Security Protocols*, Springer, 2006; www.cs.vu.nl/~melanie/rfid_guardian/papers/sec_prot.05.pdf.

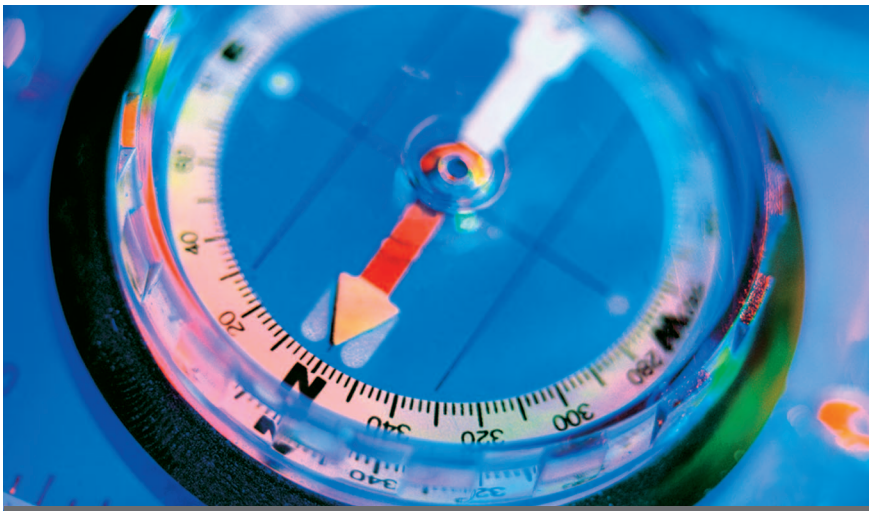
17. P. Golle et al., "Universal Re-encryption for Mixnets," *Topics in Cryptology—CT-RSA 2004*, LNCS 2964, Springer, 2004, pp. 163–178.

## the AUTHORS

**Melanie R. Rieback** is a doctoral student at the Vrije Universiteit Amsterdam in the Computer Systems Group. Her research interests include computer security, ubiquitous computing, and RFID. She received her MSc in computer science from the Technical University of Delft. Contact her at the Dept. of Computer Science, Vrije Universiteit Amsterdam, De Boelelaan 1081a, 1081 HV Amsterdam, Netherlands; melanie@cs.vu.nl; www.cs.vu.nl/~melanie.

**Bruno Crispo** is an assistant professor of computer science at the Vrije Universiteit Amsterdam. His research interests are security protocols, authentication, authorization and accountability in distributed systems and ubiquitous systems, and sensors security. He received his PhD in computer science from the University of Cambridge, UK. Contact him at the Dept. of Computer Science, Vrije Universiteit Amsterdam, De Boelelaan 1081a, 1081 HV Amsterdam, Netherlands; crispo@cs.vu.nl; www.cs.vu.nl/~crispo.

**Andrew S. Tanenbaum** is a professor of computer science at the Vrije Universiteit Amsterdam. His research interests are reliability and security in operating systems, distributed systems, and ubiquitous systems. He received his PhD in physics from the University of California, Berkeley. He's a Fellow of the IEEE and the ACM and a member of the Royal Dutch Academy of Sciences. Contact him at the Dept. of Computer Science, Vrije Universiteit Amsterdam, De Boelelaan 1081a, 1081 HV Amsterdam, Netherlands; ast@cs.vu.nl; www.cs.vu.nl/~ast.



Stay on Track

*IEEE Internet Computing* reports emerging tools, technologies, and applications implemented through the Internet to support a worldwide computing environment.

IEEE Internet Computing

www.computer.org/internet/

For more information on this or any other computing topic, please visit our Digital Library at www.computer.org/publications/dlib.