

EPC RFID Tag Security Weaknesses and Defenses: Passport Cards, Enhanced Drivers Licenses, and Beyond

Karl Koscher
University of Washington
Seattle, Washington, USA
supersat@u.washington.edu

Vjekoslav Brajkovic
University of Washington
Seattle, Washington, USA
balkan@cs.washington.edu

Ari Juels
RSA Labs
Cambridge, Mass., USA
ari.juels@rsa.com

Tadayoshi Kohno
University of Washington
Seattle, Washington, USA
yoshi@cs.washington.edu

ABSTRACT

EPC (Electronic Product Code) tags are industry-standard RFID devices poised to supplant optical barcodes in many applications. We explore the systemic risks and challenges created by the increasingly common use of EPC for security applications. As a central case study, we examine the recently issued United States Passport Card and Washington State “enhanced drivers license” (WA EDL), both of which incorporate Gen-2 EPC tags. We measure multiple weaknesses, including susceptibility to cloning, extended read ranges, and the ability to remotely kill a WA EDL. We study the implications of these vulnerabilities to overall system security, and offer suggestions for improvement. We demonstrate anti-cloning techniques for off-the-shelf EPC tags, overcoming practical challenges in a previous proposal to co-opt the EPC “kill” command to achieve tag authentication. Our paper fills a vacuum of experimentally grounded evaluation of and guidance for security applications for EPC tags not just in identity documents, but more broadly in the authentication of objects and people.

Categories and Subject Descriptors

K.6.5 [Management of Computing and Information Systems]: Security and Protection—*Authentication*; K.4.1 [Computers and Society]: Public Policy Issues—*Privacy, Abuse and crime involving computers*

General Terms

Security, Measurement

Keywords

Authentication, Cloning, EPC, Passport Card, RFID, WHTI

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

CCS’09, November 9–13, 2009, Chicago, Illinois, USA.

Copyright 2009 ACM 978-1-60558-352-5/09/11 ...\$10.00.

1. INTRODUCTION

EPC (Electronic Product Code) tags [17] are RFID devices poised to supplant optical barcodes in a wide variety of applications. Today EPC tags figure most prominently in the tracking of cases and pallets in supply chains. Proponents of the technology envision a future in which tagging of individual items facilitates a full life-cycle of automation from shop floors to retail points of sale, in home appliances, and through to recycling facilities.

As one example of this application, EPC tags are now seeing a landmark deployment in the U.S. in identity documents used at national border crossings. The United States Passport Card (also known as the PASS Card), a land-border and seaport entry document first issued in the summer of 2008, incorporates an EPC tag. This identity document was issued in response to the Western Hemisphere Travel Initiative (WHTI) [40], which, among others, phases out exemptions in document requirements for border crossing (previously, United States and Canadian citizens only had to present photo ID and a birth certificate). Certain states have issued or plan to issue Enhanced Drivers Licenses (EDLs), which are WHTI-compliant documents that will also make use of EPC. Washington State started issuing EDLs in early 2008 [29], with New York State following in September 2008 [1].

To date, the only form of EPC ratified as a technical standard by EPCglobal, the body that oversees EPC development, is the Class-1 Gen-2 tag. (For brevity, we refer to this tag simply as a “Gen-2” or “EPC” tag in this paper.) Passport Cards and other WHTI documents will incorporate this type of EPC tag, and it is likely to see the greatest use in barcode-type RFID applications as well for some time to come. EPC tags are attractive for their low cost (below ten U.S. cents each). Also, thanks to their operation in the Ultra-High Frequency (UHF) spectrum (860–960 MHz), they have a relatively long read range—tens of feet under benign conditions [34].

1.1 Our contribution: vulnerability analysis

The deployment of EDLs and Passport Cards at international borders is among the first and most prominent examples of the use of EPC RFID tags in security applications—of which many more examples may follow. We therefore use this opportunity to evaluate the use of EPC tags in the context of a real security application, with lessons, challenges, and results broadly applicable to other potential uses. We

emphasize a systemic approach, examining low-level security features and evaluating their significance in potential real-world deployment scenarios. Through the course of this research we have uncovered a number of attacks. We realize that not all of these attacks will be applicable all the time in the U.S. border crossing scenarios, but we feel that they may be applicable at some times if appropriate procedures are not in place, or may be applicable to other countries wishing to deploy similar technologies. The lessons learned from these attacks apply broadly to other potential uses of EDL tags in security applications.

Context. In its final rule on the Passport Card [2], the Department of State acknowledged objections expressed in response to its proposed rule of 2006 [3]; four Members of Congress expressed concerns about the security and privacy of the Passport Card. The Department indicated that many commenters did not understand “the business model that WHTI is designed to meet,” and cited a need for simultaneous reading of multiple EPC tags as a motivation for its choice of EPC (“vicinity read RFID”) as well as the technology’s amenability to passenger pre-processing, i.e., its relatively long read range. (Some “proximity-read” RFID devices, i.e., contactless smartcards, do not have these benefits, and some other classes of RFIDs only have the former benefit but not the latter.) The Department additionally noted that on May 1, 2007, the National Institute for Standards and Technology (NIST) certified the Passport Card as, “meeting or exceeding ISO security standards. . . and the best available practices for protection of personal identification documents.” Finally, the Department observed that Passport Cards will not carry personally identifiable information, and will be issued with protective, radio-opaque sleeves that help prevent unwanted scanning.

Our experiments: Cloning. In mid- to late-2008, we obtained a Passport Card and two Washington State EDLs for our experiments. We show first that the publicly readable data in both types of identity document can be straightforwardly cloned after a single read, despite the implication of protection mechanisms in [28]. Specifically, our analysis shows that Passport Cards and Washington State EDLs do not carry tag-unique, or even system-unique TIDs, but instead bear generic manufacturer codes. The Tag Identifier (TID) of an EPC, a tag-specific serial number that may be factory programmed, is often held forth as an anti-cloning mechanism for EPC tags. In its Privacy Impact Assessment of the Passport Card, the U.S. Department of Homeland Security (DHS) in fact highlights tag-specific TIDs as a “powerful tool” for anti-counterfeiting [28]. As Passport Cards and Washington State EDLs do not carry specially formulated TIDs, however, their readable contents are subject to direct copying into another off-the-shelf EPC tag.

Our observations about cloning only apply to a tag’s publicly readable data. Tags contain some private data in the form of PINs, which may be tag unique. Hence it is possible in principle (although improbable in our view) that a weak form of access-based authentication—an unorthodox security protocol we describe below—is in use at border crossings. In this case, reliable tag cloning would require either eavesdropping on a tag interrogation at the border or physically invasive attacks on a target identity document. Without ourselves eavesdropping on a tag interrogation at

a border crossing, we are unable to determine whether or not this technique is being deployed. We note, though, that access-based authentication is not an explicitly supported feature for EPC tags. The only reference to the technique of which we are aware is a research paper [19]. Other techniques, such as detection of unique radio fingerprints [13, 11] are also a possibility in principle, but have not yet been shown to work with EPC tags.

Our experiments: Readability. Given the ostensible vulnerability of identity documents and other Gen-2 EPC-tagged items to cloning, a key security issue is the range at which an EPC tag is subject to clandestine reading. As owners may be expected to carry their tags in any of a variety of different circumstances, we explore read ranges within several different physical environments.

We find that both Passport Cards and EDLs are subject to reading at a distance of at least 50 meters under optimal scan conditions (down a long hallway, but still operating within FCC limits). Surprisingly, although the human body—its constituent water, in particular—is known to interfere with EPC tag reading, we find that an EDL in a wallet near the body is still subject to scanning at a distance of at least two meters. We find that the Passport Card is not readable in a well maintained protective sleeve—although it is readable under certain circumstances in a crumpled sleeve. Most surprisingly, perhaps, we find that an EDL in a protective sleeve is readable at a distance of some tens of centimeters. To the best of our knowledge, our work here offers the first multifaceted characterization of EPC read ranges from the vantage point of privacy.

Our scanning experiments have a bearing not just on cloning, but also on owner privacy: While the tags do not contain personally identifiable information, they do contain unique serial numbers that can support clandestine tracking [20]. Of course, other wireless devices, like Bluetooth peripherals [18], 802.11 [14], and ANT [32], are similar in this regard, though the exposure for Passport Cards and EDLs may be greater due to their usage models, e.g., with U.S. citizens traveling abroad.

Other attacks. We also find evidence that EDLs are vulnerable to denial-of-service and covert-channel attacks. These vulnerabilities stem from issuance of cards without protection of the PIN for their tag-disablement feature, the “kill” command. Passport Cards do not have similar weaknesses. These flaws, along with EDLs’ heightened susceptibility to in-sleeve scanning, would seem to point to either a form of design drift in which technical protections implemented at the federal level did not benefit Washington State in the extension to EDLs, or the risks associated with implementing a technology before the precise security requirements have been finalized.

Ultimately, all of our experimental results, such as our observations of the failure to use card-specific TIDs or set the KILL PINs on tags, speak to the challenge of deploying even simple technologies—like EPC tags—in security applications.

1.2 Our contribution: countermeasures and recommendations

We emphasize that the security impact of tag vulnerabilities depends upon the operational environment. Copying

of a Passport Card or EDL does not automatically ensure successful use at a border crossing. The card is linked via a back-end system to a photo of its bearer which border agents use for confirmation of traveler identities. Hence, we discuss the systemic significance of the vulnerabilities we have identified.

We argue that Passport Cards and EDLs will play a role in the border-crossing process that may give impactful prominence to the data contained in the EPC tags. Like many security processes, the passenger screening process benefits from multiple layers of security, including physical inspection of passengers and documents. But as the EPC code can trigger a watchlist lookup, it serves as a frontline mechanism for passenger screening. The literature on cognitive biases suggests a risk that the EPC-layer of the security system will exercise undue influence over passenger screening [35, 33, 24, 10].

We argue that even if EPC-enabled identity documents provide adequate security at border crossings, they create a system with delicate dependence on well conceived and tightly executed border crossing procedures and card issuance. Our observations on the relative weakness of EDL in comparison with Passport Cards, for example, support the idea that states may not be as well equipped to enforce good security practices around document issuance as DHS, or that there was or is not sufficient guidance from the DHS.

Given these concerns, we study methods for improving the cloning resistance of EPC tags. We show that the elementary security features in EPC tags can be co-opted to help deter cloning. EPC tags include PIN-based protections both on tag disablement (“killing”) and modification of tag data contents. Previous research [19] proposed techniques for co-opting these features in the service of tag *authentication*, i.e., anti-counterfeiting, but offered no experimental evaluation. Given a few peculiarities of RFIDs, such as radio propagation dynamics, experimental evaluation is critical toward determining whether the approach in [19] is even feasible. We fill this gap here. We demonstrate that implementation of “kill” co-opting techniques is indeed feasible in deployed tags, but presents some delicate technical challenges. We explore some promising initial approaches to overcoming these challenges.

We believe that the lessons drawn from our case study in this paper will provide valuable guidance for the deployment of EPC tags in many security applications beyond border-crossing, such as anti-counterfeiting and secure item pedigrees for pharmaceutical supply chains [39].

1.3 Organization

In section 2, we briefly review related work on RFID security. We present our observations on the data format of the Washington State EDL and Passport Cards in section 3. We explore defensive techniques against cloning in section 4. We conclude in section 5 with a brief discussion of the broader implications of our findings.

2. RELATED WORK

There have been a number of radio-layer cloning attacks against RFID tags. Westhues developed a device called the Proxmark that he successfully used to clone both proximity cards [42] as well as the VeriChipTM [15], a human-implantable RFID tag. The devices targeted by Westhues emit static identifiers, i.e., they are essentially wireless bar-

codes. Class-1 Gen-2 EPC tags are similar in flavor to these devices, but operate in a much higher frequency band for which signal-processing is more complicated.

Bono et al. [7] reverse engineered and mounted brute-force key-cracking attacks against the Texas Instruments DST, a cryptographically enabled RFID device with short (40-bit) keys. Similarly, Nohl et al. [25] have recently reverse-engineered the Philips Mifare Classic RFID tag and revealed structural weaknesses in its cipher and random-number generator. Garcia et al. [12] demonstrated several additional, highly practical attacks against the MIFARE Classic card. Heydt-Benjamin et al. [16] demonstrated cloning attacks against first-generation RFID-enabled credit cards.

RFID tags saw their first prominent appearance in identity documents as additions to e-passports. Grunwald [27] cloned the chip in an RFID-enabled passport in the fullest sense, transferring the data from one chip to another. Juels, Molnar, and Wagner [21] evaluate the security implications of e-passport cloning. E-passports differ from Passport Cards in that they perform cryptographic authentication. The Smart Card Alliance, among others, noted the risks of EPC cloning in response to the initial DHS WHTI proposal [4].

Some commercial RFID tags include strong cryptography for challenge-response authentication. These tend to be relatively expensive and have constrained range. The literature is replete with techniques for implementing lower-cost cryptography in RFID tags. See, e.g., [20] for a survey and [6] for an up-to-date bibliography.

In view of the prevalence of Gen-2 EPC tags, Juels [19] proposed techniques for authenticating these tags using two existing commands, KILL and ACCESS. In section 4, we report on our implementation of these techniques and the practical challenges they pose.

For a more detailed discussion of how our results interact with the operational environment of Passport Cards and EDLs, please see the technical report corresponding to this paper [23].

3. EXPERIMENTAL EVALUATION OF PASSPORT CARD AND EDLS

3.1 Weakness in the TID-based anti-cloning mechanism

As mentioned above, EPC tags contain a data field known as the Tag Identifier (TID). At the discretion of the EPC manufacturer, this value may be factory programmed and locked, thereby ensuring that tags have permanent unique identities and (theoretically) cannot be cross-copied.

In its Privacy Impact Assessment (PIA) on the Passport Card [28], the United States Department of Homeland Security posits that:

...the risk of cloning RFID enabled cards and an impostor with similar physical features gaining illegal entry into the U.S., while unlikely, is real. Fortunately, 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.

However, the Gen-2 standard only requires that the TID identify the manufacturer and give enough additional information to determine the tag’s capabilities. In particular, two

classes of TIDs are defined: the $E0_h$ class, where the TID consists of a manufacturer ID and a 48-bit serial number, and the $E2_h$ class, which merely defines the manufacturer and model. The TID reported by our Passport Card is **E2 00 34 11 FF B8 00 00 02**, which corresponds to an $E2_h$ -class Alien Higgs tag. [26] states that the bytes after the manufacturer and model IDs (starting with **FF**) are Alien-specific configuration values. Using a new Higgs tag, we experimentally verified that the first three nibbles correspond to the tag’s lock configuration. The TID reported by our Washington State EDLs is **E2 00 10 50**, which corresponds to an $E2_h$ -class Impinj Monza chip.

To confirm that these TIDs do not confer anti-counterfeiting protection, we have cloned both a Passport Card and a Washington State EDL onto commercially-available, off-the-shelf tags from the same manufacturers as the originals. By *cloned*, we mean that the EPC and TID values are reported identically by the clone tags.¹ Additionally, we inferred the lock state of both card types and duplicated that as well. Provided that the Passport Card or Washington State EDL do not implement additional, undocumented functionality, the only contents that we were unable to clone were the ACCESS PIN on both cards, and the KILL PIN of the Passport Card. The TID therefore does not serve as the basic anti-cloning tool as envisioned by DHS. One explanation for this might be that (via personal communications) DHS indicated that they learned of the existence of tag-unique TIDs too late for incorporation into these cards.

We further maintain that the characterization of the full, tag-specific TID as a powerful anti-cloning tool is overly sanguine in the long term. While such tag-specific TIDs may prevent simple copying of one EPC into another, it does not prevent the *emulation* of an EPC tag in another radio device. In other words, the TID may (or may not) help prevent *physical* copying of an EPC tag, but it certainly does not prevent *logical* copying.² An ordinary RFID reader makes no distinction between a tag embodied in a flake of silicon and one emulated by a larger, more powerfully instrumented platform.

A number of general-purpose tag emulation platforms such as OpenPCD [30] and the RFID Guardian [31] already exist for HF tags. It is just a matter of time before similar tools emerge for Gen-2 EPC tags. The Intel WISP [36], for instance, is a physically compact RFID platform with a fully programmable microprocessor that operates in the UHF domain as a Gen-1 EPC tag. A version that simulates a Gen-2 EPC tag is available now as well. Thus, emulator devices are likely to be broadly accessible in coming years.

The decision to forego the security offered by the TID in the Washington State EDL and Passport Card thus increases the short-term risks of cloning, as it eliminates a basic protection against the straightforward copying of publicly viewable values into a fresh Gen-2 tag. In the longer

¹However, cloning a tag’s EPC and TID may not be sufficient for an adversary’s purposes; e.g., in some cases an adversary may also need to produce a false card itself.

²There are well documented, low-cost attacks against smart-cards, which possess tamper-resistance features well beyond those of EPC tags; see, e.g., [5]. It therefore seems probable that an attacker with modest resources can use physically invasive techniques to alter the data in an EPC tag. And if only one manufacturer makes Gen-2 tags available with programmable TIDs, they can act as clones for *any* manufacturer’s tags.

term, commercially-available emulator devices may reduce the protective value of tag-specific TIDs. That said, the TID may still have some longer-term value as a countermeasure to easy cloning of EDLs and Passport Cards into devices with the same form factor, i.e., Gen-2-equipped cards.

3.2 Other memory banks

Assuming the Gen-2 tags in the EDL and Passport Card are identical to the commercial, off-the-shelf tags indicated by their TID, the only read-protected pieces of memory on the cards are the KILL PIN on the Passport Card, and the ACCESS PIN on both. We have experimentally verified that the entire EPC memory bank (which contains the card’s unique EPC value) is readable, as is the TID memory bank. The Impinj Monza chip does not have a User memory bank, and the Alien Higgs-2 chip only uses a User memory bank when the KILL and ACCESS PINs are not used [26]. We have also verified that the cards report a “no such memory location” error when attempting to read words we do not expect to be present (such as the User memory bank).

3.3 Kill-PIN selection

The KILL PIN is unprogrammed and not locked on the Washington State EDLs. We have verified that we can directly write this 32-bit KILL PIN. We have not verified that we can in fact kill an EDL (an experiment that would be detrimental to its owner). We have verified our ability, however, to kill a cloned EDL with an identical Gen-2 tag model, an Impinj Monza, over the air. Thus, unless the Washington State EDL Gen-2 tag is specially manufactured—which seems unlikely, given the presence of a generic TID—it is subject to over-the-air killing by any reader.

Alternatively, an attacker can exploit the KILL PIN as a covert channel. She can set it as desired, thereby “marking” the EDL bearer with a 32-bit value accessible to any other reader.

3.4 Read-range experiments

To the best of our knowledge, prior to our work there has been no adversarial study of read capabilities for EPC tags—whether EDLs and Passport Cards or otherwise. Read ranges are, however, a major determinant of the vulnerability of an EDL or Passport Card to clandestine cloning attacks, as well as attacks against privacy. As explained above, a single scan of a tag in either type of identity document is sufficient to create a clone. In an attempt to mitigate resulting privacy concerns, the United States Department of State provides radio-opaque shielding sleeves with each Passport Card. These sleeves attenuate the distance at which a card may be read. Similarly, Washington State is making protective sleeves available to holders of its EDLs.

It is uncertain that EDL and Passport Card bearers will consistently use their protective sleeves. These documents require security hygiene beyond that of other commonly carried cards, demanding from bearers heightened vigilance and tolerance of inconvenience. The body of relevant literature on the psychology of fear appeals [41, 43, 8, 9] suggests that the abstract warnings accompanying EDLs and Passport Cards, e.g., the injunction on the Passport Card that, “Your Passport Card should be kept in its protective sleeve when not in use,” may be relatively ineffective in stimulating sleeve use. Additionally, as shown recently by King and Mcdiarmid [22], most bearers do not have accurate men-



Figure 1: The antenna inside a Washington State Enhanced Drivers License. Certain personally-identifiable information has been obscured.



Figure 2: The antenna inside a Passport Card. Certain personally-identifiable information has been obscured.

tal models of RFID privacy and security, and are therefore ill-equipped to make informed decisions about tag management.

The effective read ranges of protected and unprotected EDLs and Passport Cards in everyday environments therefore both have a strong bearing on the overall security of the border-crossing system, as well as on the privacy of people with these cards.

While deployers of Gen-2 EPC tags typically cite a reliable operational range of tens of feet [34], read ranges can vary considerably as a function of the material to which a tag is affixed, the configuration of the interrogating reader, the tag’s antenna, and the physical characteristics of the ambient scanning environment. We backlit and photographed both a Washington State EDL and Passport Card to examine their antennas, as shown in Figures 1 and 2.

We evaluated the read range of the Passport Card and Washington State EDL in several different physical environments, namely: (A) Indoors, freestanding, but with other objects nearby; (B) Indoors, in a corridor, with no other nearby objects; and (C) Outdoors in freespace. In all environments, we also evaluated various ways of carrying the cards, namely: (1) Held away from the body; (2) Inside a purse; both inside a wallet and in a side pocket; (3) In a



Figure 3: The sleeves used for our shielded distance tests. The crumpled sleeve is in the foreground, with the new sleeve behind it.

	New Sleeve		Crumpled Sleeve	
	EDL	PC	EDL	PC
Freespace	20 cm	N/R	29 cm	34 cm
Back wallet	27 cm	N/R	57 cm	N/R

Table 2: Maximum read range in a Secure SleevesTM shielded sleeve (N/R: No Reads)

backpack; (4) In a wallet in a back trouser pocket; (5) In a wallet in a front shorts pocket; and (6) Adjacent to a wallet in a front shorts pocket. The wallet contained 14 magnetic stripe cards, two non-magnetic stripe plastic cards, nine paper cards, and approximately six dollar bills.

To evaluate the effectiveness of radio-opaque protective sleeves, we measured the maximum read range in a variety of situations, namely: (i) In a new sleeve, held out by hand; (ii) In a crumpled sleeve, held out by hand; (iii) In a new sleeve, in a wallet in a back trouser pocket; and (iv) In a crumpled sleeve, in a wallet in a back trouser pocket.

We used Secure SleevesTM from Identity Stonghold, the manufacturer supplying sleeves for both the Passport Card and the Washington State EDL [37, 38]. The sleeves are shown in Figure 3. All shielded experiments were performed in the lab. We also experimented with the EDL in a sleeve obtained from the State of Washington and with the Passport Card in a sleeve obtained from Passport Services, and we report on these experiments as well.

To perform these experiments, we used an Impinj Speedway R1000 reader, with a Cushcraft S9028PCL circularly-polarized antenna. Effective radiated power of the antenna was 36 dBm, the maximum allowed by the FCC. The center of the antenna was 88 cm off the ground, and the cards were placed directly in front of the antenna. We measured the maximum distance at which we could read the cards when held in place for up to five seconds. We report these maximum distances in Table 1 (unshielded), Table 2 (shielded with the purchased Secure SleevesTM), and Table 3 (shielded with the sleeves provided for use with the respective cards).³

³In a few situations, we exhausted the space available to us in our experimental environment—i.e., backed ourselves into a wall—before we could find the maximum distance. These situations are denoted with a +.

Scenario	In Lab		In Hallway		Outdoors	
	EDL	PC	EDL	PC	EDL	PC
Freespace (Held Out in Hand)	530+ cm	530+ cm	4950+ cm	4950+ cm	788 cm	720 cm
Wallet in Purse	277 cm	528+ cm	1125 cm	276cm	586 cm	46 cm
Purse Side Pocket	528+ cm	528+ cm	4950+ cm	4950+ cm	833 cm	190 cm
Wallet in Back Pocket	253 cm	57 cm	193 cm	62cm	182 cm	58cm
Wallet in Front Pocket	270 cm	244cm	886 cm	65cm	240 cm	192cm
Next to Wallet in Front Pocket	417 cm	320 cm	4950+ cm	1137 cm	833 cm	580 cm
Empty Backpack	528+ cm	528+ cm	4950+ cm	4950+ cm	1050 cm	982 cm

Table 1: Maximum read range in a variety of situations

	New Sleeve		Crumpled Sleeve	
	EDL	PC	EDL	PC
Freespace	62 cm	N/R	63 cm	N/R
Back wallet	N/R	N/R	N/R	N/R

Table 3: Maximum read range in shielded sleeve provided for use with the specific cards

Remarks. An RFID tag has not a single read range, but in effect has multiple “read ranges,” depending on the operational scenario [20]. In a security context, the “eavesdropping range” is also of interest. This is the distance from which a rogue reader can intercept the reply of a tag to a legitimate, interrogating reader. Eavesdropping is feasible at a much greater distance than direct tag interrogation. Eavesdropping is also passive, undetectable by radio-monitoring devices. Eavesdropping on an EDL or Passport Card interrogation is sufficient to enable successful cloning as well as privacy attacks. We did not conduct experiments on the eavesdropping ranges for EDLs and Passport Cards, as these would require specialized firmware or equipment.

We finally note that some attackers may not be concerned about keeping their readers within FCC limits, and by increasing reader power, they may achieve even greater read ranges. Thus, the results here should be considered a lower bound on what is possible.

4. DEFENSIVE DIRECTIONS: BACKWARD-COMPATIBLE CLONING DEFENSES

The Class-1 Gen-2 specification has no explicit anti-cloning features [17]. For this reason, Juels [19] proposes the co-opting of two Gen-2 access-control commands for authentication of tags, summarized below. We focus this section on evaluating and extending these protection mechanisms for EPC tags in general, regardless of deployment scenarios. We then refine our focus on how to apply these general results to EDLs and Passport Cards in particular.

1. The KILL command. KILL is an EPC feature designed to protect consumer privacy by allowing tags to be disabled at the point of sale in retail environments. As a mandatory part of the standard, KILL is implemented (to the best of our knowledge) in all Class-1 Gen-2 EPC tags. When a tag successfully receives the KILL command along with a tag-specific 32-bit KILL PIN P_{kill} , it becomes permanently inoperative. Tag disablement, however, is a power-intensive operation. When a reader transmits the KILL command with power sufficient for the tag to respond, but

not to disable itself, the tag replies with a *Not Enough Power* response. In this type of low-power session, a side-effect is that the tag *also* indicates the correctness or incorrectness of the PIN transmitted by the reader.

Co-opting KILL for tag authentication. A reader with knowledge of P_{kill} can authenticate a tag by constructing an invalid PIN P'_{kill} and transmitting the pair (P'_{kill}, P_{kill}) in a random order across two low-power kill command sessions. A valid tag will acknowledge the correct PIN and reject the incorrect PIN; an invalid one can respond correctly with probability at most $1/2$. We refer to this idea as *KILL-Based Authentication* (KBA).

While a detection probability of $1/2$ is not high for an individual tag, it is high enough for detection of cloning on a systemic basis. Also, by transmitting $N - 1$ spurious PINs and one legitimate one, at a linear cost in authentication time, a reader can boost its probability of detection of an invalid tag to $1 - \frac{1}{N}$.

The challenge of KBA, and the one we investigate below, is the reliable transmission of commands in the low-power regime of a target tag. Too much power, and the tag will be killed.⁴ Too little, and the tag will not respond. To the best of our knowledge, KBA has remained a research proposal, and not yet seen empirical study. We fill this gap here.

2. The ACCESS command. EPC tags can carry secret data D with read-access control. Such data are readable only through use of the ACCESS command, with an accompanying tag-specific 32-bit PIN P_{access} . The KILL PIN itself is one such piece of read-protected data. Recall that the Passport Card we analyzed has both of these PINs set and locked. The Washington State EDL could have its KILL PIN set and locked over-the-air at the border (its ACCESS PIN is already set and locked).

Co-opting ACCESS for tag authentication. An entity with knowledge of P_{access} for a tag as well as D can authenticate the tag by checking D . An entity without knowledge of P_{access} cannot extract D without physically attacking the tag. This mode of authentication is a kind of one-time challenge-response that we refer to as *ACCESS-based authentication* (ABA).

We performed an experiment to determine whether ABA would impact read range. We used a new Impinj Monza tag

⁴As an alternative to power-calibration, [19] also proposes the manufacture of tags in which KILL always operates as if in the low-power regime, i.e., in which a manufacturer sacrifices KILL as a privacy feature in exchange for KBA.

for this experiment. We first determined the maximum read range of the tag outdoors (as in Section 3.4). We then programmed P_{kill} and P_{access} onto the tag, locked them against unsecured reading or writing, programmed the reader to use P_{access} to read P_{kill} , and again measured the maximum read range. For our particular tag, we found a maximum read range of 475 cm in both instances, suggesting that ABA should not significantly impact read ranges.

Variants are possible. For instance, without the presence of a secret D , a form of weak ABA is possible in which P_{access} is used in the same mode as KBA, i.e., tested through embedding in a set of spurious PINs. This weak ABA is the only form that would seem generally viable in today’s EDL/Passport Card infrastructure. Passport Cards carry secret data D in the form of P_{kill} , but EDLs, as noted above, do not have their KILL PINs set.

A stronger variant is possible as a form of crude rolling code created by overwriting D with a new random value D' on each authentication and storing this new value in a back-end system. (While an attacker could sniff D' and continue using a cloned card, once the legitimate card was read, the duplication of D' would be discovered.)

Advantages and limitations. Both KBA and ABA have advantages and disadvantages. KBA is of interest for two reasons. First, ACCESS is an optional command in the EPC standard, so tags need not support it. Second, it is possible to deploy the ABA and KBA independently. One entity can use P_{kill} to authenticate tags using KILL, but cannot perform tag cloning against a second, more privileged entity with knowledge of P_{access} . For example, P_{kill} might be revealed to state law enforcement officials, allowing them to authenticate tags (and kill them), but not to clone them.

Neither technique, of course, is resistant to eavesdropping. They are ad-hoc tools meant to allow authentication in the absence of cryptography or other supporting features. The most compelling feature of KBA and ABA (where available) is their backward compatibility. Neither requires any modifications to already deployed EPC tags. Finally, KBA, if not carefully implemented, may in some cases actually kill the cards as a side-effect.

4.1 Experiments with and extensions to KILL-based authentication

To evaluate the viability of KILL-based authentication (KBA) we explore the design space of possible KBA algorithms. As we have explained, the implementation challenge of a KBA algorithm is to calibrate the transmit power of a reader such that it can interrogate tags freely, but does not give the tags enough power to kill themselves.

As a first step, we consider a simple algorithm in which a reader ramps up power until it receives a response from a tag. In particular, our implementation ramps up the reader’s power from 15 dBm to 30 dBm (the full range of our reader) in 0.25 dB increments (the minimum supported by our reader), transmitting a KILL command at each power level in turn. (Our antenna provides an effective 6 dB gain.) When the reader successfully receives a reply from the target tag, the power level is fixed. The reader then sends a total of N KILL commands, with $N - 1$ bogus PINs, and 1 real PIN. We tested this algorithm with a tag placed at distances of 40 cm to 200 cm from the antenna, in 10 cm increments. For our tests we set $N = 10$; we repeated the algorithm 10

Distance	Successful auths	Kills
40cm	0	10
50cm	6	2
60cm	9	1
70cm	7	0
80cm	9	0
90cm	6	0
100cm	10	0
110cm	8	0
120cm	10	0
130cm	9	0
140cm	9	0
150cm	9	0
160cm	8	0
170cm	9	0
180cm	7	0
190cm	9	0
200cm	9	0

Table 4: Simple KILL-based Authentication

times at each distance. All experiments were performed in a lab with the same setup that we used in our distance tests (see section 3.4). If despite the initial power calibration, a tag did not consistently respond across the authentication session, we treat the authentication attempt as unsuccessful. We report the number of successful authentications and unintentional KILLS in Table 4.

The simple power-ramping algorithm unfortunately has a notable weakness: If the tag is too close, the reader power cannot be adjusted to a low enough level to avoid killing it. These unintended kills aside, the algorithm proves fairly robust, successfully authenticating tags a majority of the time. (In practice, of course, authentication could be repeated if unsuccessful.) A reader with support for lower-power emission could in principle support shorter-range KBA.

A good KBA algorithm should be robust enough to support a wide variety of reader characteristics. We therefore developed a more sophisticated KBA algorithm that tries to avoid unintentional kills by ensuring a sharp separation between the power levels required for read and write operations and carefully calibrating its power between these two levels. We refer to this algorithm as *scaled KBA*. Scaled KBA involves a calibration phase with five steps:

1. By means of power ramping, determine the minimum reader power level PWR_R required to read the target tag.
2. By means of power ramping, determine the minimum reader power level PWR_W required to write to the tag.
3. Verify the availability of minimum margin $PWR_W - PWR_R \geq \mu$, where μ is a minimum power-margin parameter. If not, abort.
4. Scale the reader’s power level within the range $PWR_R + \delta(PWR_W - PWR_R)$, for $\delta \in [0, 1]$.⁵
5. Ensure that the power level selected doesn’t allow a tag to write to itself.

⁵Of course, more sophisticated scaling functions are possible.

Distance	Auths	Margin Failures	Write Test Failures	Kills
10cm	0	100	0	0
20cm	0	99	1	0
30cm	0	100	0	0
40cm	0	100	0	0
50cm	0	99	1	0
60cm	98	0	0	0
70cm	91	5	0	0
80cm	96	1	0	0
90cm	91	0	0	0
100cm	88	4	7	0
110cm	63	18	14	0
120cm	58	29	12	0
130cm	62	8	2	1
140cm	50	43	4	1
150cm	84	2	2	2
160cm	83	4	7	0
170cm	88	2	0	0
180cm	89	0	0	0
190cm	89	2	0	0
200cm	83	10	4	0

Table 5: Scaled KILL-based Authentication

Note, however, that steps 2 and 5 require writing to the tag. One option is to temporarily overwrite part of the tag’s EPC value. We used this technique and performed these tests with our own tags. This technique will not work on cards where all memory is permalocked read-only (such as the Passport Card).

After some cursory tuning, we adopted $\mu = 2dBm$ and $\delta = 1/4$ in our experiments. As in the simple KBA algorithm, we incremented the power of the reader from 15 dBm to 30 dBm in 0.25 dB increments, and let $N = 10$. We evaluated this algorithm at distances from 10 cm to 200 cm from the antenna, in 10 cm increments.

We executed the scaled KBA algorithm 100 times at each distance. Table 5 reports the number of successful authentications at each distance. We also report authentication failures due to detection of a power margin below μ , to a failed write test (where the the tag’s EPC value is temporarily changed when it shouldn’t be), or to an accidental kill. Other authentication failures occur when the tag fails to respond with an “insufficient power” code on the correct PIN. This can be caused by a number of factors, from RF noise, or to the tag not having enough power to correctly execute its state machine. These results are summarized in Table 5. In Table 6, we report reader power measurements. For 100 iterations of scaled KBA, we list the mean minimum read and write power levels found, as well as their standard deviations. In Table 7, we report timing results. The mean time to determine the minimum read and write power levels, and to perform the write and authentication tests, are reported.

We see that the scaled KBA algorithm achieves its objective of reducing (and seemingly eliminating) unintentional kills at short range. Table 6 informs us that if the minimum read level is above 16 dBm, there is always at least a 2 dB margin between the mean minimum read and write power levels.

Distance	Mean Min. Read Power	SD Min. Read Power	Mean Min. Write Power	SD Min. Write Power
10 cm	15.3	0	15.0	0.0
20cm	15.3	0	15.0	0.2
30cm	15.3	0	15	0
40cm	15.3	0	15	0
50cm	15.3	0	15.1	0.1
60cm	15.3	0.1	17.1	0.2
70cm	15.7	0.9	17.7	0.8
80cm	15.3	0.4	17.6	0.4
90cm	15.6	0.4	17.9	0.4
100cm	17.7	0.9	20.1	0.8
110cm	18.0	0.9	20.3	0.9
120cm	21.2	1.3	22.9	1.3
130cm	20.4	1.3	22.8	1.2
140cm	22.3	1.6	24.7	1.5
150cm	19.8	0.8	22.5	0.8
160cm	20.0	1.0	22.4	0.8
170cm	19.6	0.8	22.4	0.7
180cm	21.8	0.5	24.8	0.5
190cm	18.7	0.6	21.4	0.6
200cm	21.6	0.8	24.6	1.1

Table 6: Scaled KBA Power calibration results (All measurements are in dBm)

Distance	Mean Read Calib. Time	Mean Write Calib. Time	Mean Write Test Time	Mean PIN Test Time
10cm	374 ms	73.0 ms	N/A	N/A
20cm	384 ms	75.7 ms	N/A	N/A
30cm	352 ms	70.9 ms	N/A	N/A
40cm	383 ms	74.8 ms	N/A	N/A
50cm	376 ms	84.8 ms	N/A	N/A
60cm	392 ms	343 ms	334 ms	44.7 ms
70cm	422 ms	361 ms	435 ms	54.1 ms
80cm	411 ms	383 ms	352 ms	45.1 ms
90cm	435 ms	395 ms	453 ms	50.7 ms
100cm	403 ms	408 ms	636 ms	73.7 ms
110cm	399 ms	355 ms	594 ms	77.7 ms
120cm	378 ms	314 ms	580 ms	67.7 ms
130cm	401 ms	409 ms	586 ms	51.3 ms
140cm	385 ms	304 ms	576 ms	63.4 ms
150cm	389 ms	420 ms	542 ms	87.8 ms
160cm	396 ms	422 ms	532 ms	53.3 ms
170cm	388 ms	455 ms	523 ms	57.2 ms
180cm	373 ms	461 ms	540 ms	49.8 ms
190cm	378 ms	396 ms	469 ms	52.8 ms
200cm	379 ms	413 ms	547 ms	53.2 ms

Table 7: Scaled KBA Timing Results

The scaled KBA algorithm does, however, produce a small rate of unintentional killing in the range of 130–150cm. The reason is unclear. (Multipath effects, for instance, can introduce unpredictable phenomena into wireless environments.) In well controlled physical environments, e.g., in an “authentication chamber” at a border crossing, however, we believe it would be possible largely to eliminate the power fluctuations that cause unintentional killing. Indeed, in such environments, the simple KBA algorithm might itself be effective. Reducing N or disregarding failed responses to spurious PINs, with an appropriate adjustment in authentication confidence, would also be advantageous.

Another potential approach to the problem of unintentional killing is to constrain the power delivered to a tag by modifying the reader protocol. In particular, we suspect that an abrupt cutting of a reader’s emission in the course of a KILL command might put a tag reliably in the low-power regime. Such approaches, however, would require modification to reader firmware and/or hardware. We therefore reserve them for future work.

In summary, our experiments show that KBA authentication is viable, and an attractive complement or alternative to ABA for off-the-shelf EPC tags.

Remark. As we have noted, the write operation is not a mandatory feature in Gen-2 tags. Our scaled KBA algorithm, however, only attempts authentication when the minimum power level is above 16 dBm. Thus for tags that do not support the write operation, a variant of our simple KBA algorithm that first checks that the minimum read-power level is 16dBm may be reasonable. If we return our focus from an investigation of EPC anti-cloning techniques in general to the Passport Cards in particular, then since Passport Cards are permalocked read-only, this variant seems the most promising approach if KBA is to be integrated.

5. CONCLUSION

In this paper, we have explored the issue of cloning in what could well become the most widely deployed radio device on the planet, the Class-1 Gen-2 EPC tag. As a point of departure and example, we have focused on deployment of these RFID tags in Passport Cards and Enhanced Drivers Licenses. We have shown that radio-layer cloning is a straightforward matter, but that the implications in the operational setting of border control are themselves somewhat more complicated.

The lessons we have gleaned here on cloning and anti-cloning extend well beyond EDLs and Passport Cards to EPC deployment wherever cloning or counterfeiting poses a risk. For example, with the encouragement of government regulators, the pharmaceutical industry is embracing EPC for tracking and anti-counterfeiting at the prompting of the United States Food and Drug Administration [39], foreshadowing the technology’s broad industry use as a security tool. Indeed, counterfeiting of consumer goods is a risk in nearly every industry. Thus the facts, observations, lessons, and new defensive directions that we have presented are of general interest in EPC deployments.

6. ACKNOWLEDGMENTS

We thank Garret Cole, Alexei Czeskis, Christina Drummond, Cynthia Matuszek, Kyle Rector, and Evan Welbourne

for their invaluable help with the experiments. We also thank the State of Washington, the United States Department of Homeland Security, the United States Department of State, and our anonymous reviewers for providing feedback on an earlier version of this paper. This work was supported in part by NSF Awards CNS-0722000, CNS-0722004, and CNS-0846065, a gift from EMC, and an Alfred P. Sloan Research Fellowship.

7. REFERENCES

- [1] New York to offer enhanced driver’s license. *Newsday*, 16 September 2008. Referenced October 2008 at <http://www.newsday.com/services/newspaper/printedition/tuesday/news/ny-nylice165845220sep16,0,5665783,print.story>.
- [2] Card format passport; changes to passport fee schedule [final action]; 22 CFR parts 22 and 51. *Federal Register*, 72(249):74169–74173, December 31, 2007. Referenced 2008 at <http://www.gpoaccess.gov/fr>.
- [3] Card format passport; changes to passport fee schedule [proposed rule]; 22 CFR parts 22 and 51. *Federal Register*, 71(200):60928–60932, October 17, 2006. Referenced 2008 at <http://www.gpoaccess.gov/fr>.
- [4] Smart Card Alliance. Comments of the smart card alliance to the department of state federal register notice, “card format passport; changes to passport fee schedule,” 22 CFR parts 22 and 51, rin 1400-ac22, public notice 5558, 3 November 2006. Referenced 2008 at http://www.smartcardalliance.org/resources/pdf/Smart_Card_Alliance_Response_Passport_Card_Final.pdf.
- [5] R. Anderson and M. Kuhn. Tamper resistance – a cautionary note. In *Second USENIX Workshop on Electronic Commerce*, pages 1–11, 1996.
- [6] G. Avoine. Online bibliography: Security and privacy in RFID systems, 2008. Referenced 2008 at <http://www.avoine.net/rfid>.
- [7] S. Bono, M. Green, A. Stubblefield, A. Juels, A. Rubin, and M. Szydlo. Security analysis of a cryptographically-enabled RFID device. In P. McDaniel, editor, *14th USENIX Security Symposium*, pages 1–16. USENIX, 2005.
- [8] E. Borgida and R. E. Nisbett. The differential impact of abstract vs. concrete information on decisions. *Journal of Applied Social Psychology*, (7):258–271, 1977.
- [9] S. Breznitz. *Cry Wolf: The Psychology of False Alarms*. Lawrence Erlbaum Associates, 1984.
- [10] D. M. Caggiano and R. Parasuraman. The role of memory representation in the vigilance decrement. *Psychonomic Bulletin and Review*, 11(5):932–937, October 2004.
- [11] B. Danev, T. S. Heydt-Benjamin, and S. Capkun. Physical-layer identification of RFID devices. In *18th USENIX Security Symposium*, pages 199–214, 2009.
- [12] F. D. Garcia, P. van Rossum, R. Verdult, and R. W. Schreur. Wirelessly pickpocketing a Mifare Classic card. In *IEEE Symposium on Security and Privacy (S&P 2009)*, pages 3–15. IEEE, 2009.

- [13] R. Gerdes, T. Daniels, M. Mina, and S. Russell. Device identification via analog signal fingerprinting: A matched filter approach. In *Network and Distributed System Security Symposium (NDSS)*, 2006.
- [14] Marco Gruteser and Dirk Grunwald. A methodological assessment of location privacy risks in wireless hotspot networks. In *First International Conference on Security in Pervasive Computing*, pages 10–24, 2003.
- [15] J. Halamka, A. Juels, A. Stubblefield, and J. Westhues. The security implications of VeriChipTM cloning. *Journal of the American Medical Informatics Association (JAMIA)*, 13(5):601–607, November 2006.
- [16] T. S. Heydt-Benjamin, D. V. Bailey, K. Fu, A. Juels, and T. O’Hare. Vulnerabilities in first-generation RFID-enabled credit cards. In *Financial Cryptography*, pages 2–14, 2007.
- [17] EPCglobal Inc. Class 1 generation 2 UHF air interface protocol standard version 1.1.0. Referenced 2008 at http://www.epcglobalinc.org/standards/uhfc1g2/uhfc1g2_1.1.0-standard-20071017.pdf.
- [18] M. Jakobsson and S. Wetzel. Security weaknesses in Bluetooth. In D. Naccache, editor, *The Cryptographer’s Track at RSA*, volume 2020 of *Lecture Notes in Computer Science*, pages 176–191. Springer-Verlag, 2001.
- [19] A. Juels. Strengthening EPC tags against cloning. In *ACM Workshop on Wireless Security (WiSe)*, pages 67–76. ACM Press, 2005.
- [20] A. Juels. RFID security and privacy: A research survey. *IEEE Journal on Selected Areas in Communication*, 24(2), February 2006.
- [21] A. Juels, D. Molnar, and D. Wagner. Security and privacy issues in e-passports. In D. Gollman, G. Li, and G. Tsudik, editors, *SecureComm*, pages 74–88. IEEE, 2005. Referenced 2008 at <http://eprint.iacr.org/2005/095.pdf>.
- [22] J. King and A. Mcdiarmid. Where’s the beep?: security, privacy, and user misunderstandings of RFID. In *Useability, Psychology, and Security*, pages 1–8, 2008.
- [23] K. Koscher, A. Juels, T. Kohno, and V. Brajkovic. EPC RFID tags in security applications: Passport Cards, Enhanced Drivers Licenses, and beyond. Technical report. Available at <ftp://ftp.cs.washington.edu/tr/2008/10/UW-CSE-08-10-02.PDF>.
- [24] R. S. Nickerson. Confirmation bias: A ubiquitous phenomenon in many guises. *Review of General Psychology*, 2(2):175–220, 1998.
- [25] K. Nohl, D. Evans, Starbug, and H. Plötz. Reverse-engineering a cryptographic RFID tag. In *USENIX Security*, pages 185–193, 2008.
- [26] F. Nylander. Alien Technology Higgs Gen2 IC LoadImage command application note 1 for 96 bit EPC memory, revision 7, 14 December 2006. Referenced 12 Sept. 2008 at http://www.alientechnology.com/docs/Load_Image_Application_Note_1.pdf.
- [27] M. C. O’Connor. Industry group says e-passport clone poses little risk. *RFID Journal*, 9 August 2006. Referenced 2008 at <http://www.rfidjournal.com/article/articleview/2559/1/1/>.
- [28] United States Department of Homeland Security. Privacy impact assessment for the use of radio frequency identification (RFID) technology for border crossings, 22 January 2008. Referenced 2008 at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_rfid.pdf.
- [29] Washington State Department of Licensing. FAQ: EDL / ID, 2008. Referenced 2008 at <http://www.dol.wa.gov/driverslicense/edlfaq.html>.
- [30] OpenPCD project, 2008. Referenced 2008 at www.openpcd.org.
- [31] M. R. Rieback, G. Gaydadjiev, B. Crispo, R. F. H. Hofman, and A. S. Tanenbaum. A platform for RFID security and privacy administration. In *USENIX LISA*, pages 89–102, 2006. Current project information referenced 2008 at www.rfidguardian.org.
- [32] T. S. Saponas, J. Lester, C. Hartung, S. Agarwal, and T. Kohno. Devices that tell on you: Privacy trends in consumer ubiquitous computing. In *16th USENIX Security Symposium*, pages 55–70, 2007.
- [33] S.J. Sherman, K.S. Zehner, J. Johnson, and E.R. Hirt. Social explanation: The role of timing, set, and recall on subjective likelihood estimates. *Journal of Personality and Social Psychology*, 44:1127–1143, 1983.
- [34] Read range for Gen2 RFID in 2008? 40 feet. *RFID Update*, 14 August 2008. Referenced 2008 at <http://www.rfidupdate.com/articles/index.php?id=1656>.
- [35] L. J. Skitka, K. L. Mosier, and M. Burdick. Does automation bias decision-making? *Int. J. Human-Computer Studies*, 51:991–1006, 1999.
- [36] J. R. Smith, A. P. Sample, P. S. Powledge, S. Roy, and A. Mamishev. A wirelessly-powered platform for sensing and computation. In *UbiComp*, pages 495–506, 2006.
- [37] Identity Stronghold. Identity Stronghold’s Secure Sleeve to protect US Passport Card. Company news release. Referenced 11 September 2008 at www.identitystronghold.com.
- [38] Identity Stronghold. Washington State Enhanced Drivers License guarded by Identity Stronghold Secure Sleeve. Company annotation on news article. Referenced 11 September 2008 at www.identitystronghold.com/links.php.
- [39] C. Swedberg. All eyes on FDA for drug e-pedigree. *RFID Journal*, 2008. Referenced 2008 at <http://www.rfidjournal.com/article/articleview/4013/1/1>.
- [40] Bureau of Consular Affairs United States Department of State. Western hemisphere travel initiative (whiti) overview, 2008.
- [41] N. D. Weinstein. Perceived probability, perceived severity, and health-protective behavior. *Health Psychology*, 19:65–74, 2000.
- [42] J. Westhues. Hacking the prox card. In S. Garfinkel and B. Rosenberg, editors, *RFID: Applications, Security, and Privacy*, pages 291–300. Addison-Wesley, 2005.
- [43] K. Witte and M. Allen. A meta-analysis of fear appeals: Implications for effective public health campaigns. *Health Education and Behavior*, 27(5):591–615, 2000.