Unlocking doors from half a continent away: A relay attack against HID Seos

Sam Haskins and Trevor Stevado

Loudmouth Security
{sam, trevor}@loudmouth.io

January 19, 2023

Abstract

HID Global is a major vendor of physical access control systems. In 2012, it introduced Seos, its newest and most secure contactless RFID credential technology, successfully remediating known flaws in predecessors iCLASS and Prox. Seos has been widely deployed to secure sensitive assets and facilities. To date, no published research has demonstrated a security flaw in Seos. We present a relay attack developed with inexpensive COTS hardware, including the Proxmark 3 RDV4. Our attack is capable of operating over extremely long ranges as it uses the Internet as a communications backbone. We have tested multiple real-world attack scenarios and are able to unlock a door in our lab with a card approximately 1960 km away. Our attack is covert and does not require long-term access to the card. Further, our attack is generic and is potentially applicable to other protocols that, like Seos, use ISO/IEC 14443A to communicate. We discuss several mitigations capable of thwarting our attack that could be introduced in future credential systems or as an update to Seos-compatible readers' firmware; these rely on rejecting cards that take too long to reply.

1 Introduction

HID Global is one of the world's largest manufacturers of physical access control systems. Seos is its newest and most secure contactless (13.56 MHz RFID) credential technology [1], intended to replace cryptographically flawed legacy credentials such as iCLASS and Prox. It is used by governments, educational instituitions, and businesses to secure sensitive assets and facilities [2–4]. In this paper, we present a relay attack against Seos using inexpensive off-the-shelf hardware including the Proxmark 3 RDV4. Our attack works over the Internet, and enables unlocking Seos-protected doors from kilometres away with under a minute of (quite subtle) access to a legitimate card. We have successfully performed our attack over distances of up to ≈1960 km. The implications of our attack are serious; with a short period of incidental access to an authorized card, a threat actor could gain unauthorized entry to a protected facility located even as far away as another country. Our attack is sufficiently

covert for such access to conceivably be unknown to the legitimate carrier of the card.

We contacted HID Global to responsibly disclose our initial findings on December 9, 2022.

This paper is organized as follows. We start with an overview of the security properties of the legacy HID credential technologies that Seos is designed to replace. After briefly discussing previous results, we then present the design of our relay attack, the tools used, and an overview of the underlying transmission protocol used by Seos. Subsequently, we present the results of testing our attack in both lab and real-world conditions, and discuss the limitations. We then discuss further lines of research, related work, and provide concluding remarks.

2 Why a Relay Attack?

HID Seos is marketed as a secure replacement to legacy credential technologies, remediating flaws that compromise their security properties [1]. We briefly look at two older card technologies, proximity and iCLASS, and compare the protections they offer against those of Seos. Legacy low-frequency (125 kHz) proximity cards, a technology which was developed prior to HID's founding in 1991, offer no protection against cloning. These cards transmit their ID in plaintext, allowing interception by an attacker within range. With only a moment of access to a proximity credential, an attacker can clone its information onto a blank card. At time of writing, a card cloner is available for $41.50 on Amazon—it is clear that proximity cards are inappropriate for securing sensitive assets. As a secure replacement for proximity cards, HID introduced high-frequency (13.56 MHz) iCLASS in 2002 [5]. iCLASS cryptographically protects the exchange between credentials and readers using a proprietary LFSR-based cipher. Garcia et al [6] reverse engineered this cipher and discovered multiple flaws; they estimate that these flaws allow cloning a card within either 5 seconds or 1 day, depending on whether elite or standard keying is used (respectively).

Unlike proximity cards, Seos cryptographically protects information exchanged between the card and the reader. Further, it seems that HID learned an important lesson from Garcia et al's work: Seos uses AES/2TDEA [1] rather than iCLASS's proprietary cipher to protect messages. In abandoning security by obscurity, HID has significantly increased the strength of their system; we know of no weaknesses that would make it possible to clone a card. Instead, we turn to a relay attack model: we rely on a legitimate card and reader to generate all messages exchanged, but relay the messages between a card and reader that are not physically proximate to each other.

From an attacker's perspective, we acknowledge that a relay attack is less useful than an attack that allows cloning. It requires simultaneous action at both the card and reader to succeed. Despite this limitation, we believe that a relay attack is sufficient to compromise many real-world installations that use Seos to protect assets. At the beginning of our research, we came up with the following attack scenario, which we used to guide our efforts:

> A threat actor would like to gain access to a secure facility protected by Seos. Agent A sidles up next to an employee on public transit and covertly holds a relay device close to the employee's pass. Concurrently, Agent B approaches the

secure facility and briefly presents another relay device, connected to the first, to the reader. The reader flashes green, and the door opens.

We initially developed our attack under the assumption that the legitimate card and reader were located within the same city, i.e., within ≈20 km of each other. Ultimately, we were able to achieve successful results over much longer distances.

The Seos protocol is proprietary and not publicly documented. In particular, precise details on how the exchange between the card and reader is protected are unknown to us. The information we have about the Seos protocol is as follows:

1. A goal of the Seos protocol is to prevent a passive eavesdropper or man-in-the-middle from being able to learn information stored on the card (e.g., the card's unique ID).
2. A goal of the Seos protocol is to prevent an attacker from pretending to be a legitimately issued card, even with knowledge of its unique ID.
3. A goal of the Seos protocol is to be resistant to replay attacks. Capturing and replaying a successful authentication should fail.
4. In order for a reader to read a card, they must be "keyed" the same. Cards and readers can be standard-keyed or elite-keyed. Every standard-keyed reader can read every standard-keyed card, worldwide. Elite keys are installation specific; an installation's elite-keyed readers will be able to read that installation's elite-keyed cards and no other cards [7]. The exact nature of the key material that must be present on the readers and cards to support this scheme is unknown to us. HID's previous credential technology, iCLASS, also distinguished standard- and elite-keying and used a shared symmetric key for this purpose [6].
5. The overarching goal of the Seos protocol is to securely assert the physical presence of an original issued credential at time of authentication. Our relay attack compromises this goal.

As our relay attack is entirely agnostic to the contents of the messages relayed, it should work without modification regardless of the keying mechanism used, including any that may be introduced in the future.

3 Previous Results

Relay attacks are not a new concept and several attacks have been presented in the literature against various technologies. The ISO/IEC 14443A ("14a") standard [8], the underlying communications protocol used by Seos, was first introduced in 2001 (though it has been revised several times since, most recently in 2018). An early relay attack on 14a-based protocols was presented by Hancke in 2006 [9]. Hancke successfully relayed the Mifare Classic[1] protocol (commonly used for transit cards) over distances of 50 metres using purpose-built hardware (total cost $100). Hancke used a "cheap FSK RF link" to relay the messages;

[1] Given as "Mifare" in Hancke's paper—we disambiguate as additional Mifare standards have since been released.

our attack is able to use the public Internet and thus has a significantly longer range. We note that a relay attack is unnecessary against Mifare Classic as weaknesses in its Crypto-1 algorithm found since 2006 enable trivial card cloning [10, 11].

More similar to our attack is Sportiello and Ciardulli's [12] long distance 14a relay attack presented in 2013. They successfully relayed the ePassport protocol over a distance of ≈541 km over the public Internet. They used Android phones running then-current CyanogenMod as the fake reader and card; our attack by comparison uses Proxmark 3 RDV4s which are quite a bit smaller and covertly fit in the palm of a hand[2]. While similar in concept, our attack shares no code with Sportiello and Ciardulli's and was developed independently.

Seos cards were first released in 2012 [13], before Sportiello and Ciardulli's attack but long after the idea of relay attacks on 14a-based protocols was introduced in the literature. To the best of our knowledge, no public attacks against Seos (relay or otherwise) have been presented to date. At the beginning of our research, it was an open question whether HID introduced any effective countermeasures against relay attacks in the development of the Seos protocol. We have conclusively answered this question in the negative.

4 Methodology

At a high level, our attack receives the messages sent by the card and reader and retransmits them to the counterparty over the Internet (or another IP network). We use two Proxmark 3 RDV4s to talk to the real card and reader. Messages are then relayed over a wireless Bluetooth serial connection to a laptop computer where they are received by a Python script and sent over a WebSocket connection to the other side. The laptops may be run headless (e.g. lid closed and in a backpack) as no user interaction is required during the attack. As all of the messages come from a legitimate card or reader, the contents are guaranteed to be correct; the only way a reader can detect our attack is by observing timing differences. At the beginning of our research, it was an open question whether the readers we tested with would do so. We have discovered that the readers do reject excessive round-trip time to the card by default; there is however a way to trick them into waiting much longer for a response.

The Seos authentication protocol is built atop ISO/IEC 14443A [8], which defines the RF layer and transmission protocol. At the beginning of our research, we captured several traces of a card directly authenticating to a reader. Before any Seos protocol messages are sent, a series of standard 14a "handshake" messages are exchanged to set various communication parameters. These messages follow a request-response model initiated by the reader. The sequence of messages exchanged in this "handshake" is shown in Figure 1. At a conceptual level, the request/response pairs exchanged are:

1. The reader sends `WUPA` (Wake-Up Command Type A) and the card replies with `ATQA` (Answer To reQuest, Type A). The 14a standard suggests that `REQA` (REQuest Command, Type A) will be sent instead of `WUPA` in some cases, but we did not observe this with readers we tested.

[2]Depending on the size of the hand in question.

2. The anticollision loop begins. This mechanism is intended to prevent multiple cards from talking over each other. As we present at most one card to the reader at a time, this is not relevant to our attack. We discuss the case where the anticollision loop completes after one iteration, i.e., only one card is present.

   (a) The reader sends `ANTICOLL` and the card replies with `UID CLn`. In the `UID CLn` message, the card offers a unique ID (UID) to the reader. While other authentication schemes use this value, Seos does not—the reader will accept any value for the UID[3]. The real card ID is exchanged after the 14a "handshake" is complete, as part of the Seos protocol.

   (b) The reader sends `SELECT_UID` with the UID discovered above and the card replies with `SAK` (Select AcKnowledge).

3. The reader sends `RATS` (Request Answer To Select) and the card replies with `ATS` (Answer To Select). This sets up several important communication parameters. The `ATS` message is key to our attack and we discuss it in more detail below.

4. The reader sends `PPS` (Protocol and Parameter Selection) and the card acknowledges it with a message we call `PPSR` (PPS Response). This message is used to set additional parameters and the response is treated as a fixed opaque value by our relay attack.

After the initial 14a "handshake" is completed successfully, the card and reader begin to exchange Seos protocol messages.

A particularly important message sent from the card to the reader is the Answer To Select (ATS) message which contains interface byte TB(1) which codes the Frame Waiting time Integer (FWI) in its high nybble. This integer is used by the reader to calculate the Frame Waiting Time (FWT), which defines how long the reader will wait for a response from the card. The FWT scales exponentially with the FWI—increasing the FWI by 1 doubles the FWT [8]—and is calculated using Equation 1 (taken from the 14a standard), where fc is the (constant) carrier frequency:

$$\begin{gathered}(\mathrm{FWI} \in \mathbb{Z}^*) \wedge (0 \leq \mathrm{FWI} \leq 14) \\ \mathrm{FWT} = \left(256 \cdot \frac{16}{fc}\right) \cdot 2^{\mathrm{FWI}}\end{gathered} \tag{1}$$

Manipulating this value redefines how long the reader will wait for the card's response, up to a maximum of ≈4949 ms. As the initial standard 14a messages (including ATS) are sent in plaintext without any sort of signature or authentication tag, changes that we make will be accepted by the reader. By changing the TB(1) byte, we are able to make the reader wait longer for messages, enabling our relay attack. As some standard 14a messages are sent before ATS, the modified waiting time does not apply to them, so they cannot be relayed. We solve this by hardcoding them in the code running on the Proxmark. We include a high-level data flow diagram as Figure 2.

[3]Real Seos cards reply with a random value each time.

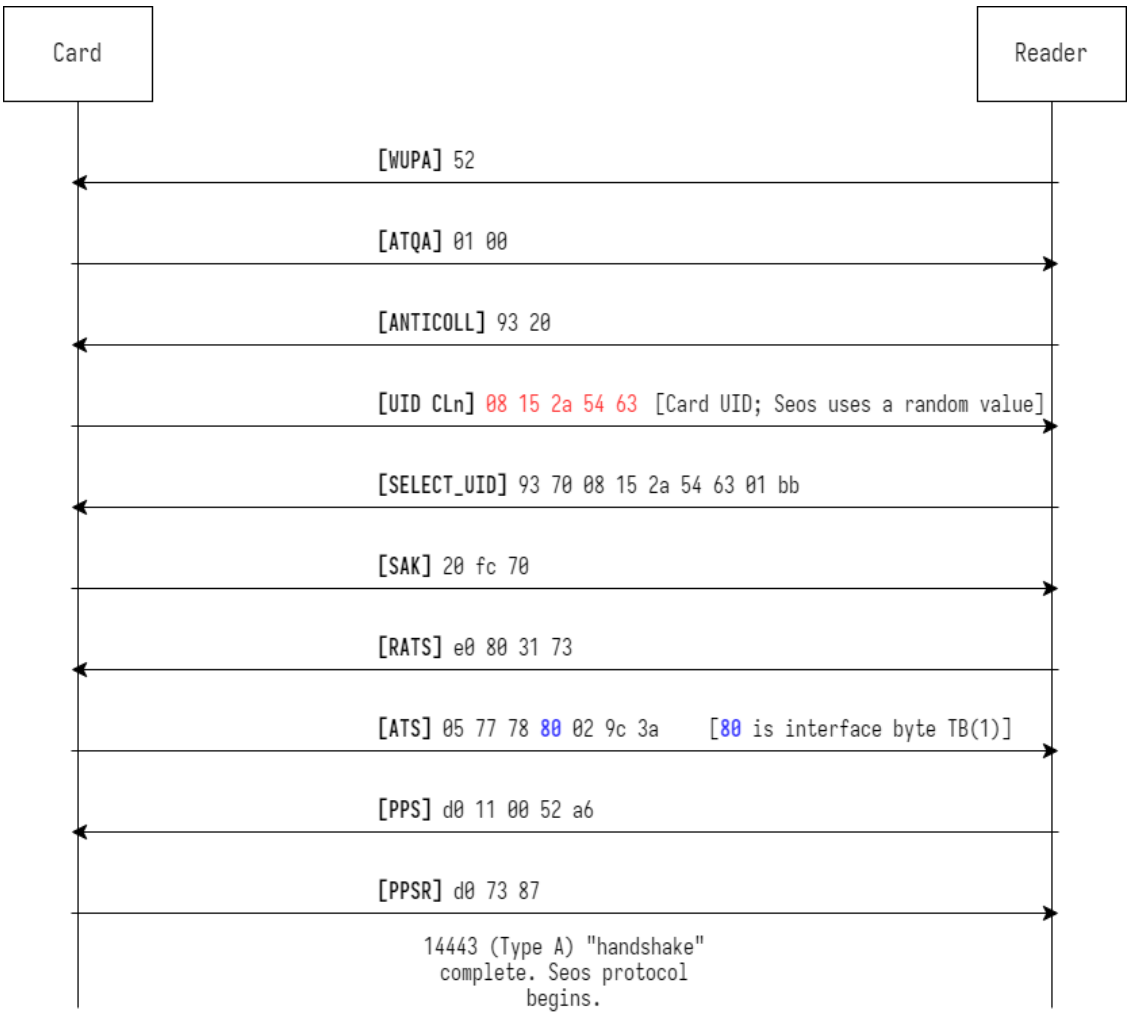

Figure 1: The 14a "handshake", as documented in [8]. The values shown were found by observing a real card authenticating to a real reader.

The key component of our relay attack is the code that talks to real cards and readers—the code running on the two Proxmarks. We based this code on Salvador Mendoza's excellent hf_reblay project [14], which performs a similar relay attack against Android tap-to-pay. Our fork of hf_reblay works as a standalone mode within Iceman's Proxmark 3 firmware [15]. We made several modifications and improvements to hf_reblay, adapting it to work with the Seos protocol and including code to send a modified ATS message to get more time from the reader (as described above). Our fork is fairly generic and—as an improvement over the original—assumes no protocol-specific details when relaying. As such, it could be used to perform relay attacks on any 14a based protocol, as long as the initial 14a handshake can be hardcoded. As another improvement over the original hf_reblay work, our complete attack operates over Bluetooth→IP instead of just Bluetooth, significantly extending the range. We will make our modified hf_reblay fork and supporting Python scripts publicly available at `https://gitlab.com/loudmouth-security/seos-tools-public` after the responsible disclosure process is complete, though we warn that the code quality leaves something to be desired.

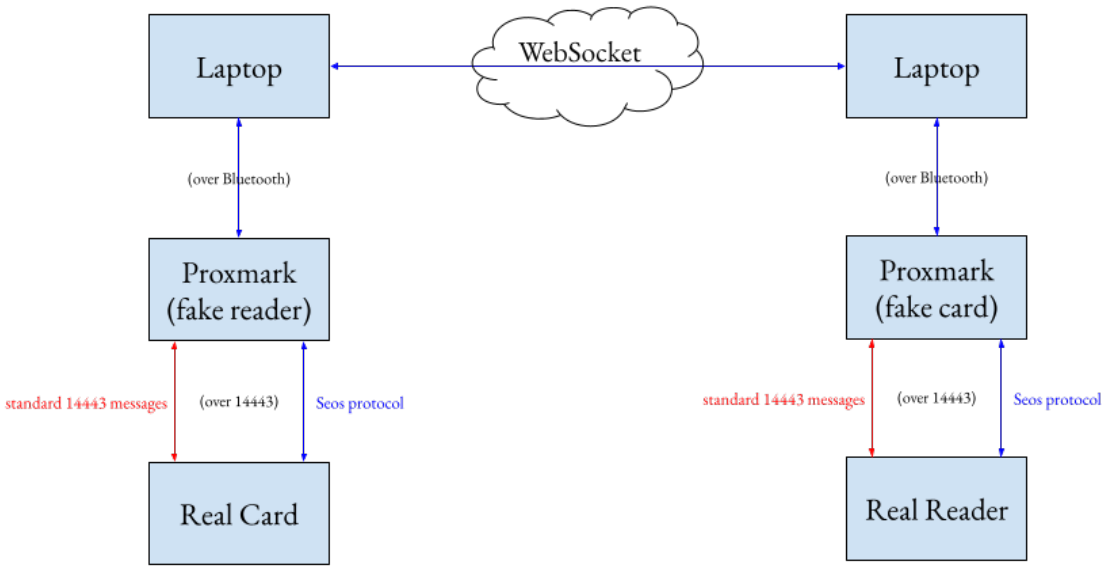

Figure 2: High-level data flow diagram of our attack. Relayed Seos protocol messages proceed along the blue arrows from the real reader to the real card, followed by the response from the real card to the real reader, and so on. Standard 14a messages are handled by the Proxmarks themselves; this is captured by the red arrows.

5 Results

We tested our attack in both our lab and simulated real-world conditions. We used one standard-keyed Seos card and tested against two readers: models iCLASS SE R40 and multiCLASS SE RPK40. Initial testing was performed in our lab, where we were able to successfully unlock a door from a distance of ≈12 feet. After refining our attack—in particular, developing operator instructions to mitigate some limitations (discussed below)—we tested two real-world attack scenarios, both over the public Internet:

1. Unlocking a door in our lab with a card in the same city: ≈13.7 km away with a round-trip time of ≈27 ms.
2. Unlocking a door in our lab with a card in a different country: ≈1960 km away with a round-trip time of ≈99 ms.

The Seos datasheet documents the typical maximum read range as 3 to 4 inches [1]; taking the larger figure of 4 inches, our attack enables a range increase of over 1.9 billion percent. We are able to repeatedly execute our attack over all tested conditions.

We executed our attack using only inexpensive off-the-shelf hardware; all special equipment required was purchased for ≈$880, excluding tax. A picture of all the equipment used for an early test run of our attack is included as Figure 3. This shows 2 Proxmark 3 RDV4s with Bluetooth add-ons, 2 laptops, 2 laptop power supplies, 2 USB A to Micro-A cables (to charge the Proxmarks), a USB Bluetooth adapter (because one laptop did not have integrated Bluetooth), and a flash drive. Under the assumption that a threat actor already has two

laptops with Bluetooth, they would only need to purchase two Proxmark 3 RDV4s (at $340 each) and Bluetooth add-ons (at $100 each). This does not present a major financial barrier to a motivated attacker.

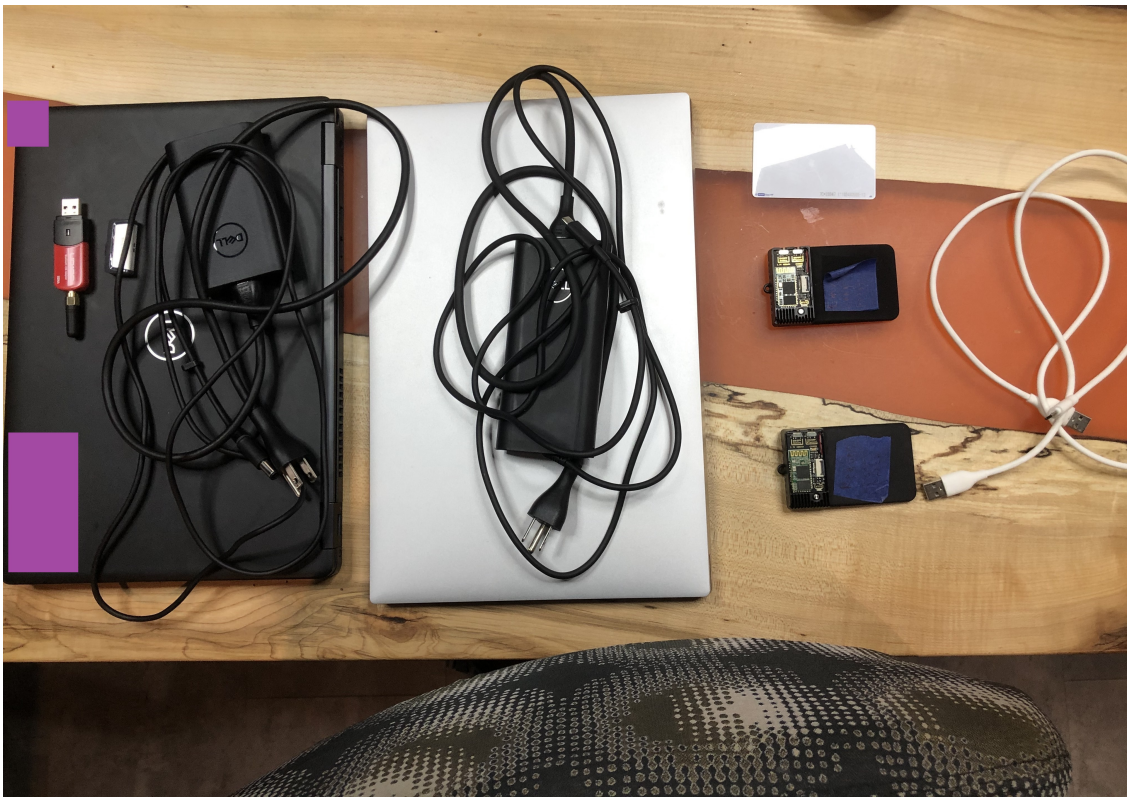

Figure 3: The equipment used in one execution of our attack. The purple boxes cover information that we do not want to share.

The only significant limitation of our attack as executed is the inability of the Proxmark hardware to successfully communicate with the legitimate Seos card 100% of the time. This slows down the attack, as it effectively must be restarted from the beginning, and can increase the time-on-target required to execute successfully. In the "same city" scenario, our attack always completes in under a minute (and usually in well under 30 seconds). With longer round-trip time—in the "different country" scenario—we observe completion times between 1 and 3 minutes. We have developed several strategies to help the fake reader Proxmark talk to the card:

- Do not place the card directly against the Proxmark; keep a finger's width of distance in between.
- Keep the Proxmark relatively far from sources of electromagnetic interference (EMI). On several occasions, we have observed the Proxmark appear to read a card—despite no card being present—when placed on the palm rest of a running laptop.
- Minimize round-trip time between the real card and reader. The probability of the Proxmark successfully communicating with the card decreases as the round-trip time

increases; we theorize that this is due to the card being designed around assumptions on how long the reader will take to respond.

- Be careful not to over- or under-charge the batteries of the Proxmark Bluetooth modules. Our attack is very sensitive to the charge level of the Proxmark Bluetooth module's battery, and is unlikely to work at all if the battery is too full *or* too empty. As the module lacks a mechanism to reliably inspect its battery level, this proved frustrating at times.

Keeping in mind the relatively modest price of the Proxmark 3 RDV4, they performed quite admirably. We believe that our attack could be made faster and more reliable with purpose built hardware.

6 Further Work

While our attack as presented is sufficiently capable to support real-world attack scenarios, we note further research that could be done to expand the reliability, speed, and applicability. We only tested on two models of HID readers (iCLASS SE R40 and multiCLASS SE RPK40); the attack may perform differently or fail completely on other models. In particular, we are unable to completely rule out the possibility that the newest line of readers, Signo, contains additional countermeasures, despite using the same Seos protocol. As our attack is agnostic to the contents of the messages relayed, it should work without any changes on elite-keyed cards. We were unable to confirm this in our lab due to expense; further research could do so.

We also suggest several ways it may be possible to improve the reliability of our attack. It is possible that making the Proxmarks talk both 14a and Bluetooth impacts their ability to successfully communicate with the card (due to EMI). Removing the Bluetooth leg of our attack, and connecting the Proxmarks to their laptops via a serial connection, may thus improve reliability[4]. It would additionally reduce the round-trip time between the real card and reader, as the Bluetooth serial connection introduces some latency. Faiqurahman et al [16] found that the similar HC-05 module introduces ≈25 ms of latency; this is enough to influence the reliability of our attack. We also observe that replacing the Proxmarks with purpose built hardware—perhaps with improved battery regulation—is likely to completely resolve any reliability issues.

7 Related Work

Multiple relay attacks on other security schemes predate our work. We discussed the evolution of relay attacks on 14a-based protocols above, in the Previous Results section, highlighting what we believe to be the first public attack in Hancke's [9] work and the first long range, Internet-based attack in Sportiello and Ciardulli's [12] work. Near-field communication (NFC), another short-range contactless communication standard, has been widely adopted and forms the basis of Apple Pay [17] and other technologies. NFC can use several RF

[4]The attack may remain covert by, for example, running the serial cable up an agent's sleeve.

protocols as a transport: 14a, ISO/IEC 14443B (14b), FeliCa, and ISO/IEC 15693 [18]. In this way, a 14a relay attack could be a part of a fully generic NFC relay attack (or be entirely sufficient for relaying applications of NFC that use the 14a transport exclusively). In 2010, Francis et al [19] presented a NFC relay attack between flip phones using Bluetooth as the relay backbone. They suggested incorporating attestations of handset location signed by the cellular network provider, the handset itself, or a trusted third party as a potential countermeasure. Bocek et al [20] presented an attack against NFC-enabled credit cards and terminals in 2016. They successfully made purchases on a public transit Point of Sale system with a NFC-enabled credit card relayed using Android tablets and a wireless router. Compared to most NFC-capable devices, the Proxmark 3 RDV4s we used provide extremely deep control over 14a protocol details—including the ability to change the Frame Waiting time Integer sent by the fake card, enabling our long range attack.

The canonical countermeasure against relay attacks is adoption of a distance-bounding protocol, that is, a protocol that allows one or both parties to securely verify their physical distance from the other. Such protocols measure signal propagation time as a proxy for distance, as bounded by the speed of light. Our attack introduces a relatively high delay[5] (measured in milliseconds), and as such could be countered by an extremely simple distance-bounding protocol: the reader would merely need to check that the card responds to all messages within a chosen low time limit. This would effectively counter any long distance relay attacks that use the public Internet. This is not a new approach; it was introduced and elaborated upon by Brands and Chaum [21] in 1994. Other attacks may not introduce such extravagant delay as ours and require a more complex distance bounding protocol to counter. As the distance and therefore signal propagation delay decreases, the processing time on both the card and reader begins to become a more important factor—and neither have particularly capable processors. Rasmussen and Capkun [22] proposed a RFID distance bounding protocol designed for fast implementations that provides 15 cm distance guarantees. They presented this in 2010, two years prior to HID's release of Seos in 2012 [13]. Adoption of Rasmussen and Capkun's protocol by future credential technologies is likely to effectively prevent all relay attacks, including short range attacks or those that do not introduce a large delay.

8 Conclusion

HID Seos remediates flaws in older generations of credential technology that enable card-cloning attacks. However, we have found that it lacks effective protection against relay attacks and is thus unsuitable in its current state for securing particularly sensitive assets. Seos is designed to assert that a credential is physically present at the time of authentication, yet we have shown that it may be up to ≈1960 km away. We speculate that HID, while developing the Seos protocol, treated the underlying ISO/IEC 14443A layer as a "black box" and failed to correctly assess its impact on the security of the overall solution. In fact, a feature of that layer that lets the card tell the reader how long to wait for a response was critical to the

[5]This remains true even when deployed over an extremely fast IP network, e.g. a single local Ethernet switch, due to the Bluetooth hops.

success of our attack. This underscores the importance of analyzing every layer, even those "below sea level", to secure system design. We propose that future HID/Seos systems can be patched to prevent our relay attack by changing the code running on the reader to check that the card responds within a specified time limit, and reject an authentication attempt if it does not. An easy way of doing this is to modify the ISO/IEC 14443A layer to reject high values of the Frame Waiting time Integer that would otherwise result in an exploitably high Frame Waiting Time. It will likely also be necessary to alter the handling of the standard 14443A Wait Time eXtension message. Absent a reader update, it is also possible to mitigate our attack by instructing cardholders to protect cards with RFID-blocking wallets, lanyards, or similar instruments when not in use, though this approach is likely to have compliance problems (especially if the cards must be used frequently).

It may be possible to prevent our attack with an update to the reader firmware. Depending on the details of a specific deployment, this may be a burdensome process, requiring visiting each door with a deck of firmware cards. Wiegand, a 1996 protocol for communication between card readers and the access control system, has no support for remotely pushing firmware updates; a 2020 report [23] found it used by over 90% of deployments. The iCLASS SE and Signo lines of readers additionally support firmware updates via Bluetooth [24], but this does not significantly reduce the burden of updating an entire campus worth of readers. And, before a firmware update can be deployed, the responsible party must know it exists and decide to actually deploy it. This is by no means a guarantee. Further, adoption of new technologies in the physical access control space is slow: a 2022 survey [25] indicated that 32% and 26% of respondents supported legacy proximity and iCLASS credentials, respectively. We are confident that deployments vulnerable to our attack will continue to exist for years to come.

References

[1] *Seos Product Brief*. HID Global. URL: https://www.hidglobal.com/sites/default/files/resource_files/pacs-seos-card-ds-en_0.pdf.

[2] *Government Agency in Dubai Selects HID Global Solutions to Open Doors with Smart Cards, Smartphones and Wearables*. Press release. Austin, TX, US: HID Global, Mar. 29, 2017. URL: https://newsroom.hidglobal.com/government-agency-dubai-selects-hid-global-solutions-open-doors-smart-cards-smartphones-and.

[3] *Vodafone Italy Selects HID Global's Mobile Access Solution to Provide Advanced and Convenient Employee-centric Applications*. Press release. Austin, TX, US: HID Global, Apr. 4, 2016. URL: https://newsroom.hidglobal.com/vodafone-italy-selects-hid-globals-mobile-access-solution-provide-advanced-and-convenient-employee.

[4] *HID Global Streamlines Student ID Issuance and Increases Security at the University of Connecticut*. Press release. Austin, TX, US: HID Global, July 16, 2020. URL: https://newsroom.hidglobal.com/hid-global-streamlines-student-id-issuance-and-increases-security-university-connecticut.

[5] *HID Introduces iCLASS Contactless Smart Card Technology*. Press release. Irvine, CA, US: HID Global, Aug. 5, 2002. URL: https://newsroom.hidglobal.com/hid-introduces-iclasstm-contactless-smart-card-technology.

[6] Flavio D. Garcia, Gerhard de Koning Gans, Roel Verdult, and Milosch Meriac. "Dismantling iClass and iClass Elite". In: *Computer Security – ESORICS 2012*. Springer Berlin Heidelberg, 2012, pp. 697–715. DOI: 10.1007/978-3-642-33167-1_40. URL: https://doi.org/10.1007/978-3-642-33167-1_40.

[7] *Readers and Credentials*. PLT-02630. Rev. D.0. HID Global. Sept. 2021. URL: https://www.hidglobal.com/doclib/files/resource_files/plt-02630-d.0-readers-and-credentials-htog_0.pdf.

[8] *Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 4: Transmission protocol*. Standard ISO/IEC 14443-4:2001. Geneva, CH: International Organization for Standardization, Feb. 1, 2002. URL: http://www.emutag.com/iso/14443-4.pdf.

[9] Gerhard Petrus Hancke. "Practical attacks on proximity identification systems". In: *2006 IEEE Symposium on Security and Privacy*. IEEE, 2006. DOI: 10.1109/sp.2006.30. URL: https://doi.org/10.1109/sp.2006.30.

[10] Ronny Wichers Schreur, Peter van Rossum, Flavio Garcia, Wouter Teepe, Jaap-Henk Hoepman, Bart Jacobs, Gerhard de Koning Gans, Roel Verdult, Ruben Muijrers, Ravindra Kali, and Vinesh Kali. *Security Flaw in MIFARE Classic*. Press release by Radboud University Nijmegen. Nijmegen, NL, Mar. 12, 2008. URL: https://www.cs.bham.ac.uk/~garciaf/publications/Security_Flaw_in_MIFARE_Classic.pdf.

[11] Nicolas Tadeusz Courtois. *The Dark Side of Security by Obscurity and Cloning MiFare Classic Rail and Building Passes Anywhere, Anytime*. Cryptology ePrint Archive, Paper 2009/137. 2009. URL: https://eprint.iacr.org/2009/137.

[12] Luigi Sportiello and Andrea Ciardulli. "Long Distance Relay Attack". In: *Radio Frequency Identification*. Springer Berlin Heidelberg, 2013, pp. 69–85. DOI: 10.1007/978-3-642-41332-2_5. URL: https://doi.org/10.1007/978-3-642-41332-2_5.

[13] *HID Global Expands iCLASS SE Platform with iCLASS Seos Cards and Open Supervised Device Protocol (OSDP) Support*. Press release. Irvine, CA, US: HID Global, Sept. 10, 2012. URL: https://newsroom.hidglobal.com/hid-global-expands-iclass-se-platform-iclass-seos-cards-and-open-supervised-device-protocol-osdp.

[14] Salvador Mendoza. *Proxmark3 Reblay: Relaying data over Bluetooth Standalone mode*. Published on personal blog. Dec. 26, 2020. URL: https://salmg.net/2020/12/26/proxmark3-relaying-iso-14443a-data-over-bluetooth/.

[15] Christian Herrmann, Philippe Teuwen, Oleg Moiseenko, M. Walker (GitHub: @mwalker33), et al. *Proxmark3 – Iceman repo*. https://github.com/RfidResearchGroup/proxmark3.

[16] Mahar Faiqurahman, Diyan Anggraini Novitasari, and Zamah Sari. "QoS Analysis Of Kinematic Effects For Bluetooth HC-05 And NRF24L01 Communication Modules On WBAN System". In: *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control* 4.2 (May 2019), pp. 187–196. DOI: 10.22219/kinetik.v4i2.826. URL: https://kinetik.umm.ac.id/index.php/kinetik/article/view/826.

[17] Apple. Cupertino, CA, US, May 2022. URL: https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf.

[18] *NFC Analog Technical Specification*. Specification. Version 2.2. Wakefield, MA, US: NFC Forum, Sept. 2021.

[19] Lishoy Francis, Gerhard Hancke, Keith Mayes, and Konstantinos Markantonakis. "Practical NFC Peer-to-Peer Relay Attack Using Mobile Phones". In: *Radio Frequency Identification: Security and Privacy Issues*. Springer Berlin Heidelberg, 2010, pp. 35–49. DOI: 10.1007/978-3-642-16822-2_4. URL: https://eprint.iacr.org/2010/228.pdf.

[20] Thomas Bocek, Christian Killer, Christos Tsiaras, and Burkhard Stiller. "An NFC Relay Attack with Off-the-shelf Hardware and Software". In: *Management and Security in the Age of Hyperconnectivity*. Springer International Publishing, 2016, pp. 71–83. DOI: 10.1007/978-3-319-39814-3_8. URL: https://doi.org/10.1007/978-3-319-39814-3_8.

[21] Stefan Brands and David Chaum. "Distance-bounding protocols". In: *Workshop on the Theory and Application of of Cryptographic Techniques*. Springer. 1994, pp. 344–359.

[22] Kasper Bonne Rasmussen and Srdjan Capkun. "Realization of RF Distance Bounding". In: *19th USENIX Security Symposium (USENIX Security 10)*. 2010. URL: https://www.usenix.org/legacy/event/sec10/tech/full_papers/Rasmussen.pdf.

[23] *Demystifying OSDP*. HID Global, Oct. 12, 2020. URL: https://www.hidglobal.com/sites/default/files/documentlibrary/pacs-demystifying-osdp-eb-en.pdf.

[24] *HID Reader Manager Mobile Application*. HID Global. URL: https://www.hidglobal.com/sites/default/files/resource_files/pacs-hid-reader-manager-app-ds-en.pdf.

[25] James Moore. *The 2022 State of Physical Access Control Report*. 2022. URL: https://www.hidglobal.com/doclib/files/resource_files/hid-and-ifsec-physical-access-control-trend-report-2022.pdf.