Safeguarding Against Legacy Downgrade Attacks

Introduction

Physical Access Control Systems (PACS) typically involve a reader (for example, HID® multiCLASS SE® or HID Signo™) scanning a credential to obtain the unique data contained within it. This credential data is sent to a control unit which uses that data to make access control decisions. For example, the control unit could trigger an electric mechanism to unlock a door.

The standard method to send credential data to a controller is via the Wiegand protocol. A series of bits (0 or 1) represent the unique card number along with optional data like a company or facility code. Within a PACS system the data on each credential (for example, a card or badge) is distinct and assists the system in accurately identifying the person seeking to gain access.

Credential Downgrades

HID readers and credentials are available in a "standard key" configuration. By design, any standard key HID reader can read any standard key compatible credential. This simplifies inventory and credential management for customers, integrators, distribution channels, and end users.

Many HID products, such as iCLASS SE®, multiCLASS SE® and Signo™ readers can operate in a "Migration mode." This mode permits more than one credential type to be used, allowing modern, high-security credentials to be phased in to existing legacy deployments. HID credentials (including Seos® and MIFARE® DESFire®) allow existing credential data to be encoded to new credentials with additional authentication and encryption, avoiding the need to program new credentials into the controller for each user. Once the upgrade phase is complete, less secure credentials such as HID Prox®, legacy iClass®, and MIFARE® Classic® should then be disabled within the reader, preventing these credentials from being accepted.

A technique called a downgrade attack has been the subject of recent publications, talks, and security forum posts. Attackers, unable to replicate the high-security features of Seos or MIFARE® DESFire® credentials, use migration mode in reverse to create a legacy version of secure credentials. The high-security credential data is read (typically with HID technology), then third-party tools are used to create a legacy credential with the same data on cards with fewer security features (like MIFARE® Classic® and legacy iCLASS Elite™), legacy iCLASS®, or cards with no electronic security at all (classic Prox®).

It is sometimes possible to reconstruct credential information without physical access to a specific credential, using a picture of a printed number or modification of credential data from another credential, for example, when sequential credential numbers are ordered.

In specialized attacks, it may be possible to extract numbers from an access control system, intercept credential data electronically between the reader and controller, "social engineer" the number out of an authorized employee (for example, by impersonation), or even simply obtain access to the label on the box of credentials (containing the values for the cards inside).

Credential numbers serve the same purpose as a password: secret values that identify a user to a system. Integrators, distributors, and end users should exercise the same care with credential numbers that they would with other sensitive information. Credential holders should protect credentials and their numbers from unauthorized access and disclosure.

How does this impact my HID products?

HID's migration-ready readers (including iCLASS SE®, multiCLASS SE® and some Signo™ readers) help reduce the upfront costs of shifting to more secure credentials (including Seos® and MIFARE® DESFire® EV3). Once migration is complete, less secure credentials must be disabled to benefit from the enhanced security these credentials offer. While legacy credential support is enabled, the risks of legacy and insecure credentials remain, including unauthorized duplication and use.

HID has a diverse customer base, including customers who opt for legacy technology with known limitations, generally for compatibility or cost reasons. These customers weigh the risks, including the possibility of unauthorized duplication, and find them acceptable within their specific operational context.

For some organizations, especially those facing minimal security threats or those with other protective measures in place, using older technologies like Prox cards can be practical. It is comparable to businesses choosing door keys that can be duplicated at the local hardware store — a matter of convenience and cost. Upgrading readers or purchasing new credentials comes at a cost, and some organizations postpone such investments based on their own timelines and budgetary constraints.

HID acknowledges the varied needs in the access control marketplace and continues to serve the needs of these customers still relying on legacy products. HID will continue to sell products supporting these customers and uses. Simultaneously, we are committed to assisting and encouraging the industry and our customers to move towards adopting more secure and advanced credential technologies. Our outreach, education, and pricing structures align with these principles.

What can I do to avoid or reduce this risk?

Improved Physical Credentials

Modern credential technologies (like Seos and MIFARE DESFire EV3) contain security-bolstering technologies. Mutual authentication requires readers and cards to prove authenticity to each other before data is transmitted, while secure messaging protects credential data in transit through per-transaction encryption keys. These credentials adopt proven and standardized cryptographic techniques recommended by international standards bodies and reviewed by the academic community for attack resistance.

Some credentials have been further verified by independent security laboratories, such as the TÜViT SEAL-5 certification for Seos 16K credentials.

We recommend users of legacy credentials upgrade to modern and secure credentials, like Seos. For legacy credential users, migration mode provides a path for in-place replacement of legacy credentials with modern and secure credentials. We recommend that any migration mode use is accompanied by a hard cut-off date communicated to users and that migration is disabled immediately if all credentials have been migrated.

Printed card numbers are sensitive information. Credentials may be ordered without a printed number, or with a non-matching number. On credentials with non-matching numbers, the number that is printed on the credential differs from the number encoded inside the credential. This prevents credential details from being photographed or visibly read by the user.

Credentials may also be ordered with random data and sequential non-matching printed numbers, allowing for easier administration without disclosure of sensitive information to users or attackers.

Mobile Credentials

HID offers mobile credentials as a scalable alternative to physical cards or fobs. HID Mobile Access® credentials are protected by Seos and Security Identity Object™ (SIO™) technology, feature customer-specific mobile keys, and are easier to manage and revoke at scale. Bulk issuance allows organizations to deploy

mobile credentials quickly and efficiently by email, while remote revocation helps remove old credentials from circulation.

The HID Origo™ API allows organizations to issue and revoke credentials in an automated manner, allowing integration with existing workflows to ensure that credentials are automatically issued, revoked, and removed at appropriate times.

Increased Reader Security

When backwards compatibility is not required, order HID Signo readers in the Seos Profile configuration. Seos Profile readers are preconfigured to only support HID's highest security credentials. They do not permit migration mode to be enabled.

HID Signo and iCLASS SE/multiCLASS SE readers support legacy Wiegand transmission (unencrypted, unmonitored) and Open Supervised Device Protocol (OSDP). Open Supervised Device Protocol (OSDP) is an access control communications standard developed by the Security Industry Association (SIA) to improve interoperability among access control and security products. OSDP v2.2 allows the implementation of AES-128 encryption and bi-directional communication between the reader and door controller.

OSDP increases the security of the connection between the reader and the access control system, protects credential data in transit, reduces the number of wires required for control signals, allows a reader to be monitored, and enhances integrated tamper detection. We recommend that customers use OSDP in Secure mode (AES-128 encrypted with non-default keys) wherever practicable.

If default (installer or "test") OSDP secure channel keys are used, it may be possible for an attacker to intercept the communication to obtain sensitive credential data, emulate credential presentation without knowing credential keys, or perform denial of service attacks or tamper with readers without detection.

Enrollment of a reader with either HID Elite™ or HID mobile credentials will restrict access to reader configuration to authorized individuals. Configuring other readers generally requires power cycling them. We recommend taking steps to prevent unauthorized physical access to readers, including reader power, to prevent unauthorized enabling of migration mode.

Customers should update reader firmware regularly to receive the latest features and fixes. Over the coming year, HID will be releasing tools to simplify and scale this process.

Card Format Security

HID offers both tracked formats like H10302 and restricted formats like HID Corporate 1000™.

Tracked formats are monitored and controlled by HID to prevent accidental or intentional issuance of duplicate credentials. Some tracked formats (like H10302) provide only a credential number, while others (like H10304) include a facility code or company code (Corporate 1000).

HID's Corporate 1000 program provides a unique format for each organization. Credentials and encoding authorization within this range are only provided to authorized purchasers. When combined with secure credentials, attackers lack the keys and tools needed to encode restricted values without authorization.

Open formats (like 26-bit H10301) may be ordered by any individual and encoded without restriction using HID CP1000 iCLASS SE encoders. When using open formats, it is possible for malicious individuals to order credentials with values that duplicate existing systems. This is true even for high security credentials.

We recommend that organizations that do not participate in the HID Elite Key program use restricted or tracked formats unless necessary for compatibility.

HID Elite Key Program

Physical and mobile credential security can be further increased through enrollment in the **HID Elite** Key Program. This program provides end-user customers with unique and restricted authentication and encryption keys. Only matching Elite cards and Elite readers will work together, preventing unauthorized cards and readers from entering or functioning within the company's Elite secured population.

When Elite keys are combined with secure credentials lacking the printed credential number, attackers have no means to read or decrypt the embedded data and are further denied the capability to write that data to a compatible card.

The **HID Elite Key** Program can use any format, including restricted formats like **HID Corporate 1000** format or tracked formats like HID H10302.

What additional steps should be taken?

Enable and monitor tamper alarms on access control readers

We recommend users ensure that all readers have tamper alarms enabled and their PACS software has monitoring enabled. This will notify security personnel immediately when a reader is removed from the wall, making it possible to swiftly respond to a potential breach.

Where practical, readers should be in areas covered by video surveillance with retained footage, allowing for later investigation of alarms and suspicious activity.

Deploy multi-factor authentication for sensitive entry locations

An access control best practice is to require additional factors of authentication (such as a Personal Identification Number [PIN] or Biometric) to be used at perimeter readers. Additional factors (like PIN or Biometric) make the use of cloned credentials more difficult.

Note that legacy credentials that store the PIN or biometric on the card itself (like legacy **iCLASS**) do not provide an additional factor, as the keys are publicly available. An attacker could edit the data on a cloned or genuine card to alter or remove PIN or biometric data, resulting in a single factor credential.

Follow key management best practices

For customers who utilize the **HID CP1000D** or other HID encoders, as well as HID or customer-created configuration cards, this equipment should be kept secure when not in use. We recommend that configuration cards be destroyed when no longer needed.

Additional Information

HID evaluates our products and systems for potential vulnerabilities, keeping abreast of global research on cryptographic and physical security challenges. We sustain active engagement with diverse expert communities to stay ahead of emerging security insights.

To facilitate this open approach, we have established the HID Security Center to provide the broader community with a secure and structured mechanism to report potential vulnerabilities so that they can be addressed. If you have additional questions or would like more technical information, please contact your integrator or HID representative.

Copyright

Trademarks

MIFARE and MIFARE Classic are trademarks of NXP B.V.

TÜVIT is a trademark of TÜV NORD AG.

HID Global, HID, the HID Brick logo, iCLASS, iCLASS Elite, multiCLASS, multiCLASS SE, HID Mobile Access, HID Origo, and HID Elite are trademarks or registered trademarks of HID Global, ASSA ABLOY AB, or its affiliate(s) in the US and other countries and may not be used without permission.

All other trademarks, service marks, and product or service names are trademarks or registered trademarks of their respective owners.