Physical Access Card Systems:
Yesterday and Today

By Dave Kearns
The Virtual Quill

September 2011

idOnDemand is not a building system vendor, but their engineers have developed considerable expertise in understanding building access technology and how that converges with information systems. During their research, idOnDemand's engineers developed software platforms, partnerships, products and techniques for embedding, emulating and integrating multiple building system card vendor solutions. They have succeeded in producing a single identity card capable of being used across multiple building systems, irrespective of their proprietary nature and flaws.

The development of this identity card led to a uniquely deep understanding of the technology, the security risks, and the issues faced by organizations. Further, it highlighted the lack of information available to most customers about how their card systems work, the security levels these systems offer, and ultimately limiting their ability to effectively consider strategic directions.

Abstract

For most users, building security systems have changed little in the past 20 years. Like doors and windows they're considered to be "part of the landscape" and may even be under the supervision of the enterprise group which paints the doors and washes the windows.

The risks to businesses have evolved, compliance is more complex and threats are much more sophisticated than in years past. Today, your organization needs to be much more security aware and flexible. Your legacy infrastructure may be holding you back, or may actually be a danger to your organization. Modern developments – including standards-based technology – can transform legacy building systems into modern digital protection and information systems.

Overview of building access market

After 20 years in the marketplace, 125 kHz (KiloHertz) proximity card technology is now the most dominant type of building system card technology with more than 300 million cards deployed and over 40 million cards sold each year. Almost every major corporation and government agency uses 125 kHz building system proximity cards.

Proximity based access cards have become common place in almost every sizable business, in office blocks, and even in many residential apartment buildings. Yet most people do not understand how their proximity card works and the limits of the privacy and security of this technology. But how do they work?

A proximity card does not require a battery; it receives its energy from an electricity field radiating 180 degrees around the face of a reader. This energy is radiating in the 125 KHz frequency band. Once the antenna in the card receives the energy, it sends it

to the tiny micro circuit chip inside the card. This chip acts as a capacitor, absorbing enough energy to send an internal binary number back to the reader. The reader receives the binary number and sends it on to the controller where the actual decision to grant access (or not) is made.

At the time (i.e., 20 years ago), the use of RFID (Radio Frequency Identification) was both the "latest thing" in technology as well as a large improvement over keyed locks. Keys were easily duplicated, and changing locks was very expensive both in terms of the hardware and installation costs as well as the cost of distribution of the new keys. There was also the problem of multiple doors – do you use different locks (and keys) for each, or the same locks for all? Of course using the same lock for all, while easier (and cheaper) was really naïve – anyone getting past the first lock could get by every lock. The security industry was quick to adopt (and adapt) to the new RFID proximity technology.

Proximity card systems, like keys and locks, were designed to be non-interoperable. This did make the system more secure than keyed locks in some respects, but it also "locked in" the customer to the vendor – you couldn't install a building security system from one vendor and then shop for prox cards from a low bidder. Also like lock and key systems, the idea was to keep out the unauthorized rather than to let in the authorized and, of course, there was no hope of authentication of the user of the device. The systems were not designed to scrutinize who is presenting the card so as long as the data in the card is recognized as valid, the user walks right through the door.

This legacy approach does not make sense today

This legacy approach to physical security no longer makes sense. Twenty years ago it was an improvement on lock and key; after all, you couldn't take the prox card to the local hardware store and have it duplicated. But today, essentially, you can – and you don't need to go to the mall.

Cloning software is readily available to download over the internet as are plans for designing common "sniffer" devices to steal the serial number embedded in the physical card. These cards are indiscriminant, even promiscuous. They'll readily give up their serial number, unencrypted, when exposed to any 125 kHz electrical field! Build a reader, place it within the proximity range of a target card and steal the authorized credential. As simple as it is to do, this is actually the hard way. Much simpler, they can be copied in about two seconds.

Most shocking of all, no technology is usually required since it is common practice for the vendor to print the serial number right on the card. A fair analogy would be for a PC manufacturer to ship laptops with the username pre-selected and engraved on the outside cover, with no password. We know that IT would never allow this, so why is it generally accepted and not even an afterthought in physical access? However, in

context of building access, it becomes even worse. Just by looking at it, one has a fair estimation of other numbers that are being used which could enable one to "mint" a hundred valid cards themselves in one sitting. This person will look like a valid user to any system (that does not scrutinize), there will be no event exceptions or flags, they will be virtually undetected wherever the card is accepted. Considering that requirements have evolved from convenience over keyed locks to that of a security system, this approach is no longer good enough.

From a security standpoint, using the most common card data format as an example, (HID® 26 bit) the total number of unique serial numbers per facility code is 65,535, while the total number of facility codes is limited to 255. While this could provide the possibility for 16,777,215 unique card numbers, it is not good enough for three reasons:

1. Most organizations only use a single facility code number which limits them to 65,535 numbers for their organization. Add up contractors, lost cards, past employees and visitors and many large organizations are quickly recycling numbers making it much like shooting fish in a barrel when guessing card numbers for amateurs with minimal motivation.
2. Even if every company that uses 26 bit data format had a unique number from one another, with over 40 million 125 kHz cards issued each year, and 26 bit being the most common data format, it far exceeds the maximum possibilities of numbers (16,777,215) which means various organizations unknowingly use the same numbers.
3. There are some vendor programs that make an effort to assign numbers unique to each organization, but there is no way to ensure this, or for any one customer to validate that this is the case.

Organizations that use proximity cards have realized that being locked in to one vendor has seriously negative effects, both on their security and on their bottom line. This realization is typically weighed in consideration of the risk of waiting for a particular vendor to address a known threat – rather than being able to move to another vendor for a more rapid response. However, organizations with a considerable investment in a particular vendor's technology become reluctant to change since change would require a full-scale rip and replace of all building security infrastructure which would be prohibitively expensive and highly disruptive to their users. The result is overwhelming passive acceptance, complacency, and ultimately a "badge and access program" rather than an adequate "security and identity program".

Finally, for various reasons to do with both the technology and the mindset of the vendors, there is a decided lack of management capabilities for these legacy (yet largely still in production) systems. Information Technology has consciously and almost unanimously put vendors on notice that they will not invest in proprietary systems that do not provide options for integration or migration. Physical access needs to, and is, heading in that direction to address these challenges to effectively put end user

organizations back in control of their physical access strategy to enable alignment with their unique policies and goals - not be limited by the vendor they have selected.

Do proprietary systems help?

Some venders have developed proprietary, or semi-proprietary, technologies and/or methods which purport to improve on the security of legacy prox card technology. But do they? Here are some examples.

Corporate 1000[TM]

Corporate 1000[TM] is a proprietary format introduced by HID Global Corporation. Its benefits supposedly include:

- Increased Security – HID uses an exclusive 35-bit format for each end user. This makes the proximity cards unique and proprietary to each client company. The availability of the cards is controlled by companies using a written authorization form to provide absolute control over the manufacture, distribution and delivery of their cards.
- Duplicate Cards Prevented – Regardless of where you buy the cards, HID keeps track of the number sequences in circulation. This prevents duplicate cards from being sold to any company ordering Corporate 1000 cards from HID.
- Increased Range of Credential Numbers – The maximum range of card serial numbers for a Corporate 1000 card is 1,000,000, in contrast to standard 26-bit prox cards which are limited to a maximum number of 65,535.

That's certainly better than the legacy RFID systems, but it does require an organization to accept vendor lock-in to HID. In addition, users must be qualified, formally enrolled and accepted by HID Global Corporation to participate in this program. But there's worse. Corp1000 does not change the inherent lack of security of the technology and can be copied just the same as any other format. Corp1000 adds no additional security.

This is perhaps the most commonly misunderstood aspect of the product. Firstly, formats are not unique to each customer as there is only one format – only the numbers change and generally the variance is focused on the facility code. Corp1000 just guarantees that HID does not assign the same number to another individual or customer. However, this does not change the technology, or put security into a prox card that has no such mechanisms. Further, it does not guarantee that no other vendor has issued the same number (since they do not have access to the Corp1000 designations) and no vendor can "own" a number to mandate that no one else can produce or use it.

Some proprietary technologies (such as iClass^{TM} from HID and MIFARE^{TM} from NXP) use the 13.56 MHz band. This frequency has become the predominant standard in mass ticketing, electronic passports and high security identification products because much larger amounts of data (compared to prox) can be transmitted very quickly between reader and a card. This is advantageous not because prox is not quick enough, but rather it can only be quick with small amounts of data. Why is using larger amounts of data without compromising speed desirable in relation to security? The answer lies in the fundamental concept of cryptography, that will unlike prox, protect (scramble) the data on the card so it is only readable by the authorized device. The more "bits" that can be applied to a cryptographic key, the stronger it is. This cryptographic key is a very large prime number – the more bits allowed the larger the number can be and the more secure it is. Even the low end of acceptance in encryption bits far exceeds a prox card chip's capacity and ability to effectively perform.

But iClass, because of its key storage system, is very insecure. Security is all about keys and after a recent discovery and subsequent detailed published report detailing the method by which one can retrieve the master key there is no longer any way to keep HID's customer key secure with cards and readers already deployed. I can therefore create cards across almost any of HID's customers, change payment amount, and get right to personal information on the card. And when I have done it once, I do not even need to do it all over again to attack another organization because they used the same key for the vast majority of their customers worldwide. Simply put, a hacker can essentially "mint" active iClass cards from anywhere. This is real, and one of the very worst security vulnerabilities that could happen in either IT or physical access. It is not effectively fixable either.

What is changing and why

Technology has come very far in the past 20 years as has our understanding of security needs – both physical security (buildings) and logical security (data systems). Think of how automobile technology, communications technology – even entertainment technology – has changed in that time. Security technology has come just as far, yet the rate of adoption appears to be low due to cost, awareness and lifespan of these systems. First, let's look at what has changed.

13.56 MHz cards, based on a standard such as ISO 14443, are now the predominant international standard. In building security, however, legacy 125 kHz RFID technology still remains popular in North America despite its security issues.

Standards

There are no known or recognized standards that cover legacy 125 kHz prox cards. But today more and more standards are being published which helps future proof your investments, ensure compatibility between vendors, drive down cost, and create a standards community that works together to solve problems. Some of the more important ones are:

ISO/IEC 14443

ISO/IEC JTC 1 (the Joint Technical Committee 1 of the International Organization for Standardization and the International Electrotechnical Commission) formulated ISO/IEC 14443 which describes two types of cards: Type A and Type B, both of which communicate via radio at 13.56 MHz, so that neither need physical contact with the reader. ISO/IEC JTC 1 also formulated ISO/IEC 7816, an international standard related to electronic identification cards with contacts. Both introduced the concept of "smart cards" to the terminology of security and identification.

FIPS 201

In the United States, the National Institute of Standards and technology (NIST) promulgates Federal Information Processing Standards (FIPS) designed to protect federal assets, including computer and telecommunications systems. The following FIPS standards apply to smart card technology and pertain to digital signature standards, advanced encryption standards:

FIPS 201 is a United States Federal government standard that specifies Personal Identity Verification (PIV) requirements for Federal employees and contractors with specific reference to the Common Access Card (CAC), a smart card used for both physical and digital access. NIST has another standard (SP 800-78) which covers cryptographic algorithms and key sizes for PIV. FIPS 140 defines cryptographic security models for objects which include both hardware and software components (such as smart cards).

From a technology perspective, the PIV smart card is a highly capable device that incorporates flexibility and government-grade security to enable organizations a platform that can meet current and future initiatives while future-proofing their investment. This standard is required for all government agencies and is being adopted by governments and enterprises worldwide. Not only is this the most secure, and the most widely accepted standard but the enormous number of cards being issued creates an economy of scale which is driving the costs down to rival legacy technology cards.

The Open Supervised Device Protocol (OSDP), an open standard for communication between access control devices and their controllers, was created to overcome a particularly difficult management problem in most legacy RFID systems: there was only unidirectional communication; they provide no means for the system to send data to the reader, nor to request data from the reader. This was a problem both from a security and a maintenance perspective.

PLAID

PLAID (Protocol for Lightweight Authentication of Identity) is a smart card authentication protocol which is cryptographically stronger, faster and more private for contactless applications than most or all equivalent authentication protocols currently available either proprietary or via existing formal standards. It is designed with two algorithms and unique mutual authentication to make hacking or privacy interception incredibly difficult. PLAID source code is published and available to the public and therefore is free for anyone to use and is in the truest sense "open".

Multi-use credentials

So just what is a "smart card"?
The smart card is a credit card (CR-80) sized identification card that contains a smart card chip, a 13.56 MHz Radio Frequency (RF) antenna and can optionally contain a 125 kHz building access chip (for legacy proximity systems). The smart card consists of a microprocessor and operating system and can securely run applications. This, combined with their unique, highly secure implementation, makes smart cards ideal for use across a broad variety of applications and uses, including building access, IT systems, cashless payments, transit cards and more.

PKI to address legacy weak models

A major benefit to having a microprocessor chip on the card is that data can be encrypted using standards such as PKI (Public Key Infrastructure). Since the private key is unique and never leaves the device (not even known in a reader like all other technologies) it makes hacking or cloning nearly impossible if implemented properly. The PIV standard has introduced this to be mandatory in Federal Agencies while prox is no longer accepted, neither is iClass.

Building access should not create new standards specific to vendors and their limitations

Looking over the standards, we can notice that few, if any, deal specifically with building access. Instead, they cover authorization – the granting of a privilege. That privilege might be admittance to a building, but equally could be access to a computer, a network peripheral (e.g., printer), a bank or credit card account or even an automobile (such as under various car sharing schemes).

Building access, then, is just another application within the enterprise and should be part of the Identity and Access Management (IAM) function of the IT department. Card identification data is then simply an attribute associated with a particular person. Audit and event management can then be coordinated across the entire enterprise – no need for proprietary event management for all of the systems which need authorization (doors, computers, vending machines, etc.).

Myths and misinformation in physical access market

A number of myths have grown up around the use of smart cards. Some might be considered "old wives tales," but some have actually been created and circulated by legacy product vendors spreading FUD (Fear, Uncertainty and Doubt). Among these are:

- There is no benefit to using a smart card over a legacy prox card – As we've seen, of course, there are many benefits (better security of data, easier control of cards, multiple use capabilities, etc.) of smart cards over legacy products.
- Smart cards are much more expensive than legacy prox cards – This was true until recently. Due to the standardization through PIV leading to mass scale and commoditization, prices are often on par with legacy products now.
- Smart card readers are more difficult to install and require special training – Smart cards can be used with the same legacy readers already installed and those that take advantage of the advanced technology on them can be installed in the same place, and usually with the same wiring, as the legacy readers. To the user, there is no difference in how they use the product, so no additional training is needed. It is entirely transparent.
- Organizations that have multiple cards due to having different building access control systems need to rip and replace most of them to get to one card. This has been the case, as it has been intended by vendors, to ensure that you had to purchase cards from them and their channel. New technology using standards-based technology provides opportunity for innovation and capabilities to put them onto one card and change transparently when a user goes from one building to another with a different system.

It's time for you to replace your out-dated legacy systems.

You will want to, though, execute that replacement with full consideration of where you are going and all options as to how you are going to get there. First and foremost, you will want to investigate and invest in products built on current public standards. Proprietary protocols should have no place in your future since they can hold your security strategy hostage and squash agility, as well as lock you in to a vendor that can disappear from the marketplace overnight - leaving you high and dry. More importantly, standards from recognized public (such as the ISO), governmental (such as NIST) or industry based (such as IEC) groups are evolving so that new and innovative uses or functions can be expected to occur within the standards and products based on them – something that rarely happens with proprietary protocols and never occurs with legacy systems.

The Future

In a few years, all of the current proprietary technologies will become unsupported and abandoned by vendors. But today you have millions of people developing and implementing the public standards that will future proof your investments, ensure compatibility between vendors, drive down cost, and create a standards community that will work together to solve problems. Essentially, you have these major government agencies (including the Department of Defense and the White House), multi-national enterprises, and hundreds of other interested parties working to solve your problems for you. Standards aren't going away.

Considerations and Strategies

The useful life of the unencrypted 125 kHz low frequency technology is approaching its end, if it hasn't already passed. It is important to begin to plan for a transition to smart card technologies, but instead of trying to take a "big bang" approach to changing all of your building system readers and cards at once you need to move in a rational manner with a well thought out process to bring your systems into the 21st century.

The industry has begun to move swiftly to the faster and more secure technologies based on 13.56 MHz high frequency. . You should, also. These new systems, which vary in their implementation and effectiveness, all offer significantly more security, interoperability and features than low frequency cards.

A starting question for most organizations is of dollars and cents. Can we afford to do this aggressively in mass or can we only afford to migrate over time thereby contributing each year toward the goal? This is entirely an internal matter than only you can answer, and it varies.

Both cards and readers can accommodate both high and low frequency within them enabling organizations to either change readers and authenticate existing card populations or migrate to new cards that support both legacy and new readers while being transparent to the end user. Some organizations are fairly aggressive in making these changes, almost hasty even, while others choose to do so within their current operating budget. As new users require a card, existing users need a new one, as readers at doors fail and new buildings are erected, instead of purchasing the same legacy reader of the past, select one that meets future requirements with legacy support. Typically this is all done without an impact to annual budgets. Most organizations that do this tend to budget in an extra 10% capital cost to swap out those cards and readers for high risk areas such as data centers, control rooms, executive suites, R&D areas, etc. Typically 90% of an organization's risk originates from less than 10% of their access points. This can demonstrate significant risk reduction to the business very quickly for a low investment while taking a more reserved approach for the rest of the population. This is a good choice for beginning a prolonged migration strategy.

It is highly recommended to begin using an ISO 14443 card. Use an ISO 14443 based platform because it provides more technology choices and suppliers. It is also what the US government is mandating for more than 10 million individuals, which has had a flow-on effect in terms of price and vendor support. Also, if you are intending to use the building card with IT access, ISO 14443 with PIV/PKI is the recommended choice due to the open standards and inbuilt support for most computer and mobile operating systems, as well as an increasing number of applications with native support.

Unlike low frequency, high frequency has a wide variety of technology available to choose from and can be quite confusing. Some are still proprietary, others meant to be open but vendors have hijacked the implementation by assigning and controlling the key or mandating their tools to be used, but there are ways to ensure you are mostly in control or completely on an open standard such as PLAID or PKI. Interestingly enough the latter two while the most open, are the most secure as well. Whatever the choice, it is highly recommended to understand the detailed pros and cons of each technology from someone that is familiar with all of them at a code level. After all, this is likely a decision to stick around for a while. It is also highly recommended that whatever is chosen, you mandate to any vendor that you own the key, it is unique, only standards-based tools are used. If an organization is "assigning" you a unique key, ensure that you understand what their process and policies are as to how they store keys internally, where they are stored and who has access to them and ultimately, it is yours to take with you when terminating the relationship with that vendor.

However, you will probably want to keep both the legacy 125 kHz proximity system and the new 13.56 MHz technology running simultaneously, often for long periods of time. This means that as door readers are upgraded to "multi-technology" readers that support both frequencies.

But – and it's an important but - when an organization upgrades to combination 125 kHz/13.56 MHz based systems it does not automatically mean that these systems are any more secure than the older 125 kHz systems. For example, one common attack with multi-class readers is to program a proximity card to have the same serial number information as a 13.56 MHz card. Unless 125 kHz has been disabled, most multi-technology readers will send the 125 kHz proximity card data to the physical access control system as if it were provided by a secure 13.56 MHz card. This of course completely defeats any over the air encryption or security features.

So in multi-technology reader environments, once all staff has been provisioned with their 13.56 MHz card, it is extremely important to disable the 125 kHz feature of those readers. This is often achieved using a configuration card from your building vendor with each reader as a manual process, and many organizations never get around to doing it due to the effort. However, there are newer options to have the readers connected to a network via Ethernet, PoE or even WiFi if the walls were not previously wired with CAT5/CAT6 which will retrofit into the same holes and wires of the previous reader for simple implementation resulting in pressing a button from a computer to make such changes than touching each reader in all locations.

idOnDemand is ready to help you plan an orderly, safe transition from your legacy or proprietary technology to a new, modern, standards-based building security system. By bringing forth innovation that goes beyond limitations imposed by legacy vendors, idOnDemand can uniquely identify alternative approaches to your future strategy resulting in decreased cost and increased security.
Visit www.idondemand.com to learn more.

All trademarks mentioned above belong to their respective owners.

Dave Kearns Bio

Dave Kearns is an internationally recognized analyst in the field of Identity Management and networking. His ground-breaking analyses of Identity, Security and Networking for Network World are read by hundreds of thousands of subscribers each week, while his books have provided a thorough grounding in the basic philosophies of directory technology and Identity Management, as well as a full understanding of networking, to a generation of technologists.