SECURING THE WEAKEST LINK

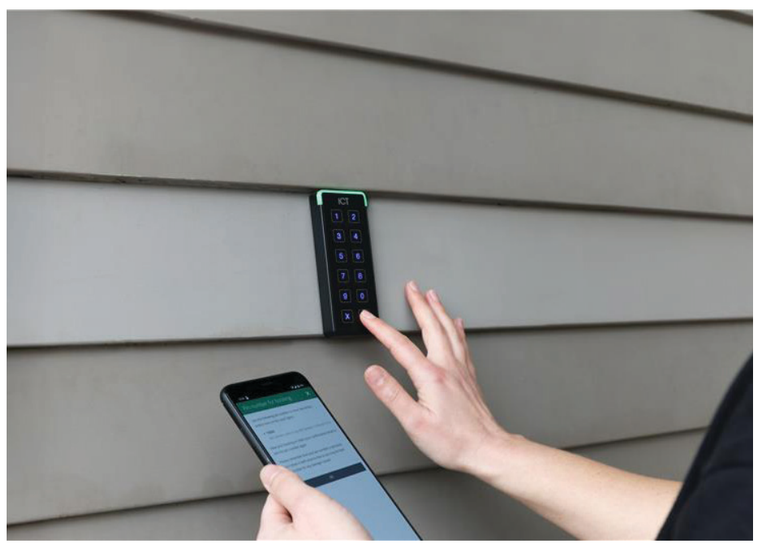
Neil Foster, Sales Director, Northern Europe for Integrated Control Technology (ICT) examines hidden weaknesses in access control, from legacy credentials to insecure protocols

NEIL FOSTER
SALES DIRECTOR, NORTHERN EUROPE
INTEGRATED CONTROL TECHNOLOGY (ICT)

MANY ORGANISATIONS STILL RELY ON 125KHZ PROXIMITY CARDS DESPITE THEIR KNOWN VULNERABILITY TO CLONING. WHY DOES THIS LEGACY TECHNOLOGY PERSIST, AND WHAT IMMEDIATE RISKS DOES IT INTRODUCE?

It is indeed surprising to see how many companies and organisations are still using a technology known for its lack of security. It defeats the purpose of having an access security system if the credentials used to operate it are so weak. 125kHz cards can be cloned in a few seconds using devices sold by main online and high street retailers for less than 20 pounds. But cloning cards is not always done malevolently, it could be done naively by a company to give access to new employees or visitors. Copying an authorised access card means another employee or a total stranger can impersonate an authorised person and access a building or site with all the risks, it implies on assets and intellectual property protection and people safety.

The main reasons for organisations to carry on using them is the lack of understanding of the technology's vulnerability and, also, the cost and possible inconvenience to upgrade the system in place.



If an organisation has hundreds or thousands of users, the practicalities of replacing the whole fleet of access cards or tags while still operating, can seem complex. End-users can also be reluctant to invest in replacing their legacy systems, however, with the correctly planned phased migration of credentials and readers this can be budgeted for and make the transition easier than anticipated.

MOBILE CREDENTIALS OFFER CONVENIENCE BUT CREATE NEW EXPOSURE POINTS, INCLUDING SHARING BETWEEN DEVICES. WHAT CONTROLS AND ENCRYPTION STANDARDS SHOULD ORGANISATIONS INSIST ON TO PREVENT MISUSE OR CREDENTIAL PROLIFERATION?

Mobile credentials are a very convenient way to give access to users, especially in education, or multitenancy environments where they could be part of an app, allowing other privileges, such as booking common areas, giving passes to visitors etc.

As mentioned above, credentials could be a weak part of a system and it is no different for mobile credentials. The communication between the app holding the mobile credential and the readers should be encrypted and authenticated. Using AES 256 encryption should be the norm as it helps prevent cloning or eavesdropping. In addition to secure communication between App and readers, an additional authentication could be added such as a PIN on the reader, for instance.

The access of a mobile credential on multiple devices should be carefully assessed and managed. As Mobile credentials are sent electronically, it is important to have a strong identity proofing during enrolment and a clear policy of lifecycle management, like a rapid revocation if the phone is lost or stolen, or if a visitor has a temporary access.

WIEGAND CONTINUES TO APPEAR IN ACTIVE DEPLOYMENTS DESPITE ITS SECURITY LIMITATIONS. WHAT PRACTICAL SECURITY AND OPERATIONAL GAINS DO ORGANISATIONS ACHIEVE BY MIGRATING TO OSDP OR RS-485, AND HOW SHOULD THEY APPROACH THIS TRANSITION?

The Wiegand interface is simple to use and widely compatible, which still makes it appealing. A lot for external devices, can be easily added to a controller, using simple and low-cost cabling, and generates a trigger to open a gate, a door etc. It is a one-way communication, there is no encryption or authentication, and no device supervision. So, while it can used easily for a wide arrange of applications, it is not secure and should only be used for small and low risk sites.

The RS-485 and OSDP (Open Supervised Device Protocol) protocols provide both an encrypted, secure two-way communication with device management. The RS-485 is unique and locked to the manufacturer bringing high security to a site, with as downside, a lack of flexibility if the users want to use third-party readers.

OSDP (Open Supervised Device Protocol) offers both openness and security and it allows to use any other OSDP compatible devices.

Organisations should approach the transition to OSDP by identifying the security risk of using Wiegand and start with the areas of the site or building with the highest risk. They will have to replace the Wiegand cabling with shielding twisted pair rated for RS-485 and ensure that existing readers, controllers, expanders support OSDP.

WHAT MEASURES SHOULD ORGANISATIONS IMPLEMENT TO SECURE COMMUNICATION BETWEEN READERS, CONTROLLERS, AND THE WIDER NETWORK?

Organisations should first ensure they are using secure credentials, Desfire EV3 is what we recommend to all our customers or mobile credentials with the safeguards mentioned earlier. Then the communication between the readers and the controllers should be encrypted, using either RS 485 or OSDP protocols. Finally, for the communication between the controller and the network, it is key to keep controllers and PC/ servers constantly updated by applying the latest security updates. It is done by downloading the latest

firmware on the controllers and updating hardware and software on the server.

POOR SYSTEM DESIGN CAN INHIBIT RAPID LOCKDOWN OR SAFE EGRESS, ESPECIALLY UNDER NEW OBLIGATIONS SUCH AS MARTYN'S LAW. WHAT DESIGN DECISIONS MOST OFTEN IMPEDE AN EFFECTIVE EMERGENCY RESPONSE?

Martyn's Law officially known as the Terrorism (Protection of Premises) Act 2025 will be a tiered legislation coming into force in the UK, with one level for buildings expecting at least 200 people permanently or occasionally, and another for 800 and more. Public protection procedures in case if an act of terrorism are aimed to reduce the risk of physical harm and relate to evacuation, invacuation and locking down premises. It will become paramount for organisations falling into the Martyn's law remit to assess which exits to release quickly to facilitate evacuation and which areas to lock down, to prevent entry of any dangerous individuals. This can be managed by the access control system if the latter has the appropriate emergency egress and rapid lock down features.

Aside of terrorism protection, lock downs are being used in more common cases, when a patient in a hospital, or a child in a school is unaccounted for, or if there is an incident in an area and the entry should be denied to any non-security staff until resolved.

HOW CAN ORGANISATIONS STRENGTHEN VISUAL VERIFICATION OR ESCALATION PROCEDURES TO TURN THESE EVENTS INTO ACTIONABLE INTELLIGENCE?

Most access controls platforms provide a list of events and alerts like a forced door, denied access but if those events are reported "blind" without additional visual verification, it slows down the security response and can be a drain on resources.

If someone forces a door open, a video clip of the event helps identify if it was a member of staff or an external person and how urgent the respond should happen.

If a person has pressed an emergency button: visual verification allows to assess the situation and the type of response needed. The same event can tigger different responses, video verification is key element to escalate serious event to a full security response, quickly and efficiently.

INTEROPERABILITY REMAINS A CHALLENGE. WHAT STEPS SHOULD ORGANISATIONS TAKE TO UNIFY ACCESS CONTROL WITH HR DATABASES, INTRUSION DETECTION, AND WIDER OPERATIONAL SYSTEMS TO REDUCE VULNERABILITIES AND IMPROVE RESILIENCE?

At ICT, we believe that unifying access control and intrusion detection is the foundation, as it allows to manage a single database of users, to reduce the risk of errors and create dynamic scenarios. If nobody is in a part of the building, it makes sense to arm it and detect any intrusion. If an employee with the right access level swipes their card, it should automatically disarm the area instead of having to add another step. Following the same logic, if the access control is connected to building automation, light and HVAC will automatically be switched on and off reducing the energy consumption. Interoperability means also the easy synchronisation of databases: for simple enrolment and disablement of users, it can be connected to HR systems to manage time and attendance, holidays, or to a room booking system.

ANYTHING ELSE TO NOTE?

Security systems are as secure as their weakest part. It isn't always obvious where the weakness lies, and it is recommended to run security audits to identify those. It could be aging hardware, not compliant with cybersecurity standards, or using non secure communication protocol between cards and readers. Regulations, the use of a building and operational requirements don't stay still, and security systems need to be re-assessed according to new laws coming into force, change of use or changes in the operational requirement of the system. It is always best to be ahead of them and have time to evaluate the various options to be compliant rather catching up and being rushed into a quick decision. **SB**