Eidola Application Note #3 – Cybersecurity and Privacy Best Practices from the Start.

January 2018

IDmachines
1264 Beacon Street, #5
Brookline, MA 02446
@idmachines
eidola@idmachines.com

Introduction

It is absolutely necessary that cybersecurity and privacy best practices are put in place from the very beginning of the design, prototype, integrate and maintain stages of the system integration process for physical security systems. This requires device and system configuration and lifecycle management. This is in contrast to many cybersecurity solutions that boast of the ability to provide a "dashboard" that allows the monitoring of and visibility into vulnerabilities or attacks. While an operational view and keeping track of the ever-growing attempts and actual compromises has value, the old adage of "an ounce of prevention equals a pound of cure" and the importance of security and privacy by design could never be more apt.

This is particularly true for physical security systems where an overwhelming percentage of the installed base is fundamentally insecure. This is true from credential to server and from design to maintenance supply chain vulnerabilities. This challenge is something that needs to be taken to heart from consultant to component vendors to system suppliers to integrators through to the end-users and their security staff as well as the information technology departments supporting them.

Getting the Design Right and the Ecosystem to Support It

It is impossible to secure an insecure system or one that does not take privacy considerations into account. Unfortunately, the baseline for physical security system very often misses this mark by a wide margin. Just because something is called a security system does not mean that it delivers on that promise. In fact, many so-called security systems are in fact vulnerabilities and time bombs. Much of this can be addressed by the adoption of current ***and*** modern standards; in some cases, unique to physical security systems and in other cases simply by adopting best practice from the information technology and networked systems world. The following provides a high-level description of a physical access control system (PACS) components and the requirements that should be part of any new deployment or system update/upgrade. While not addressed specifically here, the controller and network requirements are extensible to video surveillance and other IP and networks security devices.

Credentials

Electronic physical access control systems and access control system in general are completely dependent on the ability to leverage strong authentication as part of the process of authorizing individual access to resources. Unfortunately, the use of 125 KHz and magnetic stripe cards ***do not authenticate*** at all but simply push an identifier to a controller that determines whether or not access can be granted. In the case where authentication does exist it is critical that current sound cryptographic principles are applied that necessarily implies the use of standard based approaches. Unfortunately, over 80% of the installed base of system do not meet the need to use standard based credentials that leverage modern cryptography. And unfortunately, these insecure solutions continue to find their way into acquisition specification. At a minimum credentials should be using 128-bit AES for symmetric credentials, and RSA 2048 or ECC P256 for asymmetric ones.[1]

[1] Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175B.pdf, in addition, Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies provides additional guidance a references http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175A.pdf

Readers

Physical access control card readers ideally authenticate credentials (users) and securely pass the authenticated identifier to a controller where the access control decision then takes place. While multiple readers have had the ability to authenticate modern credentials few, until recently, have met the requirement to securely pass that information to the door controller (panel) based on a secure standards-based communication protocol. In the case where serial communications are used the Open Supervised Device Protocol (OSDP)[2] secure method should be required. This brings two critical requirements, the first is that communications are secure and the second is that a standards-based approach is used. In addition to the core functionality one of the benefits of bidirectional communication is the ability to maintain devices remotely. This capability should be part of the baseline card reader requirements. Driving home this requirement is a win-win. It provides security and reduces the lifecycle cost by not requiring a visit to each reader in order to make changes. As an example, the world today requires an ability to update firmware as features are added or vulnerabilities are addressed. This capability creates a far lower lifecycle cost than a lower cost solution without this capability. Particular given the need to maintain systems to the edge.

Controllers (Panels)

Control panels sit between readers and the network and as a result need to meet requirements both downstream and upstream. The downstream (reader) connection needs to be secure OSDP as described above. The control panel itself needs to be able to authenticate properly using digital certificates and transport layer security (TLS) current version (1.2)[3]. In addition to these two requirements (Secure OSDP and TLS) control panels as IP devices should support standards that enable IT tools to monitor and maintain them. In particular network security devices should support network scanning protocols and tools such as NMAP[4] and network monitoring protocols such as the simple network monitoring protocol (SNMP)[5].

Switches

While not often considered part of a physical security system the network on which the system operates is critical to its overall security and performance. In this regard it is important that the network switches deployed are managed. The price point of professional grade managed switches is not much more than unmanaged ones and unless a switch is managed the ability to monitor the devices connected to it is severely compromised. This is true for power over Ethernet (POE) switches as well. While this may seem like an unnecessary distinction to make for IT professionals the difference between managed and unmanaged may not be clear to those specifying or procuring physical security switches. Like control panels the switches need to support TLS 1.2, SNMP and scanning.

[2] https://www.securityindustry.org/industry-standards/open-supervised-device-protocol/

[3] https://tools.ietf.org/html/rfc5246

[4] https://nmap.org/

[5] As with TLS a number of specifications support SNMP the following site provides a good summary http://www.snmp.com/protocol/snmp_rfcs.shtml

Servers and Workstations

Much like switches, servers and workstations need to adhere to information security best practices. The same requirements again (TLS 1.2, SNMP and an ability to support scanning). A wide range of security and privacy control apply, examples include the Center for Internet Security Top 20[6] (formerly SANS Top 20), ISO 27002[7], the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)[8] and the underlying NIST Security and Privacy Control standard SP 800-53-4[9]. While there is certainly human interaction in the balance of a physical security system, workstations in particular are purpose built with a user in mind. The introduces a wide range of considerations including user authentication, role-based access control and privileged account management in addition to requirements around the device itself. It is incumbent upon security professionals to understand personally identifiable information and the purpose categories for processing personal information as a new and critical challenge.

Summary

While it is important for security systems to have monitoring and reporting that determine whether or not they are under attack, in compliance with regulations or in need of maintenance, it is equally important to make sure that proper system design requirements and practices are followed from the start. And while there are many aspects to developing hardened component and system configuration and its operation, it is very useful to start with secure authentication and communication channels and to the extent possible to leverage IT standards in physical security systems. The following table presents some of the standards that are useful to include in the design, procurement and integration of physical security systems outlined in this note.

IDmachines

Component	Cards	Readers	Controllers, Cameras, etc.	Switches	Servers and Workstations
Standards - Requirements	Modern Standards Based Cryptography • AES 128 • ECC P256 (note: attention to curve definitions) • RSA 2048	Strong Credential Authentication and Secure Bi-Directional Communication • Secure OSDP for serial communication • TLS 1.2 for IP devices	Secure Device Authentication and Secure Communication • TLS 1.2 • Other IT standards	Secure Device Authentication and Secure Communication • TLS 1.2 • Other IT Standards	Secure Device Authentication and Secure Communication • TLS 1.2 Leverage other IT ***Security and Privacy Standards***

[6] https://www.cisecurity.org/controls/

[7] https://www.iso.org/standard/54533.html

[8] https://www.nist.gov/cyberframework

[9] https://nvd.nist.gov/800-53