Using Face Recognition For Two-Factor Authentication

By Justin Schorn, VP of Product Managment

The benefits of two-factor authentication are well-understood in the cyber security world. Requiring two of the three types of authentication – something you know, something you have, or something you are – significantly improves security. Two-factor authentication is being heavily promoted by the major Internet companies. But adoption is still not universal, mostly due to issues related to user convenience and perceived complexity.

Something you have

Something you know

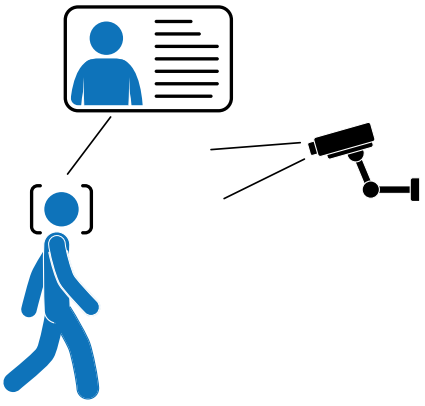
Something you are

Similar issues exist in the physical security world with access control systems. Organizations know that key cards can be lost or stolen, access codes forgotten or shared, and doors held open for the sake of convenience or social graces. These lapses can be mitigated by on-site security personnel, but only at a substantial cost (especially if there are multiple entry points). Face recognition analytics, when integrated with the site's access control and video management systems (VMS), directly address these issues at a fraction of the cost.

Two-factor authentication in action

Consider an organization that uses face recognition analytics alongside their existing key card system:

1. Access to secure areas is controlled by doors equipped with key card readers.
2. When a person approaches the entrance to a secure area, a surveillance camera captures an image of their face.
3. The face recognition analytic built into the VMS instantly compares their face against a known list.
4. If the person is authorized, the VMS instructs the access control system to allow key card access.
5. If unauthorized persons are detected, the VMS can instruct the access control system to block access, notify security, and call up a live feed



ARTICLE

The resulting benefits

Face recognition analytics can enhance access control systems in several ways:

- Adding an extra level of protection while remaining unobtrusive. The near instant speed of modern face recognition keeps authorized employee traffic unhindered – employees do not need to look directly at the camera nor pause in front of it.
- Avoids requiring employees to make physical contact with a biometric sensor or other device. This addresses practical concerns like dirty fingerprint readers or germ-spreading keypads.
- Enhances key card systems by detecting access attempts using valid key cards not yet reported as being lost or stolen.
- Enhances keypad systems by detecting access attempts using shared access codes.
- Discourages potential tailgating attempts by notifying security of unknown or banned persons near secure areas

Implementing two-factor authentication

While the design of intelligent face recognition analytics remains cutting edge, the implementation of two-factor authentication in an access control system is a far simpler process. A modern VMS should provide a relatively simple interface (typically web-based) to assist in the configuration and training of the face recognition analytic. In terms of integrating the VMS with the access control system: the detection of an unauthorized person triggers a set of rules in the VMS, which in turn communicates the event to the access control system.

Depending on the capabilities of VMS and access control systems, different integration approaches may be required:

- Combination VMS and access control system
- Certified SDK-based integration between VMS and access control system
- Open Platform Communication (OPC) standard
- Hardware-based I/O communication

Effective, unobtrusive security

Key to the success of any security program is the ability for the organization to actually implement and follow it. Face recognition analytics make two-factor authentication feasible for organizations without imposing additional burdens or hassles on daily operations.

info@senstar.com • senstar.com