Comprehensive Security Management: Enabling the Convergence of IT and Physical Security
The vision of the Open Security Exchange is to bring together the disparate technologies making up today’s security infrastructure to allow for optimal security and operational efficiencies, while respecting organization-specific operational requirements. One of today’s most significant security management challenges results from the gap between physical and IT security technologies. The lack of technical integration between the physical security systems and IT security systems has resulted in organizational and procedural gaps for virtually every organization in the world. Very few non-governmental organizations have adopted comprehensive security strategies encompassing both physical and IT security. From an organizational standpoint, a very small number of organizations have formal procedures in place to coordinate between the different departments handling physical and IT security. A 2002 study by Pinkerton Consulting and Investigation indicates that only 1% of the companies surveyed have merged their physical and IT security organizations. And while 51% percent of the respondents have some kind of informal coordination between the physical and IT security departments, only 36% have formal procedures in place to allow such coordination.

The lack of technical interoperability between the physical and IT security systems has a number of consequences, for example:

- inability to centrally manage physical access control systems from different vendors
- incompatibilities between building access hardware tokens and IT access tokens
- inability during forensic investigation to relate building access logs to IT logs
- poor individual accountability resulting from the lack of consistent standards for journal management and IT log management
- limited situational awareness because no monitoring system can provide a coordinated view of physical and IT attacks
- high operating costs resulting from manual processes for new hires and contractors to get initial building access set up and modified when their access needs change
- potential security exposure resulting from the inability to de-provision terminated staff

Effective security management combining both physical and IT controls could result in organizationally and operationally coordinated security.

The physical and IT security management convergence specifications advanced by the Open Security Exchange are designed to promote organizational and technical integration between the physical and IT worlds in order to maximize organizational security while reducing operating costs. These specifications are intended to provide the following capabilities:

**The Ability to Audit Security**

Data Across Systems

The technical specifications of the Open Security Exchange allow organizations to help ensure consistency when recording security events stored in physical and IT security systems, and provide for consolidating security data into a central repository for auditing purposes. As a result, organizations can:

- quickly detect and automatically respond to complex security incidents and vulnerabilities
- reduce the time required to audit systems and perform forensic investigations
- quickly establish the identity of perpetrators and maintain individual accountability
- more efficiently control physical access to sensitive IT systems, for example, by detecting login attempts made against a system while its authorized user is not on site


In recent years, these concepts have had a global impact on the way organizations operate. The Open Security Exchange™ is a cross-industry forum dedicated to delivering vendor-neutral interoperability specifications and best-practices guidelines in the area of security management. The members of the Open Security Exchange are also committed to developing open solutions by implementing the interoperability specifications in their respective products.

One of the most significant challenges faced by organizations today is related to the mitigation of risk. Risk exposure results from the delicate act of balancing complex heterogeneous technologies, policies and procedures with business requirements. Achieving the perfect balance is a difficult objective because there is little to no integration between the numerous technology components of an organization’s security infrastructure. As a result, organizations are left with undetected vulnerabilities, monitoring gaps, ever-increasing operating costs and the inability to enforce consistent security policies across the entire organization. Excessive risk exposure results from this lack of manageability.

Security management is about giving organizations the control they need of their security by bringing cohesiveness into their technology infrastructure. Sound security management results in the organization’s ability to considerably reduce its risk exposure and significantly diminish its operating costs.

The physical and IT security management convergence specifications advanced by the Open Security Exchange are designed to promote organizational and technical integration between the physical and IT worlds in order to maximize organizational security while reducing operating costs. These specifications are intended to provide the following capabilities:

**The Ability to Audit Security**

Data Across Systems

The technical specifications of the Open Security Exchange allow organizations to help ensure consistency when recording security events stored in physical and IT security systems, and provide for consolidating security data into a central repository for auditing purposes. As a result, organizations can:

- quickly detect and automatically respond to complex security incidents and vulnerabilities
- reduce the time required to audit systems and perform forensic investigations
- quickly establish the identity of perpetrators and maintain individual accountability
- more efficiently control physical access to sensitive IT systems, for example, by detecting login attempts made against a system while its authorized user is not on site

---

1. Pinkerton Consulting and Investigation indicates that only 1% of the companies surveyed have merged their physical and IT security organizations. And while 51% percent of the respondents have some kind of informal coordination between the physical and IT security departments, only 36% have formal procedures in place to allow such coordination.

2. The lack of technical interoperability between the physical and IT security systems has a number of consequences, for example:

- inability to centrally manage physical access control systems from different vendors
- incompatibilities between building access hardware tokens and IT access tokens
- inability during forensic investigation to relate building access logs to IT logs
- poor individual accountability resulting from the lack of consistent standards for journal management and IT log management
- limited situational awareness because no monitoring system can provide a coordinated view of physical and IT attacks
- high operating costs resulting from manual processes for new hires and contractors to get initial building access set up and modified when their access needs change
- potential security exposure resulting from the inability to de-provision terminated staff

3. Effective security management combining both physical and IT controls could result in organizationally and operationally coordinated security.

---

**Figure 1: Integrated Security Management**

The physical and IT security management convergence specifications advanced by the Open Security Exchange are designed to promote organizational and technical integration between the physical and IT worlds in order to maximize organizational security while reducing operating costs. These specifications are intended to provide the following capabilities:

**The Ability to Audit Security**

Data Across Systems

The technical specifications of the Open Security Exchange allow organizations to help ensure consistency when recording security events stored in physical and IT security systems, and provide for consolidating security data into a central repository for auditing purposes. As a result, organizations can:

- quickly detect and automatically respond to complex security incidents and vulnerabilities
- reduce the time required to audit systems and perform forensic investigations
- quickly establish the identity of perpetrators and maintain individual accountability
- more efficiently control physical access to sensitive IT systems, for example, by detecting login attempts made against a system while its authorized user is not on site
Computer Associates International, Inc. (CA) has more than 26 years of experience in enterprise and security software. CA develops and supports software solutions for 99% of the Fortune 500® companies in more than 100 countries.

CA’s eTrust™ security solutions holistically address all aspects of security, allowing organizations to quickly and effectively embrace and adapt to new opportunities, improve operational efficiencies and reduce costs.

CA’s Solutions for Auditing and Security Monitoring:
• eTrust™ Audit. Collects enterprise-wide security and system audit information, and stores it in a central database for easy access and reporting
• eTrust™ 20/20. Enables organizations to collect, correlate and analyze security events; intuitively display physical and IT security information; detect suspicious behaviors and identify perpetrators

CA Delivers Strong Authentication Through:
• eTrust™ Single Sign-On. Enhances overall security by automating access to authorized Web services and IT applications through a single authentication method
• eTrust™ PKI. Delivers strong authentication of users and management of digital certificates across the enterprise

CA Provides Access Rights and User Provisioning Through:
• eTrust™ Directory. Helps organizations manage information on employees, customers and resources—and deliver new business services with high levels of confidence and security
• eTrust™ Admin. Provides easy and cost-efficient role-Based administration of users and resources across enterprise security systems and directories

The Ability to Provide Strong Authentication
User authentication is a complex issue where security and end-user convenience meet head-on. The specifications of the Open Security Exchange enable organizations to adopt strong authentication technology while leveraging their existing physical security infrastructure investments. As a result, organizations can:
• Adopt one set of credentials to access all physical and IT assets
• Maximize security by preventing casual access to sensitive locations and resources
• Reduce help desk costs and unproductive hours related to lost passwords

The Ability to Manage Users’ Access
Managing users’ privileges and credentials is one of the biggest challenges faced by organizations today. The technical specifications of the Open Security Exchange enable central management of users, their credentials and their privileges, allowing organizations to save costs and enforce consistent role-based privileges. As a result, organizations can:
• Significantly reduce operating costs by automating the user provisioning process, for example, by using a Human Resources system to create users on physical and IT systems
• Centrally manage user access privileges, regardless of the number of locations and types of resources being accessed—minimizing operating costs while consistently enforcing access rights
• Manage a user’s life cycle and his/her credentials, from hiring and issuance, to termination and deactivation
• Reduce the risk of exposure related to inactive users and obsolete accounts

About the Founding Members of the Open Security Exchange

Computer Associates International, Inc. (CA) has more than 26 years of experience in enterprise and security software. CA develops and supports software solutions for 99% of the Fortune 500® companies in more than 100 countries.

CA Delivers Strong Authentication Through:
• eTrust™ Single Sign-On. Enhances overall security by automating access to authorized Web services and IT applications through a single authentication method
• eTrust™ PKI. Delivers strong authentication of users and management of digital certificates across the enterprise

CA Provides Access Rights and User Provisioning Through:
• eTrust™ Directory. Helps organizations manage information on employees, customers and resources—and deliver new business services with high levels of confidence and security
• eTrust™ Admin. Provides easy and cost-efficient role-Based administration of users and resources across enterprise security systems and directories

Dedicated to innovations for a safer world, BAE Systems is engaged with numerous customers to design solid security management infrastructures to protect physical and IT assets. BAE Systems decided to become a contributor to the Open Security Exchange because BAE Systems believes that the Open Security Exchange is effectively bridging the gap between physical and IT security, and this results in enhanced security and simplified implementation for our customers.

—Richard R. Schieffelin, Vice President and General Manager, BAE Systems

BAE SYSTEMS
North America, one of the top ten suppliers to the U.S. Department of Defense, and Open Security Exchange contributing member:
As the largest manufacturer of contactless access control readers and cards for the security industry, HID has shipped more than 150 million credentials to customers worldwide. HID pioneered the development of radio frequency identification (RFID) technology for security. Its experience in developing card technologies enables HID to play a critical role in the evolution and adoption of smart card technology. Some of HID’s solutions include:

- **Proximity Cards and Readers.** Proximity provides the highest level of convenience and ease-of-use available in access control technology, and is now the most utilized technology in new access control installations. Proximity credentials need only be placed within proximity of their readers to activate the system. The technology is cost-effective, virtually impossible to duplicate, and is unaffected by dirty environments, weather conditions or strong magnetic fields.

- **iCLASS™ Contactless Smart Cards and Readers.** Optimized to make physical access control more powerful, iCLASS is a 13.56 MHz read/write contactless smart card technology. Offering the same level of user convenience and reliability as Proximity, iCLASS offers a higher level of security through the use of mutual authentication and encryption. Use iCLASS to store biometric templates and useful data, and implement new applications at any time without issuing new credentials.

- **Proximity and iCLASS technologies** can be housed on the same credential and combined with other technologies, such as magnetic stripe, barcode, contact smart chip modules and anti-counterfeiting features. This allows users to leverage their investment in existing systems while seamlessly upgrading to new technologies and adding new applications.

- **Gemplus** is one of the founders of the smart card industry and is the leading provider of smart card products and services worldwide. (source: Gartner-Dataquest, Frost & Sullivan). Gemplus was also awarded Frost & Sullivan’s 2002 Market Value Leadership Award for its exceptional performance, with revenue in 2002 being 787 million euros. It is the only completely dedicated and truly global player in the industry, employing approximately 5,700 people in 37 countries throughout the world. Gemplus provides smart cards, smart chips embedded in physical access cards, middleware, readers, consulting and integration services. Other solutions include:
  - **GPK and Open OS Smart Card Platforms.** Smart cards and embedded smart chips based on Gemplus’ proprietary or open Java™ Operating Systems, with the ability to store digital certicates for multi-factor authentication.
  - **PC-Link Readers.** Readers can be connected to PCs or incorporated into keyboards to enable smart card and/or biometric authentication.
  - **GemSAFE™ Libraries.** PKI and smart card-based crypto-library product that brings portability and the highest level of security to enterprise networks. It enables secure authentication for desktop, network and web applications, digital signature and encryption of email exchange through Microsoft® and Netscape® suites, as well as digital signatures for Adobe documents.
  - **Professional Services.** Gemplus’ expert network supports users at every stage of the implementation, from consulting on design to project management and integration.

Software House, a member of Tyco Fire & Security, is a leader in integrated security solutions. Software House provides a central integration platform for video, access and other peripheral electronic security networks.

- **Software House’s powerful Application Protocol Interface (API) and Dynamic Host Configuration Protocol (DHCP) support** make it the security solution of choice for some of the most prestigious, high-security environments in the world, including the United States Capitol Police and the U.S. Department of State. Other solutions include:
  - **C·CURE® 800.** This security software and advanced event management platform enables users to control access and manage events for single- or multi-sites anywhere in the world.
  - **C·CURE® Central.** Software House’s web-based credential management system allows users to easily administer personnel and access privileges anytime, anywhere, from the corporate or wide area network.
  - **apC®/8X Serial and iSTAR™ LAN Ready Controllers.** From two doors to sixteen doors, Software House’s intelligent controllers manage even the most complex access requests.

- **Extended Business Applications.** Software House leverages strategic alliances with leading software and hardware developers to enhance the quality and scope of our products.

- **Access Control Readers.** RM Series Access Card Readers are available in three different technologies: proximity, magnetic stripe and Weigand.

- **C-CURE® NetVue.** Through the NetVue interface, C CURE 800 is seamlessly integrated with digital video management systems, providing users with the ability to view live and recorded video that are linked to access events.

For more information, please visit us at opensecurityexchange.com