network centric Security
December 2008
WHERE PHYSICAL SECURITY & IT WORLDS CONVERGE

ACCESS MEETS IDENTITY

December 2008 Supplement to *Security Products*

network centric Security
WHERE PHYSICAL SECURITY & IT WORLDS CONVERGE

Content

DECEMBER 2008 VOLUME 2 NO. 6

features

departments

Network-Centric Security welcomes vendor information and briefings. To arrange a briefing, please contact our editor, **Steven Titch,** via e-mail at **titch@experteditorial.net.** Our agreement to accept or review product material or backgrounders is not a guarantee of publication.

1105 Media
14901 Quorum Dr., Suite 425
Dallas, TX 75254

Editorial services provided by
Expert Editorial Inc.
www.experteditorial.net

We ♥ Standards

by Steven Titch, Editor

Although editors like to take credit for these sorts of things, the original plan for this issue was not to give so much attention to standards.

Going into the ASIS International conference in September, I had planned to report on H.264 cameras that were finally being introduced and shipping in quantity. That was to fill our IP video editorial calendar item for this issue. But upon arrival in Atlanta, I found the show floor buzzing about two new standards groups, the Physical Security Interoperability Alliance and the Open Video Interface Forum.

As I note in the article beginning on Page 12, an IP video interoperability standard would eliminate the time camera vendors must spend developing individual application programming interfaces so their cameras can seamlessly connect and share information with video management software from other manufacturers. There is general agreement that a standard would reduce time-to-market and lead to faster growth of IP video-based security systems.

Still, a problem for vendors is that standardization favors commoditization. Without the benefit of tight-knit integration between their own systems, camera makers have to work harder to differentiate their products from competitors. That may take the form of higher resolution, better lenses or more onboard software, such as analytics. While challenging the vendors, standards yield enormous benefits for customers because they can upgrade their systems on their own schedule in an environment where suppliers compete on innovation and value instead of being locked into a one-vendor relationship.

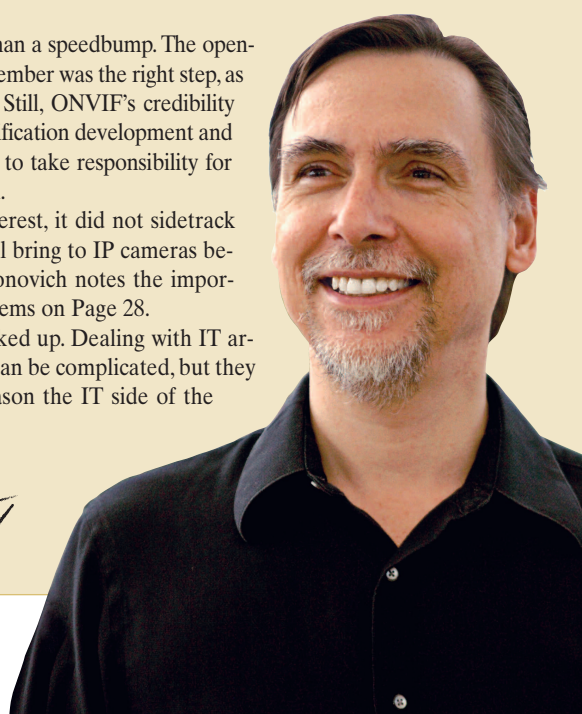
What's more, the effort envisions a standard of wide scope: a specification that could be used to tightly integrate best-of-breed video surveillance, access control, sensors and alarms. This is a welcome step in terms of approaching IT-based security networks.

PSIA, which was out of the gate first, has initiative and interest on its side. ONVIF, a countereffort launched by the three top camera vendors, Axis Communications, Bosch and Sony, must be taken seriously. But given that any common standard would benefit challengers at the cost of market share leaders (the commoditization factor), there's some cause for the skepticism that ONVIF was set up as a rival only to slow the process.

ONVIF still needs to demonstrate it is more than a speedbump. The opening of the ONVIF forum to new members in September was the right step, as is its apparent commitment to work with PSIA. Still, ONVIF's credibility will depend on how fast it moves forward on specification development and the willingness of more than one of its members to take responsibility for communicating its strategy, purpose and direction.

Although the standards battle caught my interest, it did not sidetrack me from H.264. A look at what the standard will bring to IP cameras begins on Page 8. Meanwhile, consultant John Honovich notes the importance standards will have in designing open systems on Page 28.

It shouldn't be surprising the way things stacked up. Dealing with IT architectures means dealing with standards. They can be complicated, but they deliver user control and independence, one reason the IT side of the house loves them. You will, too.



Here Comes H.264

by Steven Titch

After a year of anticipation, IP cameras incorporating the H.264 compression standard are finally available. Their bandwidth and storage benefits will be music to the IT department's ears. But what else do you need to know?

For starters, all H.264 cameras are not the same. Second, the cameras on the market now represent just the first-generation models that are limited by available processing power. Early implementers may not see a lot of difference between H.264 images and MPEG-4, but they will be getting a jump on future-proofing their surveillance systems.

The marketing mantra about H.264 has been that the standard achieves half the storage and bandwidth for the same frame rate as MPEG-4; or conversely, twice the frame rate for the same bandwidth and storage. H.264 itself comes under the MPEG-4 standards umbrella and also is known as MPEG-4 Part 10.

Sony's SNC-CS10 camera supports H.264

SMARTER COMPRESSION

In layman's terms, video compression algorithms replace entire streams of video data with simple instructions to the effect of "the next 10,000 bits are exactly the same as the one bit just sent" or "fill in the next 100x100 portion of the frame with the same 100x100 portion sent in the last image." Naturally, then, a critical feature of any compression algorithm is how well it condenses images with lots of motion.

A major innovation of H.264 is its use of variable block-size motion compensation. That simply means there is more precise segmentation of an image where there is movement in a portion of a frame. H.264 can segment an image block as low as 4x4 pixels. Further, H.264 uses predictive motion compensation, where it can instruct a video controller to display moving images based on frames sent both before and after. The result is that H.264 cameras allow much more of the stagnant part of the frame to remain compressed while retaining the necessary detail and resolution on the elements of the image in motion.

MANAGING EXPECTATIONS

The 2008 ASIS International Seminar and Exhibits, held in Atlanta in September, was something of a coming-out party for H.264. Vendors such as Arecont Vision, Axis Communications, IndigoVision, March Networks, Pelco, Sanyo and Sony were touting H.264 cameras of various types. Although vendors were high on the standard, many advised users to temper expectations, especially with the first generation.

"Most demonstrations compare H.264 cameras next to M-JPEG, not MPEG-4," said Ed Thompson, chief technology officer for DVTel, Ridgefield Park, N.J., which supplies cameras and video management software and aims to support H.264 in the second quarter of next year. "You'll be lucky to see any difference between [MPEG-4] Part 2 and Part 10."

The reason is that processing power has not caught up with the standard's capabilities, Thompson adds. Texas Instruments' newest DaVinci digital signal processor for video will have a bandwidth ac-

celerator, Thompson said, but will not be shipping until the beginning of 2009. That means current H.264 cameras still can't take advantage of the complete toolset H.264 offers.

These tools include speedier motion searches. Alex Swanson, program manager at IndigoVision, Edinburgh, U.K., said H.264 is engineered to handle special types of motion particular to security, such as the image movement created by pan, tilt and zoom operation. IndigoVision's cameras use H.264 to optimize PTZ search more effectively, Swanson said. But these tools add to the cost of processing.

"There's a layer of detail below H.264 that's not really discussed," he said. "The algorithm is clear. How you do it is up to the vendor."

Other tools and features H.264 supports is a set of up to 15 analytics algorithms, including trip wire, unattended bags and crowd counting, said Peter Wilenius, vice president of investor relations and corporate development at March Networks, Ottawa, Ontario. H.264 will compete with other standards, Wilenius said, although it is particularly suitable to megapixel cameras because of the sizable amounts of video data they need to process and transmit.

"H.264 is a necessary evil in megapixel cameras," said Tom Carnevale, president of Sentry360 Security Inc., Naperville, Ill., a megapixel camera supplier not yet supporting the standard. Currently, however, when images are placed side-by-side, Carnevale maintains there is no significant difference between H.264, MPEG-4 or M-JPEG. H.264, he said, is a future-proofing mechanism. On the other hand, M-JPEG, which Sentry360 cameras do support, "will remain a very good open architecture."

On the server side, H.264 is "delivering like it's supposed to," said Roger Shuman, marketing manager for Exacq Technologies, Indianapolis, which supports Arecont Vision's H.264 camera suite. But like others who are high on the technology, he said there needs to be more processing power on the client side before users see a full payoff.

FINDING ITS PLACE

In addition, users should avoid viewing H.264 as if it were a magic bullet for all bandwidth, functionality and cost issues. "H.264 is not completely understood by the market. There is not a wide selection of cameras, recording or management systems. It's still in its infancy," said Paul Bodell, vice president of sales and marketing at IQinVision. "There's great bandwidth savings but it's a processor hog."

Most users, Carnevale said, will likely adopt a mix of cameras after considering quality and cost trade-offs. The improved motion compensation aspects make H.264 cameras especially suitable for dense, high-traffic areas where there is a lot of activity occurring against irregular backgrounds. An H.264 camera, on the other hand, would not add much value if placed on a stationary mount to monitor a seldom-used back door.

Still, greater image quality will require a trade-off in terms of bandwidth, Bodell said. In most situations, H.264 will deliver greater bandwidth economy, but the busier the area under surveillance, the more this economy will drop.

While the outlook for H.264 is extremely favorable, gauging its full utility may take some time. For one, video management software manufacturers are traveling up the learning curve alongside camera makers. Even major players such as Milestone Systems AB suggest the jury is still out.

"H.264 is another form of MPEG. We don't know what it's going to do," said Kent Sumida, presales support manager at the Brøndby, Denmark-based company. "We haven't seen enough of it to come to a conclusion about file sizes and bandwidth consumption. The true test is movement—how it handles slow pan, fast pan and zoom. Then, we'll see how it goes."

Integrated Analytics

by Steven Titch

End users can pull together analytics tools from multiple manufacturers using a common interface that is part of a new software feature on Milestone Systems' video management system.

Milestone's Video Analytics Framework, part of its XProtect Analytics 2.0 platform, is designed to correlate alerts between and among numerous analytics functions within a security system. The framework brings together video analytics at the edge and at the server, minimizing processing power and adding value to archived video. With XProtect Analytics, said Rasmus Lund, senior technical consultant for the Brøndby, Denmark, company, users can correlate events from generic tools such as license plate recognition, facial recognition and traditional real-time access control with alerts from video content analysis tools, such as object detection. Users can build accurate evidence by cross-matching events in real-time and from archived video, he said.

At the same time, the number of false positives—a persistent problem with analytics systems—can be cut. "Having multiple systems agreeing that something happened at the same time and in the same area will reduce false positives," Lund said.

Users also can create policies that draw on multiple systems, honing surveillance to more specific alarm situations. For example, the software can be configured to trigger an alarm if both a license plate and a facial recognition system, or a camera and an access system, agree on the presence of a threat, Lund said.

Milestone expects to have the analytics framework available by the end of the year.

BEYOND PLUG AND PLAY

PSIA and ONVIF square off

By Steven Titch

With IP poised to drive video security market growth over the next five years, camera manufacturers have begun to get serious about developing a standard interface for cameras and video management systems.

But the effort may not be easy. A battle over the specification has erupted between the three leading camera manufacturers, which favor one approach, and a wider swath of the industry, which supports another.

A standard would eliminate the time camera vendors must spend developing programming interfaces for individual applications so their cameras can seamlessly connect and share information with VMS software from other manufacturers. The overall industry, however, is aiming for a standard of wider scope: a specification that could be used to tightly integrate

video surveillance, access control, sensors and alarms.

The dueling industry groups formed earlier this year. The Physical Security Interface Alliance, backed by Cisco Systems, DVTel, General Electric, Honeywell, IQinVision, Panasonic, Pelco and Verint, launched in February. In May, the three IP camera vendors with the largest market shares, Axis Communications, Bosch and Sony, formed the Open Network Video Interface Forum. Both groups seek to build on the process started by the Security Industry Association, and their work, parties representing both sides say, was an outgrowth of the frustration of SIA's slow pace.

Although analog CCTV cameras still outnumber their digital IP counterparts in terms of installed base, IP cameras make up the lion's share of new purchases. Despite the general economic uncertainty, the industry consensus is that IP camera sales are poised for explosive growth, particularly as prices fall and other standards, such as H.264, become more commonplace (see article, page 8).

The U.S. market for IP cameras today stands at $700 million and is expected to generate total sales of $20 billion to $40 billion over the next 10 years, said John Honovich, an industry analyst and publisher of IPVideoMarket.info. Worldwide, IP convergence is expected to drive the video surveillance systems market to $46 billion in 2013 from just $13.5 billion in 2006, according to ABI Research, New York.

> The aim is a spec that could be used to tightly integrate video surveillance, access control, sensors and alarms.

WHY A STANDARD?

After hearing for several years about the "plug-and-play" utility of IP, discussion of a need for a standard interface to integrate IP video gear may strike some as discordant. But while IP sets a standard way of transmitting data, equipment designed for specific applications needs a way to exchange additional information if they are to work in synchronicity.

Anyone who has connected a computer, printer and router recently recalls working with drivers. Today, most preloaded PC operating systems come with a library of drivers for various peripherals. When a new device is attached, the OS automatically retrieves and loads the appropriate driver. But up to a few years ago, printers and modems came with their own software drivers that users had to install themselves. In more cumbersome cases, they had to search a vendor Web site for the appropriate driver.

Compare and Contrast

Both the PSIA and ONVIF groups are open to all interested vendors. Documentation, materials and registration information are available at their respective Web sites:
www.onvif.org
www.psialliance.org

Likewise, even though there is a wide range of IP video management systems available, cameras from individual vendors must come with drivers or, to be more accurate, APIs to integrate with them. PSIA and ONVIF represent efforts to arrive at a common format that all cameras can use to integrate with any VMS.

"Just because a printer supports an Ethernet connection doesn't mean it can talk to another computer," said Jeremy Wilson, director of product marketing at Honeywell Systems Group, Louisville, Ky. Digital video, he said, lacks a common specification on how to send, receive, and compress and decompress an image.

"MPEG-4 doesn't say how to get from point-to-point to handshake," Wilson said. "Everyone's implementation is a bit different."

For camera, NVR and VMS manufacturers, dealing with these differences leads to greater engineering cost. "Standards make life easier for VMS companies to regulate input from the cameras, without having to spend half the engineering on interoperability," said Fredrik Nilsson, general manager at Axis Communications AB's U.S. headquarters in Chelmsford, Mass.

A common interface also would be a major step toward achieving touted plug-and-play abilities. "People have an expectation of basic interoperability," said David Bunzel, managing director of Santa Clara Consulting Group and executive director of PSIA.

"We want to be able to plug a camera into a VMS system and have the VMS know what camera it is and how to set it up."

STRENGTH VS. STRENGTH

The standards battle pits strength in numbers against strength in market clout. "PSIA is a lot further along and has broader support," Honovich said, but if the ONVIF spec picked up steam, "it would muddy the water." Generally, VMS vendors such as Milestone Systems and Genetec are neutral—they just would like a single standard. If more vendors shift toward ONVIF, though, they would have to take the specification seriously, Honovich said.

Of the two specifications, PSIA has made the most progress. As this article goes to press, a draft specification is being circulated for comment, and version 1.0 of the standard, according to Bunzel and other PSIA members, is scheduled for release this month.

ONVIF efforts, on the other hand, were largely dormant until PSIA became the buzz at the ASIS International conference in September. It was not until the following month, at the Security Essen tradeshow in Germany, that ONVIF released an outline of the specification and formally opened

PSIA www.psialliance.org		ONVIF www.onvif.org
Adesta	March Networks	**Axis**
ADT	ObjectVideo	**Bosch**
Cisco Systems	Orsus	**Sony**
CSC	Panasonic	
DVTel	Pelco	
GE	Santa Clara Consulting Group	
Honeywell	Texas Instruments	
IBM	Verint	
IQinVision	Vidyo	
Johnson Controls		

How they stack: ONVIF members together hold more than 50 percent of the IP camera market; PSIA takes in more platform vendors.

the group for wider membership.

ONVIF's charter members—Axis, Bosch and Sony—together account for more than 50 percent of worldwide camera share. As Honovich points out, this fact means that most VMS systems already support their cameras. Given the widespread adoption of these APIs, from there, it's just an easy step toward folding them into a de facto standard. Should their competitors, however, successfully collaborate on an alternative interface, it would be a boon for their businesses, because it would eliminate

> PSIA is designed much more like an API. ONVIF relies on Web services.

the costly barrier of API development while putting them on near equal footing with the leaders. This possibility has fostered speculation that ONVIF is a move by Axis, Bosch and Sony to circle the wagons to protect their market share.

Axis's Nilsson denies this, stating that Axis and the ONVIF group are looking to develop the best standard, not delay the process. His aim is to bring Axis' eight-plus years of IP product experience to bear. "We want to open up the forum to any company," he said, noting that at Security Essen, 200 companies expressed interest in ONVIF. Also at the show, interoperability based on the framework of the specification was demonstrated with three different cameras.

"We are now officially open for membership, and interested companies can choose a full, contributing or user member status," said Bob Banerjee, product marketing manager for IP video products at Bosch Security Systems Inc., Fairport, N.Y., who responded to questions via e-mail. "The membership agreement is available on the Web site, and we are planning the first meeting for members and interested parties, which will take place in the beginning of December. The event will include sessions about the forum's activities, membership and technical direction."

Officials at Sony in the United States, while expressing interest in being interviewed during the three weeks in which this article was being prepared, could not provide an executive by press time.

'ALL-ENCOMPASSING'

PSIA, for its part, sees a larger role for a common standard that extends beyond video connectivity and brings in security applications platforms of all kinds. Ed Thompson, chief technology officer for DVTel, Ridgefield Park, N.J., said ONVIF, which he sees as limited to video interoperability, "is the small tip of the iceberg. We want the standard to be broad. We see this standard covering more than just cameras. We want to consider IP standards for video, DVRs, analytics, access and audio."

At Cisco Systems, San Jose, Calif., Dennis Charlebois, director of product marketing for physical security, agrees. The overall goal is one generic API that can act as an interoperability standard across multiple security platforms. This will allow more integrators to get out of the driver business, he said, and promote interoperability among numerous IP-based security devices, including access control and other edge devices.

"We have a network-centric point of view," Charlebois said. "Anytime you don't have a specification, you make [interoperability] somewhat difficult. You walk down a path blindly."

"PSIA is a support set for all that," Honeywell's Wilson added.

UNIFICATION?

Representatives from both groups say they will seek a single standard, raising the question if the work of the two ultimately can be combined. There is some disagreement as to whether this can be accomplished easily. "Both groups have a high-level agenda—get standards," Wilson said. "ONVIF has acknowledged PSIA, but they are not close enough for reconciliation."

One reason may be the technology approach. PSIA is designed much more like an API: much of the specification is built around a physical connection. The ONVIF spec relies on Web services—software containing the instructions for machine-to-machine interaction using protocols such as the Extensible Markup Language and the Web Services Description Language. This approach involves more complexity, but, according to Nilsson, will provide more capabilities than the APIs that have been used for the last couple of years in the network video market.

But to Wilson, the standards devil you know is better than the one you don't. "Web services are a little more futuristic," he said. "There's not much legacy to build on. APIs are a known evil."

Nonetheless, others on the PSIA side think the two can ultimately be brought together.

> The route to IEEE or ANSI approval might be through SIA.

"We have reached out to ONVIF and are collaborating very closely," Charlebois said. "We want to be sure that when the differences are settled, there's only one standard."

Bunzel agrees. Parts of the ONVIF specification are "very similar" to PSIA's and can be implemented using very comparable approaches.

A ROLE FOR SIA

It's critical to remember, however, that neither PSIA nor ONVIF are standards bodies. While their members can work toward documentation, it must be formally adopted by a group such as the Institute for Electric and Electronic Engineers or the American National Standards Institute to gain status as a bona fide industry standard.

The route to IEEE or ANSI might be through SIA, which itself has been attempting to devise an IP standard for security. Its progress has been slow, sources say, and its proposed specification reportedly has drawn support from only two video vendors, said to be Salient Systems, Austin, Texas, and Hunt Electronics, Rancho Cucamonga, Calif.

An SIA endorsement could be decisive, so both groups are including SIA in the equation. "ONVIF is working on a global standard to specify how video components should communicate with each other," Bosch's Banerjee said. "In general, ONVIF will follow the SIA standard, which defines what information should be exchanged."

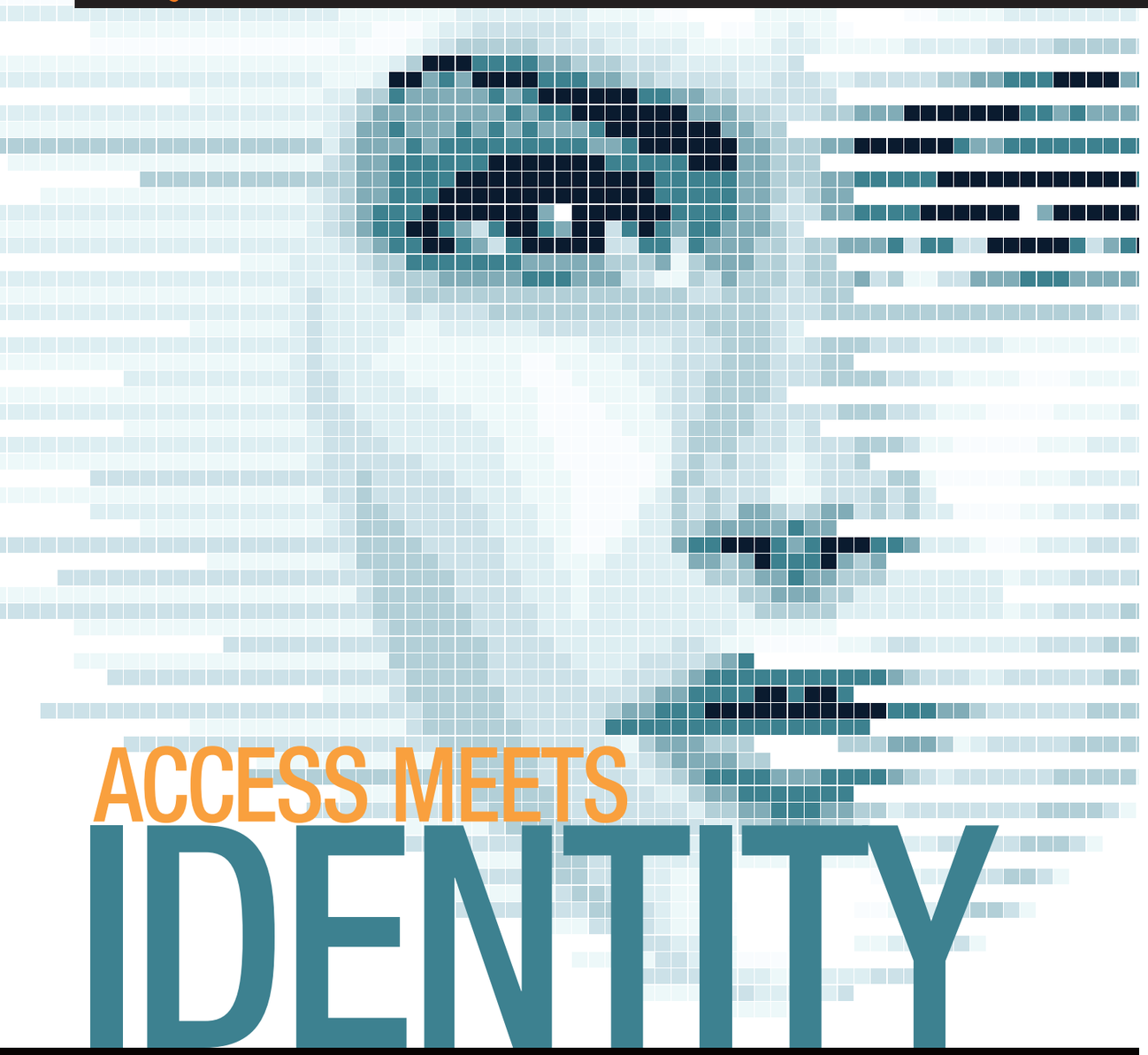
PSIA is working to integrate the API specifications with the SIA data model, Charlebois said, and the group is "actively pursuing" the incorporation of SIA's work to date.

"By taking the work that's been done by SIA and ONVIF and getting it all coordinated to end up with one standard," he said, "everybody wins."

The alternative is less attractive all around. And while the two groups seem at odds right now, neither side wants to deal with multiple standards.

"If we want to support a camera, then we have to devote general software development dollars toward supporting that camera," Wilson said—dollars that he said can be spent more constructively in product innovation and differentiation. Instead, he said, "we can end up spending a lot of money on stuff not really valuable to the industry."

Steven Titch *(titch@experteditorial.net) is editor of Network-Centric Security.*



ACCESS MEETS IDENTITY

IAM drives convergence in access control

By Sharon J. Watson

Just a few short years ago, physical access control was mainly about who could go through what doors, while logical access control focused on who got on the corporate network and into data.

Then, as more Internet protocol-based physical security devices, such as card readers and video cameras, became available, the convergence of physical and logical access control became possible. The classic example is of an employee unable to access the corporate network unless he swipes his ID card at the entrance.

Now access control, converged or not, is poised to become a key cog in a broader corporate strategy known as identity and access management. IAM, which is a largely software-oriented domain, encompasses identity lifecycle management. That means enrolling employees, provisioning their rights to the enterprise network, applications, data and, potentially, facilities, then managing those rights as they change and terminating them when employment ends.

Compliance is a strong force behind IAM, as is a growing understanding that insider malfeasance can be more costly than external attacks.

It's in this IAM space that even more opportunity for convergence is possible: that of physical and logical access control along with identity. It's a discussion occurring in companies of all sizes and across industries, though medium and larger enterprises are more likely to put money behind the concept, vendors say.

"More companies want to integrate at the identity level with building and remote access," said Geoff Hogan, senior vice president, business development and product management/marketing, at Imprivata in Lexington, Mass.

"Companies are looking to link all the component parts and identify a person in a secure, convenient manner," said Anthony Ball, global vice president of sales and marketing for IAM at HID Global in Irvine, Calif.

Compliance is a strong force behind IAM, as is a growing understanding that insider malfeasance can be more costly than external attacks. To pass audits and protect themselves, enterprises now must monitor their employees' physical and logical movements. "Companies want more security inside their firewalls," Hogan said.

Yet enterprises want IAM to be relatively transparent to their users and ensure IAM tools and strategies don't create obstacles to efficiency. "In the modern arena, you've got to make that easier for people to navigate," Ball said.

CONTROLLED CONVENIENCE

Converged physical and logical access control can offer that convenience, enabling employees to use one device to enter a facility as well as the network and applications. Such systems can be flexible, with access rules based on context. Low-risk areas or less sensitive data files might require one authentication factor, while two or more factors could be required to enter data centers or certain financial files.

Yet granting access based on a person's physical presence, denoted by a card swipe or fingerprint read, and a second factor, such as a password, is all for naught if the system doesn't know the person should no longer have access to certain facilities or files.

That's where forward-thinking companies want IAM and traditional access control to meet, vendors say. Managing physical and logical access rights throughout the identity lifecycle is critical to security. As job titles and responsibilities change, people may need access to new applications or data, while access to other file servers, databases or facilities is restricted.

"This is an area where you see a lot of security risks if rule changes don't happen

Business-based Access Strategies

A smaller health club chain wanted to build its business by staying open 24/7 but found it would be too expensive to staff a night shift. It solved that problem via IAM and access control: the company runs Brivo System's Web-based access control system in the background of its club administrative system. Personnel update client records, which automatically and transparently load to Brivo's database.

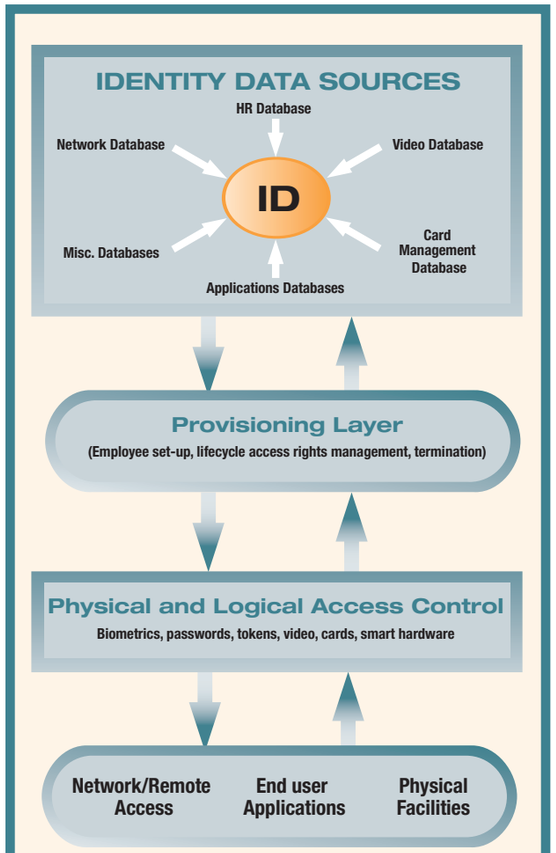
So when a club client swipes an ID card at a club door at 2 a.m., the Brivo system checks the status of that ID's client account, then grants access accordingly. The club gains the competitive advantage it needs using its existing access control system.

Converged access control also can make it easier to manage visitors gracefully yet securely. Digital Horizon Solution's Eclipse links to the popular EasyLobby product. Lobby security personnel scan a driver's license and automatically send its data to the Digital Horizons system, which in turn provisions access points for the visitor and can trigger video cameras to tape the enrollment process.

"I've been amazed at how creative IT and physical security people have been at formulating business processes," said Tom Hartman, global partner executive at Novell. These have included requiring employees to sign a required code of ethics document or suffer losing their network access, interfacing with corporate travel systems so employees' credentials transfer to satellite offices for the extent of their visit and giving retirees access to healthcare benefits systems.

That last use falls under "federated identity management," which allows someone with a set of trusted credentials to use them to access a third party's system. It has yet to become widespread but now is finding a home inside large government, financial, healthcare and telco entities, said Joe Anthony at IBM Tivoli Software.

"More than half of them are using federated solutions to bridge their own internal security spaghetti," Anthony said.



Managing Identity and Access: A Generic View

Identity data is contained in many different databases. Most vendors perform some form of data mapping to link and correlate this "metadata" to a single identity.

Provisioning assigns rights and permissions to individuals from the network level to doors to individual files and directories. The challenge: updating and disseminating new/altered rights as employee responsibilities change.

Integrated physical and logical access control tools ideally would draw rights from and share information with the provisioning layer as IP-based hardware becomes prevalent. Two-way data flows are key.

What users do with the access rights they are granted can be tracked and correlated for compliance, productivity and security purposes.

cleanly," said Jackson Shaw, senior director, product management, at Quest Software in Alieso Viejo, Calif.

Further, correlating access data across various software and physical domains can give a complete view of individual actions as well as patterns of behavior to help companies identify potential problems, says Joe Anthony, the Austin, Texas-based program director of security and compliance management for IBM Tivoli Software, Armonk, N.Y. That correlation is nearly impossible to achieve if logical and physical systems are not integrated with each other or to IAM. "If you can't take the data back to the individual user, you lose a lot of context," Anthony said.

SILOS OF IDENTITY

However, identifying an individual user in an enterprise is not as easy as it sounds. Users almost always are known to various systems, applications and even doors by different IDs and passwords, all stored in separate databases ranging from the payroll system to physical security system to the company cafeteria's stored value payment system.

When Pelco, a video management firm based in Clovis, Calif., was implementing its internal access control solution, the company realized it had key identifying data about employees in eight different databases. "It definitely would have easier to have one source," said Dan O'Malley, senior product manager at the firm.

That single source idea will probably remain as elusive as the Holy Grail, however.

"We haven't run into a single company with one authoritative source of identity data," IBM's Anthony said.

MAP MAKING

Yet correlating all the important permutations, or metadata, related to a single person's identity is critical to effective IAM. Instead of trying to create a single, centralized database of all relevant ID and access information, vendors and clients turn to data mapping. Mapping correlates scattered ID and access metadata about an individual without requiring changes in underlying databases.

"You need to link the databases to create one view of the person," Ball said. Security solutions then must then be able to recognize and authenticate that view.

Ensuring that access right changes made to one or more authoritative data sources propagate to other key access control points, logical or physical, also is critical.

"A lot of data resides in the physical access system," said Tom Hartman, global partner executive at Novell in Waltham, Mass. This includes information about vendors, auditors, contractors and visitors that might not be found in any other enterprise system. "Data needs to flow in both directions."

"You can start to link all those disparate silos of identity for security, audits and convenience," Hogan said. "We can then put a converged access policy around that to bring in the value of physical

access and network access control systems."

SLOW PROGRESS

Despite its apparent benefits, integration of physical and logical control has been slower than expected, let alone that with IAM, say some vendors.

Integration costs and complexity are two key reasons why, says Sean Kline, director of the identity and access assurance group for RSA, the security division of EMC. He cites putting digital certificates onto smart cards and then verifying them as one integration task that's turned out to be more complicated and expensive than generally anticipated.

He and other sources also say physical and logical access security often are still handled by different internal organizations, making it hard to achieve an overarching integration strategy.

> Mapping correlates scattered ID and access metadata about an individual without requiring changes in underlying databases.

IBM has been able to integrate provisioning at application, network and card management levels for about four years but has seen very few deployments, Anthony said. Lack of convergent thinking outside of the CIO's office is the obstacle he's identified. "There needs to be a lot more pushing from the top down," he said, noting that departments below the CIO level are not sharing technology, infrastructure or ideas.

For example, physical and logical access control systems that should draw data from human resources systems often don't, Shaw of Quest said. "That's partly because physical security teams haven't thought of interoperability on the data level as important," he said.

Physical security teams aren't always comfortable sharing the information within their access databases with other departments and databases, said Steve Van Till, president and CEO of Brivo Systems, Bethesda, Md. Yet IT departments increasingly see security databases as just one more source of ID information to be managed by the standards the IT shop adopts.

"It needs its set of identities managed just like any other database," Van Till said.

IT also needs to be comfortable sharing network resources with security applications.

"For our product to perform well, the IT director has to buy in," said Mohsen Hekmatyar for Digital Horizon Solutions in Frisco, Texas, which offers .NET-based access control solutions built on converged logical and physical security capabilities.

Some vendors say the bigger obstacle to converged IAM and access control is less about IT and physical security domains and more about the need to break down traditional walls among departments and business units to create comprehensive IAM solutions. Compliance requirements are accelerating these efforts, vendors say.

"Companies can be aggressive in their thinking" about how convergence can improve compliance while driving down administration and operations costs, Anthony said. "They will be pioneers in deployment, but the technology is not that hard to link."

Sharon J. Watson *(sjwatson@experteditorial.net) is a freelance journalist based in Sugar Land, Texas.*

One Goal, Many Paths

Whether the desktop or a door is the starting point for access control and identity and access management convergence, software and physical access control system vendors are ready to lead from their traditional strengths.

Imprivata initially offered a single sign-on solution to help IT departments manage dozens of user passwords, then clients began asking about using the device for network access as a second authentication factor.

The company contacted Tyco, Honeywell, Lenel and other vendors traditionally strong in the physical access control space, who said they were hearing similar customer requests. "We're integrated with all of them now at the identity level," said Geoff Hogan, senior vice president.

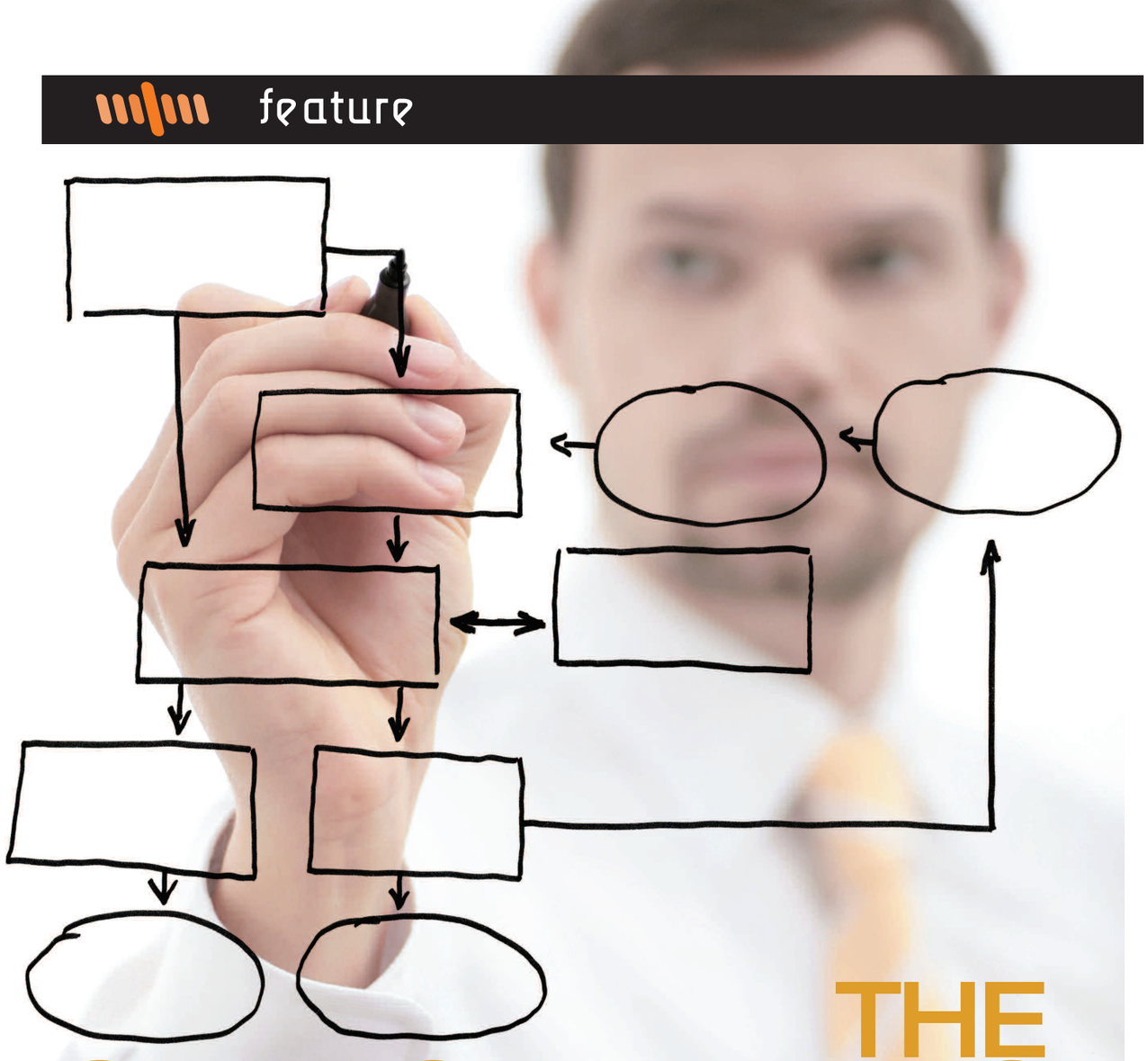
Imprivata today markets itself as an IAM company, offering security and ID management software. While saying the company "is very much on the IT side," Hogan pointed out Imprivata licenses biometrics template technology and has shipped tens of thousands of fingerprint readers with its systems.

Meanwhile, HID Global, an international leader in physical access control systems, is moving into the logical domain, where it now provides "management of delivery of secure identity," said Tony Ball, global vice president.

Ball said HID Global is emphasizing to its traditional physical security audience that they have an infrastructure in place they can exploit to create a single IP-addressable architecture encompassing cards, door readers, mobile PCs and other devices with embedded readers for an enterprise-wide converged solution.

Some vendors stress how software and hardware are complementary in the access and IAM space.

"I see a shift to smarter hardware rather than to software," said Beth Thomas, manager of product marketing for Louisville, Kent.-based Honeywell Security Systems, which partners with Novell in Waltham, Mass., on access and IAM. Adding or deleting cards, credentials and access rights — all functions that once required a separate software host platform—now can be done in the hardware of IP-addressable doors and other hardware via a Web browser. Information captured by hardware can then be shared with IAM systems.



THE OPEN-STANDARDS SOLUTION

IP-centric security offers several options for system integration

By John Honovich

Perhaps the most exciting aspect of security's convergence with information technology is the arrival of open standards. For far too long, security systems have been dominated by proprietary equipment. This constrained the scope of product choice and limited what users could achieve with their security systems.

Open standards aim to eliminate those constraints. By freeing users to choose what they want and how they want their systems to work together, standards not only lower costs but improve security operations.

Getting there will not be easy. Two major challenges exist: First, almost all large organizations have significant deployments of legacy systems that are generally quite proprietary. Designing them into an open standards-based system is difficult. Second, while

In each approach, a different system acts as the hub to manage and coordinate all the other security systems.

some open standards can be used for security systems, large and important gaps exist that have an impact on system designs. While these gaps are slowly closing, they need to be factored in.

WHAT'S A STANDARD?

A standard is a way of doing things that all parties agree to follow. The width of highway lanes is an example. All municipalities use the same width. In the famous *Seinfeld* episode when Kramer decides to widen the lanes for "comfort cruising," the result is not only comedy but obviously chaos for drivers. Unfortunately, today's security systems can often resemble Kramer's approach.

In IT, one of the most important standards is the Internet Protocol. IP ensures that any message sent from any computer can be received by another computer using IP. And since essentially every computer uses IP today, it ensures they can all communicate together. IP is the key element in allowing all security systems to use a single communication system.

IP makes sure the message is delivered but it does not guarantee that the message can be understood. It has often been compared to the postal system. If you follow the correct format for addressing and stamping a letter, your intended recipient will get it. However, if your letter is in a language that the recipient does not understand, you have a problem.

So while IP is great for moving information across networks, you still need a standard to ensure the information can be understood. This is true whether you are speaking to a friend or your access control system is sending requests to your video surveillance system.

Unfortunately, today no standard exists for one security system to speak to another. A movement is now under way to rectify this problem (see article, p. 12), but it will take at least a few years to deliver widely adoptable standards.

We definitely can benefit from IP as a fundamental standard, but we have to work around the lack of a standard for sharing information between our security systems.

BEING OPEN

All is not lost, because even without an information-sharing standard, if manufacturers decide to open up, we can design and deliver open systems that significantly improve security operations.

Returning to the analogy of the letter written in another language, the sender can include a dictionary (like those pocket Spanish-to-English ones) to overcome the lack of a standard way to communicate. Then the recipient can translate and understand the letter. For software systems, including those tools is becoming common in security: such a dictionary is called a software development kit.

Even if a system does not adhere to a standard, an SDK can allow systems to be open to one another. If you can access the SDK of your video surveillance system, you may be able to get it to communicate with your intrusion detection system so they can work together, say, to display live video of a burglar who triggers a motion sensor.

In this fashion, any system can be "open." It's the manufacturer's choice to develop and provide an SDK so its products can work with other products. Using IP as a standard and obtaining SDKs to open communication between security systems is one way to design open standards-based systems.

ALL TOGETHER NOW

The ultimate goal of open standards-based designs is to make all systems work together to reduce costs and improve the effectiveness of security operations.

Three general approaches exist. In each approach, a different system acts as the hub to manage and coordinate all the other security systems. While they all take advantage of openness and use SDKs, they differ in how they communicate with other systems. They provide various levels of functionality and power at different costs and complexity.

PSIM as the hub (Figure 1). The most elegant yet costly approach is to deploy a physical security information management application to integrate and manage all existing security systems. The PSIM application is designed to work with dozens of different manufacturers' video, access, fire and intrusion systems. Even more importantly, PSIM applications are generally developed by independent manufacturers who are not motivated to promote any vendors' products (see sidebar, "How Open is Open?"). As such, PSIM vendors strive to support as many systems as possible, maximizing the probability that all of your legacy systems will work with your new systems.

PSIM is a growing segment with a number of early stage companies. Among the most well known are CNL, Proximex, Orsus and Vidsys. Because they are all young companies, you should carefully check references and conduct due diligence on the overall cost and complexity of implementing any of their products in your organization.

The PSIM application becomes the front end for your security operators. It gathers information from all of your security systems and displays them in a common operating picture. The PSIM also allows rules to be defined to help operators quickly and effectively respond to security incidents.

The PSIM application is deployed on a server in your network and communicates with your security systems. Using SDKs, the PSIM vendors write adapters to speak with your security systems. Often, they are already available. However, sometimes the PSIM vendor will have to build an adapter to support your specific type of system.

The chief downside is that it can potentially cost millions of dollars to build an effective PSIM-based solution.

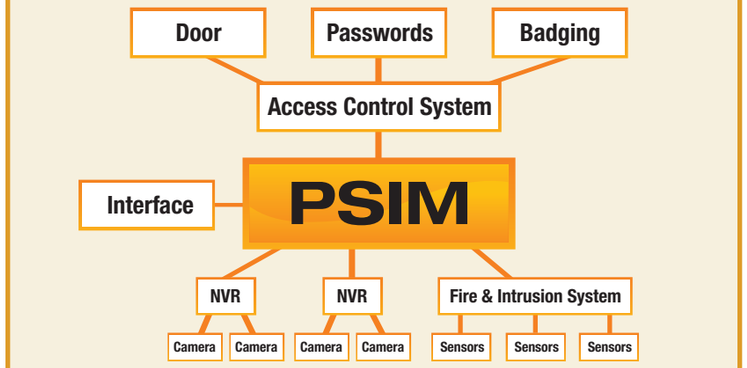


Figure 1: PSIM as the Hub

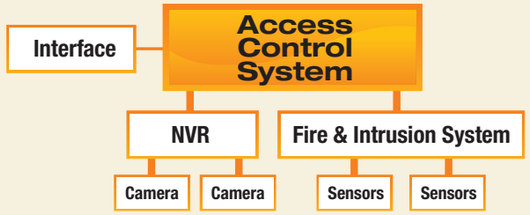


Figure 2: Access control system as the hub

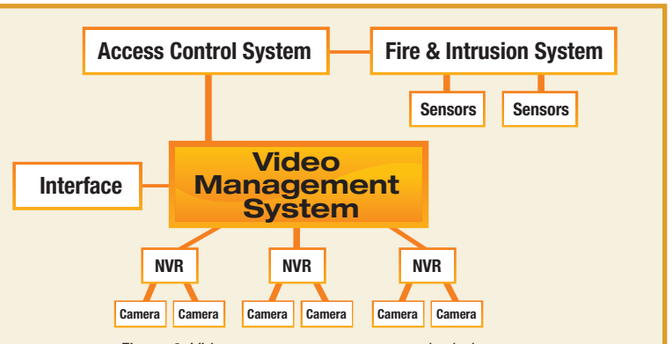


Figure 3: Video management system as the hub

What IT Wants

The corporate IP network will serve as the common platform for sharing information among your security systems. Indeed, almost all organizations are already doing this with at least some of their systems. Access control panels are connected to back-end servers by IP. DVRs or IP cameras are connected to your monitoring centers the same way.

Still, once the task turns to networking, the IT department, by necessity, must be involved. Therefore, security officers must be prepared to ensure the following three primary elements:

- *Information Security:* IT will need to verify that the systems you plan to add meet information security standards (like antivirus support). Today's security systems generally meet or exceed the standards set by IT. However, you should facilitate communication between your prospective vendors and your IT department prior to purchase to ensure compatibility.

- *IP address assignment:* Each security device that you want to communicate on the network will require an IP address. This generally is not a significant problem. Contrary to public perception, most corporations are not running out of IP addresses. Corporations almost always use private IP addresses that are practically unlimited. Nevertheless, IT will absolutely need to plan the allocation, so be up front about how many addresses you will need per location.

- *Bandwidth:* All security systems except for video require minimal bandwidth. IT will generally want to verify but this should be simple and straightforward. Even allocations of bandwidth for video are readily achievable if you are using a DVR.

Once IT approves your plan and allows your systems to be connected to an IP network, the mission is accomplished. You will be capable of communicating with all of your systems, and any one of your systems will be able to communicate with another.

Access Control as the Hub (Figure 2). The most traditional way to integrate security systems is to use your existing access control system as the information hub. For years, access control systems have been providing support to communicate with fire, intrusion and video systems. Your access control system becomes the main user interface for your security operators.

Almost all access control vendors, including AMAG, General Electric, Honeywell, Software House and Lenel, provide integration to a variety of security subsystems. Your first step should be to talk with your existing access control vendor about what specific functionalities and third-party systems they support.

Using your access control system is less flexible but also is less expensive than a PSIM application. Access control systems tend to support a limited number of security systems. They also tend to favor systems that the access control system vendor manufactures. Either of these elements could block you from building an open solution that integrates all of your systems. However, on the positive side, using your access control system is generally fairly inexpensive and can be accomplished for $10,000 to less than $100,000.

> While some open standards can be used, gaps exist that have an impact on system designs.

Video Management as the Hub (Figure 3). An emerging approach is the use of your video management system as the information hub to connect all of your security systems. None of these offerings are very sophisticated, but if you only need very limited integration (say, only with your access control system), using the video management system as the hub could provide a very user-friendly and inexpensive means for integration.

The video management vendors most focused today on providing PSIM-type functionalities include OnSSI, Verint and VideoNext.

THE FUTURE

Today, designing open standards-based systems requires some compromises and costs to accommodate the limited openness of the security systems available.

The good news is that the pressure and the momentum for openness are accelerating. Expect actual standards for security applications to significantly simplify and reduce the costs of designing open standards-based systems in the next three to five years.

In the meantime, ensure your systems run on IP networks and strongly consider which of the three options presented provide the highest value for you.

John Honovich *(jhonovich@ipvideomarket.info) is the founder of IP Video Market Info.*

What is an API?

Techies and manufacturers often like to talk about application programming interfaces. APIs simply are the computing mechanisms that allow one system to talk with another system.

A manufacturer needs to have a publicly available API to integrate systems. The good thing is that almost every manufacturer today has an API. APIs can vary in technical implementations, but most are close enough that any integration can be performed. Technical variances may cause integrations to take somewhat more time, but this is usually not a major issue.

APIs and SDKs are tightly related. SDKs are essentially the documents that explain how APIs work. Indeed, they are so tightly related that the terms are commonly used interchangeably. To perform an integration, you need both; they are almost always available as a package.

How Open is Open?

Just because any manufacturer can be open does not mean that every manufacturer is open. On the contrary, most manufacturers still can be pretty controlling on opening up to other manufacturers' systems.

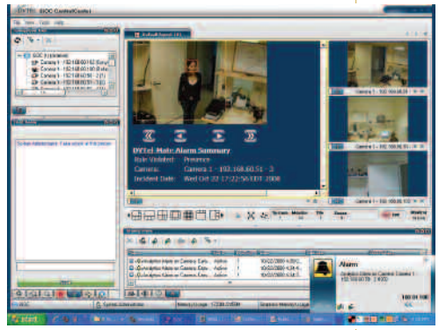
Manufacturers are motivated to maximize their sales of security systems. Because many manufacturers offer intrusion, access control and video systems, they would certainly benefit if you simply purchased all your systems from them. Then, you would not need any third-party integration, and they could simply sell you the entire solution.

In the past, it was very common for manufacturers to tightly constrain access to their SDKs. This is definitely changing as manufacturers embrace a more IP-centric philosophy. Nonetheless, real limits remain, and they vary by manufacturer.

It is essential, therefore, to always inquire and understand how open your manufacturer is to third-party integrations. Check by asking for a list of third-party products that are currently supported and how open their process is for performing new integrations.

Applications, Strategies, & Solutions

1 VMS-Analytics Integration



Mate Intelligent Video and DVTel jointly demonstrated their integrated security solution at Security Essen 2008 in Germany as part of their successful partnership.

Mate's advanced video analytics solutions seamlessly integrate with DVTel's intelligent Security Operations Center (iSOC), a video management system, to provide end users with a single interface for event and situation management. Mate's advanced edge- and server-based behavior detection solutions leverage video analysis algorithms that transform any analog or IP surveillance camera into an intelligent detection sensor. The system performs analysis using specifically designed outdoor algorithms to detect unusual events that may cause a security hazard. This automated incident detection system and real-time alarm notification solution helps security personnel increase their efficiency and response time.

www.dvtel.com
www.mate.co.il

2 Analytics, Video Servers Merge

Agent Video Intelligence Ltd. (Agent Vi), a video analytics software company, and Mango DSP, a provider of intelligent video servers for the video surveillance, homeland security and defense markets, have expanded integration of their respective products into one device capable of video encoding, decoding and transcoding high-end MPEG-4/H.264 video while analyzing the video, performing recognition, tracking objects and sending violation alerts in real time.

Based on Mango's Raven hardware platform, the device will combine the Mango IVS 3.0 operating system with version 3.2 of Agent Vi's people, vehicle and object-based analytics software. A single Mango DSP encoding device can now process real-time analytics while interfacing with any analog camera as well as a growing library of IP cameras, video servers and video management systems.

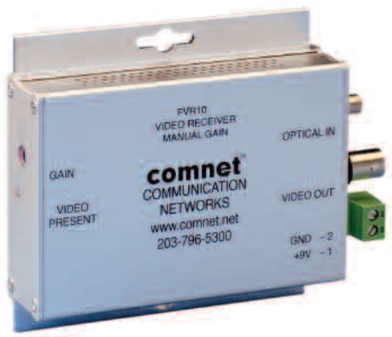
www.agentvi.com
www.mangodsp.com

3 Megapixel Cameras Catch Dumping

The Massachusetts Department of Environmental Protection has deployed IQinVision's IQeye megapixel cameras as part of its ongoing efforts to catch and prosecute illegal dumping in Boston and surrounding communities. The integrator assisting on the project is Green Pages.

The MassDEP project started three years ago with basic analog cameras and digital video recorders. Having met with some success, MassDEP expanded the project's scope. The goal of the program is to identify, prosecute and ultimately deter perpetrators dumping solid waste on city streets, vacant lots and public land. To date, the remote, camouflaged IQeyes have been directly responsible for catching seven illegal dumpers, with two of the incidents serious enough to merit prosecution and the potential for large fines.

www.iqeye.com



4 Fiber-optic Receivers

Communication Networks Inc. (ComNet) has introduced a line of video receivers for multimode optical fiber. The FVR10 and FVR11, designed to support transmission of security video over optical networks, handle baseband video signal spans of up to 2.5 kilometers. The FVR11 features automatic gain control that adjusts to changes in the camera output that might degrade the video quality. The FVR10 features a manual gain adjustment.

The devices are part of ComNet's first series of fiber-optic, video and Ethernet transmission products. The company was founded in 2007.

www.comnet.net

5 Single-output Power Adapter

Phihong has expanded its line of desktop-style, single-output power adapters to include a three-wire, 120-watt universal adapter. Designated the PSA120U series, these adapters are available with outputs of 12, 24 and 48 volts, providing power solutions for networking, peripheral, industrial and test and measurement applications.

The adapters, priced at $32.63 per unit at OEM quantities, come fully sealed in non-vented, spill-proof cases and provide short-circuit, over-voltage and over-power protection. They feature universal AC inputs, IEC320 C14 inlet receptacles, 0A minimum load, no-load power consumption of less than 0.5 watts at 115 volts AC input, Class B electromagnetic interference compliance and cUL, UL, TUV and CE safety approvals

www.phihong.com.

6 Plant and Pipeline Security

In what it claims is the world's largest wide area video surveillance network, IndigoVision has deployed an integrated IP video security solution at a liquid natural gas plant and 500-mile gas pipeline as part of the Sakhalin-2 project in eastern Russia. Installation of the 600-plus camera system coincides with IndigoVision's continued expansion in Europe.

The company uses a network of approved partners to install their systems and has developed relationships with a number of important new European system integrators, such as G4S.

www.indigovision.com

7 Access Control System

IDenticard Systems introduces PremiSys, an access control system that integrates with the company's expressionsID badgemaker.

PremiSys' features include options for both area-based and timed intelligent antipassback, which recognizes reader use only if the door is opened. Dynamic mapping can be configured with drag-and-drop convenience. The system is compatible with multiple access control formats including biometric, proximity card, smart card, magnetic stripe and ABA readers, along with network connectivity for IP-based system functionality. An IDenticard start-up kit facilitates user configuration of a flexible and scaleable access control system.

www.identicard.com

8 Mass Notification Test

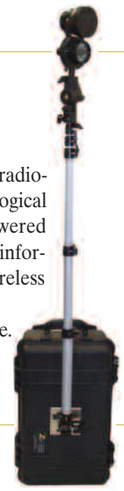
Virginia Tech has conducted the first campus-wide test of its emergency mass notification system since installing visual alerting displays. During the multimodal test, Virginia Tech instantly communicated to the vast majority of its campus community with Inova Solution's OnAlert LED displays, while other modes of communication, such as SMS/text and e-mail, took up to 20 minutes to deliver messages.

Inova OnAlert is a visual communications system that processes and displays customized messages on bright, visible LED wallboards. The displays normally show time and date information, and draw attention with audible alerts and/or color changes for emergency messages. Virginia Tech installed more than 200 OnAlert displays as part of its "VT Alerts" mass notification plan in August.

Comprised of a variety of methods, VT Alerts includes a mix of SMS/text messaging to mobile devices, calls to home, office or mobile phone numbers, e-mail notification and LED displays. The system cycles through all points of contact for a recipient until confirmation of receipt is received.

www.inovasolutions.com

9 Surveillance Camera



Zistos Corp. has unveiled its Portable Network Surveillance Camera system offering an optional built-in radiological alarm sensor. The PNSC provides a turnkey solution for day and night field surveillance and radiological monitoring applications where no power or pre-existing networks are available. The self-contained, self-powered system allows for dynamic deployment of single or multiple video surveillance cameras in the field. Video information is transmitted as IP data using a wireless 802.11 transmitter to any PC or laptop equipped with a wireless 802.11 interface.

Motion alarms can be programmed into the system to indicate changes to select areas of the video image. An optional built-in gamma alarm sensor can warn of elevated radiological levels along with the video.

www.zistos.com

10 Software Upgrade

GarrettCom has released new network timing and ring recovery capabilities to enhance the reliability of IP video security applications. MNS-6K-Secure Version 14.1, an extended security version of GarrettCom's Magnum MNS-6K managed network software, now supports rings in excess of 100 managed switches with fault recovery times averaging roughly 2 milliseconds per hop.

MNS-6K-Secure now provides synchronized time services for applications such as video surveillance where time-stamping accuracy is critical. It uses industry-standard Simple Networking Timing Protocol for interoperability. MNS-6K-SECURE also incorporates the new IEEE 802.1D-2004 standard for Rapid Spanning Tree Protocol, which offers a more robust and higher-speed implementation of RSTP that also can support larger ring and mesh networks.

www.garrettcom.com

11 Remote Access Control Monitoring

Isonas Security Systems' latest upgrade to the Crystal Matrix software, Crystal EasyWeb lets users control and monitor the ISONAS access control system from anywhere on the network through a Web browser.

Using the browser interface, users can maintain the ACS system's personnel database, monitor and control the current status of the doors within the system, review the ACS system's historical data and review the roster of who is currently logged into the facility. The software works with Windows XP Professional and Windows Server 2000/2003/2008. It requires a 1.8 GHz Pentium IV processor or higher and 1 GB memory.

www.isonas.com

SaaS Goes Mainstream

By Peter Wilenius

The growth of the software as a service model is good news for end users eager to reap the benefits of enterprise-class software solutions but unable or unwilling to purchase and host them in-house. Quick to gain traction in mainstream business application markets, the SaaS model is now poised to make its presence felt in the security and loss prevention markets.

Hosted by a software vendor and accessed over the Internet via a Web browser, SaaS applications allow end users to take advantage of powerful, enterprise-class software solutions without having to worry about an initial outlay of capital and the costs associated with support and maintenance.

By 2011, according to Gartner Inc., 25 percent of all business software spending will be for applications delivered under the SaaS model, up from 5 percent in 2005. Indeed, by that same year, Gartner predicts the worldwide market for SaaS will more than triple to $19.3 billion.

Extreme LP, March Networks' exception reporting solution, is one example of a powerful, enterprise-class application that security and loss prevention executives are now able to take advantage of on a subscription basis.

By 2011, the worldwide market for SaaS will more than triple to $19.3 billion.

A conventional, shrink-wrapped exception reporting application hosted in-house may be the best solution for tier-one retailers with the requisite financial and IT resources to acquire and support it, but many tier-two and tier-three retailers, those with anywhere from 10 to 100 locations, don't have the resources or IT infrastructure to go this route.

PAY AS YOU GO

A subscription-based, pay-as-you-go model also may be appealing to security executives with larger enterprises who may be reluctant to navigate a potentially time-consuming and unsuccessful capital approval process.

Opting for an application delivered via the SaaS model can dramatically reduce upfront

continued on page 34

costs for license fees, hardware and implementation services. It speeds deployment and frees the end user from all of the costs related to supporting and maintaining the application, including salaries, benefits, physical building space and power consumption.

Organizations subscribing to an application hosted by a software vendor also never have to worry about patches and software updates. In the loss prevention world, for example, customer-driven enhancements and new functionality reflected in updated versions of the software are immediately available to every subscriber, so the customer is never locked into a specific software release.

A single set of common code precludes customization, but applications delivered as a service can still be designed to allow the customer significant latitude to configure the software to respond to specific business requirements. The hosted Extreme LP solution, for example, flags voided transactions in excess of $50 but allows the end user to adjust the threshold to $20 and to create new rules if desired.

SECURE AND PRIVATE

The fear of relying on an Internet connection to access a hosted application may have been a factor when the SaaS model was introduced, but the risks of communication disruptions are less of a concern now, given the enhanced performance and security of today's Internet infrastructure.

Using encryption techniques compliant with Payment Card Industry Data Security Standards, for example, Extreme LP customers can transmit point-of-sale data to the vendor's data warehouse without worrying about privacy and security.

The SaaS model isn't an ideal choice for mission-critical applications, but it does offer end users a cost-efficient way to take advantage of software solutions that they might otherwise have to do without.

A cost-efficient means of deploying an exception reporting solution that reduces losses due to point-of-sale fraud is sure to be welcomed by retailers concerned about shrinking margins in today's turbulent economy. It represents just one way subscription-based delivery of software is gaining an increasing role in the broader physical security market as it is quickly going mainstream.

Peter Wilenius *is vice president of corporate development with March Networks, Ottawa, Ontario, a provider of intelligent IP video and business analysis applications.*