May 2017

ONVIF® | Standardizing IP Connectivity for Physical Security

Cyber Security's Balancing Act Between Availability and Protection

Jonathan Lewit, Chair of ONVIF Communication Committee

- As many as 50 billion IoT devices are estimated to be connected to a network in the next three years
- The IoT and the cloud presents both great opportunities for data and availability but also high cyber security risks for organizations
- ONVIF standards for interoperability incorporates industry recognized best practices for cyber security
- Manufacturers, end users and systems integrators can all take steps to improve cyber security

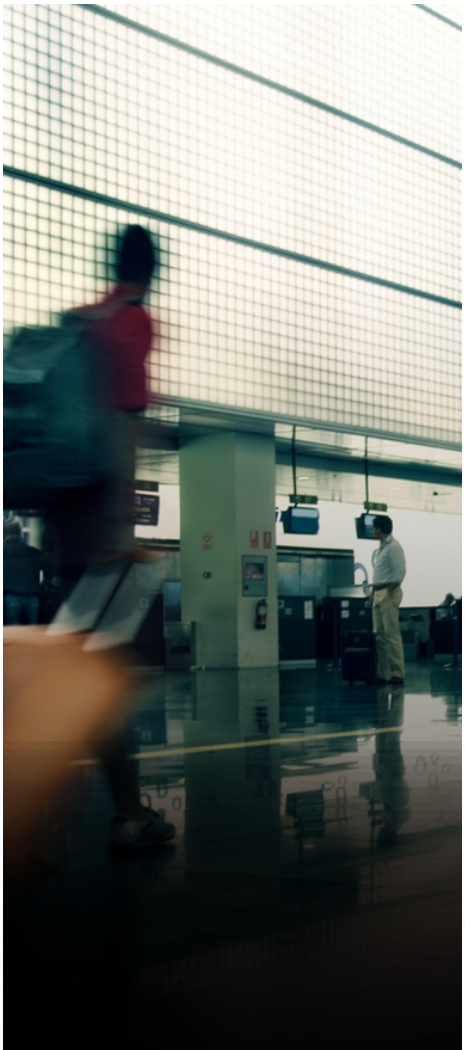
Energy security, access to the electrical grid and police and fire safety are just a handful of the networked services that we take for granted and rely upon on a daily basis. Every second of every day, sensors are digitizing the real world, creating information and transporting it across multiple networks and interfaces to a broadening audience. While there is obvious utility being gleaned from this process, from our vantage point here in the physical security space, information sharing and transmission raises issues we have to consider: what happens to this information inside those organizations, and what risks are presented by increasing the communication in and out of these organizations, in the name of utility?

In a world where convenience and anytime availability can make or break a business, information availability and always-on connectivity are here to stay. Much as the Industrial Revolution brought key innovations and new challenges, this new Information Revolution is shaking up the accepted paradigms. The explosion of demand for mobile access to information and increased opportunities for interconnectivity are a fact of life, both at home and for business. We can use security information to answer questions such as: How efficient are your delivery routes? What cameras saw the guy with the red shirt? Is that the UPS delivery man at the door?

But interconnectivity and high data availability also represent high risk for organizations that are concerned about threats to their information security. A hunger for more information upon which to base decisions and actions is driving the proliferation of big data, video analytics, cloud storage and Internet of Things deployments, while ratcheting up our risk profiles and the potential for cyber-attack.

Making Best Practices Standard

The mission of ONVIF is to establish a common communication interface for all security devices and clients, across security disciplines, systems and vendors. While ONVIF does not set security policy, what many people don't realize is that industry proven cyber security measures can be included in the common interface established by ONVIF. Among these are Certificate Based Client Authentication, Keystores and TLS Servers. There are also best practices that can be encouraged, such as forcing a default password change or out of the box hardening. ONVIF and other standards



The mission of ONVIF is to establish a common communication interface for all security devices and clients, across security disciplines, systems and vendors. ONVIF can help ensure and deploy real-time security by including these established cyber security measures in their Profiles and standards.

SOUND CYBER SECURITY PRACTICES

groups can help ensure and deploy real-time security by including these established cyber security measures in their Profiles and standards. The establishment of a common interface by ONVIF and other standards organizations helps to bring awareness about the capabilities of standards in this area and enables manufacturing companies to invest once in this approach rather than continually developing proprietary products and unique interfaces to integrate with other devices. Safe/smart city deployments and Internet of Things systems are helping to accelerate acceptance of interoperability over proprietary systems.

In fact, it's estimated that as many as 50 billion IoT devices will be connected to a network over the next three years, all requiring some measure of interoperability. If you're concerned about the security of information, that number can seem alarmingly high. The good news is that IoT security budgets are also expected to increase substantially over the next three years. And there some changes that we, as an industry, can proactively make in the meantime.

The Weakest Link

Remember that a single device or product alone cannot be cyber secure if it's connected to an unsecured network or to a network with other vulnerable devices. People, products and processes – these three elements together can provide security, but if you don't have sound cyber security practices in place for all three, you won't have complete security.

Manufacturers of physical security products can use encryption technology to help harden IoT devices. They can ship products with default settings that require end users to change the default password on install and that also require password changes periodically. It's also worth exploring whether some settings on devices should be locked down to protect our customers, for example making encryption part of the factory settings, increasing the likelihood that encryption is left enabled on the device.

End users and system integrators also have some responsibility to bear. Approximately 95 percent of the security breaches that occur today are due to some sort of simple password error or lack of organizational policies with respect to password management. It takes only a matter of seconds to very quickly choose a simple, easy to remember password. However, relying on the most convenient solution – often the default password - can most definitely increase the potential for compromised access to our most private information.

As is the case with many things, a balancing act is required when it comes to information availability and securing access to that information. Each end user and system integrator has to find the right balance between availability of data and protection of that data, taking cost into consideration as well.

Strong user authentication, event monitoring, activity logging, encryption of data and other controls that are built into our IT networks go a long way in increasing cyber security. Using standards like those offered by ONVIF may actually be the key to having the best of both worlds: the ability to share information with other devices using standardized, encrypted communications.