BY RAY COULOMBE

The Inside Scoop on ONVIF

The first in a series of columns outlining security interoperability standards

This is the first of a series on security industry standards, de-facto-standards, or near-standards to address user need for security devices to seamlessly interoperate. The first is on ONVIF.

ONVIF was originally organized as the Open Network Video Interface Forum in 2008 by Axis, Bosch and Sony. With IT standards in mind, these companies realized that standards for devices and clients to communicate and operate with a high level of functionality would be vital to the long-term health of the industry. Today, ONVIF has 31 full members, an additional 21 contributing members and another 454 user members (see www.onvif.org for more info). The initial focus was on video systems, but ONVIF has expanded to include access control and other technologies.

Tackling Interoperability

A key to any approach tying together disparate systems is the software means through which they interact. ONVIF uses a protocol called SOAP (Simple Object Access Protocol), originally designed in 1998. A SOAP message is an XML document which contains an envelope and message body and may contain a header and fault information. HTTP or HTTPS is typically used as the transport protocol.

One critique of SOAP is the verbosity of its messages; however, it has a defined set of specifications for security and reliable messaging, and requires its standards to be strictly followed. Note that UPnP (Universal Plug and Play) — a set of networking protocols for network device discovery and communications — uses HTTP, XML and SOAP.

There is controversy about SOAP vs. a competitive technique called REST (for Representational State Transfer) used by the PSIA standardization effort. REST is said to be more architecture than protocol, and it has become popular for web interface and cloud applications.

Inside the Specifications and Profiles

ONVIF maintains one core specification and a series of "profiles" — which are subsets of the main specification that denote sets of similar features and functions. Specifications evolve, get updated and have version numbers; profiles, once adopted, do not change and do not have version numbers. All ONVIF-conformant devices and clients comply with the requirements of one or more profiles, rather than declaring conformance to the current version of the core specification.

The Network Interface Specification Set contains the latest core specification, version 2.5 (Dec. 2014), which covers device discovery, device management and an event framework; data format specification for streaming and export file format; and the relevant service specifications, which define the ONVIF-compliant services used by the particular device type (such as PTZ, device IO and door control).

There are also specifications for WSDL (Web Services Description Language), an XML-based language used to describe and access services; and XML schema (an organizational structure of the data).

> "Profile Q targets **integrators, installers, specifiers and users** by addressing out-of-the-box interoperability and quick set-up."

ONVIF Profiles provide the means to identify interoperable products and the spell out the requirement level that devices and clients must meet. Mandatory features and functions must be supported unconditionally — for example, streaming of MJPEG video using RTSP. Optional features and functions are not required to be implemented; however, if they are, they must meet the ONVIF profile (e.g., streaming of MPEG4 video and successfully pass the tests described in the ONVIF test specification). If a conditional feature or function appears in a product, it must be supported per its profile (for example, door lockdown in access control). Currently, there are three profiles that have been finalized, with a fourth slated for release in June 2015.

The S Main Video Profile was adopted in Dec. 2011, and covers video and audio streaming. It also includes PTZ, metadata and relays. The C Access Control Profile was adopted in Dec. 2013, and includes information retrieval, door control and events. The

G Profile is for storage and content management, and was adopted in June 2014.

Perhaps the most impactful is the pending Profile Q, which was expected to be adopted this June. Interestingly, there had been no requirement for the actual enabling of ONVIF services in compliant devices. Profile Q targets integrators, installers, specifiers and users by addressing out-of-the-box interoperability and quick set-up. A Profile Q compliant device can be discovered and configured for parameters such as network address, time setting, authentication and security settings by a similarly compliant client. Read more about Profile Q in this exclusive article from the March issue of *SD&I*: www.securityinfowatch.com/12046194.

Industry cyber expert Rodney Thayer of RSG Modelworks is naturally skeptical of auto-configuration tools, feeling that, without proper safeguards, an exploitation opportunity may exist. He counsels: "Mechanisms to provide auto-discovery should be able to be disabled or turned off after installation."

ONVIF representatives have verified that, after first being setup, the security protocols and authentication methods are fully turned on.

Ensuring Conformance

So how does ONVIF administer its conformance process to ensure that the functionality people expect is actually there? While the process is a self-declaration by the manufacturer, it uses the ONVIF Device Test Tool that generates a Declaration of Conformance — an XML document that provides information and guidance for initial steps to operate the ONVIF device or client.

The current ONVIF Profile Q Test Specification covers the Profile Q-conformant transition from a device (unsecure) status after a factory reset command has been executed up to when ONVIF Default Access Policy is applied. Testing will employ packet capture to validate the content of data and tests will also include applying the setup stages and verifying the correct settings, including security and authentication.

"Today's test tool has evolved since we first launched it, and it is much stricter than before," explains Stuart Rawling, Chairman of the ONVIF Communication Committee and Director of Business Development at Pelco by Schneider Electric. "In the past, a device might pass the test tool, but occasionally have issues in a real-world environment. The latest test tool drastically reduces that potential." ■

» **Ray Coulombe** is Founder and Managing Director of SecuritySpecifiers.com and RepsForSecurity.com. Email him at ray@SecuritySpecifiers.com, or follow him on Twitter, @RayCoulombe.