
The Case for an Open Source Physical Security Software

I have integrated several physical security systems with logical identity and access management systems over the last several years. Each time I was amazed at the way that the physical security vendors worked: proprietary software with proprietary hardware. Every time I'd think that one day digital convergence would bring an end to this. This paper will outline my views on why an open source physical security software's time has come.

Open Source

Open source is the practice of making available a product's "blueprints" in the public domain. "Open Source" began in the days of Henry Ford, when he broke a monopoly on car patents and created the beginnings of the Motor Vehicle Manufacturers Association. Open source came into its own in the software industry with IBM releasing its code for source releases, the development of the internet using TCP/IP and many subsequent others including Netscape Navigator and Linux.

Does open source software enable better security? Any weaknesses are out there for the public to identify and then be quickly remedied. Many software security experts such as Bruce Schneier say "demand open source code for anything related to security" [Schneier 1999].

However, just because software is open source doesn't mean it is more secure. If vulnerabilities exist in the software and remain undetected, then the code is vulnerable. The way the software is implemented and maintained often opens up security vulnerabilities. Therefore the organization that manages the overall code and the folks who implement it need to have very high standards.

This compares to the usual defence of saying by keeping software code private it is more "secure". Security by obscurity has been argued for many years, especially by proprietary vendors. In the early days of a new technology, obscurity can aid in protecting the security. However, over time, the value of obscurity decreases as the technology becomes better understood. Generally, security increases when minimizing reliance on obscurity.

My premise is that physical security software is not new technology anymore. The technology has been around for many years and therefore there is little value to the argument by keeping the source code private that the overall security will be better.

Benefits of Open Source Security Code

I think there are many potential benefits to open source physical security software:

- Lower cost for software
- Plug and play with many different physical security hardware vendors
- Easy integration with identity and access management systems
- Defined security standards
- Lower cost operations for enterprises who outsource their physical security monitoring

Lower Cost Software

The open source formula usually delivers free software with a low yearly license. Use of this software should lower enterprises overall physical security budget over time as opposed to paying proprietary vendors large purchase amounts and annual license fees.

Plug and Play

There is an ongoing initiative within the physical security industry to develop protocols allowing for easier interoperation. However, I believe that open source software will result in dramatic increases in the ability to have different devices, sensors and authentication mechanisms working with the software.

Easy Integration with Identity and Access Management Systems

Open source software would automatically have built into it open protocols such as SAML (Secure Assertion Markup Language), SPML (Service Provisioning Markup Language), XACML (eXtensible Access Control Markup Language), LDAP (Lightweight Directory Access Protocol) and many other emerging privacy, identity and network standards. This means that the integration with enterprise identity and access management systems would become much easier, quicker to implement and at a lower cost than it is today.

Defined Security Standards

Open source would use accepted encryption and other security standards. These would be subject to much public testing and over time, will result in a secure system.

Lower Cost Operations for Enterprises Outsourcing

Many larger enterprises have out-sourced their security guard, physical security camera and overall physical security operations to out-sourced vendors. I believe that, over time, as physical security open source software comes into its own, this will aid enterprises in easier replacement of one out-sourced vendor for another. Why? The training costs for operating the software should be lower since the software will be the same.

A Five to Seven Year Vision

Just because someone will one day introduce open source physical security software does not mean that all the above benefits will magically appear. It will take time for the source code to be tested and for enterprises to want to adopt the code. There will likely be a huge push back from the main physical security vendors as this occurs.

I take a five to seven year vision of this happening. First the code has to be written and a credible organization created to oversee the code development, test the code and design implementation standards. Then enterprises will start to step up and use the code. It's likely that smaller enterprises will be first adopters. Then as the wave begins to roll, it will expand to larger enterprises.

Five to seven years from now I see open source physical security software, running over IT networks, talking to open source authentication and sensor devices tightly integrated with the enterprise identity and access management systems.

In larger enterprises, I see them using this software to help them centralize all physical and logical security policies into one central policy store (with many localized subsets). This will enable the enterprise to match a identity's access rights to both physical and logical and to do simultaneous policy assessments on their rights.

About the Author

Guy Huntington has been in the identity industry for the last 14 years. He has rescued several large Fortune 500 identity projects and written numerous white papers on identity and physical and logical access and integration (<http://www.authenticationworld.com/papers.html>). Guy can be reached at guy@hvl.net or 1- 604-861-6804.