How a Standard Interface Heightens Cybersecurity Measures using Location Data

A white paper for corporate security system integrators

Mohammad Soleimani,
CTO Kastle Systems and Chairman PSIA
August 2016

65 Washington St., Suite 170 • Santa Clara, CA 95050 • 650-938-6945 • FAX 408-516-3950

Abstract

This white paper presents the use-case and solution for industries where the protection of critical infrastructure is of paramount importance. The approach that is outlined integrates physical access control systems (PACS) with a logical system that receives real-time location information from the PACS, which serves as a gating mechanism for high-security operations. This integration solution uses a standardized method and extends the use of multi-factor authentication for cybersecurity.

In today's world, virtually no large industry or small business is impervious to some form of security threats or breaches. Consequently, corporations and business owners are taking the necessary steps to protect their employees, building staff, and visitors, to safeguard their building perimeter, and to shield their assets through access control systems and cybersecurity measures.

Many companies are deploying PACS in order to maintain secure and appropriate building access for personnel, even across multiple locations, and to restrict access to designated areas for building tenants. Already well-equipped to perform up to three-factor authentication checks, PACS offer robust security measures and tracking to support these requirements where verification includes a combination of one or more of:

- What you have (credentials)
- What you know (passcode or pin)
- What you are (biometric, such as fingerprint or iris scan)

Even so, industries where the protection of highly-sensitive controls is essential, this approach leaves to chance potentially devastating effects if security is violated by remote hackers. To combat this risk, the need to verify location information as provided by the PACS is an important line of defense.

Streamlining the integration of PACS with a logical system for high-security operations, the Physical Security Interoperability Alliance (PSIA) provides a standard interface that enables passing of location data to an event consumer: the Physical-Logical Access Interoperability (PLAI) specification. This paper describes the PLAI solution and its application and benefits in high-security PACS environments, and presents how one client is implementing PLAI to use the location data over an event stream in order to perform authentication functions.

Potential Risks in High Security Environments

Particularly challenging in the realm of cybersecurity is the fast pace at which security risks are constantly evolving. Protecting networks, computers, programs, and data from damage or unauthorized access requires a combination of continuously advancing technologies, processes, and practices. The urgency to stay ahead of cybercrime is reflected in the projection that spending on worldwide cybersecurity will increase to $170 billion by the year 2020.[1]

Industry sectors such as utilities, transportation, federal agencies, and others are increasingly becoming enticing targets for remote hackers. While multi-factor authentication is a key part in guarding against hacking, the industry is rapidly realizing the value current location in decision making. In high-security environments, where knowing that the individual requesting permission to perform a sensitive task or operation is qualified and on-site, leveraging the PACS via the PLAI standard interface is a smart approach.

PLAI Heightens Security Measures using Location Data

PLAI provides the ability to integrate PACS and a logical system (the event consumer) for access to high-security controls and over a well-defined HTTPS REpresentational State Transfer (REST) application program interface (API); it is adaptable when having to add or replace one or more of the PACS or high-security components. This standard interface is built with extensibility in mind, which makes not only adding features into the specification relatively easy, but also makes it so that users can customize and extend the features of PLAI if necessary.

Figure 1 shows how PLAI is implemented in a high-security PACS environment to support the sharing of location data over a REST API. In this scenario:

- The PACS (REST servers) pass location data over the PLAI event stream as requested via HTTPS GETs from the REST client. With the content type multipart-mixed, multiple events can stream in one transaction, limiting the HTTPS overhead involved while still leveraging standard HTTP protocols.
- The event consumer (REST client) performs HTTPS GETs and then executes its functions based on location information and other verification checks.

Figure 1

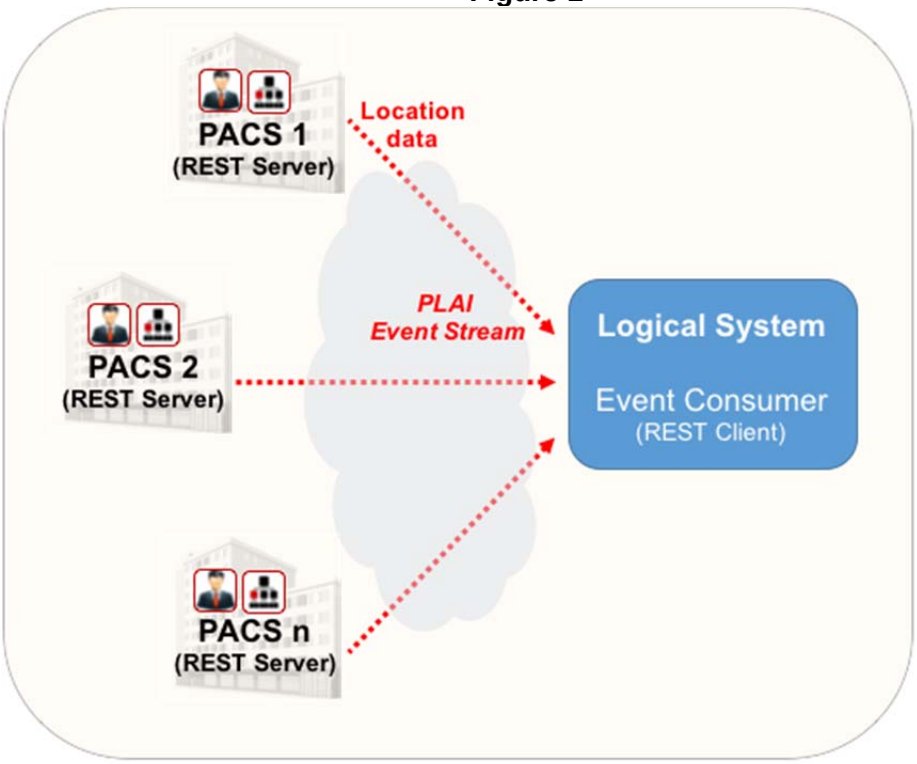

Figure 1. Physical-Logical Access Interoperability (PLAI) provides sharing of location data between the PACS's and the event consumer over an HTTPS REST API. The event consumer uses this data for "3+1" multi-factor authentication for heightened security measures. This data enables verification that the individual performing the high-security operation is on-site.

In this scenario, integrating PACS with a logical system/event consumer provides the ability to perform verification checks on any combination of credentials, passcodes, or pins, biometrics, and also passes the user's location. Doing so ensures that the individual who is requesting access to perform a high-security task is actually on-site and intends to execute the operation. The ability to perform the additional location verification heightens multi-factor security measures and provides a critical safeguard in the defense against overseas hackers.

Solution Benefits

In high-security PACS environments, PLAI offers benefits such as:

- Clearly-defined specifications for security device communications, which offers significant cost savings on API development and potentially more resources for the development of new features and enhancements.
- Plug-and-play integration, which delivers a streamlined solution in lieu of costly and labor-intensive custom code and scripts.
- Common-event language interoperability, which provides a unified view of security data and the ability to trigger automated responses or alerts in other systems.
- Backwards compatibility, which ensures scalability with compliant devices regardless of version level.
- Robust specifications, which support operating system or application software upgrades with transparency and eliminate custom interface maintenance expenses.[2]

Application Example

More than 65 physical security manufacturers and systems integrators have been involved in advancing standards through the PSIA. Most of the leading access control companies are engaged in the development of the PLAI specification. Their focus is on promoting interoperability of IP-enabled security devices and systems and developing open specifications pertaining to networked physical security technology.[3]

PLAI was demonstrated at ISC West (April 2016) and extensions to the specification are continually being evaluated within the PSIA PLAI Working Group to enhance its functionality. Other vendors actively involved in the development of PLAI include Tyco, Lenel, Honeywell, Kastle Systems, Stanley Security, Tridium, Right Crowd, AlertEnterprise!, and Gallagher.

For the ASIS 2016 PSIA demo, AlertEnterprise! implemented PLAI for the purposes of providing a gating mechanism, granting users the permission to perform high-security tasks such as activating or changing an industrial control parameter only if they are physically present at the site. By way of a connector that listens to PLAI event streams, AlertEnterprise! is able to maintain location awareness of individuals who have access to highly sensitive controls. This security measure involves integration with PLAI-compliant PACS and, as needed, multi-factor authentication to verify what the individual has (their credentials), what they know (passcode or pin), what they are (biometric verification), and additionally, where they are (current location). If their presence is not validated, then it is assumed that an unexpected cyberevent is unfolding and appropriate mitigation steps can be initiated. For this demo, Kastle Systems and Lenel provided PLAI-based access event streaming functionality.

Summary

Across the gamut of industry sectors that depend upon multi-factor authentication to function highly-sensitive controls – including power and gas companies, transportation and airports, government agencies, and others – PLAI offers a cost-efficient and scalable approach to integrate PACS and logical systems.

In these high-security environments, PLAI leverages the sharing of location data to strengthen multi-factor authentication checks by further verifying that the individual requesting access to perform a sensitive task is indeed on-site. High-security PACS integration solutions using PLAI provide a standardized approach for connecting to a logical system/event consumer and boast "3+1" factor authentication checks for:

- What you have (credentials)
- What you know (passcode or pin)
- What you are (biometric, such as fingerprint or iris scan)
- +1 = Where you are (current location)

This application of PLAI enhances multi-factor authentication with location verification to defend against remote hackers. As the need for cybersecurity continues to grow, this heightened measure of security to protect critical infrastructure is an important shield to counteract cybercrime.

With PLAI, a flexible PACS system integration with logical systems is possible. The PLAI solution offers all the benefits of a standards-based interface and is suitable for the integration needs of today and easily scalable to meet future needs as directed by growth and change.

To become a PSIA member, or for PLAI specification details and other documentation to help meet your integration needs, please visit the PSIA website: www.psialliance.org.

References

[1] Morgan, Steve. "Worldwide Cybersecurity Spending Increasing To $170 Billion By 2020." *Forbes.* March 9, 2016. Retrieved from http://www.forbes.com/sites/stevemorgan/2016/03/09/worldwide-cybersecurity-spending-increasing-to-170-billion-by-2020/#56b4ce2e76f8.
[2] PSIA Alliance, "Backgrounder: The PSIA Family of Specifications," PSIA Specifications and Documents. Retrieved from http://psialliance.org/SpecificationsOverview.html.
[3] PSIA Alliance, "Organization," PSIA About the Organization. Retrieved from http://www.psialliance.org/org.html.

Mohammad Soleimani *is CTO at Kastle Systems and chairman of PSIA. He may be contacted at msoleimani@kastle.com.*

Appendix – PLAI Specification XML Code Sample

The following PLAI XML sample shows the structure and parameters for the location information of a credential holder:

```
<?xml version="1.0" encoding="utf-8"?>
<AreaControlEvent xmlns="urn:psialliance-org">
<MetadataHeader>
  <MetaVersion>1</MetaVersion>
  <MetaID>/psialliance.org/AreaControl.Portal/access.granted/20719027</
MetaID>
  <MetaSourceID>{B02AD31A-4AF2-41F0-AA61-75CBD6B200C6}</MetaSourceID>
  <MetaSourceLocalID>20719027</MetaSourceLocalID>
  <MetaTime>2016-09-06T16:21:04.1052888-04:00</MetaTime>
  <MetaPriority>4</MetaPriority>
</MetadataHeader>
<EventData>
  <ValueState><Granted>OK</Granted></ValueState>
  <PortalIDList><PortalID><ID>20719027</ID><Name>DC0989 Reader
405</Name></PortalID></PortalIDList>
  <CredentialIDList><CredentialID><GUID>{88736DD5-4A82-4766-BDEB-
D1D42EA1FEF8}</GUID></CredentialID></CredentialIDList>
  <CredentialHolderIDList><CredentialHolderID><GUID>{583D2E27-1058-
477B-A0E8-
6AE58D5871EF}</GUID></CredentialHolderID></CredentialHolderIDList>
  <Info>Lobby Level, In Zone 1</Info>
</EventData>
</AreaControlEvent>
```