Securiteam Case Study - Access Control

Background

Customer is involved in shipping and transportation at a local port, responsible for docking ships, offloading, storage and distribution of cargo. Due to the nature of their business, coupled with the constraints and logistics of their physical geography, the property is tightly regulated as to who can, or cannot gain access. In addition to their internal regulations and protocols, they are subject to directives and requirements of the Department of Homeland Security aalong with the Department of transportation. As the port expands both in acerage and volume, being able to more thororughly and accurately identifypersonnel as they 'come and go' becomes increasingly vital.

Problem Being Addressed

As Securiteam began their discovery and design process, there were two major issues that need to be accounted for:

1. Transportation workers are required to carry a TWIC card, which serves as a means to validate an individual who may be attempting to enter a port area. The TWIC card utilizes FIPS technology, a level of data encoding that contains more information that with a standard Weigand output. This data would then be displayed on a monitor at 2 attended guard stations to provide staff with a method of visual verficiation.
2. The means of Transportation Worker validation would only serve as a first step in the organization's overall Physical Access Control System (PACS) deployment. The actual comprehensive access control system would not be installed for 18 months from the completion of the initial phase.

The factors, combined with additional "wants" of the stakeholders (centralized remote management, ease of operation, database migration, video integration, etc…) meant that whatever system installed would by necessity have to be scalable nationally as well as locally. This could not be treated as a standard "6 door" access control system. The chosen solution would require creativity as well as technical skill to successfully configure.

The Approach Taken

Because of the reuirements for conclusive validation of identification, we Securiteam utilized a linux based, embedded access control solution along with FIPS compliant reqaders. These initial appliances have been combined with a server interface to a national TWIC holder database ensuring that the information received by guards at the point of port access is as current and accurate as possible. This initial phase has since been incorporated to an overall port access control system which serves not only to validate, but to regulate who is granted access where and under what conditions.

Results

Having used the system for over 2 years, the client is extrememly pleased with how the initial deployment has exceeded their original requirements and expectations.

The scalability of the overall solution has ensured that further deployment can proceeed without an additional investment in infrastructure or software. Additionally, the database, along with permissions and allowances, can be managed remotely at the corporation headquarters.

Finally, the infrastructure will enable rollout of similar design solutions at other port locations within the area and nationwide. As a person is entered into the system, they can be granted access at any site within the network. Another benefit for the end user is that the server is eligible for firmware upgrades when improved technology is available for distribution, ensuring that their technology is never out of date.

Finally, we were able to pass along to the custiomer the lower installation costs and economies of scale available with an IP based solution. As a result, less of their investment dollar went toward labor costs and expendables such as wire and hardware associated with older, less technologically advanced, analog systems and more was invested in the flexibility of the technology.