

Why Active Directory Represents the Future of Physical Security

Executive Summary and Background

This white paper discusses a new architecture for physical security being developed by VSI Viscount based on the concept that Active Directory has the inherent ability to render control hardware obsolete.

At a core level there is very little difference between Active Directory and physical security systems. Active Directory assigns IT permissions defined by schedules, groups and times. A physical security system also assigns door open permissions based on schedules, groups and times. However, physical security systems require masses of expensive control hardware.

Other than the sheer cost of installing and maintaining control hardware the real issue is that control panels are designed using C+ or other code that precludes the ability to properly deploy access control on IT platforms and that must be matched to PC programming software. Each new panel software version or PC programming version sows the seeds of obsolescence of previous versions. Panels are also proprietary and are not interoperable between suppliers.

End users, having selected a system and having deployed masses of control panels often feel trapped and compelled to continue with the same system. IT departments see little logic to this hardware based architecture and are often at odds with security departments over the management of security software.

Active Directory as a Physical Security System

An Active Directory structure is a hierarchical framework of objects. Each object represents a single entity — whether a user, a computer, a printer, or a group — and its attributes. In general, there is no difference between an Active Directory object and a physical security object. In physical security typical entities would be users and devices (door readers, elevators, and locking hardware). However, because control hardware provides additional functions required to control doors and sensors, the challenge to developing an Active Directory Physical Security system is developing low cost IP bridges (see Freedom bridge hardware below).

In Active Directory an object is uniquely identified by its name and has a set of attributes — the characteristics and information that the object can contain — defined by a schema, which also determines the kinds of objects that can be stored in Active Directory. So, for physical security the objects and attributes will be contained within a physical security schema within Active Directory and with an over layed messaging protocol applet.

MESH Freedom Hardware

Instead of control panels the new architecture allows users to connect any standard reader type (wiegand, iclass, FIPs etc.) directly to a network through inexpensive IP

bridges. Each bridge is essentially an IP switch that includes specialized card access components including reader inputs and ports to manage inputs and door outputs. When a card is presented at a reader, the reader sends a message to the bridge that encrypts the message. The message is sent to an Active Directory server for validation and a message is then sent to the bridge to enable door control. High availability and synchronized Active Directory servers can supply redundancy not possible with control panels.

Each Freedom Bridge is designed with fault tolerant software that will allow the bridge to connect to any synchronized server on a network. For example, if a server in facility A fails, the bridge will simply contact other servers B thru X within the Enterprise to find an open path for door control.

Each Freedom Bridge comes with 2 inputs and 1 door open output per reader. All wired switches are POE enabled with a power input where necessary.

Summary

VSI sees the future of physical security as one in which card readers and sensors will simply be managed devices within an IT platform and user databases will be managed within the framework of existing logical security databases. For large Enterprises, further integration with XACML, SAML, and SPML policy servers will allow physical security policies to be written and enforced from the enterprise access control policy store. This is simply not possible with today's proprietary control panels.

For end users, this represents a more sensible and much more affordable approach to physical security. This new architecture represents a severe technological disruption to the business model of control panel suppliers. However, for major IT suppliers this represents an excellent opportunity to enter an otherwise closed market due to the presence of control panels by providing physical security as a software application using their existing IT architecture and within their existing market channels.

VSI – Freeing the world from the oppression of proprietary hardware

Prepared By: Stephen Pineau

President and CEO Viscount Systems Inc.

November 2010