Open-data Architecture Identification Systems

Lobby Track, integrated security software

by

Sandeep Jolly & Kurt Bell

Jolly Technologies

Open-data Architecture Identification Systems

Aside from physical barriers like doors and locks, information has become today's single-most critical security mechanism. Intelligent information management is the new backbone for secure environments

Effective security systems need to provide the information to answer these five basic questions about ANYONE on premises:

- Who are they?
- What are they doing?
- When will they be or when were they on the premises?
- Where are they going and where have they been?
- Why are/were they on the premises?

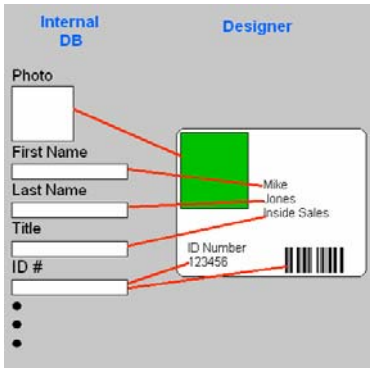
More importantly, if that information exists, is it readily available to the key personnel that need it?

Background

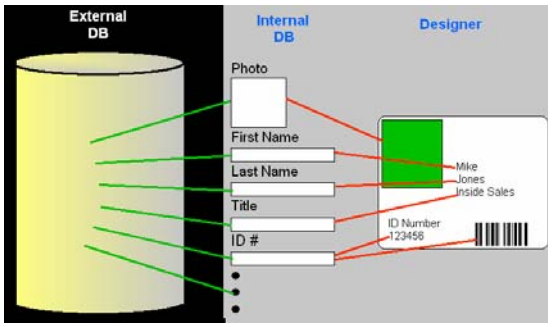
Most of today's existing security products emerged on the market with a single purpose: To print an ID card, to control access policy, to track visitors, etc. That these products could be a piece of a much broader information system was an afterthought.

To illustrate this point, look at the evolution of ID card software.

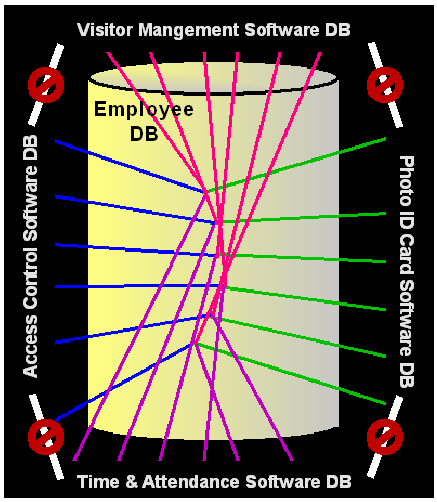
Historically, identification production software existed in a vacuum: Closed systems for entering an individual's personal information, taking a photo and producing an ID card. These systems either utilized a fill-in form for entry without any historical recording or an internal database, without connectivity to any external information systems. The form elements were tied to a card design tool and ID cards could be printed.



With the evolution and prevalence of network computing, single-purpose data entry made little sense. In most instances today, some or all of the data required for credentialing already exists in some data repository. To accommodate this fundamental shift, historical products developed a process for tying product-internal databases to external organizational data networks. Utilities emerged with misnomers such as "link-live." Through open database connections and a series of complex field mapping, these products established synchronized data connections. Synchronized data is not "live."



Visitor management, access control and time & attendance software share a similar history: Each maintain internal data structures though can link to an external data source. The result has been the emergence of disjointed systems sometimes linked to common databases that may share some record data, though otherwise share no behavioral information with each other:



This current situation for most organizations shares a striking resemblance to the disjointed U.S. security agencies prior to 9/11: A lot of data, but no information.

Given this situation; ask yourself some questions. When an incident does occur, is it possible to identify: *Who was where when?* and, *Why were they there then*? How many systems need to be consulted? How fast are you able to respond? Can you answer these questions at all?

This environment has also made central security information management cumbersome. Take, for example, the simple scenario of transitioning from barcode-identification cards to proximity cards. In the diagram above, all five of the data systems may need a new field added to accommodate the proximity card number; each may have a different database type; each may have a different systems manager; and each would need the database link re-established and the fields remapped. In some systems, adding the field is not even possible.

The recent trend amongst many security manufacturers is to combine several of these key security software functions into a single product or product suite, that yield some abilities to combine some data, log and reporting functionality. In the majority of instances, however, the driver for this product integration has been the cross-sell opportunity rather than tighter information management. And, proficient manufacturers in one respect may ultimately step out of bounds of competency in another arena in their pursuit of the horizontal dollar. Result: weakened, not strengthened security.

Another major drawback is the limitation of data-mapping itself. Internal data architecture prohibits mapping to more than one other database simultaneously. The only fix for this has been importing several databases into a single personnel, visitor, contractor or ID cardholder database. The result is more tedious management processes and the loss of relevant information.

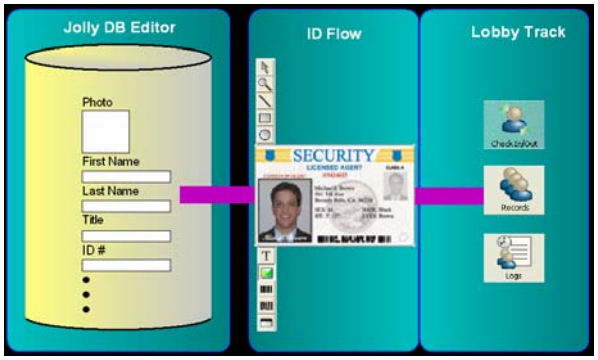
The vast majority of today's security software products share this common architectural shortcoming simply because they evolved from stand-alone products and inherited the trait. The only answers have been comprehensive solutions from the big security vendors and expensive systems integration projects: until recently.

The dawn of open-data architecture security software

Jolly Technologies (www.jollytech.com) of San Carlos, California has recently launched a new line of security products with a *why-doesn't-everyone-do-this* architecture.

The product line includes ID Flow for ID card design and production and Lobby Track billed as "visitor" verification, tracking, and access control; though extends these functions to any number of cardholder groups: visitors, employees, contractors, students, faculty…

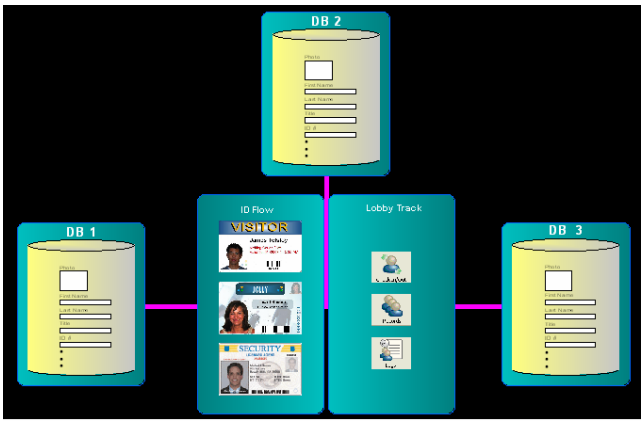
Incorporating open-data architecture enables Jolly to piggy-back on any open data source without needing an internal database. (Jolly does provide a generic and five vertical specific databases should the customer prefer one.) Through a few mouse clicks, users establish an ODBC or OLE DB that places a rich data-editor on top of the existing database. The single link establishes connection and provides access to all the data fields.



Jolly's data editor is essentially a shell that allows the data layout to be customized through drag-and-drop tools. It enables data fields to: be formatted with different captions, fonts and colors; be made visible or not; have their data types modified; have drop-down lists created; and be automatically updated after actions without affecting the functionality of the original database.

Fields may also be set as look-up fields that quickly populate data fields from other data sources.

Through the use of ***cardholder groups***, Jolly products are able to connect to multiple data sources simultaneously.



Detailed logs may be run for each cardholder, cardholder group and across all cardholder groups. Lobby Track records and verifies cardholders through check points. Database connections, logs, reports, user permissions and other configuration are centrally managed though a single "company" file. This also allows additional locations to be added and networked quickly.

Lobby Track contains the ability to set access rules intended to be monitored by an attendant. Through the open data structure, in may also interface directly with existing access control systems. Time & Attendance information may be exported into other accounting software.

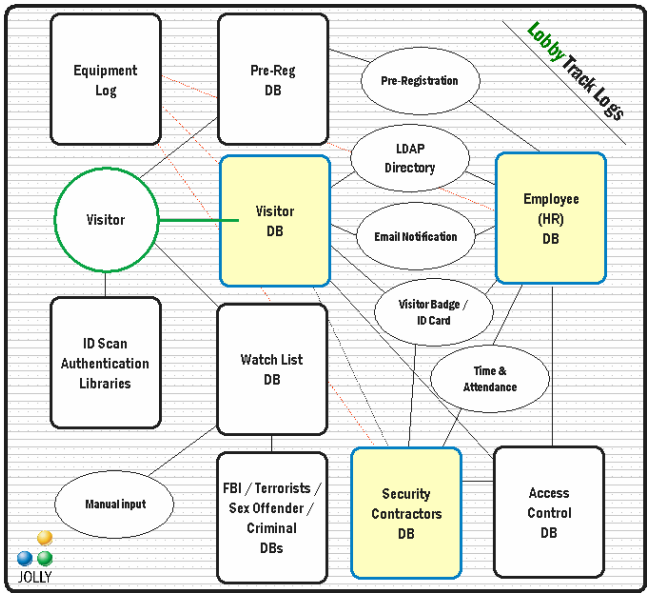
The products also permit internet data to be imported via XML and a Command Line Interface enables ID cards to be printed in the background from other products.

The Missing Link

The Lobby Track management system establishes a secure community for disjointed data sets to connect.

The key to this rich information system is that ability to connect to multiple data systems simultaneously in real time. As such, reports can be run across the activity of all the independent systems. Visitors can verify against other data systems and data fields can be populated from other data fields. Fields can even automatically update based on the cardholders activity.

In the scenario below, eleven different points of data are combined into one seamless security system that includes 3 cardholder groups: visitors, employees and members of an outsourced security company.



Here's how this scenario works:

1. Visitors present their driver's license, passport of other government identification. The ID is scanned and verified against a library to authenticate its validity. The visitor's name, address, photo, signature and other information automatically populate the visitor record.
2. The watch list may be populated by data from government terrorists, sex offender and other criminal lists.
3. Disgruntled former employees, estranged spouses, troubled students and those with restraining orders can also be imported into the watch list. The visitor is checked against the combined watch list.

4. Guests may be pre-registered by employees through the pre-registration database and lists imported.
5. The visitor record's host fields are populated either directly from an employee cardholder group or by LDAP lookup and the host can be automatically emailed notification when their guest arrives.
6. The visitor is issued a temporary visitor badge, employees and contractors receive permanent identification cards that are printed directly from their cardholder group record using ID Flow.
7. Each time a cardholder enters the facility, or crosses a checkpoint, the badge is checked against expiration and access rules through barcode, magnetic stripe or RFID readers and the event is logged.
8. The security force checks into the facility and also Log into Lobby Track as users so there is both a record of when the security guard was checked in and what visitors the security guard checked in.
9. Access control systems may be tied in to ensure each cardholder has appropriate facility access settings.
10. Employees check into and out of the facility and their time and attendance is tracked and individual attendance reports may be produced.
11. Personal equipment is checked in and company equipment is checked out of the facility. All pieces of equipment are tied to a cardholder.
12. Lobby Track logs all activity across all cardholder groups.
13. Reports may be generated to show who is/was in the facility at any given time, when cards were printed, when records were added or changed and by whom, among other things.

This is scenario represents just one of hundreds of different configuration possibilities. Because it is open data source, Lobby Track can connect to a limitless number of cardholder groups, the source of the data and information contained and displayed is completely configurable by the user.

Lobby Track easily adapts to corporate, multi-tenant, government, healthcare, K-12 and higher education, membership and other environments. Thus the information tracked and reported is highly relevant to that environment.

It is highly scalable; locations networks quickly without specialized server software.

Most importantly, from any location, Lobby Track allows your security team to answer ***who was where when*** and ***why they were there then*** across the entire organization.

Lobby Track has Small Business, Corporate and Enterprise editions priced at $600, $1,200 and $2,400 respectively, per location. It is available through Jolly Technologies and their network of VARs and distributors.