Access Control Mobile Applications - Best Practices for Deployment

Overview

The rise of smart device technology has made mobile computing a regular topic of conversation; particularly within the security industry. Requests for mobile solutions are on the rise as today's mobile devices provide a reliable monitoring platform. Mix in the benefits provided by mobile solutions and the timing is ripe for deployment opportunities.

However, even with the inherent benefits mobile functions offer, many customers have yet to integrate a mobile strategy into their operations. Security, usability, and notification drawbacks are the most common concerns currently limiting mobile deployments. While reasonable concerns, the risk associated with each can be greatly mitigated with proper design and implementation.

Security Concerns Independent of Mobile Applications

Security Information on the Core Network. The potential risks introduced when security events travel across a common network infrastructure can be mitigated using the following best practices:

1. Create a separate network with limited access for people and devices. This significantly reduces the risk of information being exposed and tampered with.
2. Encrypt network traffic using standard cryptographic protocols. This makes it harder to obtain sensitive information.

Creating a dedicated encrypted network to prevent unauthorized access from the outside world is a great first step; however it does little to lessen "risk and exposure from the inside" which leads into the next concern.

Management of System Operator Controls. Developing a fundamentally sound control policy is central to creating a secure operating environment. System users who gain improper or unauthorized access to the software could perform malicious activity as well as gain access to sensitive organizational data.

The following are recommended best practices to alleviate this risk:

1. Immediately change the password of the default Super Admin or SA account. This password is known by hundreds to thousands of people within any given manufacturer's VAR and End User community. In fact, it is many times documented in installation and user manuals. Thus, it is crucial that this password is changed upon initial system deployment.
2. Require every system user to have a unique user account. Accurate system auditing is simply not possible when shared user accounts are deployed.
3. Adopt a complex password policy and require passwords to be changed regularly.
4. Lock user accounts from accessing the system after a number of failed login attempts.

5. Limit the number of people who have "Super Admin" access. Volatile privileges/commands can have an adverse effect on your system (such as deleting information) and should be limited to only those operators with proper authority.

In addition, it is important to regularly audit operator accounts and their related privileges. The audit should include a thorough review of each operator's role/responsibility within the organization to ensure their system privileges align accordingly.

Security Concerns Introduced with Mobile Applications

The same concerns surrounding exposure of sensitive information and unauthorized malicious activity are prevalent when mobile applications are introduced but with a new variable in play; the Internet. To account for this new variable, additional system design best practices should be considered to minimize the risks associated with deployment of a security application across the Internet.

1. **Cloud Hosting.** A cloud based solution is the best approach when a minimal amount of configuration on the internal network is desired. Typically, data is securely relayed between a server hosted on the public Internet and the internal access control system. When selecting a cloud based solution, proper diligence must still be performed to verify the hosting system provides suitable security measures.
2. **Internal Hosting.** An internal hosting solution is ideal when having complete control of access to the access control system is desired. In this model, the mobile request is forwarded from the Internet to the internal network. This assures complete ownership of the data. The main drawback to this approach is that it requires additional configuration and cyber security knowledge.

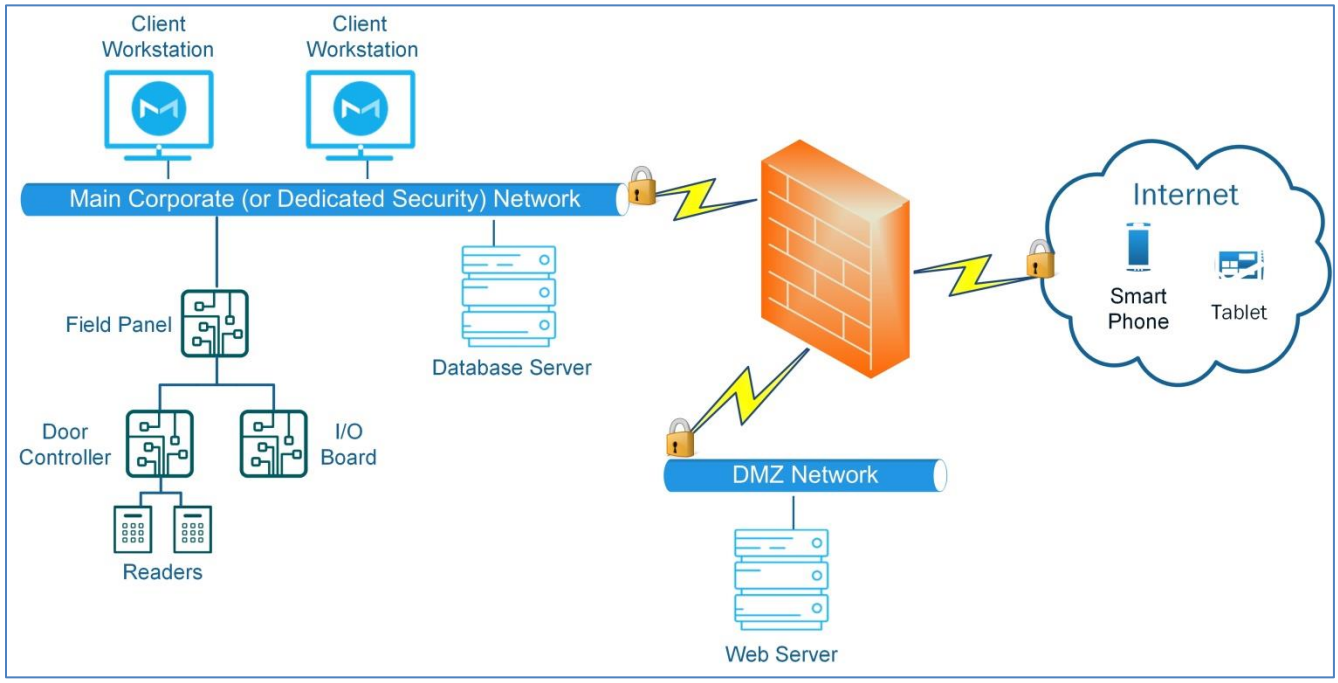
Mobile Applications require access from outside the internal network which means the system must have Internet connectivity. Two components required to minimize risk with mobile deployments that access the Internet are a protected network and a separate web server.

A protected network (DMZ) adds an additional layer of security to the existing security network. Also known as a perimeter network, the DMZ contains the required external facing services that are exposed to the Internet.

A web server, which resides on the DMZ, allows mobile applications to:

1. connect to the database server (through the web server) and other related services from the Internet in order to access system related data.
2. perform functionality inherent to the mobile app.
3. respond to incoming Internet requests.

Access to the web server should be limited by implementing a firewall in order to restrict unauthorized access to other services on the web server. Only the required services for Internet access should be placed on the DMZ. The system's database server and other related components should always be placed on the internal security network to minimize their exposure to the outside world. An added benefit to this design is increased overall system performance due to the inherent load sharing when separating servers.



Encryption

Encrypting web server traffic adds another crucial layer of security by reducing the risk of transmitted data being intercepted and read. Standard encryption protocols typically used include Secure Socket Layer (SSL) and Transport Layer Security (TLS). Since SSL and TLS are also used for server validation, the web server identity can be validated using a certificate obtained through a trusted certificate authority. Thus, the mobile application should be set to only allow secure encrypted connections to the web server.

The final piece of the DMZ/Web server topology is to ensure encrypted communication between the database and web servers. SSL is typically used to protect database engines such as Microsoft's SQL Server.

One last thought on mobile security. A mobile device spends most of its time outside of your internal network, and thus has a greater chance of being lost or stolen. Because of this, all mobile devices should be registered with the security system. Doing so allows the system to verify the device has been registered (and is legit) each time the device attempts to connect. The device's registration should also be disabled if it becomes lost or stolen.

User Experience Considerations

The biggest difference in user interaction with mobile applications (as opposed to desktop applications) is the touch screen of the mobile device. This must be taken into account when designing the mobile UI. An exact copy of the desktop application UI should not be used. Even if the mobile device has greater resolution than a monitor, the physical size is smaller. A button that is easily clicked on desktop monitor could become too small for sensing a finger touch.

There is less real estate on mobile devices making it essential to simplify the user experience. Putting too much functionality into a mobile screen makes it difficult for users to perform even the most basic tasks. Instead, mobile applications should focus on tasks that are commonly needed when not at the security workstation, such

as viewing alarms or opening a door. The need to perform complex system configuration tasks is rare, and these functions are best performed from a traditional client.

There is an inherent expectation that mobile applications work across device platforms (Android, iOS, etc.). This is particularly true with organizations that have BYOD (bring your own device) policies in place. While the various mobile platforms utilize a common set of user controls, there are subtle differences with how each platform handles the layout and navigation within their UI. Embracing the mobile platform's standard user experience makes it easier for the user to operate the app. Customers should seek out manufacturers who follow the recommended design conventions for each mobile platform so that their users enjoy an optimal user experience.

Screen orientation frequently changes and must be taken into the account. Users expect mobile applications to automatically adjust their layout. Manufacturers that implement a fluid design allow their customers to better handle screen size changes when the app is running in either phone or tablet devices.

Notifications

Timely mobile alerts are critical in the security world. Yet sending notifications to mobile devices is not a simple task due to battery power and network connectivity limitations inherent in mobile devices. There are two common implementation methodologies for notification delivery. Both have limitations, so it is important to understand the drawbacks of each and be aware of potential operational limitations.

SMTP/SMS Notifications are pushed to devices using older messaging protocols that preceded smartphones. These methods include sending email or SMS text messages. While this technology is dated, the protocols are mature and proven to be reliable. Security systems often use their existing notification service to send messages to mobile devices. Mobile integration is achieved by embedding URL links in email messages that automatically opens a mobile application. The main drawback of this method is lack of tight integration. Notifications arrive in the same inbox as other email making it difficult to highlight security related messages.

Push Notifications use native services to push notifications directly to the app (through Apple's Apple Push Notification Service (APNS) and Android's Global Cloud Messaging (GCM)). These services allow actions to be performed that are specific to the mobile app and include audio alerts, vibration or screen display updates. There are two main drawbacks to this methodology. First, notifications are not guaranteed to be sent / received successfully. Depending on the environment and nature of alert messages, it may not be acceptable to have critical alerts indiscriminately drop during transmission. Second, these services require a SSL certificate on the hosting server which is not always practical or feasible unless the security system is a cloud hosted solution.

Summary

Security manufacturers provide mobile applications to enhance the capabilities of their desktop solutions. While mobile apps are popular and convenient, administrators must maintain balance to ensure the security of the system is not compromised. Careful review of the network architecture, including notification methods, is highly recommended before exposing servers to the Internet. Not all apps are created equal so be sure the app is tailored for small touch devices. Mobile applications are here to stay. When properly designed and deployed, they can add significant value to a security deployment.