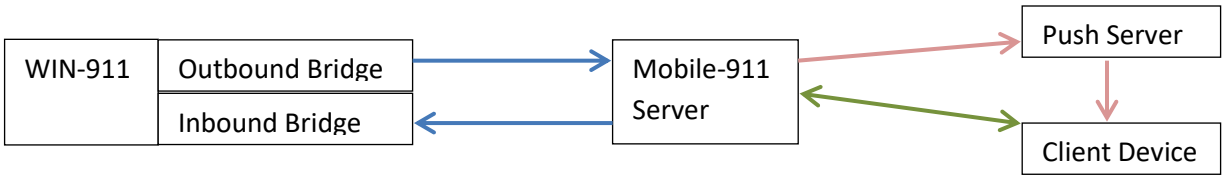
Mobile-911 Network Overview

Components Overview

WIN-911 sends messages to the Mobile-911 Server via an Outbound Bridge component. It receives messages from the Mobile-911 Server via an Inbound Bridge component over a completely independent channel. Both Bridges components are services running on the same machine as WIN-911.

The Mobile-911 Server sends push notification to internet-based push notification servers (e.g. Apple or Google servers). When a client device receives a push notification, the user launches the Mobile-911 client application which establishes a point-to-point connection between the client device and the Mobile-911 Server. The following diagram outlines these components:



Communications Overview

Network and Internet communications fall into 3 categories: secured WCF, secured SSL, and unsecured communications. Communications between WIN-911 and the Mobile-911 Server (blue above) are secured with WCF; the specific IP ports used are configurable. Communications between the Mobile-911 Server and the client (green above) are secured with SSL; again the port is configurable. Communications to and from the push server (red above) are unsecured and unencrypted; since these push servers are general purpose, their addresses are well known.

WCF Overview

WCF is a distributed programming platform based on SOAP messages. Using WCF, you can create applications that function as both services and service clients, creating and processing messages from an unlimited number of other services and clients. In such a distributed application, messages can flow from node to node, through firewalls, onto the Internet, and through numerous SOAP intermediaries. This introduces a variety of message security threats. The following examples illustrate some common threats that WCF security can help mitigate when exchanging messages between entities:

- Observation of network traffic to obtain sensitive information. For example, in an online-banking scenario, a client requests the transfer of funds from one account to another. A malicious user intercepts the message and, having the account number and password, later performs a transfer of funds from the compromised account.
- Rogue entities acting as services without awareness of the client. In this scenario, a malicious user (the rogue) acts as an online service and intercepts messages from the client to obtain

sensitive information. Then the rogue uses the stolen data to transfer funds from the compromised account. This attack is also known a phishing attack.

- Alteration of messages to obtain a different result than the caller intended. For example, altering the account number to which a deposit is made allows the funds to go to a rogue account.
- Hacker replays in which a nuisance hacker replays the same purchase order. For example, an online bookstore receives hundreds of orders and sends the books to a customer who has not ordered them.
- Inability of a service to authenticate a client. In this case, the service cannot assure that the appropriate person performed the transaction.

Source: http://msdn.microsoft.com/en-us/library/ms735093.aspx

WCF Message Security Overview

Message security uses the WS-Security specification to secure messages. The WS-Security specification describes enhancements to SOAP messaging to ensure confidentiality, integrity, and authentication at the SOAP message level (instead of the transport level). In brief, message security differs from transport security by encapsulating the security credentials and claims with every message along with any message protection (signing or encryption). Applying the security directly to the message by modifying its content allows the secured message to be self-containing with respect to the security aspects. This enables some scenarios that are not possible when transport security is used.

Transport security, such as Secure Sockets Layer (SSL) only secures messages when the communication is point-to-point. If the message is routed to one or more SOAP intermediaries (for example a router) before reaching the ultimate receiver, the message itself is not protected once an intermediary reads it from the wire. Additionally, the client authentication information is available only to the first intermediary and must be re-transmitted to the ultimate receiver in out-of-band fashion, if necessary. This applies even if the entire route uses SSL security between individual hops. Because message security works directly with the message and secures the XML in it, the security stays with the message regardless of how many intermediaries are involved before it reaches the ultimate receiver. This enables a true end-to-end security scenario.

Source: http://msdn.microsoft.com/en-us/library/ms733137.aspx

SSL Message Security

Messages transferred between the Mobile-911 app and the Mobile-911 Server use a self-signed SSL certificate with 128-bit encryption.

Mobile-911 id

The Mobile-911 id is used by WIN-911, Mobile-911 Server and the Mobile-911 app for authentication and message routing. They are not related to the physical device but they are unique to the install on the device. The id's are stored in the private data store of the app. The Mobile-911 id can be viewed from within the app. Messages generated from the app includes theMobile-91 id. If you remove the id from theWIN-911 Configurator, the app cannot talk to WIN-911.