SkySpark® Everywhere™ – Introducing the Distributed Informatics Architecture

The Edge-to-Cloud IoT Data Platform for the Built Environment

SkyFoundry

Security - Built Into the Architecture from the Edge to the Cloud

SkySpark is built with a security first philosophy. It starts with the fundamental notion that complexity breeds security holes. Security must be strong, but simple for users to implement in order to achieve a secure system. SkySpark's simple, easy to understand security architecture provides for a secure environment and utilizes multiple redundant layers of security. We incorporate the latest security practices and technology, and continually evaluate security enhancements during every release.

Network Security. Securing SkySpark's network interfaces is a critical aspect to ensure system security. SkySpark supports two primary network interfaces: a websocket based peer-to-peer protocol named Arcbeam for communication between SkySpark nodes in a distributed system, and an HTTP interface typically utilized by users to interact with the system. Additionally, with any project, there will likely be one or more secondary network interfaces for the various connectors that get configured, such as BACnet, Modbus, etc., with their own security considerations.

SkySpark Node-to-Node Security - Arcbeam.
The Arcbeam protocol is SkySpark's peer-to-peer technology, which underpins the advanced SkySpark Everywhere distributed architecture. It is designed to work in tandem with existing security best practices such as firewalls, VPNs, and TLS encryption. Arcbeam is layered above "websockets" to establish a peer-to-peer communication link using a HTTP handshake. Once a communication link is established the connection is fully peer-to-peer, which means that either end point can initiate the connection without loss of any features. This makes it easy to establish distributed architectures where one endpoint is safely hidden behind a firewall. It eliminates all of the complexity of traditional IoT architectures and decisions about push-vs-pull communications links and concerns over requests for data coming from outside the network.

WebSocket is a computer communications protocol, providing full-duplex communication channels over a single TCP connection. The WebSocket protocol was standardized by the IETF as RFC 6455 in 2011, and the WebSocket API in Web IDL is being standardized by the W3C.

Unlike HTTP, WebSocket provides full-duplex (bi-directional) communication. Additionally, WebSocket enables streams of messages on top of TCP. TCP alone deals with streams of bytes with no inherent concept of a message. Source: Wikipedia: https://en.wikipedia.org/wiki/WebSocket)

And because it sits on top of tried and true IP infrastructure of TCP, HTTP, and Websockets it works cleanly over standard security technologies such as VPNs.

Cryptographic Keys for Secure Authentication. SkySpark uses cryptographic key pairs to bi-directionally authenticate each Arcbeam connection between nodes. Each SkySpark node is secured with a 2048-bit RSA public/private key pair. For two SkySpark nodes to establish an Arcbeam link, each node must be securely configured with the remote node's public key. This ensures a secure network connection is made only once each side verifies trust in the other endpoint.

Arcbeam security can be further enhanced with the use of a TPM chip. TPMs, provide highly secure management of cryptograph keys using a hardware chip. TPMs guarantee that access to the sensitive private keys is only available to the hardware itself, making it extremely difficult to steal private keys.

The ability to utilize TPMs further increases security and streamlines acceptance by IT security departments. Already, organizations like the DoD are specifying that new hardware products use TPMs.

Taking Security Keys to the Next level – Integration with TPM – the Trusted Platform Module

SkySpark's Arcbeam implementation enables keys to be based on the highly secure TPM technology.

Trusted Platform Module (TPM) is an international standard for a secure crypto processor, which is a dedicated microcontroller designed to secure hardware by integrating cryptographic keys into devices. TPM's technical specification was written by an industry consortium called Trusted Computing Group (TCG). Many new IoT devices now include a TPM. Since each TPM chip has a unique and secret RSA key burned in as it is produced, software (like SkySpark) can use the Trusted Platform Module to generate unique certificates to authenticate hardware devices and communications across clusters of nodes.

Source: Wikipedia: https://en.wikipedia.org/wiki/Trusted_Platform_Module

User Access. User authentication often still requires traditional username/password combinations. SkySpark utilizes a set of industry leading security technologies to manage and authenticate user passwords. Passwords themselves are stored using a technology called "PBKDF2 hashing". PBKDF2 leverages a "key stretching" algorithm, which requires significant CPU cycles to compute a hash of a password. This raises the difficulty of guessing the original passwords even if the system is compromised. Authentication of username and passwords uses another cyber security standard - SCRAM (Salted Challenge Response Authentication Mechanism). SCRAM leverages the PBDKF2 hash to ensure that neither the original password, nor the PBDKF2 hash are sent over the network. It also allows both client and server to verify that they agree on the password.

Arcbeam - Highly Efficient Message Protocol Minimizes Bandwidth

Arcbeam messages are encoded using Brio, our data compression technology. This is the same technology that makes it possible for a time stamped value to be stored in an average of 12 bits in the SkySpark's Folio database. In Arcbeam it compresses the entire message payload. The result – less latency and less bandwidth utilization on networks. Another feature that IT departments look for.