HOBOlink® Data Security and Infrastructure

Background

HOBOlink is an online service designed to communicate with remote data loggers, store environmental and meta data, and allow users authenticated access to configure loggers, view data, view inventory, export data, and perform data analysis. HOBOlink is made up of several components distributed amongst a set of managed virtual servers.

U30/RX3000 devices and HOBOlink communicate via both TCP/IP sockets and UDP, with the device initiating the connection. The device is programmed to communicate with dil.hobolink.com at four specific ports depending on protocol and device type. The device does not need to be visible to the outside world; rather, it only needs to be able to establish a connection to the Internet via cellular, Wi-Fi, or Ethernet.

Because the device calls the servers, there will only be an issue with the device (Wi-Fi and Ethernet only) getting through to the servers if a customer's firewall blocks traffic based on the destination port. This would be unusually restrictive. In general, a firewall would block all inbound traffic other than a select few ports, but this would not be a problem for HOBOlink because the server does not call the device. If a customer's firewall does block based on destination port, customers would need to work with their IT department to open up the correct port to dil.hobolink.com.

HOBOlink also supports data upload from the HOBOmobile mobile app, which pulls data from Onset's line of Bluetooth Smart data loggers (MX series). Data is pushed from the mobile app to HOBOlink via a set of REST web services, using SSL and username/password authentication for security. Additional web services ensure that duplicate data does not reach the servers.

HOBOlink Administration Team

Onset employs a staff responsible for the administration of HOBOlink. That staff works to maintain and improve the remote monitoring software applications and data warehouse used in the collection, storage, and transmission of environmental data. Responsibilities include application uptime, remote troubleshooting, backups, application monitoring, continuous infrastructure improvements, and general focus on product maintenance, maintainability, and hands-off operation. The administration team works with the HOBOlink development team, but is not responsible for the actual development.

In the event that a member of the team is no longer employed by Onset, the HOBOlink Employee Separation Plan is used to secure the system.

Data Transmission Protocols Security

For U30 and RX3000 devices, the data transmission between the devices and the servers is not formally encrypted, but each packet is stamped with a session ID, making it exceedingly difficult to emulate. In addition, a proprietary algorithm is used to wrap each packet with a digital signature. If the signature does not match when HOBOlink receives a packet, that packet is rejected. Finally, Onset's data is encoded in a proprietary binary and Google Protocol Buffers (GPB) data format that requires confidential Onset documentation to interpret or mimic.

For MX logger data from the mobile app, SSL and username/password authentication is used along with a proprietary GPB data structure.

Data Storage Security

All logger and configuration data is stored in Amazon Web Services (AWS) data centers in the United States, both in proprietary binary datafile format and in a password-protected full redundant RedShift data warehouse and MySQL master-slave cluster. All customer data is in these systems, referenced by an ID key to a user's account and device serial number. Access to these servers is limited to only Onset Engineering, specific Onset-controlled IP addresses, and is controlled by a rollable pem key. The database access passwords

for the development team only allow read access. Write access is limited to Onset's HOBOlink Administration Team. Data is backed up daily to separate servers.

The customer accesses data over the web using https (http with the SSL protocol) and a custom HOBOlink username/password. Login credentials are further encrypted in the database such that passwords are not transferred or stored in plain text. Reverse encryption of the hashed passwords is not possible. Logged data is not encrypted in the database.

Access to control of a device is also password protected. The logged in user has the ability to make any device public, which provides a public URL to the latest data. Public URLs do not provide the ability to configure the U30 or RX3000 device. The logged in user must choose to enable this feature in HOBOlink User Settings as it is disabled by default.

Data Retention

Data is held in Onset's servers for a period of 10 years. If, during that time, the subscription to a device uploading data is not renewed, the previously stored data will continue to be available. Users who want to export their data from the servers may do so at any time.

Data Mining

Unless a device is specifically configured for public access, all data remains accessible only to the HOBOlink account under which that device is registered. Onset does not mine, distribute, or use the data for any purpose.

Data Backups

Data that is stored within the Redshift and MySQL databases is backed up nightly and retained for a period of 14 days. Logger and configuration data is backed up nightly and retained for a period of 30 days. Additional details are contained in Onset's internal backup process documentation.

Source Control

Subversion (SVN) is used for source control, and Go for continuous delivery. Additional details are contained in Onset's internal software release process documentation.

Disaster Recovery Plan

In the unlikely event that all three AWS data centers in our region are down for an extended period, Onset will migrate the HOBOlink server instances and databases to another region. All efforts will be made to minimize the downtime and get the services back online as quickly as possible. Three hours of downtime is estimated. Onset Computer Corporation maintains a corporate Disaster Recovery Plan that covers business systems outside of HOBOlink.

Server Patching, Updates, and Customer Notification

Onset maintains a schedule for patching the HOBOlink server instances. If customer downtime is required, a notice will be placed on the HOBOlink banner at least 48 hours in advance, unless emergency updates are required. If unplanned customer issues occur, they are handled on a case-by-case basis by Onset Technical Support, including any necessary customer notifications. Additional details on the patch process are contained in internal documentation.

Application Logging

Logging is enabled in all components of HOBOlink. Actions performed by the user or the remote clients are logged, with Onset's HOBOlink Administration Team having the ability to set the granularity of logging.

Logs are rolled once per day. A nightly script is run that compresses the log files and pushes them to Amazon's S3 file repository. Logs are maintained in S3 for six months.

Explicit SOPs exist to allow administrative access to viewing logs. Additional details on viewing logs are contained in internal documentation specific to the sub-components of HOBOlink.

Service Level Agreements

Terms of Use and Data Uploading Terms can be viewed by logging into HOBOlink and visiting the Terms tab under Support. All data remains accessible to users if the contract is allowed to expire. Contracts only dictate the transfer of data into the system, not access to the data once it is in the system. Data can always be exported from the system via the standard Custom Data mechanisms in HOBOlink.

Questions

If you have any other questions or concerns regarding data security, please feel free to contact an Onset Technical Support Representative at 1-800-LOGGERS or http://www.onsetcomp.com/support/contact.