Olibra Security Whitepaper

Olibra LLC

4 May 2020

Contents

Introduction

Olibra provides hardware, software, and services supporting smart home applications. Olibra's users rely on Olibra's products every day to keep their smart homes operational and their data secure. This document describes how Olibra handles information security. Specifically, this document describes the security roles of Olibra and users of the Bond Home platform, how security works within the platform, and the procedures for reporting of information security incidents.

This document is addressed to end-users ("users") of the Bond Home platform, which includes users of all products---both Olibra products (such as Bond Bridge) and partner products running on Bond Home (such as Smart by Bond ceiling fans). Therefore, we use the second-person ("you") to refer to the user's role and the first-person ("we") to refer to Olibra's role.

Shared Responsibility Model

Olibra and users share responsibility for information security within the Bond Home platform. While most of the responsibilities fall on Olibra as the author of the software stack and operator of the cloud services, users have an important role in security which must be played to ensure the confidentiality, integrity, and availability of the information and information processing within the platform.

Olibra Security Responsibilities

Olibra is responsible for:

- security of cloud software and infrastructure (servers, networks, administration, etc.)
- secure connection between devices and servers
- patching security vulnerabilities in the platform (firmware, mobile apps, and cloud)
- correcting performance or availability issues throughout the platform
- providing timely notifications and updates about serious information security incidents

User Security Responsibilities

You are responsible for:

- not telling anyone your account password---not even an Olibra support agent
- restricting physical access to Bond devices
- local (WiFi) network security
- installing firmware and mobile application updates
- reporting any suspicious activity (such as phishing) or other security incidents to Olibra

Security within the Bond Home Platform

General

We protect your data and devices in several ways. We follow industry standards for information security as laid out in ISO27001 and ISO27017 and we require that our cloud service providers be certified in these standards. In particular, we have policies in place which restrict access to confidential information and critical systems, policies which restrict employee use of software to only that software which is necessary for the performance of their work and which has been approved by our security management, and automated monitoring of systems to ensure sensitive information is not revealed to persons with malicious intent.

Authentication

Access to your Bond Home account is secured by password authentication. Your account is only as secure as your password. It is your responsibility to choose a sufficiently complex password, to never use the same password for multiple services, and to never share your password with anyone. In particular, Bond customer support will never ask you for your password or for a security code.

If you forget your account password, you may reset your account by using the Forgot Password feature. However, please note that anyone with access to your email account will be able to reset your password and then access your account, so please take care to secure your email inbox.

Cryptography

The connection between Bond products and the cloud servers occurs via the MQTT protocol and is protected with transport encryption and cryptographic authentication. When a Bond device connects to our cloud, it uses Transport Layer Security (TLS) to protect the confidentiality of the connection between the two hosts. The Bond device checks the server's TLS certificate to authenticate the server to the device. To authenticate the device to the server, the server checks the validity of the device's TLS certificate and checks that the device's reported serial number matches the serial number embedded in the device certificate.

The connection between the Bond Home app and the cloud occurs over two means (a) an HTTPS API and (b) an MQTT/TLS connection. The HTTPS API uses best-in-class OAuth2 authentication (provided by AWS Cognito). The Bond Home app uses this API for all communications purposes except for communicating with the Bond devices themselves. Among these purposes is the delivery of client certificates which are used to secure the MQTT/TLS connection. The Bond Home app then uses MQTT to operate the Bond devices on your account, even when you are not on your home WiFi network.

When on the same local network as the Bond device, the Bond Home app may communicate directly with the Bond device using unencrypted HTTP. Only basic token-based authentication is used to protect the connection against accidental access and unsophisticated attacks. You are responsible for securing your WiFi and local area networks. For a moderate level of security, please ensure that:

- the WiFi network uses at least WPA2 security
- you do not share your WiFi password with any untrusted parties
- you do not connect any untrusted devices to your network

If you are especially concerned about the security of your Bond devices (and the appliances they may control), you may consider using VLANs or a seperate WiFi network only for Bond devices.

Data At Rest

Although we provide industry standard access controls to data stored on the Bond Home platform, we do not encrypt data at-rest within the cloud databases. This means that authorized Olibra employees are able to read your data, including personally identifiable information, within the Bond Home platform. However, our use of your data is subject to our Privacy Policy and applicable law.

Furthermore, data within the Bond devices' databases is also not encrypted. This means that a sophisticated attacker who steals a Bond device would be able to read out your WiFi network password. In the case of Bond Bridge, such an attacker would also be able to learn the RF signals of your devices and control those devices when within RF range of your home. It is your responsibility to ensure that physical access to Bond devices is restricted to trusted persons.

Backups

Although we may internally use database backups to improve platform resilience, we do not provide our users with backup features at this time. Data within the Bond cloud or Bond device databases could be unrecoverably lost at any time. In particular, this means that users should:

- maintain some other (manual or remote-based) means of operating their appliances
- keep the remote controls for their appliances in case of a need for re-programming

Product Development Process

Crucial to preserving the security of the platform is a secure product development process. We have designed security into the platform from its conception and no feature or product gets added to the platform without security review at the design stage. We also insist on secure prototyping. There are no insecure product versions created or backdoors installed in products, even when it would be expedient for development or debugging to do so. Furthermore, we insist on the principle of least privilege, whereby components in the system have minimal trust of other components so as to limit the impact of a security breach. For example, even after successfully authenticating to the cloud MQTT server, rules for message handling on the server ensure that a Bond device is only privileged to receive commands addressed to it and to respond to those commands. A compromised Bond device does not have the privileges to read or delete any information other than that which may already be stored inside the device, nor does it have the ability to compromise other devices on the account.

The implementation phase of our development process also follows strict rules intended to maintain the security and availability. We use agile software development methodologies, peer code review, coding standards as enforced by review and automated checkers ("linters"), continuous integration testing, and both pre- and post-release quality assurance testing.

Supplier Agreements

We engage suppliers for the purpose of conducting our business, developing our products, and providing you with services. As a general precaution, we enter into Non-Disclosure Agreements with all suppliers and apply the principle of least privilege in sharing information or granting access to Olibra systems. We never share your personally identifying information except as laid out in our Privacy Policy.

Software Updates

We frequently release updates for Bond device firmware and for the Bond Home mobile applications. These updates typically contain feature enhancements, aesthetic changes, support for new products, and minor bug fixes. However, from time to time, updates may also patch security vulnerabilities which---if left unaddressed---could result in performance degradation that limits access to the platform or your data, or even in data loss, corruption, or leakage to unauthorized parties. For this reason, we strongly encourage you to keep your software up to date.

We release updates for the Bond Home apps via the Google Play Store and the Apple App Stores. Please check frequently for app updates or enable automatic app updates on your mobile devices. We release firmware updates and make them available via the Bond Home app. At this time, the Bond Home app must be used to check for firmware updates.

Although for most releases, firmware updates are performed only after you request the upgrade, we may perform updates of Bond devices without asking your consent if the security of your devices, data, or the platform is at risk. In such a case, we will inform you of the actions taken.

We take full responsibility for performing software updates to the Bond Home cloud.

Critical Operations

The Bond Home platform provides turn-key smart home features with minimal administrative responsibility on your part (or our brand partners' parts for that matter). However, there are several critical information operations which you may perform:

- deletion of your personal information under the California Consumer Privacy Act (CCPA)
- requesting a copy of your personal information under the CCPA

In case of deletion requests, after positive verification of your identity, we will permanently delete your Bond account and all personally identifiable information (as defined and qualified in our Privacy Policy). This deletion is irreversible and therefore you should ensure that you still have a means for operating your home appliances before requesting deletion.

In case of requesting a copy of your personal information, you then take responsibility for the secure storage and handling of that information. So please take information security into account before downloading this information to a possibly insecure computer system.

Information Security Incidents

We report the following types of information security incidents to affected users:

- misuse or leakage of Personally Identifiable Information, whether confirmed or suspected
- major software bugs which may compromise confidentiality or integrity of user information
- major software bugs which may cause major system malfunction or unavailability
- other incidents which gravely affect platform confidentiality, integrity, or availability
- planned cloud maintenance impacting system availability for more than 2 minutes
- unplanned interruptions to cloud services for more than 15 minutes

Olibra's Responsibilities

Olibra takes full responsibility for all information security incidents within the Bond Home cloud. This includes all our servers, cloud infrastructure, source code repositories, and marketing platforms.

User Responsibilities & How to Report an Incident

There are however two cases where we are not responsible for an information security incident. Firstly, it is your responsibility to secure your local area network (WiFi network). Therefore, Olibra is not responsible for incidents of unauthorized access to Bond devices caused by breaches of your network via some route other than Bond devices (such as via WiFi password leakage, compromised router or other device). However, if you suspect that your devices, account, or personal information may have been compromised for any reason, please report the incident via email to customerservice@bondhome.io or use the Chat feature within the Bond Home app. We are always glad to assist our customers. We may ask you to provide evidence to prove your identity as well as provide evidence to assist in verifying and investigating the reported incident.

Our Brand Partners' Responsibilities

The other category of security incident for which Olibra is not responsible are breaches of information security during the manufacturing processes and supply chain of Smart by Bond products. For example, installation of sniffing devices into appliances or leakage of cryptographic certificates at the factory. We do provide guidance to our partners on proper handling of information security so as to produce secure smart appliances, however these processes occur at our business partners' facilities and are therefore outside of our control. In the event of an information security incident occurring at a partner facility, our partners are required to contact us via email and cooperate with the investigation and resolution of the issues.

Communication and Updates

We will report incidents affecting your account via email to the email address used to set up your Bond account. For ongoing incidents, we will provide updates not less than once every 14 days. You may track the status of any reported information security incident by contacting customer support.

Revision History

Rev 0 -- 4 May 2020 -- Initial Draft -- Author: Chris Merck -- Approved:
Zohar Shinar May 6th 2020