BRIVO ONAIR®
INFORMATION SECURITY

Providing Assured Control of Facilities and Information

brivo®
simply better security

www.brivo.com

Legal Disclaimer

Documentation Disclaimer and Restrictions

Information in this document is subject to change without notice and does not represent a commitment on the part of Brivo Systems LLC. For the most up-to-date information, visit www.brivo.com.

This document and the data herein shall not be duplicated, used or disclosed to others for procurement or manufacturing, except as authorized with the written permission of Brivo Systems LLC. The information contained within this document or within the product itself is considered the exclusive property of Brivo Systems LLC. All information in this document or within the hardware and software products themselves is protected by the copyright and/or other intellectual property laws of the United States.

Table of Contents

INFORMATION SECURITY

As a provider of physical security services, we at Brivo believe that information security is of paramount importance to maintaining the safety and security of your facilities. That's why information security has been a consideration since day one, in our datacenters, our field hardware, our people and our processes.

Introduction

This paper describes the information security provisions built into the Brivo Onair® technical architecture. It is primarily intended for IT professionals and others familiar with computer networks and information security, and contains a basic introduction to Internet security concepts.

The topics covered include specific aspects of information security in the Brivo Onair architecture and system design, as well as background materials on cryptography, firewall technology, digital certificates, and networking. Brivo has applied networking and application security best practices to the domain of cloud-based access control systems.

The scope of this document includes the following major topics:

- Brivo data centers, where our web applications are hosted
- The Brivo control panel which resides as the customer premises
- Data communications
- Web browser client security considerations
- Brivo mobile application security considerations
- Authentication, authorization and accounting
- IP networking considerations for data security
- Cryptography

References

While this paper is intended to be a stand-alone document, you may have additional interest in either the Brivo system or some aspects of information security discussed. For that reason, a brief list of Brivo references is provided below.

The following additional reference documents are also available at www.brivo.com or by contacting Brivo via sales@brivo.com.

- Brivo Onair administration manual
- Brivo hardware installation manuals
- Brivo Onair Architecture and Engineering (A&E) specification

SYSTEM OVERVIEW

Brivo services are based on a centralized, cloud-based architecture, where all users and distributed hardware devices (control panels and cameras) share a common set of network and server resources at our data centers. In particular, Brivo hosts a physical security system, primarily targeted at commercial properties with employee, resident and visitor populations for whom access needs to be regulated and recorded. The wide area networking inherent in the system is an excellent fit for geographically distributed applications that span multiple properties.

SaaS Provider Model

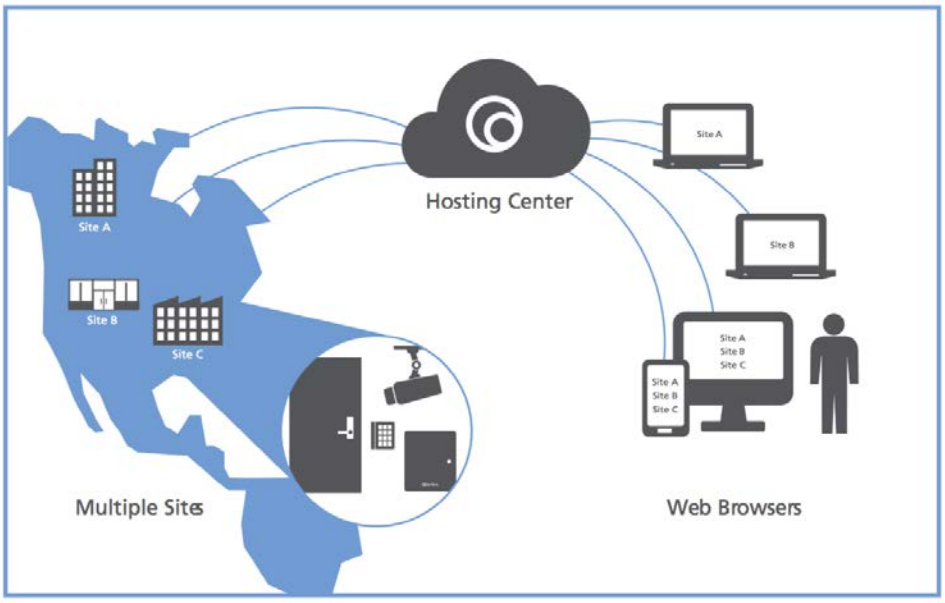
Brivo provides hosted services using the Software as a Service (SaaS) model. Software-as-a-service (SaaS) is a software licensing and delivery model that eliminates the need for individual entities to purchase, deploy and maintain IT infrastructure or application software. SaaS vendors are able to amortize their infrastructure costs over thousands of users yielding lower total costs of ownership (TCO) for customers. This ability to amortize costs enables SaaS vendors to make investments that guarantee the security and resiliency of their solutions that would not be viable for many business customers.

Several key advantages of the SaaS model for physical security include:

- No dedicated on-premises computer equipment and software to maintain
- Access to superior technology at a lower Total Cost of Ownership (TCO)[1]
- Continuous maintenance and upgrades are included with the service
- Ability to rapidly scale and modify service levels on demand
- Simple and secure access to your system anytime and anywhere
- Shifting workload to the SaaS provider allows you to focus on your business

[1] Go to www.brivo.com for our Total Cost of Ownership whitepaper

Figure 1: Brivo System Overview



Basic System Operation

As shown above in Figure 1, there are four major components to the overall operation of the Brivo Onair® service:

- Customer premises equipment (control panels, credential readers, cameras)
- Network communications via Internet
- Brivo's centralized, cloud-based applications resident at our data centers
- Web browser on the end-user's PC or mobile device

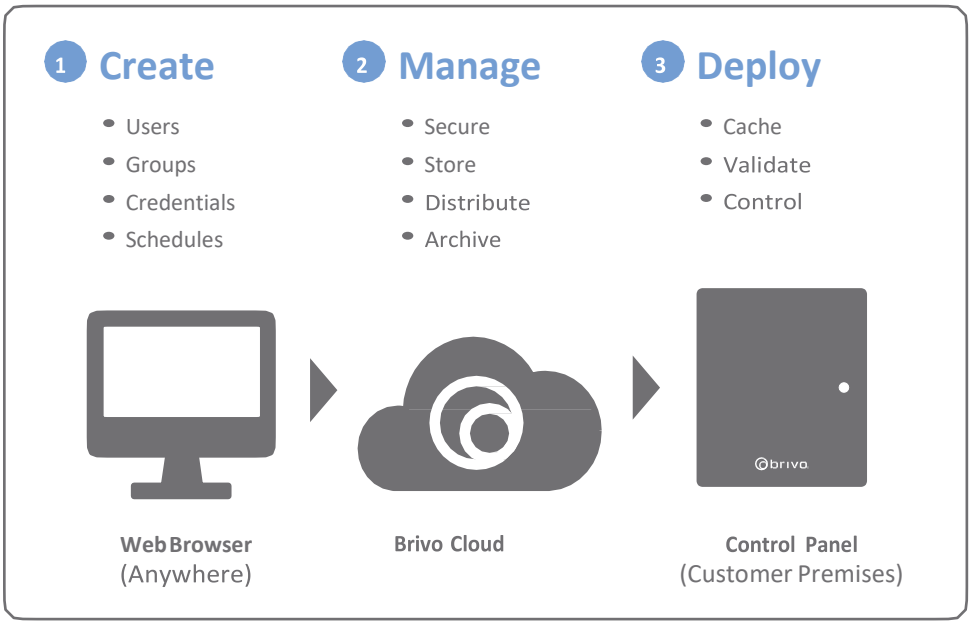
These components share data across multiple platforms and networks in order to manage access control privileges, deliver alarm and event records and to provide other services such as software updates to control panels.

Control panels are networked to our data centers through a variety of technologies, both wired, and wireless. Wired options include a built-in Ethernet port for connection to a corporate LAN, or broadband modem, or any other IP-based networking technology with connectivity to the Internet. Wireless networking options include a cellular network router. Alternatively, sites with a wireless 802.11 network may use a wireless bridge to the control panel to simplify wiring requirements.

Data Life Cycle – Creation and Distribution

The access control life cycle begins with an administrator logging into the Brivo application and setting up users, groups, credentials, schedules, and other security policy elements that dictate who has permission to enter which facilities at which times. Security policy data is stored centrally and then distributed to the control panels where policy rules determine access to each connected door. When policy changes are made, updates are pushed to the panel immediately. Maintaining a local copy of the security policy allows a panel to operate even if temporarily disconnected from the Internet. When connectivity is restored any changes to the security policy are immediately applied.

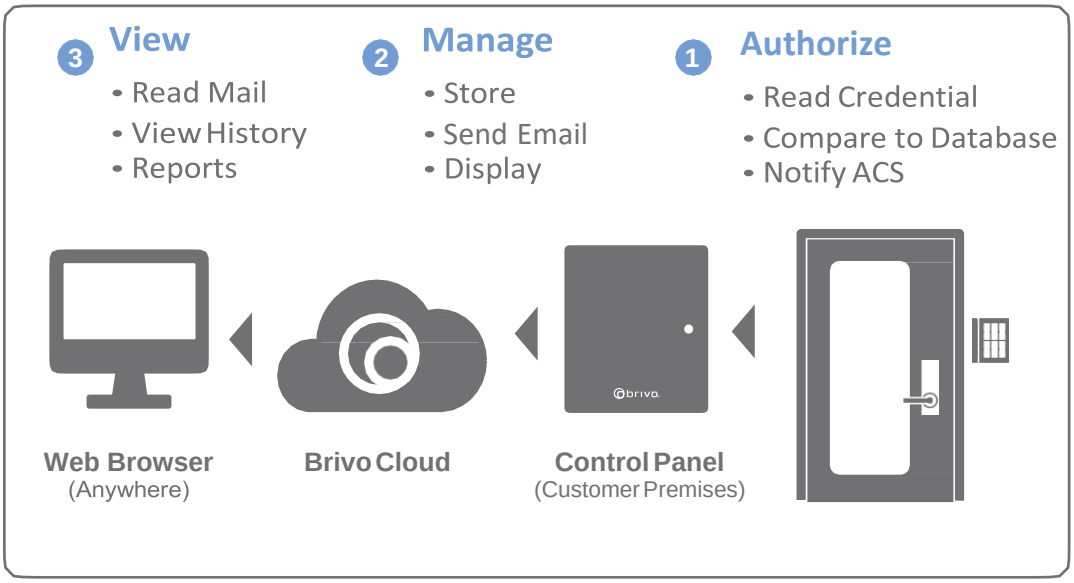
Figure 2: Data Creation and Distribution



Data Life Cycle – Access Event Notification

Control panels manage access to doors by comparing the credentials acquired by a reader (e.g., proximity cards, PIN codes, fingerprints, mobile credentials, etc.) with a local database of credentials. When a person presents a credential to a reader attached to a Brivo control panel, the panel makes a comparison against its database to determine whether access is allowed at that door, at that particular time.

Figure 3: Data Returned from Access Events



The control panel then grants or denies access, and immediately sends a transaction record to the data center which can then be viewed or searched. After this transaction record has been received at the data center, the Brivo application software stores the information for subsequent customer viewing and reporting.

The software can associate business rules with these transaction types, and can take action based on observing transactions being reported. A common use of this capability is to request an email notification when a particular type of event is observed. The application immediately sends an email notification to a list of addresses set up for notification on the account. These transactions are also available to administrators via our Brivo Onair Mobile Application.

Of course, all of these transactions are handled securely. The next section of this paper introduces some Internet security basics, the building blocks for ensuring that all Brivo customer data remains protected.

INTERNET SECURITY BASICS

The methods Brivo uses to secure customer data are proven techniques based on industry best practices from existing Internet security technologies and the field of cryptography. Brivo uses a variety of these techniques, including:

- Authentication, authorization, and accounting
- Digital certificates and Public Key Infrastructure (PKI)
- Transport Layer Security (TLS)

Authentication

Authentication is the cornerstone of secure information exchange in Brivo Onair®, because each party must be able to verify that they are communicating with a trusted partner.

Authentication is the process whereby each party verifies the mutual identity. Within the Brivo architecture, there are two exchanges requiring such verification: administrative login to the Brivo applications, and control panel communication with the data center.

Administrator Authentication

An administrator is a Brivo customer with privileges to sign in to the Brivo Onair application and observe or make changes to an account that controls one or more sites. For an administrator to securely establish a session with the Brivo cloud, Brivo must be able to verify the identity of the administrator. The administrator also must be able to verify that he or she is, in fact, logging into the Brivo website and not an imposter website.

Administrators are authenticated by entering an administrator ID and password to the Brivo Onair application. The ID/password combination allows Brivo to verify that the person attempting to connect to Brivo is, in fact, using a valid pair of identifiers to gain access to the system. Optionally, administrators may add a second factor for authentication of each logon using an out-of-band Short Service Message (SMS). This feature affects all administrators within an account. Once activated, when an administrator logs into the system, he or she will receive an email with a login token that must be used to complete the login process. The token is only valid for a limited time and is sent to the email address on file within the administrator's profile.

The entire ID/password exchange takes place within a Transport Layer Security (TLS) session that begins when the administrator accesses the logon page of the Brivo Onair® application via Hypertext Transfer Protocol Secure (HTTPS). The TLS session protects the exchange of authentication data by encrypting it thus establishing secure communication.

Steps are also taken to ensure that the Brivo Onair administrator can be sure that they are logging in to the real Brivo Onair® application. This is accomplished through the establishment of the TLS session itself. By checking the validity of the digital certificate presented at the beginning of the TLS session, the administrator can verify that he or she is indeed connected to Brivo and not another website masquerading as Brivo. This is possible because Brivo uses a digital certificate (see section titled "Digital Certificates") issued by a recognized third-party Certificate Authority who took steps to verify the Brivo corporate identity in the process of issuing the certificate.

Through the process outlined above, the administrator may now be assured that access to an account in the Brivo system is legitimate.

Mobile Applications

Brivo Onair Pass is an iOS or Android application that can be used in place of a physical credential when the Brivo Onair Administrator grants these permissions. Communications are secured using TLS. The Brivo Onair Pass application must authenticate itself to the Brivo API every time it is used. The software on the phone follows industry best practices by using the iOS Keychain or Android's Private Mode to secure access. The iOS Keychain is used to store refresh tokens. Android tokens are secured and stored in Private Mode so only the app has access to the data. If the phone is stolen or comprised, an administrator should cancel any mobile passes associated with that user.

Brivo Onair for iOS and Android is an application designed for use by Administrators for mobile access to their account functions. Communications are secured using TLS. The software on the phone follows industry best practices by using the iOS Keychain or Android's Private Mode to secure access. The ID and password used to sign in are secured and stored in the iOS keychain and in Private Mode for Android. If the phone is stolen or comprised, an administrator should change their password.

Whenever mobile devices are used for physical access, we recommend a PIN (or equivalent security mechanism on the phone) be used to secure access to the phone. On an iOS device, iCloud can be used to erase all data remotely. On an Android device, data can be erased remotely if the phone is linked to a Google account.

Control Panel Authentication

A control panel is dedicated hardware containing a microprocessor, memory, and I/O interfaces that allow it to interconnect to credential input devices such as readers, and door control and sensor hardware such as latches and switches. Brivo has designed and manufactured several models of control panels which differ in capacity, communication options, and features.

Control Panel Verifies Brivo's Identity

All control panels exchange credential and event information with the Brivo data center, and therefore must be assured that they are communicating with Brivo and not an imposter. Additionally, Brivo must be sure that a device attempting to connect as a control panel is, in fact, an authorized device, and that it is only asking for the information it is authorized to receive.

The control panel uses the same method as the administrator to verify the Brivo identity: namely, checking a digital certificate on the servers at the Brivo data center. Like a browser, a control panel establishes a TLS session with Brivo before it begins to exchange information. In doing so, Brivo presents its digital certificate to the control panel, which it can check in much the same manner as an administrator might.

In the case of the control panel, however, the process of checking the digital certificate must be automated because there is no human present to check its validity.

The first step of this automation occurs during manufacturing by embedding information in the control panel that will allow it to check the validity of the digital certificate presented by the Brivo data center. Specifically, the control panel has knowledge of the 'public key' associated with the digital certificate on one or more Brivo web servers.

The second step of the identity verification process takes place when setting up the TLS session used to exchange event and credential data. If the certificate presented by the Brivo data center (or an imposter) does not match the certificate that the control panel expects, then it will refuse to communicate with the Brivo data center.

Brivo Verifies Control Panels' Identity

It is just as important for the servers at Brivo to be able to verify the identity of a control panel to ensure data is shared with only genuine and authorized control panels.

Our servers are able to verify the control panel's identity because Brivo installs a unique digital certificate (used as a client certificate in the context of TLS) on each control panel at the time of manufacture. This certificate is digitally signed by Brivo so that its origin can always be confirmed at a later time and cannot be faked.

When a control panel attempts to establish a TLS session to download data or report events, the Brivo servers force it to present its client certificate before gaining access to the system. If it has a valid certificate that was issued by Brivo, then a TLS session is initiated and it is allowed to download data and upload event information. If not, it is blocked for any further activity on the server.

In addition to blocking attempts at spoofing or impersonation, the client certificate requirement also blocks out unauthorized attempts to gain access to these web servers.

API user security and authentication

The Brivo API use the OAuth2 three-legged authorization code workflow for account access. Account Administrators are provided the ability to selectively enable API connections to their Brivo Onair account. All communications via the API are secured via TLS.[2]

[2] For technical information on the Brivo API, please visit http://apidocs.brivo.com

Digital Certificates

The preceding two sections discuss the use of a digital certificate to provide authentication between various parties in the Brivo system architecture. But what is a digital certificate?

A digital certificate is an electronic document containing unique data that allows a device (or person) to authenticate itself to another device (or person). Its use in this context is part of a cryptographic protocol known as public key infrastructure or PKI. In particular, a digital certificate contains the public key of the owner of the certificate. This public key is shared with other people or systems with whom you wish to communicate.

A corresponding private key is held secret and not shared with anyone else. When two parties – say Alice and Bob – wish to authenticate themselves to each other, they present digital signatures based on their private keys. They can each then check the respective signatures using each other's public key to verify that they are indeed communicating with the right party.

If Bob then wishes to send an encrypted message to Alice, he can encrypt the message with Alice's public key. The message can then be decrypted only by Alice's private key, which she has kept secret to herself.

In the Brivo architecture, both the data center and the control panel have digital certificates that allow them to verify the identity of the other, and subsequently encrypt their communications so that no one else can intercept them. This is true regardless of whether the communications occur on wired or wireless media.

Brivo Use of Digital Certificates

Brivo uses a type of digital certificates described by the ANSI X.509 specification for public key infrastructure (PKI) systems.

The reference architecture calls for a certificate authority (CA) – a trusted party who can externally validate the identity of certificate holders prior to their issuance – to manage the creation, management, and revocation of certificates.

For control panels, Brivo acts as its own CA because it can guarantee a physical chain of custody during the installation of certificates into control panels in our manufacturing process, and because there are no third parties communicating with those panels who need to be part of the authentication process.

TLS Encryption

There have been numerous references to the Transport Layer Security (TLS) in the preceding sections. While it is a familiar term to most web users, it can be used in several different ways.

In the case of Brivo Onair®, it is used for both its embedded encryption functions, as well as its authentication capabilities.

First, some background on TLS is needed. TLS and its predecessor SSL are best known as an encryption protocols favored by such secure web services as online banking, stock trading sites, and e-commerce in general. It is used in these contexts because of its wide availability in commercial browsers and software libraries, and because it is highly secure. Properly implemented, TLS is virtually invulnerable to attack.

TLS is most commonly used to encrypt sessions between a browser and a web site. In these applications, the website typically uses a digital certificate as part of the TLS handshake, which is what allows users to verify that they are starting a secure session with the expected web site. However, the browser client does not typically use a client certificate, which means that the web site cannot verify the identity of the client. In the Brivo Onair® architecture, both server and client certificates are used so that both parties can verify each other's identity. The resulting TLS session is therefore both secure and authenticated.

TLS is available in different strengths depending on the size of the cryptographic key used to seed the encryption process. The Brivo servers enforce 256-bit encryption, which on average requires billions of processor years to decrypt without the correct keys.

Introduction to encryption

256-Bit TLS refers to the length of the encryption key used to encrypt the data exchange session. Generally speaking, the bigger the key, the more secure your data will be.

The encryption algorithm uses this key to create a unique session. In the Brivo system, the 256-bit encryption between the control panel and host uses the Digital Signature Algorithm (DSA) verified with a digital certificate signed with a key length of either 1,024 or 4,096 bits, depending on the device.

Our web applications and APIs communicate over HTTPS (TLS 1.2 or higher) using the SHA-256 algorithm with a 2048-bit RSA key.

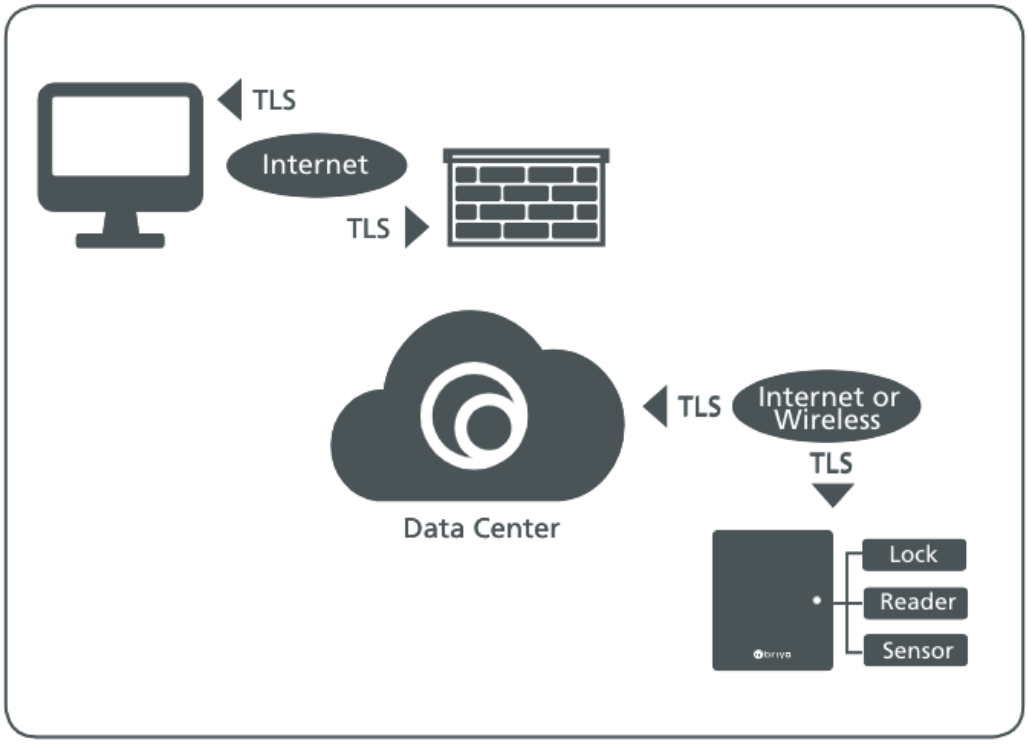
SECURITY FEATURES IN SYSTEM DESIGN

The basic Internet security components described previously are put to use in the Brivo Onair system as shown in Figure 4.

Secure Web Browser Access

Administrators access their data via the Internet, using a web browser in an encrypted Transport Layer Security (TLS) session. Brivo supports 256-bit encryption on this link. This is the same level of encryption used by banks and financial institutions to protect access to online accounts.

Figure 4: TLS 1.2+ Is Used for Encrypted Communications



Secure Control Panel Access

The Brivo Onair® control panels also use 256-bit encryption technology to protect data transmissions between the data center and the control panel itself.

The TLS encryption technology is independent of the physical communications medium used between the data center and the control panel. Brivo uses this technology on any link that supports the IP protocol stack and HTTPS. The architecture therefore allows communications across Ethernet-based corporate LANs that have a broadband link to the Internet. It also operates over the cellular communications networks that support the IP protocol.

CONTROL PANEL SECURITY DESIGN

The design of the Brivo control panel follows information security best practices. In addition to the strong 256-bit TLS encryption described above, the networking and application design of the product follow sound security principles.

Networking

In most IP networks, any device on the network is susceptible to hacking or unauthorized access. First and foremost, this is because most devices listen to network traffic in order to receive communications that might be intended for them: commands, broadcast messages, network management interactions, and so on. The willingness of a networked device to accept unsolicited external communications is its key vulnerability.

The Brivo control panel will not accept inbound connections. It will only listen to network traffic within the HTTPS session which was initiated by the control panel itself. This protects the control panel against unauthorized access because it simply will not accept unsolicited communications. For example, it is not possible to do any of the following to a Brivo control panel; initiate a telnet, FTP, HTTP/S or any other type of communications session; burden the device through a denial of service (DoS) attack (although the rest of your network may be affected); give the device a virus; or gain access to the file system.

IP Configuration and DHCP

The control panel must still have some communications with the rest of the IP network on which it resides, particularly with respect to establishing network operating parameters.

First, the control panel will need to have an IP address. This can be established in one of two ways: by a command line interface (CLI) accessible via a crossover Ethernet port, or via the "DHCP" protocol.

The Brivo control panel supports the DHCP protocol for ease of configuration. DHCP has become the preferred method of managing network devices on most corporate LANs. Supporting DHCP presents no additional security risks for the control panel or the Brivo Onair® service itself due to other precautions Brivo has designed into its products. Specifically, our implementation of certificate-based authentication (see section titled "Authentication") defeats "DNS spoofing" and "host impersonation" types of attacks which can arise when a DHCP server points to a compromised or malicious DNS server.

For networks that do not support DHCP, or network administrators who would prefer to assign an IP address manually, the Brivo control panel has a local web interface that allows the

administrator to enter all network configuration parameters using a laptop and an Ethernet cable.

Overview of DHCP

DHCP stands for dynamic host configuration protocol. Before DHCP, network administrators had to enter various configuration parameters into every networked device in order for it to know how to communicate with the rest of the devices on the network.

DHCP is a mechanism for allowing a network device to query a "DHCP server" to obtain an IP address, a subnet mask, a default gateway, DNS server address, and other configuration information that allows the device to communicate on the LAN and on IP networks in general.

DHCP greatly simplifies network administration and has become common on most corporate networks.

Non-Routable IP Address and NAT

The Brivo control panel initiates all communication sessions with the Brivo data center, so the IP address assigned to the panel need not be a static or routable IP address. Non-routable IP addresses cannot be transported over the Internet. This protects the device from exposure to the Internet because it is shielded behind the corporate routers and firewalls like all other devices on the network with non-routable IP addresses.

Specifically, this means that the control panels will operate with routers and firewalls configured to use Network Address Translation (NAT).

Compatible with Firewalls and Proxy Servers

Many corporate networks are protected with proxy servers (stand-alone or in combination with a firewall). Brivo anticipated this network architecture and built in support for the SOCKS5[3] and HTTP proxy protocols, so that it can authenticate itself to the proxy service and access the Brivo data center.

For network administrators, this design ensures that no changes will have to be made to your existing IT architecture. For example, the Brivo control panel does not need to have a "hole" put into the corporate firewall to listen for incoming traffic. All it requires is that outbound HTTPS traffic be allowed to go to the data center. Nor does the control panel need to be situated in a "DMZ" on your network. Since the panel operation does not depend on externally

[3] SOCKS5 proxy servers allow for more opaque communication than HTTP since the external server communicates with the SOCKs server as if it were the actual client. Many large corporations deploy SOCKs proxy servers on their networks.

initiated transactions, there is no need to expose it to open Internet traffic. For networks with a proxy server, normal operations can continue, with only the addition of a login and password for the control panels added to your LAN.

DATA CENTERS AND HOSTING

Brivo Onair services are hosted within a multi-cloud environment leveraging both Amazon Web Services (AWS) and Microsoft Azure environments. Primary and disaster recovery (DR) services are located in separate US geographic regions within multiple availability zones.

Brivo data centers have the following general capabilities;

Physical Security

Brivo data centers are outfitted with biometric scanners and secure card access to the collocation services areas of the data center. Additionally, all Brivo equipment is kept in secure locations. On-site security personnel monitor hosting facilities 24/7 via indoor and outdoor video surveillance. Data center access requires security desk check-in and is managed 24/7. Local key management is enforced for racks and cabinets.

Network Security

Brivo has instituted a multi-layered approach to network security for the production Brivo Onair and disaster recovery environments to ensure the confidentiality of networks and data. The network security architecture includes the use Next Generation Firewalls (NGFW), IPS, network address translation (NAT), and network segmentation such that database servers are not visible to the public. In addition, these environments are both logically and physically distinct from the Brivo corporate office network.

Access to the production and disaster recovery networks is controlled, logged, and monitored by Brivo. In addition, encryption techniques are used to support the confidentiality of information sent from one system to another. Between data centers data is transmitted via IPSEC using randomly generated key values.

Redundancy and Disaster Recovery

Every component in the Brivo production data center is redundant in either an active/active or active/passive configuration. The Brivo Onair infrastructure at the production data center is designed with scalability and redundancy in mind so that there is no single point of failure. Therefore, every production component of the Brivo Onair has a redundant counterpart; including firewalls, load balancers, web servers, application servers, and database servers. The

data center hosting provider also features redundant power supplies, dual management cards in each switch, redundant Ethernet, redundant gigabit fiber aggregators, and redundant routers.

In case of disaster, Brivo maintains DR services in three local availability zones and three more availability zones located more than 2,000 miles from our primary data center.

An Independent Network

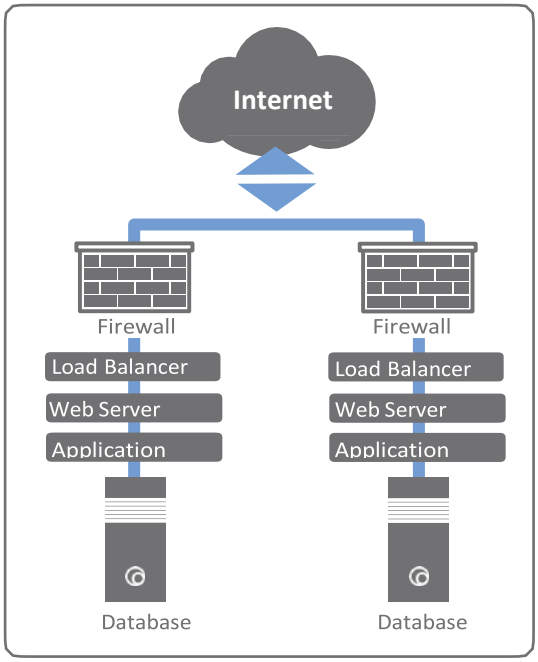
For security reasons, the Brivo operational network at its primary data center is completely independent of our corporate office network. What this means from a technical standpoint is:

- Physically distinct networking equipment
- Distinct ISP relationship
- Distinct network address space
- Gateway to data center is dedicated link, with firewall against corporate network

What this means in practice is:

- Brivo employees cannot access data center accidentally or intentionally
- Access to operational network requires firewall logon
- Any compromise of our internal corporate network does not “spread” to the operational network

Figure 5: Brivo Data Center Detail



NETWORK SECURITY AT BRIVO'S DATA CENTER

Network security begins with analyzing the potential threats that your network is designed to withstand. In the case of the Brivo hosted applications at our data center, we have built safeguards against all of the following types of threats:

- Denial of service (DoS) attacks
- Database attacks
- Cross-site scripting attacks
- Cross-site forgery attacks
- Web server exploits
- Malicious employees
- Applications server exploits
- 'Social engineering' attacks
- Operating system exploits

Firewalls

The first line of defense that protects your data at the Brivo data center is a firewall. A firewall is a device which examines incoming and outgoing data traffic and decides whether it should be allowed or blocked, based on a set of rules programmed by the network administrator. At our data center, firewalls are configured to screen out all types of traffic except for HTTP (for our public site) and HTTPS (once you have accessed your account). There are no other "services" available on the Internet-facing aspect of our transaction processing system.

This means that many of the common forms of gaining access to computer systems are blocked right at the firewall itself. For example, it is not possible to access Brivo using FTP, Telnet, POP or IMAP mail protocols, instant messaging protocols, or any of the many other types of IP traffic common on the Internet today.

Denial of Service Attacks

Denial of Service (DoS) attacks are floods of traffic that slow down computers and networks to the point where they can no longer perform their primary functions. They come in two different forms: those that cripple an entire network, such as the Internet itself, and those that debilitate a specifically targeted computer system by forcing it to respond to too many requests.

While Brivo can do nothing about DoS attacks that slow down the Internet itself, our data center resources are protected against DoS attacks at multiple layers. First, the firewalls block out the vast majority of types of traffic responsible for most widespread DoS attacks. The servers inside of the firewall never even see this traffic, and are thus unaffected by it. This would include all forms of attack that use protocols other than HTTP/S to achieve their effect.

A second line of defense is provided by the load balancers (see Figure 5: Brivo Data Center Detail) used to spread traffic across multiple servers for scalability. The load balancers examine incoming traffic and make decisions about how (or whether) it should be routed. As part of this operation, they are also about to guard against a common form of attack known as a "SYN flood", a technique whereby computers are disabled by trying to respond to connection requests.

Intrusion Prevention Systems

Brivo uses an intrusion prevention system (IPS) to examine all incoming traffic for signs of hacking or other unauthorized access. An IPS is, in effect, a security guard that sits at the front door of the network and watches for "burglars." If it sees one, it can directly respond to threats as well send out a notification that trigger human intervention.

SERVER SECURITY

Beyond the perimeter defenses provided by networking equipment, servers themselves must be secured against unauthorized entry in the event that the perimeter is penetrated.

There are three levels at which information security measures have been applied in the Brivo server environment:

- Operating systems
- Web and application servers
- Database severs

Operating Systems

The security of an application is ultimately only as good as the security of the operating system on which it is running, some operating systems being simply more immune to attack than others.

All operating systems have vulnerabilities, and, as they are discovered and published to the industry, it is essential to apply updates to the operating systems to ensure that all known weaknesses are eliminated. Brivo monitors all of the major security advisories and makes a practice of constantly updating its server operating systems with the safest available software.

Web and Application Servers

Web servers are vulnerable to a variety of attacks. Some of these will disable the server, while others may allow hackers to gain access to the operating system of the server itself, which then provides a beach-head for further malicious activities within the network under attack.

Due to their internal architecture, the web servers used in the data center are not vulnerable to many of the common types of attacks such as buffer overflows and malformed strings. This is largely due to the fact that they are based on the Java programming language, which has built-in safeguards against such errors.

Database Server

The database server is a highly protected resource which is separated from all other server resources. There are no unnecessary services running on the database server, which severely restricts the options for accessing the system at the operating system level or with direct connections to the database itself.

APPLICATION SECURITY

As discussed above (see section titled “Authentication”), the Brivo system requires administrators and control panels to authenticate themselves before they can access any system resources or data. But what does this really mean? And, once someone or something has authenticated itself to Brivo, how can its access to data be controlled? Can another valid user access my account information?

Application Security Model

Our application security model is based on the notion of Access Control Lists (ACLs). An ACL is a set of rules which specify which users can access with objects in a system. This concept will be familiar to anyone who uses a file server. The administrator of the file server establishes *permissions* for files, directories or folders, and executable programs. These permissions specify such properties as to who may read, write or execute the resource(s) in question, and under what circumstances they may do so.

In Brivo applications, the same concepts are used, both explicitly at the UI level, as in the case of our Tiered Administration capabilities, and implicitly, in a behind-the-scenes “matrix” that indicates, for every object in the system, which authenticated entities may look at or alter the object.

For example, the object representing the control panel in an office may be accessed by any Administrator *in your account* who has sufficient permissions to do so. No Administrator outside of our account can see or make changes to the control panel.

Can an Administrator from another account get around these restrictions? Can they get around the application restrictions by accessing directories or files directly? The answer is "No" and the detailed technical reasons are explained in the next section.

Instance-Based Security

Brivo has implemented a computer industry standard application security model known as instance-based security. This approach is based on a programming model and set of modules which allows developers to implement a set of security measures that are consulted each time an end-user attempts to access an instance of data, such as a user record.

In contrast to some application designs (web-based as well as other technologies), the security framework enforces permissions not only when an end-user enters the application, but each and every time that user attempts to perform an operation on an object. In other words, a user's permissions (such as those of an Administrative login) are checked each time an action is attempted. This means that even if an Administrator from another account attempts to gain access to another account (e.g., by altering URLs), the attempt will fail because that Administrator will not pass the authorization check for the object he or she is trying to change.

INFORMATION SECURITY POLICY

Brivo recognizes the key role played by humans in the security of its systems. Without strict information security policies and control, no amount of technology can provide security for your data. In fact, human error and malice are two of the most frequent causes of information security breaches. That's why Brivo has invested in information security policy development and training, augmented by frequent internal reviews and audits.

Our corporate information policies are based on the best practices of financial institutions and managed service providers, and are vetted by industry experts to ensure that they are always complete and up-to-date.

Audits

Our 3rd party data centers have more 10,000 security controls and compliance policies formatted for FFIEC reporting and comprehensive practices for SSAE 16 SOC 1, SOC 2, PCI DSS, ISO 27001, Safe Harbor, Global Risk Management, BCDR, and FISMA (NIST 800-53).

Our data center's accreditations are in addition to the Brivo certifications of its internal controls.

Brivo Onair has been validated with more than a decade of information security audits as well as the Cloud Security Alliance STAR designation and Privacy Shield certification from the Department of Commerce. SOC 2 audits are conducted by Brivo with our independent service auditor.

These audits ensure that Brivo:

- Utilizes proper administrative controls to protect sensitive information
- Implements the controls in a verifiable and measurable way
- Allows independent auditors to periodically check controls and systems to verify compliance

Information Security Audit Overview

An information security audit is a check to ensure that a service provider has implemented and is following a standard set of security policies or controls. The audit reviews policies and practices that are technical, physical and administrative in nature. Audits are typically based on regulations and guidance from industry groups, government agencies and regulatory entities such as these:

- The American Institute of Certified Public Accountants (AICPA)
- The International Organization for Standardization (ISO)
- The Cloud Security Alliance (CSA)
- The National Institute of Standards and Technology (NIST)
- Payment Card Industry Data Security Standard (PCI DSS)

Audits cover topics such as the physical security of data centers, the logical security of applications as well as the disaster recovery processes and administrative procedures of service providers. One common US audit standard uses criteria set forth in the AICPA Guide, Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy. This is known as a SOC 2 audit standard.

A recognized international standard is ISO 27001, which is provided by the International Organization for Standardization (ISO) and is a certification and information security management system standard for IT systems.

Specific Controls

Brivo employs independent auditors to verify the following:

- Employees with access to sensitive information undergo background checks and receive enhanced security training
- A risk management strategy is employed and that all risks and the mitigating controls are documented
- Brivo monitors the activity of systems and employees to ensure the quality and security of products
- There is a clear communication channel between support personnel, management, and customers, and an incident or problem is recorded.
- Changes to the system are reviewed, tested, and recorded prior to implementation

Continuous Vulnerability Scans

Brivo routinely conducts vulnerability scans with multiple tools to enhance the security of its products. These tests are critical elements of any cloud security program. These tests ensure the privacy and security of customers by detecting, testing, and repairing vulnerabilities that could be exploited by a malicious party.

Brivo conducts these tests in several layers to isolate problems and to ensure maximum security for our clients. First, each product is scanned during development for known errors. The second phase is to install each product in an isolated security environment with simulated data, and attempt to exploit the discovered or previously known vulnerabilities. Once any discovered weaknesses are addressed, the product is retested and released for general use.

Passwords

Brivo has imposed a password management protocol on its employees which ensures that passwords are changed frequently, that they are not likely to be guessable, that they are not written down anywhere, and that they not be shared across multiple servers or security domains.

Training

All Brivo staff receive information security awareness and policy training on a periodic basis. The training covers general background knowledge of information security threats as well as specific precautions which have been designed into the Brivo systems. It also addresses issues such as confidentiality, privacy, and social engineering.

Customer Service

The Brivo Customer Service Representatives (CSRs) are a major focal point of our information security policies.

The customer service group is frequently called upon to verify the identity of callers seeking assistance with their accounts, which, as often as not, will ultimately require sharing of certain information.

The CSRs therefore use an identity verification protocol with all callers so that they can ensure that any requested account changes, forgotten passwords, or other information requests are being made by an authorized party.

Because of the sensitivity of the CSR function, the hiring process for these positions includes extensive screening and background checks.

Conclusions

Brivo has implemented every major information security precaution available with today's technology, consistent with the nature of the application and our customers' desire to be able to use the technology from anywhere, at any time.

We also pay constant attention to human factors. It has been widely reported that most security breaches - whether in the physical world or the world of information, - are a result of human carelessness or malicious intent. While Brivo can never change that, we can make sure that our staff is held to the highest ethical standards for handling your data, and that our internal audit processes will continue to safeguard vital customer data.

FREQUENTLY ASKED QUESTIONS

What data is recorded in Brivo Onair?

Brivo Onair provides the capability for Subscribers to store basic personal information such as an individual's name, email address and photograph. This information is used to correlate security events to the correct individual as well as to enable notifications and Brivo Onair Pass functionality. Though the system has the capability to store a number of personal data elements, these items are not essential for operation of the system. Brivo Onair records the actions of system Administrators as well as the status and the settings of various devices that have been configured to operate with Brivo Onair.

How is my data used?

Customer Data entered in Brivo Onair by Subscribers or collected through the operation of the system are for the exclusive use of our Subscribers. Brivo may access Customer Data only for the purpose of providing the Services or preventing or addressing service or technical problems or as may be required by law. Brivo does not sell, rent or trade personally identifiable customer information with third parties. Brivo shares data with relevant 3rd party processors when explicitly authorized by administrators in the relevant Brivo Onair account, for example, to enable integrations via our Application Programming Interface (API).

How secure is my data?

The security of Customer Data, including personal data, is very important to Brivo. Brivo maintains a comprehensive, written information security program that contains industry standard, administrative, technical, and physical safeguards designed to prevent unauthorized access to Customer Data. Brivo Onair safeguards Personally Identifiable Information (PII), in accordance with NIST SP 800-122 and OMB memos M-06-16 and M-07-16 with specific provisions enabled by the Subscriber.

How does Brivo prevent against hacking the web site?

As described in the Brivo Information Security white paper, Brivo has followed industry best practices for securing data and applications in our data center. These measures include: physical security of the data center itself, network security instruments such as firewalls, authentication and string encryption, operational practices such as keeping operating systems and applications secure against known vulnerabilities, and engineering application-level security into Brivo web services.

Can Brivo employees see my data?

Customer Service Representatives (CSRs) can view certain data within your account when you authorize them to do so. The Journal in your account will reflect all such access.

No other Brivo employees are permitted to view your data. This policy is enforced in several ways. First, the Brivo corporate LAN is completely separate from the LAN at our data center. Network operations employees are authorized to access the data center via a dedicated link from our headquarters, but only

through a firewall and only with the proper password information. Per the Brivo information security policy, these passwords are known by very few individuals and are changed on a regular basis.

Can I get my data out of Brivo Onair?

Yes, customer data can be exported from Brivo Onair via our report functions. In situations of termination of an account Brivo will provide a complete copy of the account data upon request.

GLOSSARY

ACCOUNT	An Account on the Brivo Onair® system, which is the control mechanism for associating logins, sites, users, etc.
ACS	Access Control System is an electronic system for allowing or barring entry to a facility based on a credential held by a user.
AES	Advanced Encryption Standard is a reference to the Rjindael symmetric encryption algorithm, the winner of the NIST's (National Institute of Standards of Technology) worldwide competition to develop a new encryption technique that can be used to protect computerized data; considered more secure than earlier standards such as 3DES.[4]
API	An Application Programming Interface
CREDENTIAL	A piece of information, usually digital, which serves as a means of identifying a user to an Access Control System for the purposes of authenticating the user and determining what that user's permissions are within the system. In an ACS, credentials are typically PIN codes, proximity card values, biometric data, mobile credentials, etc.
CONTROL PANEL	The hub of an access control system to which all other devices are connected. Examples from Brivo include the ACS6000 series and the ACS300 series.[5]
DIGITAL CERTIFICATE	An electronic document for uniquely identifying a party in a communication session, issued by a Certificate Authority.
DOS	Denial of Service is an attempt to slow down computers and networks to the point where they can no longer perform their primary functions.
GSM	Global System for Mobile Communications is a standard set developed by the European Telecommunications Standards Institute (ESTI) to describe the protocols for second generation (2G) digital cellular networks by mobile phones.
HTTPS	Hypertext Transfer Protocol Secure is a communications protocol for secure communication over a computer network, especially wide deployment on the Internet.

[4] http://csrc.nist.gov/archive/aes/rijndael/wsdindex.html
[5] Datasheets on Brivo products are available at www.brivo.com

JOURNAL	A permanent, non-editable record of all changes made to a Brivo customer account. The Journal is accessible to Administrators within the Brivo application.
KEY	A unique digital string of information used in cryptographic protocols to validate the identity of the bearer of the key or to encrypt and decrypt information exchanged with other parties.
NIST	National Institute of Standards and Technology is a federal technology agency that works with industries to develop and apply technology, measurements, and standards.
READER	One of the several types of devices mounted at the facility entrance which serves as an input device for credentials such as proximity cards, smartcards, PIN codes, biometrics, mobile credentials, etc.
SSL	Secure Sockets Layer is a protocol that provides a framework for authenticating and encrypting communications sessions. The successor to SSL is TLS
TLS	Transport Layer Security is a protocol that provides the framework for authenticating and encrypting communication sessions.