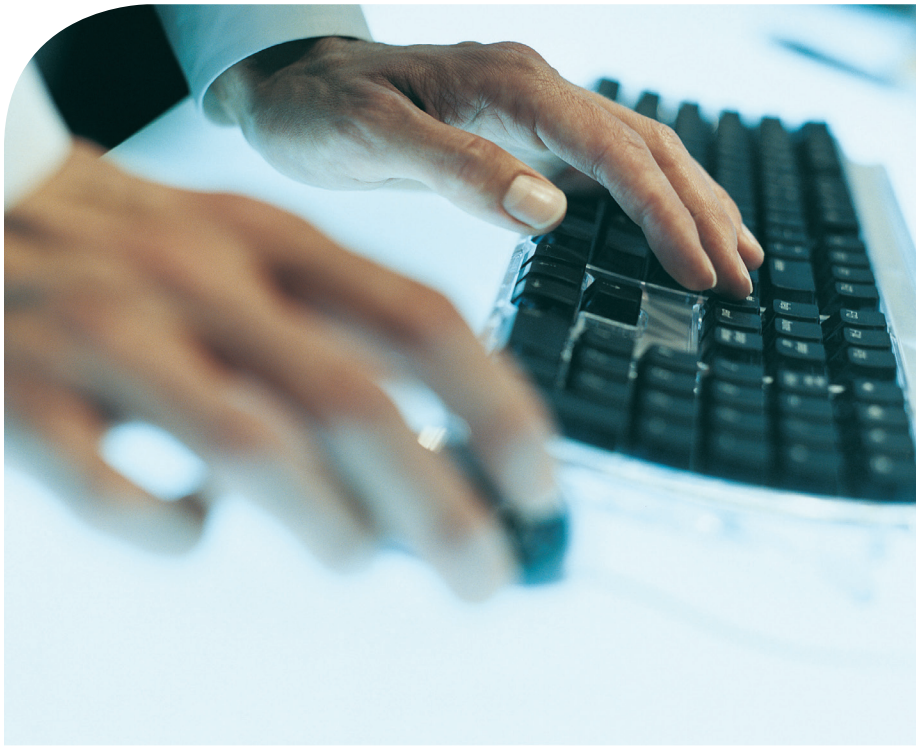
WHITEPAPER
Revised October 2013

Brivo OnAir℠ Information Security

Providing Assured Control of Facilites and Information



brivo®
simply better security

brivo
simply better security

Legal Disclaimers

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 product themselves is protected by the copyright and/or other intellectual property laws of the United States.

Brivo is a wholly owned subsidiary of The Duchossois Group, a privately held holding company, which also owns AMX, The Chamberlain Group and Milestone AV Technologies.

brivo
simply better security

301.664.5242 | Toll Free: 866.692.7486 | www.brivo.com

Table of Contents

Information Security

As a provider of physical access control 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 engineered into Brivo services since day one, both at our central hosting site and in our field hardware.

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, but it does contain a basic introduction to Internet security concepts.

The topics covered in this paper 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 in general. Some of these topics will already be familiar to IT professionals and others who have studied information security. Brivo has not reinvented network and application security, but rather applied it to a new domain: cloud-based access control systems.

The scope of this document includes the following major topics:

- Brivo's data center, where our web applications are hosted
- The Brivo control panel which resides at the customer premises
- Wired and wireless data communications
- Web browser client security considerations
- Authentication, authorization and accounting
- Cryptography
- IP networking considerations for data security

References

While this paper is intended to be a stand-alone document, some readers may have additional interest in either the Brivo system or some aspects of information security discussed herein. For that reason, a brief list of Brivo references is provided below. Footnotes and URLs throughout the text will indicate where readers can find more extensive discussions of information security documents.

The following Brivo publications are also available at **www.brivo.com** or by contacting Brivo at **sales@brivo.com:**

1. Brivo Architectural and Engineering Specification
2. Brivo Installation Manual
3. Brivo Administrator's Manual

System Overview

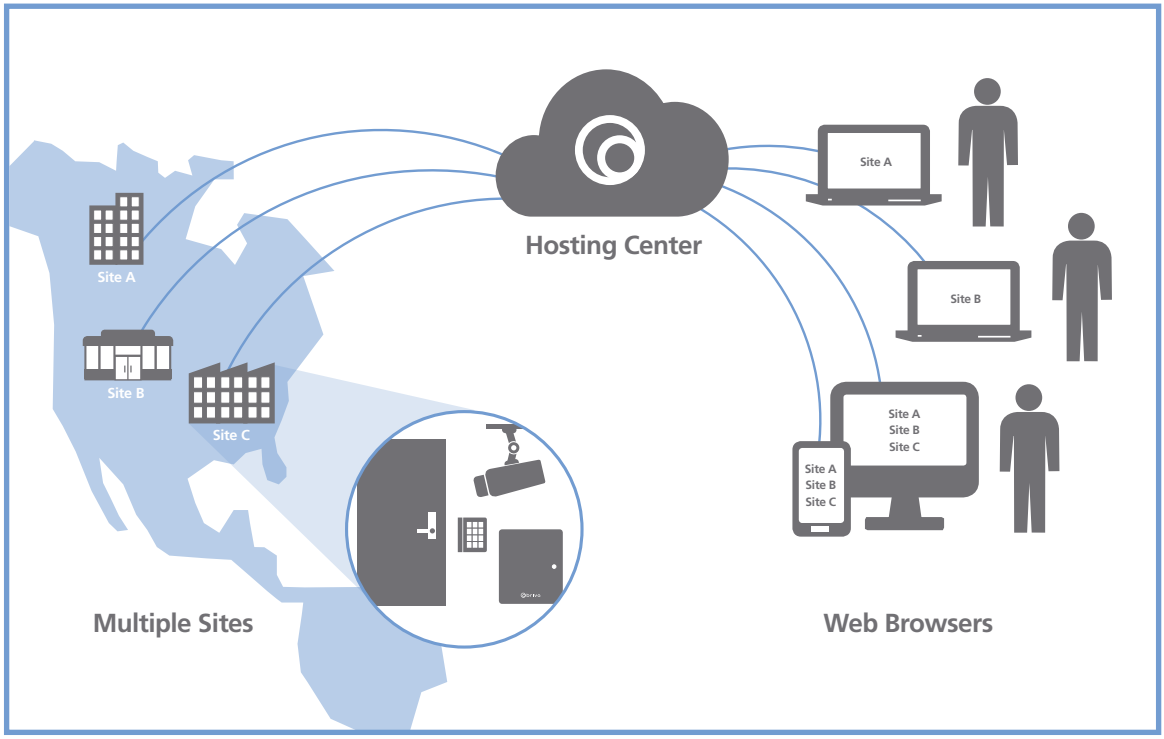
Brivo services are based on a centralized, cloud-based architecture, where all users and distributed hardware devices (control panels) share a common set of network and server resources at our data center. In particular, Brivo hosts a facility access control system, primarily targeted at commercial properties with employee, resident and visitor populations whose 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

This way of doing business is often referred to as a Software as a Service (SaaS) model. The core characteristic is that software and data processing are provided as a service, rather than as an outright sale, which requires server and other equipment installation at the customer premises. Several of the key advantages for access control are:

- Lower Total Cost of Ownership (TCO)
- No dedicated on-premises computer equipment
- Ease of installation
- Automatic application updates (both web and device firmware)
- Redundancy and archival data storage built into service offering

Figure 1: Brivo System Overview



Basic Access Control System Operation

As shown above in Figure 1, there are 4 major components to the overall operation of Brivo OnAir℠ service:

- Customer premises equipment consisting of a control panel and credential readers
- Wide Area Network (Internet, GSM / CDMA, etc.)
- Brivo's centralized, cloud-based applications resident at our data center
- Web browser on the end-user's PC or mobile device

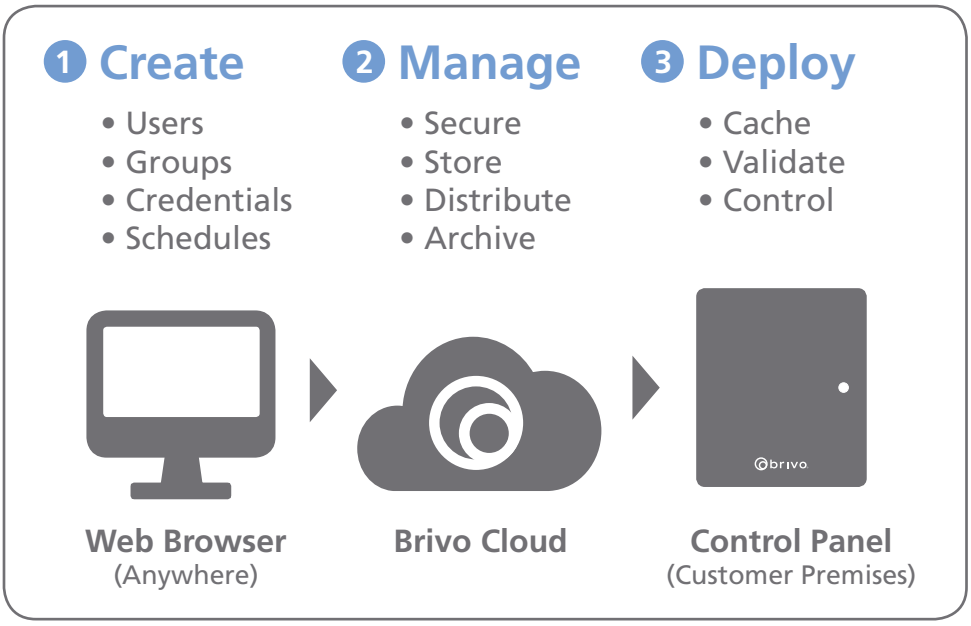
These components share data across multiple platforms and networks in order to distribute credentials, centralize access and alarm event records, and provide other services such as software updates to control panels.

Control panels are networked to our data center 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 GSM / CDMA cellular modem. Alternatively, sites with a wireless 802.11 network may also use a wireless bridge to the control panel to simplify wiring requirements.

Data Life Cycle – Creation and Distribution

The access control cycle begins with an administrator logging into Brivo's application and setting up users, groups, credentials, schedules, and other data elements that dictate who has permission to enter which facilities at which times. Data is centrally stored and then distributed to the control panels that need them to operate. Once downloaded, they are used to control access to each door that is wired to a control panel.

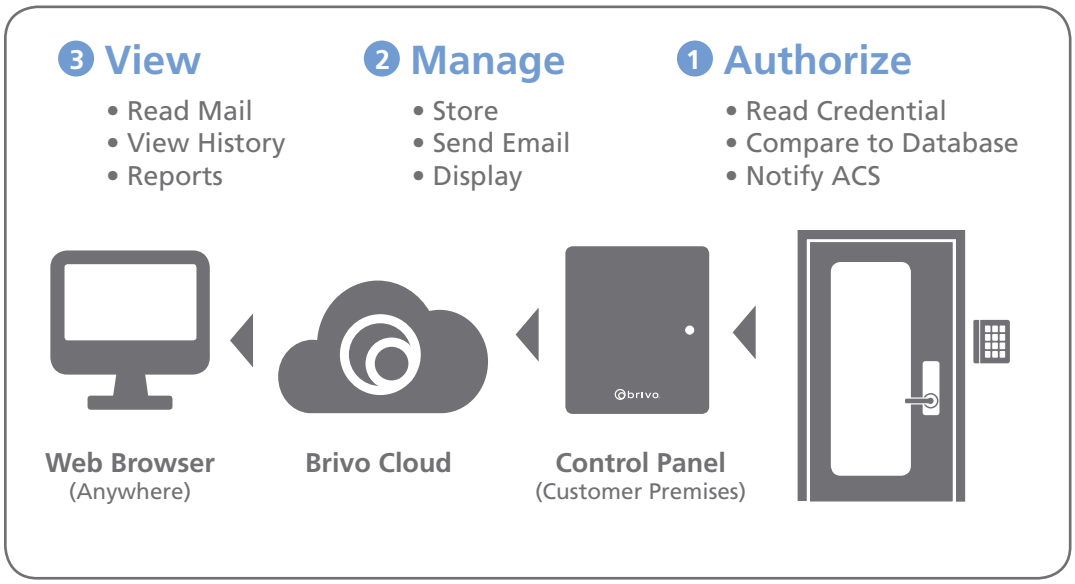
Figure 2: Data Creation and Distribution



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, etc.) with a local database of credentials. When a person presents a credential to a reader attached to a Brivo control panel, the reader 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, Brivo's application software stores the information for subsequent customer viewing and reporting.

The software also consults business rules to determine whether the customer has requested email notification for the type of event in question. If so, the application immediately sends an email notification to the list of addresses the customer has set up for his or her account.

Of course, all of these transactions must be 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.

The methods Brivo uses to secure customer data are proven techniques borrowed 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
- SSL Encryption

Authentication

Authentication is the cornerstone of secure information exchange in the 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 communications with the data center.

Administrator Authentication

An administrator is a Brivo customer with privileges to log-in to the Brivo OnAir℠ application and to make changes to an account that controls one or more local access control systems. 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 web site and not an imposter web site.

Administrators are authenticated by providing a user ID and password to the Brivo OnAir℠ application. The user ID / password combination allows Brivo to verify that the person attempting to connect with 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, which must be activated by Brivo Technical Support, 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 which 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.

This entire logon/password exchange takes places within an Secure Socket Layer (SSL) session that begins when the administrator accesses the logon page of the Brivo OnAir℠ application via Hypertext Transfer Protocol Secure (HTTPS). The SSL session protects the exchange of authentication data by encrypting it so that a third-party cannot read the authentication data.

The Administrator must also be able to make sure that he or she is logging into the real Brivo OnAir℠. This is accomplished through the establishment of the SSL session itself. By checking the validity of the digital certificate presented at the beginning of the SSL session, the administrator can verify that he or she is indeed connected to Brivo and not another web site 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 Brivo's 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.

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, communications options, and features.

Control Panel Verifies Brivo's Identity

All control panels exchange credential and event information with Brivo's data center, and therefore must be assured that they are communicating with Brivo and not an imposter. By the same token, 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 Brivo's identity: namely, checking a digital certificate that resides on the servers at Brivo's data center. Like a browser, a control panel establishes an SSL 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 present by the Brivo data center. Specifically, the control panel has knowledge of the "public key" associated with a digital certificate on one or more Brivo web servers.

The second step of the identity verification process takes place when setting up the SSL 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 data center.

Brivo Verifies Control Panel's Identity

It is just as important for the servers at Brivo to be able to verify the identity of a control panel. Otherwise, it would be possible for someone to set up an imposter control panel, have it assume the identity of a legitimate control panel, and then download all of the credentials intended for the real panel. This would obviously compromise a customer's account by allowing a third-party to obtain credential information.

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 SSL) 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 an SSL session to download data or report events, Brivo's 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 an SSL session is initiated and it is allowed to download data and upload event information. If not, it is blocked from any further activity on the server.

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

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 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 keys 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.

Where Does Brivo Get Certificates?

Brivo uses a type of digital certificate described by the ANSI X509 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, and because there are no third parties communicating with those panels who need to be part of the authentication process.

SSL Encryption

There have been numerous references to SSL in the preceding sections. And, while it is a familiar acronym to most web users, it can be used in several different ways. In the case of the Brivo OnAir℠ system, it is used for both its embedded encryption functions, as well as its authentication capabilities.

First, some background on SSL. It is best known as the encryption protocol 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, SSL is virtually invulnerable to attack.

SSL is most commonly used to encrypt sessions between a browser and a web site. In these applications, the web site typically uses a digital certificate as part of the SSL 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 SSL session is therefore both secure and authenticated.

SSL is available in different strengths depending on the size of the cryptographic key used to seed the encryption process. Brivo's servers enforce 128-bit encryption, which on average requires billions of processor years to decrypt without the correct keys.

What Does 128-bit SSL Mean?

128-bit SSL encryption refers to the length of the key used for the symmetric encryption of data exchanges after the authentication phase of an SSL session has been completed. Generally speaking, the bigger the key, the more secure your data will be.

This key is fed into an encryption algorithm to tell it how to encrypt this session versus all other SSL sessions (so they all remain unique).

Since SSL does not dictate a specific encryption algorithm, the key length itself does not mandate a specific encryption technology. This is up to the specific implementation of SSL itself.

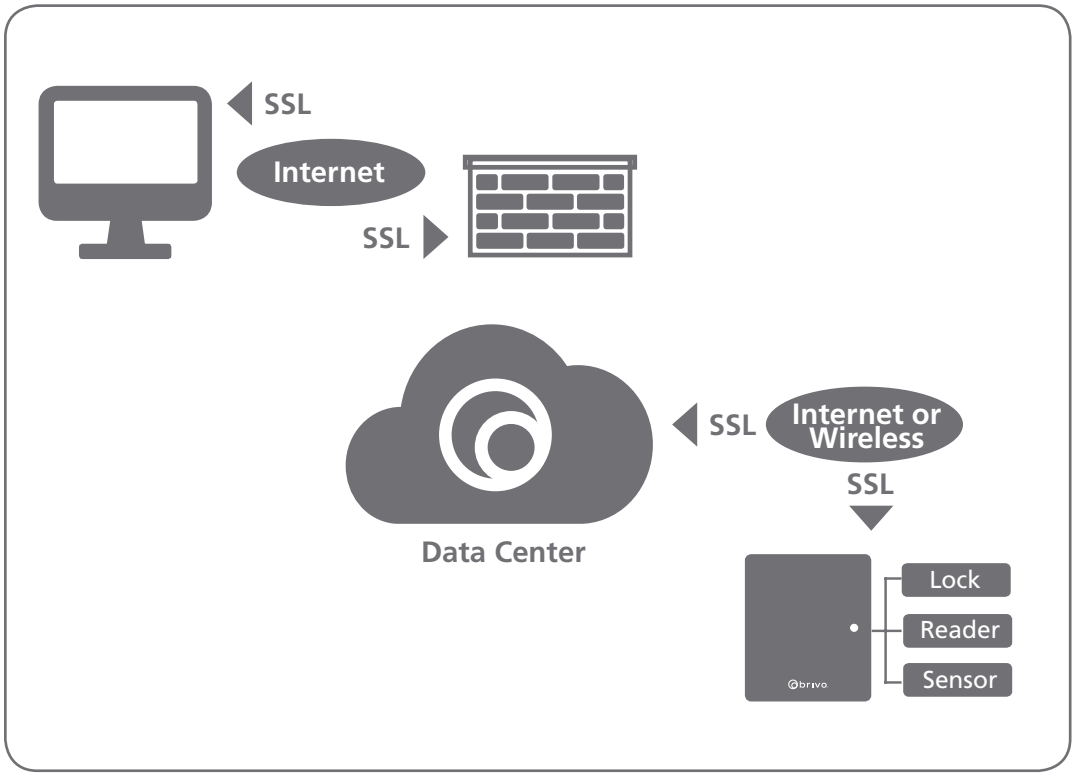
In the Brivo system, the 128-bit encryption to the control panel uses the AES algorithm. The encryption to the web browser can be negotiated between the browser and the server, but is also typically RC4 for North American users with Internet Explorer.

All of these Internet security principles apply to the Brivo system as shown in Figure 4.

Secure Web Browser Access

Administrators access their data via the Internet, using a web browser in an encrypted secure sockets layer (SSL) session. Brivo supports 128-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: SSL Is Used to Encrypt All Communications



Secure Control Panel Access

The Brivo OnAir[SM] control panels also use 128-bit SSL encryption technology to protect data transmissions between the data center and the control panel itself.

The SSL 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 GSM / CDMA cellular communications networks that support the IP protocol.

Control Panel Security Design

The design of Brivo's control panel has been strongly shaped by information security considerations. In addition to the strong (128-bit) SSL encryption described above, the networking and application design of the product are intrinsically secure.

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.

In Brivo's control panel design, however, the system software will not listen to any network traffic outside the context of an HTTPS session which the control panel itself has initiated. 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, and therefore has become the preferred method of managing network devices on most corporate LANs. Does supporting DHCP present security risks for the control panel or the Brivo OnAir℠ service itself? The short answer is "no" – in conjunction with the 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.

What is 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

Because the control panel initiates all communication sessions with Brivo's data center, 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 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 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 Brivo's 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 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

The core of the Brivo system is the hosted application which resides in our primary data center. Brivo owns and manages its own "server farm" which is hosted at several collocation facilities throughout the United States.

As discussed above, data is always encrypted when it leaves or enters our servers, therefore our customers can be sure that no one can intercept it during transmission. But what about the application and database servers where your information is processed and stored? How are they protected?

Physical Security

The collocation facilities where Brivo servers reside are secure web hosting facilities that are protected by 24/7 guards, alarm and fire systems, and require positive photo identification, as well as credentials for entry.

The facilities are protected against attack through various types of barriers, riot glass, and other "hardening" measures which deter both casual and intentional crime and intrusion.

Redundancy in the Brivo Architecture

A security information processing system is important, but only if it can continue to operate through normal maintenance periods and the unexpected equipment repair that inevitably strikes any system.

That's why every component in the Brivo data center has a redundant counterpart that is on "hot standby" and ready to take over if the primary system exhibits any problems.

Brivo also has a complete disaster recovery system located at a separate facility in the event of massive disruption at our primary hosting facility.

An Independent Network

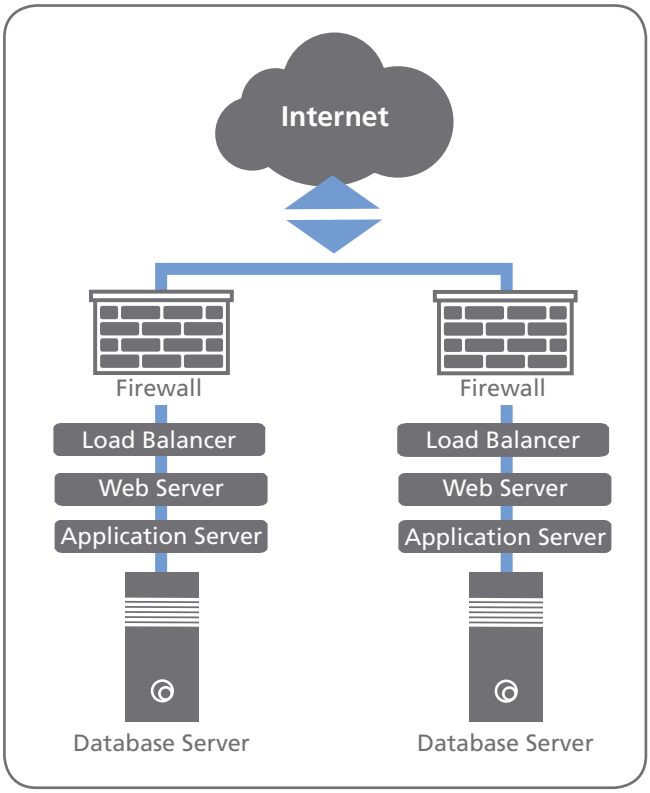
For security reasons, Brivo's operational network at its primary data center is completely independent of our corporate office network. What this means from a technical standpoint is:

- 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 Brivo's 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
- 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 Brivo's data center is, of course, 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, Brivo's firewalls are configured to screen out all types of traffic except for HTTP (for our public web 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 the 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 a part of this operation, they are also able 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 Detection Systems

Brivo uses an intrusion detection system (IDS) to examine all incoming traffic for signs of hacking or other unauthorized access. An IDS is, in effect, a security guard that sits at the front door of the network and watches for "burglars." If it sees one, it sends out a notification so that the crime can be stopped in its tracks via 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 Servers

Operating Systems

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

All operating systems have vulnerabilities, and, as they are discovered and published in the industry, it is essential to apply updates to the operating system 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 attack 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.

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

Brivo application security model is based on the notion of Access Control Lists (ACLs). An ACL is a set of rules which specify which user can access which 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 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 that 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 your 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 allow 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.

Wireless Security

For some models of control panels, the Brivo OnAir℠ uses two-way wireless communications between its control panels and its central servers. The purpose of this link is to allow the administrator to configure the control panel, and to relay access events which take place on doors connected to the control panel. It is an alternative to using hard-wired solutions such as Ethernet.

The security of the data crossing these communication channels is of utmost importance in Brivo's system design, which is why all data is always encrypted when it flows to or from Brivo's central servers. Encryption prevents eavesdroppers from knowing what information is contained in legitimate communications, and also prevents both the control panel and our central applications from being "spoofed" by devices or systems pretending to be part of an authorized Brivo system.

SSL on Wireless Links

The specific networks used in Brivo's wireless products are operated by various providers. Because they are third-party data networks, and because radio transmissions are easily susceptible to interception, Brivo's encryption layer is independent of the network provider, and offers the strongest protection available to its users.

As previously discussed, Brivo uses 128-bit encryption for all control panel access to its central servers. This is also true for the wireless versions of the Brivo product. What this means for users is that data is just as safe on wireless channels as it is traveling over wired channels, such as a corporate LAN and the Internet.

Other Attacks on Wireless Channels

Unlike wired communications channels, wireless communications are also subject to other types of attacks besides eavesdropping. One popular form of attack is simply "jamming" the radio receiver with a strong radio signal at the same frequency, thus preventing the device from sending or receiving any real transmissions. In this case, the Brivo control panel responds by buffering all events and transmitting them after the jamming signal is no longer present. In the mean time, the logic and database of the control panel application is unaffected, and all authorized users may continue to use the door, and unauthorized users are barred. When the wireless network is restored, the event logs show all events in correct sequence with accurate time stamps.

Information Security Policy

Brivo has not forgotten the human side of security, either. 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

Brivo's information security practices are verified by independent auditors to assure compliance with industry best practices. The industry leader Brivo OnAir[SM] is the only cloud-based access control system that is SSAE16 certified and hosted in a FISMA moderate rated data center. 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.

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.

Audits are conducted yearly with quarterly compliance reviews. Additional controls and copies of the audit reports are available from Brivo or our auditors upon request.

Penetration Testing

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

Brivo conducts penetration testing 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 discovered or previously known vulnerabilities. Once any discovered weaknesses are addressed, the product is retested and released for general use.

SSAE16 Overview

Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization, was finalized by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA www.aicpa.org) in January 2010.

SSAE 16 effectively replaces SAS 70 as the authoritative guidance for reporting on service organizations. Changes under SSAE16 include:

· The SAS 70 auditing standard only called for a description of "controls," while the SSAE 16 attest standard now requires a description of its "system," which is considered to be more comprehensive and expansive than that of the SAS 70 description of controls.

· SSAE 16 requires a written statement of assertion, something that was not required under SAS 70. This written statement of assertion must be crafted by management and contain a number of essential clauses which management of the service organization will "assert" to. What is important to note is that the written statement of assertion can be included within or attached to the description of the "system."

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, Brivo's hiring process for these positions include 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 this technology from anywhere, at anytime.

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

Here are some frequently asked questions regarding Brivo's information security:

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?

Brivo's Customer Service Representatives can view certain data in 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 Brivo's information security policy, these passwords are known by very few individuals and are changed on a regular basis.

Glossary

Account
An Account on the Brivo OnAir[SM] system, which is the control mechanism for associating log-ins, sites, users, etc. in Brivo's security model.

ACS
Access Control System, and electronic system for allowing or barring entry to a facility based on a credential held by a user.

AES
Advanced Encryption Standard, a reference to the Rijndael symmetric encryption algorithm, the recent winner of NIST's (National Institute of Standards and Technology) worldwide competition to develop a new encryption technique that can be used to protect computerized data; considered more secure than earlier standard such as 3DES. See http://csrc.nist.gov/encryption/aes/.

CDMA
Code Division Multiple Access, a digital radio system that underpins a mobile phone network standard developed by Qualcomm.

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, etc.

Control Panel
The hub of an access control system to which all other devices are connected.

Digital Certificate
An electronic document for uniquely identifying a party in a communications session, issued by a Certificate Authority.

DoS
Denial of Service, an attempt to slow down computers and networks to the point where they can longer perform their primary functions.

GSM
Global System for Mobile Communications, a standard set developed by the European Telecommunications Standards Institute (ETSI) to describe protocols for second generation (2G) digital cellular networks used by mobile phones.

HTTPS
Hypertext Transfer Protocol Secure, a communications protocol for secure communication over a computer network, especially wide deployment on the Internet.

Glossary

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, a federal technology agency that works with industries to develop and apply technology, measurements and standards.

Reader

One of several types of devices mounted at the facility entrance which serves as an input device for credentials such as proximity cards, smart cards, PIN codes, biometrics, etc.

SSL

Secure Sockets Layer, a protocol that provides a framework for authenticating and encrypting communications sessions.