ClickShare Security Whitepaper

DATE 27/03/2019

AUTHOR Filip Louwet | David Martens | Jef Neefs | Hanne Page | Hans Mortier | Adrien Decostre | Kristof Demeyere | Lieven Bertier | Willem Van Iseghem | Michael Vanderheeren | Karel Paternoster

Table of content

Introduction

ClickShare was introduced in 2012. In 2016, four years after the introduction, a new generation of ClickShare Enterprise products was presented to the market. New design, better performance, enterprise integration and built-in, configurable security are key features of this new generation, code-named CS(E)-xxx. At the beginning of 2019, another two products were added to the CS(E)-xxx range, with ClickShare now offering a broad portfolio in terms of functionality and features.

The increasing amount of cyber-threats and professional espionage on the one hand and the increased focus on information security from professional organizations on the other hand have been driving forces to make security a key feature of the CS(E)-xxx range.

Security and usability have always been difficult to balance in product development and user experience design. Increased security often results in poorer usability, while too much focus on usability will deliver a great experience with potential security holes. The exercise to find a perfect balance between the two is a challenging one and needs to be tackled from the first stages of product design onwards.

Already from the early beginning when the architecture of the next generation ClickShare solution was on the drawing table, security has been taken into account as a top priority. The envisioned embedded nature of the ClickShare components adds an extra degree of difficulty to integrate security, as less computational power seems contradictory to more security. However, Barco's engineers and product managers investigated and discussed security at length during design and development, resulting in a secure, but at the same time very user-friendly collaboration system. Moreover, focusing on security from the initial steps of the project ensures that customers and users of ClickShare are protected against malware, hackers and eavesdroppers.

This technical white paper will go in depth on the possible threats for different components and features, and the measures that have been taken to mitigate these. The white paper applies to the second ClickShare generation (CS-100 Huddle, CS-100, CSE-200, CSE-200+, CSE-800. The security aspects related to the eXperience Management Suite (XMS) as well as XMS Cloud are discussed in the XMS Security Whitepaper.

Barco obtained the ISO 27001:2013 certification at the beginning of 2019. The scope of the certification is restricted to the business processes and infrastructure that relate to the software development, sales, deployment and support of the wireless collaboration (ClickShare) product line. This proves that Barco is not only concerned about security on a product technical level, but also aims to consistently improve information security management of all processes involved in the deployment of ClickShare. Barco engaged in the thorough procedure of getting ISO certification for its processes as a whole, aiming to confirm its leading market position in terms of security in the market of wireless collaboration technology.

Given the increased focus on privacy, Barco moreover follows the privacy by design principle. Within the ClickShare product line, personal data (IP, username, MAC addresses) is not stored in any way (log files or persistant memory), nor transferred outside the ClickShare solution. ClickShare users can thus be assured their personal data is not used/distributed.

Modelling the ClickShare threats

Over the last couple of years, Barco noticed an increase of market questions and requests concerning security, user scenarios, integration methods, etc. With all those topics in mind, **extensive threat modelling** has been applied during design and development phases of the second generation ClickShare system.

Threat modelling is one of the most powerful security engineering activities since it focuses on vulnerabilities as well as actual threats. A threat is defined as an external event that can damage or compromise an asset or objective, whereas a vulnerability is a weakness within a system that makes an exploit possible. Vulnerabilities can and should be solved, but threats can live on indefinitely or change over time and cannot be controlled by the people managing or using the device or system. Threat modelling facilitates a risk-based product development approach by uncovering external risks and encouraging the use of secure design and development practices. Threat modelling therefore not only needs to focus on software, but also hardware and even production related topics need to be covered to create a secure product in every aspect.

What does the system look like?

Barco's ClickShare collaboration system gets all meeting participants involved by giving everybody the opportunity to share content on screen at the click of a Button, both for empoyees and guest users. Whether you are using a laptop PC, Mac, iPad, iPhone or Android-powered device, you are able to present your content on the central meeting room screen in the most simple and intuitive way possible.

Following components can be identified in a ClickShare collaboration system:

- **Base Unit**: Although not always visible, the Base Unit is the heart of the ClickShare system. This processing unit receives the wireless stream from the Buttons,ClickShare App or mobile devices and ensures it gets displayed correctly on the display.

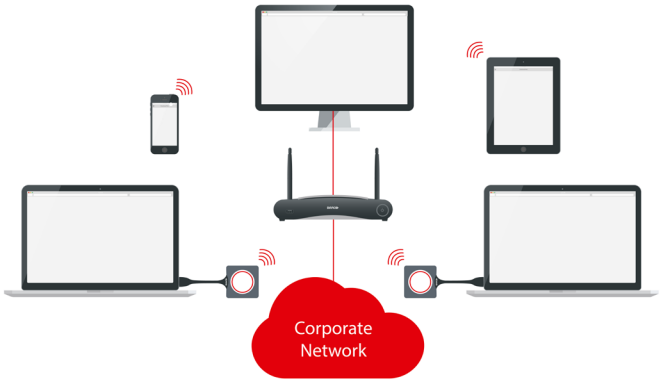
- **Button**: The ClickShare Button is a USB-powered device that announces itself both as external read-only mass storage device (containing the client application) and as audio capable device. Simply connect it to your laptop's USB port, start the application and click the Button – your laptop's screen content and optionally its audio is transferred instantly to the large meeting room screen display and speakers attached to the Base Unit. On the CSE-200, CSE-200+ and CSE-800 Base Units, the button allows touch back functionality with compatible touch screens.

- **Software client**: The application is running on your laptop PC or Mac and gathers the screen content to send it via the Button to the Base Unit. On the CSE-800 the client allows a user to moderate the ClickShare composition on screen. On the CSE-800 and CSE-200+, the client allows to receive and distribute the resulting files from blackboarding/annotation sessions from the Base Unit.

- **ClickShare App** for Windows and Mac: At the beginning of 2019, the ClickShare App was introduced, providing the option to share laptop content without the use of a physical Button, instead making use of a software application. Barco aims to offer the same user-friendly experience as with the Button on the ClickShare App, at the same time offering additional

functionalities and features. The ClickShare app can be used as stand-alone application or in combination with the ClickShare Button.

- **Mobile Apps** (iOS, Android): The ClickShare App on your Android tablet, smartphone, iPad or iPhone which enables you to share documents, photos and other screen content on the display attached to the Base Unit.
- **AirPlay**: The AirPlay protocol allows wireless streaming of audio and video from compatible Apple devices. ClickShare supports AirPlay streaming as well as AirPlay mirroring.
- **Google Cast**: The Google Cast protocol allows wireless streaming of video from supported devices (Android, Chrome browser).



What data needs to be protected?

Not only all data that is transferred via the ClickShare collaboration system must be protected, but also the data that is stored on devices participating in a ClickShare session. When users want to share data on the display and audio on the speakers attached to the Base Unit, only attendees of the meeting should be able to see and hear the content. Other data/audio may never be accessed and/or transferred, so the user remains in full control and responsibility of which data and/or audio is shared. When using ClickShare, people must be assured that they run original Barco software, so that they know their device will not be compromised or infected with malware when plugging in a Button or installing the app. In a board room, the contents of a display are often highly confidential. As a consequence the system handling the content must assure the **confidentiality, integrity and availability** of this data.

The ClickShare content is delivered in real-time and is never stored on non-volatile memory in one of the ClickShare components.

What physical system interfaces and services can be detected?

	Base Unit	Button
		

Externally accessible	• **USB**[1]
	  ○ Bootloader access/Linux CLI access
	• **Ethernet**
	  ○ Web UI
	  ○ REST API
	  ○ Communication with Client and desktop/mobile Apps
	  ○ AirPlay
	  ○ Google Cast
	• **Wi-Fi**
	  ○ Web UI
	  ○ REST API
	  ○ Communication with Client and desktop/mobile Apps
	  ○ AirPlay
	  ○ Google Cast
		• **USB**[2]
		  ○ Communication with Client/Base Unit
		• **Wi-Fi**
		  ○ Communication with Base Unit

Internally accessible	• **Serial**
	  ○ Bootloader access/Linux CLI access
	• **JTAG**
	  ○ Flash access
		• **Serial**
		  ○ Bootloader access/Linux CLI access

Where is the system physically located?

The Base Unit will primarily be found in a professional environment. It is recommended to connect the Base Unit to a "trusted" corporate network via the Ethernet interface[3], although scenarios are known where ClickShare is used in a standalone or ad hoc mode. Nevertheless, data which is handled by the system can be highly confidential and must be protected as such. The range of the built-in wireless interface will exceed the physical boundaries of the meeting room and maybe even those of the corporate building. Therefore access to the Wi-Fi and Ethernet interfaces of the Base Unit must be protected in an appropriate way.

[1] The CSE-200+ offers a USB-C connection on the back panel, all other USB ports are USB-A.

[2] The CS-100, CSE-200, CSE-200+ and CSE-800 units come pre-packaged with USB-A buttons (resp. 1, 2, 2 and 4), whereas the CS-100 Huddle has no buttons included in the box. Both USB-A and USB-C buttons can be ordered separately and are compatible with all Base Units.

[3] On the CSE-200+, Wireless Client Mode will be made available in the course of 2019, allowing to connect the Base Unit to the network via the built-in Wi-Fi module.

Who is using and who is managing the system?

In a professional environment most users will be employees of the company, but during meetings with customers, suppliers, etc., external people (guests) might also participate and make use of the same ClickShare collaboration system. This means that a range of **different devices** are connected to the same system, bringing along potential security risks. This emphasizes once more the importance of only sharing content with people attending the meeting and ensuring that only data is shared that the user explicitly has given access to by clicking the Button, using the ClickShare App or via Airplay or Google Cast.

Configuration of the ClickShare systems in a professional environment is primarily managed by IT departments or facility management teams. They assist employees in making use of all facilities the company offers, in the best way possible. The ClickShare Enterprise range of collaboration systems introduces several levels of security. Switching between different **security levels** can be managed through the ClickShare Configurator of the Base Unit, which clearly mentions the consequences of changing to a certain security level. Choosing the right security level will depend on an internal company risk analysis and compatibility needs.

Technical implementation

Layered approach

The cornerstone principle of information security is the **CIA triad**: Confidentiality, Integrity, and Availability. All parts of a product or system must honour this concept throughout the system's life cycle to guarantee a secure environment.

Before dealing with the technical implementation related to security of ClickShare, it is important to emphasize that the use of **Wi-Fi communication** renders the availability corner of the CIA triad very fuzzy. Every source of interference in the vicinity of a wireless system can — intentionally or unintentionally — cause that system to function incorrectly and thus be unavailable. It is strongly advised to use professional Wi-Fi integrators for the analysis, planning, and deployment of large installations. In that way at least unintentional interference can be eliminated. The proper functioning of a ClickShare system starts with an environment suffering from a minimum of interference.

A network connected system can be divided into **different layers**: physical, network, host, and application layer. Mapping these four layers onto the CIA triad will reveal how security is implemented in a system and reveal where safeguards are missing. The layered approach and the implementation of multiple safeguards to protect a system will ensure that in case one safeguard fails, another safeguard prevents compromising the system. The safeguards must correspond to and mitigate the threats identified in the threat modelling.

Background information

Identification and authentication steps during set-up of a communication channel are crucial to trust the other side, encrypt transferred data and prevent alteration of data during transfer.

The ClickShare Base Units and Buttons contain a **device certificate**, which is provisioned during production of the devices and is stored in encrypted format in non-erasable memory on the device. A Public Key Infrastructure (PKI) has been set up to generate device certificates and guarantee a chain of trust during authentication between ClickShare devices. Every device gets a unique certificate with a private/public key pair based on elliptic curve technology (sect283k1, NIST/SECG curve over 283 bit binary field) and which is signed based on ECDSA. This device certificate is created and signed by a Barco Certification Authority, is not renewable and not revocable.

Not all ClickShare devices are connected to the Internet, which makes a device certificate management with revocation strategy almost superfluous and utterly complex, which is contradictory to the ease of use of ClickShare. To lower the risk to an acceptable level, **additional mitigation actions** have been implemented. The PKI infrastructure is hosted on internal premises, physically decoupled from the corporate network and situated in a restricted area with physical access control. Transfer of device certificates between Barco and production locations happens over an IPsec tunnel in an encrypted container and additionally the private key is stored in encrypted format on the device.

Physical layer

Embedded devices are easy to steal due to their small physical size and a malicious hacker could easily gain access to the physical interfaces with the intent to reverse engineer the firmware and load malicious malware on the device. Protecting the physical interfaces of embedded devices is as important as protecting the other layers of the system.

Both connectors of the **serial and JTAG interface** of the **Base Unit** have not been populated on PCBA of deployment units. Input on serial interface is disabled from bootloader level onwards and the JTAG interface is secured with a secret response key. The key is stored in one-time programmable memory, read or write access to the key is prevented via hardware lock.

Connecting a Button to the **Base Unit** via **USB** starts a pairing process where the Base Unit will share all parameters with the Button to be able to access the Wi-Fi of the Base Unit (in case the Button connects to the AP in the Base Unit; out-of-the-box use and network connected mode) or the corporate Wi-Fi (in case the Button connects to the APs of the corporate network; network integrated mode). It will also upgrade the button to the most recent firmware if available. The Base Unit will only interact over USB with a ClickShare Button if mutual authentication using both device certificates is successful. This means that first generation buttons cannot pair or update unless the lowest security level is configured.

Regular USB devices can also be connected to the Base Unit. When an external storage device is connected via USB, the top directory will be scanned for a firmware update image. If this file is found, the Base Unit will attempt to upgrade. This upgrade can only be successful if the firmware is correctly encrypted and signed, otherwise it is aborted. In all other cases, connecting USB devices will result in no action.

Similar to the Base Unit, the **serial connector** on the PCBA of the **Button** is left unpopulated. From bootloader level onwards the input of serial interface has been disabled as well.

A connected **Button** (via **USB** to a laptop PC or Mac) announces itself as:

- A USB Human interface device (HID) which will communicate with the ClickShare software Client;
- An Audio device which captures the audio and transfers it to the Base Unit;
- A read-only mass-storage device containing the ClickShare Client executable both for Windows and Mac.

Access to the **Ethernet interface** allows to connect to the network stack and services running on the Base Unit, therefore additional authentication, confidentiality and integrity controls at application layer are necessary. These controls are present for both Ethernet and wireless connections. Depending on the network setup, Wi-Fi has additional security controls at the network layer which is not always the case for the Ethernet interface in the ClickShare system. The Base Unit acts as Wi-Fi access point, while the Buttons connect as stations. Any device with access to the Wi-Fi can interact with the other Buttons connected to the Base Unit, causing a need for additional authentication, confidentiality and integrity controls at application layer on the Button. In following sections, these controls are explained.

Network layer

The **wireless interface** of the Base Unit is default protected with WPA2-PSK, a method for securing the Wi-Fi (Wi-Fi Protected Access 2) with the use of a Pre-Shared Key (PSK) authentication. WPA2-PSK encryption ensures the confidentiality and integrity of all data passing through the wireless channel. Confidentiality is provided by the AES block cipher with a 128-bit key length. Integrity is provided by using the Counter Mode CBC-MAC Protocol (CCMP) to create a Message Integrity Check (MIC). Using the WPA2-PSK passphrase and SSID, both of which can be configured by the administrator in the ClickShare Configurator, a set of temporary keys is derived that are used for authentication (CCMP) and encryption (AES), in accordance with the IEEE 802.11i security standard. The Base Unit can be configured to hide the SSID of its Wi-Fi interface. It should be noted that SSID cloaking can provide a false sense of security. Using tools freely available on the Web, it is fairly easy to scan an area for hidden networks.

Like aforementioned the **Ethernet interface** does not contain any security controls by default. Experiences with set-ups at corporate customers show that frequently, ClickShare systems are grouped in separate VLANs with additional access controls to separate them from the corporate data network (dedicated network integration mode). It is however possible to activate 802.1x authentication for the Base Unit, which is listed as "Wired Authentication" on the ClickShare Configurator. With this mode enabled, the Base Unit will authenticate itself on the Ethernet interface using PEAP, EAP-TLS or EAP-TTLS. This ensures that a Base Unit can also connect to corporate networks where devices need to be authenticated in order to gain access.

The **Wi-Fi and Ethernet are strictly separated**, not a single packet is forwarded between both interfaces, the Base Unit is the endpoint for all traffic. This separation is ensured by the firewall which is present on the Base Unit and has been verified by penetration tests executed by a third party. Both interfaces work solely on IPv4 based traffic. Also in Dual Network setup (CSE-800 and CSE-200+[4]), there is a strict separation between the two network interfaces, without bridging the two data streams.

OS layer

Both Base Unit and Button run an **embedded Linux OS**. They are upgradeable through a monolithic firmware image, which is periodically released by Barco. The Base Unit can be upgraded either manually via uploading the firmware image in the ClickShare Configurator or through the Auto Update feature. The Auto Update feature uses a secure connection to a Barco server to obtain and install new firmware at the time it becomes available. Buttons are upgraded automatically when a more recent firmware is available on the Base Unit. This either happens when pairing a Button with the Base Unit via USB (both USB-A and USB-C buttons are available), or in the background over Wi-Fi when plugged-in into a laptop. Upgrading and pairing multiple buttons at a time can be performed using the ClickShare Button Manager (free download for Windows 7 & 10), which pairs up to four buttons to the selected meeting room. The Button Manager uses the same secure method to pair a Button, as if it were plugged into the Base Unit.

[4] The CSE200+ will be able to connect to two different networks, one via an Ethernet cable and another via Wi-Fi. The CSE-200+ will also be able to connect solely via its wireless interface to a network of choice (Wireless Client Mode), without needing an Ethernet cable for network integration. Both functionalities will become available in the course of 2019 for the CSE200+.

To assure a failsafe upgrade mechanism a **double copy strategy** has been implemented on the **Base Unit**. A Base Unit contains a primary storage partition, with the current firmware, and a secondary partition for upgrade purposes. After validation of the signature, and checking on the encryption, the new firmware version will be written to the secondary partition. After a reboot, the new firmware will be started by switching the primary and secondary partition. In case a failure to boot happens, the device will automatically revert back to the old firmware.

Firmware signing and encryption assures integrity and confidentiality of the software running on the Base Unit. It guarantees the customer that the firmware is originally created by Barco, that it has not been tampered with and that a firmware image cannot be reverse engineered. The firmware image consists of three parts: bootloader, kernel and root filesystem. Bootloader and kernel are signed, but not encrypted, the root filesystem is encrypted but not signed. The integrity check starts from bootloader level onwards and is locked to the hardware, the so-called secure boot. The keys to verify the signature of the different boot components (bootloader and kernel) have been written in encrypted format in one-time programmable memory at production and are not readable from OS level. During upgrade the root filesystem part of the upgrade image is decrypted and encrypted again with a different symmetric key when writing the filesystem to flash, the related symmetric keys have been written to flash in encrypted format at production and are only accessible via a device unique key which cannot be read from OS level. Copying the flash will not facilitate reverse engineering the ClickShare solution due to the encrypted filesystem on flash.

The **Button** follows the same **double copy upgrade strategy**, although both images are updated to the most recent version, and the root filesystem is not encrypted on flash. The firmware image of the Button is signed and encrypted, the integrity check also starts from bootloader level onwards and is locked to the hardware. Signing and encryption key material has been written in encrypted format to one-time programmable memory at production and is not readable or writable from OS level.

The Base Unit firmware contains a **watchdog** which monitors all important services. In case a monitored service crashes or hangs, the watchdog will restart it. This ensures a high availability of the Base Unit.

The embedded Linux OSes in Base Unit and Button contain multiple **open-source software packages**. A list of these packages is available in the End User License Agreement. Barco closely monitors new vulnerabilities detected in open-source packages embedded in our products. If a vulnerability is detected or reported, it will be analysed and depending on the criticality and impact, planned in for a future release.

Application layer

- Communication protocols

Out of the box, second generation ClickShare units (CS(E)-xxx range) are on security level 1 to ensure compatibility with the first generation of ClickShare products. Higher security levels do not support any interaction with components from the first generation ClickShare. Before diving into the details of the different security levels, an overview of the communication protocols is given.

Two different, proprietary protocols form the backbone of ClickShare: a protocol to communicate over USB and a protocol to communicate between sender and receiver at application level. Both protocols contain a control and a data plane. Protocols of the first generation do not support any form of authentication, encryption is only applied for screen content which is shared with a Button. Protocols of the second generation do support authentication with additional integrity checks and encryption to guarantee confidentiality.

USB protocol

- **Control plane**: Both ends (Base Unit and Button) must have access to a Barco device certificate and the corresponding private key. The key material available in the certificates is only used for authentication by verifying the digital signatures of both sides (ECDSA) and will not be used during key agreement. A separate ephemeral key agreement protocol (ECDHE) is used to derive a session key for the data plane, this session key will be different each time a new connection is set up.
- **Data Plane**: For encrypting data over USB, AES-256 in GCM mode is used, providing both confidentiality and integrity. The key used for this exchange is the derived session key from the key agreement protocol.

Application protocol

- **Control Plane**: All components will use the control plane to set-up a communication channel with the Base Unit. First a TLS v1.2 connection is created with server-side authentication, all client side components do have the Barco CA certificate to verify the Base Unit. Once the TLS connection is set up, an additional client authentication step is executed at application level depending on the component it is interacting with. Buttons will use their device certificate to authenticate, the Apps will use a 4-digit passcode[5], first generation Buttons won't be able to use client side authentication. The requested authentication mode is negotiated and depends on the configured security level at the Base Unit side. Only security level 1 will allow unauthenticated access from first generation Buttons, all higher levels require authenticated access.
- **Data Plane**: The screen content is transferred over TCP and confidentiality and integrity controls have been implemented at the application layer to protect this content. Salsa20 in combination with VMAC is used to obtain an authenticated encryption scheme. Salsa 20 is a stream cipher and VMAC is a block-cipher based message authentication code. Both require parameters that are known at sender and receiver side and these are shared via the control plane. The audio data is transferred in unencrypted format, though it is established via an authenticated and encrypted connection at control plane level.

- Security levels

Because the ClickShare use-cases are vast and large, the resulting security design to incorporate all those features is huge and very complicated. **Security levels** have been introduced to group these features in logical blocks. This approach makes a suitably secure configuration of the ClickShare collaboration system easier to manage. Each level is designed to be self-contained with regards to the features it provides, meaning that moving up our down in the security levels will change the capabilities of the ClickShare system.

[5] Support for passcodes is available for the CS(E)-xxx range from firmware release v01.03 onwards

The following statements describe how a security level change works:

- If the security level of a Base Unit is changed from 1 to 2 or 3, thereby altering Button compatibility, it must change its shared secret; which is used during client side authentication with device certificate; to a different pseudo random value. This requires re-pairing of all related Buttons.
- If a second-generation Button is paired with a second-generation Base Unit, it will automatically change its security level to that of the Base Unit (No levels are changed when paired with first generation Base Units).
  Two components should always use the protocol and authentication mode with the highest priority that its current security level allows it to use.

The following table gives a brief overview of the available security levels of all ClickShare components, both first and second generation:

Device / Service	Security Level 1	Security Level 2 & 3
Button R9861500D01 (included with CS(E)-xxx sets)	✓	✓
Button R9861006D01 (included with CSM-1 and CSC-1 sets)	✓	Not supported
CSC-1, CSM-1	✓	Not supported
CS(E)-xxx	✓	✓
Software Client	✓	✓
ClickShare App (pc/mac)	✓	Blocked
Mobile App (iOS & Android)	✓	Blocked

Three security levels have been defined:

Security Level 1 offers enterprise security, whilst maintaining compatibility with first generation ClickShare components and foresees following security features:

- Possibility to activate passcode for desktop app, mobile apps & Buttons[6]
- ClickShare Configurator: HTTPS, log-in session management, disable sharing with apps
- Hide SSID of the Wi-Fi network

Security Level 2 contains Security Level 1 features plus:

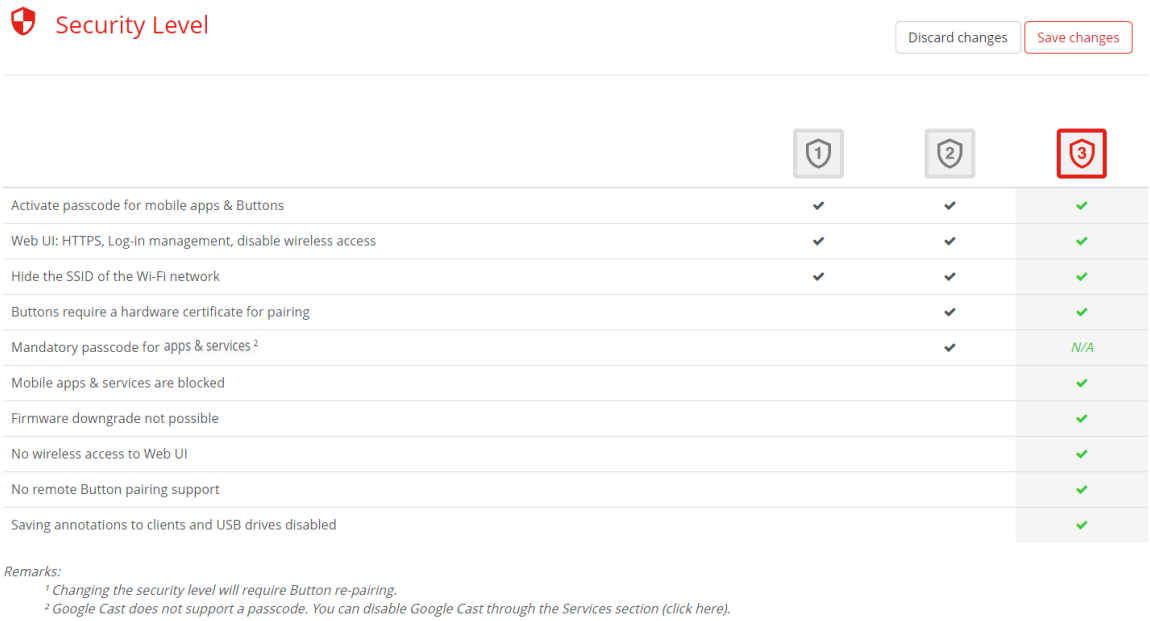
- Mandatory passcode for desktop and mobile apps
- Button hardware certificate required for pairing

[6] CSM-1 and CSC-1 models feature all level 1 security features except for passcode support

Security Level 3 contains Security Level 2 features plus:

- Desktop app and mobile apps are blocked
- Firmware downgrade not possible
- No access to ClickShare Configurator via Wi-Fi

The ClickShare Configurator allows to set the Security Level in a clear and easy way, as indicated in the screen capture below.



A **Base Unit can be configured** through the ClickShare Configurator or REST API. Both are only serviced via HTTPS to assure an authenticated and encrypted connection with the Base Unit. TLS cipher-suites and versions are configured to resist the latest known attacks. Access to both the ClickShare Configurator and REST API is protected via password credentials, and no data can be accessed without authentication.

The **ClickShare Configurator** login uses a session, bound to a cookie, that stays valid until logout or expiration. To assist users in selecting a strong and secure password, an indicator shows the password strength of the entered password. The passwords for the ClickShare Configurator are hashed using bcrypt, a widely used, secure hashing algorithm. Each password has its own unique salt, preventing rainbow table attacks.

The **REST API** is protected with Basic Authentication (over HTTPS). The password for the REST API is protected in a similar way to the ClickShare Configurator.

Furthermore, all inputs for both ClickShare Configurator and REST API are validated to prevent injection vulnerabilities.

By default the Base Unit will use a self-signed certificate for the TLS connections. If desired, this can be replaced by either a single-domain certificate or a wildcard certificate. Once applied, they will be used for both the ClickShare Configurator and the REST API.

- Client application

The only application running on the laptop PC or Mac when using a Button is the **ClickShare client software**. This piece of software is developed and maintained by Barco, and no external party has access to it. The executable is signed and timestamped, ensuring that no one has altered it and thus guaranteeing its integrity. The ClickShare code-signing certificate has been issued by GlobalSign, a WebTrust-certified certificate authority. The software is stored on the read-only mass storage device inside the ClickShare Button. This mass storage section can only be changed when updating the firmware of the button, which only happens during production, pairing or over-the-air upgrades as described in the OS Layer section. A user cannot write to this storage device, intentionally or unintentionally. The client software is a single execution binary, only affecting volatile RAM memory and CPU. The software does not require any special drivers to be installed on the laptop PC or Mac and does not install any drivers itself.

Optionally the ClickShare Extension Pack can be installed on the user's laptop. The Extension Pack contains a Launcher application, which will automatically launch the software client when a Button is connected, and a driver for enabling Extended Desktop support. The Launcher will only launch the client from mass storage if the PID/VID combination of the plugged-in USB device matches. It is also possible to deploy a client version, and let the Launcher start this version when a Button is plugged in. The Extension Pack can be installed ad hoc or deployed company-wide.

The Blackboarding and Annotation functionality on the CSE-200+ and CSE-800 allows to draw on compatible touch screens (either in blackboarding mode or on a presented slide), after which the created content can be distributed to connected devices. This saving will store the file to the connected users' devices (connected buttons and/or pc's connected with the Desktop App) or to USB flash storage devices plugged into the Base Unit. The files are stored in volatile memory on the Base Unit and are deleted after the sreen has been erased. The BlackBoarding and Annotation functionality can be disabled in the ClickShare Configurator.

- Desktop app

The **ClickShare App for Windows and Mac** is a software application designed, developed and maintained by Barco. It has been designed to bring the physical Button experience to a software interface. It can work in tandem with the Button or without the Button as stand-alone application. The ClickShare App can be downloaded from www.clickshare.app, a website which is maintained by Barco. The ClickShare App has an auto-update function which downloads and installs the most recent version from the Barco server. For content sharing the app will communicate with the Base Unit at application layer via the control plane over TLS with server-side authentication to set up a connection on the data plane and can be further secured with an on-screen passcode. The ClickShare App uses mDNS (multicast DNS) for advertisement and discovery, as well as SSDP (Simple Service Discovery Protocol). The ClickShare App can be installed ad hoc or deployed company-wide.

- Mobile apps

Both **iOS and Android apps** have been developed to share content on the display attached to the Base Unit. Please use the links on the Corporate Barco website or scan the QR code on the display of the Base Unit to download and install the Barco ClickShare apps. If the mobile device is connected to the Wi-Fi of the Base Unit, the app will identify the Base Unit via the Bonjour protocol. When connected to a corporate Wi-Fi access network, the IP address of the Ethernet interface of the Base Unit can be entered to start presenting screen content on the display. Apps will communicate with the Base Unit at application layer via the control plane over TLS with server-side authentication to set up a connection on the data plane to share content. Because of the contained approach in the security model of both iOS and Android, apps can only share content of documents or pictures, not the full screen. The mobile apps use mDNS (multicast DNS) for advertisement and discovery.

- AirPlay

AirPlay mirroring is supported on the Base Units without the need to connect an Apple TV device; it is fully integrated in the Base Unit firmware. Authentication is fully integrated via the same passcode which is also used for the Barco apps. Airplay uses an Apple proprietary mDNS (multicast DNS) protocol named Bonjour for advertisement and discovery.

AirPlay is a protocol designed, defined and developed by Apple. The application of the security standards upheld by Barco is therefore limited by the design and definition of the protocol. Support for AirPlay can be disabled in case the AirPlay protocol is not considered secure.

- Google Cast

Google Cast mirroring is supported on the Base Units without the need to connect a Chromecast device; it is fully integrated in the Base Unit firmware. However, Google Cast does not allow passcode verification within their protocol and therefore passcode support is not available. Google Cast uses mDNS (multicast DNS) for advertisement and discovery.

Google Cast is a protocol designed, defined and developed by Google. The application of the security standards upheld by Barco is therefore limited by the design and definition of the protocol. Support for Google Cast can be disabled in case the Google Cast protocol is not considered secure.

- Passcode

As described earlier, all components will use the control plane to set-up a communication channel with the Base Unit. The ClickShare Apps and AirPlay use a **passcode for an additional client authentication** step at application level when passcode authentication is enabled on the Base Unit. Every time such a Client connects to the Base Unit, a passcode will be generated by a random number generator in the Base Unit and be displayed in the top-right corner of the connected screen. This passcode is 4 digits long. When multiple users connect at the same time they can use the same passcode to authenticate their session. The displayed passcode remains valid while an authentication attempt is ongoing, and is refreshed on timeout or after a period of 10 minutes. The passcode will be invalidated and is removed from the screen once the user succeeds at authentication, or when the attempt times out.

Each time a user tries to connect through the ClickShare App or AirPlay, a pop-up will be generated on the screen with the passcode for authentication. Social observation should prevent unwanted users to connect to the Base Unit when trying to read the passcode on screen from outside the meeting room.

To prevent brute-force attempts an additional security measure has been implemented to block a user from attempting to enter a pin more than 5 times in a row. After these 5 failed attempts, that user's IP address will be blocked from connecting to the Base Unit for a period of 5 minutes.

- Logging

The ClickShare system contains an extensive **logging engine** based on rsyslog. No individual Button stores logs; rather, the Buttons forward all messages to the rsyslog server running on the Base Unit. The Base Unit also logs its own activities. The log files can be downloaded via the ClickShare Configurator by users with admin access. The data stored in the log files contains information about the current system state: component temperature, frame rate statistics, statistics on the wireless link quality, number of connected users, and so on. In any event, no data from the screen or audio capture and no passwords or any other confidential data is reproduced in the log files.

- Overview

Layer		Confidentiality	Integrity	Availability
Application	Audio	No encryption	No integrity check	-
	Screen	Salsa20 encryption	VMAC integrity check	-
	Control Plane	Control Plane: server authenticated TLS (ECDHE_ECDSA) with device certificate or pin authentication	Control Plane: server authenticated TLS (ECDHE_ECDSA) with device certificate or pin authentication	-
	Management	ClickShare Configurator or REST API: server authenticated TLS (RSA based), basic authentication for client	ClickShare Configurator or REST API: server authenticated TLS (RSA based), basic authentication for client	SSH disabled Input validation of ClickShare Configurator
Host		Base Unit: Encrypted rootfs on flash Encrypted rootfs in upgrade package Secure boot locked to hardware Button: Encrypted image (bootloader, kernel and rootfs) in upgrade package	Base Unit: Signed bootloader and kernel Secure boot locked to hardware Button: Signed image (bootloader, kernel and rootfs) in upgrade package	Base Unit: Firewall Button: Watchdog
Network		WPA2-PSK (CCMP to create Message Integrity Check)	WPA2-PSK (CCMP to create Message Integrity Check)	Interference and wireless hacking can cause unavailability
Physical		Secure JTAG	Secure JTAG	Access to serial input is blocked

Interoperability with first generation ClickShare products

To allow existing customers to extend their current ClickShare install base, CS(E)-xxx units can by default still interact with first generation ClickShare products[7], because they are at security level 1. Once security level is changed to level 2 or 3, compatibility with the first-generation products is broken due to lack of device certificates which makes authenticated communication impossible.

[7] Note however that the June 2019 Firmware release will drop support for the Wave I Button (R9861006D01) on CS(E)-xxx Base Units.

Closing

The second generation of ClickShare collaboration systems contains significant security improvements. Moreover, the CS€-xxx range of ClickShare offer best in class security, configurable in three levels of security. Next to the efforts spent on designing and implementing security features, Barco guarantees that no backdoors or hidden transfers have been implemented.

Should you have further questions, please let us know via clickshare@barco.com. To report any security vulnerability, please contact our product security incident response team via psirt@barco.com.