Security Whitepaper ClickShare Conference

DATE 23/03/2020

AUTHOR David Martens | Willem Van Iseghem

ENABLING BRIGHT OUTCOMES

BARCO

Executive summary

ClickShare Conference is the next generation ClickShare solutions which extends the current local sharing and collaboration capabilities with remote collaboration features by embracing traditional UC&C tools.

Digital transformation has made the traditional perimeter-based network defence obsolete. Employees and partners expect to be able to collaborate and access organizational resources from anywhere, on virtually any device, without impacting their productivity. The security perimeter now extends to SaaS applications used for business-critical processing, untrusted networks used by employees to access corporate resources while traveling, unmanaged devices used by your customers to collaborate and interact with, and IoT devices installed throughout the corporate environment and inside customer locations. The traditional perimeter-based security model belongs to the past and has shifted to a zero trust security model that more effectively adapts to the complexity of the modern environment, embraces the mobile workforce, and protects people, devices, applications, and data wherever they are located.

The new remote collaboration features in ClickShare Conference, by embracing the traditional UC&C tools, perfectly fit in this digital transformation evolution and the zero-trust security model. Integrating ClickShare Conference into a corporate environment might bring along risks, mitigating those risks is a shared responsibility between the customer and Barco. Throughout the development lifecycle security best practices and tooling are used to detect and mitigate security issues as soon as possible in the development lifecycle, the so-called Shift Left principle. Furthermore, Barco has processes in place to monitor and manage risks related to development, deployment, sales and service of ClickShare products and obtained ISO27001:2013 certification for this. Barco expects from customers to take their responsibility and configure the devices as secure as possible aligned with the risk appetite of the customer and to apply all firmware updates in a managed way to patch security vulnerabilities as soon as possible.

When designing innovative products and solutions a security risk is present both on the vendor as on the customer side. The intellectual property is costly, resource intensive and should therefore be well protected with the relevant security controls. The customer installing ClickShare Conference in their corporate network and the end customers that will finally use the products must be also be protected very well. ClickShare Conference contains security controls to prevent that someone with malicious intentions can get persistent access to a ClickShare device with the final goal to use it as a pivot point to further penetrate the customer's corporate network. The end customer, using the ClickShare Conference solution, must be sure that any shared data is not leaked to or altered by any non-authorized individual. The fact that ClickShare Conference is a solution with embedded, tangible components where people have physical access to, even puts security requirements on hardware component level.

With the increased market focus on privacy, the privacy aspects for ClickShare Conference have been considered from the early stages of the development lifecycle. This privacy-by-design principle aims to minimize or eliminate the amount of collected personal data (e.g. IP, username, MAC addresses). The ClickShare Conference product line does not store any personal data in any way (log files or persistent memory), nor that any of it is transferred outside of the ClickShare Conference ecosystem. ClickShare users can thus be assured their personal data is not used/distributed, aligned with GDPR regulation.

ENABLING BRIGHT OUTCOMES

BARCO

Table of content

ENABLING BRIGHT OUTCOMES

BARCO

Introduction

ClickShare was introduced in 2012, revolutionizing the collaboration market. In 2016 a second generation of ClickShare Enterprise followed which added enterprise security features. In 2020 the third generation of ClickShare products was presented to the market. This third generation includes all features of the second generation and brings a new design as well as an agnostic conferencing solution.

The ever increasing number of reported information security incidents make the need for a secure solution a baseline requirement rather than an option. Combining this baseline requirement of security with usability and user experience has always been a challenge. Increasing security can result in poorer usability while an exclusive focus on user experience and usablity can result in a poorly secured product. Finding a perfect balance between these three requires attention from the very start of a product lifecycle.

This technical white paper will cover the threat model for different components and features of the ClickShare Conference products. For information about the eXperience Management Suite (XMS) as well as XMS Coud, please refer to the XMS Security Whitepaper, which can be found onthe Barco website[1].

The ClickShare development teams follow the Software Development Life Cycle (SDLC) process, and during the initial stages of this process the security aspect of the ClickShare solution was already accounted for and given top priority. This focus on security ensures that the final product is a very user-friendly collaboration system that is protecting users of the system against malware, corporate espionage and hackers at the same time.

Another important aspect that was taken into account from the early stages of the SDLC process is the privacy-by-design principle which aims to minimize or eliminate the amount of collected personal data (e.g. IP, username, MAC addresses). Barco can proudly state that the ClickShare product line does not store any personal data in any way (log files or persistent memory), nor that any of it is transferred outside of the ClickShare ecosystem. ClickShare users can thus be assured their personal data is not used/distributed.

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 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 and conferencing technology.

---

[1] https://www.barco.com/en/support/docs/TDE9786

BARCO

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 third 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 Conference 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, guest users and remote participants. Whether you are using a laptop PC, Mac, iPad, iPhone or Android-powered device, you are able to present your content in the most simple and intuitive way possible, both locally and using conferencing programs.

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. It can also pass back data streams from connected conference peripherals for usage in a conference call.

- **Button**: The ClickShare Button is a USB-powered device that announces itself as a CD-ROM drive (containing the client application), as speakerphone and/or as webcam. Simply connect it to your laptop's USB port, start the application and click the Button. Depending on the model of the Base Unit, the button enables additional features.

- **ClickShare Desktop App** for Windows and Mac: The ClickShare Desktop App is the universal client that comes on a Button, or that can be pre-installed on a user's laptop. It provides the option to share laptop content without the use of a physical Button. For conferencing functionality a Button is still required.

- **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.

- **External protocol integration:**

  - **AirPlay**: The AirPlay protocol allows wireless streaming of audio and video from

compatible Apple devices. ClickShare supports AirPlay streaming as well as AirPlay mirroring. Has support for a pincode for improved security.

- **Google Cast**: The Google Cast protocol allows wireless streaming of video from supported devices (Android, Chrome browser). Does not support a pincode.

- **Miracast**: The Miracast protocol allows wireless streaming of video from supported devices (Windows, Android). Does not support a pincode.
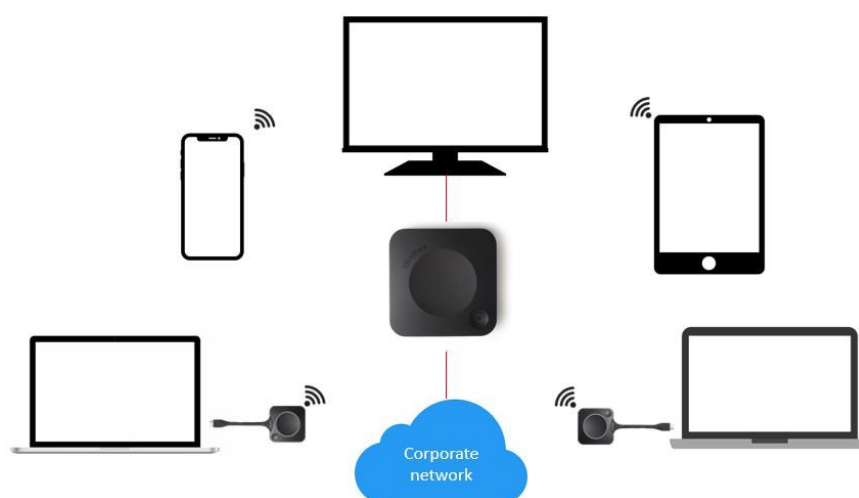
What data needs to be protected?

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 in the meeting room or with remote participants, only invited attendees of the meeting should be able to see and hear the content. Other data/video/audio may never be accessed and/or transferred, so the user remains in full control and responsibility of which data, video 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 running the provided software. Finally, 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.

BARCO

What physical system interfaces and services can be detected?

Base Unit	Button

Externally accessible

- **USB**
  - Communication with Button
  - Communication with conference peripherals
- **Ethernet / Wi-Fi**
  - XMS (Edge)
  - Web UI
  - REST API
  - Communication with ClickShare App and mobile Apps
  - Communication with AirPlay, Google Cast, Miracast

- **USB**
  - Communication with Client/Base Unit
  - Pass-through of Base Unit connected peripherals
- **Wi-Fi**
  - Communication with Base Unit (direct, or using corporate network)

Internally accessible

- **Serial**
  - Bootloader access/Linux CLI access
- **JTAG**
  - Access to internal components

- **JTAG**
  - Access to internal components

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[2], 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.

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 and conferencing system. This means that a range of different devices are connected to the same system, bringing along potential security risks. This

---

[2] On the CX-50, CX-30 and CX-20, Wireless Client Mode will be made available in the course of 2020, allowing to connect the Base Unit to the network via the built-in Wi-Fi module.

ENABLING BRIGHT OUTCOMES

BARCO

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, Google Cast or Miracast.

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 Conference range of 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 manufacturing 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 (secp256r1, NIST/SECG curve over 256 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.

ENABLING BRIGHT OUTCOMES

BARCO

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. In the event a device certificate would leak, the firmware contains a mechanism to blacklist these certificates, rendering them useless for updated devices.

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. This concern is taken into account from the very first phases of the project, but it needs to be noted that Barco also depends on the hardware features which third-party suppliers provide.

To protect against physical theft a Kensington lock can be connected to the Base Unit, while the ClickShare Button contains a loop hole for a cable to be connected.

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 or completely disabled. 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.

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.

If the USB device is a camera or other meeting room peripheral, the device will be detected by the Base Unit and an appropriate action depending on the type of peripheral will be undertaken.

Similar to the Base Unit, the **JTAG connector** on the PCBA of the **Button** is left unpopulated. At manufacturing the JTAG connector interface is permanently disabled by blowing the related efuses.

ENABLING BRIGHT OUTCOMES

BARCO

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 (loudspeaker) which captures the audio on the laptop and transfers it to the Base Unit;
- A read-only CD-ROM drive containing the ClickShare App both for Windows and Mac;
- A vendor-specific interface to trigger the installation of a driver that will automatically launch the App upon further use of the Button;
- A camera peripheral (if attached to the Base Unit) that can be used as camera input for a conference program;
- A speakerphone peripheral (if attached to the Base Unit) that can be used as both speaker and microphone for a conference program;

The listed USB interfaces above that forward peripherals are strictly checked and will only be forwarded if they are conforming with the expected output to prevent malicious content (such as a keyboard or mouse) to be transferred unchecked.

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.

ENABLING BRIGHT OUTCOMES

BARCO

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 (often referred to as "Air Gap"). 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 (please refer to the chapter Testing, validation and responsible disclosure). Both interfaces work solely on IPv4 based traffic.

OS layer

The Base Unit runs 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, through the Auto Update feature or via XMS. The Auto Update feature uses a secure connection to a public Barco service to obtain and install new firmware at the time it becomes available.

The Button runs a **Real Time OS (RTOS)**. They are upgradeable through a monolithic firmware image, which is periodically released by Barco. 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, or in the background over Wi-Fi when plugged-in into a laptop.

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 and 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 encrypted on the storage. 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

ENABLING BRIGHT OUTCOMES

BARCO

monitored service crashes or hangs, the watchdog will restart it. This ensures a high availability of the Base Unit.

The embedded Linux OS on the Base Unit contains 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 surfaces it will be analysed and depending on the criticality and impact, planned in for a future release.
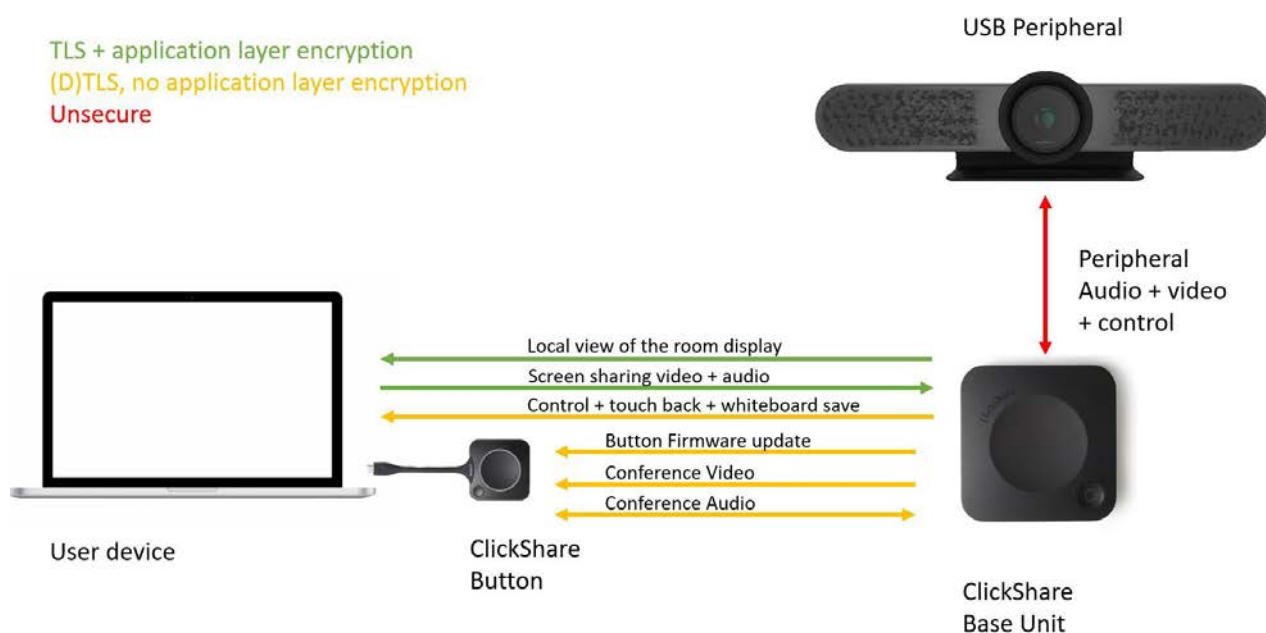
Application layer

- Cloud connectivity

During first installation the ClickShare Conference Base Unit can register itself to the Barco XMS Cloud, identifying itself via its unique device certificate, which was described in more detail in a former paragraph. The connection with XMS Cloud relies on a mutually authenticated TLS connection, configured with industry best practices. Registering the device to XMS Cloud will provide additonal advantages for more transparent management of your ClickShare Conference install base and 5 years of service coverage. For information about the eXperience Management Suite (XMS) as well as XMS Coud, please refer to the XMS Security Whitepaper, which can be retrieved from the Barco website[3].

- Communication protocols

Third generation ClickShare Base Units (C 3010S and C 5010S) are **not** compatible with any previous ClickShare Buttons. Similarly, the Button (R9861600D01C) is not compatible with previous generations of the Base Unit.

Before diving into the details of the different security levels, an overview of the communication protocols is given.

---

[3] https://www.barco.com/en/support/docs/TDE9786

ENABLING BRIGHT OUTCOMES

BARCO

TLS + application layer encryption
(D)TLS, no application layer encryption
Unsecure

An overview of all used ports for the different functionality that ClickShare offers can be found in the Network Integration whitepaper, downloadable on the Barco website[4].

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 third 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

---

[4] https://www.barco.com/en/support/docs/TDE9786

ENABLING BRIGHT OUTCOMES

BARCO

authenticate, the Apps will use a 4-digit passcode. The requested authentication mode is negotiated and depends on the configured security level at the Base Unit side.

- **Data Plane**: The screen content and audio are 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. Salsa20 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 conference peripherals that are sent from the Base Unit to the user via the Button are also secured with the same mechanism over the TLS connection.

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.

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.
  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:

Device / Service	Security Level 1 & 2	Security Level 3
ClickShare App using Button (pc/mac)	✓	✓
ClickShare Desktop App (pc/mac)	✓	✓
Mobile App (iOS & Android)	✓	✓
ChromeCast, AirPlay and other BYOD services	✓	Blocked

Three security levels have been defined:

Security Level 1 offers enterprise security and foresees following security features:

- Possibility to deactivate passcode for desktop and mobile app, as well as BYOD services
- 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:

ENABLING BRIGHT OUTCOMES

BARCO

- Mandatory passcode for desktop and mobile apps
- Mandatory passcode for BYOD services (in case the protocol supports it)

Security Level 3 contains Security Level 2 features plus:

- Consumer grade BYOD services such as Airplay, Google Cast and Miracast 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.

Security Level

	1	2	3
Activate passcode for mobile apps & Buttons	✔	✔	✔
ClickShare Configurator: HTTPS, Log-in management, disable wireless access	✔	✔	✔
Hide the SSID of the Wi-Fi network	✔	✔	✔
Mandatory passcode for mobile apps & services		✔	✔
BYOD services and features are blocked			✔
Firmware downgrade not possible			✔
No wireless access to ClickShare Configurator			✔

Remarks:
 [1] Changing the security level will require Button re-pairing.

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 password for the ClickShare Configurator is hashed using bcrypt, a widely used, secure hashing algorithm. The 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 the same as the one from the ClickShare Configurator, hence also protected.

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.

ENABLING BRIGHT OUTCOMES

BARCO

- ClickShare Desktop App

The only application running on the laptop PC or Mac when using a Button is the **ClickShare Desktop App**. The ClickShare App can be installed ad hoc or deployed company-wide.

The ClickShare App is developed and maintained by Barco, and no external party has access to it. It is a single execution binary which only affects volatile RAM and CPU. 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 App does not require any special drivers to be installed on the laptop PC or Mac and does not install any drivers itself. For the extended desktop feature, a driver might be required on Windows 10. Please refer to the Extension Pack explanation below for more information on this.

The software is either stored on the read-only CD-ROM device that is presented by the ClickShare Button or retrieved from the official clickshare.app[5] website. The CD-ROM device image 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 - intentionally or unintentionally - write to this device. When installed on a user's device, the ClickShare App has an auto-update function which downloads and installs the most recent version from the Barco server.

When used without a Button, the ClickShare App uses mDNS (multicast DNS) for advertisement and discovery, as well as SSDP (Simple Service Discovery Protocol) and Wi-Fi triangulation to provide a list of available ClickShare Conference systems.

- ClickShare Driver for Windows

The Button, upon first plug in on a Windows machine, will attempt to install a small, WHQL certified driver to automatically launch the App whenever the Button is plugged in next time. This driver gets a notification from Windows whenever a Button was plugged in. It will start a service that will validate and start the App. This service only runs when the Button is plugged in, and terminates when the Button is unplugged. As such this driver (and service) are resource-friendly and not consuming power when there's no Button plugged in.

- ClickShare Extension Pack

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 Extension Pack can be installed ad hoc or deployed company-wide. The Launcher will only launch the App from the CD-ROM drive if the PID/VID combination of the plugged in USB device matches. It is also possible to deploy a client version to end-user devices and let the Launcher start the deployed version when a Button is plugged in.

---

[5] https://www.clickshare.app

ENABLING BRIGHT OUTCOMES

BARCO

- 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. If the mobile device is connected to the Wi-Fi of the Base Unit, the app will identify the Base Unit via mDNS. 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.

- 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.

The ports that AirPlay uses are listed in the Network Integration whitepaper, which can be found on the Barco website[4].

- 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 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.

The ports that Google Cast uses are listed in the Network Integration whitepaper, which can be found on the Barco website[4].

- Miracast

Miracast streaming is supported on the Base Units and is fully integrated within the Base Unit firmware, requiring no additional devices. It does not allow passcode verification however, therefore passcode support is not available.

The Miracast protocol is designed, defined and developed by the Wi-Fi Alliance. The application of the security standards upheld by Barco is therefore limited by the design and definition of the

ENABLING BRIGHT OUTCOMES

BARCO

protocol. Support for Miracast can be disabled in case the protocol is not considered secure.

 The ports that Miracast uses are listed in the Network Integration whitepaper, which can be found on the Barco website[4].

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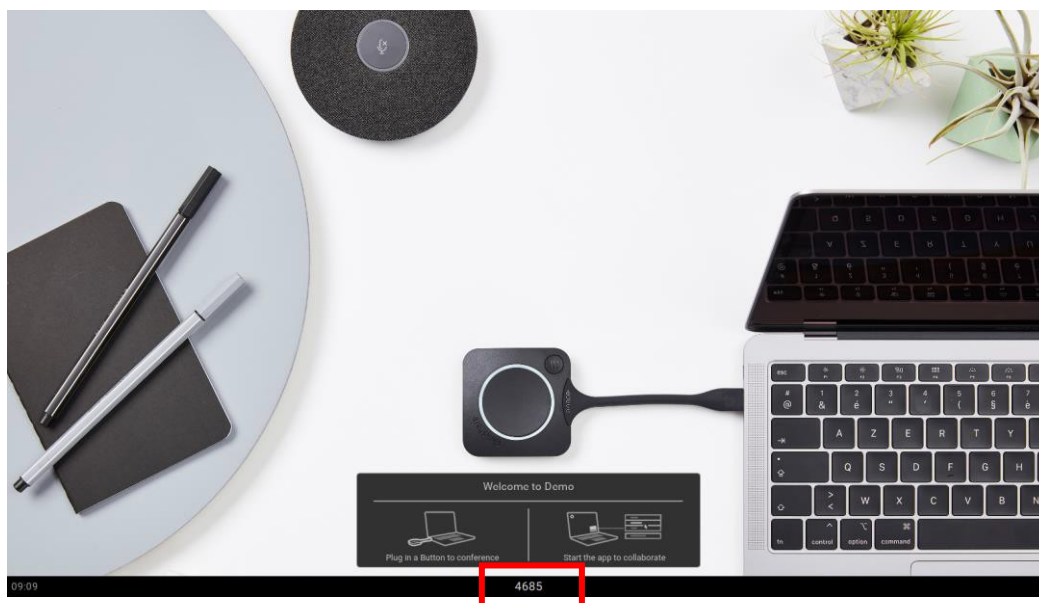
To prevent brute-force attempts an additional security measure has been implemented to block a user from attempting to enter a pin more than 5 times in a row. After these 5 failed attempts, that user's IP address will be blocked from connecting to the Base Unit for a period of 5 minutes.

•   Local View

The Local View option allows a connected user (through the ClickShare Button) to view the contents of the room display in a secure manner. To indicate that this feature is being used, a

small eye is shown in the bottom left corner of the screen.

- 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 Base Unit overs a secure TLS connection. The Base Unit also logs its own activities. The log files can be downloaded via the ClickShare Configurator by users with administrative 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.

ENABLING BRIGHT OUTCOMES

BARCO

- Overview

Layer		Confidentiality	Integrity	Availability
Application	Audio / Screen	Salsa20 encryption	VMAC integrity check	-
	Room peripherals	server authenticated TLS (ECDHE_ECDSA) with device certificate	server authenticated TLS (ECDHE_ECDSA) with device certificate	-
	Control Plane	server authenticated TLS (ECDHE_ECDSA) with device certificate or pin authentication	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 on ClickShare Configurator and REST API
Host		Base Unit: - Encrypted rootfs on flash - Encrypted rootfs in upgrade package - Secure boot locked to hardware Button: - Secure boot locked to hardware - Encrypted image in upgrade package	Base Unit: - Signed bootloader and kernel - Secure boot locked to hardware Button: - Signed image in upgrade package	Base Unit: - Firewall
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		Disabled / Secure JTAG	Disabled / Secure JTAG	Access to serial input is blocked

Testing, validation and responsible disclosure

It is not enough to only think about possible risks and ensure that they are brought down to a manageable risk or even eliminated entirely. These technical implementations above also need to be verified that they work as intended.

For the validation of these Barco makes use of both internal and external tools and partners. These validation methods can be either white-box (where the actual source code can be examined, architecture details are available and so on) or black-box (where only the device and the public interfaces are known).

ENABLING BRIGHT OUTCOMES

BARCO

Internal validation

Before a software update for a ClickShare product is released, various quality control gates must be passed. These encompass peer review, automated code quality scans, software composition analysis, vulnerability scans and are mostly white-box.

External validation

External validation is mostly done in the form of black-box assignments, where an external company sanctioned by Barco tries to circumvent the various implemented protections. In general, this is done before a product is released to the market, to ensure that a product does not contain any known issues at introduction time.

Responsible disclosure

The second form of external validation comes from independent external parties that spend time on validating the ClickShare solution and then submit responsible disclosure reports. These reports are reviewed by Barco and then acted upon if deemed valid.

To report any security vulnerability, please contact our product security incident response team via https://www.barco.com/en/about-barco/legal/responsible-disclosure.

Closing

The third generation of ClickShare collaboration systems contains significant security improvements. Moreover, the CX 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.

ENABLING BRIGHT OUTCOMES

BARCO