White Paper

ClickShare Security White Paper

Authors:

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

March 2017

BARCO

Visibly yours

Table of Contents

1. 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 these products, code-named CSE-xxx.

According to the Global State of Information Security Survey 2016[1] executed by Price Waterhouse Cooper (PwC), 38% more security incidents were detected in 2015 compared to 2014 in professional organizations, while information security budgets were raised by 24% last year. 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 CSE-xxx range.

Security and usability have always been hard 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. Our engineers and product managers discussed security at length during design and development, resulting in a secure, and at the same time very user-friendly collaboration system. The embedded nature of the ClickShare components adds an extra degree of difficulty to integrate security, less computational power is contradictory to more security. Moreover, focusing on security from the initial steps of the project ensures customers and users of ClickShare are protected against malware, hackers and eavesdroppers, as well as protection against reverse engineering the product.

This technical white paper will focus in more detail on the different components and features of the ClickShare products in general, and the CSE range of products in particular (CSE-200, CSE-800 and any CSE-xxx model brought to market).

[1] http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html

2. Modelling the ClickShare threats

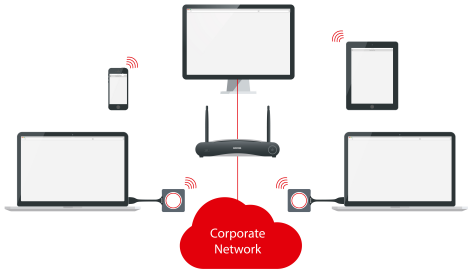
The past three years, lots of questions and requests were raised by customers about security, user scenarios, integration methods, etc. With all those topics in mind extensive threat modelling has been applied during design and development phases of the second generation ClickShare system. Threat modelling is one of the most powerful security engineering activities because it focuses on actual threats, not simply on vulnerabilities. A threat is an external event that can damage or compromise an asset or objective, whereas 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 they are often not in control of 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 should not only focus on software, hardware and even production related topics must also be involved to create a secure product from bottom up.

2.1. What does the system look like?

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

Following **participating 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, and makes sure they get 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 optional audio is transferred instantly to the large meeting room screen display and speakers attached to the Base Unit.
- Client: The application is running on your laptop PC or Mac which gathers the screen content and sends it via the Button over the wireless link to the Base Unit. On the CSE-800, the application allows to moderate the ClickShare composition and receive both blackboarding and annotation sessions from the Base Unit over the wireless link to the Base Unit.
- Apps (iOS, Android): The app on your Android tablet, smartphone, iPad or iPhone which enables you to share the screen content of documents and photos on the display attached to the Base Unit.
- AirPlay: The AirPlay protocol allows wireless streaming of audio and video from Apple devices. ClickShare supports AirPlay streaming as well as AirPlay mirroring.
- Google Cast: The Google Cast protocol allows wireless streaming of video from Android devices. ClickShare supports Google Cast streaming as well as Google Cast mirroring.



2.2. What data needs to be protected?

All data which is transferred via the ClickShare collaboration system must be protected, but also data, which is not shared on the display or speakers and stored on devices participating in a ClickShare session, must be protected. Users want to share data on the display and audio on the speakers attached to the Base Unit, only attendees of the meeting are able to see and hear the content. Data/audio which is not shared may never be accessed and/or transferred, the user has full control and responsibility of which data and/or audio is shared. People connecting the Button to their laptop PC or Mac, or installing the apps on their mobile devices, must be assured that the original Barco software is running and no malware is affecting their devices by using ClickShare. Contents of a display at the board meeting room can be highly confidential the system handling that data must assure the confidentiality, integrity and availability of this data. The content is delivered in real-time and is never stored on non-volatile memory in one of the ClickShare components. The basic security tenet is to make the cost of an attack more than the data is worth to an attacker.

2.3. Which physical system interfaces and services can be identified?

Both Base Unit and Button run an embedded Linux OS and have physical interfaces exposing certain services:

- **Base Unit:**

  Externally accessible

  - USB
    Bootloader access/Linux CLI access
  - Ethernet
    Web UI
    REST API
    Communication with Client and Apps
    AirPlay
    Google Cast
  - Wi-Fi
    Web UI
    Communication with Client and Apps
    AirPlay
    Google Cast

  Internally accessible

  - Serial
    Bootloader access/Linux CLI access
  - JTAG
    Flash access

- **Button:**

  Externally accessible

  - USB
    Communication with Client/Base Unit
  - Wi-Fi
    Communication with Base Unit

  Internally accessible

  - Serial
    Bootloader access/Linux CLI access

2.4. Where is the system physically located?

Primarily the Base Unit is located in a professional environment (recommended to be connected to a "trusted" corporate network via the Ethernet interface, 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 power range of the wireless interface will exceed the physical boundaries of the meeting room and maybe even those of the corporate building. Access to the Wi-Fi and Ethernet interfaces of the Base Unit must be protected in an appropriate way.

2.5. Who is using and who is managing the system?

In a professional environment, most users will be employees, although during meetings with customers, suppliers, etc., external people will also participate and make use of the same ClickShare collaboration system. But whatever the setup, a range of different devices are connected to the same system, bringing along potential security risks. This emphasizes once more that content may only be shared with people attending the meeting and that the system guarantees that only data is shared to which the user explicitly has given access to by clicking the Button or sharing content with the apps.

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 new ClickShare Enterprise range of collaboration systems introduces several levels of security. Switching between different security levels can be managed through the web interface of the Base Unit, which clearly mentions the consequences of making the switch. The higher the security level, the lesser compatibility is guaranteed with first generation ClickShare components (CSM-1 and CSC-1). Choosing the right security level will depend on a risk analysis and compatibility needs.

3. Technical implementation on the CSE-xxx range

3.1. 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 the technical implementation related to security of ClickShare, one specific fact has to be emphasized: the use of Wi-Fi communication makes the availability corner of the 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; that way, at least unintentional interference can be eliminated. The proper functioning of a ClickShare system starts with an interference-free environment.

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 if one safeguard fails, another safeguard prevents compromising the system. The safeguards must correspond to the threats identified during the threat modelling exercise.

3.2. Background information

Identification and authentication steps during set-up of a communication channel are crucial to trust the other side, encrypt trans- ferred 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 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 with 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 keys between Barco and production happens over an IPsec tunnel in an encrypted container and additionally the private key is stored in encrypted format on the device.

3.3. 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 will pair both, the Base Unit will share all parameters with the Button to be able to access the Wi-Fi of the Base Unit and optionally upgrade it if more recent firmware is available. The Base Unit will interact over USB with a valid ClickShare Button only if mutual authentication is successfully applied based on both device certificates, unless the lowest security level is configured, then a Base Unit can interact with first generation Buttons which do not hold a device certificate. There is one additional exception on authenticated access, when an external storage device is connected via USB, the top directory will be scanned for a file named "clickshare_firmware.enc". If this file is present, the Base Unit will start the upgrade procedure which will only be successful if the firmware is correctly encrypted and signed, otherwise the upgrade is aborted.

Also on the Button the serial connector is not populated on the PCBA and from bootloader level onwards the input of serial interface has been disabled.

Connected via USB to a laptop PC or Mac the Button announces itself as:

- A USB Human interface device 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 will give similar protection for access over Wi-Fi, although Wi-Fi has security controls at network layer which is not 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 also a need for additional authentication, confidentiality and integrity controls at application layer on the Button.

3.4. 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 Base Unit web interface, 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. Keep in mind 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. 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.

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. Both interfaces work solely on IPv4 based traffic.

3.5. OS layer

Both Base Unit and Button run an embedded Linux OS, which can be upgraded in the field as a monolithic firmware image, which will be periodically released by Barco. The Base Unit can be upgraded manually via uploading the firmware image in the web interface or it can be configured to automatically start upgrading via an authenticated https connection to a Barco server when a new image is released and published. The Buttons will be upgraded when a more recent firmware is available on the Base Unit, this can happen in the background over Wi-Fi when configured as such in the web interface of the Base Unit, or it happens when the Button is paired via USB with the Base Unit.

To assure a failsafe upgrade mechanism a double copy strategy has been implemented on the Base Unit. The upgrade firmware will be written to the inactive partition after signature verification and decryption, the updated partition will be marked as activated after a successful verification step to check if the image has been correctly written to flash. The active partition toggles after every upgrade.

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 out 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 at the same time, 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 is monitoring all important services, if one is hanging or has crashed, the watchdog will restart the service.

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 would be detected, it will be analysed and scheduled to be solved. Based on the criticality of the vulnerability, the solution will be made available in an intermediate release or be part of the next planned release.

3.6. Application layer

Communication protocols

Out of the box, CSE-xxx units 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, 1/ a protocol to communicate over USB and 2/ 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 or 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 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 which component it is interacting with. Buttons will use their device certificate to authenticate, the apps will use a numeric or alphanumeric passcode[2], 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 running over TCP, confidentiality and integrity controls have been implemented at application layer. 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 also in the second generation sent in unencrypted format, though established via an authenticated and encrypted connection at control plane level.

[2] Support for passcodes is available for the CSE-range from firmware release v01.03 onwards

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 certain security features and backwards compatibility. This approach will make security 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.

Three security levels have been defined, the following statements describe how changing the security level should work:

- Two components should always use the protocol and authentication mode with the highest priority that its current security level allows it to use.
- 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).
- 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.

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

	Security level 1	Security levels 2-3
Button R9861500D01 (included with CSE-xxx sets)	x	x
Button R9861006D01 (included with CSM-1 and CSC-1 sets)	x	NOT SUPPORTED
CSC-1	x	NOT SUPPORTED
CSM-1	x	NOT SUPPORTED
CS-100	x	NOT SUPPORTED[3]
CSE-xxx	x	x
Software Client	x	x
iOS app	x	x
Android app	x	x

[3] Although the CS-100 uses second generation communication protocol, the unit does not feature configurable security

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

- Activate passcode for mobile apps & Buttons[4]
- Web UI: 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 mobile apps
- Alphanumeric passcodes for mobile apps and Buttons
- Button hardware certificate for pairing

Security Level 3 contains Security Level 2 features plus:

- Mobile apps are blocked
- Firmware downgrade not possible
- No access to Web UI via Wi-Fi

		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	Web interface or REST API: server authenticated TLS (RSA based), basic authentication for client	Web interface or REST API: server authenticated TLS (RSA based), basic authentication for client	SSH disabled Input validation of web interface
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 Secure boot locked to hardware	Base Unit: Signed bootloader and kernel Secure boot locked to hardware Button: Signed image (bootloader, kernel and rootfs) in upgrade package Secure boot locked to hardware	Base Unit: Firewall Button: Watchdog
Network		WPA2-PSK (AES encryption, 128-bit key)	WPA2-PSK (CCMP to create Message Integrity Check)	Interference and wireless hacking can cause unavailability of the system
Physical		Secure JTAG	Secure JTAG	Access to serial input is blocked

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

WebUI and REST API

Configuration of the Base Unit can be managed via the web interface or the 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 web interface and REST API is protected via password credentials with Basic Authentication (over HTTPS). All functionality of the web interface and REST API needs authentication to be accessed or changed.

The web interface login is a session which is bound to a session cookie which stays valid until logout or expiration. When changing your password, an indicator indicates the password strength. User passwords are hashed using bcrypt, a widely used, secure hashing algorithm. Each password has its own unique salt, preventing rainbow table attacks. Furthermore, all inputs for both web interface and REST API are validated to prevent injection vulnerabilities.

Client application

The only application running on the laptop PC or Mac is the ClickShare client software. This piece of software is developed and maintained by Barco, and no external party has access to it. The binary software image 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. It can only be programmed at production, or re-programmed by the ClickShare Base Unit after mutually authenticated access over USB based on the trusted device certificates, unless the lowest security level is configured, then a Base Unit can re-program the client software on first generation Buttons. A user cannot write to this storage device, intentionally or unintentionally. All re-programming is managed by software running on the Base Unit that is also developed, maintained, and signed by Barco, with no access by any external party. To guarantee the integrity of the software running on the Base Unit and to avoid tampering with the mass storage device inside the ClickShare Button, only signed images are permitted to upgrade the Base Unit. 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. Additionally, a launcher application can be installed on the laptop PC, which will automatically launch the software client when a Button is connected. This can be done ad hoc or company-wide via MSI installer.

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 QR 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 Bonjour protocol. If the mobile device is 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. All Base Units support iOS10 which contains improved security features. Authentication will be fully integrated via the same passcode which is also used for the Barco apps. 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.

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 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.

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 characters long and can be numeric or alphanumeric as chosen in the Base Unit's ClickShare Configurator WebUI settings. In case multiple users connect at the same time they use the same displayed passcode to enter on their ClickShare App or Airplay for authentication with the Base Unit. The displayed passcode remains valid during the authentication attempt of a user, limited to a maximum period of 10 minutes. After authentication of a user or a timeout, the passcode is not used anymore and is removed from the screen.

Every user trying to connect via a ClickShare App or Airplay generates a pop-up on the screen with the passcode to be used for authentication of the connection attempt. 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. Note that after 5 failed connection attempts in a row, 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 web interface 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, MAC addresses, and so on. If the "Debug logging" check-box is checked in the Base Unit web interface, the username of the person currently sharing will also be logged. 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.

3.7. Interoperability with first generation ClickShare products?

To allow existing customers to extend their current ClickShare install base, CSE-xxx units can default still interact with first generation ClickShare products, 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.

4. Closing

The second generation of ClickShare collaboration systems contains significant security improvements. Moreover, the CSE-range of ClickShare offer best in class security, configured around 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 or report a vulnerability, please let us know via clickshare@barco.com.