whitepaper

ClickShare Security

Introduction

ClickShare was introduced in 2012. Four years later, in 2016, 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.

Back in the early days when the architecture of the next-generation ClickShare solution was on the drawing board, security was already being taken into account. Our engineers and product managers discussed security at length during design and development, resulting in a secure yet very user-friendly collaboration system. Moreover, focusing on security from the initial stages of the project ensures that customers and users of ClickShare are protected against malware, hackers, and eavesdroppers, and also against product reverse engineering.

Modeling the ClickShare threats

Over the past three years, customers have had many questions and requests about security, user scenarios, integration methods, and so on. With all these topics in mind, extensive threat modeling was applied during the design and development phases of the second-generation ClickShare system. Threat modeling is one of the most powerful security engineering activities because it focuses on actual threats, not simply on vulnerabilities. Threat modeling facilitates a risk-based product development approach by identifying external risks and encouraging the use of secure design and development practices. To create a secure product from the bottom up, threat modeling should not only focus on software and hardware, but also take production-related aspects into account.

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, 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.

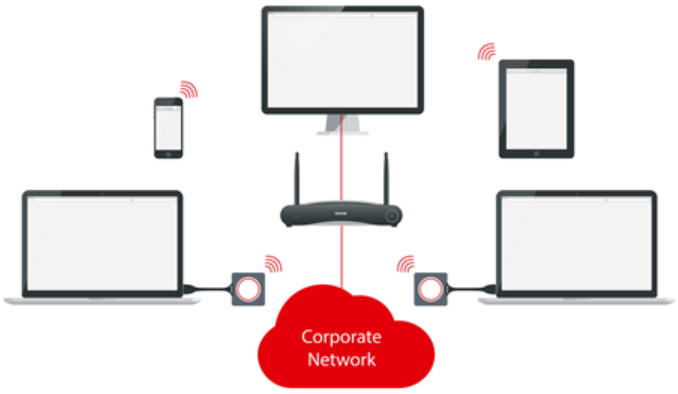
The following components can be identified in a ClickShare collaboration system:

- 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, and makes sure it is reproduced correctly on the display.
- Button: The ClickShare Button is a USB-powered device that is both an external read-only mass storage device containing the client application and an audio-capable device. Simply plug it into 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 to the speakers attached to the Base Unit.
- Client: The application runs on your laptop 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 enables you 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 that 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.

What data needs to be protected?

All data that is transferred via the ClickShare collaboration system must be protected, but this also applies to data that is not shared on the display or speakers and is stored on devices participating in a ClickShare session. Users want to share data on the display, and audio on the speakers attached to the Base Unit, in such a way that only attendees of the meeting are able to see and hear the content. Data/audio that is not shared may never be accessed and/or transferred; the user must have full control over and responsibility for what data and/or audio is shared.

People connecting the Button to their laptop or Mac, or installing the apps on their mobile devices, must be sure that the original Barco software is running and that no malware is affecting their devices by using ClickShare. The content of a display at a board meeting can be highly confidential, so the system handling that data must ensure its confidentiality, integrity, and availability. 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.



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

Where is the system physically located?

The Base Unit is primarily located in a professional environment (it is recommended that it should be connected to a “trusted” corporate network via the Ethernet interface, although scenarios are known where ClickShare is used in standalone or ad hoc mode). Nevertheless, data that is handled by the system can be highly confidential and must be protected. The power range of the wireless interface will exceed the physical boundaries of the meeting room and possibly even those of the corporate building. Access to the Wi-Fi and Ethernet interfaces of the Base Unit must be appropriately protected.

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 parties will also be involved and will make use of the same ClickShare collaboration system. But whatever the setup, a range of different devices are connected to the same system, giving rise to potential security risks. This emphasizes once again 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 has explicitly given access by clicking the Button or sharing content with the apps.

Configuration of the ClickShare system in a professional environment is primarily managed by the IT department or facility management team. They assist employees in making the best possible use of all facilities the company has to offer. 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 indicates the consequences of making the switch. The higher the security level, the less 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 requirements.

ClickShare's CSE range offers best-in-class security

Layered approach

A network-connected system can be divided into different layers: physical, network, host, and application layer. Mapping these four layers onto the CIA triad (Confidentiality, Integrity, and Availability) will reveal how security is implemented in a system and where safeguards are lacking. The layered approach and the implementation of multiple safeguards to protect a system will ensure that if one safeguard fails, another prevents the system from being compromised. The safeguards must correspond to the threats identified during the threat modeling exercise.

	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

Background information

Identification and authentication steps during setup of a communication channel are crucial to be able to trust the other party, 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 has been set up to generate device certificates and guarantee a chain of trust during authentication between ClickShare devices. Every device receives a unique certificate with a private/public key pair based on elliptic curve technology (sect283k1, NIST/SECG curve over 283-bit binary field), which is signed based on ECDSA. Created and signed by a Barco Certification Authority, this device certificate is non-renewable and cannot be revoked.

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 intention of reverse engineering the firmware and loading malicious malware on the device. Protecting the physical interfaces of embedded devices is as important as protecting the other layers of the system.

The connectors of the serial and JTAG interface of the Base Unit have not been populated on the PCBA of the deployment units. Input on the 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, while read or write access to the key is prevented via hardware lock.

Connecting a Button to the Base Unit via USB will pair them: 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.

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

Access to the Ethernet interface makes it possible to connect to the network stack and services running on the Base Unit; additional authentication, confidentiality and integrity controls at application layer are therefore necessary. These controls will give similar protection for access over Wi-Fi.

Network layer

The wireless interface of the Base Unit is protected by default with WPA2-PSK, a method for securing the Wi-Fi (Wi-Fi Protected Access 2) by using 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 ensured 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 readily available on the Web, it is fairly easy to scan an area for hidden networks.

OS layer

Both Base Unit and Button run an embedded Linux OS and 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 by 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 Button will be upgraded when more

recent firmware is available on the Base Unit. This can happen in the background over Wi-Fi when appropriately configured in the web interface of the Base Unit, or it can happen when the Button is paired via USB with the Base Unit.

Firmware signing and encryption ensures the integrity and confidentiality of the software running on the Base Unit, and provides a guarantee to the customer that the firmware was originally created by Barco, that it has not been tampered with and that a firmware image cannot be reverse engineered.

The Base Unit firmware contains a watchdog that monitors all important services. If a service is hanging or has crashed, the watchdog will restart it.

The embedded Linux OSs in Base Unit and Button contain multiple open-source software packages. A list of these is available in the End User License Agreement. Barco closely monitors new vulnerabilities detected in the open-source packages embedded in our products. If a vulnerability were to be detected, it would be analyzed and scheduled to be remedied. Depending on the criticality of the vulnerability, the solution would be made available in an intermediate release or as part of the next planned release.

Security levels

Security levels have been introduced for ClickShare's CSE range, in order 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 regard to the features it provides, meaning that moving up or down in the security levels will change the capabilities of the ClickShare system.

Security Level 1 offers enterprise security, while maintaining compatibility with first-generation ClickShare components, and provides the following additional security features:

- Activate passcode for mobile apps & Buttons[1]
- 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

Out of the box, CSE-xxx units are on security level 1 to ensure compatibility with the first generation of ClickShare products. Once the security level is changed to level 2 or 3, compatibility with the first-generation products is no longer supported due to the lack of device certificates, which makes authenticated communication impossible.

[1] CSC-1 model features all level 1 security features except for passcode support.

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
CS-100	x	NOT SUPPORTED[2]
CSE-xxx	x	x
Software Client	x	x
iOS app	x	x
Android app	x	x

Conclusion

The second generation of ClickShare collaboration systems contains significant security improvements. Moreover, the CSE range of ClickShare offers best-in-class security, configured around three levels of security. In addition to the efforts devoted to designing and implementing security features, Barco guarantees that no back doors or hidden transfers have been implemented.

If you have any further questions or wish to report a vulnerability, please let us know by e-mailing clickshare@barco.com.

M00699-R00-1117-WP

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