ホワイトペーパー

ClickShare セキュリティ白書

著者：Filip Louwet, David Martens, Jef Neefs, Hanne Page, Hans Mortier, Adrien Decostre, Kristof Demeyere, Lieven Bertier

BARCO

Visibly yours

目次

1. はじめに

ClickShare は 2012 年に発売されました。発売から 3 年が経ち、新世代の ClickShare エンタープライズ製品を市場に出す準備が整いました。CSE -200 を皮切りにコードネーム CSE-xxx と呼ばれる新製品群は新しいデザイン、向上した性能、エンタープライズ・インテグレーション、設定可能な内蔵セキュリティが重要な特徴となっております。

プライス・ウォーターハウスクーパー（PwC）が実施したグローバル情報セキュリティ調査 2016[1] によれば、2014 年と比較して 2015 年に検出されたセキュリティ案件は 38%増加し、情報セキュリティ予算も前年から 24％上昇しました。その一方でサイバー脅威やプロフェッショナルなスパイ活動、さらにプロフェッショナルな組織における情報セキュリティへの関心の高まりが、セキュリティを CSE-xxx レンジの重要な機能とする原動力となっています。

セキュリティと使い勝手のバランスを保つのは製品開発とユーザーエクスペリエンスデザインの面から常に困難がともないます。セキュリティを高めると往々にして使い勝手が悪くなり、逆に使い勝手を重視しすぎると、使用感がよくなるものの、潜在的なセキュリティホールを作ることになります。この 2 つの完璧なバランスを見出すのは難しく、製品設計の第一段階から取り組む必要があります。

次世代 ClickShare ソリューションのアーキテクチャが設計される初期段階からすでにセキュリティが考慮されていました。当社のエンジニアとプロダクトマネージャーは設計中も開発中も根気強く話し合いました。その結果、安全であると同時に極めてユーザーフレンドリーなコラボレーションシステムを完成させました。埋め込みを重視する ClickShare コンポーネントの方針のため、結果的にセキュリティの統合はより一層難しくなりました。計算能力の低下はセキュリティの増強と相反するものです。さらにプロジェクトの初期段階からセキュリティに重点を置いたおかげで、ClickShare の顧客とユーザーの皆様をマルウェア、ハッカー、盗聴者から守るとともに、製品をリバース・エンジニアから守ることができます。

この技術白書は ClickShare 製品全般、特に CSE 製品シリーズ（CSE-200 とそれ以降に市場に投入される CSE-xxx モデル）のさまざまなコンポーネントと機能に焦点を当てて詳しく説明していきます。

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

2. ClickShare 脅威モデリング

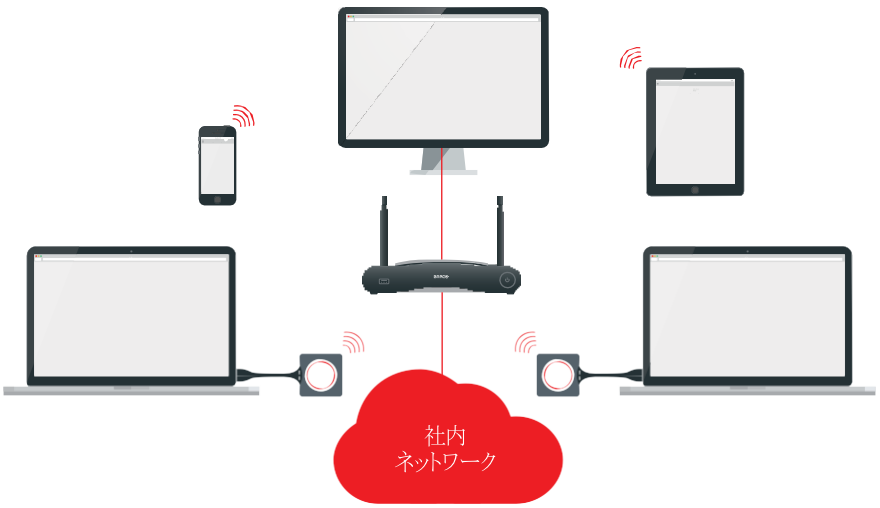
これまでの 3 年間、お客様からセキュリティ、ユーザーシナリオ、インテグレーション方法についてたくさんの質問と要請が寄せられました。こうしたことを念頭に置き、第 2 世代の ClickShare システムの設計開発段階では大規模な脅威モデリングを活用しました。脅威モデリングは最も強力なセキュリティエンジニアリングの 1 つです。それは脅威モデリングが単に脆弱性だけでなく、実際の脅威を重視しているからです。脅威とは資産に損害を与えるとか目標への妥協を強いられる恐れのある外部の事象です。一方、脆弱性とはシステム内の利用されやすい弱点を指します。脆弱性は解決できますし、そうしなければなりません。ですが脅威は永遠に続き、時とともに変化するもので、デバイスやシステム使う人やそれを管理する人の手の及ばないところで起こっていることが多いのです。脅威モデリングのおかげで、危険がある前提（リスクベース）での製品開発アプローチが行われ、外部リスクを洗い出すとともにセキュアな設計と開発手順が採用されています。脅威モデリングはボトムアップでセキュアな製品を作るためにソフトウェアやハードウェアに重点を置くだけでなく、関連製品さえも対象としなければなりません。

2.1 どのようなシステムなのか？

バルコの ClickShare コラボレーションシステムなら、ボタンをクリックするだけで、参加者全員がコンテンツを共有できるようになります。ノートパソコン、マッキントッシュ、iPad、iPhone、AndroidOS デバイスのいずれからでも、可能なかぎり単純かつ直感的な方法で中央会議室のスクリーンにコンテンツを表示できます。

ClickShare コラボレーションシステムを構成するコンポーネントとして識別できるものは次のとおりです：

- ベースユニット：常に目にする物ではありませんが、ベースユニットは Clickshare システムの中核となります。このプロセシングユニットはボタンからワイヤレスストリームを受け取ってディスプレイに正確に表示します。
- ボタン：ClickShare ボタンはクライアントアプリケーションが入った外部読み取り専用大容量記憶装置およびオーディオ対応デバイスだと自らアナウンスする USB バスパワーテバイスです。それをお客様のノートパソコンの USB ポートに接続し、アプリケーションを起動してボタンのアイコンをクリックするだけで、ノートパソコンのスクリーンコンテンツとオプションの音声が即座にベースユニットに接続された会議室用大型スクリーンとスピーカーに転送されます。
- クライアント：これはお客様のノートパソコンやマッキントッシュで稼動し、スクリーンコンテンツを集めてボタンを介してワイヤレスリンクでベースユニットに送るアプリケーションです。
- Apps (iOS, Android)：ベースユニットに接続しているディスプレイと、スクリーンコンテンツやドキュメント、写真を共有できるようにするお客様の Android タブレット、スマートフォン、iPad、iPhone のアプリです。
- AirPlay：AirPlay プロトコルはアップルのデバイスから音声とビデオのワイヤレスでストリーミングを可能にします。ClickShare は AirPlay ストリーミングとともに AirPlay ミラーリングにも対応しています。



2.2 守る必要があるデータは？

ClickShare コラボレーションシステムによって転送されるすべてのデータだけでなく、ディスプレイやスピーカーで共有してないデータや ClickShare セッションに参加しているデバイスに保存されているデータも守らなければなりません。使う側としてはディスプレイでデータを、スピーカーで音声を共有したいけれども、コンテンツを見聞きできるのはミーティングの参加者だけにしたいでしょう。共有していないデータ/音声は決してアクセスや転送ができないので、ユーザー様側が共有するデータや音声を完全にコントロールし、それに責任を持ちます。ボタンにノートパソコンや Mac に接続しているか、モバイル機器にアプリをインストールしている方々は、オリジナルのバルコ社製ソフトウェアをきちんと稼動させ、ClickShare を使うことによってマルウェア（悪性ソフト）による影響がモバイル機器に起こらないようにしなければなりせん。取締役会議室にあるディスプレイに映されるコンテンツは極秘情報なこともあり、そのデータを処理するシステムはデータの機密性、完全性、可用性を確保する必要があります。コンテンツはリアルタイムで送信され、ClickShare コンポーネントの 1 つにある不揮発性メモリには一切保存されません。セキュリティ戦略の基本は攻撃者にとって攻撃のコストをデータより高くつくようにすることです。

2.3 どの物理システムインターフェースとサービスが識別されますか？

ベースユニットとボタン両方とも組み込み LinuxOS で駆動し、特定のサービスを提供する物理インタフェースがあります：

- **ベースユニット:**

  製品の外部からアクセス可能

  - USB
    - ブート ローダーアクセス/Linux CLI アクセス
  - 有線 Ethernet
    - Web UI
    - REST API
    - クライアントとアプリとの通信
    - AirPlay
  - ワイヤレス Wi-Fi
    - Web UI
    - クライアントとアプリとの 通 信
    - AirPlay

  製品の内部からアクセス可能

  - シリアル
    - ブート ローダーアクセス/Linux CLI アクセス
  - JTAG
    - Flash アクセス

- **ボタン:**

  製品の外部からアクセス可能

  - USB
    - クライアント/ベースユニットとの通信
  - ワイヤレス Wi-Fi
    - ベースユニットとの通信

  製品の内部からアクセス可能

  - シリアル
    - ブート ローダーアクセス/Linux CLI アクセス

2.4 システムの物理的設置場所は？

主にベースユニットはプロフェッショナルな環境（Ethernet インタフェースを経由して「信頼できる」社内ネットワークに接続することを推奨しています、もちろん ClickShare を独立型ないしアドホック方式で使うシナリオもありますが）に位置しています。とはいえ、システムが扱うデータは高度に機密性が高いこともあり、然るべきセキュリティが欠かせません。ワイヤレスインタフェースの有効範囲は会議室の物理的な境界はおろか、社屋の境界さえ越えます。ベースユニットの Wi-Fi インタフェースおよび Ethernet インタフェースへのアクセスは適切な方法で守らなくてはなりません。

2.5 誰がシステムを使い、誰が管理するのか?

プロフェッショナル環境において大半のユーザーは社内の人間でしょうが、顧客や供給元などとの会議には外部の人間も参加し、同じ ClickShare コラボレーションシステムを利用することになるでしょう。どんな設定でも、多種多様なデバイスが同じシステムに接続しているため、潜在的なセキュリティリスクが発生します。それゆえに繰り返しになりますが、コンテンツが会議の出席者にしか共有されず、システムもボタンをクリックするかアプリケーションを使ってコンテンツを共有することで明確にアクセス権を与えられたユーザーにしかデータを絶対に共有しないことが重要になります。

プロフェッショナル環境にある ClickShare システムの設定は主に IT 部門か施設・設備運営管理部が管理します。施設・設備運営管理部の役目は従業員が会社の提供するすべての設備や施設を最大限活用するのを助けることです。新しい ClickShare エンタープライズ・レンジのコラボレーションシステムでは数段階のセキュリティレベルが用意されており、セキュリティレベルの切り替えはベースユニットのウェブインタフェースを通して行えます。この際、ベースユニットはセキュリティレベルの切り替えの結果起きることを明示的に通知します。セキュリティレベルを上げると、第 1 世代の ClickShare コンポーネント（CSM-1 と CSC-1）との互換性が下がります。適切なセキュリティレベルの選択はリスク分析と互換性の必要性によって決まります。

3. CSE-xx レンジでの技術的実装

3.1 階層的アプローチ

情報セキュリティの根本原理は CIA の三文字、Confidential（機密性）、Integrity（完全性）、Availability（可用性）に集約されます。製品やシステムのどの部分もセキュアな環境を保証するためにシステムのライフサイクルを通してこのコンセプトを重んじなくてはなりません。

ClickShare のセキュリティに関連する技術的な実装の前に、強調しておかねばならないことがあります。それは WiFi 通信を使うと CIA の境界線が極めて曖昧になってしまうことです。ワイヤレスシステムの周辺にあるあらゆる干渉源が－意図的でも意図でなくても－システムの機能に不具合を起こし、結果システムは使えなくなります。大型設備の分析、プランニング、配置ではプロフェッショナルな WiFi インテグレータを使うことを強く推奨します；これによって少なくとも意図的でない干渉を除くことができます。ClickShare システムの適切な稼動にまず必要なのは、干渉のない環境です。

ネットワークに接続したシステムは 4 つの階層、物理、ネットワーク、ホスト、アプリケーションに分けられます。この 4 つの階層を CIA 三箇条に照らすことで、セキュリティがシステムにおいてどのように実装され、セーフガードの穴がどこにあるのかが明らかになります。システムを守る階層的アプローチと複数のセーフガードの実装によって、たとえ 1 つのセーフガードが突破されても、別のセーフガードがシステムのセキュリティが破られるのを防いでくれます。セーフガードは脅威モデリングの実施にて判明した脅威に対応しなくてはなりません。

3.2 予備知識（背景情報）

通信チャンネルを確立する際の識別と認証のステップは、両サイドを信頼するとともに、転送中に転送データを暗号化し、データの改変を防ぐ上で重要になります。ClickShare ベースユニットとボタンにはデバイス認証書が入っています。これはデバイスの製造中に準備され、デバイスの非消去メモリに暗号化された形式で格納されています。公開鍵のインフラストラクチャは ClickShare のデバイス間の認証中にデバイス証明書を作成し、トラストチェーンを保証するようにセットアップされています。公開鍵のインフラストラクチャは ClickShare のデバイス間の認証中にデバイス証明書を作成し、トラストチェーンを保証するようにセットアップされています。すべてのデバイスには、楕円曲線（暗号）技術（sect283k1、NIST/SECG カーブの 283 ビット以上の 2 進数フィールド）をベースとし、ECDSA に基づいて署名された秘密鍵/公開鍵ペアを有する固有の証明書が与えられます。このデバイス証明書はバルコ認証局によって作製と署名が行われ、再発行と取り消しは行えません。ClickShare デバイスがすべてインターネットに接続しているわけではありません。そのためにリボケーション（取り消し）方針に従うデバイス証明書管理はほとんど余計なものとなり、完全に複雑になってしまいます。これは ClickShare の使いやすさと相容れないことです。そこで許容できる範囲までリスクを押さえるために、追加の緩和措置が実装されています。PKI インフラストラクチャ（公開鍵基盤）は社内システムから物理的に隔離された、物理的アクセスが制限されている社内の別の場所でホストします。バルコと生産の間の鍵の転送は暗号化されたコンテナに入れて IPsec トンネルを使って行われ、さらに秘密鍵はデバイスに暗号化された形式で格納されています。

3.3 物理層

組み込みデバイスは物理的に小さいので盗まれやすく、ファームウェアをリバース・エンジニアして、デバイス上に悪意のあるマルウェアをロードしようとする悪意のあるハッカーによって物理インタフェースへ簡単にアクセスされてしまいます。組み込みデバイスの物理インタフェースを守ることはシステムの他のレイヤーを守ることと同じぐらい重要です。

ベースユニットのシリアルインタフェースと JTAG インタフェースの両方コネクターはディプロイメントユニットの PCBA に組み込まれていません。シリアルインタフェースの入力はブートローダー以上のレベルから停止でき、JTAG インタフェースは秘密の応答鍵によって安全を保たれています。この鍵はワンタイム（One-Time Programmable）メモリに格納され、読み込み書き込みアクセスはハードウェアロックが防ぎます。

USB を経由してボタンとベースユニットを接続することで両方はペアリングし、ベースユニットはボタンとパラメータを共有し、ベースユニットの WiFi にアクセスできるようにし、最新のファームウェアが利用可能になればオプションとしてアップグレードもできるようにします。相互認証が両方のデバイス証明書に基づいて成功した場合にのみ、ベースユニットは USB を介して有効な ClickShare ボタンと通信します（最低のセキュリティレベルに設定されない場合を除いて）。最低のセキュリティレベルに設定されている場合、ベースユニットはデバイス証明書を持たない第 1 世代のボタンとも通信できます。認証されたアクセスにもうひとつ例外があります。外部記憶装置が USB を介して接続されているとき、トップのディレクトリは「clickshare_firmware.enc」という名前のファイルを探してスキャンされます。もしこのファイルが存在しているなら、ベースユニットはアップグレードプロセスを始めます。これが成功するのはファームウェアの暗号化と署名が正しく行われている場合で、そうでなければアップグレードは中止されます。

またボタン上にも、シリアルコネクターは PCBA に組み込まれておらず、ブートローダーレベル以降、シリアルインタフェースの入力が停止状態になっています。

USB を介してノートパソコンや Mac に接続するボタンがアナウンスする役割は、以下の通りです。

- ClickShare ソフトウェアクライアントと通信する USB ヒューマンインタフェースデバイス
- 音声をキャプチャーしてベースユニットに転送するオーディオデバイス
- WIndows と Mac の両方で実行可能な ClickShare クライアントを持つリードオンリーの大容量記憶装置

Ethernet インタフェースへアクセスすることでネットワーク・スタックとベースユニットで実行しているサービスへの接続が行えるので、アプリケーション層での追加の認証、機密性、完全性のコントロールが必要になります。この 3 つをコントロールすることで WiFi を介したアクセスに同じような保護が与えられます。ただしネットワーク層のセキュリティコントロールを握っているのは WiFi です。ClickShare システムの Ethernet インタフェースの場合は異なります。ベースユニットは WiFi アクセスポイントの役割を果たし、ボタンはステーションとして接続します。WiFi にアクセスするデバイスはどれもベースユニットに接続した他のボタンと通信できます。そのため、ボタンのアプリケーション層での追加の認証、機密性、完全性のコントロールが必要になります。

3.4 ネットワーク層

ベースユニットのワイヤレスインタフェースは WPA2-PSK によってデフォルトで保護されています。WPA2-PSK は事前共有鍵（PSK）の認証を使って WiFi（Wi-Fi Protected Access 2）をセキュアする 1 つの方法です。WPA2-PSK の暗号化はワイヤレスチャンネルを通るすべてのデータの機密性と完全性を保証します。機密性は 128 ビットキー長の AES ブロック暗号化によって、完全性はカウンタモード CBC-Mac プロトコル（CCMP）を使ってメッセージ完全性確認（MIC）を算出することで確保されています。WPA2-PSK パスフレーズと SSID（ベースユニットのウェブインタフェース管理者により設定可能）を使って得られた一時的な鍵により、IEEE 802.11i セキュリティ規格に従った認証（CCMP）と暗号化（AES）が行われます。ベースユニットは WiFi インタフェースの SSID を隠すように設定することが可能です。気をつけていただきたいのは、SSID クローキングは安全だと誤認させる恐れがあることです。ウェブで自由に利用可能なツールを使って、エリアをスキャンして簡単に隠れたネットワークを見つけられると言っても差し支えないでしょう。

先に書いたように Ethernet インタフェースでのセキュリティコントロールはありません。法人顧客様でのセットアップの経験から、ClickShare システムを社内データネットワークから分離するためにアクセスコントロールを追加した別の VLAN にまとめることが多いです。

WiFi と Ethernet は厳格に切り離され、1 つのパケットも両方のインタフェースの間に転送されることはなく、ベースユニットはすべてのトラフィックの端点となります。両方のインタフェースは IPv4 ベースのトラフィックでのみ作動します。

3.5 OS 層

ベースユニットとボタンの両方とも組み込み LinuxOS で作動します。この OS は現場でモノリシックファームウェアイメージとしてアップグレードが可能で、このイメージは定期的にバルコからリリースされます。ベースユニットならウェブインタフェースを使ってファームウェアイメージをアップロードすることによって手作業でアップグレードできますし、また新しいイメージが正式に公開されたときに自動的にバルコサーバーに認証された https に接続してアップグレードを始めるように設定することもできます。ボタンは最新のファームウェアがベースユニットで利用可能になるとアップグレードされます。これは WiFi を通じてバックグラウンドで行うようにベースユニットのウェブインタフェースを設定することもできますし、またボタンをベースユニットと USB を介してペアリングしても行われます。

万全のアップグレード機構を保証するために、二重のコピー方針がベースユニットには実装されています。アップグレードファームウェアは署名認識と復号化後に非アクティブなパーティションに書き込まれます。こうしてアップデートされたパーティションは、イメージが正しくフラッシュに書き込まれたかを確認する検証作業が成功してからアクティブとなります。アクティブなパーティションはアップグレードが終わるごとに切り替わります。

ファームウェアの署名と暗号化により、ベースユニット上で作動するソフトウェアの完全性と機密性が守られています。それはユーザー様にファームウェアが正真正銘バルコによって作成され、不法に変更されておらず、イメージファームウェアがリバース・エンジニアできないことを保証します。ファームウェアイメージはブートローダー、カーネル、ルートファイルシステムの 3 つのパーツで構成されています。 ブートローダーとカーネルは署名されていますが、暗号化されておらず、ルートファイルシステムは暗号化されていますが、署名されていません。完全性チェックはブートローダーレベルから始まり、ハードウェアまでにロックされています。いわゆるセキュアブートです。異なる起動コンポーネント（ブートローダーとカーネル）の署名を検証するための鍵は製造時にワンタイムメモリに暗号化された形式で書かれていて、OS レベルから読むことはできません。アップグレード中、アップグレードイメージのルートファイルシステム部分は復号され、フラッシュにファイルシステムを書き込む際に別の対称鍵で再び暗号化されます。関連する対称鍵は製造時に暗号化された形式でフラッシュに書き込まれており、OS レベルから読み込めないデバイスのユニークキーでしかアクセスできません。フラッシュをコピーしても、フラッシュのファイルシステムは暗号化されているので、簡単には ClickShare ソリューションをリバース・エンジニアできません。

ボタンも同じく二重のコピーアップグレード方針に従いますが、両方のイメージが同時にアップデートされ、ルートファイルシステムはフラッシュで暗号化されません。ボタンのファームウェアイメージは署名と暗号化が行われ、完全性チェックもブートローダーレベルから始まりハードウェアにロックされています。 署名と暗号化鍵情報は製造時に暗号化された形式でワンタイムメモリに書き込まれており、OS レベルから読み取りも書き取りもできません。

ベースユニットファームウェアには重要なサービスをすべてモニターしているウォッチドッグが入っていて、サービスの 1 つがハングするかクラッシュすると、サービスを再起動します。

ベースユニットとボタンの組み込み Linux OS は多数のオープンソースソフトウェアパッケージが入っています。こうしたパッケージのリストは末端消費者ライセンス契約にて利用できます。バルコは弊社製品に組み込まれているオープンソースパッケージで新たな脆弱性が見つからないか、つぶさにモニターしています。もし脆弱性が見つかった場合には分析が行われて解決策を講じることになっています。 脆弱性の重大性に基づいて、解決策をただちにリリースするか、次に予定されているリリースに含めるが決まります。

3.6 アプリケーション層

通信プロトコル

箱から出したばかりの CSE - xxx ユニットは第一世代の ClickShare 製品と互換性を持たせるためにセキュリティレベルを 1 にしてあります。セキュリティレベルが上がると、第 1 世代の ClickShare のコンポーネントとの対話に対応できなくなります。セキュリティレベルごとの詳細な説明に入る前に、通信プロトコルの概要を説明します。

2 つの異なる独自プロトコル、(1) USB を通じた通信プロトコルと(2)アプリケーション層における発信側と受信側の通信用プロトコルが ClickShare の屋台骨を形成しています。両方のプロトコルにコントロールプレーンとデータプレーンがあります。 第一世代のプロトコルはいかなる形式の認証にも対応しておらず、暗号化はボタンと共有されるスクリーンコンテンツにしか適用されません。 第二世代のプロトコルは機密性を保つために追加の完全性チェックと暗号化を行う認証に対応しています。

USB プロトコル:

- コントロールプレーン: 両方のエンド(ベースユニットないしボタン)にバルコのデバイス証明書へのアクセス権と、対応するプライベートキーがなくてはなりません。証明書で利用可能な鍵情報は認証のために両側のデジタル署名(ECDSA)を検証するときにしか使われず、鍵の共有には使われません。別個の一時的な鍵共有プロトコル(ECDHE)がデータプレーンのセッションキーを得るのに使われ、新しい接続がセットアップされるたびに、このセッションキーは変わります。

- データプレーン: USB を介したデータの暗号化には GCM モードの AES を使って機密性と完全性の両方を保ちます。この交換に使われる鍵は鍵共有プロトコルからの派生セッションキーです。

アプリケーションプロトコル:

- コントロールプレーン:すべてのコンポーネントはコントロールプレーンをベースユニットとの通信チャンネルをセットアップするのに使います。 まず、TLSv1.2 接続がサーバーサイドの認証とともに確立されます。すべてのクライアント側コンポーネントはベースユニットの検証に使うバルコ CA 証明書を持っています。 TLS 接続がセットアップされると、どのコンポーネントが対話しているかに応じて、追加のクライアント認証ステップがアプリケーション層で実行されます。 ボタンは認証にデバイス証明書を使い、アプリケーションは数字ないし英数字のパスコードを使います。第 1 世代のボタンはクライアントサイド認証を使うことができません。求められた認証方式の交渉が行われ、成功するかどうかはベースユニット側で設定されたセキュリティレベルに左右されます。なおセキュリティレベル 1 でしか第 1 世代のボタンから認証されていないアクセスは認められず、それより高いレベルでは認証されたアクセスが求められます。

- データプレーン:スクリーンコンテンツは TCP 上で起動しており、機密性と完全性のコントロールはアプリケーション層にて実行されます。認証された暗号化方式を得るために VMAC と組み合わせた Salsa20 が使われます。 Salsa 20 は逐次暗号で、VMAC はブロック暗号化ベースのメッセージ認証コードです。 両方とも発信側と受信側で既知のパラメータを必要とし、こうしたパラメータはコントロールプレーンを通じて共有されます。 音声データも第二世代のものでは、暗号化されていない形式で送られますが、接続はコントロールプレーンレベルでの認証および暗号化を通じて確立されます。

[4] パスコード対応が v01.03 以降のファームウェア公開から CSE-レンジで使えるようになります。

セキュリティレベル

ClickShare の仕様事例は広大かつ計り知れないことから、こうした特徴をすべて盛り込むためのセキュリティデザインは巨大かつ極めて複雑になります。セキュリティレベルは特定のセキュリティ機能と後方互換性をまとめるために導入されています。このアプローチを採用することで、ClickShare コラボレーションシステムのセキュリティ設定の管理が楽になります。各レベルとも提供する機能に関して自己完結となるように設計されています。それはセキュリティレベルを上げ下げすると、ClickShare システムの能力が変わるということです。

3 つのセキュリティレベルが定義されています。セキュリティレベルの変更がどういう仕組みになっているのか説明しましょう:

- 2 つのコンポーネントは常に現在のセキュリティレベルが認められるプロトコルと認証方式を最優先で使うものとします。
- 第二世代のボタンが第二世代のベースユニットとペアリングされると、ボタンのセキュリティレベルがベースユニットのセキュリティレベルに自動的に変更されます(第一世代のベースユニットとペアリングされても、セキュリティレベルは変わりません)。
- ベースユニットのセキュリティレベルが変更された場合は、共有秘密鍵(デバイス証明書によるクライアントサイド認証に使われる)が疑似ランダム値に変わります。これにより、すべての関連したボタンの再ペアリングが必要になります。

次の表はすべての ClickShare コンポーネント(第一世代および第二世代両方)において利用可能なセキュリティレベルの概略です:

	セキュリティレベル 1	セキュリティレベル 2〜3
ボタン R9861500D01 (CSE-xxx セットを含む)	x	x
ボタン R9861006D01 (CSM-1 と CSC-1 セットを含む)	x	非対応
CSC-1	x	非対応
CSM-1	x	非対応
CS-100	x	非対応[5]
CSE-xxx	x	x
ソフトウェアクライアント	x	x
iOS アプリ	x	x
Android アプリ	x	x

[5] CS -100 は第二世代の通信プロトコルを使いますが、ユニットに設定可能なセキュリティは搭載されていません。

レベル 1 は第一世代の ClickShare コンポーネントとの互換性を維持しつつエンタープライズセキュリティを提供し、次に挙げる追加のセキュリティ機能に備えます:

- 携帯アプリおよびボタンのためのパスコードを有効化 [6]
- ウェブ UI:HTTPS、ログインセッション管理、アプリとの共有を停止
- WiFi ネットワークの SSID を隠す

セキュリティレベル 2 はセキュリティレベル 1 の機能に加えて次の機能も含まれます:

- 携帯アプリのための必須パスコード
- 携帯アプリとボタンの英数字パスコード
- ペアリングのためのボタンのハードウェア証明書

セキュリティレベル 3 にはセキュリティレベル 2 に機能に加えて次の機能も含まれます:

- 携帯アプリをブロック
- ファームウェアのダウングレードを認めない
- WiFi を通じてウェブ UI へのアクセスを認めない

		機密性	完全性	可用性
アプリケーション	音声	暗号化なし	完全性チェックなし	-
	スクリーン	Salsa20 暗号化	VMAC 完全性チェック	-
	コントロールプレーン	コントロールプレーン:デバイス証明書ないし PIN 認証によるサーバー認証済み TLS(ECDHE_ECDSA)	コントロールプレーン:デバイス証明書ないし PIN 認証によるサーバー認証済み TLS(ECDHE_ECDSA)	-
	管理	ウェブインタフェースないし REST API: サーバー認証済み TLS(RSA ベース)、クライアント向けの基本的認証	ウェブインタフェースないし REST API: サーバー認証済み TLS(RSA ベース)、クライアント向けの基本的認証	SSH 停止 ウェブインタフェースの入力検証
ホスト		ベースユニット: フラッシュの暗号化ルート・ファイルシステム(rootfs)、アップグレードパッケージの暗号化 rootfs、ハードウェアにロックされたセキュアブート ボタン: アップグレードパッケージの暗号化イメージ(ブートローダー、カーネル、rootfs)、ハードウェアにロックされたセキュアブート	ベースユニット: 署名されたブートローダーとカーネル、ハードウェアにロックされたセキュアブート ボタン: アップグレードパッケージの署名されたイメージ(ブートローダー、カーネル、rootfs)、ハードウェアにロックされたセキュアブート	ベースユニット: ファイアウォール ボタン: ウォッチドッグ
ネットワーク		WPA2-PSK (AES 暗号化, 128-bit キー)	WPA2-PSK (MIC(メッセージの整合性チェック)算出のための CCMP)	干渉やワイアレスハッキングにより、システムの中断が起こる可能性あり
物理		セキュア JTAG	セキュア JTAG	シリアル入力へのアクセスをブロック

[6] CSM-1 および CSC-1 型はパスコード対応を除くすべてのレベル 1 セキュリティ機能を有しています。

WebUI と REST API

ベースユニットの設定はウェブインタフェースや REST API を通じて管理できます。両方ともベースユニットとの認証および暗号化された接続を保証するため HTTPS を介してのみ提供されます。 TLS の暗号スイート(ciphersuites)とバージョンは最近知られるようになった攻撃に対抗するように設定されます。ウェブインタフェースと REST API の両方へのアクセスは基本的認証のあるパスワードクレデンシャルによって(HTTPS を介して)で守られています。 ウェブインタフェースと REST API のすべての機能はアクセスや変更に認証が必要です。

ウェブインタフェースログインは、ログアウトないし期限まで有効なセッションクッキーに縛られたセッションです。パスワードを変えるとき、インジケータがパスワード強度を表示します。ウェブインタフェースと REST API の両方の入力はすべてインジェクション脆弱性を防ぐために妥当性が検査されます。

クライアントアプリケーション

ノートパソコンや Mac 上で稼動するアプリケーションは ClickShare クライアントソフトウェアしかありません。このソフトウェアはバルコが開発し、保守を行いますので、外部の人間がアクセスすることはありません。2 進法のソフトウェアイメージは署名され、タイムスタンプを押されているので、誰も改変できず、完全性が保証されています。ClickShare コードサイニング証明書は GlobalSign という WebTrust の審査を受けた認証局が発行しています。ソフトウェアは ClickShare ボタン内のリードオンリーの大容量記憶装置に格納されています。プログラムは製造時にのみ、再プログラムはベースユニットから信頼されるデバイス証明書に基づいて USB 経由で相互に認証されたアクセス後にのみ可能です。なお、セキュリティレベルが最低に設定されていなければ、ベースユニットは第一世代ボタンのクライアントの再プログラムが行えます。ユーザー様はこの保存デバイスに意図的でも意図的でなくても書き込むことができません。すべての再プログラムはベースユニット上で稼動するソフトウェアが管理します。このプログラムもまたバルコが開発、保守、署名が行われ、外部の人間はアクセスできません。ベースユニット上で稼動するソフトウェアの完全性を保証し、ClickShare ボタン内の大容量記憶装置の改変を避けるために、署名されたイメージしかベースユニットのアップグレードは認められません。クライアントソフトウェアは単一の実行バイナリで、揮発性 RAM メモリと CPU にしか影響を与えません。 ノートパソコンや Mac へのインストールに特別なドライバーを必要とせず、ドライバー自体のインストールも不要です。 さらにランチャーアプリケーションをノートパソコンにインストールできます。これをインストールしておくとボタンが接続されたときに、自動的にソフトウェアクライアントを起動します。インストールは MSI インストーラーによって局所的ないし会社規模で行えます。

Apps

iOS と Android 向けのアプリケーションがベースユニットに取り付けられたディスプレイに表示されたコンテンツを共有するために開発されています。バルコ ClickShare アプリケーションをダウンロードおよびインストールする際にはバルコ社の公式ウェブサイトのリンクを使うか、ベースユニットのディスプレイにある QR コードを使ってください。 モバイルデバイスがベースユニットの WiFi に接続しているなら、アプリはボンジュールプロトコルを介してベースユニットの識別を行います。もしモバイルデバイスが社内 WiFi アクセスネットワークに接続している場合、ベースユニットの Ethernet インタフェースの IP アドレスを入力すれば、ディスプレイのスクリーンコンテンツの提供が始まります。アプリはコントロールプレーンを通じてアプリケーション層にてベースユニットとサーバー側の認証をともなう TLS による通信を行い、データプレーンとの接続をセットアップしてコンテンツを共有します。 iOS と Android 両方のセキュリティ保護モデルが自己完結型アプローチなので、アプリは全画面ではなく、ドキュメントないし画像コンテンツしか共有できません。

AirPlay

AirPlay ミラーリングはベースユニットに対応しており、アップル TV デバイスに接続する必要はありません。ベースユニットファームウェアに完全に一体化しています。すべてのベースユニットはセキュリティ機能が改善された iOS9 に対応し、認証はバルコアプリにも使われる同じパスコードを通じて完全に統合されています。

ロギング

システムには rsyslog をベースにした強力なロギングエンジンが搭載されています。個別のボタンにログは格納されず、すべてのメッセージはボタンからベースユニットで稼動する rsyslog サーバーに送られます。ベースユニットも自己の活動を記録します。ログファイルは admin アクセス権を持つユーザーによりウェブインタフェースを経由してダウンロード可能です。 ログファイルに格納されたデータは現在のシステム状態について情報が含まれています。具体的にはコンポーネントの温度、フレームレート統計、ワイヤレスリンククオリティの統計、接続したユーザー人数、MAC アドレスなどです。ベースユニットウェブインタフェースの「デバッグロギング」にチェックを入れると、現在共有しているユーザーの名前も記録されます。どんな場合でも、パスワードではなく、スクリーンからもデータや音声のキャプチャー、パスワード、それ以外のいかなる機密データも、ログファイルで再現されることはありません。

3.7 第一世代 ClickShare 製品との相互運用性は？

現在の顧客が現在の ClickShare の設置基盤（インストールベース）を拡張できるように、CSE-xxx ユニットならデフォルトで第一世代の ClickShare 製品と対話できます。というのも第一世代のセキュリティはレベル 1 だからです。セキュリティレベルがレベル 2 ないし 3 に変わると、第一世代製品はデバイス証明書がないために認証された通信ができないために互換性は崩れます。

4. 最後に

第二世代の ClickShare コラボレーションシステムはセキュリティが大幅に改善されています。しかも CSE レンジの ClickShare はクラス最高のセキュリティを誇り、三段階のセキュリティレベルが設定されています。 バルコはセキュリティ機能の設計と実装に努力を払っており、バックドアや隠れ転送がこれまで一切実装されていないことを保証します。

さらなるご質問や脆弱性のご報告などは clickshare@barco.com までご連絡ください。