L-019

SDN を用いたクラウド型暗号/復号システムの構築
Cloud type encryption / decryption system using SDN

木綱 啓人† 安部 則孝‡ 佐藤 裕幸†
Hiroto Kizuna Noritaka Abe Hiroyuki Sato

1. はじめに

昨今，コンビニや大型量販店など主要な店舗では Suica など各種非接触 IC カード(以下，IC カード)を用いた決済が可能であり，これら決済可能な店舗及び IC カードの種類と共に増加傾向にある．また，買い物の決済だけではなく，特定地域内で利用できるポイントカードやクローズドマネー等，情報を勝手に改竄，盗聴されないセキュアな情報保持デバイスとして利用される事例もある[1].

この事例でも利用されている FeliCa Pocket 媒体である IC カード内情報の更新手順を説明する．IC カードを認証端末が検知すると，ポケットと呼ばれる各サービス情報をセキュアに保存する領域から暗号文の読み出を行う．暗号文を複合するために SAM(Secure Application Module)と呼ばれるアクセス鍵を用い復号化し情報を更新し，再度暗号化を行い，同一ポケット領域へ書き込むことで更新が完了する．この認証端末は店舗などに SAM と共に設置されており，盗難により端末内のメモリ上に展開されたアクセス鍵が流出する可能性がある．その対策として，HSM(Hardware Security Module)が存在する．これでは複数アクセス鍵と専用の暗号/復号化チップを物理筐体へ格納し，データセンタのようなセキュアな場所で集約管理/運用することで盗難によるアクセス鍵流出を防止することができる．しかし，HSM は非常に高性能かつ高価であり，なおかつ専用チップにより実装され数千端末からの大量のトランザクションを安定して処理する必要のある用途に向く．よって，前述のような地域で活用されるポイント/クローズドマネーサービスには，導入規模及びコスト面から適していないといえる．そこで HSM のように暗号文をサーバへ転送し，SAM による暗号複合処理を行うソフトウェア実装が考えられる．しかし，複数の認証端末から同時にトランザクションを受けることが想定され，複数の SAM に対して処理をディスパッチしつつすすめる必要があり，非常に複雑な実装が想定され，実装やテスト，保守など導入から運用までのコストが非常に高い．

本研究では，複数認証端末からのトランザクションをサーバ内に SAM が紐付いたコンテナ(以下，SAM サーバ)を複数用意し，SDN 技術により外部からの認証パケットをトランザクション未実行中な SAM サーバへ動的に転送することで認証を完了するシステムを構築する．これにより，各 SAM サーバは単一の復号/暗号処理を行うことで認証が完了するため，シンプルな構成でありながらアクセス鍵をセキュアに集中管理することが可能となる．

2. SDN(Software-Defined Networking)

従来のネットワーク機器で行われていた送受信端末間の最短経路を算出する等の機能を固定されたプロトコルにより実現し，自律分散的動作をする．SDN では個々の機器同士で協調するだけではなく，ドメインネットワークに於ける様々な情報を包括的に把握/管理することで，より高度なパケットフローを実現する．SDN の定義をプロトコルとして実装したもので最も有名な OpenFlow[2](以下，OF)がある．これは主に図 1 のように基本的なパケット転送を行う OF Switch(以下，OFS)とその転送経路を決定する OF Controller(以下，OFC)の 2 つの機能間でのプロトコルを定めるものである．これにより OF 上で動作するアプリケーションはパケット転送制御などを考慮することなく，経路選択制御の実装を可能とする．OFS では FlowEntry によるパケットフローを静的に記述できる．また，OFC ではより詳細な情報をもとにした条件分岐によるフロー制御やパケット流量などの統計情報を取得する際に用いられ，動的で柔軟な解析と制御を可能とする．本研究では，OF のライブラリ実装である Ryu[3,4]を用いて開発する．

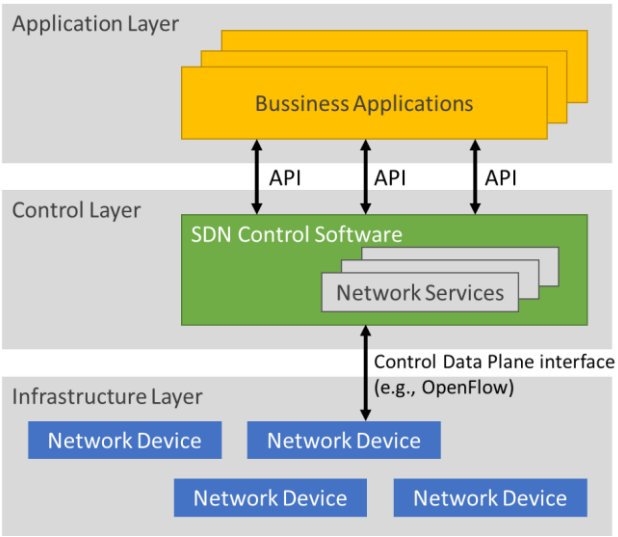

図 1 OpenFlowProtocol

3. システム概要

本システムの構成を図 2 で説明する．SAM を USB リーダによりホストサーバへ接続し，各 Docker コンテナに紐付ける．各コンテナとゲートウェイ間は OF Switch により接続され，OFS 越しに SAM サーバへパケットを転送することで認証を行う．

SAM サーバは単一の認証トランザクションを実行するため認証中は他の認証を割り当てることが出来ない．多数の認証トランザクションを各 SAM サーバへ割り当て，認証終了後 SAM サーバを解放することで実現する．本システムにおいて処理する事項は，TCP コントロールビットなどから状態に応じた SAM サーバの割り当て/開放処理，受理したパケットの宛先または送信元 IP 書き換え，転送を行うことが考えられる．

TCP コネクションを適切に転送するためには，クロージングシーケンス等通信の状態遷移を解析/把握することが不

†岩手県立大学大学院ソフトウェア情報学研究科
‡株式会社イイガ

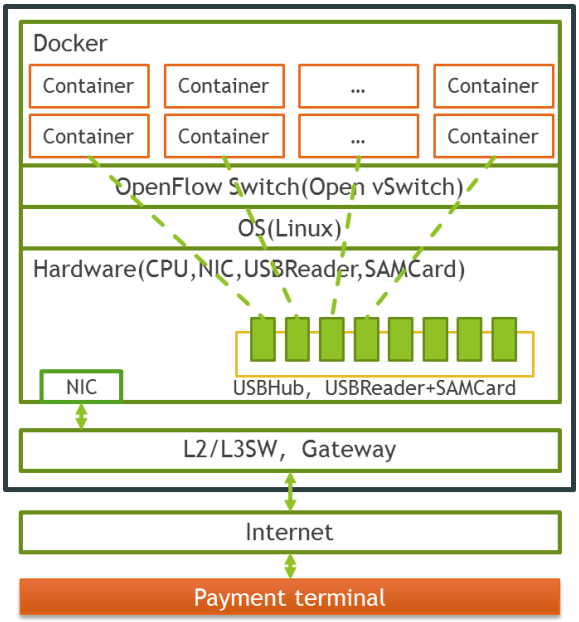

図 2 認証システム構成図

可欠である．これらシーケンスの完全な解析は OFS の FlowEntry では完結しない．よって本実装では，すべてのパケットを OFC へ転送し TCP コネクション状態をトレースによる制御，TCP コネクション確立後に FlowEntry によるデータパケット転送を行う 2 つの方式による実装を行った．以下に 2 方式の実装詳細を記載する．

3.1 OF Controller による全パケット転送

TCP コネクションの接続状態を把握するには IP/MAC アドレスやポート番号，確認応答/シーケンス番号及び状態遷移用のコントロールビット等，OSI 参照モデルに於ける 2-4 レイヤの情報が必要となる．本方式では OFC による全パケットの転送を行う． TCP コネクションの状態は大きく，接続要求，接続確立，データ送受信，接続断要求，接続断完了の 5 状態が考えられる．接続要求及びその接続許可はいわゆる 3way hand-shake であり，前者はパケットのコントロールビットの Syn で検知できる．後者は Syn に対する Ack であるかを照合する必要があるため，各状態遷移時に確認応答/シーケンス番号をシステムで保持/更新を行うことで対応した．これらにより TCP コネクションの特定とその状態を把握することが可能となる．

OF ではすべてのパケットを OFS が受理後，FlowEntry 内で経路が定義されていればそのままパケットの送出が可能である．もし FlowEntry 内に経路が未定義であればそのパケットを OFC へ転送(Packet-In)し，経路を決定する．本システムに於ける認証パケットを OFC が Packet-In した後，前述の方法により転送先を特定し，端末から SAM サーバへのパケット転送であれば転送先 IP/MAC アドレスを書換え後，SAM サーバへ送出することで処理を完了する．

3.2 FlowEntry を用いたパケット転送

3.1 ではすべてのパケットを OFC へ転送，解析した後，その送出を行っている．しかし，OFS 内の FlowEntry による転送時間に対して OFC によるその時間は比較的大きく，できるだけ FlowEntry によるパケット経路制御を行うことが望ましい．しかし，本システムに於けるパケット経路制御には前述の通り，SAM サーバ資源の稼働率を上げるためにも TCP コネクションの接続状態を把握した上で即時割り当て/開放することが重要である．使用する OFS は OF Protocol の v1.3 までが利用可能である．OF v1.3 における FlowEntry により抽出可能なヘッダレイヤは L3 までであり，L4 の TCP ヘッダのコントロールビット等を抽出できない．そこで，最初の 3way hand-shake のみ OFC へ転送し，コネクション確立が確認されると同時に FlowEntry へ特定のコネクションを転送するためのフローを投入することで，データ転送状態のパケットを高速に送出することができる．しかし，その場合コネクション終了の Fin パケットを OFC が検知できないため終了判定できない問題がある．そこで，決済端末が処理を終えた後システムの処理終了通知 API により終了判定を行うこととした．

以上の実装を行うことで FlowEntry によるコネクション転送を実現した．

4. 性能検証

3 章で述べた 2 方式により，SDN 技術と複数の SAM サーバの組み合わせにより，クラウド型暗号文の暗号/復号化を行うシステムを実現した．また，実際に決済端末からの認証速度を検証する．検証対象としては，決済端末-本システム-SAM サーバを利用し，3 章の 2 種類の方式による認証速度の評価を行う．認証システムは東京に設置され，認証端末は専用の組み込み端末向けに実装されたアプリケーションを利用している．

本システムを 3.1 のすべてのパケットを OFC による転送を行う方式及び，3.2 の FlowEntry を利用した方式により実用的な認証速度を達成することが出来た．今後詳細な転送計測を行う．

5. おわりに

以上， SAM とコンテナが 1 対 1 で対応したシンプルな認証サーバとインターネットとサーバ間のパケット転送を制御する OFS 及び OFC でよるディスパッチ処理により SAM とソフトウェアルーティングによる認証システムを実現した．

今後の展望としては，IC カード認証用の SAM カードだけでなく，その他のセキュリティデバイス等を、IoT 等デバイスコストや物理制約の多いデバイスに対して、本システムを利用することで、物理的にセキュリティデバイスを実装、接続することなく認証に利用するなど，汎用的に転用したシステムを構築していく．

参考文献

[1] FeliCa Pocket Marketing, http://www.felicapocketmk.co.jp/ FeliCapocket, FeliCa Pocket Marketing, 2016/1.
[2] Ben Pfaff, Bob Lantz, Brandon Heller, Casey Barker, Curt Beckmann, et al., OpenFlow Switch Specification Version 1.3.0, June 2012.
[3] Ryu component-based software defined networking framework, https://osrg.github.io/ryu/
[4] 久保 類, 藤田 智成, et.al., “Ryu SDN Framework —オープンソースの SDN 基盤ソフトウェア, NTT 技術ジャーナル(2014).