urandom

Computer Security Magazine

vol.10

TPM通信の観察 op

urandom出版システム2022 mayth

目次

TPM通信の観察

1 はじめに

コンピューターに求められるセキュリティ要件は年々厳しくなりつつあり、それと相まって、その厳しい要件を達成可能にする技術が登場し続けている。そのうちの一つがTrusted Platform Module（TPM）である。TPM は Trusted Computing Group（TCG）[*1]が仕様を策定するコンポーネントで、暗号計算・署名計算・完全性検証などの機微な処理を、計算機の他の部分と分離された環境で実行するためのものである。Windows 11 ではシステム要件[*2]で TPM が必須になるなど、TPM は既に広く普及しており、今後もコンピューターセキュリティにとって重要な要素であり続けると考えられる。

セキュリティにおいて重要な役割を担う TPM は必然的に関心の対象となる。一方で、一般の草の根的なコンピューターセキュリティのコミュニティでは、TPM についての情報があまり豊富ではないように思われる。そこで、この記事では TPM の調査・研究の最初のステップとして、実世界のユースケースで TPM に入出力されている通信を観察した事例を紹介する。

2 参考資料

この記事で紹介する内容は TPM 通信の観察に留めることとし、通信の内容に関して詳しい調査は行わない[*3]。不明点については次に示す資料などを併せて確認すること。

TPM 2.0 Library | Trusted Computing Group

`https://trustedcomputinggroup.org/resource/tpm-library-specification/`

TCG PC Client Specific TPM Interface Specification (TIS) | Trusted Computing Group

`https://trustedcomputinggroup.org/resource/pc-client-work-group-pc-client-specific-tpm-interface-specification-tis/`

[*1] Trusted Computing を推進する非営利団体。Intel、AMD、Microsoft、Google などが構成員。

[*2] `https://www.microsoft.com/ja-jp/windows/windows-11-specifications`

[*3] 紙面的・時間的制約による。

A Practical Guide to TPM 2.0
: https://library.oapen.org/handle/20.500.12657/28157

Linux TPM2 & TSS2 Software
: https://github.com/tpm2-software

Official TPM 2.0 Reference Implementation (by Microsoft)
: https://github.com/microsoft/ms-tpm-20-ref

3 準備

3.1 観察対象

TPM 通信を観察する対象の環境は次の構成とした。

CPU
: Intel Celeron Processor G5905

Chipset
: Intel B560 Chipset

TPM
: Discrete TPM w/ SPI bus (TPM 2.0)

ファームウェア
: TPM と UEFI のファームウェアは執筆時点[*4]の最新版

Windows
: Windows 11 Build 22621

Linux
: Ubuntu 22.04 LTS, Kernel version 5.15.0-25, Clevis version 18

3.2 検証機材

TPM 通信を観察するために使用した機材とソフトウェアは次の通り。

ロジックアナライザー
: Saleae Logic Pro 16

デコーダー

[*4] 2022/12/19

urandom出版システム 2022 Edition

1　はじめに —— 出版システム暗黒時代

C91（2016 年 12 月）で頒布した urandom vol.3[*1]にて『urandom 出版技術部活動報告』という記事を書きましたが、それから 6 年も経ちました。その間、システムは順調に稼働し続けていたのかというとそうではありません。

2020 年から C99 が開催される 2021 年 12 月までの約 2 年間、urandom は新刊を作っておらずこれらの出版システムは完全に放置されていました。C99 で当選してスペースを頂き、さて記事を書いてビルドするか、となったとき、Jenkins は完全に沈黙していました。2 年も放置された執事は完全に腐乱死体となっていたのです……。

TeXLive も Docker 化していたわけですが、2020 年にはなかった Apple M1 アーキテクチャーの登場に追従できておらず、M1 Mac ではコンパイルできない状況となっていました。そのためメンバーのマシン上（M1 Max MacBook Pro, 2021）での Docker を用いたビルドが不可能になっていました。ビルドサーバーは x86_64 ですがそのサーバーでは今度はビルドシステムが動いてない。そうこうしているうちに締切をぶっちぎって無事キンコーズ出版と相成ったわけですが、前日夜になって某キンコーズ横の路上でギリギリまで構成や組版修正を行い、マシンに直接 TeXLive + Pandoc の環境を構築して手動コンパイルした PDF データを印刷するという vol.1 時代の出版システムへ無事に退化しました。

そして記念会となった C100 にも urandom はめでたくサークル参加しますが、このときにもまだ出版システムは復旧しておらず、結局はメンバーのパソコンでコンパイルするという状況が続きます。

今回の C101 でそのような状態から脱出し、出版システムを復活させて記事を書こう、というのが今回の記事の趣旨です。とはいったものの、結局スケジュールはかなり逼迫しており、行き当たりばったりの調整を繰り返しながら成果をこの記事にしているという状態なので、色々とゴミがあったり逆に不足（説明が足りないという意味も、設定が足りないという意味も含む）があったりするかと思いますが、右往左往した様を想像しながら温かい目で見て頂ければと思います。

[*1] https://urandom.team/books/urandom-vol3/

2 システム構成

ソースコード（記事や PDF を生成するビルドスクリプト等）の管理には GitBucket[*2]を使用しています。GitHub のプライベートリポジトリも数は無制限に使えるようになったのですが、特に移行せずに使っています。ここはもしかすると今後移行するかもしれません。

CI システムは Jenkins[*3]を採用しています。いくつか他のものも試してみましたが、Docker や k8s を使わずごくシンプルな構成で使う分には Jenkins が一番楽に思えます。とは言いつつ結局様々な問題を踏むのですがそれは後ほど。

次にサーバーの話をします。以上のソフトウェアはさくらの VPS[*4]の 2G プランを契約して運用しています。2G プランだとスペックは 3vCPU、メモリ 2GB、ストレージは SSD 200GB[*5]です。vol.3 時点では Fedora をインストールしていましたが、現在は Ubuntu 22.04.1 LTS（Jammy Jellyfish）を使用しています。また、以前はビルド用の Mac mini を mayth 宅に用意して VPN を通してこのサーバーと接続していましたが、このビルドマシンは廃止しました。

3 システムの構築

それでは、前記のソフトウェアをサーバー上にセットアップするところを説明していきます。vol.3 時点との差分を述べていますが、基本的にはこの記事だけ読んで何をしたのかは分かるようになっています。

前回からの大きな違いは、個別に Dockerfile や設定ファイルを用意して `docker run` をするのではなく、Docker Compose を使うようになった点です。以降の説明では `docker-compose.yml` を説明対象のサービスの部分のみ切り取って紹介しますが、実際には全て 1 つの `docker-copmose.yml` に記述されていると思って見てください。

3.1 GitBucket のセットアップ

vol.3 時点ではかなりミニマルな構築をしており、GitBucket が使用するデータベースは組み込みの H2 データベースを使っていました。この辺りをもう少し真面目に運用するにあたって、Docker Compose のサービスとして DB サービスを追加することにしました。

[*2] `https://gitbucket.github.io/`

[*3] `https://www.jenkins.io/`

[*4] `https://vps.sakura.ad.jp/`

[*5] 現在新規で契約するとデフォルトで 100GB、有料オプションで 200GB ですが、このサーバーは旧 HDD プランからのアップグレードのため料金据え置きで 200GB の契約になっています。不利益にならないように措置してもらって有難い限りです。

urandom vol.10

発行者	urandom
表紙デザイン	秋弦めい
発行日	2022 年 12 月 31 日
バージョン	1.00
コミット ID	c8d76d2
連絡先	https://urandom.team/
印刷所	株式会社ポプルス

urandom

•ω•

presented by urandom

Comic Market 101 (Dec. 31st, 2022)