TRUSTED COMPUTING GROUP

TCG 設立 25 周年記念・TCG 日本支部(JRF)公開ワークショップ（第 14 回）

次世代サイバーセキュリティへの TCG のチャレンジ

～Security by Design with TCG Technology ～

概 要 OVERVIEW

日時: 2 月 29 日(木)13:00～20:00（受付 12:30）

主催: Trusted Computing Group 主催、TCG 日本支部(JRF)企画

会場: ヒルトン東京(新宿区西新宿 6 丁目 6 番 2 号) 3 階 藤の間 1･2･3

対象: TCG 会員および、情報セキュリティに関わる開発者、利用者、政策関係者および TCG の活動･技術にご興味をお持ちの方

定員: 100 名

概要: “TCG Remote Attestation”技術のサイバーセキュリティ利用について理解を深め、意見交換を行い、今後の TCG 技術の応用や向かう先について考察する。

詳細: https://bit.ly/tcg-jrf-2024

プログラム AGENDA

時間(JST)	内容 （同時通訳 ； 敬称略）
13:00 - 13:20	**開会の挨拶:** 安藤 万理江 TCG 日本支部共同議長; ST Microelectronics **歓迎の言葉: TCG 創立 25 周年メッセージ** Joe PENNISI, TCG President & Chairman; NVIDIA （ビデオ） Stephanie SCHULTZ, TCG Executive Director
13:20 - 14:10 (QA 5mins)	**基調講演: サイバーセキュリティにおける脅威動向と JPCERT/CC の取り組み** 堀 充孝 一般社団法人 JPCERT コーディネーションセンター(JPCERT/CC) 早期警戒グループ 脅威情報アナリスト
14:10 - 14:55 (QA 5mins)	**講演#1: TCG Attestation Framework と IETF Remote Attestation 手順:TCG と IETF Attestation WG の概要** Ned SMITH, TCG Attestation WG チェアー; Intel
14:55 - 15:05	休憩 （葵）
15:05 - 15:50 (QA 5mins)	**サプライチェーンセキュリティの最前線:ハードウェアセキュリティ技術による Remote Attestation, Platform Certificate の解説** 小林 宰 TCG 日本支部メンバー; NEC
15:50 - 16:20 (QA 5mins)	**講演#2: デバイス ID 及び Attestation のための TCG 技術の概要** Guy Fedorkow, TCG Technical Committee Member and Editor; Juniper Networks
16:20 - 16:30	休憩 （葵）
16:30 - 17:15 (QA 5mins)	**ライトニングトーク: Google 社における Remote Attestation の取り組み** **講演#3: TCG の耐量子計算機暗号(PQC)ビジョン** Chris FENNER, TCG TPM WG Chair; Google
17:15 - 17:45	**座談会: 次世代サイバーセキュリティへの TCG のチャレンジとは？**
18:00 - 20:00	**デモンストレーション、ネットワーキング(軽食/ドリンク提供)**
	Remote Attestation のデモの実演 TCG 日本支部メンバー; NEC チーム
20:00	**閉会**

※プログラムは、予告なく変更もしくは内容を変更する場合があります。(更新:2/26/2024)

TRUSTED® COMPUTING GROUP

講演詳細 SESSIONS & SPEAKERS

堀 充孝 / *Mitsutaka HORI*
一般社団法人 JPCERT コーディネーションセンター(JPCERT/CC)
早期警戒グループ 脅威情報アナリスト

堀氏は、製造業の社内 SE やベンチャー企業でのシステム開発などを経て、2017 年 9 月、JPCERT コーディネーションセンター制御システムセキュリティ対策グループに着任。主に制御システムセキュリティに関する脅威情報や脆弱性情報などの収集・分析、情報発信業務などに従事。2024 年 1 月から、早期警戒グループにおいて早期警戒情報や注意喚起などの情報発信業務に従事。また講演等、普及啓発活動にも取り組んでいる。

講演内容：サイバーセキュリティにおける脅威動向と JPCERT/CC の取り組み

IoT 技術の広がりとともに、インターネットに接続されたソフトウェア製品はますます増加しており、近年においてはこれらの製品の脆弱性を突いた攻撃が初期侵入経路として利用されるケースが相次いでいる。本セッションでは、近年におけるサイバーセキュリティの脅威動向や課題について説明しながら、直近の事案対応なども含む JPCERT/CC の取り組みについて紹介する。

ネッド・スミス / *Ned SMITH,*
TCG Attestation WG チェアー;
Principal Engineer, Security Privacy Mitigation Team
Intel Corporation

スミス氏は、インテル社の Security Privacy Mitigation Team Principal Engineer。Internet Engineering Task Force (IETF) における Remote Attestation Procedures (RATS) Work Group および Trusted Computing Group (TCG)の Attestation Work Group の共同議長を務める。また、TCG の DICE 標準(Device Identity Composition Engine)Family の主要寄稿者であり、発案者でもある。

講演内容： TCG Attestation Framework と IETF Remote Attestation 手順： TCG と IETF Attestation WG の概要

“Trust”と”Attestation”は、クラウド、エッジ、および分散コンピューティングにおいて注目を集め、その重要性が高まっている。プラットフォームにおける Attestation 機能とクラウド、エッジ、および IT エンタープライズ内の Attestation サービスは、コストを最小限に抑え、技術の拡張を最大限に広げるために、相互運用が必要とされる。多くの標準規格が積極的に Attestation 技術を定義しているが、相互運用性は保証されていない。本講演では、TCG の Attestation および IETF（Internet Engineering Task Force）の Remote Attestation Procedures（RATS）WG での取り組みについて双方でのチェアをつとめる Ned Smith が双方の技術の概要を説明する。

© 2024 Trusted Computing Group
3855 SW 153rd Drive Beaverton, Oregon 97003 USA | Phone: +1 503-619-0562 (USA) | Fax: +1-503-644-6708 | www.trustedcomputinggroup.org

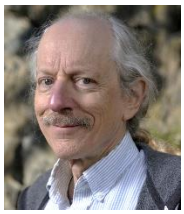
小林 宰 / *Tsukasa KOBAYASHI*
TCG 日本支部メンバー;
日本電気株式会社
テクノロジーサービスソフトウェア統括部 ディレクター

小林氏は、入社以来、通信系組み込みソフトウェア開発、無線通信技術開発、IoT セキュリティ領域の製品開発を担当し、現在はトラストサービスのビジネス開発に従事。昨今は Trust Computing Group（TCG）日本支部（JRF）が主催するイベント等で、TPM やその他 TCG 技術の社会実装や普及に向けて活動を展開する。

講演内容：サプライチェーンセキュリティの最前線：ハードウェアセキュリティ技術による Remote Attestation、Platform Certificate の解説

近年、グローバルなサプライチェーンのリスクが急速に増加しており、その対策が喫緊の課題となっています。この背景を受けて、TCG や IETF ではコンピューティングデバイスのサプライチェーンリスクに対応するための国際規格やガイドラインの整備が進められています。

今回、サプライチェーンセキュリティを具現化する技術である、RFC9334 RATS (Remote Attestation Procedures)や TCG Platform Certificate について、その概要や仕組みを、デモの説明を交えてご紹介します。本技術はハードウェアセキュリティ機能を実装したコンピューティングデバイスの安全性を、サプライチェーンを通して検証可能とする技術であり、効果的なセキュリティ対策を目指す企業にとって、大変興味深い内容となっています。



ガイ・フェドルコウ / *Guy FEDORKOW*
TCG Technical Committee Member and Editor;
Distinguished Engineer, Juniper Networks

フェドルコウ氏は、マサチューセッツ州ケンブリッジの Bolt, Beranek and Newman 社、シスコシステムズ社、ジュニパーネットワークス社で通信および高スループット並列コンピュータアーキテクチャーの開発に携わり、数多くの通信製品のシステムアーキテクトとして活躍。 現在、ジュニパーネットワークスでは、インフラストラクチャセキュリティとコンピューティングの信頼性にに関わるプロジェクトを担当し、トラステッド・コンピューティング・グループと IETF の活動を担当している。

講演内容：デバイス識別及び Attestation のための TCG 技術の概要

本講演では、 重要なシステムの安全性を確保する上で、「Roots of Trus」がどのように重要な役割を果たしているかを考察する。また、TCG で現在開発されている 3 つの異なる Root of Trust 技術である TPM、MARS、DICE についても紹介する。

© 2024 Trusted Computing Group

クリス・フェナー / Chris FENNER
TCG TPM WG チェアー;
Software Engineer, Google

フェナー氏は、現在 Google で使用されている at-scale のデータセンターattestation systems に携わるソフトウェアエンジニア。TCG の TPM（Trusted Platform Module）ワークグループの共同議長を務め、TCG の将来の標準バージョンでポスト量子脅威モデルに対応するための取り組みを主導している。

講演内容：ライトニングトーク: Google 社における Remote Attestation の取り組み

TCG の耐量子計算機暗号(PQC)ビジョン

耐量子計算機暗号(PQC)問題は、ユーザーにとって機器に組み込みこまれた（すなわち、ハードウェアまたはファームウェアで実装されアップデートができない）暗号化機能の顕在化しつつある脅威のひとつである。私たちは、今後数年間に製造されるデバイスが、現在の暗号の解読が可能となる量子コンピュータが利用可能になった時（一部の専門家によれば、早ければ 10 年後）にもまだ使用されている可能性があると予想しています。本講演では、量子コンピュータが古典暗号に与える影響の概要と、アプリケーション開発者が Store Now, Decrypt Later のような脅威にどのように対策を始めるべきかについて説明する。

なお、ライトニングトークでは、グーグルの TPM ベースのデータセンターAttestation Solution の概要と、その過程においてチームが克服したいくつかの課題について概説する。

永田 篤志 */ Atsushi NAGATA*
TCG 日本支部メンバー;
日本電気株式会社
マリタイムセキュリティ統括部　テクニカルエキスパート

永田氏は、日本電気株式会社(NEC)のテクニカルエキスパートとして、ゼロトラストセキュリティシステム開発チームを率いる。コンピュータシステムおよびネットワーク製品の開発に 17 年の経験を有する。

デモ概要： TPM は、TCG によって標準化され、多くの組織や企業の持続的な努力を通じて、その普及および活用が進んでいます。セキュリティの基本原理である信頼の基点（Root of Trust）およびシステム間の信頼関係（Chain of Trust）を確保する技術として、IETF により Remote Attestation の規格が昨年策定されました。TPM を活用してリモートアテステーションを行うことは、システム全体のセキュリティを強化するための効果的なアプローチとして、近年注目されています。本セッションでは、TPM を搭載した x86 ベースのサーバ、ラップトップ、デスクトップから、ARM ベースの小型コンピューターに至るまで、様々なアーキテクチャのコンピューターが Remote Attestation を用いてどのようにセキュリティの検証が可能であるかについて、デモンストレーションを行います。さらに、リモートアテステーションを利用したシステムが、より強固なネットワークアクセス環境を実現するための、近い将来の実装可能性についても探求します。

© 2024 Trusted Computing Group

富田 亨 / *Toru TOMITA*
TCG 日本支部メンバー;
株式会社サイバーディフェンス研究所
技術統括部長

富田氏は、ICT 分野におけるサプライチェーンセキュリティの向上を目指し、他の TCG メンバーと協力して、OpenSSL で TCG プラットフォーム証明書を利用可能にする機能拡張に取り組んでいる。この取り組みによって、TCG プラットフォーム証明書の核心技術である RFC 5755 に準拠した属性証明書を実装することで、利用者がデバイスの出所、真贋判定、変更の有無、およびトレーサビリティを容易に検証が可能となる。

■事前アンケート: https://forms.gle/QWPNVpRAe3dtmjay8

■資料ダウンロード先: https://bit.ly/3uztZaA（当日以降に準備が整い次第オープンします）

■お問い合わせ先: TCG-JRF ワークショップ運営窓口 TCG 事務局 (日本窓口) 重村
E メール: japan_admin@trustedcomputinggroup.org

© 2024 Trusted Computing Group