Ellisys Expert Note | EEN_BT06
Rev. B

Bluetooth セキュリティのウソ？ホント？

Bluetooth のセキュリティに関する誤解と事実

はじめに

Bluetooth のセキュリティは複雑で、しばしば誤解されています。また、誤った実装を行うと、たとえ優れた設計であっても商業的に失敗する危険性があります。Bluetooth が今日の最も一般的な無線規格の1つになったことで、Bluetooth 技術の実装者は、そのセキュリティ原則を理解することがこれまで以上に重要になっています。

Ellisys の Bluetooth アナライザは、エンジニアがセキュリティを含む広範囲な仕様要件へ準拠しているかを評価するために最適化されています。また、Ellisys のアナライザは、新たに発見された攻撃シナリオを理解したり、Bluetooth のセキュリティを回避する新しい方法を探したりすることに有効で、学術機関やその他の研究者が Bluetooth をより安全にすることを支援します。

このエキスパート ノートでは、誤解されがちな10個のセキュリティに関する噂を取り上げ、Ellisys アナライザのユーザーが、セキュリティがどのように実装に影響するかを理解できるようにします。

以下の “ウソ？ホント？” テストを受けて、すべて正解できるかどうか確認してください。

ウソ？ホント？

1. バージョン 4.2 以降のすべての Bluetooth Low Energy 機器は、LE セキュアコネクションペアリングを採用しています。

   回答：ウソ！

   Bluetooth Low Energy デバイスは、LE セキュアコネクションペアリング（バージョン 4.2で導入）または LE レガシーペアリング（バージョン4.0で導入）を使用して接続を確立します。LE レガシー ペアリングでは、Short-Term Key (STK) を作成するためにTemporary Key (TK) が使用され、これは接続時の最初に、暗号化セキュリティキーを配布する目的で使用されます。LE のセキュア・コネクションでは、ECDH（Elliptic Curve - Diffie Hellman）暗号を使用して安全性の高い Long-Term Key (LTK) を作成し、この LTK は両方のデバイスで保持されます。

   ペアリングプロセスでは、機能情報の交換 (Features Exchange) シーケンスを使用して、両方のデバイスが LE セキュア コネクションのサポートを通知し、双方がサポートしている場合にはセキュアコネクションが使用され、そうでない場合は LE レガシーペアリングが使用されます。

   > ヒント: Ellisys社の解析装置は、LE レガシーペアリングの手順を解読し、無線トラフィックのみに基づいて STK を計算します。

ウソ？ホント？

2. Bluetooth セキュリティにおいて、下位互換機能は常に利用可能で、強制されています。

   回答：ウソ！

   FIPS モードとも呼ばれる “Secure Connections Only” モードでは、Bluetooth 機器は、このモードをサポートしていない機器との下位互換機能よりもセキュリティを優先します。このモードはホストによって強制され、ホストは Secure Connections が有効でない場合、接続試行を拒否することができます。この機能は、Bluetooth LE および BR/EDR (Secure Simple Pairing の拡張機能) で利用可能です。

ウソ？ホント？

3. Bluetooth 機器は一般的に、ペアリング時に最も攻撃を受けやすいと言われています。

   回答：ホント！！

   実際、Bluetooth デバイスは、重要な認証および暗号化プロセスが行われるペアリングプロセス中に最もよく攻撃されます。また、確立された接続時にも攻撃を受ける可能性がありますが、これはペアリング時の攻撃に比べ困難なため、一般的ではありません。

ウソ？ホント？

4. デュアルモードのデバイスでは、1つのペアリング手順で両方の通信用のキーを生成することができます。

回答：ホント！！

Cross-Transport Key Derivation（CTKD）と呼ばれる手順により、機器は（特定の状況下で）一度だけペアリングを行い、リンクキーの導出を一方の通信から他方の通信 (BR/EDR および Bluetooth LE) に共有することができます。これにより、ユーザーは2つの異なるペアリング手順を管理する必要がなくなり、利便性が向上します。

ウソ？ホント？

5. BR/EDR のピンコードのペアリングは安全ではありません。

回答：ホント！！

LE レガシーペアリングと同様に、この BR/EDR レガシーペアリング方法は、実際のセキュリティを提供するものではありません。SSP (Secure Simple Pairing) が導入される前ほど一般的ではありませんが、さまざまな新規開発機器や古い機器で使用されています。

ヒント：Ellisys のアナライザは、ピンコード（通常4桁）を自動的に判定し、数百ミリ秒以内に関連するリンクキーを推測することができます。

ウソ？ホント？

6. FHSS は、Bluetooth の攻撃者にとって強い障害となります。

回答：ウソ！

FHSS (Frequency Hopping Spread Spectrum) は、ISM バンドの干渉による Bluetooth 通信チャネルへの悪影響を軽減するのには有効ですが、攻撃者にとっては大きな障害にはなりません。ホッピングシーケンスは、中程度のハードウェアとソフトウェアを使って、すぐに習得することができます。

ヒント：Ellisys が開発した広帯域同時監視技術は、FHSS を完全に明らかにします。

ウソ？ホント？

7. LE レガシーペアリングでは、OOB（Out-of-Band）アソシエーション モデルのみがパッシブな盗聴から保護されます。

回答：ホント！！

実際、LE レガシーペアリングでは、”Just Works” と “Passkey Entry” の両アソシエーションモデルは受動的な盗聴の影響を受けやすいのですが、OOB 方式はこの種の攻撃に対して本質的に保護されています。LEセキュアコネクションでは、ECDH 暗号を追加することで、受動的盗聴に対する保護が追加されます。

ウソ？ホント？

8. SSP または LE セキュアコネクションが使用されている場合、アナライザは通信を復号化することができません。

回答：ウソ！

Secure Simple Pairing (BR/EDR) および LE セキュアコネクションでは、非対称公開鍵暗号方式を用いてセキュアなリンクキー (ECDH) を作成します。また、公開鍵と数学的に関連性のある秘密鍵も、公開鍵と秘密鍵のペアの一部として各デバイスに作成されるので、リンクキーの取得は困難です。リンクキーは無線で暗号化されていないため、監視装置でペアリングのトラフィックを記録するだけでは推論できません。

アナライザが監視（記録）しているホストコントローラインターフェース(HCI) 接続 (UART、SPI、USB など) でリンクキーが交換された場合、Ellisys ソフトウェアは自動的にキーを保持し、ユーザーの介入なしに適切なデバイスのペアに適用します。SSP のデバッグキーも同様に自動的に検出され、ユーザーの介入なしに適用されます。利用可能な場合は、SSP 秘密鍵を入力してローカルに保存することで、さらに使いやすくなります。

ウソ？ホント？

9. BIG（Broadcast Isochronous Group）では、暗号化はオプションです。

   回答：ホント！！

   BIG は、セキュリティモード 3、レベル 1、2、3 のいずれかを使用します。レベル2（未認証）およびレベル3（認証）では、ブロードキャスト コードを用いて、暗号化および復号化に必要な鍵を作成します。これらの鍵には、Group Long-Term Key (GLTK)、Group Session Key (GSK)、Group Session Key Diversifier (GSKD) が含まれます。レベル 1 には認証や暗号化はありません。

ウソ？ホント？

10. CIS（Connected Isochronous Stream）は、暗号化のために、関連する ACL で使用されているものと同じセッションキーを使用します

    回答：ホント！！

    ACL 接続のマスターは、ホストからの指示により、その ACL に関連付けられた CIS (Connected Isochronous Stream) を作成することができます。複数の CIS を同じ ACL に関連付けることができます。ACL が暗号化されている場合、関連するすべての CIS は暗号化されていなければならず、逆に ACL が暗号化されていない場合、関連するすべての CIS も暗号化されていないことになります。

おわりに

さて、あなたのスコアは何点でしたか？上記のすべてのトピックの正解を知っていた方は、次回のUPF イベントで Ellisys にご連絡いただければ、ビールまたはお好きな飲み物をご馳走します。いずれにしても、Bluetooth のセキュリティは包括的ですが、そのプロセスを学び理解した後は、実はそれほど複雑ではないということがお分かりいただけたと思います。また、Ellisys のプロトコル アナライザは、Bluetooth 関連の学習曲線と実装の課題を克服するのに役立ちます。

本文書について

本文書は、”EEN_BT06 - Better Analysis™ Reveals the Myths – Explains the Science (Rev. B Updated 2021-09)" を翻訳したものです。原文、本文書及び Ellisys 製品に関するお問い合わせは、Ellisys 日本総代理店ガイロジック株式会社 (0422-26-8211, es@gailogic.co.jp) までご連絡ください。
その他の翻訳版エキスパートノートは、https://www.gailogic.co.jp/db/bt/expert_notes をご覧ください。

Bluetoothプロトコル・アナライザ販売窓口　(ガイロジック株式会社)

0422-26-8211　@ **es@gailogic.co.jp**　**https://www.gailogic.co.jp/db/bt**