Secure Simple Pairing について

はじめに

PIN コードに基づいた最初のバージョンの Bluetooth ペアリングは、スニッフィングに対して本当のセキュリティを提供しませんでした。Ellisys Bluetooth Explorer 400 のようなスニッファは、ペアリング プロセスを傍受するだけで自動的かつ即座に PIN コードを検出しリンクキーを算出します。

Bluetooth がますます広範囲に使われるようになり、将来的な成功を保証するために安全なペアリング方法の技術が強い要求となりました。Bluetooth 2.1 仕様に含まれる Secure Simple Pairing (SSP) の発表で、それまでのペアリングにあった問題が解決され、Bluetooth デバイスのペアリングをそれまで以上にシンプルにしました。

より強固なセキュリティは、同時にBluetooth エンジニアに対する新たな挑戦を意味します。既製品のデバッグを、困難から不可能になります。しかし、物事は一般に考えられるほど悪くありません。この文書は SSP の基礎を解説し、Bluetooth コミュニティでよく見られるいくつかの誤解を明確にします。

ペアリング プロセス

デバイスのペアリングは、2 つの Bluetooth デバイス間でリンクキーと呼ばれる共通のシークレットキーを作成することを意図しています。そして、このリンクキーはお互いのデバイス認証や交換するデータの暗号化に使用されます。実際には、データはリンクキーを直接用いて暗号化されず、暗号化トラフィックの直前に交換されるリンクキーと乱数を用いて作られたテンポラリー暗号化キーを用います。そして、この暗号化キーは両方向のデータを暗号化するのに使用されます。それは、コネクションが有効な限りいつでも変えることができ、コネクションがクローズするか暗号化をやめるとすぐに破棄されます。

Bluetooth の仕様は 2つの標準ペアリング手順、LMP ペアリング （PIN コードベースとして知られているもの） と SSP を定義しています。標準でないペアリング方法も可能ですが、両方のデバイスが同じメーカーから提供される必要があります。どのようなペアリング方法も結果は同じで、共有されるリンクキーを作成します。

2つのデバイスが、一度同じリンクキーを持ったら、この共有シークレットキーが後の相互のデバイス再認証に使用されます。再接続の時、番号をそれぞれ交換し、デバイス双方が同じリンクキーを持っているか確認します。リンクキーが合致した場合、セッションキーの作成を続けることができます。そうでない場合、ペアリングプロセス（LMP ペアリングでも SSP でも）ちょうど新しいリンクキーを作成するのと同じように、かなり最初の部分から再開しなければなりません。

LMP ペアリング （PIN コードベース）

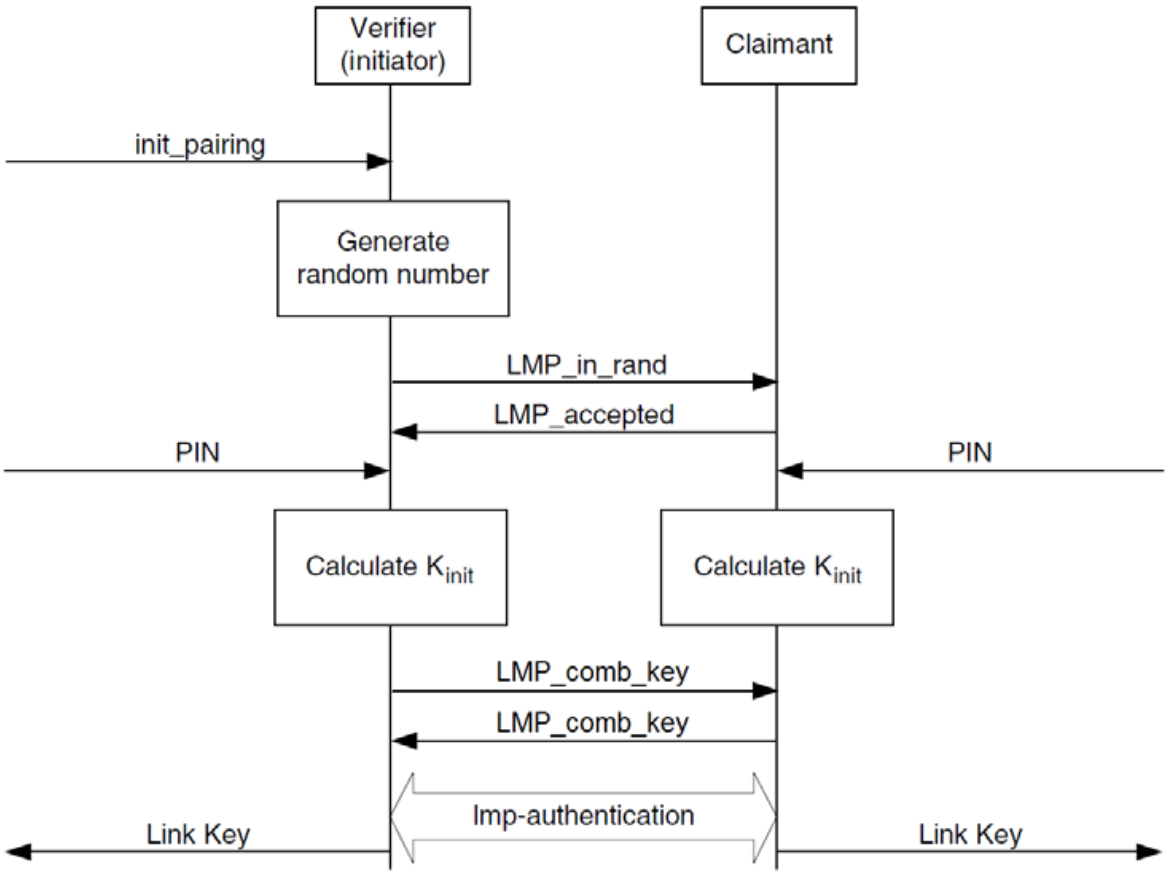
LMP ペアリング用のリンクキーを作成するために使用されるアルゴリズムに入力される手順

- 2つのデバイスの BDADDR
- イニシエーターが作成した 16 バイトの乱数
- 双方のデバイスで入力された PIN コード （ユーザーが変更できない固定 PIN コードを除く）

これらの番号は、最初にテンポラリー共有初期化キーを作成するのに使用され、その後キー生成手順を踏み LMP ペアリングで使用するリンクキーに変換されます。

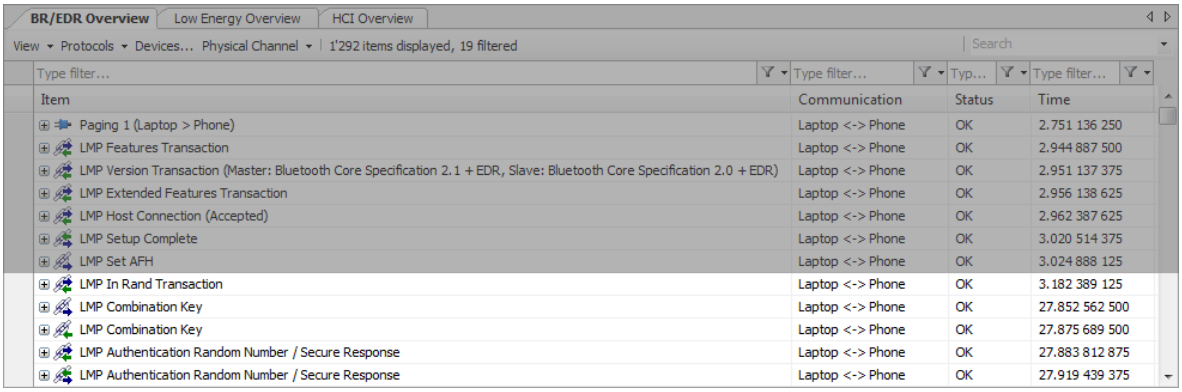
開示されていない唯一の情報は PIN コードですが、使用可能なシークレットリンクキーの数は使用可能な PIN コードの数に制限されます。4桁の PIN コードが使用されている場合、トラフィックを暗号化できるようになる前にアタッカーは最大でも10,000 の異なるリンクキーで試すだけです。これは、実際に存在する LMP ペアリングの弱点です。

以下のフローチャートで LMP ペアリング手順を説明します。

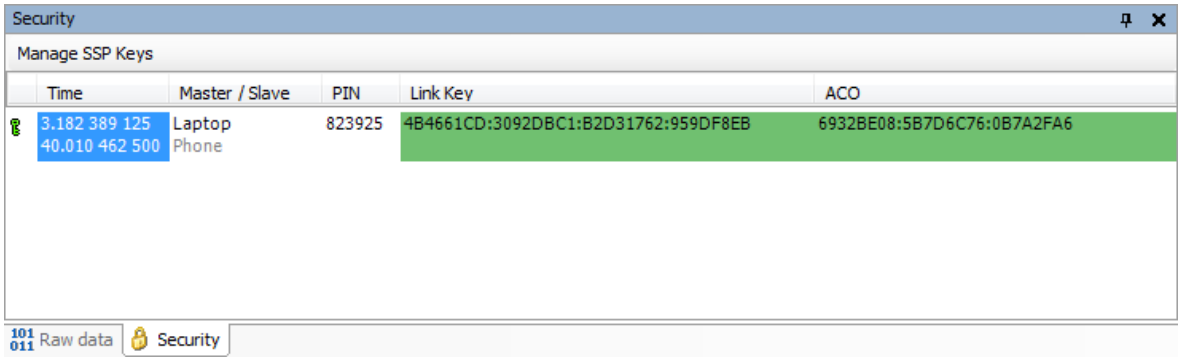


無線で送出されない情報は、PIN コードだけです。

下図は、Ellisys のスニッファでキャプチャされたトラフィックです。



キャプチャされた情報から、Ellisys のソフトウェは自動的に PIN コードを決定し、ユーザーの介在なしにリンクキーを計算します。下図は、Ellisys ソフトウェアの結果です。



この後、Ellisys ソフトウェアは以降のあらゆるセキュア接続のデータを自動的に復号化します。このプロセスは以降の Authenticated Connection （認証接続）の章で説明します。

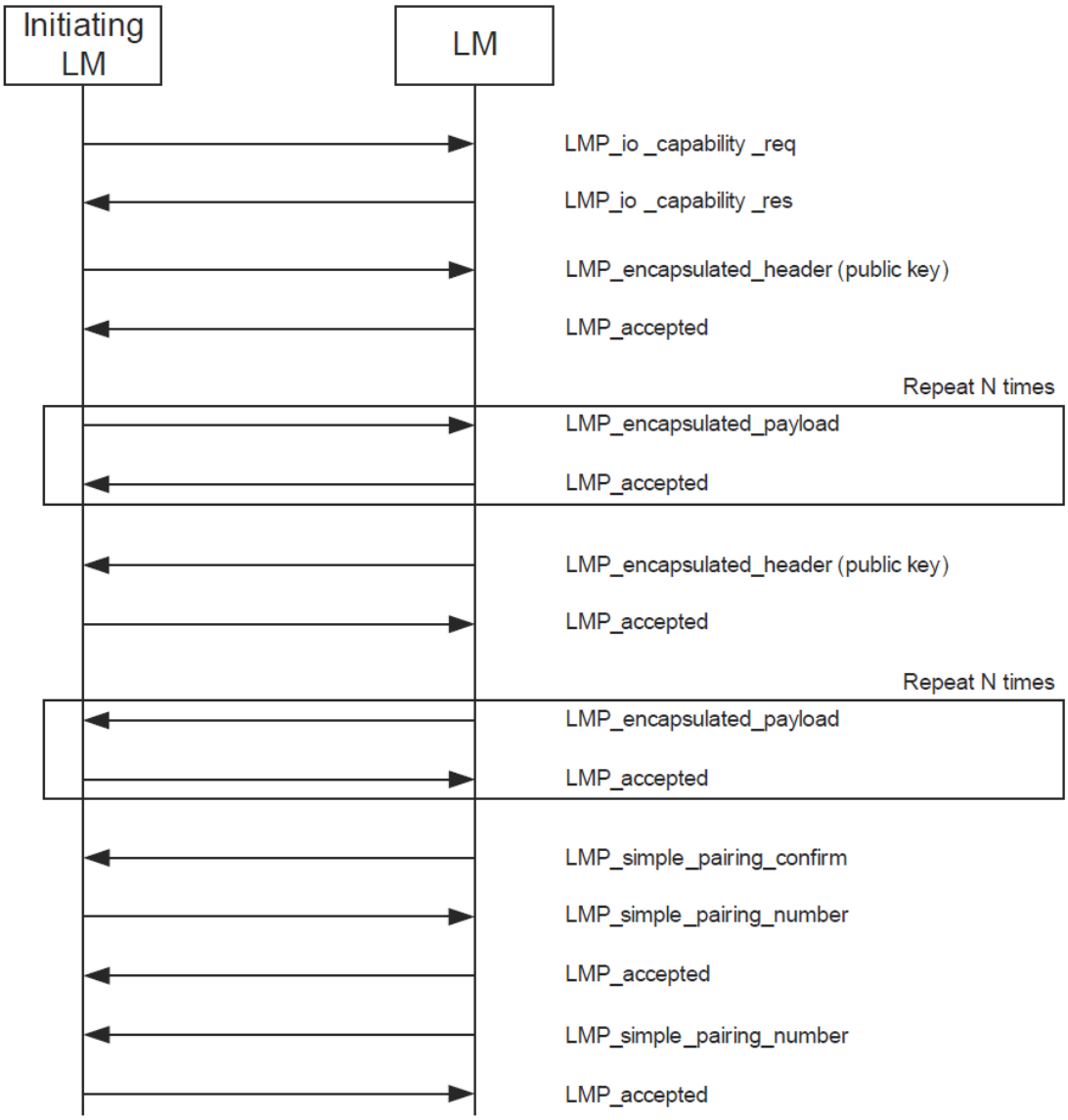
Secure Simple Pairing（SSP）

SSP は更により精巧なメカニズムを使用しています。楕円曲線暗号システムとして知られているもので、リンクキー計算プロセスの一部（PIN コードまたは他のユーザー番号は認証プロセスの一部で使用されます）で PINコードを使用することを回避し、リンクキーの計算には非常に大きな乱数を使用します。使用可能なリンクキーの数は現実的なアタッカーの能力を超え 2128 となり、もはや制限はありません。

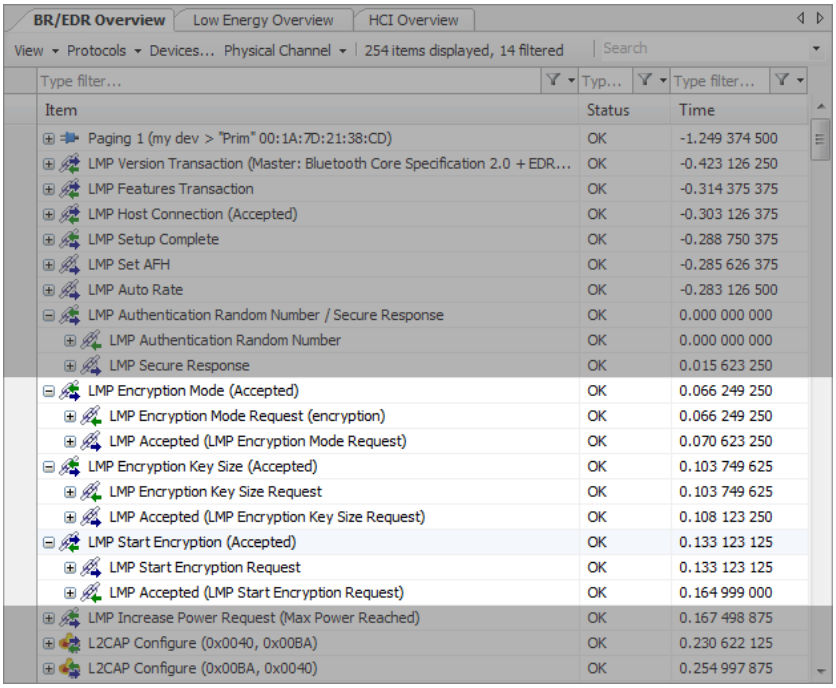
これを現実のものとするために、2つのデバイス間で異なる種類の共有シークレットキーを確立して SSP プロセスは開始されます。この共有シークレットキーは、Diffie-Hellman key (DHKey) として知られる 192ビットの乱数です。前提条件として、双方のデバイスがそれぞれプライベートキーとパブリックキーを持っています。パブリックキーは無線で飛ばされ誰でも見えますが、プライベートキーは決して公開されません。ここでは、これら 2つのキーを SSP パブリック/プライベートキーペアと呼びますが、これらは Diffie-Hellman Public / Private key pair（Diffie と Hellman の二人がこのアルゴリズムを開発）として知られているものです。

以下は SSP キーペアの作成で使用される、注意深く決定された数学的な内容とアルゴリズムです。

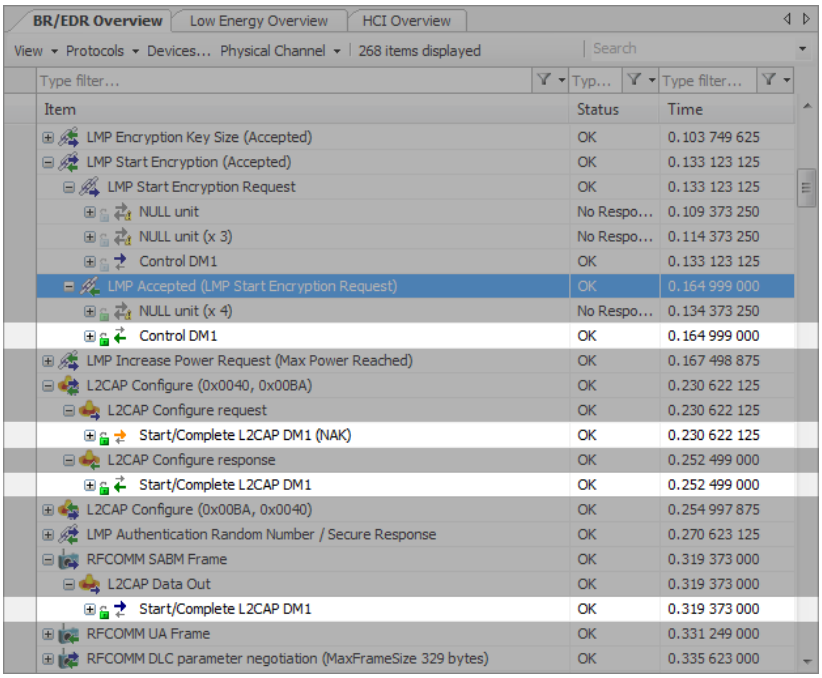
・パブリックキーを用いたプライベートキーの計算が（例え現在の最先端のコンピュータを用いても不可能）困難 （しかし、プライベートキーを用いたパブリックキーの計算は簡単）
・A と B の与えられた 2つの SSP キーペアはよく知られた関数 F、例えば F (Public A, Private B) =F (Public B, Private A) で表せます。この関数の結果が、DHKey です。2つのデバイスが、A と B を所有している時のみ同じDHKey を算出することができます。
このマジックが SSP の背後にあり、2つのデバイスは重要な情報を無線で送出することなく、また外部のメカニズム（例えばキーボードの入力）で情報を共有することもなくペアリングすることができます。DHKey はリンクキーの計算のために使用されます。残りのペアリングプロセスは、LMP ペアリングに似ています。SSP ペアリングプロセスを、以下のフローチャートで説明します。



下図は、Ellisys のスニッファでキャプチャされたトラフィックです。



パケットがMP_start_encryption リクエストの直後に暗号化されることに注目すると、MP_accepted ハンドシェークは既に暗号化されていて、これは非常に興味深いことです。以下のスクリーンショットは、どのパケットが暗号化されているかを表示しています。ロック アイコンが青い場合、これはパケットがプレーン（暗号化されていない）ことを意味します。ロック アイコンが緑の場合、これはパケットが正常に復号化されていることを意味しています。



おわりに

広帯域スニッフィングは、これまで不可能だったBluetoothのデバッグや相互運用性のテストを可能にします。広帯域スニッフィングは、よりエレガントなアプローチを提供し、ユーザーはすべてのパケットを即座に記録し、Ellisysアナライザソフトウェアアプリケーションの強力なフィルタリングを使用して、潜在的な問題を調査することができます。

詳細はellisys.comをご覧いただくか、es@gailogic.co.jp までご連絡ください。

本文書について

本文書は、″ EEN_BT07 - Secure Simple Pairing Explained (Rev.A Updated 2011-05)″ 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