リンクキーへのアクセス方法

はじめに

SSP (Simple Secure Pairing) が登場して以来、Bluetooth エンジニアは Bluetooth デバイスのデバッグにおいて新たな課題に直面しました。SSPは、エンドユーザーのペアリング作業を簡素化すると同時に、接続のセキュリティを強化しますが、アナライザが記録した Bluetooth トラフィックを復号化しようとする Bluetooth エンジニアにとっては、本質的な障害となります（もちろん、このような復号化を行おうとする人にとっては、このような障害の存在は承知の上です）。

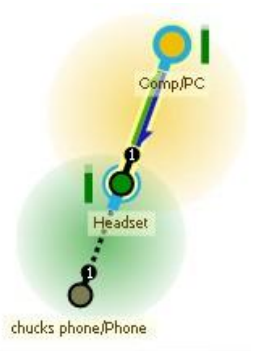
この課題の中心となるのは、リンクキーへのアクセスです。このドキュメントでは、このキーを見つけてアクセスするためのいくつかの方法を紹介します。Ellisys Bluetooth Explorer 400 アナライザは、リンクキーを事前に知らなくても、暗号化されたBluetoothトラフィックを記録することができるユニークな製品です。Ellisys アナライザを使用して記録された暗号化通信は、後に取得したリンクキーで復号化でき、Bluetooth 技術者はトラフィックの内容を完全に理解することができます。

リンクキーは 128ビットの乱数で、デバイス間で共有されますが、無線で送信されることのない秘密の値です。リンクキーはペアリングの際に作成、保存されますが、接続のたびに認証と暗号化キーの生成にも使用されます。リンクキーを作成するためのペアリング シーケンスの一部も暗号化されています。

リンクキーは、暗号化キーを生成するためのパラメータのひとつに過ぎません。SSPの仕組みについては、「？？？EEN_BT07 - Secure Simple Pairing Explained」を参照してください。

リンクキーは無線で送信されることがないため、Bluetooth エンジニアはこのキーにアクセスするためのさまざまな方法を知っておく必要があります。このエキスパートノートでは、これらの方法のいくつかを紹介します。なお、Bluetooth Low Energy (BLE) では、重要なキーの無線伝送が行われるため、少し事情が異なります。

キーコンセプト

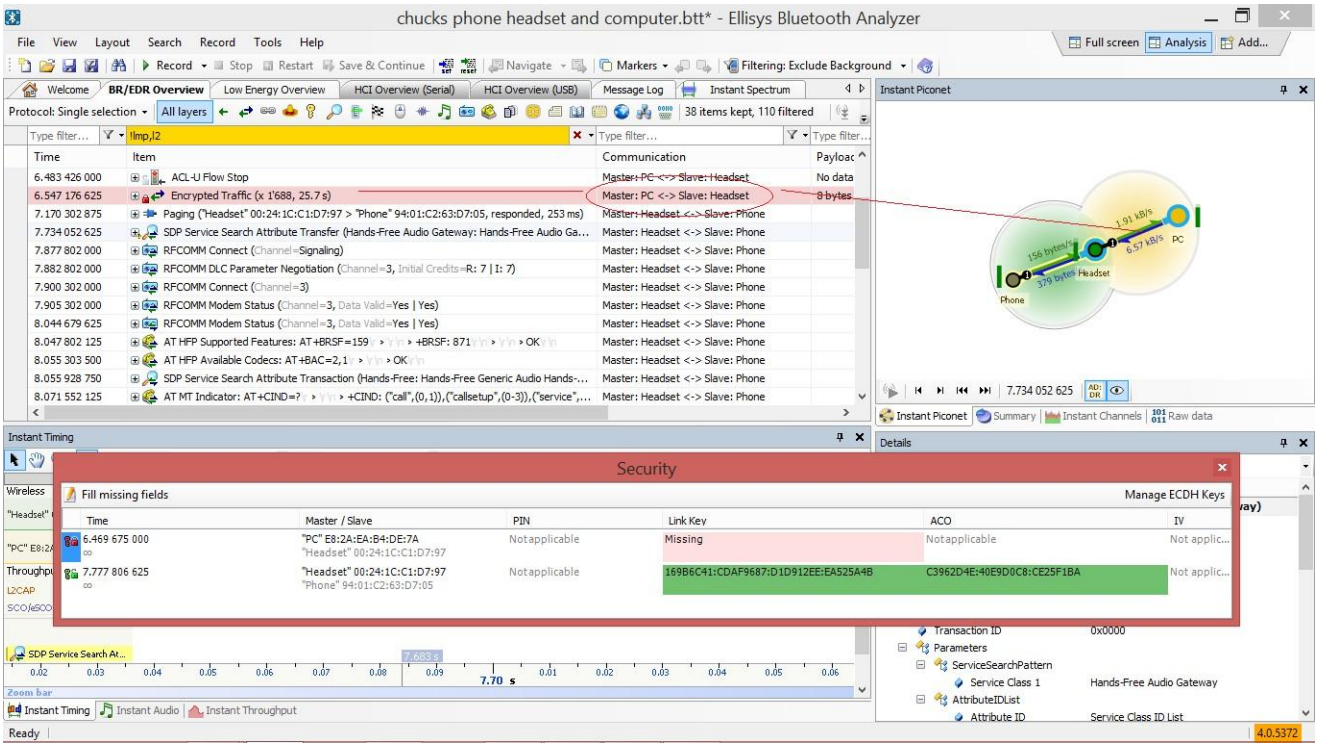


下と右の図は、Ellisys の Bluetooth アナライザソフトウェアを使って、いくつかの重要なコンセプトを説明しています。この右図では、3つのデバイス（電話機、ヘッドセット、PC）あり、2つのピコネットを組み合わせた（1つのスキャッターネット）構成であることがわかります。PC はヘッドセットのマスターであり、ヘッドセットは電話機のマスターであると同時に PC のスレーブでもあるという二つの役割を担っています。

ヘッドセットと電話機の接続については、リンクキーが取得されているため、完全に復号化されています（Security ウィンドウに表示されています）。しかし、ヘッドセットと PC の接続は、リンクキーがまだ取得されていないため、暗号化されたままです。

電話機とヘッドセットの間のリンクキーは、ベンダー固有の方法で取得されており、後述の“ベンダー固有の方法”の Android スタックのセクションに記載されています。

アナライザは、PC – ヘッドセット間の暗号化された通信データを記録し、これを 1行で表示していることに注目してください。この行は、記録中または保存後にリンクキーを入力することで、復号化された通信データとして展開されます。このPC – ヘッドセット間の暗号化された通信データがどのように復号化されるかについては、後述の“ベンダー固有の方法”のセクションを参照してください。



標準的な方法

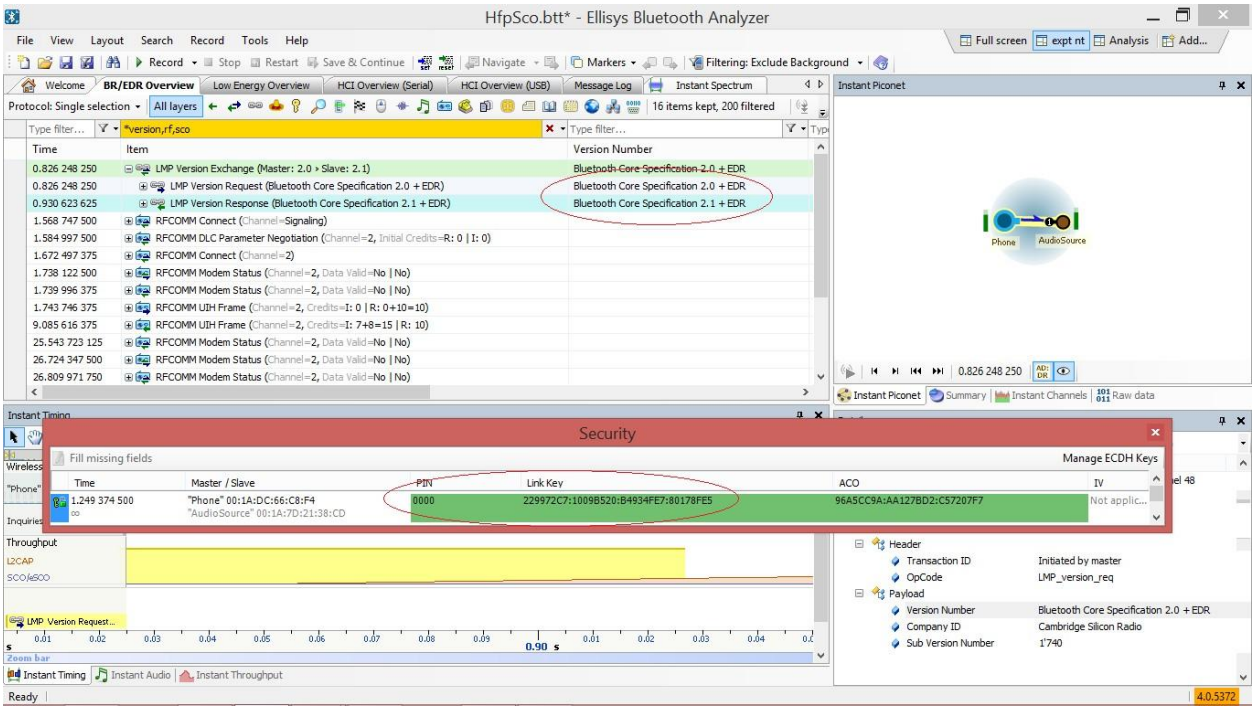
以下の方法は、使用するBluetooth チップやスタックのメーカーに関係なく動作します。ただし、これらの方法は、Bluetooth ハードウェアへのアクセスを必要とするため、既製品には適用できない場合があります。

PIN コードによるペアリング

PIN コードベースのペアリングとしても知られている LMP ペアリングは、レガシー ペアリングとも呼ばれ、全く安全ではありません。このペアリングでも SSP と同様に、トラフィックを暗号化するためのリンクキーを作成・使用しますが、Ellisys Bluetooth アナライザソフトウェアは、記録したペアリングのトラフィックを見るだけで、自動的にPINコードを解読し、リンクキーを推測することができます。PIN コードベースのペアリングは、Bluetooth 2.1 以降のデバイス (SSP 対応デバイス) は、*これらのデバイスが Bluetooth 2.0 以前のデバイスとペアリングする場合を除き*、使用されません。つまり、SSP に対応したデバイスを Bluetooth 2.0 以前のデバイスとペアリングした場合、Ellisys アナライザを使って SSP 対応デバイスからのトラフィックも完全に復号化することができ、SSP 対応デバイスを（解読可能な）PINコードベースのペアリングに戻すことができます。

以下は、Bluetooth 2.1（またはそれ以上）のデバイスが Bluetooth 2.0（またはそれ以下）のデバイスとペアリングする際に、ペアリングが PIN コードペアリングに戻った例です（Bluetooth 2.0 デバイスには SSP の概念がありません）。アナライザソフトウェアは、PIN コード 0000 を解読してリンクキーを計算し、その後のトラフィックを自動的に復号化しています。

なお、ユーザーが間違った PIN コードを入力した場合は、アナライザソフトウェアがこのエラーを通知し、入力すべき正しいPINコードを表示します。非常に便利で簡単です。



SSP デバッグモード

SSP デバッグモードは、SSP 対応デバイスで使用される特別なモードで、通常の プライベート/パブリック キーのペアの代わりに、既知のプライベート/パブリック キーのペアが使用されます。2台のデバイスのうち少なくとも1台が SSP デバッグモードになっている場合、既知のパブリック キーが無線で送信されるので、デバッグモードであることが解り、アナライザソフトウェアはリンクキーを自動的に推測します。繰り返しになりますが、2台のデバイスのうち1台だけがデバッグモードになっていればよく、両方の必要はありません。2台のデバイスのうち 1台がデバッグモードになっている場合、アナライザはその SSP プライベートキー を知ることができるため、各デバイスで使用されているのと同じアルゴリズムでリンクキーを計算することができます。

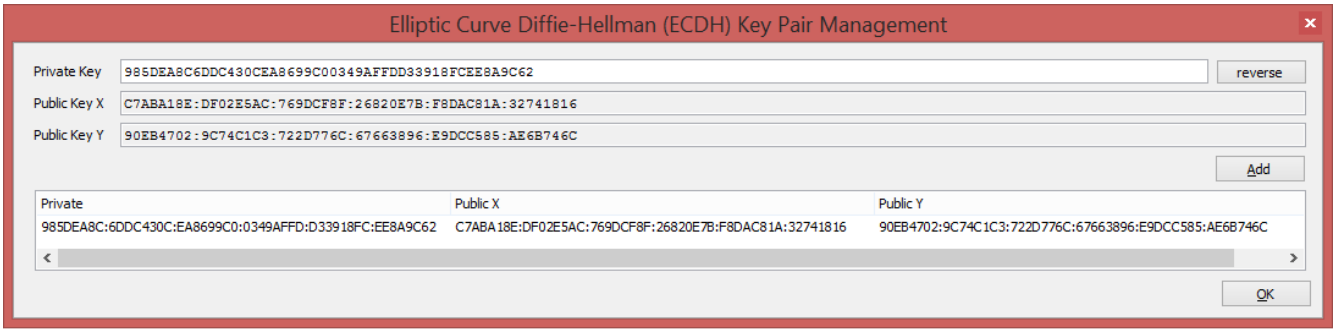
なお、一部のメーカーのデバイスでは、自分がデバッグモードになっていない場合、デバッグモードになっている他のデバイスとの SSP のペアリングを受け付けないという選択をしているものもあります。これは非標準的な動作で、残念ながらデバッグモードの有用性を損なうものです。このような場合、両方のデバイスをデバッグモードにする必要があります。

SSP プライベートキー　インジェクション

上記で説明したように、SSP デバッグモードは既知の SSP プライベートキー を使用するための手段に過ぎません。SSP デバッグモードを使用しない場合でも、プライベートキー を知っていれば、ユーザーはそのプライベートキー をアナライザソフトウェアに入力することができます。プライベートキー を知っていれば、既知のプライベートキー を含むペアリングが検出された場合、アナライザソフトウェアは自動的にリンクキーを決定することができます。これにより、リンクキーを手動で入力する必要がなくなるため、非常に使い勝手がよくなります。

この方法では、特定の SSP プライベートキー で構成されたアナライザのみがリンクキーを決定できるため、SSP デバッグモードのセキュリティ・レベルが向上します。

この機能（プライベートキー の入力）は、Ellisys アナライザソフトウェアの Security ウィンドウにある Manage ECDH Keys ウィンドウを使います（下図）。



HCI 記録

リンクキーは無線では送信されませんが、無線チップとホストの間で規定されている HCI (Host Controller Interface) を介して送信されます。これにアクセスできるのは良いことです。さらに良いことに、Ellisys のアナライザは、HCI トラフィックを Bluetooth 無線通信と同時に記録することができるので、アナライザはこの方法でリンクキーにアクセスすることができます。

HCI へのアクセスは、開発段階のプロトタイプや開発キット (SDK) では簡単に利用できますが、市販のデバイスではほとんど利用できないでしょう。ただし、Bluetoothドングルに代表されるようなUSB HCI は例外です。例えば、USBドングルを装着した PC を使用すれば、以下のように簡単にアクセスできます。

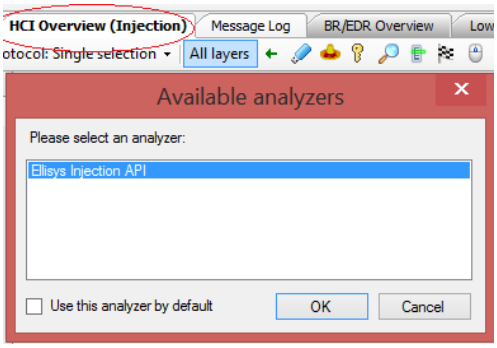
ドングルを BEX400 アナライザの STD-A ポート（アンテナの下）に取り付け、隣接する Micro-B ポートに USB Micro-B – STD-A ケーブルを挿し、そのケーブルを PC に接続します。アナライザソフトウェアは、USB HCIトラフィックと同時に Bluetooth 無線データを記録し、そのトラフィックを復号化するためのリンクキーを自動的に抽出します。

なお、リンクキーは両方のデバイスで同じであるため、HCI アクセスは両方ではなく片方のデバイスのみで十分です。

以下は、Bluetoothドングルから USB HCI の記録を行う典型的なセットアップです。アナライザは、Bluetooth 無線データと HCI データの両方を同時に記録しています。通常の場合、ドングルは 6インチの USB STD-A 延長ケーブルを使ってアンテナから離しています（そうしないと、ドングルがアンテナに近いのが原因で、信号が強くなりすぎる可能性があるからです）。

下のスクリーンショットでは、BEX400 アナライザが BR/EDRトラフィックと同時に USB HCI を記録し、HCI のデータからリンクキーが自動的に抽出され、BR/EDR 通信データを自動的に復号化しています。同様の方法で、BEX400 アナライザの背面に接続したロジック ケーブルを使用して、UART や SPI などの他の形態の HCI データを記録することができます。

Ellisys HCI インジェクション API



アナライザソフトウェアは、Record メニューの Available Analyzers で HCI Injection API が選択することができます。インジェクションAPI は、UDP (User Datagram Protocol) を使用して HCI 通信データをアナライザソフトウェアに転送します。この通信データは、アナライザの標準 HCI ポートの1つとして記録されているかのように、HCI Injection Overview にリアルタイムで表示されます。

この方法で取得したリンクキーは、アナライザソフトウェアが機器の接続に関連付けて保存するため、以降の同じ機器間の Bluetooth 無線データを記録しても自動的に復号化されます。

Bluetooth Analyzers User Manual には、各種参考資料やサンプルコードをダウンロードするためのリンク情報が掲載されています。

Ellisysリモートコントロール API

Ellisys リモートコントロール API は、アナライザソフトウェアにリンクキー（任意のソースから取得）をプログラムで注入するために使用できます。例えば、Windows レジストリの変更を監視し、新しいリンクキーをソフトウェア アプリケーションにプッシュするリモートコントロール API クライアントを構築することができます。

以下のリンクには、Microsoft Visual Studio 2010 を使用して C# で記述された入門ガイド、プラグイン DLL、およびサンプルコードが含まれています。Visual Studio 2005 以上で互換性があります。

http://www.ellisys.com/better_analysis/bex400a_remote_api.zip

ベンダー固有の手法

BEX400 アナライザは、暗号化された通信データも含め、周辺のすべての Bluetooth 通信データを記録します。アナライザソフトウェアでは、通信データを復号化するために、記録中、または記録されたトレースファイルに、ユーザーがリンクキーを手動で入力することができます。HCI の記録や HCI インジェクションなどの標準的な方法が適用できない場合でも、ベンダー固有の方法でデバイスからリンクキーを抽出し、アナライザの Security ウィンドウにリンクキーを入力して復号化できる場合があります。

このような場合、無線チップ、オペレーティングシステム、SDK、またはホストスタックの特別な機能にアクセスすることが必要です。例えば、リンクキーが保存されている Windows のレジストリへのアクセスや、一部の携帯電話で提供されている開発者モードへのアクセスなどが挙げられます。

以下のリストは完全なものではなく、現在進行中のものです。Ellisysでは、様々なデバイスやスタックなどからリンクキーを見つける方法を提案していただき、このドキュメントに掲載することを推奨しています。Ellisys への連絡方法については、このドキュメントの最後に記載されています。また、Ellisys は、システムソフトウェアに変更を加える前に、デバイスメーカーに確認することを強くお勧めします。

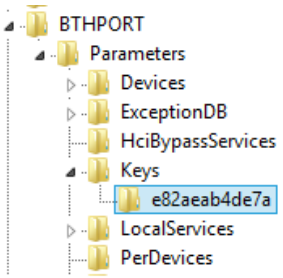
ほとんどの Bluetooth スタックプロバイダーやチップメーカーは、Bluetooth 機器開発者向けに、システム レジスタへのアクセスを提供する API または SDK を提供しており、その中には Bluetooth リンクキーを読み取るオプションも含まれているようです。詳細については、必要に応じてサプライヤーにお問い合わせください。

Windows の Bluetooth スタック

Windows ベースのシステム（Windows スタックを使用）のリンクキーは、多くの場合、Windows レジストリから入手できます。多くの場合、このリンクキーは、該当する Bluetoothアドレス（システムが接続されている Bluetooth デバイス）に関連付けられた、以下のような BTHPORT フォルダ内にあります。なお、このフォルダへのアクセスには管理者権限が必要な場合があり、アクセスするためにはその権限を変更する必要があります（この管理者オプションでアクセスする場合はフォルダを右クリックしてください）。

```
HKEY_LOCAL_MACHINE_SYSTEM\CurrentControlSet\Services\BTHPORT\Parameters\Keys
```

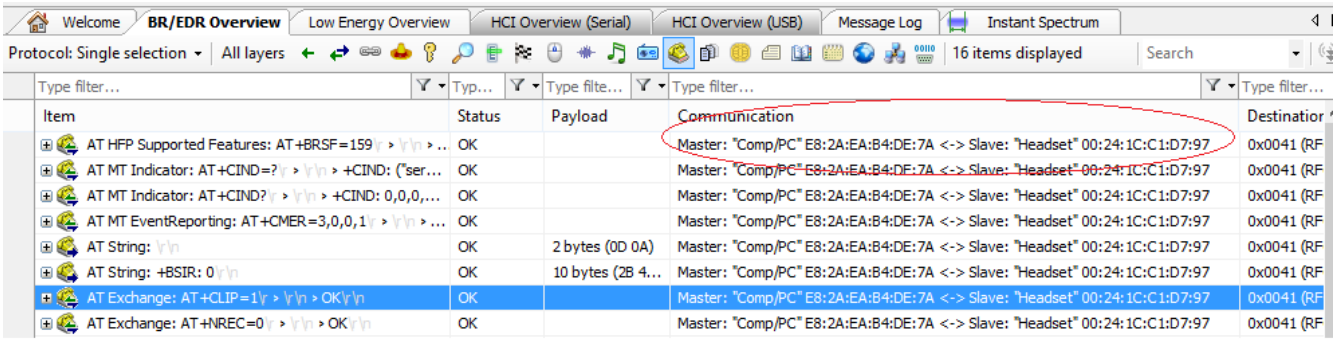
このケース（右図）では、コンピュータ（WIN8 PC）のレジストリのディレクトリ`BTHPORT/Parameters`の「e82aeab4de7a」（PC の BD ADDR）と表示されてい



下の図は、このディレクトリの内容を示しており、「00241cc1d797」が接続されたデバイス（この場合はヘッドセット）の BD ADDRとして示されています。このヘッドセットに関連するデータがリンクキーです。このリンクキーをコピーして、解析ソフトウェアの Security ウィンドウに貼り付けるだけで、以下のように、これらのデバイス間のトラフィックが直ちに解読されます。

Name	Type	Data
(Default)	REG_SZ	(value not set)
00241cc1d797	REG_BINARY	58 48 f3 de ff d5 9c 2b a9 e4 8b 53 9c 3c 1e 61

下の図は、アナライザが通信データを復号化したことを示しています（AT プロトコルのみを表示するようにフィルタリングされています）。通信欄には、2台の通信機器とその BD ADDR が表示されています。



多くの Windows システムでは、Microsoft のスタックではなく、Toshiba、Widcomm などのサードパーティのBluetooth スタックが使用されています。このようなサードパーティ製スタックへのレジストリアクセスは情報が少ないため、システムをサードパーティ製スタックから Windows 用スタックに強制的に戻すという方法があります。ユーザーは、システムの復元ポイントを設定し、サードパーティ製スタックをアンインストールしてから再起動します。すると、システムはデフォルトで Microsoft スタックになります。

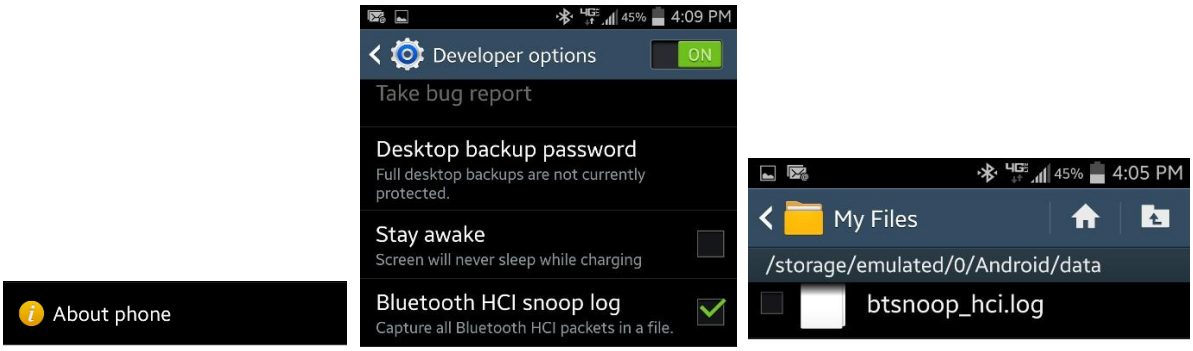
場合によっては、オンラインのフォーラムを閲覧することも有効です。下記 URL はその一例です。http://superuser.com/questions/229930/finding-bluetooth-link-key-in-win7-to-double-pair-a-device-on-dualboot-computer

Android スタック

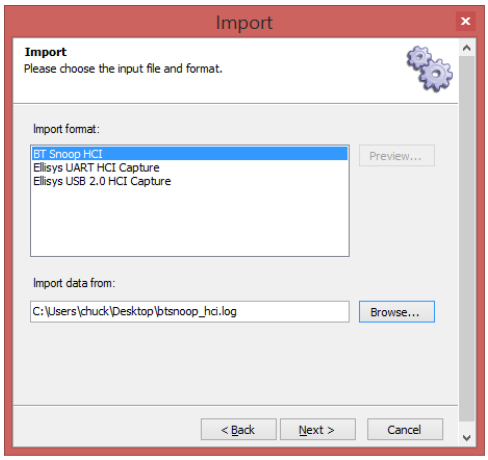
Android OS の後期バージョンでは、開発者モードが提供されています。このモードは、*「設定」/「携帯電話について」*メニューで、*ビルド番号*の選択を数回（通常は7回）繰り返し押すことで有効になります。開発者モードが利用できるかどうか、また具体的な方法については、お使いの携帯電話のユーザーマニュアルをご参照ください。

開発者モードには、HCI 通信のログファイルを有効にするオプションなど、さまざまな機能があります。このファイルは BT Snoop 形式です。このファイルには、ペアリング時のリンクキーが含まれており、アナライザソフトウェアは簡単にインポートすることができます。アナライザソフトウェアは、これらのリンクキーを保存し、それらを使用しているデバイスと関連付けるので、接続されたデバイスの無線通信は自動的に復号化されます。

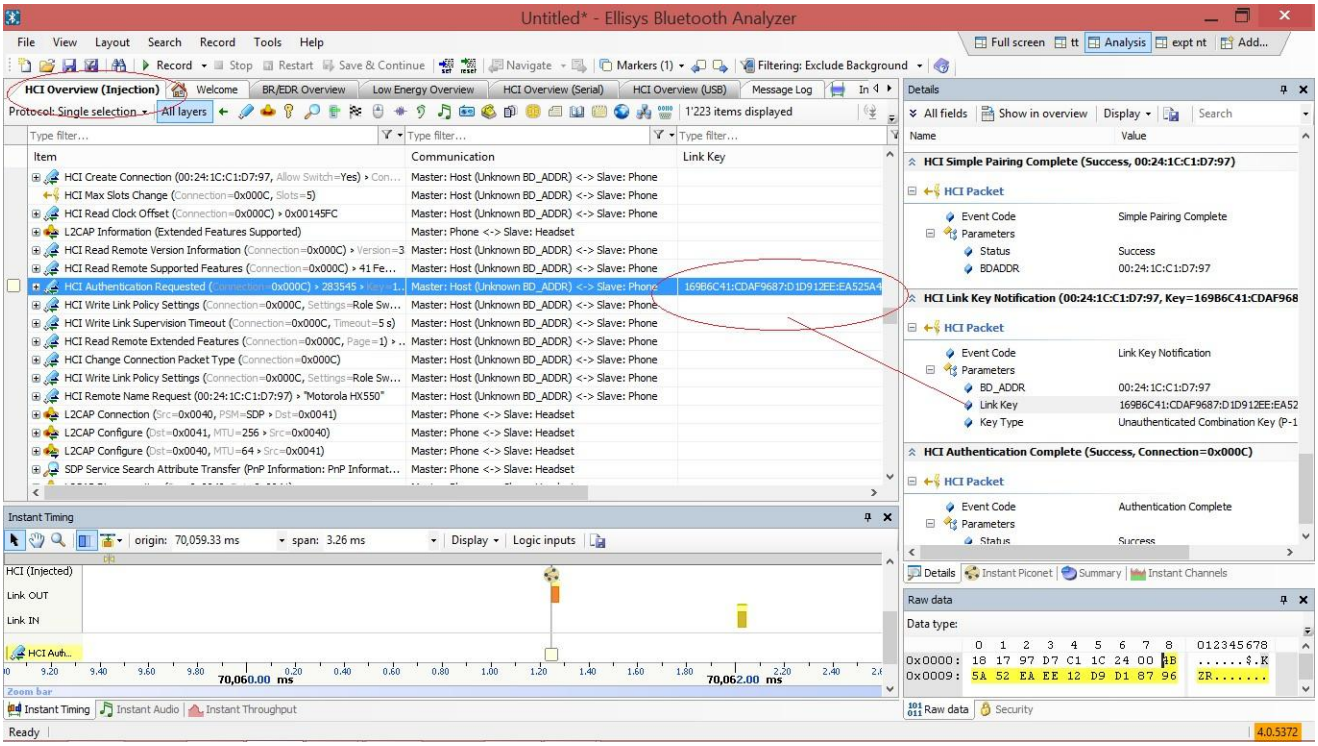
以下のスクリーンショットは、開発者モードを有効にするための簡単な手順と、その結果としての BT Snoop HCI ログファイルです。このファイルは、携帯電話の USB 接続でアクセスできるほか、電子メールなどさまざまな方法で共有することができます。



下のスクリーンショットは、アナライザソフトウェアの Import ダイアログボックスで BT Snoop HCI を選択したところで、携帯電話で作成された BT Snoop ファイルが保存された場所を参照しています。



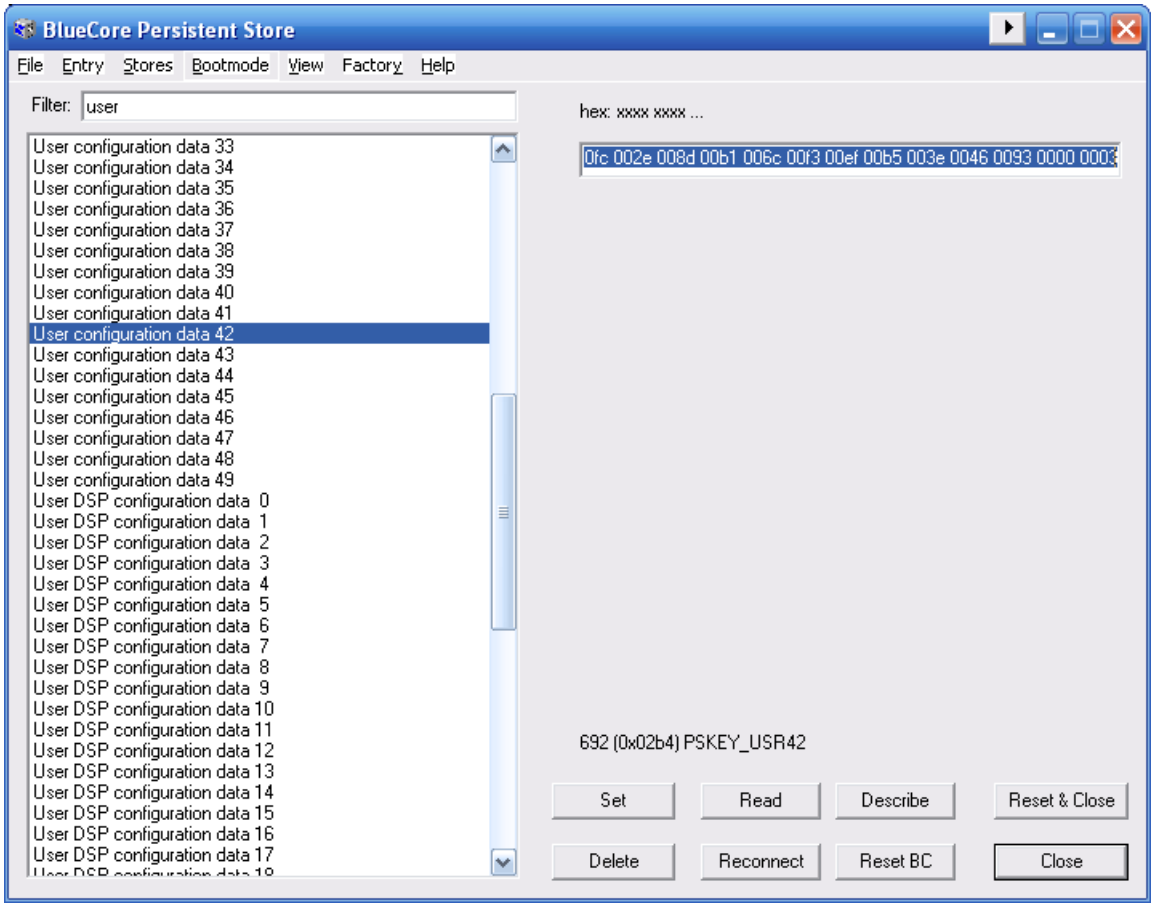
下のスクリーンショットは、アナライザソフトウェアが携帯電話の BT Snoop ログファイルをインポートした後の状態です。　また、赤枠、ハイライト部は、携帯電話とヘッドセットの間で確立されたリンクキーを示しています。このキーはアナライザソフトウェアによって保存され、携帯電話とヘッドセット間で行われる後続の通信の複合化に使用されます。



Android Developer SDKについては、以下のリンクを参照してください。http://developer.android.com/sdk/index.html

CSR パーシステント ストア

アナライザソフトウェアは、CSR の PSTool ユーティリティのフォーマットを標準でサポートしています。 キーは設定データ42～49に格納されています。



16進数のデータはアナライザソフトウェアで直接サポートされており、変換せずにそのまま Security ウィンドウの Link Key フィールドに入力することができます。アナライザソフトウェアは CSR フォーマットを認識し、自動的に変換します。

ノキアの携帯電話

ノキアの一部の機種では、*#2873#と入力することでデバッグモードにすることができます。

Linux/BlueZ Bluetoothスタック

BlueZ は、Linux の公式 Bluetooth プロトコル スタックです。このスタックは、多くの Android プラットフォーム（Android 4.2より前）でも使用されています。リンクキーにアクセスするのに便利なユーティリティについては、www.bluez.org を参照してください。

以下のリンクには、HCI ツールを搭載した BlueZ Utils アプリケーションの情報があり、これも役に立つかもしれません。https://www.linux.com/news/hardware/peripherals/44623-working-with-bluetooth-connecting-to-all-those-cool-devices

```
/var/lib/Bluetooth/[BD_ADDR]/linkkeys
```

Widcomm 社製 Bluetooth スタック

Widcomm 社は、Windowsで使用された最初のBluetoothスタックでした。 上記のWindows のスタックのセクションと同様に、Widcomm の下記のレジストリの場所を試してみてください。なお、Widcomm 社は Broadcom 社に買収されました。

```
HKEY_CURRENT_USERSoftware_Widcomm\BTConfig\LinkKeys
```

Bluetooth Low Energy

Bluetooth Low Energy (Bluetooth v4.0) のセキュリティ機能は、BR/EDR で使用されているものとは異なります。Bluetooth Low Energy のペアリングでは、Long Term Key (LTK) が生成されますが、この LTK は、BR/EDR で使用されているリンクキーの生成プロセスとは大きく異なります。Bluetooth Low Energy デバイスは、BR/EDR デバイスよりもシンプルな動作を目的としているため、アーキテクチャ的にシンプルであり、一般的にこれらのデバイスの処理能力や記憶能力は低く、実際にはプライバシーに対するアプローチもシンプルで安全性が低いものとなっています。

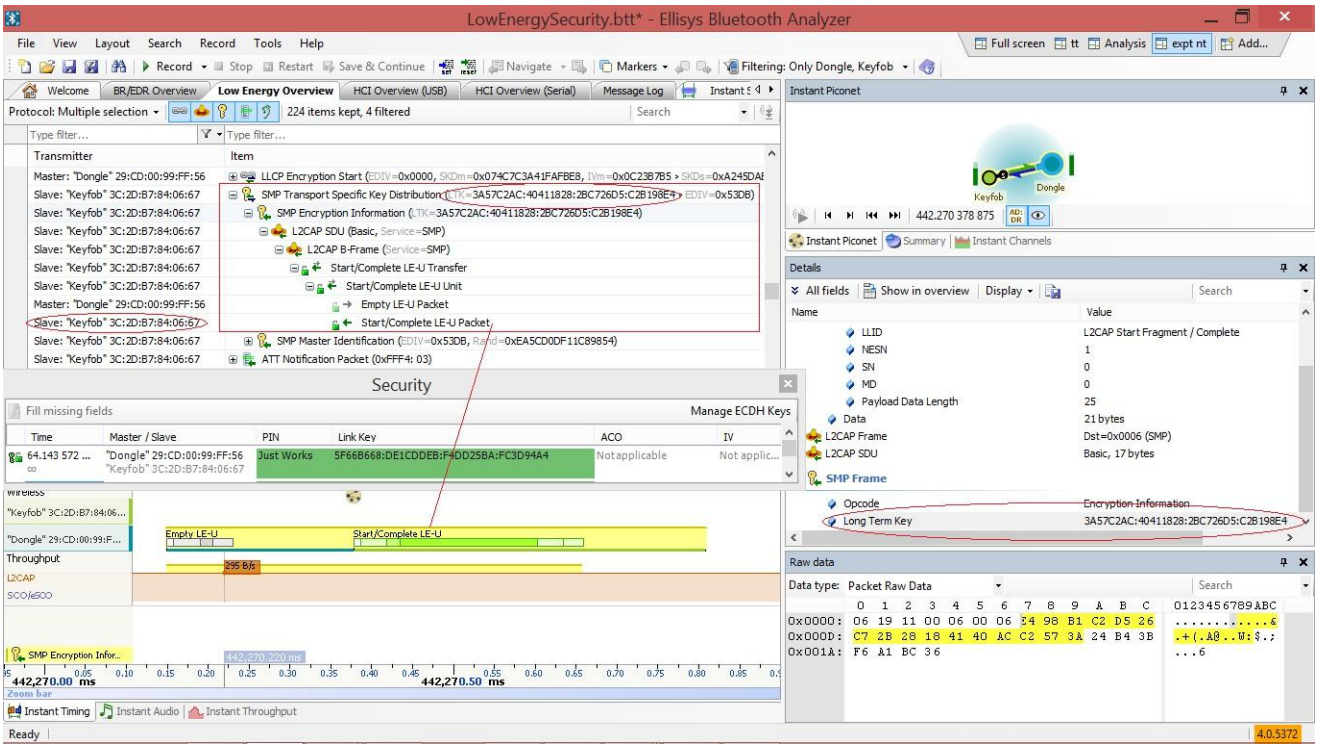
Bluetooth Low Energy のセキュリティに関する今後の変更については、下記の “Bluetooth Low Energy のセキュアな接続” をご覧ください。

Bluetooth Low Energy では、ある機器が LTK を決定し、これを Short Term Key (STK) に基づく一時的な暗号化を用いて別の機器に送信します。このシンプルなアプローチの利点は、接続および再接続の高速化であり、これは Bluetooth Low Energy の主要な設計目標であり、接続までの時間が長い BR/EDR との大きな違いとも言えます。欠点としては、盗聴防止機能がないことが挙げられます。

そこで、Bluetooth Low Energy では、”キーの合意” （リンクキーを両機器で対称的に決定する）ではなく、”キーの転送” （LTK を相手に送信する）を採用しています。

BEX400 のユーザーにとって重要なことは、Bluetooth Low Energy のセキュリティを解析できるため、キーを探す必要がないことです。Bluetooth Low Energy の将来の進化により、これはより困難になると思われますが、BEX400 のアーキテクチャはこのような変化に容易に対応できます（下記の “Bluetooth Low Energy のセキュアな接続” を参照してください）。

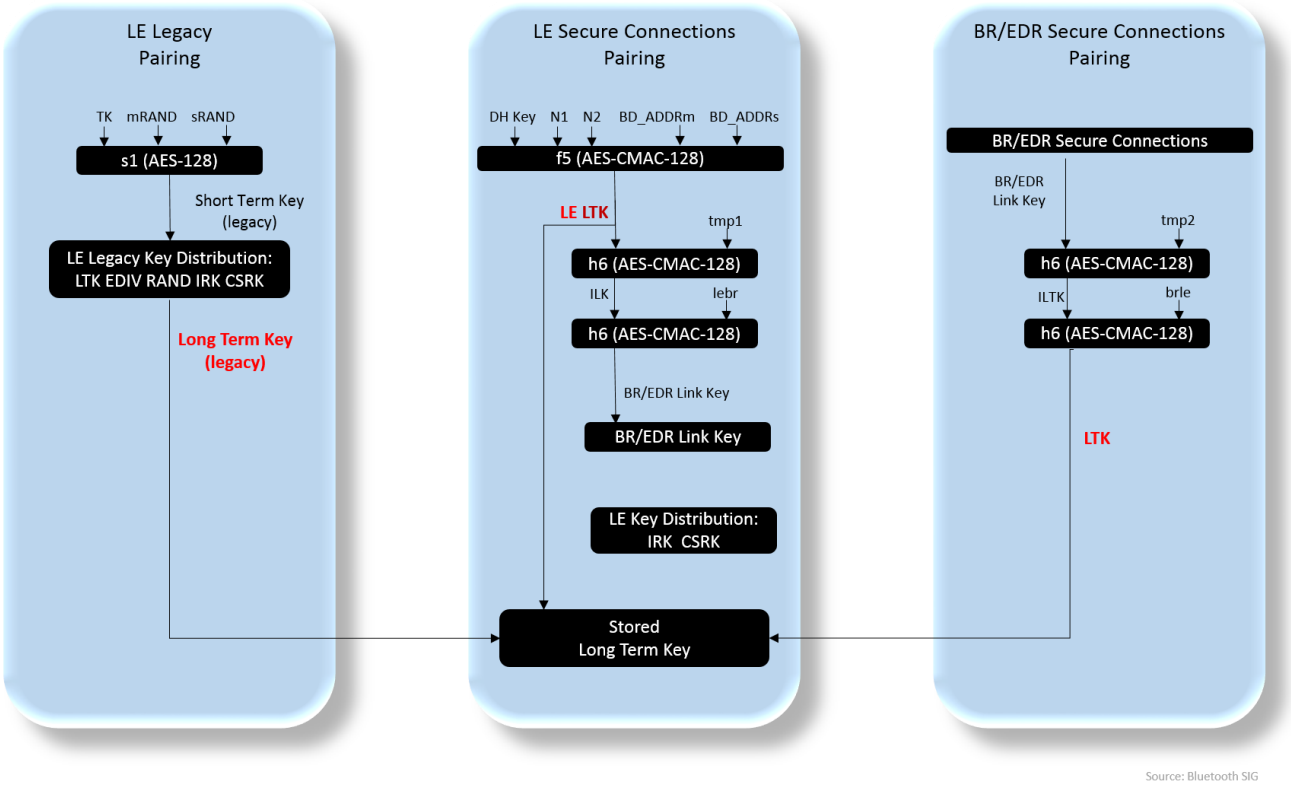
下のスクリーンショットは、キーフォブ デバイスからドングルに LTK が送信される様子を示しています。このパケットが送信される時点で、STK 対応の暗号化がすでに行われていることに注意してください。



Bluetooth Low Energy のセキュアな接続

近日中に予定されている Bluetooth 仕様の改訂 (v4.2) では、Bluetooth Low Energy デバイスのセキュリティを大幅に向上させる LE セキュア コネクションの追加を含む、様々な機能強化が行われます。この追加により、BR/EDR のセキュアな接続、つまり SSP と同様の方法で、P-256 楕円曲線と FIPS 承認のアルゴリズム (AES-CMACとP-256楕円曲線) を利用するペアリング手順が可能になります。この変更には、共有されるシークレット キーの規定も含まれます。LE のレガシーペアリング（上記のセクションで説明）は引き続き利用可能です。BR/EDR の場合、セキュア・コネクションは v4.1 の仕様で追加され、主に暗号化方式の変更で構成されていることに注意してください。ペアリング方式は SSP のままですが、プライベート/パブリック キーの長さが長くなっています（192ビットから256ビット）。

下図は、LE セキュア コネクションの予想されるアーキテクチャと、LE レガシー ペアリングおよび BR/EDR のセキュア コネクションとの比較を表しています。



このように、LE セキュア コネクションでは、ある接続（BR/EDRなど）で生成されたキーを別の接続（Bluetooth Low Energy など）で使用することも可能です。つまり、BR/EDR と Bluetooth Low Energy の両方をサポートする2つのデバイスがあり、両方のデバイスが BR/EDR と Bluetooth Low Energy の両方でセキュア コネクションをサポートしている場合、1回ペアリングするだけで済みます。言い換えれば、LE のペアリングで生成された LTK は、BR/EDR 接続で使用するために BR/EDR のリンクキーに変換することができ、逆に、BR/EDR SSP のペアリングで生成された BR/EDR のリンクキーは、LE 接続で使用する LTK に変換することができます。

フィードバック募集

リンクキーにアクセスするための他の方法をご存知の方や、このドキュメントで提案されている内容の実装についてご意見をお持ちの方は expert@ellisys.com までご連絡ください。このドキュメントを適宜更新したいと考えています。ご希望であれば、更新されたドキュメントにあなたの意見を反映させます。これは、Bluetoothコミュニティにとって大きな助けとなります。

本文書について

本文書は、″ EEN_BT09 - Methods for Accessing a Link Key (Rev. A Updated 2014-10)″ 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