コースコード：VER-IOTHACK
税込価格：396,000円 (税抜価格：360,000円)
日数：3日間

ここに注目!!

受講対象者

このトレーニングはこのような方におすすめです。

・IoTデバイスおよびIoTシステムのセキュリティについて学びたいとお考えの方

前提条件/前提知識

このコースを受講する前に受講者が習得しておく必要がある知識およびスキルは次のとおりです。

・一般的なOS、コンピュータ・アーキテクチャ、ネットワーキングに関わる基本的な知識
・IoTに関する基本的な知識
・Linuxの基本操作のご経験がある方

目的

このコースを修了すると次のことができるようになります。

・デバイスファームウェアの抽出と分析
・バイナリのデバッグと逆アセンブル
・UART、SPI、JTAGの悪用、JTAGのデバッグとそれを用いたエクスプロイト
・ファームウェアのダンプ、ハードウェアとソフトウェアのデバッグ
・IoTデバイスのクラウドやモバイル機能への攻撃
・スニッフィング、リプレイ、MITM、無線通信による攻撃、BLEによるエクスプロイト
・ARMとMIPSのリバースエンジニアリング、従来型攻撃と非従来型攻撃の手法
・プラットフォームへの攻撃、 など

アウトライン

主な講座内容
1日目
IoTセキュリティの基礎を説明した後に、実際のIoTデバイスに対して、既知脆弱性を使用したサイバー攻撃に関する基本的なテクニックを学びます。
・IoTセキュリティアーキテクチャーの内部概念
・既知のIoTデバイスの脆弱性（ケーススタディ）
・IoTデバイスのファームウェア取得とリバースエンジニアリング

2日目
実際のIoTデバイスを分解して、回路基板の持つコンポーネントを理解し、基板のサイバー攻撃に関する基本的なテクニックを学びます。また、車載ネットワークの基礎を説明いたします。
・回路基板のコンポーネントとデバイスルートの取得

・UARTのエクスプロイト
・車載ネットワークの内部概念

3日目
車載を模擬したシミュレーション環境にて、車載ネットワークのサイバー攻撃に関する基本的なテクニックを学びます。
・CANバスの盗聴および再送攻撃
・UDSプロトコルを用いた攻撃

主な習得内容
・IoTデバイスへ基礎的な攻撃
・デバイスファームウェアの抽出と分析
・バイナリのデバッグと逆アセンブル
・ファームウェアのダンプ、ハードウェアとソフトウェアのデバッグ
・IoTデバイスの通信機能への攻撃
・車載ネットワークの基礎知識
・CANバスの盗聴、再送攻撃
・UDSプロトコルを用いた攻撃の一例 その他

※ 当日の進行状況により、内容変更の可能性がございます。