Monthly Research 2016.5

IoT デバイスのセキュリティの現状

F F R I , Inc.
http://www.ffri.jp

E-Mail: research-feedback[at]ffri.jp
Twitter: @FFRI_Research

目次

- IoT デバイスの現状
- IoT デバイスのセキュリティに関する事例
  - インシデント
  - 研究
- IoT デバイスに考えられる脅威と対策
  - 脅威
  - 脅威を引き起こす原因
  - IoT デバイス開発における対策の例
- 考察
- 参考情報

IoT デバイスの現状

- IoT (Internet of Things) とはモノのインターネットと言われており、
  任意のデバイスをインターネットに接続する概念である

- IoT デバイスは多種多様である
  - オフィス、工場、農場、医療機関、家庭などあらゆる場所で利用されている
  - スマートフォンアプリで操作・利用できるものもある

- インターネットに接続されるという性質上、セキュリティリスクが懸念されており、
  実際のインシデントも報告されている

- 本稿では IoT デバイスに関連するインシデント、研究、対策手法の一部を紹介する

IoT デバイスに関連するインシデント(2015～2016年)

- IoT 機器を標的とした攻撃の観測について – 警察庁(2015/12/15)
  - Linux ベースの IoT デバイスで動作する Telnet への攻撃を多数観測
  - 攻撃を受けたデバイスがボットになっている

- 「パナソニック」製品など標的―日本の防犯カメラ、約6,000台がネットでのぞき見対象 – INTERNET COM(2016/01/22)
  - デフォルトパスワードのまま利用していることなどが原因

- 住宅機器の遠隔操作サービス「リモートプラス」ならびにガスの消し忘れ確認サービス「確かめ～る」における不適切なパスワードの発行について – 東京ガス(2016/03/25)
  - 利用者変更時にパスワードをリセットしていないことによる不正アクセスの可能性
  - 悪用された場合、ガス遮断の操作ができる

IoT デバイスに関連する研究(2014～2016年)

- LIGHTS OFF! THE DARKNESS OF THE SMART METERS
  - Black Hat EU 2014 での発表
  - あるメーカーのスマートメーターが同一の暗号鍵を利用していた事により、なりすましによって電力の遮断などのコマンドが送信可能であったという事例

- IoTPOT: Analysing the Rise of IoT Compromises
  - USENIX WOOT 2015 での発表
  - IoT デバイスを模したハニーポットの開発と収集したマルウェアの研究

- HACKING A PROFESSIONAL DRONE
  - RSA Conference 2016, Black Hat Asia 2016 での発表
  - ドローン操作用のスマートフォンアプリを解析して脆弱性を発見し、中間者攻撃を実証

IoT デバイスに考えられる脅威

- マルウェア感染
  - ボット化
    - 気が付かないうちに感染し、サイバー攻撃に加担する恐れ
  - ランサムウェア
    - 被害はまだ確認されていないが、影響範囲の広い脆弱性の発見などをきっかけに急増する恐れがある

- 物理的侵害
  - スマートロックに対するサイバー攻撃による建物等へ不法侵入
  - IoT デバイスによって制御されている機器、環境の破壊など

- 情報の流出
  - IoT デバイスを介して収集される情報の流出によるプライバシーの侵害

脅威を引き起こす原因

- マルウェア感染
  - 脆弱性攻撃によるリモートコード実行
  - Telnet や HTTP, FTP など平文通信の盗聴による乗っ取り
  - デフォルトパスワードの利用などの設定不備による乗っ取り

- 物理的侵害
  - 耐タンパ性の低い設計・実装によるハードウェア・ソフトウェアの解析・改造
  - 暗号化、認証、通信などの処理の実装不備による脆弱性
  - ファームウェア書き換えによる不正ソフトウェアの実行

- 情報の流出
  - IoT サービスを提供するサーバーへの不正アクセス
  - ユーザーの理解不足による意図しない情報の送信・公開

IoT デバイス開発におけるセキュリティ対策の例

- 共通対策
  - 脆弱性を修正するアップデートや緩和策を速やかに提供する
  - TLS による通信の暗号化
  - 適切なパスワードや認証設定

- 物理的なセキュリティの強化
  - 筐体の分解を困難にする
  - デバッグインターフェイスの無効化

- ソフトウェアの難読化
  - デバイスのファームウェアやスマートフォンアプリの難読化

考察

- IoT デバイスは生活を便利にするが、既にサイバー攻撃のターゲットとなっている

- IoT デバイス利用者はセキュリティリスクについて認識する必要がある
  - サイバー攻撃による遠隔操作や情報漏えいによるプライバシーの侵害
  - セキュリティ設定、送受信するデータの選択、データのバックアップなどを実施すべき

- IoT デバイス開発者は IPA が公開している
  ”IoT開発におけるセキュリティ設計の手引き” などを参考にして対策を講じるべき
  - 従来のセキュリティ対策に加え、物理的な対策も必要である

参考情報

- A Simple Explanation Of 'The Internet Of Things'
  - http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#52f161566828
- How the Internet of Things Got Hacked
  - https://www.wired.com/2015/12/2015-the-year-the-internet-of-things-got-hacked/
- IoT機器を標的とした攻撃の観測について - 警察庁
  - https://www.npa.go.jp/cyberpolice/detect/pdf/20151215_1.pdf
- 住宅機器の遠隔操作サービス「リモートプラス」ならびにガスの消し忘れ確認サービス「確かめ～る」における不適切なパスワードの発行について - 東京ガス
  - http://www.tokyo-gas.co.jp/important/20160325-06.pdf
- 「パナソニック」製品など標的―日本の防犯カメラ、約6,000台がネットでのぞき見対象 – INTERNET COM
  - http://internetcom.jp/200103/insecam-again
- HACKING A PROFESSIONAL DRONE - Nils Rodday
  - https://www.blackhat.com/docs/asia-16/materials/asia-16-Rodday-Hacking-A-Professional-Drone.pdf
  - LIGHTS OFF! THE DARKNESS OF THE SMART METERS - Alberto Garcia Illera & Javier Vazquez Vidal
  - https://www.blackhat.com/eu-14/briefings.html#lights-off-the-darkness-of-the-smart-meters
- 組み込み機器への攻撃を観測するハニーポットIoTPOTの機能拡張
  - 鈴木 将吾, イン ミン パパ, 江澤 優太, 鉄 穎 , 中山 颯(横浜国立大学), 吉岡 克成, 松本 勉(横浜国立大学先端科学高等研究院／横浜国立大学環境情報研究院), ICSS2015-48 pp.7-12
- IoT開発におけるセキュリティ設計の手引き - IPA
  - https://www.ipa.go.jp/files/000052459.pdf