講演番号：5

IoT デバイス侵入におけるセキュリティ対策の検討

B－7　　Study of security measures using IoT device intrusion

大橋　建也　　末田　欣子
Kenya Ohashi　　Yoshiko SUEDA
明星大学情報学部
School of Information Science, Meisei University

1. はじめに

IoT は近年では大手メーカーなどのテレビの CM でも「IoT」というフレーズを使い始めるほど生活に欠かせない技術となってきている。しかし、便利になる一方で IoT デバイスのセキュリティに関しても検討を進める必要がある[1][2]。そこで本研究では、IoT デバイスへの侵入によりペネトレーションテストを実施し、異常がないかを確認する。脆弱性が確認された場合、どのようなセキュリティ対策を実施するべきかを考察する。

2. ペネトレーションテスト

ペネトレーションテストとはネットワークに接続されているコンピュータシステムに対し、実際に既知の技術を用いて侵入を試みることで、システムに脆弱性がないかどうかテストする手法のことである[3]。侵入実験または侵入テストとも言われる。

3. 提案手法

ペネトレーションテストの図１の手順に従い、Raspi On Zumo(以降、Zumo)とルンバを対象の IoT デバイスとする。

ツールとして、Kali Linux を用い、Zumo とルンバへのペネトレーションテストを行う。IoT デバイスの動作ロジックは、Zumo の説明書から、有効となるログイン情報を取得する。攻撃経路は、Nmap コマンドを使用して、ポートスキャンを行い、どのポートが開いているかを確認する。ペネトレーションテストの目的は、Zumo とルンバを遠隔操作することである。ルンバと Raspberry Pi の接続は、ルンバオープンインターフェースと呼ばれるシリアルインターフェースを使用する。Zumo とは違って、シリアル変換アダプタを用いたハードウェアを介した侵入となる。

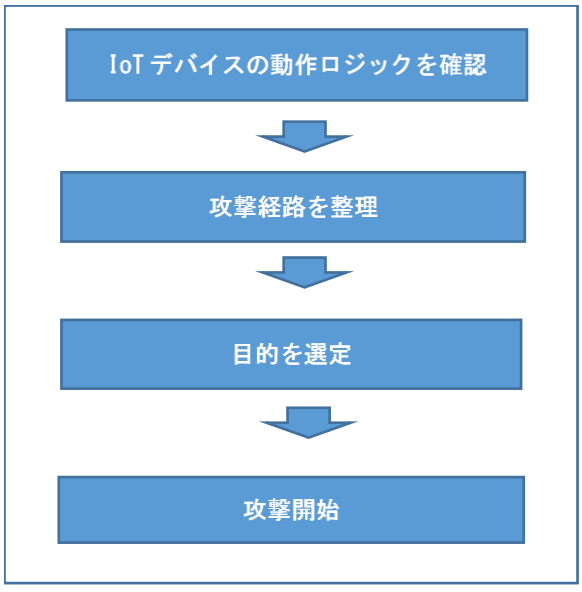

図1　IoT ペネトレーションテストの概要

4. 実験結果

説明書から得たログイン情報を用いて、Zumo の侵入に成功し、Zumo の起動にも成功した。ログイン情報を用いることで誰でも侵入でき、操作可能になるだけでなく、ログイン情報や中のデータを改ざんできる恐れがある。ルンバもポートスキャンの情報から Web ページにアクセスし、ルンバの起動に成功した。侵入されると侵入者からの制御が優先され、自律的な動作ができなくなる。

5. 考察

セキュリティ対策としては、SSH のポート番号変更、辞書型ブルートフォース攻撃をされないようにするためのパスワードの複雑化、root（管理者権限）のパスワード設定をしっかりすることが必要である。その他、Web ページのアクセスは http から https にリダイレクトにして暗号化する方法も考えられる。

6. まとめ

今後 IoT デバイスの数はますます増えていくので、セキュリティ問題は深刻化すると考えられる。今後は、多くの IoT デバイスを対象にペネトレーションテストを実施し、共通的な要素を抽出し、個人で実施可能なセキュリティ対策を明確にしていく。

参考文献

[1] 黒林檎・村島正浩, “ハッカーの学校 IoT ハッキングの教科書”(2018)
[2] 初心者向！Raspberry Pi 最低限のセキュリティ設定【所要時間 30 分】 https://qiita.com/mochifuture/items/00ca8cdf74c170e3e6c6(2019.12 閲覧)
[3] ペネトレーションテスト-Web アプリケーション侵入試験 https://cybersecurity-jp.com/ad-lp/31498(2019.12 閲覧)