IPカメラのセキュリティ調査手法の提案と検証

Proposal and Verification of a Security Investigation Method for IP Cameras

下山啓・ネットワーク分科会・情報セキュリティ大学院大学

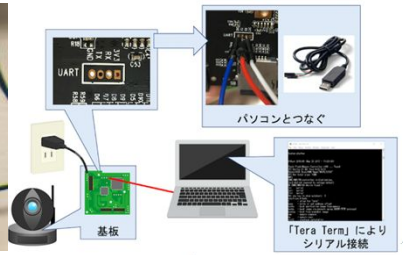
研究背景と目的

人の関与しないIoTデバイス特にIPカメラに対する攻撃数は増加しているが、堅牢なセキュリティが考慮されない設計となったデバイスが多い。IoTデバイスのセキュリティ向上を図るためには、多くのIPカメラのセキュリティについて調査を実施し、問題点を明らかにし、対策を考察することが必要。そしてその調査について、セキュリティ診断実施者などが容易に調査を行うことができるよう系統的な調査手法が必要。

提案調査手法

攻撃者視点に立ち、情報収集などの外側から内側に攻撃を進めていくイメージで、調査方法を提案。

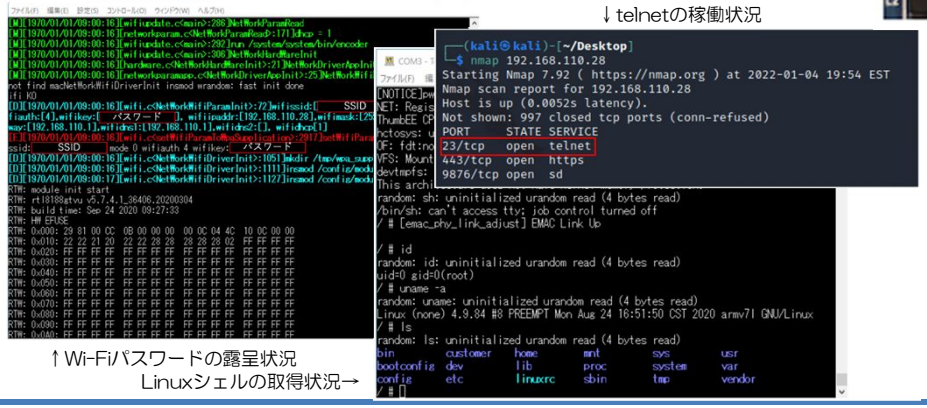
1. インターネット検索による調査（情報収集）
2. 通常利用時における動作の調査（ﾎﾟｰﾄｽｷｬﾝなど）
3. シリアル接続からの調査（起動ﾛｸの確認、U-boot・ｼｪﾙ操作）
4. ファームウェアからの調査（ﾌｧｰﾑｳｪｱ抽出・解析）



洗い出された問題点

- 起動ログによるWi-Fiパスワード流出
- U-bootのコマンド操作可能
- Linuxシェルの取得可能
- 管理者用パスワードの露呈
- 不要コマンドの存在
- 不要サービスの動作及び稼働可能
- 稼働ウェブサーバーの設定不備　など

容易に分解でき、またデバッグ用ポートが存在することがそもそもの問題点



↑Wi-Fiパスワードの露呈状況
Linuxシェルの取得状況→

対策案

【デバッグ用ポートを販売製品に残さない】

専門家などによる定期的なメンテナンスを必要としない安価で簡易的なIoTデバイスについては、故障時などに修理や原因調査などを行うことはなく買い換えるといった利用者が多いことから、デバッグ用ポートを必要としない。

◆デバッグ用ポートを残す必要がある場合
- 起動時のログなど不要な情報を表示しない
- Linuxのログイン認証をしない
- U-bootのプロンプトに入れない
  - 不要コマンドを残さない　などの対策が必要

IPカメラの動作にrootユーザーが利用されていることから、一般ユーザーを適切に利用することも重要

↓確認されたUART

今後の課題

本提案手法は、OSにLinuxが利用されるIPカメラを対象にしたものである。今後多くのIoTデバイスにおいてLinuxが利用されることが予想され、よって本提案調査手法の適用の可能性が考えられることから、調査手法の一般化を検討する。