5X-06

脆弱なパスワードが設定されたIoT機器の管理及びパスワード自動変更システムの開発

塩田晃平*　江川悠斗†　谷口義明*,‡　井口信和*,‡
近畿大学理工学部情報学科*
近畿大学大学院総合理工学研究科エレクトロニクス系工学専攻†
近畿大学情報学研究所‡

1. 序論

IoT 機器の数は年々増加しており，2022 年には約 350 億台まで増加するとされている[1]．そのため，ネットワークを経由したサイバー攻撃の増大が懸念されている．また，IoT 機器特有の性質として，脅威の影響範囲・影響度合いが大きいことや，IoT 機器の監視が行き届きにくいことが挙げられる．そのため，特定のIoT機器がマルウェアに感染した場合，関連システム・サービス全体へ影響が及ぶ可能性がある[2]．

2016 年には，脆弱なパスワードが設定された IoT 機器を標的としたマルウェア「Mirai」による Telnet を介した DDoS(Distributed Denial-of-Service)攻撃が甚大な被害を齎している．また，2019 年に 4，583 台の IoT 機器に対してパスワードの脆弱性を調査した研究がある．調査から，Telnet で使用する 23 番ポートが開いているものが 81 台あり，その内の 11 台に脆弱なパスワードが設定されていることが判明している[3]．

そこで本研究では，脆弱なパスワードが設定された IoT 機器の管理及びパスワード自動変更システム(以下，本システム)を開発する．本システムにより，22 番・23 番ポートが開いている脆弱なパスワードが設定された IoT 機器の存在の確認とそれを悪用した不正アクセスを防止することが期待できる．

2. 研究内容

本システムの構成を図1に示す．本システムはローカルサーバ上で動作し，LAN 上に存在する脆弱なパスワードが設定されたIoT機器のパスワードを自動的に変更し，それを管理する．IoT 機器管理画面では，本システムでパスワードを自動的に変更した全てのIoT機器を閲覧可能である．IoT 機器調査画面では，単一，もしくは複数のIoT機器を調査することが可能である．調査対象が単一の IoT 機器の場合，調査したい IoT 機器の IPv4 アドレス(以下，IP アドレス)を直接入力することで調査が可能である．複数の IoT 機器の場合，IP アドレスに加えて CIDR 表記のサブネットを入力することで調査が可能である．また，本システム上で入力をプライベート IP アドレスのみに制限しているため，LAN 上に存在するIoT機器に限定して調査することが可能である．調査から，脆弱なパスワードが設定された IoT 機器を発見した場合，本システムで，その IoT 機器のパスワードを自動的に強固なパスワードに変更する．これにより，総当たり攻撃等のパスワード攻撃に対して，LAN 上の IoT 機器の保護が可能となる．以下に実装した機能について述べる．

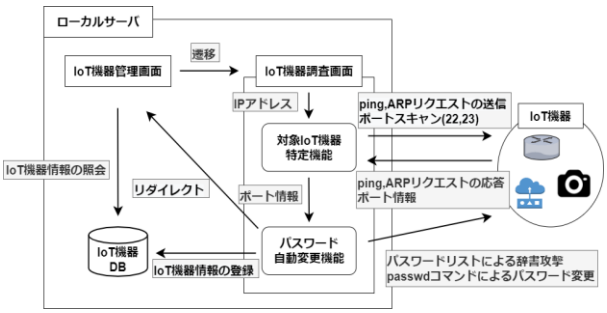

図 1:システム構成図

2.1. 対象 IoT 機器特定機能

本機能は，利用者が LAN 上に存在する IoT 機器から 22 番・23 番ポートが開いている遠隔操作可能な IoT 機器を特定する機能である．ここでは単一の IoT 機器に対する調査の方法を示す．

はじめに，利用者は IoT 機器調査画面から調査する IoT 機器の IP アドレスを入力する．本システムは IP アドレスが入力されると，入力された IP アドレスに ping を送信し，IoT 機器との疎通を確認する．また，ping に応答しない IoT 機器も存在するため，ARP テーブルの確認による IoT 機器との疎通も確認する．その後，疎通を確認した IoT 機器に 22 番・23 番ポートを対象としたポートスキャンを実行し，どちらかのポートが開いていれば対象 IoT 機器として本システム上に一時的に記録する．本機能により，LAN 上に存在する 22 番・23 番ポートが開いている IoT 機器の特定が可能となる．

2.2. パスワード自動変更機能

本機能は，脆弱なパスワードが設定された対象 IoT 機器のパスワードを自動的に変更する機能である．

はじめに，対象 IoT 機器特定機能で特定した IoT 機器に対して，脆弱なパスワードが設定されているかどうかを確認するために辞書攻撃を行う．利用者はユーザ ID・パスワードの組み合わせが 360 通りの簡易辞書と 2，500 通りのハニーポット辞書から使用する辞書を選択可能である．ハニーポット辞書は，22 番・23 番ポートの攻撃パケットを観測する Cowrie というハニーポットから収集したユーザ ID・パスワードの上位 50 件を抽出している．本研究において，これらの辞書に含まれている文字列を

Development of a Management and Automatic Password Change System for IoT Devices with Weak Passwords,
Kohei SHIOTA*, Yuto EGAWA†,
Yoshiaki TANIGUCHI*,‡,Nobukazu IGUCHI*,‡
* Kindai University, Faculty of Science and Engineering
† Kindai University, Department of Electronics and Systems Engineering, Interdisciplinary Graduate School of Science and Engineering
‡ Kindai Univesity, Cyber Infomatics Research Institute

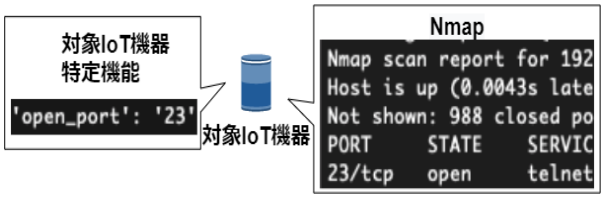

図 2:対象 IoT 機器特定機能と Nmap の比較一例

脆弱なパスワードと定義する. 辞書攻撃により対象 IoT 機器にログインが可能である場合, 対象 IoT 機器のパスワードを自動的に強固なパスワードに変更する. 本研究では, 強固なパスワードとは半角大小英数字・記号かつ 15 文字のランダムな文字列のことを示す[4]. パスワード変更後, IoT 機器 DB に変更した IoT 機器の IP アドレス, MAC アドレス, ユーザ ID, パスワード, 登録日時を登録する. 本機能により, LAN 上の脆弱なパスワードが設定された IoT 機器の存在を防ぐことが可能となる.

3 実験・考察

実験では, 2 つの性能評価を行った. 性能評価 1 では, LAN 上に存在する IoT 機器から対象 IoT 機器を正しく特定することが可能であるか計測した. 性能評価 2 では, 脆弱なパスワードを設定した対象 IoT 機器のパスワードが自動的に正しく強固なパスワードに変更されているか確認した. 実験環境には, 実験用 LAN と対象 IoT 機器 4 台と 22 番・23 番ポートが開いていない対象外の IoT 機器 6 台を用意した. 実験で使用したサーバ PC は, CPU:Intel Core i5 1.6GHz, Memory:8GB, OS:Mac OS Catalina 10.15.6 である.

性能評価 1 では, まず, 用意した対象 IoT 機器と対象外の IoT 機器を全て LAN 上に接続し, 対象 IoT 機器特定機能を動作させる. 次に, Nmap で SYN スキャンを実験用 LAN に実行し, 22 番・23 番ポートが開いている IoT 機器のポート情報を取得する. その後, 対象 IoT 機器特定機能で取得した対象 IoT 機器のポート情報と Nmap で取得したポート情報を比較する. 比較した結果の一例を図 2 に示す. 左側が対象 IoT 機器特定機能で取得した対象 IoT 機器のポート情報, 右側が Nmap で取得したポート情報である. 実験の結果, 対象 IoT 機器特定機能で取得した情報は全て対象 IoT 機器であり, ポート情報も 22 番・23 番ポートのどちらかが開いていることを確認した. このことから, LAN 上に IoT 機器が 10 台接続された環境下において, 22 番・23 番ポートが開いている IoT 機器を対象 IoT 機器として特定可能であることを確認した.

性能評価 2 では, まず, ユーザ ID と脆弱なパスワードを設定した対象 IoT 機器を 1 台用意する. 対象 IoT 機器に設定したユーザ ID・パスワードの例を表 1 に示す. 次に, パスワード自動変更機能を動作させ, 対象 IoT 機器のパスワードを自動的に変更する. その後, ユーザ ID・変更前パスワードと本システムに記録してあるユーザ ID・変更後パスワードでログイン操作を手動で実行する. 最後に, ユーザ ID・変更後パスワードでのみログイン可能であることを確認する. これを辞書毎に 10 回ずつ

表 1:設定したユーザ ID・パスワードの例

ユーザ ID	パスワード
root	123456
guest	000000
mother	asdfghjkl
support	iloveyou
888888	password1

表 2:変更した対象 IoT 機器のパスワードの例

変更後パスワード
XBx6n;k|p{?.aLX
Yez=[v4hCwgnGyI
/4od<[1|gy9,oS
JKw%a[~?~jhL(e*
jKw&H$BE(~_<Hd@

実行する. 実験の結果, どちらの辞書においても 10 回中 9 回, 自動的に強固なパスワードに変更され, ユーザ ID・変更後パスワードのみログイン可能であることを確認した. また, パスワード自動変更機能で自動的にパスワードを変更した対象 IoT 機器のパスワードの例を表 2 に示す. どちらの辞書においても 1 度パスワードが変更されなかった原因として, 今回使用した IoT 機器はデフォルトで root ログインが拒否されていたからであった. 実験により, 脆弱なパスワードが設定された IoT 機器のパスワードを自動的に正しく強固なパスワードに変更できることを確認した.

4 結論

本研究では, 脆弱なパスワードが設定された IoT 機器の管理及びパスワード自動変更システムを開発した. 実験から, LAN 上の対象 IoT 機器を正しく特定することと脆弱なパスワードが設定された IoT 機器のパスワードを自動的に正しく強固なパスワードに変更できることを確認した. これにより, 22 番・23 番ポートが開いている脆弱なパスワードの IoT 機器の存在の確認とそれを悪用した不正アクセスを防止することが期待できる.

今後は, 80 番ポートも対象 IoT 機器として分類できるように対象 IoT 機器特定機能の拡張を行う予定である.

参考文献

1) 総務省:情報通信白書,入手先<https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r02/html/nd114120.html>(参照 2020-11-27)
2) 総務省:IoT セキュリティガイドライン, 総務省(オンライン), 入手先<https://www.soumu.go.jp/main_content/000428393.pdf>(参照 2020-08-16)
3) 舟根優作,永見健一,遠藤貴裕,時崎涼輔:IoT デバイス管理システムによる家庭 LAN 内の IoT デバイス脆弱性調査,コンピュータセキュリティシンポジウム 2019 論文集,Vol.2019,pp.1313-1320(2019)
4) Oregon FBI Tech Tuesday: Building a Digital Defense with Passwords,入手先<https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/oregon-fbi-tech-tuesday-building-a-digital-defense-with-passwords>(参照 2020-11-26)