ポスター | 第40回医療情報学連合大会（第21回日本医療情報学会学術大会） | ポスター発表

ポスター7
薬剤情報システム・モバイル/セキュリティ

2020年11月20日(金) 11:20 ～ 12:20 G会場 (イベントホール・特設会場2)

[3-G-2-07] 無線通信の中間者攻撃による医療情報窃取の危険性についての検討

*渡辺 和典[1]、吉澤 智之[1] （1. 株式会社FYF）
*Kazunori Watanabe[1], Tomoyuki Yoshizawa[1] （1. 株式会社FYF）

キーワード：Security, WiFi, Man in the Middle Attack, MitM

昨今の医療業界では多くの施設内に無線 LANが整備されている。無線 LANは電波の届く範囲であれば誰もがアクセスができてしまう特性上、正規の通信経路に割り込むことで通信を窃取する中間者攻撃の危険性がある。有線 LANであれば NW機器の未使用ポート装置側で通信を止めること等で中間者攻撃を防ぐことが可能だが無線 LANはこうした対策が難しい。無線 LANはセキュリティ機能として接続時の認証方式がいくつかある。本稿では認証方式の違いによる中間者攻撃のリスクについて検証する。中間者攻撃は、正規の無線 AP（以下 AP)に正規の APに偽装した不正な APを接続し、正規の端末を不正 APに接続させる。これにより、不正 APは正規 APと端末の間で通信を中継するため、情報窃取が可能となる。つまり、この不正 APを構成するための要件として、正規の APの接続情報が必要である。本稿では、 WEP、 WPA2-PSK、 WPA2-EAP、 WPA3-SAEを対象として、中間者攻撃の実行可能性について考察する。実験により WEP及び WPA2-PSKについては、総当たり攻撃によるパスワード解析が現実的な時間で可能であり、中間者攻撃が可能であった。 WPA2-EAPは、認証サーバーを用いて相互認証するため中間者攻撃が難しい。また、 WPA3-SAEについては WEPや WPA2-PSKと同様の事前共有鍵による認証だが、より堅牢な鍵交換プロトコルによりパスワード解析が難しいことが分かった。これらの結果より、医療機関では WPA2-EAP方式もしくは WPA3-SAEを採用することが望ましいと考えられる。 WPA2-EAP方式はユーザー毎の ID、パスワードや電子証明書等の管理が必要になる為、運用負荷が高くなる。一方、 WPA3-SAEは運用負荷は低いが WPA3に対応している製品を揃える必要がある。各医療機関に適した認証方式を採用されることが望ましい。

無線通信の中間者攻撃による医療情報窃取の危険性についての検討

渡辺　和典[*1]、吉澤　智之[*1]、
*1 株式会社 FYF

A study on the risk of medical information theft by Man-in-the-Middle Attacks in wireless communication

Kazunori Watanabe[*1], Tomoyuki Yoshizawa[*1]
*1 FYF Inc.

Abstract in English comes here.

With the recent spread of IT in the medical industry, wireless networks has been installed in many medical facilities. These network systems require measures to prevent unauthorized accesses use by outsiders. In this paper, we consider how to construct and operate the wireless networks in medical facilities, and confirm that WPA2-PSK can be accessed illegally by a password attack and can also be used to steal information by a Man-in-the-Middle attack. From these verification results, it was found that WPA2-EAP or WPA3 is the preferred authentication method for medical facilities now. However, as a practical matter, not all healthcare organizations are able to take such measures due to the technical difficulty problems. So we also need to consider the strength of our passwords to slow down the attack.

Keywords: Security , WiFi , Man-in-the-Middle Attacks

1. 緒論

昨今の医療業界への IT の普及に伴い、多くの施設内に有線 LAN 及び無線 LAN が整備されてきており、これらのネットワークシステムは部外者等に不正に利用されないような対策が必要である。有線 LAN は、安全な場所に設置したネットワーク機器側で通信を制御することや、壁面情報コンセント等の有線 LAN ポートへ近づけさせない等の物理的な対策によって、接続できる人や端末を制御できる。一方、無線 LAN は電波の届く範囲であれば誰でもアクセスを試みることができるため、有線 LAN のような物理的な対策を取ることが難しく、アクセスポイント(以下 AP)とクライアント間での暗号化によって、通信の安全性及び秘匿性を担保する仕組みとなっている。この暗号化の仕組みは 1997 年頃に登場した WEP に始まり、時代とともに、より強い暗号化の技術が次々と開発されている。弱い暗号方式を使用している場合、様々な攻撃をうける恐れがあり、その中で本稿では中間者攻撃に着目した。中間者攻撃というのは、正規の通信経路を、不正な機材等により中継し、通過する通信の内容を窃取し、または改ざんすることを指す。有線 LAN ネットワークに対して中間者攻撃を行う場合、ネットワーク機器や情報コンセントに対して、LAN ケーブルで接続することが必要となるため、発覚の恐れがあり、攻撃の難易度は高い。一方、無線 LAN については物理的なケーブルは不要のため、暗号方式さえ突破できれば、怪しまれることなく実行可能である。

2. 目的

本稿では、医療機関で無線 LAN を使用する際に、どのような点に注目して構築、運用をすべきかについて検討する。悪意のある第三者が各種暗号方式に対してどのような攻撃が可能なのか、またその容易性について実際に機材を用いて検証する。そのうえで中間者攻撃が実際に行われた際の想定される被害の検討を行い、適した暗号方式やその運用方法について考察を得ることを目的とする。

3. 方法

本稿では攻撃を2つの段階に分けて実施した。まず WPA2-PSK に攻撃を行い、事前共有鍵(以下、パスワード)を解析し、その後、対象の無線ネットワーク上に流れている通信を傍受した。

3.1 WPA2-PSK の攻撃

WEP については、暗号強度が弱いことが知られており[1)]、推奨されていない。従って現状、広く一般的に使用されている WPA2-PSK に攻撃を行う。使用する機材は、一般的な IEEE802.11a/b/g/n/ac に対応した無線 AP、DICOM サーバ及びクライアント用の Windows10 PC、ペネトレーションテスト用 Linux ディストリビューションの Kali Linux(以下攻撃用 PC)と、IEEE802.11 フレームをキャプチャーするための無線 LAN アダプタ(ALFA Networks Atheros AR9271)を使用した。WPA2-PSK のパスワード攻撃の流れは Aircrack-ng というツールを用いて次の手順で行う。

1. 対象の無線 AP の SSID、または MAC アドレス(BSSID)を特定する
2. 攻撃用 PC 側の無線 LAN アダプタをモニターモードにし、IEEE802.11 フレームのキャプチャーを開始する
3. 無線 AP にクライアントの認証が行なわれるまで待つか、あるいは、既に認証済みのクライアントの認証解除をさせるパケットを送信し、再度認証されるのを待つ
4. クライアントの認証時に発生する 4way Handshake のパケットを収集する(図1)
5. 別途用意したパスワードリストと呼ばれるテキストファイルを用い、手順 4 で取得したパケットから、無線 AP のパスワードを解析する(以下辞書攻撃)

3.2 中間者攻撃

前項で得た、パスワードを使用し、無線APへのアクセスし、ARP スプーフィングと呼ばれる手法で中間者攻撃を行う。ARP スプーフィングとは、正規のクライアントからの ARP 要求に対して、攻撃者が不正な ARP 応答を返すことで、通信を攻撃者の機器を中継させる手法である(図 1)。

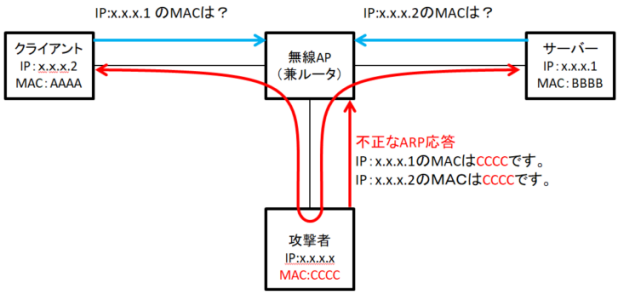

図 1　ARP スプーフィング概略図

4. 結果

3.1 項の WPA2-PSK の辞書攻撃を行った結果を図2に示す。

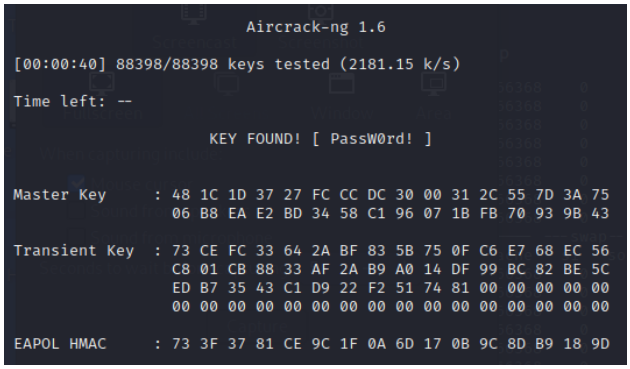

図 2　パスワード解析完了画面

尚、攻撃用 PC は Intel® Core™ i7-6600U（2.81GHz:2コア 4スレッド）を用いたところ、パスワードの解析は概ね毎秒 2000～2200 個程度の速度で進捗した。

攻撃者は、無線 AP への不正アクセス後、LAN 内のサーバまたはネットワーク機器になりすますことで通信の傍受が可能になる。Ettercap というツールを使用して、ARP スプーフィングを実際に行ってみた結果を図 3 及び図 4 に示す。まず、Ettercap を起動して端末の検索をかけると、LAN 内に存在する IP とその端末の MAC アドレスが表示される。攻撃者は、その中から中継したい 2 つの端末をそれぞれ Target に指定して開始する、という極めて簡単な操作だけで実行できた。

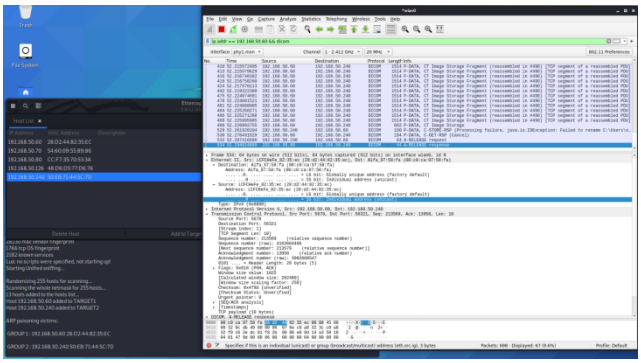

図 3　中間者攻撃実行中画面（全体）

ARP スプーフィングを実行した状態で、DICOM サーバの IP アドレスが 192.168.50.60 で、クライアント PC の IP アドレスが 192.168.50.240 として DICOM 通信を発生させたところ、攻撃者 PC に DICOM 通信が流れてくることが確認できた（図 4）。これを見ると、IP アドレスはお互い正しい宛先を指定しているが、

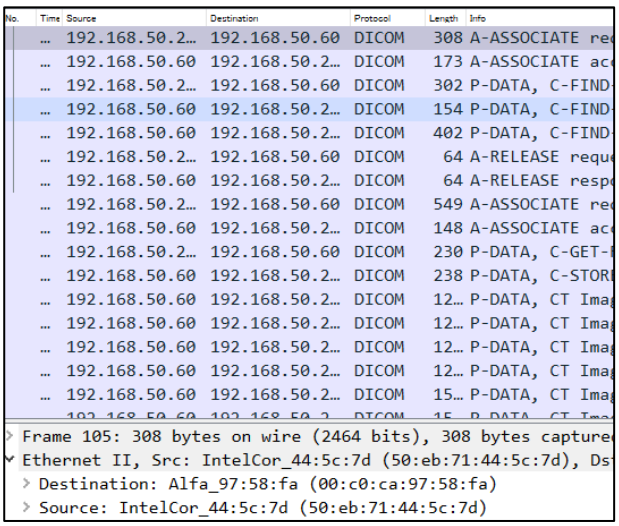

図 4　中間者攻撃実行中の攻撃用 PC でのパケットキャプチャ

MAC アドレスは攻撃者 PC の Alfa networks（00:c0:ca:97:58:fa）のものとなっており、中間者攻撃が成功していることがわかる。

今回、中間者攻撃の手法として ARP スプーフィングを使用したが、その他の手法として Evil Twin と呼ばれる不正な無線 AP を正規の無線 AP として振る舞い、無線通信を中継する手法もあるが、いずれも WPA2-PSK のパスワード攻撃の成功が実行可能な条件となっている。

5. 考察

5. 1. 攻撃手法の容易性について

今回使用した攻撃はいずれも Kali Linux に標準インストールされているソフトのみで行うことができた。Kali Linux は、インターネット上で無償配布されており、誰でも使用可能であり、今回の攻撃も手順さえ知っていれば実行可能なため、技術的な難易度は低い。

5. 2. パスワード解析について

今回実施した検証では、WPA2-PSK のパスワード攻撃が成功した場合に情報の窃取が可能であることが確認できた。攻撃者は任意のルールを設定して膨大なワードリストを生成することができるため、現時点で存在しているワードリストに含まれていなければ安全ということにはならない。今回の攻撃手法は、医療施設の現地に出向いて行う類の攻撃であることから、標的型の性質が強い。従って、対象施設の関係の単語、あるいはその特定の施設に関連するキーワードを用いてワードリストを作成し攻撃を仕掛けてくることが想定される。

また、WPA2-PSK のパスワード解析の作業自体は、現地でなくても実行できる点も攻撃者にとっては都合が良い。4way Handshake のパケットを取得できた場合、それを持ち帰り、別の場所で解析ができる。高性能なマシン、あるいはクラウドサービス等で提供される GPU や FPGA を使用したマシン [2)]等での解析により 1 秒間あたり数十万～数百万個という高速な解析等も可能だ。

5. 3. 対策と課題

無線の認証規格は次々と新しいものが開発されてきており、現在では WPA3 という規格が普及し始めている。WPA2-PSK と同様のパスワードによる認証方式である WPA3-SAE はより高度な認証アルゴリズムが採用されており、辞書攻撃への耐性が向上している。また、従来の WPA2 でもデジタル証明書を利用

した EAP 方式であれば、不正な端末がアクセスできなくなるため安全性は高くなる。しかし、いずれの場合も、対応する機材を用意する必要があり、またEAP 方式を採用する場合は、デジタル証明書を使用するため、運用上の負荷が増えることが考えられ、医療施設によっては導入が難しいことが課題だ。

5.4. WPA2-PSK を使用する上での注意事項

WPA2-PSK を採用しつつ、セキュリティ面の安全性を担保するためには、強いパスワードを使用することが考えられる。強いパスワードとは、多くの文字種かつ、長い文字列である。但し、文字種を増やす方法としてよく使われている、例えば、”a”を“@”に、”S”を”$”に置き換えて文字種を増やす手法は良く知られており、攻撃者に推測されやすい。またこの他にも、キーストロークのパターンや、複数の単語を使用する場合はその単語間の順序性、関連性等、パスワードの強度を下げる要因は様々だ。

6. 結論

本稿では、無線アクセスポイントに対するパスワード攻撃及び中間者攻撃を通じ、認証方式によるリスクについて検証した。WPA2-PSK を使用している場合、時間をかければ、いずれはパスワード解析に至り、これを用いることで情報窃取が可能であることが確認できた。新しい規格のWPA3や、証明書を用いたEAP認証方式を採用すれば、この問題は解消されるが、必ずしも全ての医療施設で採用できるものではない。パスワードの強度を高めることで、攻撃を遅らせることは可能だが、運用上の負荷とのバランスについては考慮が必要だ。

参考文献

1) IPA 情報処理推進機構　一般家庭における無線 LAN のセキュリティに関する注意
[https://www.ipa.go.jp/security/ciadr/wirelesslan.html(cited 2020-Aug-31)].

2) Markus Kammerstetter , Markus Muellner , Daniel Burian , Christian Kudera , Wolfgang Kastner . Efficient High-Speed WPA2 Brute Force Attacks using Scalable Low-Cost FPGA Clustering, Wien: Vienna University of Technology, 2016
[https://eprint.iacr.org/2016/547.pdf (cited 2020-Aug-31)]