様式 C-19

科学研究費補助金研究成果報告書

平成２３年６月１２日現在

機関番号：１５４０１
研究種目：若手研究（B）
研究期間：２００９～２０１０
課題番号：２１７０００１８
研究課題名（和文）ストリーム暗号の安全性評価手法に関する研究

研究課題名（英文）A STADY ON EVALUATION METHOD FOR STREAM CIPHER

研究代表者
大東　俊博（OHIGASHI TOSHIHIRO）
広島大学・情報メディア教育研究センター・助教
研究者番号：８０５０８１２７

研究成果の概要（和文）：
本研究では，ストリーム暗号を利用した無線 LAN プロトコル WPA-TKIP について，改ざん攻撃への安全性を評価した．従来の方法は IEEE802.11e (QoS 機能)を利用した通信のみ改ざん可能という制限があったが，本研究で提案した攻撃対象のパケットを QoS パケットへ修正の上で改ざんする方法ではその制限を回避できることが分かった．さらに，改ざん攻撃の手順を改良することで攻撃の実行時間を削減することに成功した．その結果，WPA-TKIP において偽造した DNS サーバの IP アドレスを受理させる攻撃が実環境で実行できることが明らかになった．

研究成果の概要（英文）：
In this research, I proposed falsification methods against WPA-TKIP, which is a security protocol for wireless LAN with stream cipher, for evaluating its security. Previous method succeeds only for a network that supports IEEE802.11e QoS features. First, I removed this condition by modifying any packet to QoS packet. Second, I improved the execution time of the falsification method, and it enables DHCP-DNS attack, which is a method to accept forgery IP address of DNS server, in a realistic environment.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2009 年度	1,100,000	330,000	1,430,000
2010 年度	600,000	180,000	780,000
年度			
年度			
年度			
総　計	1,700,000	510,000	2,210,000

研究分野：情報セキュリティ
科研費の分科・細目：情報学・情報学基礎
キーワード：暗号系，ストリーム暗号，無線 LAN，WPA-TKIP

１．研究開始当初の背景

通信の高速化及び情報の大規模化に伴い，高速処理に優れた暗号化技術であるストリーム暗号の需要は高くなっている．しかしながら，ストリーム暗号の安全性評価の研究は十分に成熟しているとはいえず，包括的な評価基準が定まっているとは言い難い．ストリーム暗号の安全性評価に関する技術を向上させ，その基準を作るためには，暗号アルゴリズム単体への解読法(攻撃)や暗号プロトコルへ応用した場合での攻撃について議論をし，脆弱性が生じる要因を分析することが重要になる．

本課題の開始当初には，ストリーム暗号のアルゴリズム単体では Cube 攻撃や差分攻撃，暗号プロトコルでは無線 LAN で用いられる

WEPへの鍵復元攻撃やWPA-TKIPへの改ざん攻撃が新たに提案されていた．予備調査としてこれらの文献のサーベイを行った結果，WPA-TKIP への改ざん攻撃は重大な欠陥となり得る可能性が高く，市販されている無線LAN 製品の安全性に関わる緊急性の高いものであったため WPA-TKIP の安全性に関する検討を優先して実施することとした．

WPA-TKIP に対する初めての改ざん攻撃(Beck-Tews 攻撃)は 2008 年に Beck と Tews によって提案された．この方法は WEP 用に開発された chopchop 攻撃というリプレイ攻撃に基づく方法を WPA-TKIP に適用したものであり，IEEE802.11e(QoS 機能)に対応した無線LAN 機器のみに有効な方法であった．また，その攻撃の実行時間は攻撃対象の暗号化パケットの未知のバイト数に依存する．具体的には，ARP パケットという攻撃が容易なパケットに対して，改ざん検知用の鍵(MIC 鍵)の導出に 12 分程度，ARP パケット自体の改ざんに 4 分程度の時間が必要となる．

さらに，Beck-Tews 攻撃は DHCP によって配布される DNS サーバの IP アドレスを改ざんする攻撃(DHCP-DNS 攻撃)にも応用されたが，40 分程度の実行時間が必要となる．この攻撃は MIC 鍵が更新された場合に無効化され，市販の製品の初期設定では MIC 鍵が 30 分で更新される設定が多くあることから，DHCP-DNS 攻撃は直接的な脅威とはなり難い状況であった．

２．研究の目的

Beck らは WPA-TKIP における改ざんに関する安全性について一定の評価を与えた．しかし，その結果だけでは安全性について判断するには不十分であり，厳密な評価が必要であった．そこで，本課題では Beck-Tews 攻撃を複数の観点から分析し，攻撃手法を拡張することで WPA-TKIP の安全性について更なる評価を与えることを目的とした．具体的には以下の 2 つの観点から検討を行った．

（１） 攻撃対象の拡張

Beck-Tews 攻撃では IEEE802.11e 対応機器が攻撃対象であったが，そのような機器の条件を前提としない方法が存在するかについて検討する．もし IEEE802.11e 対応機器に限定される特別な攻撃しか不可能であるならば，IEEE802.11e に対応していない製品を使う，または OS レベルで IEEE802.11e を無効化することで改ざん攻撃を回避できる．

（２）攻撃実行時間の短縮

Beck-Tews 攻撃の手順を改良することで，攻撃実行時間を短縮することが可能かについて検討する．攻撃実行時間は安全性を確保するための MIC 鍵の更新タイミングの決定に影響し，市販の製品の初期設定で安全に運用できるかについて判断する材料となり得る．

３．研究の方法

（１）攻撃対象の拡張

① Beck-Tews 攻撃とその能力

Beck-Tews 攻撃の基となった chopchop 攻撃は過去に通信路に流れた暗号化パケットを再送する方法(リプレイ攻撃)によってパケットの解読及び改ざんを実現する．WPA-TKIP では暗号化パケットに付加しているカウンタ(TSC と呼ぶ)及び受信者のカウンタ(TSC カウンタ呼ぶ)を利用し，暗号化パケットの送信/受理の毎にカウントアップさせる．受信者は TSC カウンタより小さな TSC を持つ暗号化パケットを棄却することでリプレイ攻撃を防ぐ．

Beck-Tews 攻撃では IEEE802.11e を採用することにより QoS 制御をしている通信に注目した．IEEE802.11e では優先度が付加されたパケット(QoS パケット)をやり取りし，WPA-TKIP では受信者は優先度毎に TSC カウンタを保持する．Beck と Tews は QoS パケットの優先度の値を変化させても WPA-TKIP ではそのパケットを受理する点に注目し，TSC カウンタの値が小さい優先度を探し，その値に QoS パケットの優先度を書きかえる方法でリプレイ攻撃を成立させている．この方法によって chopchop 攻撃が実行でき，パケットの解読および改ざんが可能となる．

② 中間者攻撃の検討

攻撃対象を拡張する一つの方法として中間者攻撃のモデルを導入することが考えられる．中間者攻撃とは，攻撃者が送信者と受信者の間に入り，通信の妨害・傍受・改ざんを行える攻撃モデルである．このモデルでは受信者にパケットを受理させずに暗号化パケットを傍受することが可能であるため，攻撃者が自由に改ざんできる暗号化パケットの TSC 値は TSC カウンタの値より必ず小さくなる．したがって，IEEE802.11e を利用しない場合でもリプレイ攻撃が可能となる．

中間者攻撃のモデルは Beck らの論文でも触れられており，本課題でも攻撃の手順を複数のモードの単位に分割する方法で詳細を検討している．しかしながら，中間者攻撃はパケットの送受信の妨害が必要となるため，無線 LAN の利用者や攻撃者の位置や機器の性能など，実行環境の制限が大きく，実環境では実行に困難が生じることが考えられる．そこで，Beck-Tews 攻撃と同程度の環境で実行可能な攻撃として以下の方法を検討した．

③ QoS 偽造攻撃の提案

Beck-Tews 攻撃では優先度の値を改ざんしても受信者にパケットを受理させられることを利用したが，本課題では優先度のフィールドが存在しない非 QoS パケットから QoS パケットへ改ざんする場合でも chopchop 攻撃

を動作させる方法(QoS 偽造攻撃)を提案する．QoS パケットを受信できるように製造された IEEE802.11e 対応の無線 LAN クライアントの場合，非 QoS パケットしか流れないネットワークで QoS パケットが送信されたとしても，それに対応する優先度の TSC カウンタを使ってチェックをしてしまうためパケットを受理すると予想される．

次に IEEE802.11e を使用可能にした無線 AP の通信について考える．この無線 AP は「QoS パケットを扱える」わけであり，「QoS パケットのみしか通信できない」わけではない．この無線 AP に接続している無線 LAN クライアントは全てが IEEE802.11e を利用しているわけではなく，QoS パケットと非 QoS パケットの通信が混ざっている状態となる．このような環境で正常に通信を成立させるためには，IEEE802.11e に非対応な製品でも「QoS パケットを作ることはできないが QoS パケットを受信するはできる」必要があると考えられる．この予想が正しい場合，多数の無線 LAN クライアントに対して QoS 偽造攻撃は有効に働くことになる．

（２）攻撃実行時間の短縮

① Beck-Tews 攻撃とその能力

Beck-Tews 攻撃の基となった chopchop 攻撃は，ストリーム暗号により暗号化され，CRC32 をチェックサムとして利用している条件での攻撃である．WPA-TKIP で chopchop 攻撃を実行する場合，MIC エラーと呼ばれるパケットを観測する毎に 1 バイトの平文情報が得られる．平文情報は下位バイトから上位バイトに向かって順に得ることができ，既知のバイトの処理は省略することができる．MIC エラーが 1 分間に 2 回以上送信されると MIC 鍵が更新される仕組みが導入されているため，x バイトの平文を得るためには少なくとも x-1 分の時間を要する．さらに，WPA-TKIP では暗号化パケットの全ての平文を得ることができれば，無視できる程度の時間で MIC 鍵を得ることができ，改ざんを検知されないパケットを作ることができる．

Beck-Tews 攻撃では MIC 鍵を短時間で得るために ARP パケットに注目している．ARP パケットは推測可能なデータが多く，Beck らは送信者と受信者の IP アドレスの最下位バイト(2 バイト)だけが未知というモデルで議論している．実際はデータの後ろに連結される MIC(8 バイト)とチェックサム(4 バイト)を含む 14 バイトが未知となる．チェックサムはデータと MIC から CRC32 によって計算される．Beck-Tews 攻撃は MIC とチェックサムの 12 バイトを chopchop 攻撃で復元する．その後，データの 2 バイトを全通り試してチェックサムが一致する値を探すことで正しいデータを復元する．これらの処理に要する時間は 12 分程度となる．

Beck-Tews 攻撃の改ざん処理を行う際，自由に暗号化パケットを作るために正規の平文の情報を得る必要がある．ARP パケットを改ざんする場合は 14 バイト必要となるわけである．MIC 鍵を手に入れている場合には平文を復元する時間は短縮される．MIC は MIC 鍵と IEEE802.11 ヘッダ(既知のバイト列)とデータから計算される値である．すなわち，データの 2 バイトに依存して MIC は一意に決定される．そのため，チェックサムの 4 バイトだけ chopchop 攻撃で復元した後，データの 2 バイトとそれに対応する MIC から計算されるチェックサムが一致するものを探すことで正しいデータと MIC の値を復元できる．これらの処理に要する時間は 4 分程度である．

② reverse chopchop 攻撃の提案

本課題では chopchop 攻撃を利用して得る平文情報について注目する．MIC やチェックサムは事前に推測することが困難であるが，データの中には長時間変更されない値も存在する．例えば IP アドレスと MAC アドレスの関係は MIC 鍵の更新時間と比べても長い間変化しない場合が多い．このような，時間経過によって変化が少ない平文情報を知ることができれば，その後に実行される攻撃で推測する必要があるバイト数を減らすことができるため高速化を果たせる．このような，時間経過によって変化が少ない平文情報を知るための攻撃を「情報収集攻撃」と呼ぶ．

情報収集攻撃に chopchop 攻撃を利用したとき，下位バイトから復元する性質より，MIC とチェックサムを復元するために余計に 11 分程度の時間を要するため効果的とは言えない．そこで，本課題では未知のバイトを上位バイトから順に復元する reverse chopchop 攻撃を提案する．この方法は WEP 用として Arbaugh によって提案された方法と同様の原理であり，chopchop 攻撃のように MIC エラーを観測する必要がある．reverse chopchop 攻撃を用いた場合，直接データから復元することが可能なため，情報収集攻撃の実行時間が短くなる．

４．研究成果

（１）攻撃対象の拡張

まず初めに QoS 偽造攻撃の手順について与えた．非 QoS パケットを改ざんする際には，IEEE802.11 ヘッダの Frame Control の値を 0x08 から 0x88 へ変更し，QoS Control フィールドを追加することで QoS パケットへ変更することができる．このような変更を施した暗号化パケットでも chopchop 攻撃や reverse chopchop 攻撃は正常に働き，データや MIC，チェックサムの情報が得られることが分かった．なお，MIC の計算には IEEE802.11 ヘッダの情報が含まれているため，MIC 鍵を復元

するアルゴリズムにQoSパケットへの改ざんによって生じる差異を含める必要があった．

次に，QoS 偽造攻撃の有効性を確認するために実証実験を行った．無線LANクライアントは複数の会社の製品(会社名は仮名)でUSBタイプ，CardBus タイプ，内蔵チップ等，異なる条件で10種類用意した．10種類の中には，IEEE802.11e に対応していると仕様書などには記載されていない製品(OSからも利用できることが確認できない）も含まれている．これらの無線LANクライアントが接続する無線 AP は IEEE802.11e に対応していない機器であり，QoS パケットの通信が無いためBeck-Tews 攻撃では攻撃ができない．この条件の下，QoS偽造攻撃により無線APから無線LANクライアントへ送信される非QoSパケットARPをQoSパケットへ改ざんする．実験ではARPパケットを対象とし，無線LANクライアントがARPのテーブルを更新したことを確認できれば攻撃成功と判断している．

表１　QoS偽造攻撃による実証実験の結果

製品	IEEE802.11e	発売年	結果
A社(USB)	対応	2007	成功
A社(USB)	未対応	2007	成功
A社(Card Bus)	未対応	2004	失敗
B社(USB)	未対応	2009	成功
B社(Card Bus)	未対応	2006	失敗
C社(Card Bus)	未対応	2007	成功
D社(Card Bus)	未対応	2006	成功
E社(内蔵チップ)	対応	2008	成功
F社(内蔵チップ)	対応	2008	成功
G社(内蔵チップ)	対応	2006	成功

＊ 無線LANクライアントのIEEE802.11eへの対応の有無はWebページや製品仕様に記載されているかにより判断した

実験結果を表１に示す．IEEE802.11e に対応している全ての無線LANクライアントに対して改ざんが成功しており，QoS 偽造攻撃が有効に働いていることを確認できる．また，IEEE802.11e に非対応とされている無線 LANクライアントでも多くの場合で攻撃が成功しており，３．（１）で述べたように無線LANクライアントはQoSパケットを受信する機能を持っており，IEEE802.11e に対応していないと記載されている場合でも本攻撃の影響を受けることが分かった．また，IEEE802.11e対応機器において，OSの設定でIEEE802.11eを無効にした場合でも攻撃は成功したことを確認している．

実験で攻撃が失敗している機器について詳細を調べた．A 社(Card Bus)の製品はIEEE802.11e が制定される以前のものであったため，QoS 制御の処理自体が存在しないためにQoS偽造攻撃が成功しなかったと考えられる．また，B社(Card Bus)の製品は1回のchopchop 攻撃(または reverse chopchop 攻撃)で2回のMIC エラーが送信されたためにMIC 鍵が更新されて攻撃が失敗している．これはIEEE802.11eに準拠していない（プロトコル違反の）実装と言える．

上記のような例外を除いた製品ではQoS攻撃を防げるものは確認できていない．したがって，現状では市販されている無線LANクライアントの多くは，たとえ利用者がIEEE802.11e を利用しないことを選択したとしても，WPA-TKIPへの改ざん攻撃を受ける可能性が高いと考えられる．QoS 偽造攻撃への対策としては本質的に chopchop 攻撃およびreverse chopchop 攻撃を実行できないWPA-AESやWPA2-AESを利用することが挙げられる．

（２）攻撃実行時間の短縮

reverse chopchop攻撃を用いた情報収集攻撃により，MIC 鍵の復元に要する時間を短縮することを考える．まず初めにARPパケットを対象にし，情報収集攻撃を実行する．各ARPパケットに対して 1～2 バイトの復元をすることになるため，1 分程度で IP アドレスとMAC アドレスの関係を得ることができる．この攻撃を繰り返すことで攻撃者は無線ネットワークのARPテーブルを作ることができる．ARP テーブルを作る間にMIC 鍵が更新されても，その影響で IP アドレスと MAC アドレスの関係を変更されるわけではないため，得られたARPテーブルの情報は有用なデータとなる．次にMIC鍵を得るためにARPパケットに対して reverse chopchop 攻撃により平文を全て復元する．データ部分はARPテーブルを参照することで既知となる．MIC の 8 バイトは未知バイトとなるため reverse chopchop攻撃を8回実行する．チェックサムはデータとMICから計算して求めることができるため推測しなくても良い．したがって，reverse chopchop攻撃を8回実行するだけで良いため，最小7分程度でMIC鍵を復元することができる．この攻撃を防ぐことを考える．情報収集攻撃とMIC鍵の復元の間にMIC鍵が更新されたとしても攻撃に影響は無いことから，MIC鍵を復元されないためにはMIC鍵を 7 分に 1 度は更新する必要がある．

MIC 鍵が得られた際の ARP パケットの改ざんは更に高速化が可能である．作成した ARPテーブルからデータ部分は既知になり，MIC

は MIC 鍵と IEEE802.11 ヘッダとデータから計算可能，チェックサムもデータと MIC から計算可能であるため reverse chopchop 攻撃を利用する必要が無い．したがって，ARP パケットを作成するのと大差ない程度の時間で改ざんパケットを作ることが可能となる．

最後に DHCP-DNS 攻撃について攻撃実行時間を短縮する．この場合も，事前に情報収集攻撃を実施し，ネットワークに関する予備情報を得て利用することで短縮できる．DHCP-DNS 攻撃は DHCP ACK パケットを改ざんすることで DHCP によって設定される DNS サーバの IP アドレスを変更する攻撃である．攻撃シナリオの中で改ざんした DHCP ACK パケットを受理させるためには改ざん ARP パケットを 4 つ受理させなければならない．これら 5 つのパケットの改ざんは従来の方法では 40 分程度要していたが，情報収集攻撃で得られた情報を活用することで 18 分程度まで短縮できることが分かった．MIC 鍵の更新間隔は初期設定で 30 分に設定されていることが多いことから，30 分以下で実行できる方法が発見されたことで DHCP-DNS 攻撃の脅威は増大したと言える．なお，DHCP-DNS 攻撃自体が一部の OS(現在知られているのは Mac OS X 10.5)における特定の動作を利用しているため，全ての条件で有効では無いことに注意が必要である．

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 4 件）

[1] Yoshuke Todo, Toshihiro Ohigashi, Masakatu Morii, “Effective Falsification Attack on WPA-TKIP by Modifying Any Packet to QoS Packet,” Proceedings of the fifth Joint Workshop on Information Security (JWIS2010), 査読有, 巻無し, 2010, pp.118-132.

[2] Yuki Ozawa, Yoshuke Todo, Toshihiro Ohigashi, Masakatu Morii, “Practical DHCP DNS Attack on WPA-TKIP -- Breaking WPA-TKIP in realistic environment --,” 第 9 回科学技術フォーラム(FIT2010)査読付き論文, 査読有, 第 4 分冊, 2010, pp.7-12.

[3] Yoshuke Todo, Yuki Ozawa, Toshihiro Ohigashi, Masakatu Morii, “Attack against WPA-TKIP using Vulnerability of QoS Packet Processing -- WPA-TKIP is not safe in realistic environment --,” 第 9 回科学技術フォーラム(FIT2010)査読付き論文, 査読有, 第 4 分冊, 2010, pp.13-18.

[4] Toshihiro Ohigashi, Masakatu Morii, “A Practical Message Falsification Attack on WPA,” Proceedings of the fourth Joint Workshop on Information Security (JWIS2009), 査読有, 巻無し, 2009, CD-ROM.

〔学会発表〕（計 6 件）

[1] 小澤 勇騎, 藤堂 洋介, 大東 俊博, 森井 昌克, “WPA-TKIP におけるメッセージ改ざん攻撃による現実的な被害に関する考察,” 電子情報通信学会 情報セキュリティ研究会, 2010 年 3 月 4 日～5 日, 長野県長野市.

[2] 藤堂 洋介, 小澤 勇騎, 大東 俊博, 森井 昌克, “WPA-TKIP の実装における QoS パケット処理の脆弱性を利用した偽造攻撃 ～大部分の WPA-TKIP の実装は偽造攻撃を防げない ～,” 電子情報通信学会 情報セキュリティ研究会, 2010 年 3 月 4 日～5 日, 長野県長野市.

[3] 藤堂 洋介, 小澤 勇騎, 大東 俊博, 森井 昌克, “WPA-TKIP におけるメッセージ改ざん攻撃に関する考察,” 2010 年暗号と情報セキュリティシンポジウム(SCIS2010), 2010 年 1 月 19 日～22 日, 香川県高松市.

[4] 大東 俊博, 小澤 勇騎, 森井 昌克, “WPA-TKIP におけるメッセージ改ざん攻撃の高速化,” 電子情報通信学会 情報セキュリティ研究会, 2009 年 11 月 12 日～13 日, 岐阜県岐阜市.

[5] 小澤 勇騎, 大東 俊博, 森井 昌克, “無線 LAN 暗号化方式 WPA-TKIP の脆弱性とそれを用いた攻撃方法の提案,” コンピュータセキュリティシンポジウム 2009(CSS2009), 2009 年 10 月 28 日～30 日, 富山県富山市.

[6] 小澤 勇騎, 大東 俊博, 森井 昌克, “無線 LAN 暗号化 WPA への改ざん攻撃の実装と評価,” 電子情報通信学会 ライフインテリジェンスとオフィス情報システム研究会, 2009 年 9 月 24 日～25 日, 広島県東広島市.

６．研究組織

(1)研究代表者

大東 俊博 (OHIGASHI TOSHIHIRO)
広島大学・情報メディア教育研究センター・助教
研究者番号：８０５０８１２７

(2)研究分担者

（ ）
研究者番号：

(3)連携研究者

（ ）
研究者番号：