7-2　SSL の脆弱性を検証するシステム XPIA（エクスピア）

黒川貴司　野島　良　盛合志帆

Secure Socket Layer（以下「SSL」）/Transport Layer Security（以下「TLS」）は、電子政府システムから、インターネットバンキング、オンラインショッピングなど国民生活の身近な所に至るまで、広く普及している暗号プロトコルである。その一方で、オンラインサービスの発展と普及に歩調を合わせるかのように、SSL/TLS に対する攻撃手法が日々進化し、巧妙化している。本稿では、第 3 中長期目標期間（2011 年度から 2015 年度まで）において、セキュリティ基盤研究室が行った SSL/TLS に対する攻撃手法に関する研究／開発の概略を紹介する。

1　まえがき

インターネット上では電子商取引、オンラインショッピングなどのネットワークを介したサービスが広く普及している。このようなサービスを安全に利用するための基盤技術として SSL/TLS が利用されることが多い。

利用者が接続先を認証する際には、公開鍵基盤（Public Key Infrastructure: PKI）技術を用いて、公開鍵証明書に記載されている情報の正当性が検証される。ヘニンガー（N. Heninger）らとレンストラ（A.K. Lenstra）らは、それぞれ独立に、RSA の鍵生成時に利用する乱数の偏り等が原因で、同じ秘密鍵（素数）を含む公開鍵が多数生成され、サーバー証明書に組み込まれて利用されていることを 2012 年に報告した [1][2]。RSA の安全性を支える大きな数の素因数分解は難しい問題と考えられているが、2 つの大きな数の最大公約数を求めることは容易であり、2 つの RSA 公開鍵に同じ秘密鍵（素数）が含まれていた場合、最大公約数を求めることで簡単にその秘密鍵が暴かれてしまう（図 1）。秘密鍵が暴かれることにより、サーバー証明書の偽造

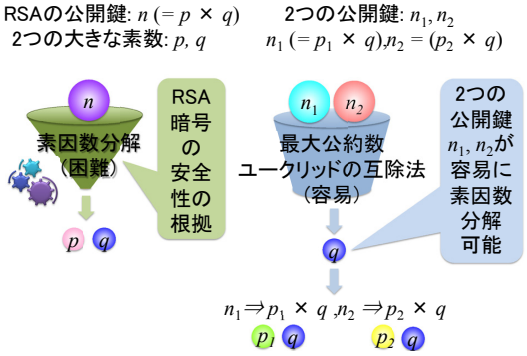

図 1　RSA 公開鍵における秘密鍵の共有

などが可能となる。このような脆弱性を有するサーバーの数の報告例はあったが、具体的にどこで利用されているのか等の報告例は少なかったため、我々は JP ドメインにおいてそのような公開鍵がどの程度存在するのかの調査を行った。これについては **2** で概説する。

SSL/TLS を使った暗号化通信の際には、RSA、DH、AES、RC4、CBC モード、HMAC など多数の暗号プリミティブが組み合わされる。近年報告された脆弱性の中で代表的なものに、SSL3.0 及び TLS1.0 における CBC モードの脆弱性とブラウザのバグを利用した BEAST 攻撃や POODLE 攻撃、RC4 のキーストリームにおける偏りを利用して統計的に平文を推定し、暗号化されたクッキーに含まれるパスワードを盗み出す攻撃手法が報告されている。

暗号化通信においてブロック暗号を選択した場合、SSL3.0 及び TLS1.0 においては CBC モードが用いられ、仕様上、初期化ベクトル IV は前回暗号化した暗号文の最終ブロックから選ばれる（図 2）。IV が予測可能であるため識別不可能性は満たさないが、識別不可能性を満たさないからといって直ちに攻撃者による平文の復元まで意味するわけではない。しかしながら、BEAST 攻撃における手法を使うと、Web ブラウザ及び周辺ソフトウェアに同一生成元ポリシー（Same Origin Policy: SOP）に関わるセキュリティバグがある場合、現実的な計算量で平文を復元できることが、ドゥアン（T. Duong）とリッツォ（J. Rizzo）により実証された [3]。その後、SOP に関わる未知のバグが他にも多く存在する可能性があることから、各ブラウザベンダから CBC モードのセキュリティパッチが公開された。相互接続性の観点から採用されたこのセキュリティパッチは、1 /n-1 レコード分割パッチ（1 /n-1 Record Splitting Patch）と呼ばれている。我々は、こ

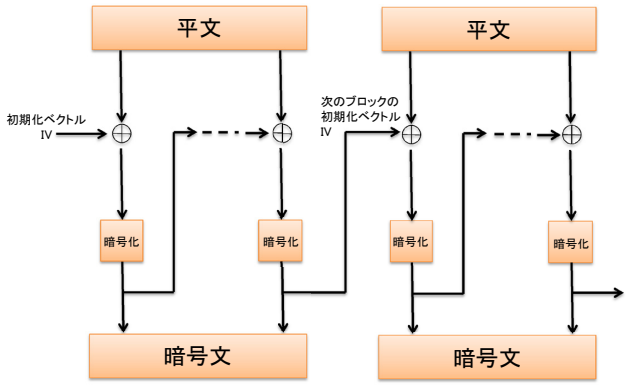

図 2　SSL3/0 及び TLS1.0 における CBC モード

の分割パッチが安全性上妥当なものである、すなわち、IND-CPA 安全性を満たすことを証明した。これについては **3** で概説する。

2　RSA 公開鍵の脆弱性について

ここでは文献 [4] にて報告した内容の概略を述べる。

2.1　公開鍵証明書の収集と RSA 公開鍵の抽出

我々は、公開鍵証明書を IPv4 のアドレス空間全体からクローリングして収集する方法は採用せずに、SSL Observatory[5] によって収集されていた公開鍵証明書を用いた。公開鍵証明書は X.509 に基づいて記述されており、RSA の場合、公開鍵証明書における subjectPublicKey フィールド内の modulus フィールドに DER エンコーディングにより変換されて格納されている。

2.2　RSA 公開鍵の解析

大量の公開鍵証明書の中から脆弱な RSA 公開鍵を抽出する場合、単純に RSA 公開鍵同士の最大公約数 GCD を計算する方法では、対象とする RSA 公開鍵の数を n としたとき、計算量は n^2 のオーダーのために非常に多くの時間を要するが、ペアごとに 2 分木状に計算していく手法を用いれば、計算量を $n \log n$ のオーダーに抑えることができる。本調査時においては SSL Observatory が収集した公開鍵証明書（2010 年）の中から、1,024 ビットの RSA 公開鍵を格納している公開鍵証明書を 2,742,833 通取り出して共通因子の有無の調査を行い、8,703 個の脆弱な RSA 公開鍵を検出できた。

2.3　可視化

通常は、公開鍵証明書内に格納されているフィールドから、脆弱な RSA 公開鍵を有しているユーザーに関する何らかの情報（国情報、ホスト名など）を明らかにできるが、脆弱な公開 RSA 鍵を検出した公開鍵証明書の subject フィールドの多くは国情報すら記されていないもの多かった。そのため、各地域インターネットレジストリ（AfriNIC、ARIN、APNIC、LACNIC、RIPE NCC）が公開している IP アドレスの割当てに関する情報を参照して国情報を判別した（図 3）。

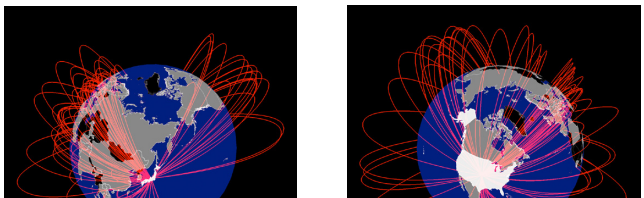

図 3　共通因子の共有状況（左側は日本側から、右側は米国側から見た様子）

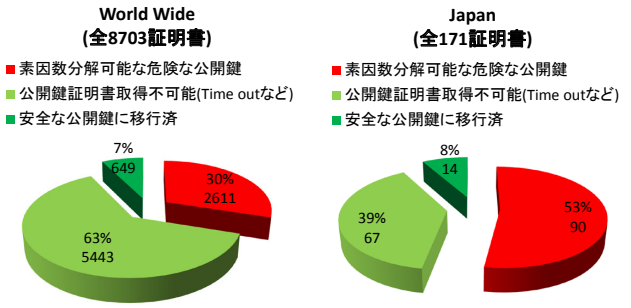

図 4　脆弱な公開鍵を持つ公開鍵証明書の 2013 年 10 月頃の状況

2.4　クローリングとログ情報の分析

脆弱な公開鍵証明書は更新されている可能性があるため、クローラを作成して最新の公開鍵証明書を入手し直した。本調査時においては、5,443 通からは公開鍵証明書を得ることができず、残りの 3,260 通のうち、素因数分解可能な RSA 公開鍵をいまだに利用していたホスト数は 2,611 台であった。また、JP ドメインで利用されている 171 通の公開鍵証明書の中で、素因数分解可能な RSA 公開鍵をいまだに利用していたホスト数は 90 台あった（図 4）。

次に、どういったホストが素因数分解可能な公開鍵を保持しているかを調査するため、2,611 台のホストに接続し、そのトップページを調べた。本調査時においては、2,611 台のホスト中 2,233 台のホストのトップページを入手することができた。詳しくは、文献 [4] を参照いただきたい。

2.5　JIPDEC への協力

上記で得た情報を NICT から JIPDEC（日本情報経済社会推進協会）へ技術移転を行った結果、2014 年 8 月に、認定認証業務の自己署名証明書に含まれる公

開鍵について検証を行い、脆弱性に起因する危険性がないことが確認された [6]。なお、ここで利用した公開鍵証明書は、SSL Observatory が収集していたものではなく、https://scans.io/ にて収集されたデータセットを用いた。

3 TLS1.0 におけるパッチ済み CBC モードの安全性証明について

ここでは文献 [7]–[9] にて報告した内容の概略を述べる。

3.1 TLS1.0 におけるパッチ

サイト [10] によると、現在、SSL/TLS の中で TLS1.0 が最も広くサポートされており、CBC モードが多くの暗号スイートで利用されている。TLS1.0 の CBC モードにおいては、メッセージ認証コードがパディングには適用されないため、もしパディングのエラーとメッセージ認証コードのエラーが区別できてしまう場合、パディングオラクル攻撃と呼ばれる攻撃が存在することが知られていた [11]。このため、空のフラグメントを付ける方法が提案されていたが、相互接続性に支障があるためにパッチとして正式に採用されることはなかった [12]。しかしながら、BEAST 攻撃の発見により対策が求められたため、相互接続性に問題がなかった、文献 [13] で提案された 1 /n-1 レコード分割パッチが採用されるようになった。1/n-1 レコード分割とは、平文の 1 バイト目とそれ以降の残りのバイトに平文を分割してから、それぞれ別々に暗号化する方法である（表 1）。1 /n-1 レコード分割パッチを適用した後の CBC モードによる暗号化及び TLS1.0 の元々のメッセージ認証コードを合わせて、SplTLS1.0 と定義することにする。

表 1　1/n-1 レコード分割の例

括弧内はバイト、C>S はクライアントからサーバーへの送信、S>C はサーバーからクライアントへの送信を意味する。AES の場合、パッチを適用すると最初のアプリケーションデータは 32 バイトの暗号文となる。したがって、この場合はクライアントにのみパッチが適用されている。

C>S	V3.1	(1)	ChangeCipherSpec
C>S	V3.1	(48)	Handshake
S>C	V3.1	(170)	Handshake
S>C	V3.1	(1)	ChangeCipherSpec
S>C	V3.1	(48)	Handshake
C>S	V3.1	(32)	application_data
C>S	V3.1	(80)	application_data
S>C	V3.1	(328)	application_data
S>C	V3.1	(608)	application_data

3.2 パッチ済み CBC モードの安全性

文献 [7] では下記の定理 1 を証明した。詳しくは、文献 [7] を参照のこと。鍵生成アルゴリズム $\mathcal{K}$ は確率的多項式時間アルゴリズムであり鍵 K を生成する。評価アルゴリズム $\mathcal{F}$ は決定性の多項式時間アルゴリズムであり、鍵 K と x を入力として受け取り、$\mathcal{F}(K, x)$ を出力するものとする。

定義 1. $\mathfrak{P} = (\mathcal{K}, \mathcal{F})$ が擬似ランダム関数（PRF）であるとは、任意の確率的多項式時間アルゴリズム $\mathcal{A}$ に対して、無作為に鍵 K を選んで $\mathcal{F}(K, \cdot)$ を実行したときに $\mathcal{A}$ が 1 を出力する確率と、$\mathcal{F}(K, \cdot)$ と定義域及び値域の両方が一致する関数の中から無作為に関数 $\mathcal{F}'$ を選んで $\mathcal{F}'$ を実行したときに $\mathcal{A}$ が 1 を出力する確率の差が negligible [*1] であるときをいう。また、$\mathcal{F}(K,\cdot)$ が置換であるとき、$\mathfrak{P}$ を擬似ランダム置換（PRP）という。

$\mathcal{E}$ を共通鍵暗号の暗号化アルゴリズムとするとき、関数 $\mathrm{LR}_{K,b}(M_0, M_1) = \mathcal{E}(K, M_b)$ を考える。ただし、$b \in \{0,1\}$ である。

定義 2. 共通鍵暗号 $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ が IND-CPA 安全であるとは、任意の確率的多項式時間アルゴリズム $\mathcal{A}$ に対して、鍵 K、$b \in \{0,1\}$ 及び $\mathrm{LR}_{K,b}$ を実行したときに $\mathcal{A}$ が出力する $b' \in \{0,1\}$ を無作為に選んだときに、$b = b'$ である確率と 1 /2 との差の絶対値が negligible であるときという。

定義 3. $\mathcal{MA} = (\mathcal{K}, \mathcal{T}, \mathcal{V})$ がメッセージ認証コードであるとは、鍵生成アルゴリズム $\mathcal{K}$ は確率的多項式時間アルゴリズムであり、鍵 K を出力し、タグ生成アルゴリズム $\mathcal{T}$ は決定性の多項式時間アルゴリズムであり、鍵 K と平文 M を入力として、タグ t を出力し、検証アルゴリズム $\mathcal{V}$ は決定性の多項式時間アルゴリズムであり、K、M、t を入力として、0 か 1 を出力するときをいう。また、$\mathcal{MA}$ が完全であるとは、$\mathcal{V}(K, M, t) = 1$ と $t = \mathcal{T}(K, M)$ が同値であるときをいう。なお、$\mathcal{T}(K, \cdot)$ が擬似ランダム関数であるとき、$\mathcal{MA}$ を擬似ランダム関数であるということにする。

定義 4. $\mathcal{MA} = (\mathcal{K}, \mathcal{T}, \mathcal{V})$ が IND-CPA 安全であるとは、任意の確率的多項式時間アルゴリズム $\mathcal{A}$ に対して、鍵 K、$b \in \{0,1\}$ 及び $\mathrm{LR}_{K,b}$ を実行したときに $\mathcal{A}$ が出力する $b' \in \{0,1\}$ を無作為に選んだときに、$b = b'$ であ

＊1　関数 ε が negligible であるとは、任意の $c > 0$ について、ある k があって、$\varepsilon(n) < 1/n^c$ $(n \geq k)$ が成り立つときをいう。

る確率と 1 /2 との差の絶対値が negligible であるときという。

定理 1.$\mathfrak{P}$ は擬似ランダム置換であり、$\mathcal{MA} = (\mathcal{K}, \mathcal{T}, \mathcal{V})$ は擬似ランダム関数で、完全あるならば、SplTLS1.0 は IND-CPA を満たす。

4　むすび

我々は、SSL で使用される RSA 公開鍵の脆弱性を検証するシステムを構築するプロジェクトを開始し、そのシステムを XPIA（X.509 certificate Public-key Investigation and Analysis system）と名付けたが、その後、TLS1.0 の 1 /n-1 レコード分割パッチの安全性証明を与える研究まで範囲が広がった。このため、SSL/TLS の安全性に関する研究全般に対して XPIA と呼ぶようになった。今後とも SSL/TLS に関する研究動向に注意を払い、国内における認定認証業務への貢献のように、研究成果が電子政府等に利用される暗号技術の安全性及び信頼性の確保に展開されることを願っている。

謝辞

この場を借りて、XPIA に関するプレスリリース及び技術移転等にご協力していただいたすべての方々に感謝いたします。

【参考文献】

1 N. Heninger, Z. Durumeric, E. Wustrow, and J.A. Halderman, “Mining Your Ps and Qs:Detection of Widespread Weak Keys in Network Devices,” USENIX Security 2012, 2012.
2 A.K. Lenstra, J.P. Hughes, M. Augier, J.W. Bos, T. Kleinjung, and C. Wachter, “Pub-lic Keys,” CRYPTO 2012, LNCS 7417, pp.626–642, 2012.
3 T. Duong and J. Rizzo. “Here Come The ⊕ Ninjas,” http://netifera.com/research/beast/beast_DRAFT_0621.pdf , May 2011.
4 黒川貴司 , 野島良 , 盛合志帆 , “Mining Your Ps and Qs” のその後 ,” CSS2013, 2013.
5 The SSL Observatory, Available from https://www.eff.org/observatory/ (2013-08-26)
6 独立行政法人 情報通信研究機構 , 一般財団法人 日本情報経済社会推進協会 ,“電子入札、電子申請や電子契約等を支える認定認証業務の安全性を検証 ,” 2014 年 12 月 17 日 , NICT プレスリリース , http://www.nict.go.jp/press/2014/12/17-1.html
7 黒川貴司 , 野島良 , 盛合志帆 , “TLS1.0 における CBC モードの安全性について ,” SCIS2014, 2014.
8 T. Kurokawa, R. Nojima, and S. Moriai, “Can We Securely Use CBC Mode in TLS1.0?,” ICT-EurAsia/CONFENIS 2015, pp.151–160, 2015.
9 T. Kurokawa, R. Nojima, and S. Moriai, “On the security of CBC Mode in SSL3.0 and TLS1.0,” Journal of Internet Services and Information Security, 6(1), 2–19, Feb. 2016.
10 SSL Pulse, “Survey of the SSL Implementation of the Most Popular Web Sites,” https://www.trustworthyinternet.org/ssl-pulse/
11 S. Vaudenay, “Security Flaws Induced by CBC Padding - Applications to SSL, IPSEC, WTLS ...,” EUROCRYPT 2002, pp.534–546, 2002.
12 Bodo Moeller, “Security of CBC Ciphersuites in SSL/TLS:Problems and Countermeasures,” http://www.openssl.org/~bodo/tls-cbc.txt
13 X. Su,“Bugzilla Bug 665814 Comment 59,” https://bugzilla.mozilla.org/show_bug.cgi?id=665814#c59 , July 2011.

黒川貴司　（くろかわ　たかし）
サイバーセキュリティ研究所
セキュリティ基盤研究室
技術員
暗号技術の安全性評価

野島　良　（のじま　りょう）
サイバーセキュリティ研究所
セキュリティ基盤研究室
主任研究員
博士 (工学)
暗号理論、暗号プロトコル、情報セキュリティ、プライバシー、セキュリティ

盛合志帆　（もりあい　しほ）
サイバーセキュリティ研究所
セキュリティ基盤研究室
室長
博士 (工学)
暗号技術、セキュリティ評価、プライバシ保護技術