4E-01

POODLE attack 公開後のSSL/TLSサーバのバージョン移行状況

須賀 祐治 *
株式会社インターネットイニシアティブ

あらまし SSLv3にてCBCモードを利用する際に起きるPadding Oracle Attacksの1種であるPOODLE attackが2014年10月に公開された．RC4も危殆化していると認識されていることからSSLv3で安全に利用できる方法は現在のところ皆無となった．主要なSSL/TLSサーバの設定状況について2014年4月にクロールした結果と比較し，特にバージョン情報に関して移行状況について報告する．

キーワード SSL/TLS, POODLE attack, 暗号世代交代, 移行工学

1 背景：潜在的なCBCモードの問題と攻撃

IETF等で標準化されたセキュアプロトコルには秘匿性を確保するためにデータ暗号化機能が備わっている．暗号化アルゴリズムのうちブロック暗号を利用する際には，ブロック長よりもはるかに長いデータを暗号化することが多いため，何度も逐次的に暗号化アルゴリズムで暗号処理を行う必要がある．1つ前のブロック暗号処理で得られたデータを次のデータ処理でどのように利用するかを定めた方式のことを暗号モードと呼び，いくつもの方式が提案されている．CBC（Cipher Block Chaining）モードはその1手法であり広く利用されている．

CBCモードにおいて平文パートP_iを暗号化するには，前のブロック暗号化処理で得られたC_{i-1}をXOR演算で足し合わせたデータを平文として入力して暗号化する，すなわち$C_i = ENC\,(P_i \oplus C_{i-1})$という暗号化処理を繰り返すことで，データ全体の暗号化を行う．復号時には$P_i = DEC\,(C_i) \oplus C_{i-1}$という復号処理を逐次的に繰り返すことで，平文を復元することができる．

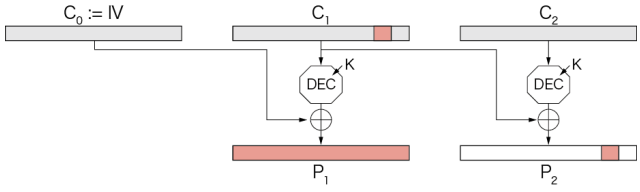

図1: CBCモードにおける暗号文改ざんの波及範囲

図1はCBC暗号モードにCBCモードを利用した復号時において，暗号文が改ざんされた場合の波及範囲を示しています．この図において暗号文C_1の一部を改ざんすることで平文P_1はブロック全体が変更されてしまうが，平文P_2は攻撃者の意図する箇所を自由に変換することができる．この特徴を用いた「トライ&エラー」を繰り返すことで暗号文から平文の情報を少しずつ不正に復元するPadding Oracle Attackと呼ばれる一連の攻撃があり，SSL/TLSだけでなくSSHやIPsecにおいても同様の攻撃が公開されてきた[1] [2]．いずれも仕様で定められた「データ形式の制約」に則っているかどうかを，サーバからのエラー情報を基に判定して暗号化データを復号する攻撃手法である．

一方でCBCモード単体としては致命的な攻撃手法は知られておらず．最新のCRYPTREC暗号リストにおいても推奨暗号として記載されるなど，安全に利用可能である．前述のようにパディング処理を通してCBCモードをセキュアプロトコルで利用する場合に多くの問題が多発している．そのため当該脆弱性が報告される度に，CBCモード以外の暗号モードの利用やRC4などのストリーム暗号の利用にシフトしてサーバ運用するという対策が行われてきた．

2 POODLE attackの登場とSSLの終焉背景

前章で示したCBCモードによる暗号化処理において，ブロック長でちょうど割り切れないデータを扱う場合にはパディング処理が必要となる．これは，平文の最後のパートがブロック長に満たない場合に何がしかのデータでブロック長になるように埋めてブロック暗号化処理が行えるようにする処理である．TLSではPKCS#5 padding方式が採用されており「パディングするバイト長」で残りのデータを埋めてブロック長で区切れるように平文データを追加する．一方で，SSLv3で採用されているパディング方式は，パディングする最終バイトをPKCS#5 padding方式と同様に「パディングするバイト長」とし，それ以外のパディングデータはランダムデータを埋めていく方式である．これら2つのパディング方式のちょっとした違い，すなわち「パディングデータに揺れがあり確定的でない」という点が後述するPOODLE attack [3]を成功させる要因となっている．

図2はこの特徴を用いたPadding Oracle Attackの原

* Version transition status about SSL/TLS servers after disclosure of POODLE attack Internet Initiative Japan Inc., Iidabashi Grand Bloom 2-10-2 Fujimi, Chiyoda-ku, Tokyo, 102-0071, Japansuga@iij.ad.jp

理を示している．平文の長さが分かっているという前提で P_n までのデータが暗号化されている場合，最後のブロック C_n を中間者が「攻撃対象」，つまり復号したいデータである C_i に差し替えるとき平文の長さが既知のため，パディングされたデータ長が格納されている P_n の最終バイトは既知となる．SSL/TLS サーバは手順どおりパディングチェックを行い，もし仕様で定められたパディング方式に則っていない場合にはエラーを返却する．このエラー返却機能（Padding Oracle）を使うと，サーバが暗号化データをアクセプトした場合，パディング部分には正しいデータが格納されていることを意味する．SSLv3 においては P_i の最終バイトと P_n の最終バイトが一致するときにアクセプトされるため，既知情報から P_i の最終バイトを（暗号化鍵を知らなくても）復元することができてしまう．

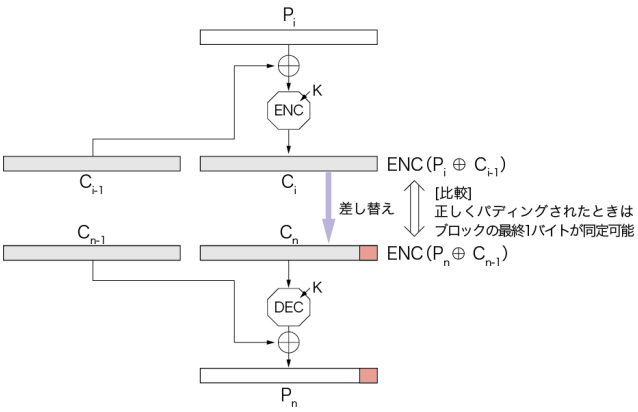

図 2: Padding Oracle Attack の原理

POODLE attack と同様に Padding Oracle Attack に分類されている BEAST 攻撃は，SSLv3 及び TLSv1.0 にて成功可能であり，TLSv1.1 にて仕様としてこの脆弱性を回避する設計がなされている．しかし TLSv1.1 以降への移行が進められていないのは，1/n-1 分割法と呼ばれる対策方法が有効であることが知られているためである．この手法は主要ブラウザ・サーバにおいて既に対策されているが，この対策を POODLE attack に適用することはできない．一方で RC4 における近年の一連の攻撃 [4][5] が存在することから，現時点では SSLv3 を安全に利用する方法が皆無となった．

今回の攻撃に対する対策として，1）SSLv3 を無効にする（クライアント・サーバのいずれか），2）$TLS\_FALLBACK\_SCSV$ の導入（クライアント・サーバ共に対策が必要）の 2 つが知られている．後者は潜在的なフォールバック攻撃を防ぐ根本的な対策であるがブラウザ側への対策が必須であり，組み込み機器，特にゲーム機器やフィーチャーフォンなどにおいては迅速な対策が見込めないことから，サーバサイドでは 1) の SSLv3 無効化の対策が進められている．

3 SSLv3 無効化と TLS への移行状況調査

SSL/TLS サーバのバージョン対応状況について，2014 年 4 月の Heartbleed bug 発覚時のサーバ設定調査結果 [6] との比較を行うため 2015 年 1 月 7 日にクローリングを行った．クロール環境，クロール対象は [6] に準じている．クロール対象は.jp ドメイン　5668 サイト，Alexa top sites の上位 20000 サイトのうち SSL-enable な 6835 サイトである．以下，結果を示す．数値は各バージョンの対応比率をパーセンテージをあらわしており，サーバサイドでの SSLv3 無効化が加速していることが分かった．

version	2014-04-27	2014-11-26	2015-01-07
SSL2.0	24.08	12.91	12.12
SSL3.0	99.91	62.32	57.44
TLS1.0	99.86	98.84	98.63
TLS1.1	15.61	27.27	28.94
TLS1.2	17.86	29.98	31.67

表 1: SSL/TLS バージョン対応状況 (.jp ドメイン)

version	2014-04-27	2014-11-26	2015-01-07
SSL2.0	5.23	1.73	1.62
SSL3.0	98.57	37.42	33.78
TLS1.0	99.48	99.69	99.75
TLS1.1	56.66	72.66	74.46
TLS1.2	60.66	76.42	78.37

表 2: SSL/TLS バージョン対応状況 (Alexa top sites)

参考文献

[1] M.R. Albrecht, K.G. Paterson, G.J. Watson, Plaintext Recovery Attacks Against SSH, 30th IEEE Symposium on Security and Privacy, 2009, http://www.isg.rhul.ac.uk/~kp/SandPfinal.pdf

[2] J.P. Degabriele and K.G. Paterson, On the (In) security of IPsec in MAC-then-Encrypt Configurations, Proceedings of the 17th ACM Conference on Computer and Communications Security, 2010, http://portal.acm.org/citation.cfm?id=1866363

[3] This POODLE Bites: Exploiting The SSL 3.0 Fallback, https://www.openssl.org/~bodo/ssl-poodle.pdf

[4] Takanori ISOBE, Toshihiro OHIGASHI, Yuhei WATANABE, and Masakatu MORII, Full Plaintext Recovery Attack on Broadcast RC4, Proc. the 20th International Workshop on Fast Software Encryption (FSE 2013).

[5] N.AlFardan, D.J.Bernstein, K.G.Paterson, B.Poettering, J.C.Schuldt, On the Security of RC4 in TLS, USENIX Security 2013., http://dl.acm.org/citation.cfm?id=2534793

[6] 須賀, SSL/TLS サーバにおける Forward Secrecy への対応状況について（＋速報版 Heartbleed Bug 発覚後の状況変化, 第 65 回 CSEC・第 25 回 IOT 合同研究発表会, 2014. 参考 : https://sect.iij.ad.jp/d/2014/04/157355.html