計算機援用工学前半レポート

ソフトウェア科学コース
09B22084 山久保孝亮

2024 年 12 月 19 日

1　選んだ理由

今回私が選んだ授業で出てくるワードは暗号化技術である．特に，POODLE による SSLv3 の脆弱性について詳しく調査した．私がこのテーマを選んだ理由としては，この脆弱性が原因でガラケーからスマホへの移行が進んだという講義内の話に関心を持ったためである．

2　調査の概要

2.1　技術の背景

SSLv3 は暗号化通信用のプロトコルであり，ドコモ，au，ソフトバンクなどのキャリアが提供する i モードブラウザ等でサポートされていた．[1] SSLv3 で利用される暗号は CBC 方式のブロック暗号を選択することができ，以下の図 1 のように一定のサイズのブロックごとに暗号化・復号を行う．[2] 図 1 では直前の暗号文と複合処理を行った暗号文を XOR している．

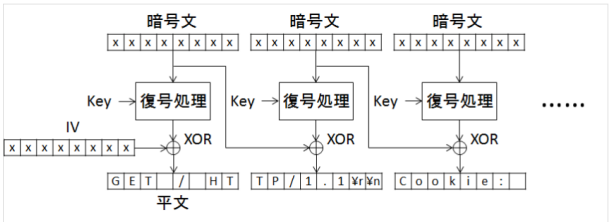

図 1: ブロック暗号の復号処理

このとき，一定サイズごとに復号を行うため，平文の最後がブロック長に比べて中途半端な長さになることが発生してしまう．その場合はダミーの文字を入れて調整を行っており，この文字を Padding という．また，一番最後のバイトは Padding 長として規定されており，例えば平文がブロックサイズちょうどであっても，Padding 長を格納するためにダミー文字と Padding 長のみのブロックが追加される．

2.2　手法

POODLE では 2.1 で述べた Padding 長を利用して暗号文から平文を解読する．
まず解読したい暗号文のブロックをコピーし，Padding 長を格納しているブロックと置き換えてサーバに送信する．これにより，基本的には Padding 長が変わるためサーバからエラーが返されるが，Padding 長は 1byte で表されるため $\frac{1}{2^8} = \frac{1}{256}$ の確率で一致してしまう．これが偶然一致した場合サーバからはエラーが

返されないので攻撃者は Padding 長が一致したことを知ることができる．さらに，図 1 のように CBC 方式のブロック処理では復号処理を行った暗号文と直前の暗号文を XOR するのみであるため，直前の暗号文を攻撃者が意図した内容に変更することでエラーが返されない場合の Padding 長を求めることができる．[3] その後，以下の図 2 のようにすることでコピーした暗号文の復号結果の最下位バイトを知ることができる．[2]

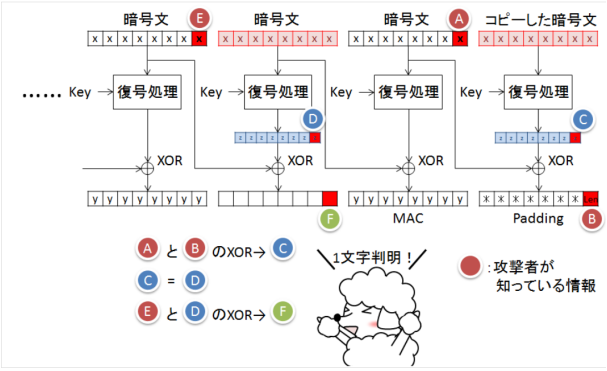

図 2: ブロック暗号の復号処理

右下の B の赤い部分は上で求めた Padding 長であり，A は攻撃者が変更した暗号文である．右二列はコピーした暗号文に対して復号処理が行われ C が生まれ，これと A を XOR することで B になることを表している．左から二番目は解読したい暗号文が本来あった位置を表し，これに対し復号処理が行われ D が生まれている．このとき，C と D はどちらも同じ暗号文に対して復号処理を行った結果でありその値は同じになるはずである．また，E の暗号文の最下位バイトを攻撃者は確認できるため解読したい暗号文の最下位バイトをＸＯＲすることで求められる．

2.3　結果

HTTP のプロトコルを使用すれば求めたい平文の byte の位置を変更することができるため，2.2 の処理を繰り返し行うと暗号文を解読することができる．

3　自分の見解

今回私が POODLE の脆弱性について詳細に調査して，一見解読不可能に見えるような仕組みのセキュリティでも解読する方法が存在するということについてとても驚いた．そして，現在普及しているプロトコルにおいても今後脆弱性が発見される可能性があるということを再認識させられた．ただ，脆弱性があるという事のみを知るのではなく，どのような脆弱性があるのか，何が原因だったのかを把握することは情報セキュリティの分野だけでなく全ての分野において持つべき姿勢であると考えた．常に理解する姿勢を崩さないことは来年以降の研究に役立つと思って継続していきたいと思う．

参考文献

[1] https://qiita.com/harukasan/items/dee779c0a3f624758230　12/16 アクセス

[2] https://engineering.dena.com/blog/2014/10/poodle/　12/16 アクセス

[3] https://partender810.hatenablog.com/entry/2021/06/08/225105　12/18 アクセス