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 16 日

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．

1　選んだ理由

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授業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．

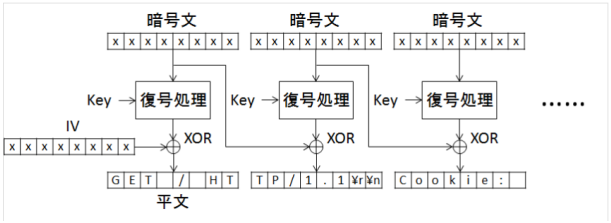

図 1: ブロック暗号の復号処理

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いた．この調整のために平文の最後に追加される文字を 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ていた．そしてこの Padding 長を使って復号の際に何文字 Padding を無視するかを判断していた．

2.2　手法

POODLE では 2.1 で例として挙げた Padding のみで構成されるブロックを使用してほかのブロックの平文の推測を行う．具体的には，

2.3　結果

3　自分の見解

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