Университет ИТМО, факультет программной инженерии и компьютерной техники
Двухнедельная отчётная работа по «Информатике»: аннотация к статье
Дата лекции: __ 9 октября____ Дата сдачи: ____11 января____

Выполнил(а) _____Лагус М.С._____, № группы _3114__, оценка _____
Фамилия И.О. студента не заполня

Название статьи/главы книги/видеолекции

Padding oracle attack, или почему криптография пугает

ФИО автора статьи (или e-mail)	**Дата публикации (не старше 2018 года)**	**Размер статьи (от 400 слов)**
Nostr	"_10_" 01_2019 г.	____714_

Прямая полная ссылка на источник и сокращённая ссылка (bit.ly, goo.gl, tr.im и т.п.)
https://habr.com/ru/post/247527/
https://bit.ly/3Eakw8q

Теги, ключевые слова или словосочетания
Криптография, блочное шифрование, криптоанализ, информационная безопасность

Перечень фактов, упомянутых в статье

1. На методы шифрования информации закреплённые в международных стандартах существуют взламывающие их атаки
2. Padding oracle attack - известная атака на криптографические системы с блочным шифрованием и сервером, который сообщает тебе, корректен ли поданный на вход шифротекст
3. Даже имея криптостойкий алгоритм шифрования, всё равно можно создать уязвимую для взлома систему, не подумав об соответствующем окружении

Позитивные следствия и/или достоинства описанной в статье технологии (минимум три пункта)

1. Данная атака является наглядным примером почему не стоит реализовывать свои собственные криптографические алгоритмы без должного опыта и знаний
2. Используя немного другую логику работы back-end части сервиса, данной уязвимости можно было бы избежать
3. Для реализации алгоритма атаки, необходимо много запросов на один и тот же сервер, следовательно,отслеживая подозрительный траффик можно защитить своё приложение

Негативные следствия и/или недостатки описанной в статье технологии (минимум три пункта)

1. Порой достаточно одного канала дополнительной информации о сервисе для его взлома
2. Попытки внедрить свою собственную модель защиты данных или новый криптографический алгоритм чаще всего делают вашу систему наоборот гораздо более уязвимой
3. Криптография сложна и обширна, на каждый криптографический алгоритм существует какая-то криптографическая атака, взламывающая его при некоторых обстоятельствах

Ваши замечания, пожелания преподавателю *или* анекдот о программистах[1]
Это наверное самая известная криптографическая атака на данный момент, многие сервисы осведомлены о её существовании и, как следствие, защищены

[1] Наличие этой графы не влияет на оценку