DF&C Lab.
Digital Forensic & Cryptanalysis
KOOKMIN UNIVERSITY

2023 2학기 보안프로토콜

팀 프로젝트

국민대학교 금융정보보안학과, DF&C 연구실
https://dfnc.kookmin.ac.kr

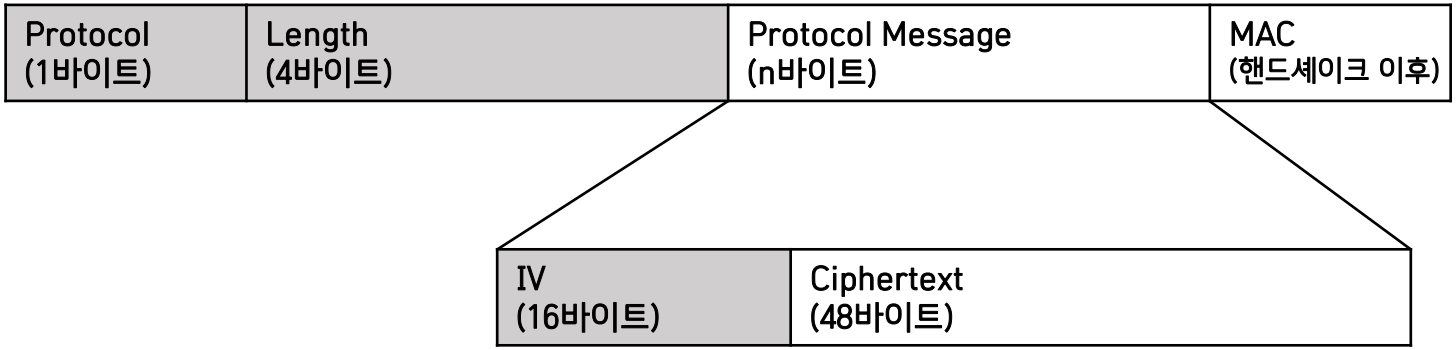
조교 : 김기윤 (gi0412@kookmin.ac.kr)
오픈톡 : https://open.kakao.com/o/gnMXxOHf

02

Padding Oracle Attack

Padding Oracle Attack

- MINI-TLS 활용
  - 핸드셰이크 이후 Protocol - Data Decryption Mode 사용



  - IV와 Ciphertext는 ecampus를 통해 배포 예정

Padding Oracle Attack

- 클라이언트가 서버에게 전송하는 메시지
  - Msg : IV || Ciphertext
    - 예시

      79 16 66 64 F1 FB DF CE B7 ED E7 36 BD 11 E3 AC

      74 2C 69 5D 69 AA 0A 3E 50 F0 DE 94 AE 3B FB E7

      D2 E0 28 BD 71 47 3C 61 94 68 4E D0 E9 CC E2 4A

      44 84 1F E8 83 E0 09 34 58 3D D7 C4 7A E7 7C 42

- 반환 받는 메시지
  - OK+ 또는 Wrong Padding
  - 이 외의 정보는 반환되지 않음
  - 단, 패킷이 이상하거나 프로토콜이 이상한 경우 Error 메시지 전송

- 서버 측 로깅 정보

```
[         1]=====================================================
IV :
 79 16 66 64 F1 FB DF CE B7 ED E7 36 BD 11 E3 AC
Ciphertext :
 74 2C 69 5D 69 AA 0A 3E 50 F0 DE 94 AE 3B FB E7
 D2 E0 28 BD 71 47 3C 61 94 68 4E D0 E9 CC E2 4A
 44 84 1F E8 83 E0 09 34 58 3D D7 C4 7A E7 7C 42
Decrypted Message :
 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30
 31 31 31 31 31 31 31 31 31 31 31 31 31 31 31 31
 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10
Result (SendMsg) : b'OK+'
============================================================
[         2]=====================================================
IV :
 79 16 66 64 F1 FB DF CE B7 ED E7 36 BD 11 E3 AC
Ciphertext :
 74 2C 69 5D 69 AA 0A 3E 50 F0 DE 94 AE 3B FB E7
 D2 E0 28 BD 71 47 3C 61 94 68 4E D0 E9 CC E2 5B
 44 84 1F E8 83 E0 09 34 58 3D D7 C4 7A E7 7C 42
Decrypted Message :
 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30
 22 E1 59 D5 1E A8 94 9C 6E 8E 1C 65 C2 0A 74 C8
 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 01
Result (SendMsg) : b'OK+'
============================================================
[         3]=====================================================
IV :
 79 16 66 64 F1 FB DF CE B7 ED E7 36 BD 11 E3 AC
Ciphertext :
 74 2C 69 5D 69 AA 0A 3E 50 F0 DE 94 AE 3B FB E7
 D2 E0 28 BD 71 47 3C 61 94 68 4E D0 E9 CC E2 58
 44 84 1F E8 83 E0 09 34 58 3D D7 C4 7A E7 7C 42
Decrypted Message :
 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30
 0D C9 D1 BF 4E 06 9B 25 CB 11 8D 2E C4 DA DD 0D
 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 02
Result (SendMsg) : b'Wrong padding'
============================================================
```

Q&A