

Crypto Lab 12월 21일 세미나 발표

최승주

목차

- 연구 주제 선정
- 정보 보호 학회 논문
- Cain & Abel

연구 주제 선정

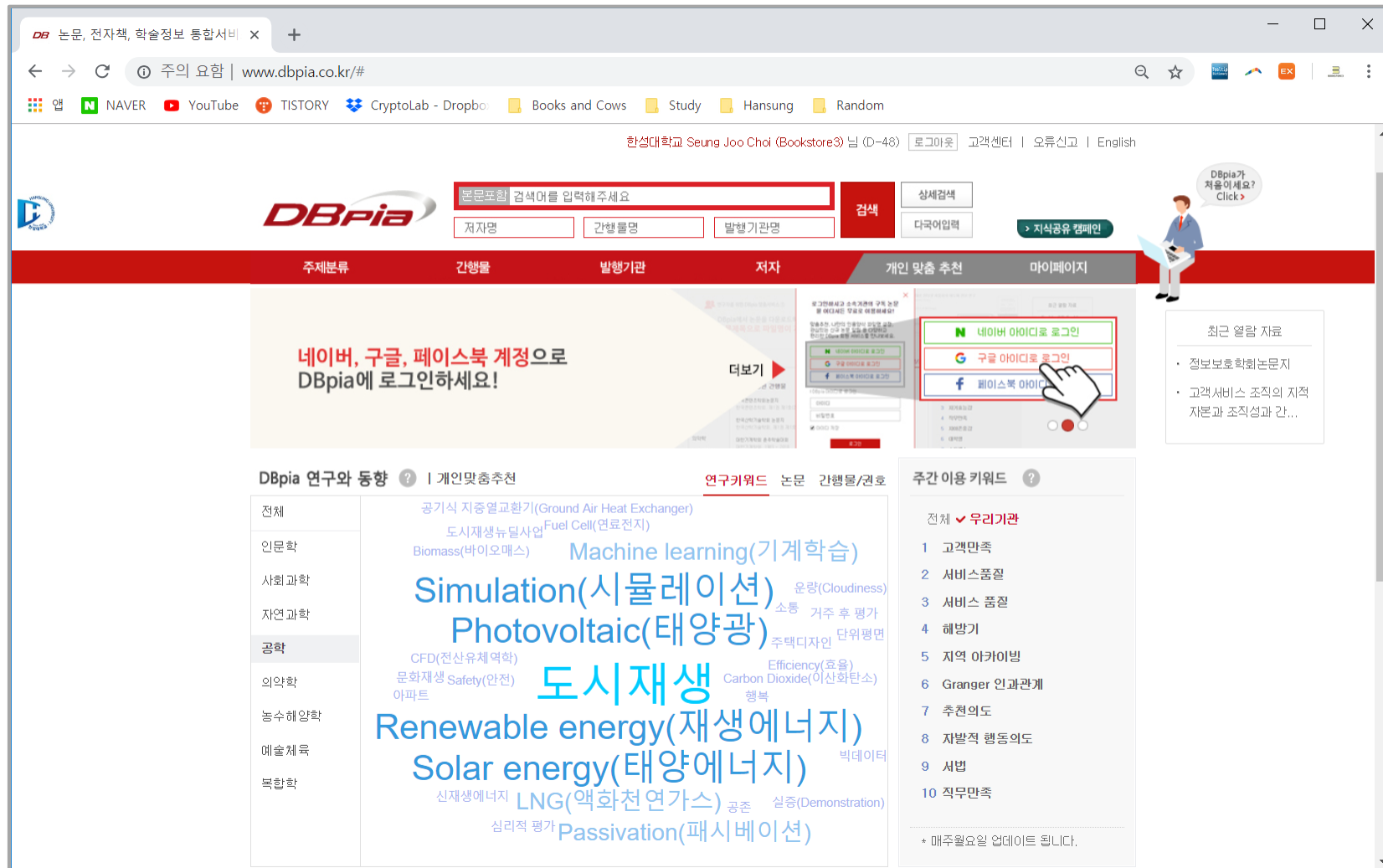
주제 선정

석사 과정 구체적 연구 주제의 방향을 잡기 위함

- 교수님과 상담
- 정보 보호 학회 논문 – Dbpia
- 간단한 해킹 맛보기 – Cain & Abel

정보 보호 학회 논문

정보 보호 학회 DBpia



정보 보호 학회 논문

- 블록체인 기반 IoT 디바이스 인증 스킴
- 공공기관 프린터 관리 시스템의 취약점 분석
- 개인정보 노출에 대한 인터넷 사용자의 태도에 관한 연구

블록체인 기반 IoT 디바이스 인증 스킴

블록체인 기반 IoT 디바이스 인증 스킴

- 블록체인 기반 IoT 디바이스 인증 스킴 제안
- IoT 디바이스에 단순 해시 연산만을 요구
저성능인 IoT 디바이스에서도 동작 가능

블록체인 기반 IoT 디바이스 인증 스킴

- 고성능 OS 칩셋을 장착한 경우 암호 프로토콜 지원
- 단순 기능만 존재하는 저성능 디바이스

암호화 프로토콜 지원 X

인증서 지원 X

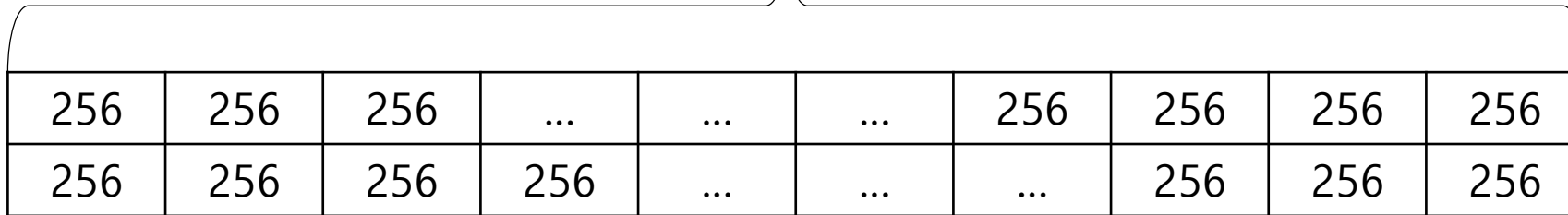
블록체인 기반 IoT 디바이스 인증 스킴

- 램포트 서명 방식
- 블록체인 방식
- 기존 IoT 인증 프로토콜

블록체인 기반 IoT 디바이스 인증 스킴

- 램포트 키 생성

난수 256개



256	256	256	256	256	256	256
256	256	256	256	256	256	256

단위: bit

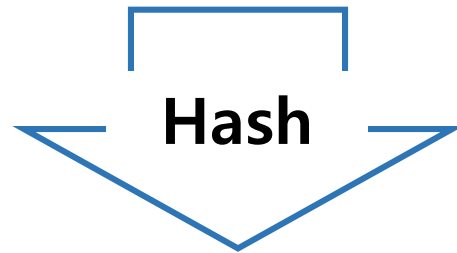
$$256 * 256 * 2 = 16kb$$

블록체인 기반 IoT 디바이스 인증 스킴

- 램포트 공개 키 생성

Private Key

256	256	256	256	256	256	256
256	256	256	256	256	256	256



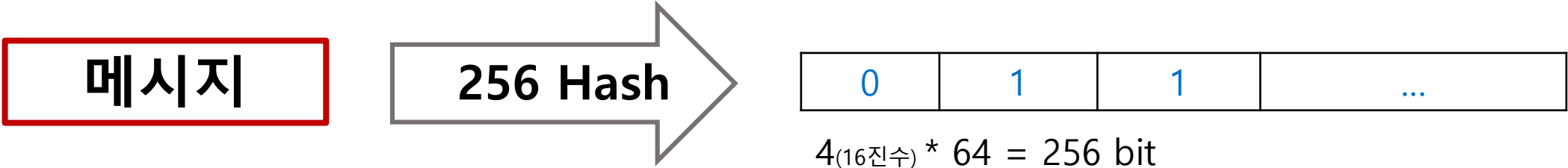
Public Key

256	256	256	256	256	256	256
256	256	256	256	256	256	256

단위: bit

블록체인 기반 IoT 디바이스 인증 스킴

- 램포트 메시지 서명

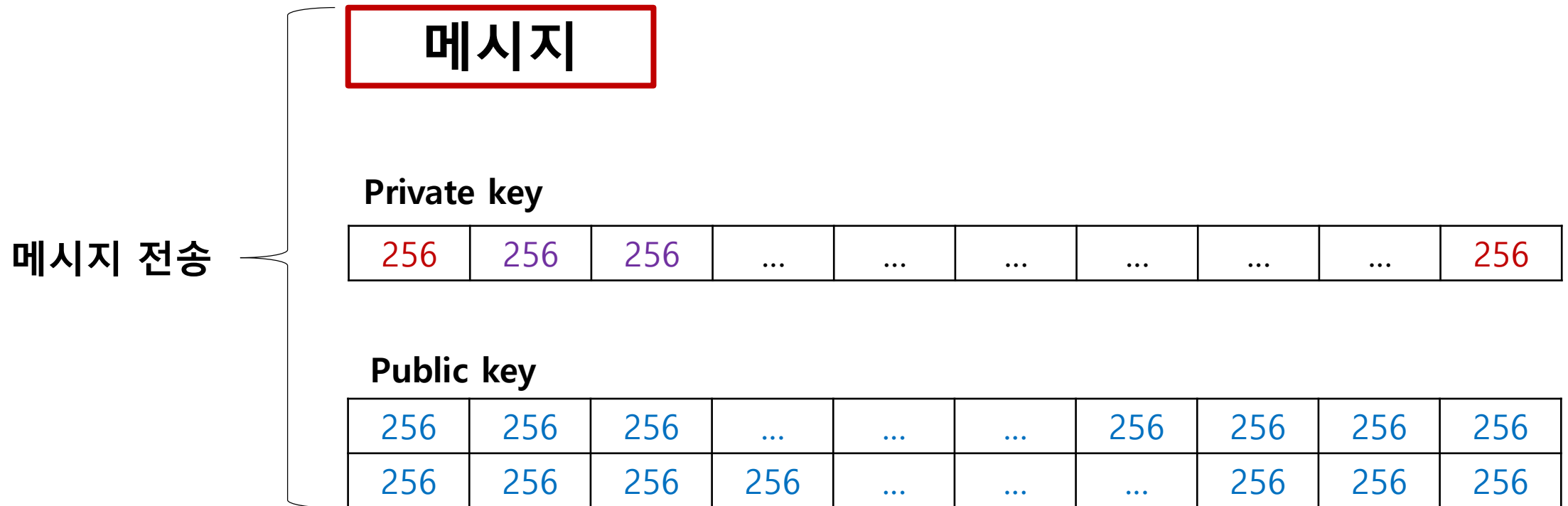


Private Key
Index

0	1	2	3			256
256	256	256	256	256	256	256
256	256	256	256	256	256	256
256	256	256	256

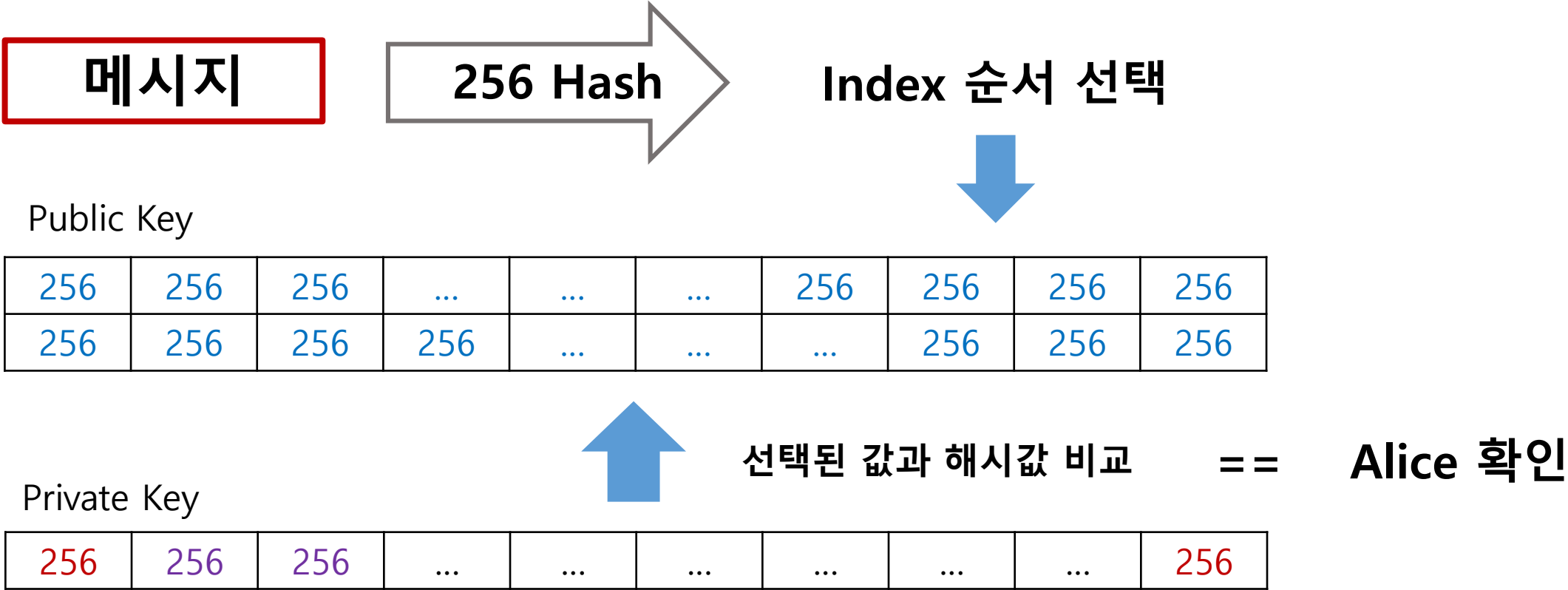
블록체인 기반 IoT 디바이스 인증 스킴

- 램포트 메시지 전송



블록체인 기반 IoT 디바이스 인증 스킴

- 램포트 메시지 확인



블록체인 기반 IoT 디바이스 인증 스킴

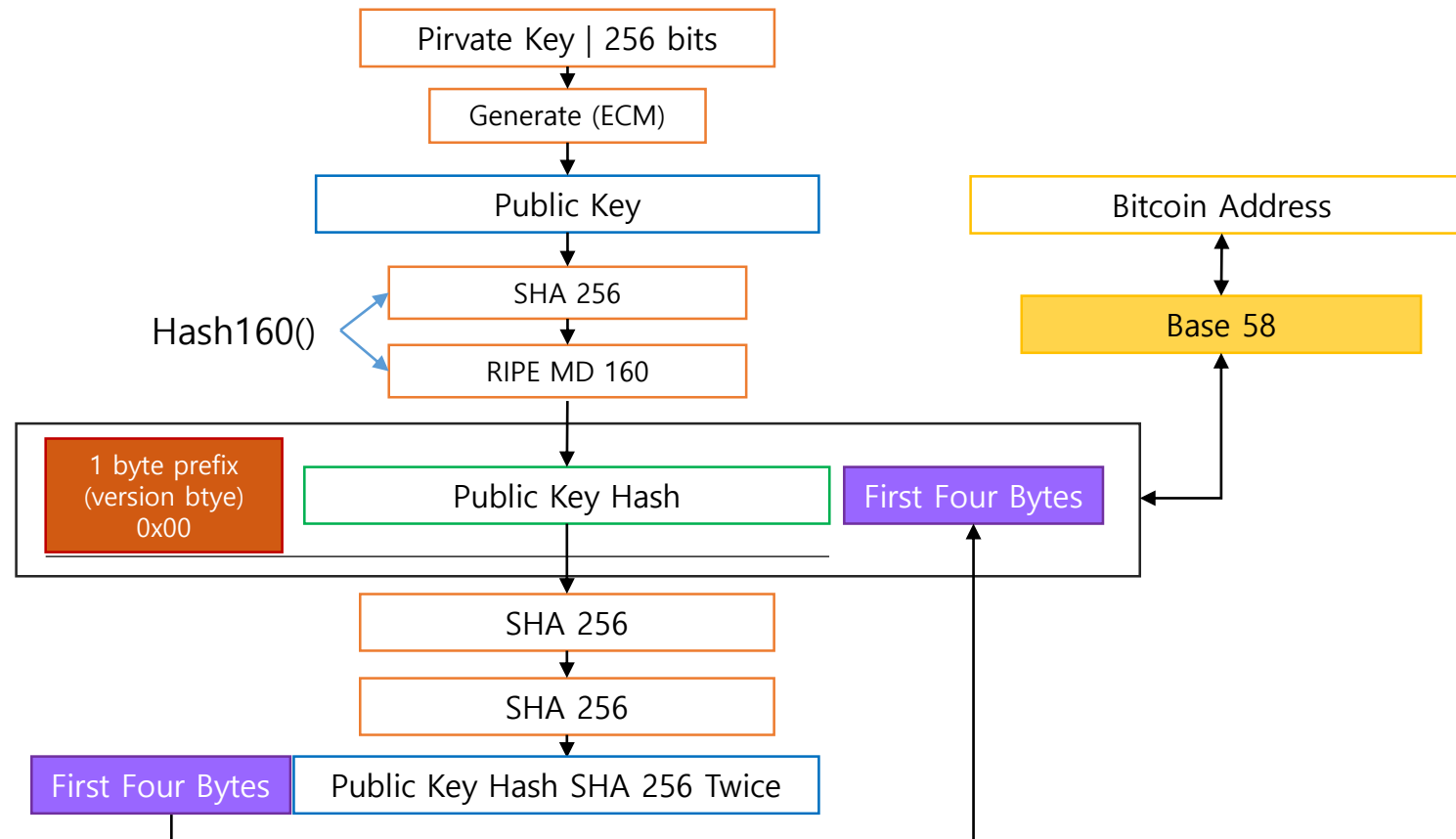
- 램포트 방식

개인키의 절반이 공개됨

한번 사용하면 안전을 위해 삭제 후 새로 생성

블록체인 기반 IoT 디바이스 인증 스킴

- 블록체인 방식



블록체인 기반 IoT 디바이스 인증 스킴

- 블록체인 방식

<Signature> <PublicKey>

OP_DUP OP_HASH160 <PublicKey160> OP_EQUALVERIFY OP_CHECKSIG

블록체인 기반 IoT 디바이스 인증 스킴

- 기존 IoT 프로토콜
 1. ID/Password 기반 인증
 2. MAC 주소 기반 인증
 3. 암호 프로토콜 기반 인증
 4. 인증서 기반 인증
 5. IBE를 이용한 인증

블록체인 기반 IoT 디바이스 인증 스킴

- 기존 IoT 프로토콜

1. ID/Password 기반 인증

- 서버 부하, 기기 추가시 사람 개입

2. MAC 주소 기반 인증

- 새로운 MAC Address 양식 규정 필요, 위장 가능

3. 암호 프로토콜 기반 인증

- 암호 기술에 의존: 취약점 발견시 문제

4. 인증서 기반 인증

- 기기 인증 알고리즘: 높은 처리량 필요

5. IBE를 이용한 인증

- ID 위장 공격에 취약

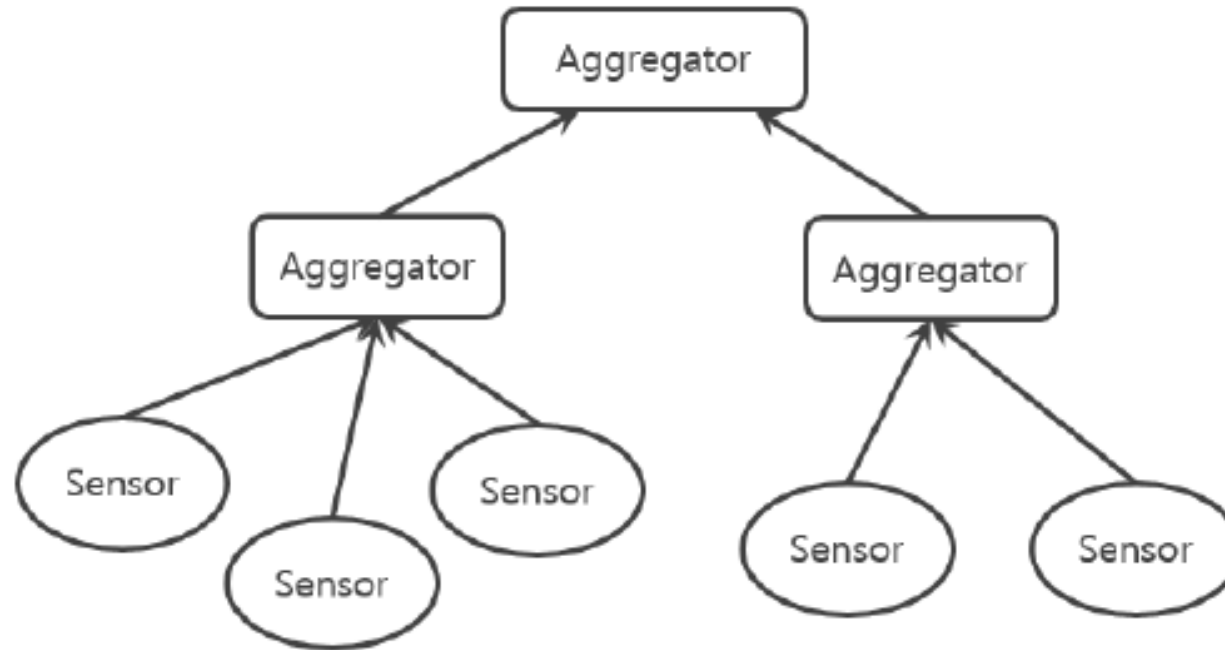
블록체인 기반 IoT 디바이스 인증 스킴

- 제안 스킴 활용 기술

램포트 해시 체인 및 블록 체인 기술 활용

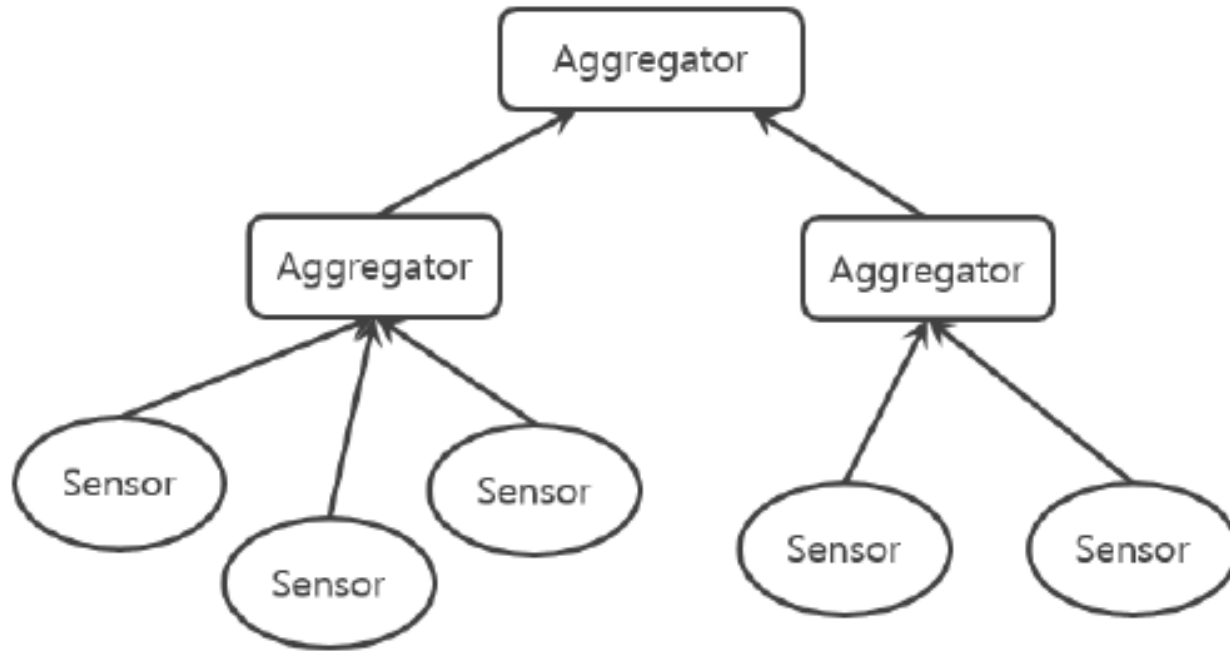
블록체인 기반 IoT 디바이스 인증 스킴

- 제안 스킴



블록체인 기반 IoT 디바이스 인증 스킴

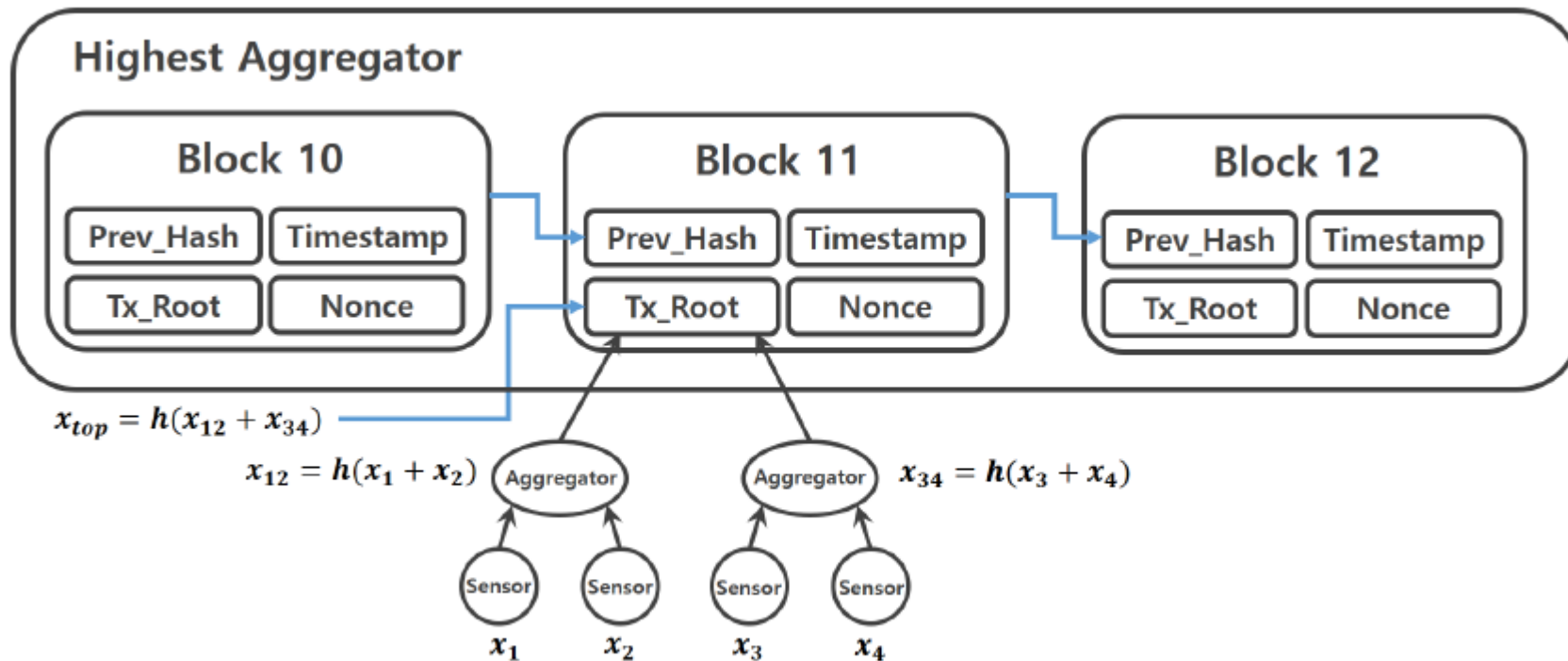
- 제안 스킴



- Aggregator 그룹키 분배
- 램포트 해시 체인 사용 그룹키 생성
- 새 디바이스 그룹키 할당
- 몇 번째 디바이스의 키인지 검증
- 해시 체인 - 다음 키 예측하기 힘들

블록체인 기반 IoT 디바이스 인증 스킴

- 제안 스킴



블록체인 기반 IoT 디바이스 인증 스킴

- 제안 스킴
- 최상위 Aggregator가 공개키 검증, 해시체인 생성 등 연산 처리
디바이스들 연산 부담 감소

블록체인 기반 IoT 디바이스 인증 스킴

- 논문 후기
 - 램포트 알고리즘 및 블록 체인 기술 활용
 - 저성능인 IoT를 위한 인증 방법
- 생각
 - Aggregator가 취약점이 될 수는 있는지

공공기관 프린터 관리 시스템의 취약점 분석

공공기관 프린터 관리 시스템의 취약점 분석

- 학교 도서관 등 공공 기관의 프린트 관리 서비스
- 프린트 관리 서비스의 취약성 분석

공공기관 프린터 관리 시스템의 취약점 분석

- 보안 통신을 사용하지 않아 도청에 취약
- 정보 인증 제공되지 않아 데이터를 쉽게 변조 가능
- 프린터의 스펙링 파일 정보 쉽게 획득 가능

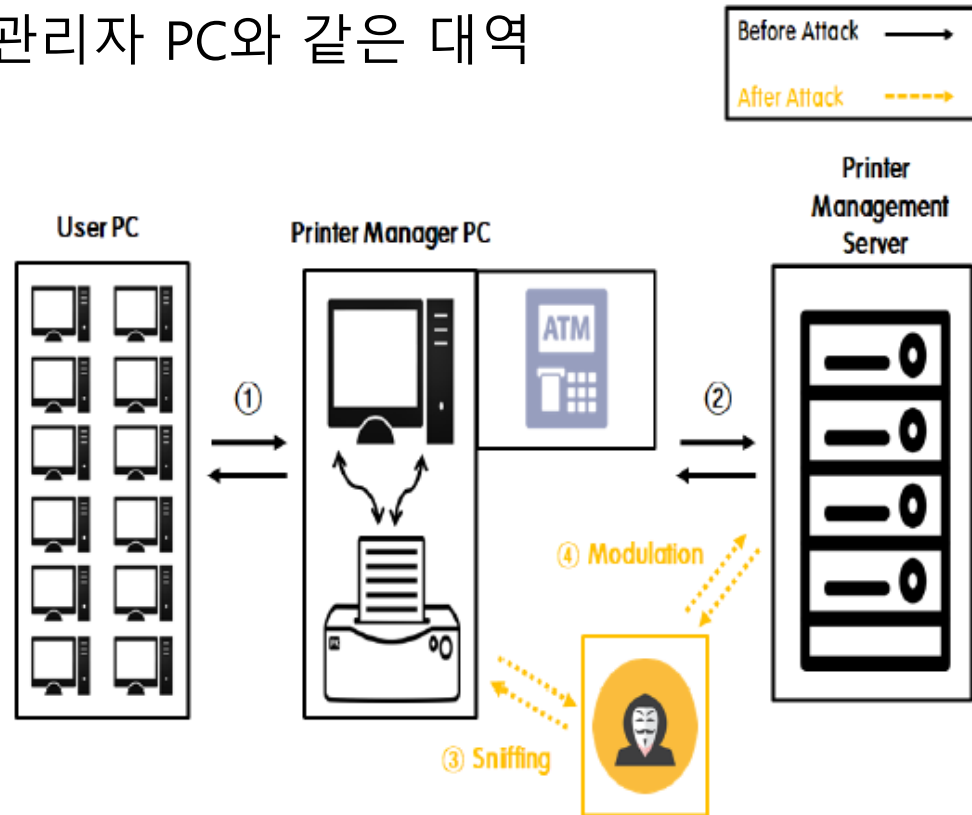
공공기관 프린터 관리 시스템의 취약점 분석

- 공격 시나리오
 1. 네트워크에 대한 공격
 2. 메타 데이터에 대한 공격 시나리오

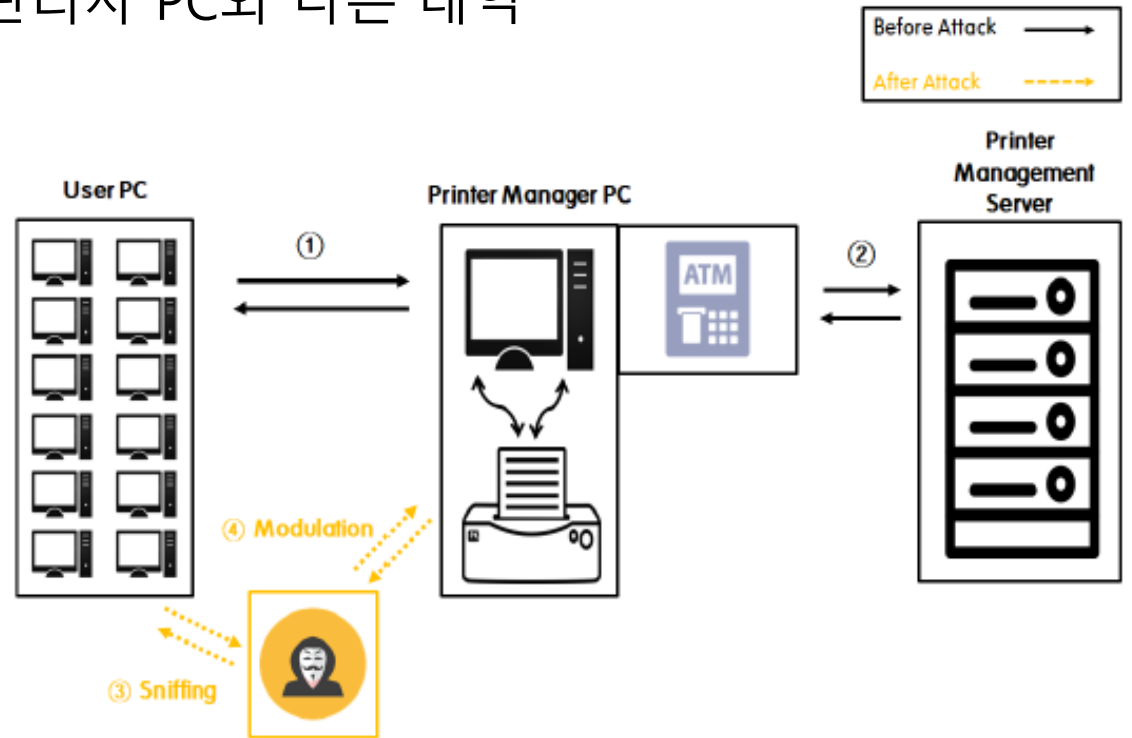
공공기관 프린터 관리 시스템의 취약점 분석

1. 네트워크에 대한 공격

관리자 PC와 같은 대역



관리자 PC와 다른 대역

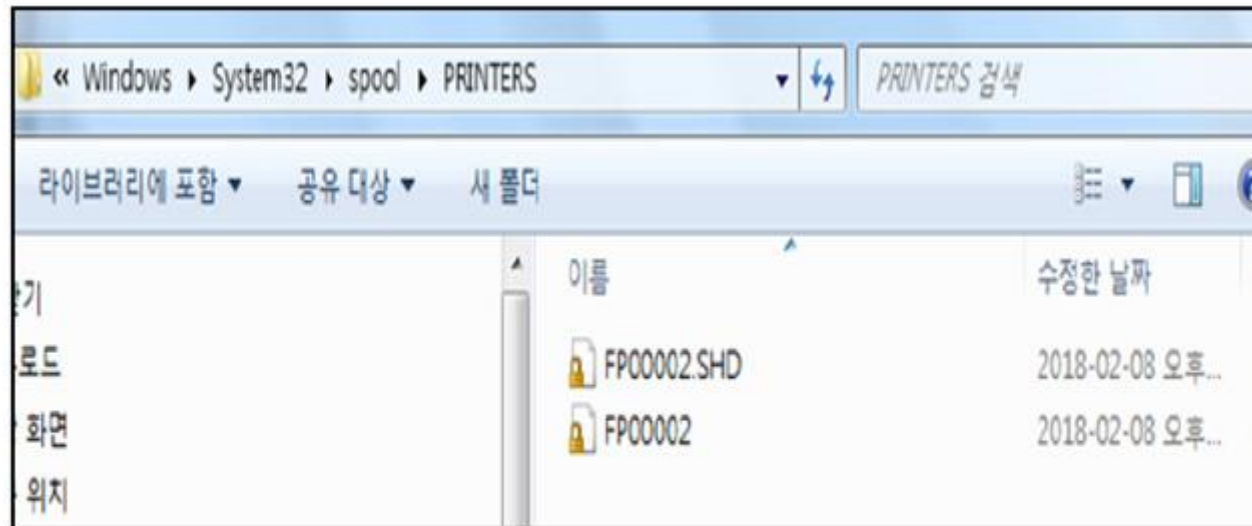


공공기관 프린터 관리 시스템의 취약점 분석

2. 메타 데이터에 대한 공격 시나리오

네트워크 접근이 불가능 - PC에 물리적인 접근

스풀 데이터에 직접 접근 - 대부분 기본값이 정해져 있음



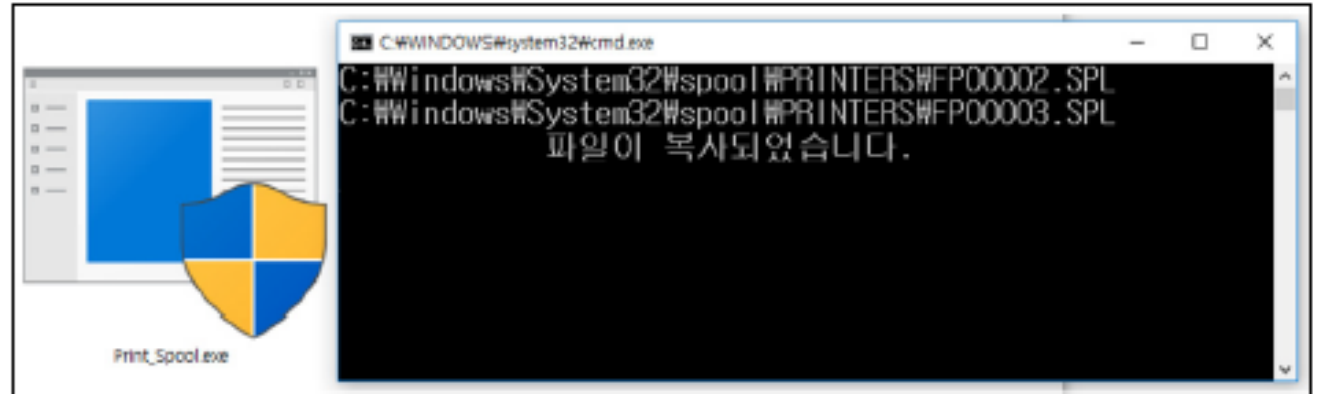
The spool file stored in the spool path
C:\Windows\System32\spool\PRINTERS

공공기관 프린터 관리 시스템의 취약점 분석

- 공격 결과

```
POST [redacted] HTTP/1.1
Host: [redacted]
Connection: keep-alive
Content-Length: 51
Cache-Control: max-age=0
Origin: [redacted]
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/61.0.3163.100 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/
webp,image/apng,*/*;q=0.8
Referer: [redacted]
Accept-Encoding: gzip, deflate
Accept-Language: ko-KR,ko;q=0.8,en-US;q=0.6,en;q=0.4
Cookie: JSESSIONID=B5A3BCD69A129712C0FA7FDFBA8946BC

svc=LOGIN&loginId=fafa9121&passwd=[redacted]&x=4&y=12 HTTP/1.1 200 OK
```



공공기관 프린터 관리 시스템의 취약점 분석

- 개선 방안
 - HTTPS를 통한 보안 통신
 - 인증서 설치
 - 인증서 관리는 하드웨어 보안 모듈 이용

공공기관 프린터 관리 시스템의 취약점 분석

- 신고 결과
 - 개선 되지 않음
 - 개선을 해야 할시 비용 발생
 - KISA(한국 인터넷 진흥원)에 신고 하였으나

“실제 서비스 중인 웹사이트나 시스템에 특정 데이터를 전송하여
영향을 줄 우려가 있는 서비스의 취약점은 평가 및 포상 대상에서 제외된다.”

공공기관 프린터 관리 시스템의 취약점 분석

- 논문 후기
 - 네트워크 스니핑 구조
 - 공공 프린터 관리 서비스의 취약점
 - 취약점을 밝히는 것을 꺼려하는 기업 문화
 - 보안 불감증

개인정보 노출에 대한 인터넷 사용자의 태도에 관한 연구

개인정보 노출에 대한 인터넷 사용자의 태도에 관한 연구

- 기업들이 소비자의 개인정보를 수집하는데 많은 노력
- 불법으로 소비자 개인정보를 거래하는 사건도 발생
- 정보 수집을 위한 인센티브를 제공하고 있으나 효과 미비

개인정보 노출에 대한 인터넷 사용자의 태도에 관한 연구

- CFIP – Concern for Information Privacy

개인정보 노출에 대한 염려 측정 모델

개인정보 노출에 대한 인터넷 사용자의 태도에 관한 연구

결론

- 개인정보가 다른 용도로 기업에서 이용되는 것에 제일 민감
정보 수집 시에 목적 및 이용 범위에 대한 구체적 설명 필요
- 정보 제공에 대한 경제적 보상
경제적 보상만으로는 정보제공 의도를 높이는 데는 한계가 있음

개인정보 노출에 대한 인터넷 사용자의 태도에 관한 연구

결론

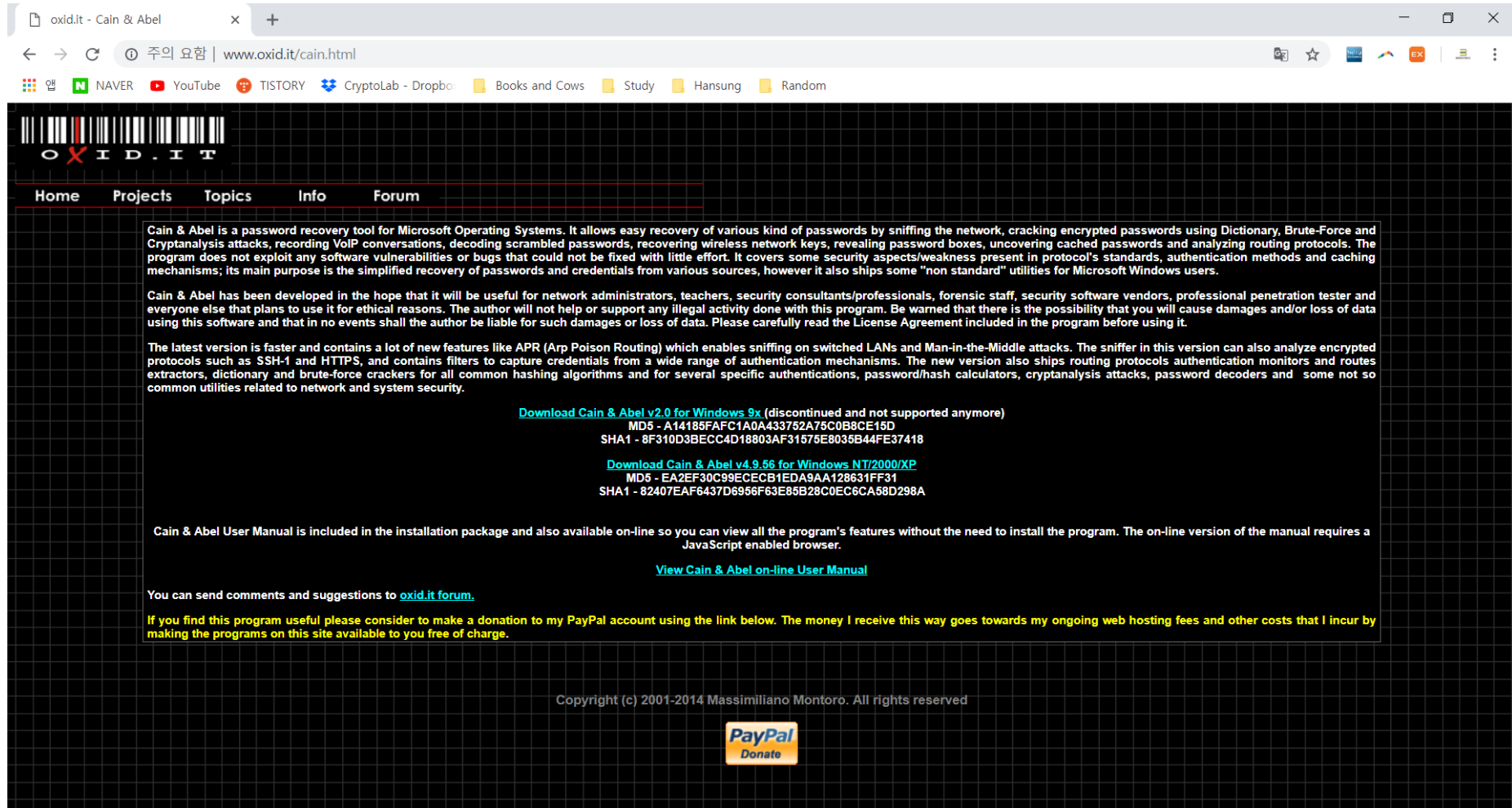
- CFIP 모델을 제외한 다른 요인들 고려해야 함
정보를 제공하는 기업에 대한 신뢰도 등

개인정보 노출에 대한 인터넷 사용자의 태도에 관한 연구

- 논문 후기
 - 보안은 단순 기술만의 문제가 아니다
 - 법, 규제 등과 밀접한 분야
 - 사람이라는 변수

Cain & Abel

Cain & Abel



Cain & Abel

- ARP 스푸핑
- DNS 스푸핑

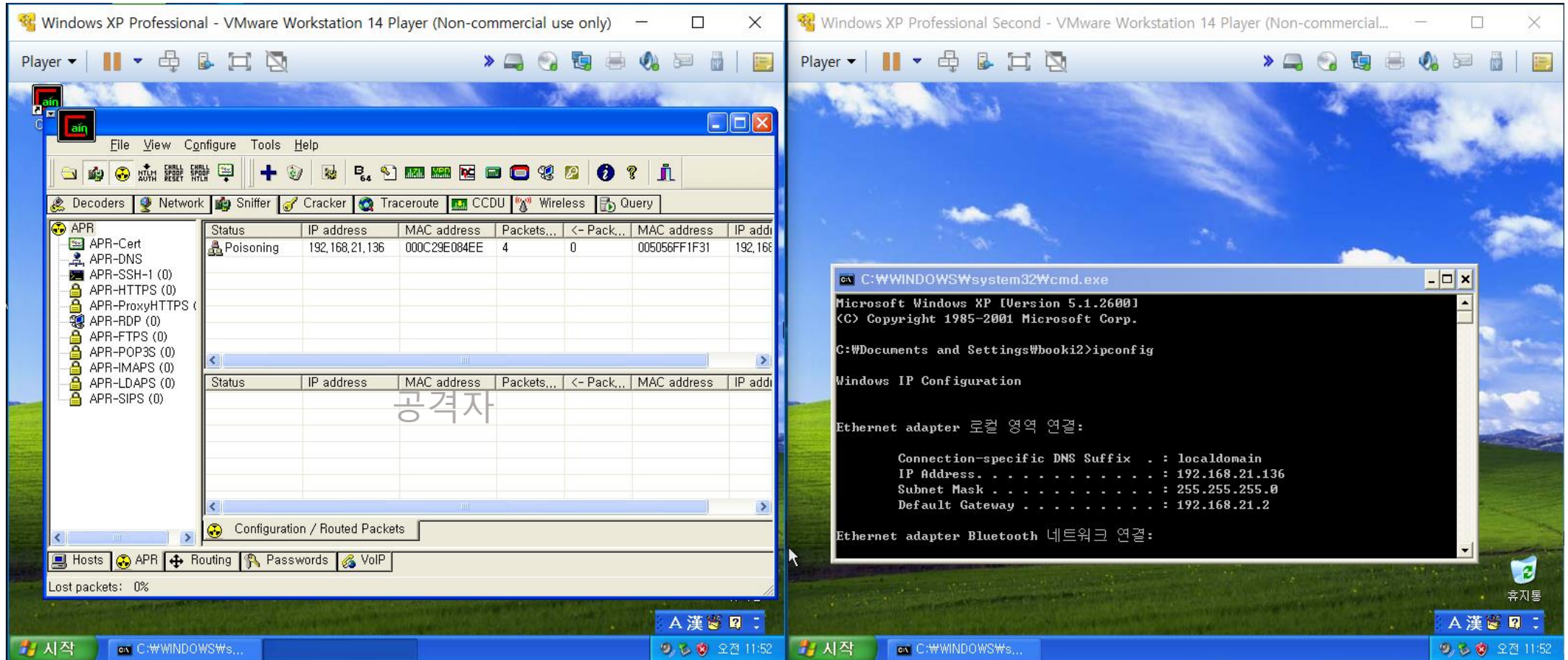
Cain & Abel

ARP 스푸핑

- 근거리 통신망에서 주소 결정 프로토콜(ARP) 메시지 이용
상대방의 데이터 패킷을 중간에서 가로채는 중간자 공격 기법

Cain & Abel

- 실험 환경



Cain & Abel

- 연결

The left window displays the Cain & Abel network sniffer interface. The 'Sniffer' tab is active, showing a list of captured packets. A red box highlights a table of packets with the following data:

Status	IP address	MAC address	Packets...	<- Pack...	MAC address	IP a
Full-routing	192.168.21.136	000C29E084EE	4	4	005056FF1F31	1,22
Full-routing	192.168.21.136	000C29E084EE	11	16	005056FF1F31	204
Full-routing	192.168.21.136	000C29E084EE	84	135	005056FF1F31	175
Full-routing	192.168.21.136	000C29E084EE	4	4	005056FF1F31	175
Full-routing	192.168.21.136	000C29E084EE	6	7	005056FF1F31	40,6
Full-routing	192.168.21.136	000C29E084EE	6	5	005056FF1F31	184
Full-routing	192.168.21.136	000C29E084EE	4	4	005056FF1F31	22,6

The right window displays the MSN homepage in Microsoft Internet Explorer. The address bar shows the URL <http://www.msn.com/ko-kr/>. The page includes a search bar, a navigation menu, and a weather forecast for Seoul (서울) showing a high of 8°C and a low of -1°C.

Cain & Abel

- 실험 결과

The image displays two side-by-side screenshots from a Windows XP Professional virtual machine running on VMware Workstation 14 Player. The left window shows the Cain & Abel network sniffer interface, and the right window shows a Windows Internet Explorer browser displaying the Hongcheon Elementary School homepage.

Cain & Abel Interface:

- File View:** File, View, Configure, Tools, Help
- Decoders:** Network, Sniffer, Cracker, Traceroute, CCDU, Wireless, Query
- Left Panel:** List of protocols including FTP, HTTP (3), IMAP, LDAP, POP3, SMB, Telnet, VNC, TDS, TNS, SMTP, NNTP, DCE/RPC, MSKerb5-PreAut, Radius-Keys, Radius-Users, ICQ, IKE-PSK, MySQL, SNMP, SIP, GRE/PPP, and PPPoE.
- Table:**

Timestamp	HTTP server	Client	Username	Password	URL
19/12/2018 - 12:34:20	124.138.129.149	192.168.21.137	sh657o	hack_@#	http://www.hon
19/12/2018 - 12:34:29	124.138.129.149	192.168.21.137	sh657o	ani12_>#	http://www.hon
19/12/2018 - 12:35:40	124.138.129.149	192.168.21.138	sh657o	hack_@#	http://www.hon

- Bottom Panel:** Hosts, APR, Routing, Passwords, VoIP. Status: Lost packets: 0%.

Internet Explorer Interface:

- Address Bar:** http://www.hongcheon.es.kr/wah/main/
- Page Title:** 홍천초등학교 홈페이지에 오신걸 환영합니다. - Windows Internet Explorer
- Page Content:** Hongcheon Elementary School homepage with navigation links (학교소개, 학교마당, 학생마당, 학부모마당, 혁신공감학교, 방과후학교, 학교평가) and a large image of the school building.

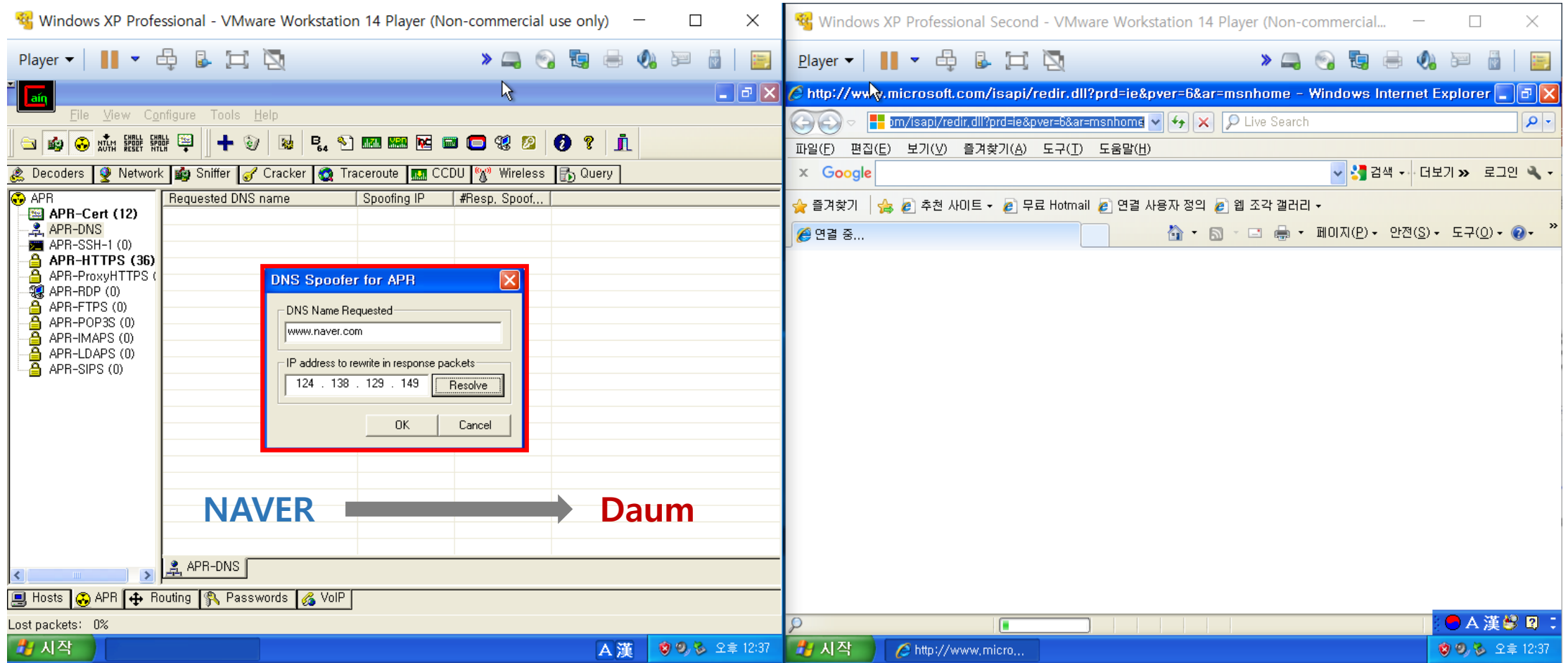
Cain & Abel

DNS 스푸핑

- 도메인 네임 시스템에서 전달되는 IP 주소 변조
사용자가 의도하지 않은 주소로 유도

Cain & Abel

- DNS 스푸핑



Cain & Abel

- DNS 스푸핑

The image shows two side-by-side windows from a VMware Workstation 14 Player. The left window is titled "Windows XP Professional - VMware Workstation 14 Player (Non-commercial use only)" and displays the Cain & Abel interface. The right window is titled "Windows XP Professional Second - VMware Workstation 14 Player (Non-commercial use only)" and displays a Windows Internet Explorer browser window showing a Daum error page.

Cain & Abel Interface:

- Menu:** File, View, Configure, Tools, Help
- Toolbar:** Decoders, Network, Sniffer, Cracker, Traceroute, CCDU, Wireless, Query
- Left Panel:** Tree view showing various protocols: APR, APR-Cert (14), APR-DNS, APR-SSH-1 (0), APR-HTTPS (36), APR-ProxyHTTPS, APR-RDP (0), APR-FTPS (0), APR-POP3S (0), APR-IMAPS (0), APR-LDAPS (0), APR-SIPS (0).
- Table:** A table with columns: Requested DNS name, Spoofing IP, #Resp, Spoof...
 - Row 1: ☒ www.naver.com, 203.133.167.16, 2
- Bottom Panel:** Hosts, APR, Routing, Passwords, VoIP. Status: Lost packets: 0%.

Internet Explorer Window:

- Title Bar:** Daum 요청하신 페이지의 사용권한이 없습니다. - Windows Internet Explorer
- Address Bar:** http://status.daum.net/error/error403.html
- Page Content:** Daum logo, "다음첫화면 고객센터", and a large red text message: "요청하신 페이지의 사용권한이 없습니다." (The page you requested does not have the required permissions).
- Footer:** "이용에 불편을 드린 점 진심으로 사과드립니다." (We sincerely apologize for the inconvenience caused by the use.)

계획

- 정보 보호 학회 논문
- WireShark
- 네트워크
- 암호학

감사합니다