MPIS 2020

2020 의료기관 개인정보보호&정보보안 컨퍼런스

KU MEDICINE

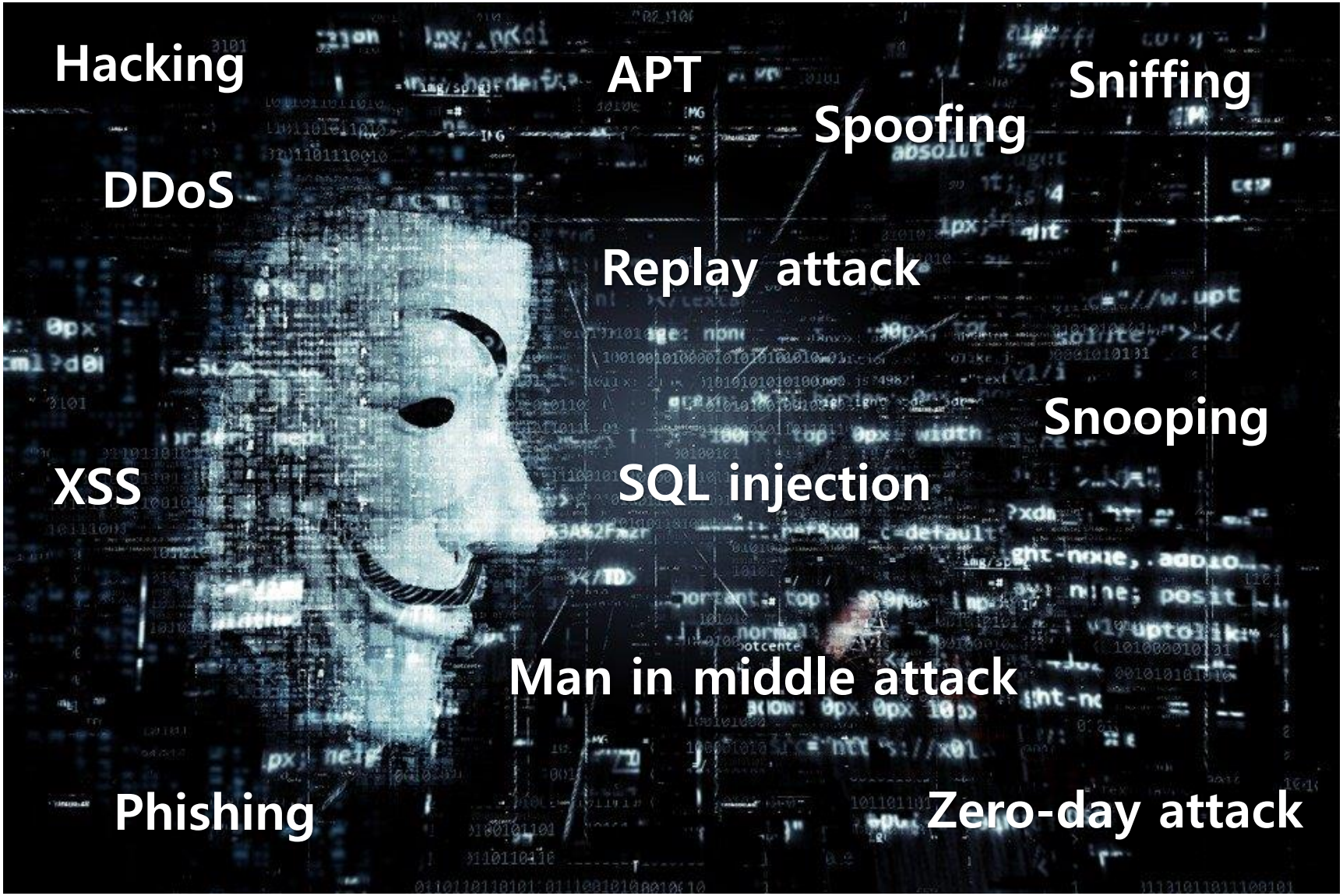
KOREA UNIVERSITY MEDICINE

슬기로운 병원보안생활

2020. 7. 30

강병익

시작하면서


Hacking
APT
Sniffing
Spoofing
DDoS
Replay attack
Snooping
XSS
SQL injection
Man in middle attack
Phishing
Zero-day attack

시작하면서

국가주요정보통신 기반시설 취약점 점검 기준

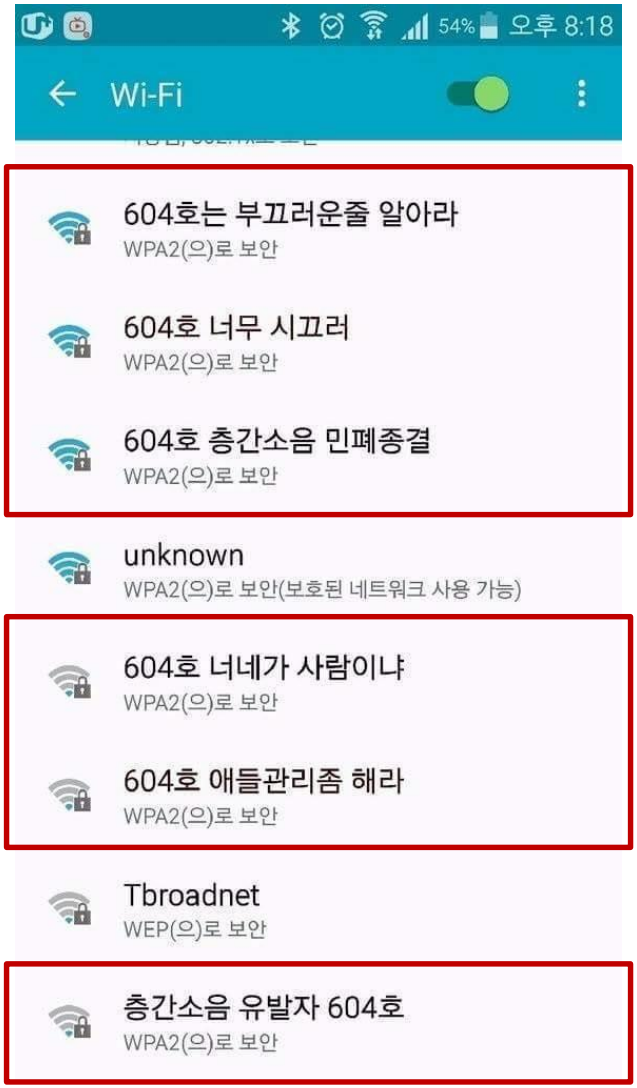
PC 취약점 분석·평가 항목

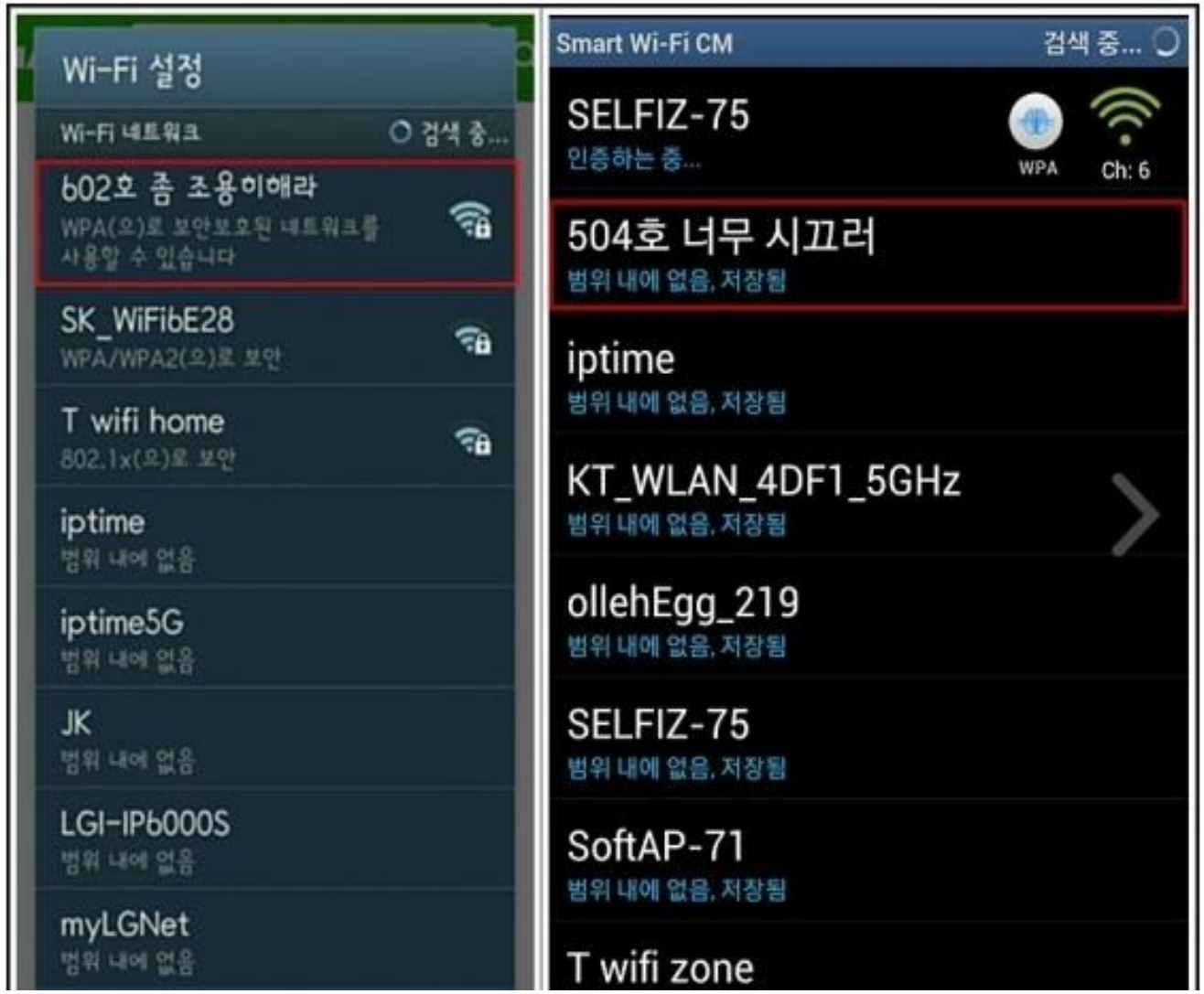
분류	점검항목	중요도	항목코드
1. 계정관리	패스워드의 주기적 변경	상	PC-01
	패스워드 정책이 해당 기관의 보안 정책에 적합하게 설정	상	PC-02
	복구 콘솔에서 자동 로그온을 금지하도록 설정하여 사용하고 있는가?	중	PC-15
2. 서비스관리	공유 폴더 제거	상	PC-03
	항목의 불필요한 서비스 제거	상	PC-04
	Windows Messenger(MSN, .NET 메신저 등)와 같은 상용메신저의 사용 금지	상	PC-05
	파일 시스템이 NTFS 포맷으로 되어 있는가?	중	PC-16
	대상 시스템이 Windows 서버를 제외한 다른 OS로 멀티부팅이 가능하지 않도록 설정하여 사용하는가?	중	PC-17
	브라우저 종료 시 임시 인터넷 파일 폴더의 내용을 삭제하도록 설정하여 사용하는가?	하	PC-18
3. 패치관리	HOT FIX 등 최신 보안패치 적용	상	PC-06
	최신 서비스팩 적용	상	PC-07
	MS-Office, 훈글, 어도비 아크로뱃 등의 응용 프로그램에 대한 최신 보안패치 및 벤더 권고사항 적용	상	PC-08
4. 보안관리	바이러스 백신 프로그램 설치 및 주기적 업데이트	상	PC-09
	바이러스 백신 프로그램에서 제공하는 실시간 감시 기능 활성화	상	PC-10
	OS에서 제공하는 침입차단 기능 활성화	상	PC-11
	화면보호기 대기 시간 설정 및 재시작 시 암호 보호 설정	상	PC-12
	CD, DVD, USB 메모리 등과 같은 미디어의 자동실행 방지 등 이동식 미디어에 대한 보안대책 수립	상	PC-13
	PC 내부의 미사용(3개월) ActiveX 제거	상	PC-14
	시스템 부팅 시 Windows Messenger가 자동으로 시작되지 않도록 설정되어 있는가?	중	PC-19
	원격 지원을 금지하도록 정책이 설정되어 있는가?	중	PC-20

PC-03 (상)	2. 서비스 관리 > 2.1 공유폴더 제거
취약점 개요	
점검내용	■ 기본 공유 폴더(C$, D$, Admin$), 미사용 공유폴더가 존재하는지 점검하고 공유폴더를 사용하는 경우 공유 폴더 접근 권한에 "Everyone"이 존재하거나 접근을 위한 암호가 설정되어 있는지 점검
점검목적	■ 사용하지 않는 불필요한 공유 폴더를 해제하거나 불가피하게 사용하고 있는 공유폴더의 경우 암호를 설정하는 등의 조치를 통해 인가된 사용자만 접근이 가능하게 함으로써 무분별한 접근을 제한함
보안위협	■ 시스템 기본 공유 폴더의 경우 기본 드라이브를 개방해놓고 사용하는 것과 동일함(예 : 실행창 -> ₩₩192.168.16.xxx₩c$ 으로 C드라이브 접근 가능) ■ 접근권한이 Everyone으로 설정된 공유 폴더는 정보 유출 및 악성코드 유포의 접점이 될 수 있음
참고	-
점검대상 및 판단기준	
대상	■ Windows XP, Windows 7, Windows 8.1, Windows 10
판단기준	**양호 :** 불필요한 공유 폴더가 존재하지 않거나 공유폴더에 접근권한 및 암호가 설정되어있는 경우
	취약 : 불필요한 공유 폴더가 존재하거나 접근권한 및 암호 설정 없이 공유폴더를 사용하는 경우
조치방법	공유 폴더 불필요 시 삭제 공유 폴더 필요 시 적절한 접근권한 부여 및 암호 설정 조치 후 AutoShareServer(또는, AutoShareWks)값 변경으로 자동 공유 방지
점검 및 조치 사례	
< 공유 폴더 설정 기준 > 1. C$, D$, Admin$ 등의 기본 공유 폴더 제거 2. 기본 공유 폴더 제거 후 시스템 재부팅 시 "기본 공유 폴더가 자동으로 공유되는 것"을 방지하기 위해 해당 레지스트리의 AutoShareServer 값을 "0"으로 설정 3. 일반 공유 폴더 사용 시 공유 폴더 접근 권한에 "Everyone" 제거 4. 일반 공유 폴더 사용 시 접근이 필요한 계정에만 적절한 (읽기, 변경)권한 설정 5. 일반 공유 폴더 사용 시 공유 폴더 접근을 위한 암호 설정	

출처 : 기술적 취약점 분석/평가 상세가이드 (KISA, 한국인터넷진흥원)

무선 AP


54% 오후 8:18
Wi-Fi
604호는 부끄러운줄 알아라
WPA2(으)로 보안
604호 너무 시끄러
WPA2(으)로 보안
604호 층간소음 민폐종결
WPA2(으)로 보안
unknown
WPA2(으)로 보안(보호된 네트워크 사용 가능)
604호 너네가 사람이냐
WPA2(으)로 보안
604호 애들관리좀 해라
WPA2(으)로 보안
Tbroadnet
WEP(으)로 보안
층간소음 유발자 604호
WPA2(으)로 보안


Wi-Fi 설정
Wi-Fi 네트워크
검색 중...
602호 좀 조용이해라
WPA(으)로 보안보호된 네트워크를 사용할 수 있습니다
SK_WiFi6E28
WPA/WPA2(으)로 보안
T wifi home
802.1x(으)로 보안
iptime
범위 내에 없음
iptime5G
범위 내에 없음
JK
범위 내에 없음
LGI-IP6000S
범위 내에 없음
myLGNet
범위 내에 없음
Smart Wi-Fi CM
검색 중...
SELFIZ-75
인증하는 중...
WPA
Ch: 6
504호 너무 시끄러
범위 내에 없음, 저장됨
iptime
범위 내에 없음, 저장됨
KT_WLAN_4DF1_5GHz
범위 내에 없음, 저장됨
ollehEgg_219
범위 내에 없음, 저장됨
SELFIZ-75
범위 내에 없음, 저장됨
SoftAP-71
범위 내에 없음, 저장됨
T wifi zone

무선 AP

공부/네트워크

공유기 초기 비밀번호 모음

2017. 5. 25. 14:35

공유기 초기 비밀번호 모음

KT 와이파이

KT_WLAN - 1234567890

KT SSID , KT_WLAN -1234567890

택시 EGG - SHOW3382

개인 EGG - Password

SKT 와이파이

Tbroadnet - 123456789

sk - a123456789

LG U+ 와이파이

myLgnet, mylg070 - 123456789a , 987654321a, 1234567890

기타 와이파이

스타벅스 : 매장별 전화번호(영수증에 보통 있음)

헬로우디 : 534f4b4354

맥도날드 : 16005252

hellowireless: 534f4b4354

so070voip : 2127393302

tobis : 1234

옆집 사람이 아마도 캘럭시 S10 5G를 구입했나봅니다

그냥그렇게살아 — A — 2020-03-27 16:12:30 — 2762

제 데스크탑에 계속 블루투스 연결을 하라고 잡히네요...;;;;

굳이 옆집 사람이 뭘 갖고 있는지 궁금하지는 않은데 말이죠...

나름 공해네요...;;;

4 Comments

albatros~ — Updated at 2020-03-27 16:15:42 — 1

저도 그런적 있었는데, 한 이틀 내내 그러길래, "몇호 입니다. 짜증나게 자꾸 연결하지 마세요." 라고 기기 이름을 바꿔 놨더니 두어번 더 연결하다가 안하더군요.

헤브류 — 2020-03-27 16:41:54 — 2

꽤 오래전 이야긴데가요. 인터넷을 아파트로 들여올때

한동에 스위칭허브 하나로 물려서 한동의 모든 세대의 공유폴더를 다 볼수있었던 시절도 있었습니다.

요즘은 블루투스도 블루투스지만

스마트뷰기기가 아랫집윗집것이 떠서 윗집 아랫집 TV인치를 확인할수 있게 되었습니다.

참고로 윗집은 얼마전에 70인치로 바꾸었더군요..

Cosmos — 2020-03-27 16:50:29

그때는 그랬었죠... 공유기에 암호 걸린데도 거의 없었지요...

공유폴더 노출 사례

#1.직장인 김지훈씨(32)는 지난 주말 집에서 노트북PC로 무선인터넷망을 검색하다가 깜짝 놀랐다.

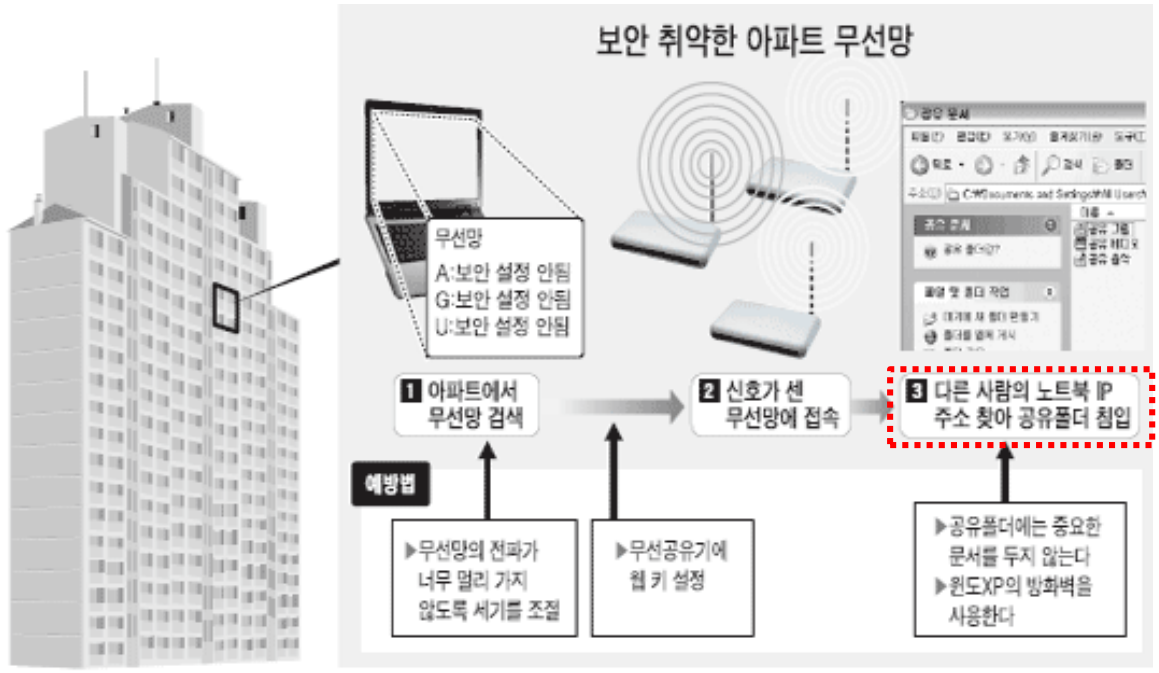
자신의 노트북으로 접속할 수 있는 무선랜망이 있는지 찾아보려고 네트워크 공유폴더에 들어가 여러 파일 중 하나를 열었더니 이웃 집 아저씨 이름의 치아 사진이 떴다.

이 파일들은 김씨의 주상복합아파트 옆 건물에 입주해 있는 A치과에서 흘러 나왔다.

치과에서 무선랜 공유기에 비밀번호를 설정하지 않아 공유폴더에 있는 파일이 그대로 열린 것이다.

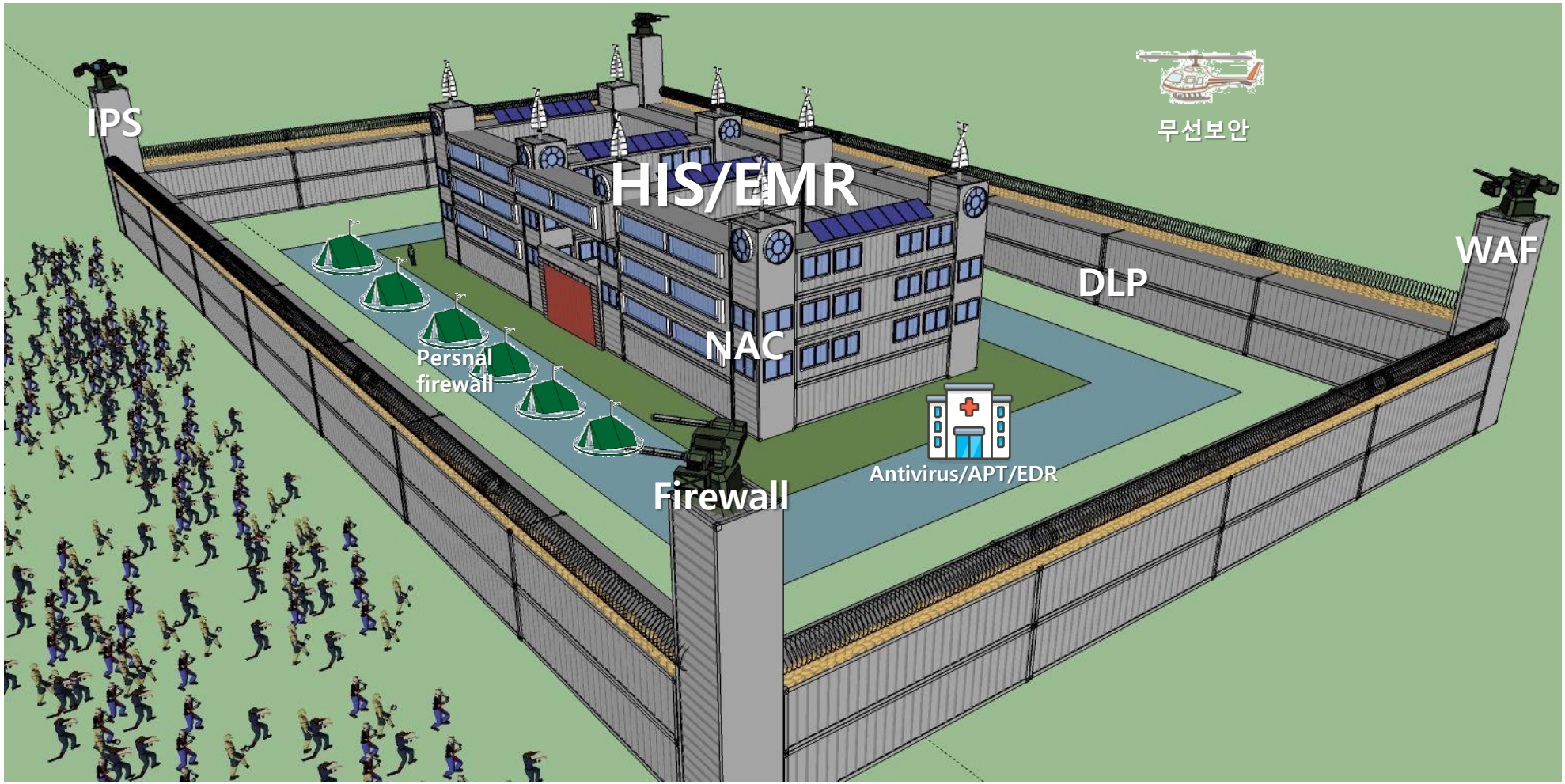
김씨가 접속한 공유폴더에는 병원 환자들의 개인 정보는 물론 진료 기록과 의료보험 관련자료 파일까지 들어있었다.

출처 : 어! 내 PC서 다보이네... 무선랜 보안 비상 (한국경제, 2008년)



출처 : 아파트 단지서 접속 실험해 보니 남의망 그대로 떠 (중앙일보, 2006년)

인트라넷과 보안


IPS
HIS/EMR
무선보안
WAF
DLP
NAC
Persnal
firewall
Antivirus/APT/EDR
Firewall

공유폴더 접근 방법

공유폴더 자료

병원 환경의 특징

병원 PC 환경의 특징

1. **병원별 PC가 수백~수천대로 많다.**
2. **공용 PC가 많다. (스테이션, 의국, 검사실, 외래 등)**
3. **매년 다양한 직종의 신입 직원들이 입사한다. (간호사, 인턴, 의료기술직, 행정직 등)**
4. **원내에서 다양한 형태와 많은 양의 데이터를 주고 받는다. (PC, 의료장비 등)**
5. **많은 양의 데이터 보다 1건의 민감 데이터가 더 중요할 수 있다.**

맺음말

공유폴더

1. 내일부터 공유폴더 절대 쓰지마!!!!! (X)
2. 공유폴더 사용시 암호 설정 및 필요한 권한만 설정

관리적

1. 주기적/지속적인 공유폴더 위험성 교육 (정보보호의 날, 신입직원 교육)
2. 주기적/지속적인 공유폴더 점검 (사이버보안진단의날 등 보안점검 체크)

기술적

1. 대체 방법으로 전환 (NAS, 파일서버 등)
2. 공유폴더 중앙제어 (NAC, AD, Antivirus, DLP, 내PC지키미 등)
   - 사전 충분한 테스트 必

KU MEDICINE

MPIS 2020
2020 의료기관 개인정보보호&정보보안 컨퍼런스

감사합니다

Email : finaldoit@kumc.or.kr