情 報 保 護 學 會 誌
第21卷 第5號, 2011. 8

스마트폰 DDoS 공격 동향

장 기 헌*, 최 상 명**, 염 흥 열***

요 약

스마트폰 시장이 전체 모바일 시장에서 큰 비중을 차지하고 있으며, 사용자 수는 급격하게 증가하고 있다. 스마트폰은 다양한 인터페이스 및 기능 등 기존 휴대폰과는 차별화된 장점을 가지고 있으며, 사용자의 취향에 따라 어플리케이션 설치 및 제거가 가능하다. 또한 신용정보, 인증서, 전화번호부 등 다양한 개인정보를 저장하고 있으며, 업무용으로도 사용되고 있다. 이러한 정보를 저장하고 있는 스마트폰에는 다양한 보안 위협이 존재하고 있으며, 개인 및 기업에게 치명적인 피해를 발생 시킬 수 도 있다. 특히 스마트폰을 이용한 DDoS 공격은 기존 DDoS(Distributed Denial of Service) 공격과 비슷하지만 스마트폰만이 가지고 있는 환경 때문에 여러 가지 다른 특징을 보인다. 본 논문에서는 기존 DDoS 공격 기법 및 동향을 알아보고, 좀비 스마트폰과 좀비 PC의 환경을 비교 분석함으로써 스마트폰 DDoS 공격 동향을 살펴본다.

Ⅰ. 서 론

스마트폰은 전체 모바일 시장에서 차지하는 비중이 지속적으로 높아지고 있으며, 다양한 기능을 가지고 있기 때문에 여러 용도에서 사용되고 있다. 사용자들은 필요한 어플리케이션을 다운로드하여 사용할 수 있으며, 금융 거래 및 정보활동을 할 수 있다. 기업에서는 업무용 으로도 사용하고 있으며, 업무용으로 사용되는 스마트폰의 경우 기업 기밀정보를 담고 있을 수 있기 때문에 보안강도는 더 높아야 한다.

하지만 편리한 기능 및 어플리케이션을 통해 사용자의 스마트폰이 악성코드에 감염되어 주요 정보를 유출시킬 수 있다. 또한 좀비 스마트폰이 되어 DDoS공격이 발생할 수 도 있다. 2009년 7.7 DDoS 대란 이후로 DDoS에 대한 많은 기술적, 정책적 방안이 수립되어 졌다. 하지만 2011년 3월 4일 발생한 DDoS 공격을 통해 아직까지 대응체계가 미비하다는 것을 알 수 있었다. 스마트폰의 성능이 급속도로 높아지고 있고, 휴대성, 이동성이 간편하기 때문에 좀비스마트폰으로 DDoS 공격이 발생한다면 기존 좀비 PC를 이용한 DDoS 공격에 비해 보다 더 큰 피해가 발생될 것으로 판단된다. 또한 통신망에 마비가 올수 있기 때문에 불편함은 더욱 커질 것이다. 때문에 이러한 위협을 신속히 파악하여 대응할 수 있는 다양한 방안이 제시되어야 할 것이다.

따라서 본 논문에서는 기존 DDoS 공격 및 스마트폰 DDoS 공격 동향을 살펴본다. 2장에서는 기존 DDoS 공격 기법 및 동향을 살펴보고, 3장에서는 좀비 스마트폰과 좀비 PC의 환경을 분석하고 DDoS공격 가능성을 살펴본 뒤 4장에서 향후 전망을 서술하고 결론을 맺는다.

Ⅱ. 기존 DDoS공격 동향

본 장에서는 최근 발생하는 주요 DDoS 공격기법의 종류와 동향에 대해서 알아본다.

2.1 공격기법

- 플래그먼트 플루딩(Fragment Flooding) 공격[1] : 가장 단순하면서 강력한 공격수단 중 하나로, ICMP(Internet Control Message Protocol)를 이용하여 대량의 트래픽을 발생시키는 공격이다. 공격 트래픽 생성이 수월하고 효과가 크기 때문에

이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. 2010-0025393).
* 순천향대학교 정보보호학과 (nvdark@gmail.com)
** 순천향대학교 정보보호학과, (주)하우리 선행기술팀 팀장 (sionics@hauri.co.kr)
*** 순천향대학교 정보보호학과 (hyyoum@sch.ac.kr)

많은 DDoS 공격에 사용되고 있는 기법이다. 플래그먼트 플루딩 공격에 대한 탐지는 어렵지 않게 식별이 가능하나, 탐지된 시점에서 이미 공격 대상은 공격 트래픽이 허용 대역폭을 넘고 있기 때문에 대응이 제한적이다.

- HTTP 플루딩 공격[1] : 최근 HTTP (hyper text transfer protocol)관련 공격이 늘어가고 있으며, 고도화 되고 있다. HTTP 플루딩 공격은 공격대상 웹 서버에게 대량의 HTTP요청을 전송하여 웹 서버 운영에 장애를 발생시킨다.
- SYN 플루딩 공격[1] : 서버의 자원을 고갈시키기 위해 사용되는 공격으로 상대적으로 공격의 탐지 및 방어가 용이하다. 기존에는 허위 IP를 이용한 공격이 많았으나, 점점 대량의 좀비 PC를 이용한 실제 IP기반의 공격이 많아지고 있다.
- URL 리다이렉트 우회 공격[6] : 좀비 PC에서 특정 URL에 요청을 수행할 경우, 좀비 PC에 다른 URL로 리다이렉트 신호를 전송함으로써 공격을 차단하는 방법을 우회하는 공격으로 302 URL 리다이렉트 신호를 인식하여 전송된 새로운 URL로 접속을 수행하여, URL 리다이렉트를 통한 대응 기법을 우회하는 특징이 있다.

이 밖에 Slowloris/Pyloris Attack, Slow HTTP POST Attack 등이 있으며[6], 공격 대상으로 구분하면 [표 1]과 같고, 대상에 따라 공격 방법과 피해 범위가 다르다.

〔표 1〕 DDoS공격 대상/계층에 따른 분류[2]

분류	내용
L7(응용) 공격	특정 호스트 내의 응용에 대한 공격으로 정당한 사용자의 서비스를 제한. 공격대상 응용만 서비스가 제한되기 때문에, 동일 호스트 내 다르 응용은 정상동작될 수 있음. 트래픽 양이 매우 적으며, 탐지가 어렵다
L4(TCP/UDP) 공격	특정 호스트의 모든 네트워킹 서비스 혹은 시스템 자체를 마비시키기 위하여 시도되는 공격. 시스템 내부의 TCP, UDP 스택의 자원관리 상의 취약점을 공격하는 것으로 L4이상 계층에 대한 마비를 초래하며 TCP SYN, SYN-ACK, RESET Flooding, UDP Flooding 등이 있다
L3(IP, ARP, ICMP) 공격	특정 호스트의 모든 네트워킹 서비스 혹은 시스템 자체를 마비시키기 위해 시도되는 공격. IP Flooding, ARP, RARP 스푸핑, ICMP Flooding등이 있다
중요 노드 공격	공격 대상 네트워크내의 중요 자원에 대한 공격으로 DNS, 라우터 등이 대상이다
대역폭 소비 공격	한정된 대역폭을 가지는 네트워크 회선 상에 막대한 공격 트래픽을 전송함으로써 네트워크를 마비시키는 공격이다
하부 공격	전체 인터넷 망 자체를 마비시키기 위한 공격이다. 핵심은 공격 대상을 어떻게 마비시키는 가에 있는 것이 아니라, 동시 다발적으로 인터넷 인프라에 대하여 공격이 시도되는 것에 있다.

2.2 공격동향

2009년 7.7 DDoS대란에 이어 2011 발생한 3.4 DDoS를 비교 하면 [표 2]와 같다.

이 중 3.4 DDoS 공격 구성은 다음과 같다. 파일공유 사이트(P2P)에서 악성코드를 다운로드 하고 설치되면 암호화된 통신을 통하여 C&C(Command&control)서버에 설정된 공격 대상 IP 및 Main DLL(Dynamic linking library)을 받아오게 된다. 그 후 공격에 사용되는 파일을 생성 또는 변종을 다운로드 하게 되며, host 파일을 변조한다. DDoS 모듈은 공격대상 IP에 공격을 시도하고, MBR/파일파괴 모듈은 MBR/파일을 파괴한다. 최근 발생하는 DDoS공격은 하나의 악성코드가 아닌 다수의 악성코드가 유기적으로 연동되어 동작한다. 즉 악성코드간의 관계가 중요해졌으며, 추가 파일을 다운로드할 수 있는 모듈들과 연동된다. 또한 공격 시나리오에 맞게 주요 파일 업데이트가 가능하며, 공격 스케줄에 맞춰서 공격 대상으로 동시 다발적 공격이 가능하다. 여러 가지 공격기법을 이용하여 다수의 목표를 공격하

〔표 2〕 7.7DDoS와 3.4DDoS 비교

구분	7,7 DDoS	3.4 DDoS
유포경로	파일 공유 사이트	파일 공유 사이트
유포방법	자동 업데이트되는 파일을 악성코드로 바꿈	자동 업데이트되는 파일을 악성코드로 바꿈
공격방법	Cache Control 공격, 같은 파일 구성에 의한 공격	Cache Control 공격, 공격할 때마다 변화하는 파일 구성
특징	특정 일시에 동시 공격, 공격대상 재지정, 데이터 삭제 등	특정 일시에 동시 공격, 공격대상 재지정, 데이터 삭제, 정보 유출, 스팸발송 등(7.7)
C&C서버	70개국 746대 3단계 구조 및 마스터 서버 존재	61개국 435대 4단계 구조 및 마스터 서버 존재

기 때문에 대응이 어려우며, 주요 문서 및 파일을 유출하거나 삭제(자신 포함)가 가능하다.

2008년도 3월에 발생했던 미레에셋 DDoS 공격은 1만여대의 PC가 감염되고, 미국에 있는 공격 명령 서버에 270대의 좀비 PC를 조종해 증권사 사이트 접속장애를 일으켰으며[3], 경쟁 게임사이트에게 DDoS공격을 13만여대의 좀비 PC와 홍콩과 미국에 위치한 공격명령서버로 시행했다.[4]

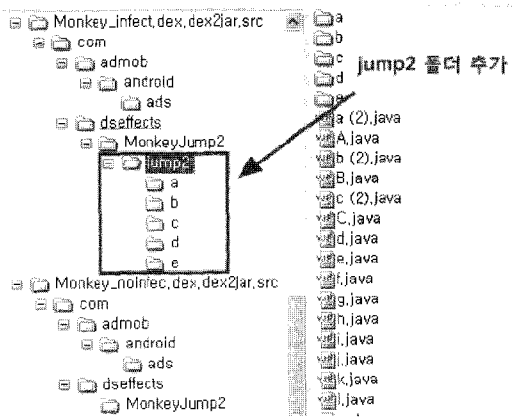
2011년 5월에도 뉴질랜드 의회에 정기적인 DDoS공격이 있었다는 보도 또한 있었다.[5]

Ⅲ. 스마트폰 DDoS공격 동향

스마트폰을 이용한 DDoS공격 동향 및 환경을 알아본다. 또한 스마트폰 환경에서만 발생할 수 있는 추가 위협을 알아본다.

3.1 환경비교분석

스마트폰은 2010년에 2.97억대가 판매[11] 되었으며, 이동성과 휴대성이 뛰어나 때와 장소를 가리지 않고 앱



〔그림 1〕 리패키징 악성코드

스토어를 통해 필요한 어플리케이션을 다운로드 할 수 있다. 이는 PC보다 다양한 경로와 환경을 통해 악성코드에 감염될 수 있는 상황을 제공한다. 안드로이드 폰의 경우 정식 마켓이 아닌 제3자(3rd-party) 마켓에서 어플리케이션을 무료로 다운로드 받아 사용할 수 있지만 많은 어플리케이션이 검증되지 않았기 때문에 악성코드에 감염될 확률이 매우 높다. 또한 스마트폰을 통한 인터넷 동영상 플레이, 웹 검색 등으로 모바일 트래픽이 대폭

〔표 3〕 좀비 PC 와 좀비 스마트폰의 환경 비교[7]

구분	좀비 PC DDoS	좀비 스마트폰 DDoS
CPU	2Ghz 이상 (Dual / Quad core)	1~1.2Ghz(Single / Dual core)
Power	Power Cabl(상시전력)	- 베터리 사용(약 1350mAh~1930mAh) - 스크린 사용 시 (약 4시간)
Network	Ethernet(100Mbps, 1Gbps)	- 802.11 b/g/n (54Mbps) - 3G (2.4Mbps) - 4G (저속이동 시 1Gbps, 고속이동 시 100Mbps)
System Thread	대량의 쓰레드 생성 가능	다수의 쓰레드 생성 시 성능 저하 및 발열
악성코드 감염 및 전파 방법	- 웹 브라우저 취약점(IE) - 웹 컨텐트 - E-mail, SNS, Messenger - ARP Spoofing - USB	- 공식 마켓, 3rd-party 마켓 - SMS 메시지, 연락처 목록 - QR Code - Rogue AP - 웹 브라우저 취약점(Webkit) - 웹 컨텐트 - E-mail, SNS, Messenger
공격 범위	- DDoS 공격대상 서버 및 백본 네트워크망	- DDoS 공격대상 서버 및 백본 네트워크 망 - 3G/4G 네트워크 망
공격 지속성	시스템 종료 시까지 가능	- 베터리 방전 시 진행 불가 - WiFi/3G(4G) 전환시 진행 불가
공격 시 증상 및 피해	시스템에 큰 부하없이 공격 가능	- 시스템 속도 저하 및 단말기 발열 - 배터리 방전 - 3G망 이용시 과금 발생

증가했다. 이러한 스마트폰에 악성코드가 감염되어 좀비 스마트폰이 될 경우 사용자의 개인정보는 물론 스마트폰 DDoS 공격이 발생할 수 있다.

기본적으로 좀비 PC와 좀비 스마트폰은 [표 3]에서 보는바와 같이 환경이 다르다. 기존 DDoS 공격과 비슷하지만 스마트폰만이 가지고 있는 환경과 특징이 다른 추가 위협을 만들 수 있다.

3.2 공격동향

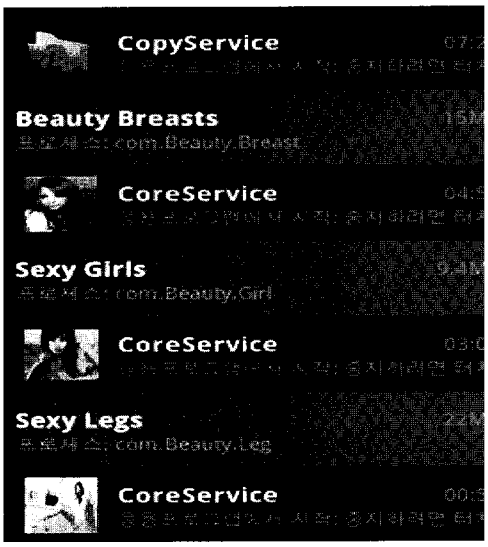
최근 스마트폰 악성코드 트렌드를 살펴보면 [그림 1]과 같이 정상적인 어플리케이션에 악성코드를 추가하여 리패키징한 후 유포하는 방식이 많으며, [그림 2]와 같이 취약점을 이용한 강제 루팅을 통해 최고 관리자 권한을 획득하는 악성코드도 등장했다. 이를 통해 개인정보를 유출하게 된다.

지난 3월에 공식 마켓을 통해 유포되는 DDLight (DroidDreamLight) 안드로이드 악성코드의 경우 Magic Photo Studio, BeeGoo, ManGoo, Mango Studio, E.T.Tean, DroidPlus, GluMobi라는 개발자 계정으로 25개 이상의 악성 앱(App)이 공식 안드로이드 마켓을 통해 유포되었다. DDLight 악성코드의 경우 다소 선전적인 앱에 리패키징하는 형태로 제작되었으며, 감염되면 [그림 4]와 같이 CoreService 서비스가 등록되며 단말기의 주요 정보가 원격 서버로 전송된다.

본 앱에 대한 정보는 AndroidManifest.xml파일에서 서비스와 리시버 정보를 확인할 수 있으며, "android.intent.action.PHONE_STATE" 인텐트(Intent)[1]를 통해 사용자가 전화를 수신하거나 발신하는 이벤트가 발생하면 CoreService 서비스가 실행되도록 구성되어 있다. DDLight 안드로이드 악성코드는 단말기 모델, 언어, 국가, IMEI, IMSI, SDK 버전 및 설치된 앱 리스트 정보를 [그림 4]와 같은 루틴을 통해 수집하고 복호화된 URL을 이용해 수집된 정보를 전송한다.

```
public boolean go4root()
{
  boolean bool1 = prepareRawFile();
  if (!bool1);
  for (boolean bool2 = bool1; ; bool2 = bool1)
  {
    return bool2;
    bool1 = runExploid();
    if (bool1)
    {
      changeWifiState();
      bool1 = install5u();
      restoreWifiState();
    }
    removeExploit();
  }
}
```

〔그림 2〕 루팅 악성코드



〔그림 3〕 DDLight 서비스 등록정보

이러한 악성코드를 통하여 좀비 스마트폰이 만들어질수 있다. 좀비 스마트폰이란 악성코드에 감염되어 해커의 명령에 의해 제어되는 스마트폰을 말하며, 개인정보 유출 및 DDoS 공격에 악용될 수 있다.

악의적인 목적으로 제작된 스마트폰용 악성코드가 사용자의 스마트폰에 감염되어 좀비 스마트폰이 된 경우, 모바일 백신의 업데이트를 방해할 수 있으며, Wi-Fi를 통한 인터넷망 DDoS 공격이 가능하다. 좀비 스마트폰을 통해 DDoS 공격이 발생할 경우 좀비 PC를 이용한 공격과 마찬가지의 피해를 일으킬 수 있으며, 위치추적이 힘들다. 배터리 소모로 인한 공격 중단이 일어날 수 있지만 통신기기의 특성상 사용자가 불편함을 느끼고 충전기를 꼽아 놓거나 예비 배터리로 교환하기 때문에 공격의 지속성이 보장될 수 있다. 또한 데이터 망에서 Wi-Fi망으로의 전환 시 공격이 중단될 수 있지만 악성코드는 망에 상관하지 않고 인터넷에만 연결되어 있

1) Activity(사용자 인터페이스 화면을 제어하는 서비스) 사이에서 호출하기 위한 시스템

```
private String b()
{
  d("<?xml version=\"1.0\" encoding=\"UTF-8\"?>\n");
  d("<Request>\n");
  switch (this.d)
  {
  default:
  case 2:
  }
  while (true)
  {
    d("</Request>");
    return this.a.toString();
    a("Protocol", "2.0");
    String str1 = String.valueOf(this.d);
    a("Command", str1);
    b("MobileInfo");
    String str2 = Build.DEVICE;
    a("Model", str2);
    String str3 = Locale.getDefault().getLanguage();
    a("Language", str3);
    String str4 = Locale.getDefault().getCountry();
    a("Country", str4);
    String str5 = "IMEI";
    Object localObject = (TelephonyManager)this.c.getSystemService("phone");
    if (((TelephonyManager)localObject).getDeviceId() == null)
    {
      localObject = "";
      label150: a(str5, (String)localObject);
      str5 = "IMSI";
      localObject = (TelephonyManager)this.c.getSystemService("phone");
      if (((TelephonyManager)localObject).getSubscriberId() != null)
        break label368;
      localObject = "";
      a(str5, (String)localObject);
      c("MobileInfo");
      b("ClientInfo");
      a("PlatformID", "5");
      StringBuilder localStringBuilder1 = new StringBuilder();
      int i = Build.VERSION.SDK_INT;
      String str6 = i;
      a("OSVersion", str6);
    }
```

〔그림 4〕 단말기 정보 수집 관련 코드

으면 공격의 지속성이 보장될 수 있다.

3G/4G망에 DDoS를 수행함으로써 다른 사용자의 서비스 이용을 방해 할 수 있다. 좀비 스마트폰이 3G데이터망에 직접적인 DDoS 공격을 시도할 경우 통신망에 마비가 올 수 있으며, 이를 통해 기존 통신 서비스 이용자는 3G 데이터 통신을 사용하지 못하는 상황이 발생할 수 있다. 또한 통신 대역에서의 DDoS 공격을 통한 리소스 고갈 등의 공격을 통해 서비스를 마비시킬 수 있다.[10]

이밖에도 좀비 스마트폰은 좀비 PC와 마찬가지로 스마트폰에 저장된 중요정보 유출이 가능하며, 내장메모리 파괴가 가능하다.

스마트폰의 기능 및 서비스가 다양해지면서, 인터넷 연결 수단, PC 동기화, SMS 메시지 등 악성코드 침입 경로 또한 다양해 졌으며[8], 대응 체계가 필요하다.

Ⅳ. 향후전망

이미 중국에선 좀비 스마트폰에 대한 좀비 악성코드가 100만대 감염된 일이 있었다.[9] 이는 충분히 좀비 스마트폰을 통해 DDoS 공격을 수행할 수 있는 가능성을 내포하고 있다.

DDoS 공격이 3G 데이터 망으로 수행될 경우 3G 데이터망 이용자들이 피해를 받을 수 있다. 머지않아 4G 서비스가 시작되어 보다 높은 대역폭과 빠른 속도를 제공하겠지만, DDoS 공격이 발생할 경우 피해를 막기는 힘들다. 데이터망 이용자들은 불편을 느끼지 못할 수 도 있지만 오히려 공격대상서버는 대량으로 들어오는 트래픽 때문에 피해가 심해질 수 있다.

웹 서비스를 대상으로 하는 공격 기법의 진화, 스위치, 방화벽 등 네트워크 시스템의 공격, 스마트폰 서비스를 포함한 주요 서비스 시스템, 데이터 통신망 등에서 발생할 수 있는 DDoS 공격을 미리 분석/파악 하고 대응방안을 수립해야 한다.

Ⅴ. 결론

스마트폰의 성능과 서비스를 제공하는 환경이 향상됨에 따라 사용자의 편리함은 보다 높아지겠지만 반대로 공격자는 이러한 환경을 이용하여 수월한 공격을 진행할 수 있게 된다. 특히 악성코드 감염 루트와 공격에 사용되는 공격 패턴 등이 다양해지고 있다.

이러한 내용을 종합해 볼 때 근시일내에 스마트폰 DDoS 공격 현실화가 가능할 것으로 보이며, DDoS 공격자는 기존의 대응방안을 우회하는 효과적인 공격방안을 모색하고 시도할 것이다.

이에 3.4 DDoS 이후 좀비 PC의 공격 및 좀비 스마트폰 DDoS 공격에 대비하여 효율적인 대응체계 구축이 필요하며, 새로운 DDoS 공격을 연구하고 대응방안을 구축해야 한다.

또한 앱 스토어에서 다운로드 받은 어플리케이션을 설치 할 때 해당 어플리케이션에 주어진 권한을 사용자가 확인하여 설치하고, 의심되는 어플리케이션을 신고하여 사고를 미연에 방지해야 할 것이다.

참고문헌

[1] http://www.datanet.co.kr/news/articleView.html ?idxno =53614

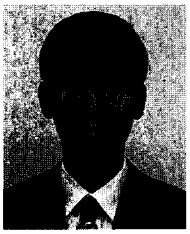
[2] 전용희, 장종수, 오진태, " DDoS공격 및 대응 기법 분류", 한국정보보호학회 학회지, 19(3), pp. 46-57, June, 2009

[3] http://www.ddaily.co.kr/news/news_view.php?u id=

78494
[4] http://www.boannews.com/media/view.asp?idx=26279&kind=1&search=title&find=DDoS
[5] http://www.computerworld.com.au/article/38511 4/new_zealand_parliament_denies_ddos_attack/
[6] 곽창규, "DDoS 공격 기법의 변화 및 전망", 금융보안연구원 이슈리포트, Mar, 2011
[7] 최상명, "좀비 스마트폰과 DDoS 공격", 하우리, Apr, 2011
[8] 장기헌, 염흥열, "스마트폰 침입 경로 및 위협 분석", 한국정보보호학회 추계학술발표대회, pp 238-244, Oct, 2010
[9] http://www.boannews.com/media/view.asp?pag e=2&idx=23591&search=key_word&find=%BE%C7%BC%BA%C4%DA%B5%E5
[10] Arun Raj Kumar, P. and S. Selvakumar, "Distributed Denial-of-Service(DDoS) Threat in Collaborative Environment A Survey on DDoS Attack Tools and Traceback Mechanisms", IEEE International Advance Computing Conference (IACC 2009), Mar, 2009
[11] http://www.gartner.com/technology/home.jsp

〈著者紹介〉

장 기 헌(Ki-Hun, JANG)
학생회원
2010년 2월 : 순천향대학교 정보보호학과 졸업
2009년 4월~2010년 5월 : (주)인포섹 모의해킹팀
2010년 9월~현재 순천향대학교 정보보호학과 석사과정
<관심분야> 정보보호, 스마트폰 보안, 네트워크 프로토콜, 역추적



최 상 명(Sang-Myung CHOI)
종신회원
2005년 8월: 순천향대학교 정보보호학과 졸업
2007년 8월: 순천향대학교 정보보호학과 석사 졸업
2007년 9월~현재 (주)하우리 선행기술팀 팀장
2011년 3월~현재 순천향대학교 정보보호학과 박사과정
<관심분야> 정보보호, 악성코드 분석, 스마트폰 보안

염 흥 열(Heung-Youl YOUM)
정회원
1981년 2월 : 한양대학교 전자공학과 학사 졸업
1983년 9월 : 한양대학교 대학원 전자공학과 석사 졸업
1990년 2월 : 한양대학교 대학원 전자공학과 박사 졸업
1982년 12월~1990년 9월 : 한국전자통신연구소 선임연구원
1990년 9월~현재 : 순천향대학교 공과대학 정보보호학과 정교수
1997년 3월~2000년 3월 : 순천향대학교 산업기술연구소 소장
2000년 4월~2006년 2월 : 순천향대학교 산학연컨소시엄센터 소장
1997년 3월~현재 : 한국정보보호학회 총무이사, 학술이사, 교육이사, 총무이사, 논문지편집위원 위원장, 수석부회장(역), 학회장(현)
2005년~2008년 : ITU-T SG17 Q.9 Rapporteur(역)
2006년 11월~2009년 2월 정보통신연구진흥원 정보보호전문위원
2009년 5월~현재 : 국정원 암호검증위원회 위원
2009년~현재 : ITU-T SG17 부의장/SG17 WP2 의장
<관심분야> 인터넷 보안, USN 보안, IPTV 보안, 홈네트워크 보안, 암호 프로토콜