스마트폰 환경에서 무선 모바일 웜 확산 방식 연구

신원*

Epidemics of Wireless Mobile Worms on Smartphones

Weon Shin*

요 약

스마트폰을 이용하여 누구나 쉽게 인터넷에 접속할 수 있는 환경이 구축됨에 따라 스마트폰을 대상으로 하는 다양한 위협도 함께 등장하고 있다. 그 중 무선 환경에서 확산되는 모바일 웜은 개인정보 탈취는 물론 무선 통신망을 뒤흔들 수 있는 위협으로 인식되고 있다. 본 논문은 무선 네트워크 환경에서 모바일 웜 확산의 모델링을 목표로 적용 가능한 모바일 웜 확산 모델을 제안하고 여러 무선 환경에서 스마트폰 모바일 웜의 확산을 시뮬레이션한다.

ABSTRACT

Now we are facing various threats as side effects against the growth of smartphone markets. Malicious codes such as mobile worms may bring about disclosures of personal information and confusions to upset a national wireless backbone. In this paper, we examine the existed spreading models and try to describe the correct spread of mobile worms on smartphones. We also analyze the spreading effects, and simulate bluetooth, MMS and Wi-Fi worms by various experiments.

키워드

모바일 웜, 스마트폰, 웜 확산, 무선 네트워크

Key word

Mobile worm, Smartphone, Worm spreading, Wireless network

* 정회원 : 동명대학교 정보보호학과 (shinweon@tu.ac.kr)

접수일자 : 2013. 01. 28
심사완료일자 : 2013. 03. 01

Open Access http://dx.doi.org/10.6109/jkiice.2013.17.5.1154

Ⅰ. 서 론

언제 어디서나 손가락만으로도 원하는 정보를 얻고, 다양한 인터넷 서비스를 활용할 수 있는 스마트폰이 등장함에 따라 예상하지 못했던 역기능들도 함께 증가하고 있다. 정상적인 어플리케이션으로 위장하여 단말 정보 및 개인정보의 유출, SMS(Short Message Service) 자동 전송을 통한 과금 유도, DDoS(Distributed Denial of Service) 공격을 위한 봇넷형 악성코드 유포도 발생하고 있다[1]. 그 중 자기 복제를 통하여 확산하여 가용성에 타격을 주기 위해 가장 효과적인 방법이 모바일 웜을 통한 공격이다.

인터넷 웜은 "독립적으로 자기복제를 실행하여 번식하는 빠른 전파력을 가진 컴퓨터 프로그램 또는 실행 가능한 코드"로 정의할 수 있는데[1], 대부분 네트워크에서 같은 취약성을 가진 다른 호스트로 자기 자신을 복제하도록 구현되어 있다. 모바일 웜은 인터넷 웜과 기본 개념은 동일하나 감염 대상이 PC가 아니라 스마트폰이라는 점과 주로 무선 네트워크를 통하여 확산된다는 점에서 인터넷 웜과 확연히 구분된다.

본 논문에서는 기존 인터넷 웜 확산 모델을 기반으로 무선 환경에서 확산하는 블루투스, MMS (Multimedia Message Service), Wi-Fi 모바일 웜을 적용하여 그 영향을 분석하고자 한다. 먼저 2장에서 기존의 웜 확산 모델을 도입하여 스마트폰 특성에 맞는 모바일 웜 확산을 검토하고, 3장에서 다양한 무선 네트워크 환경을 고려한 모바일 웜 확산 시뮬레이션을 수행한 후 마지막 4장에서 결론을 맺는다.

Ⅱ. 스마트폰을 위한 웜 확산 모델

현재 인터넷 웜에 대한 연구는 탐지 및 대응, 실행 메커니즘, 웜 확산 등이 주류를 이루고 있는데, 본 논문은 그 중 인터넷 웜 확산에 적용하기 위해 S(Susceptible), I(Infectious) 상태로 구성되는 SI 모델[2]과 S(Susceptible), I(Infectious), R(Recovered) 상태로 구성되는 SIR 모델[3]을 개선하여 스마트폰 특성을 반영한 새로운 웜 확산 모델을 도입한다.

2.1. 인터넷 웜 확산 모델의 도입

Zou 등[4]은 인터넷 웜의 스캐닝에 따른 성능을 분석하였는데, 단위시간당 균등 스캐닝을 수행하는 RCS (Random Constant Spread) Worm의 동작에서 다음 식을 유도하여 인터넷 환경의 웜 확산을 설명하였다.

$$\frac{dI(t)}{dt} = \beta I(t)[N - I(t)],\ \beta = \frac{\eta}{\Omega} \quad (1)$$

여기서, β는 웜 확산율, η는 웜의 단위 시간 당 평균 스캐닝 수, Ω는 웜이 스캐닝할 수 있는 전체 호스트 주소 공간, N은 감염가능한 전체 호스트 수, $I(t)$는 시각 t에 감염된 호스트 수를 나타낸다. 특히, RCS Worm은 호스트 주소 공간을 균등하게 스캐닝하므로 웜 확산율 β는 고정값이다.

수식 (1)에서 확산율 β가 고정된 상수값인데 반해 Two-factor Worm Model[5], 개선된 웜 확산 모델[6]에서는 웜 확산 속도 감소 정도를 반영하여 확산율 β를 시간에 따라 변화하는 함수 $\beta(t)$로 나타낸다.

$$\beta(t) = \beta_0 (1 - \frac{I(t)}{N})^{\phi} \quad (2)$$

여기서, β_0는 초기 확산율이고 ϕ는 감염 호스트 비율에 의해 변화하는 확산율을 반영하는 값이다. 수식 (1)에서 β를 함수 $\beta(t)$로 변경하고, 수식 (2)를 대입하면 다음과 같은 수식을 구성할 수 있다.

$$\frac{dI(t)}{dt} = \beta_0 (1 - \frac{I(t)}{N})^{\phi} I(t)[N - I(t)],\ \beta_0 = \frac{\eta}{\Omega} \quad (3)$$

위 식을 이용하여 2001년 7월 전세계 컴퓨터 359,000대를 감염시켰던 코드레드(Code Red) 웜의 확산을 그래프로 그린 것이 그림 1이다. 여기서, 취약한 호스트 전체 수는 $N = 359{,}000$, 확산율은 이미 알려진 $\beta = 358/2^{32}$이다. CAIDA[7]에서 제공하는 코드레드 웜의 실제 측정치가 그림 2이다. 두 그림을 비교해 보면 모델링에 의한 웜 확산과 실제 측정값이 아주 유사한 형태를 그리고 있음을 확인할 수 있다.

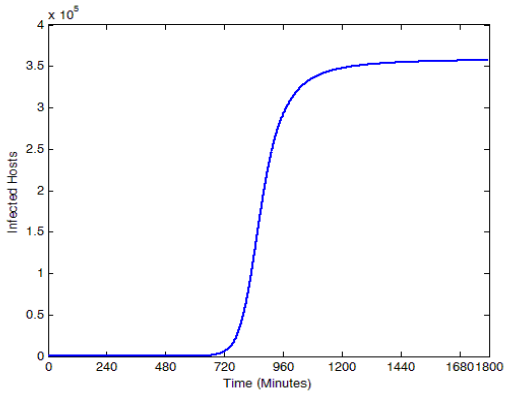

그림 1. 모델링에 의한 코드레드 웜 확산
Fig. 1 The modeling spread of Code Red worm

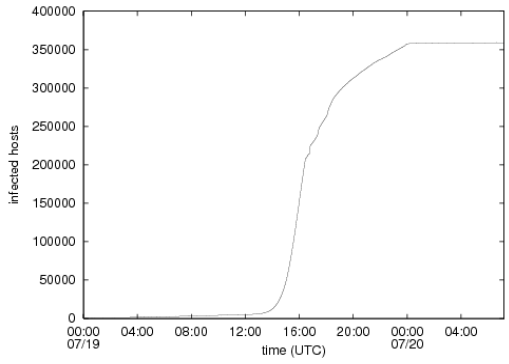

그림 2. 실제 측정에 의한 코드레드 웜 확산
Fig. 2 The spread of Code Red worm

2.2. 스마트폰 모바일 웜의 확산 특징

모바일 웜은 자신을 확산시키기 위해 취약한 대상을 찾는 과정인 스캐닝(Scanning)을 위해 대량의 패킷을 생성하도록 구현되어 있으므로, 스마트폰은 물론 무선 네트워크 자체에 오버헤드를 초래한다. 즉, 무선 네트워크 환경에서 모바일 웜의 확산은 악성 코드 확산이라는 일반적인 피해뿐만 아니라 모바일 웜에 감염된 스마트폰이 새로운 공격자가 되어 또 다른 스마트폰을 공격하는 2차적인 피해로 스마트폰을 통한 서비스 전체를 불능으로 만들 수 있다. 이러한 모바일 웜 확산의 특성은 다음과 같다.

1. 확산의 다양성 : 모바일 웜은 인터넷 웜과는 달리 다양한 통신 방식을 이용하여 확산한다. Wi-Fi망 또는 3G/LTE망을 이용하고, 블루투스를 이용하기도 한다.
2. 확산의 제한성 : 스마트폰은 PC보다 훨씬 더 다양한 운영체제가 사용되고 있고 특정 네트워크 기술을 활용하여 모바일 웜이 확산될 수 있으므로, 3G/LTE망이나 Wi-Fi 접속 유무에 따라 모바일 웜에 바로 감염되지 않을 수도 있다.
3. 확산의 비효율성 : 인터넷 웜은 고성능 PC에서 동작하므로 최대 네트워크 속도에 근접한 확산이 가능하나, 모바일 웜은 스마트폰 성능 상의 문제로 네트워크 속도보다는 스마트폰의 처리율에 따라 확산율이 결정될 수도 있다.

스마트폰을 대상으로 확산되는 모바일 웜과 기존 PC를 대상으로 확산되는 인터넷 웜의 특징을 비교하면 표 1과 같다.

Ⅲ. 웜 확산 모델의 적용

3.1. 블루투스 모바일 웜의 확산

근거리 무선 데이터 전송을 위한 블루투스(Bluetooth)[8]는 스마트폰에서 주변장치와의 통신은 물론 간단한 데이터 전송을 위해서도 많이 사용된다. 블루투스 모바

표 1. 모바일 웜과 인터넷 웜 비교
Table. 1 Comparison of mobile worm and Internet worm

분류	모바일 웜	인터넷 웜
대상	스마트폰 등 모바일 기기	PC, 노트북 등 컴퓨터
확산 경로	주로 3G/LTE망과 무선 네트워크를 활용하지만 블루투스, MMS 등도 활용	주로 유무선 네트워크이나 USB 메모리, 파일 등도 활용
성능	상대적으로 저성능	고성능
상태	항상 온라인	항상 온라인

일 웜(Bluetooth Mobile Worm)은 이러한 블루투스 통신 기능을 이용하여 확산하는 웜으로써, 수 미터 이내의 가까운 거리에 있는 두 스마트폰에 대해 애드혹(ad hoc) 방식으로 확산된다. 수도권과 같은 밀집 지역에서 블루투스 모바일 웜이 스마트폰 사이를 확산한다면, 결국 면대면 형태를 띠게 될 것이다. 스마트폰에서 블루투스를 통한 $10KB$ 크기의 모바일 웜 확산은 그림 3과 같다. 여기서, $N=10{,}000$이고 모든 스마트폰이 블루투스 기능을 켜놓았다고 가정한다. β_0는 Bulygin[9]의 값 $0.5/day$, $1.0/day$, $2.0/day$는 그대로 사용하고, 추가로 $5/day$도 사용한다. 최초 스마트폰 1대에서부터 면대면으로 감염을 시작한 웜은 하루 5대씩 확산한다면 약 10일 만에, 하루 0.5대씩 확산한다면 약 75일 만에 모든 스마트폰이 웜에 감염됨을 알 수 있다.

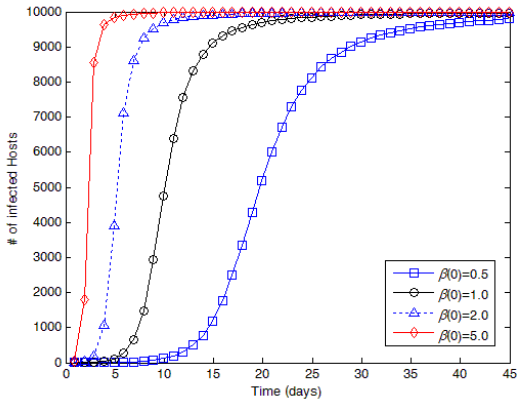

그림 3. 블루투스 모바일 웜의 확산
Fig. 3 The spread of bluetooth worm

3.2. MMS 모바일 웜의 확산

MMS[10]는 기존의 SMS를 개선하여 멀티미디어 전송을 가능하게 한 서비스로 현재는 3G 음성망을 그대로 사용한다. 국내에서 사용하는 스마트폰 전화번호 체계는 $010-abcd-wxyz$ 형태를 사용하고 있으므로 이를 활용한 모바일 웜은 010을 고정하고 나머지 8자리 전화번호를 임의로 생성한 후, 전국의 스마트폰을 대상으로 스캐닝하여 다음 대상자를 감염시킬 것으로 예상된다. 스마트폰의 MMS를 통한 $10KB$ 크기의 모바일 웜 확산은 그림 4와 같다. 여기서, $N=10{,}000$이고 $\Omega=10^8$이다, β_0는 스마트폰의 성능을 고려하여 MMS 메시지를 초당 1회 전송하는 경우와 MMS 메시지 전송을 위한 3G $144Kbps$ 업링크 및 $384Kbps$ 업링크의 경우를 실험하였다. 최초 스마트폰 1대에서부터 MMS로 감염을 시작한 웜은 $384Kbps$에서 확산한다면 약 20시간 만에, 초당 1대씩 스캐닝하여 확산한다면 약 75시간 만에 모든 스마트폰이 웜에 감염됨을 알 수 있다.

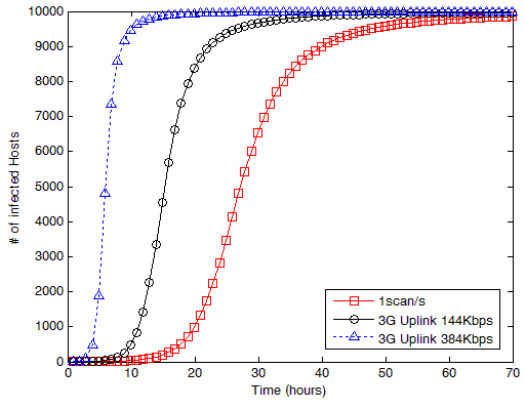

그림 4. MMS 모바일 웜의 확산
Fig. 4 The spread of MMS worm

3.3. Wi-Fi 모바일 웜의 확산

최신 스마트폰은 대부분 무선 네크워크 접속을 위한 Wi-Fi[11] 기능을 가지고 있으며, 이를 통하여 저렴한 비용으로 인터넷 접속, 각종 어플리케이션 설치, 파일 송수신 등을 수행한다. Wi-Fi 모바일 웜은 이를 이용한 웜으로써 IP 주소를 기반으로 취약한 스마트폰을 스캐닝하여 다음 대상자를 감염시킨다. 현재 국내에서 서비스되고 있는 Wi-Fi 망은 802.11b, 802.11g가 대부분이며 802.11n을 사용하기도 한다. 스마트폰의 Wi-Fi 접속을 통한 $10KB$ 크기의 모바일 웜 확산은 그림 5와 같다. 여기서, $N=10{,}000$이고 $\Omega=2^{32}$이다. Wi-Fi 환경에서 국내 3사 평균 속도 $12.6Mbps$, 실제 측정 데이터 전송속도 $15.5Mbps$와 $26.3Mbps$, Wi-Fi 802.11g 최대 속도 $54.0Mbps$의 경우를 실험하였다. 최초 스마트폰 1대에서부터 Wi-Fi로 감염을 시작한 웜은 이론적인 최대 속도에서 확산한다면 약 6시간 만에, 3사 평균 속도에서 확산한다면 약 22시간 만에 모든 스마트폰이 웜에 감염됨을 알 수 있다.

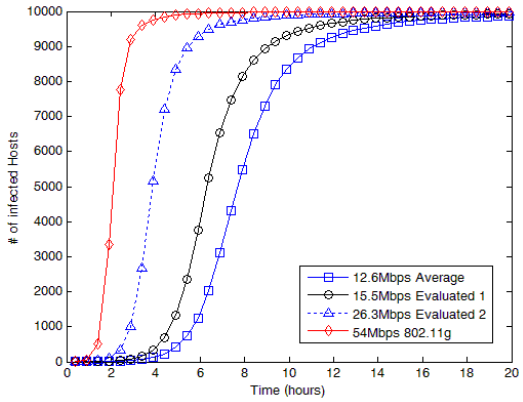

그림 5. Wi-Fi 모바일 웜의 확산
Fig. 5 The spread of Wi-Fi worm

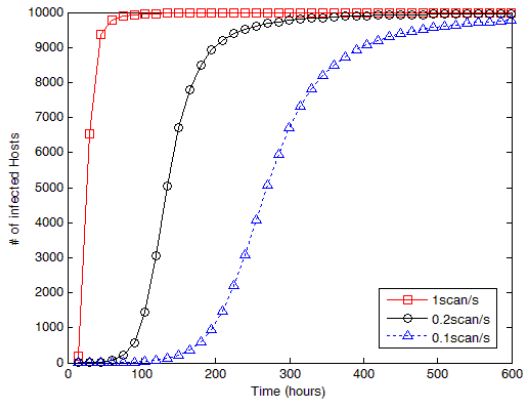

그림 6. 스캐닝에 따른 MMS 모바일 웜의 확산
Fig. 6 The spread of MMS worm by scanning rate

3.4. 각 모바일 웜의 확산 방식 분석

블루투스 모바일 웜의 확산은 얼마나 많은 수의 스마트폰이 블루투스의 유효거리 내에 들어오는가 하는 것이다. 전송속도와 모바일 웜의 크기와는 큰 관련이 없고, 웜 확산은 감염된 스마트폰을 휴대한 사람이 블루투스가 켜진 스마트폰을 휴대한 다른 사람을 얼마나 만나느냐에 의존한다.

MMS 모바일 웜의 확산은 단위 시간 내에 MMS 메시지를 얼마나 많은 스마트폰에 전송하느냐에 좌우한다. 웜 확산은 전송속도와 모바일 웜의 크기에도 영향을 받지만, 스마트폰의 성능에 가장 큰 영향을 받는다. 그림 6은 그림 4와 동일 조건 하에서 스마트폰의 성능을 고려하여 초당 MMS 전송 횟수를 $0.1scan/s$, $0.2scan/s$, $1scan/s$로 변화한 확산이다.

Wi-Fi 모바일 웜의 확산에서 스마트폰의 성능을 고려하지 않는다면, 무선 네트워크 속도, 모바일 웜 크기, 최초 감염자 수의 순으로 영향을 끼친다. 즉, 웜 확산은 스마트폰의 성능이 높아짐에 따라 무선 네트워크의 대역폭을 더 효율적으로 사용할 수 있을 것이며, 향후 PC에서 인터넷 웜의 확산 양상과 유사해질 것으로 예상된다.

그림 7은 그림 5와 동일 조건 하에서 최초 감염자 수($i(0)=1, 3$), 모바일 웜 크기($s=10KB, 30KB$), 무선 네트워크 속도($12.6Mbps, 37.8Mbps$)를 각각 변화시켜 살펴본 웜 확산이다.

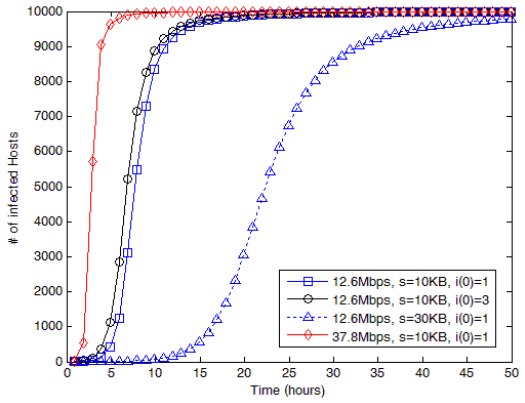

그림 7. 여러 조건에 따른 Wi-Fi 모바일 웜의 확산
Fig. 7 The spread of Wi-Fi worm by various factors

MMS 모바일 웜과 Wi-Fi 모바일 웜 확산에서 살펴보면, MMS 모바일 웜은 국내 스마트폰 8자리 전화번호 체계를 활용($\Omega=10^8$)함으로써 취약한 스마트폰을 효율적으로 스캐닝할 수 있으나 번호체계가 국가마다 다르므로 지역성을 띨 수밖에 없다. Wi-Fi 모바일 웜은 인터넷 주소체계를 사용($\Omega=2^{32}$)하여 대규모의 주소를 스캐닝해야 하지만, 지역성에 관계없이 IP 주소를 기반으로 확산할 수 있는 특징을 가진다. 그림 8은 MMS 모바일 웜의 전송속도($1scan/s$, $2scan/s$)와 Wi-Fi 모바일 웜의 무선 네트워크 속도($12.6Mbps, 25.2Mbps$)만을 변화하여 살펴본 웜 확산이다.

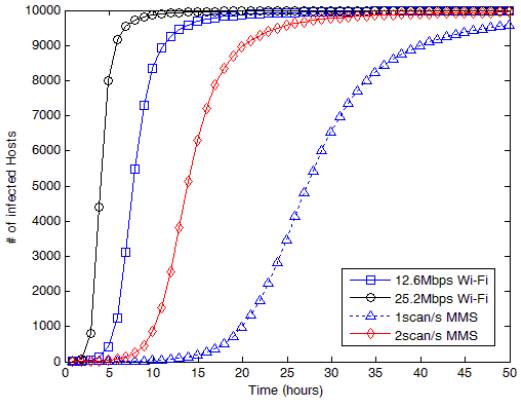

그림 8. MMS 모바일 웜과 Wi-Fi 모바일 웜 확산
Fig. 8 The spread of MMS Worm and Wi-Fi worm

Ⅳ. 결 론

일반 PC의 취약점을 이용하여 확산되던 인터넷 웜은 인터넷 하부구조를 공격하는 가장 큰 위협 중 하나였으나, 컴퓨팅 환경의 변화에 따라 스마트폰을 대상으로 하는 모바일 웜으로 변모하고 있다. 이러한 모바일 웜의 확산은 해당 스마트폰의 정상적인 동작을 방해할 뿐만 아니라 무선 인터넷 서비스의 신뢰성에 심각한 타격을 줄 수 있다. 본 논문에서는 현재 문제가 되고 있고, 향후 더 큰 문제를 야기할 것으로 보이는 모바일 웜의 확산을 예측하고, 각종 무선 네트워크 환경에 따른 요인을 고려하여 실험한 후 그 영향을 분석하였다. 본 논문의 결과는 무선 네트워크의 고속화와 스마트폰의 고성능화에 따른 모바일 웜 확산의 대응 방안을 마련하는데 활용할 수 있을 것이다. 이를 기반으로 향후 LTE(Long Term Evolution) 등 신기술과 유무선 통합망의 네트워크 구조에 따른 웜 확산 모델링에 대한 연구와 서로 이질적인 네트워크 환경에서 모바일 웜 확산에 대한 연구도 진행될 수 있을 것으로 예상한다.

참고문헌

[1] “인터넷침해사고 동향 및 분석월보”, 한국인터넷진흥원, 2012

[2] H. W. Hethcote, “The Mathematics of Infectious Diseases”, SIAM Review, Vol. 42, No. 4, 2000

[3] James D. Murray, “Mathematical Biology”, Springer-Verlag, 1993

[4] Cliff C. Zou, Don Towsley, Weibo Gong, ″On the Performance of Internet Worm Scanning Strategies″, Elsevier Journal of Performance Evaluation, vol. 63, no. 7, pp. 700-723, 2006

[5] Cliff C. Zou, Weibo Gong, Don Towsley. “Code Red Worm Propagation Modeling and Analysis”, 9th ACM Conference on Computer and Communication Security (CCS’02), 2002

[6] 신원, 이경현, “인터넷 환경에서 웜 확산 모델의 제안과 분석”, 한국정보보호학회논문지, Vol.16 No.3, pp. 165-172, 2006

[7] “The Spread of the Sapphire/Slammer Worm”, http://www.caida.org/outreach/papers/2003/sapphire/sapphire.html

[8] Bluetooth, http://en.wikipedia.org/wiki/Bluetooth

[9] Y. Bulygin, “Epidemics of Mobile Worms”, Performance, Computing, and Communications Conference, 2007. pp.475-478, 2007

[10] Multimedia Messaging Service, http://en.wikipedia.org/wiki/Multimedia_Messaging_Service

[11] Wi-Fi, http://en.wikipedia.org/wiki/Wi-Fi

[12] P. Wang, M. Gonzalez, C. A. Hidalgo, A.-L. Barabasi, “Understanding the spreading patterns of mobile phone viruses”, Science 324, pp. 1071-1076, 2009

저자소개

신원(Shin, Weon)

2005.3～현재 동명대학교 정보보호학과 전임강사, 조교수, 부교수
2002.3～2005.1 (주)안철수연구소 선임연구원

※관심분야 : 소프트웨어 보안, 악성코드 확산, 디지털 포렌식