http://www.calsec.or.kr/jsebs
ISSN: 2288-3908

The Journal of Society for e-Business Studies
Vol.19, No.4, Nov 2014, pp.31-43
http://dx.doi.org/10.7838/jsebs.2014.19.4.031

S/W 취약점으로 인한 손실비용 추정

Estimating Economic Loss by S/W Vulnerability

김민정(Min-jeong Kim)*, 유진호(Jinho Yoo)**

초 록

최근 많은 사이버 공격은 S/W의 취약점을 이용한 익스플로잇(exploit)으로 이루어지고 있다. 주기적으로 취약점 동향이 발표되고 있으며 이를 참고로 보안의 방향이 제시되고 개선 방안도 수정되고 있다. 그럼에도 불구하고 2011년 한 해 동안 발생한 해킹 등 사이버 공격은 2010년 대비 81% 증가하였고, 이러한 사이버 공격의 약 75%가 S/W 자체의 보안 취약점을 악용하고 있다. 본 논문에서는 S/W 취약점으로 인한 손실비용 측정을 위해 질병 전파 모델인 SIR 모델을 응용하여 취약점에 의한 악성코드 감염 확산 모델인 VIR모델을 제시하고, 이를 훈글 S/W 취약점에 적용하여 손실비용이 어느 정도인지를 추정하였다.

ABSTRACT

These days a lot of cyber attacks are exploiting the vulnerabilities of S/W. According to the trend of vulnerabilities is announced periodically, security directions are suggested and security controls are updated with this trend. Nevertheless, cyber attacks like hacking during the year 2011 are increased by 81% compared to 2010. About 75% of these cyber attacks are exploiting the vulnerabilities of S/W itself. In this paper, we have suggested a VIR model, which is a spread model of malware infection for measuring economic loss by S/W vulnerability, by applying the SIR model which is a epidemic model. It is applied to estimate economic loss by HWP(Hangul word) S/W vulnerabilities.

키워드 : S/W 취약점, 손실비용, SIR 모델, VIR 모델
S/W Vulnerability, Economic Loss, SIR, VIR

본 연구는 2014년도 상명대학교 교내연구비를 지원받아 수행하였음.

* First Author, Dept. of Information Security Management, Sangmyung University(korea.minjeong@gmail.com)
** Corresponding Author, Dept. of Business Administration, Sangmyung University(jhyoo@smu.ac.kr)

2014년 07월 16일 접수, 2014년 09월 01일 심사완료 후 2014년 09월 23일 게재확정.

1. 서 론

주기적으로 'OWASP의 보안 위협 Top 10', 'SANS TOP 20 보안리스트' 등 다양한 취약점 동향이 발표되고 있다. 국내에서는 2005년부터 국가사이버안전센터에서 '보안 취약점 8종'을 발표하고 있다. 이를 참고로 보안의 방향이 제시되고 있고 개선 방안도 수정되고 있다. 그럼에도 불구하고 취약점에 의한 공격은 증가하고 있다. 2012년 행정안전부에 따르면 2011년 한 해 동안 발생한 해킹 등 사이버 공격은 55억 건으로 2010년 대비 81% 증가하였다. 특히 최근의 사이버 공격은 침입차단 시스템 등 보안장비를 우회하거나, 보안패치가 발표되기 이전의 보안 취약점을 악용하는 제로데이 공격, 웹사이트 해킹 등이 상당 부분을 차지하고 있다[10]. 특정 S/W의 보안 취약점을 대상으로 지능화된 기법을 이용하여 지속적으로 공격하는 APT(Advance Persistent Threat)공격 또한 전 방위적으로 확산되는 추세이며, 사이버 공격의 약 75%가 S/W 자체의 보안 취약점을 악용하여 진행되고 있다[10].

〈Table 1〉 OWASP Top 10(2013)

A1 – Injection
A2 – Broken Authentication and Session Management
A3 – Cross Site Scripting(XSS)
A4 – Insecure Direct Object References
A5 – Security Misconfiguration
A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control
A8 – Cross Site Request Forgery(CSRF)
A9 – Using Known Vulnerable Components
A10 – Unvalidated Redirects and Forwards

NIST의 연구 결과에 따르면 사이버 공격을 선제적으로 예방 및 대응하기 위해서는 제품 출시 이전 단계인 S/W 개발단계에서 보안 취약점을 제거하는 것이 가장 효과적이다[11]. S/W 설계단계에서 제품출시까지 오류·취약점 등 결함을 제거하는 시점에 따른 비용 차이를 분석한 결과, 보안 취약점 제거 비용이 최대 30배까지 차이가 발생할 수 있는 것으로 나타났다. 또한 S/W의 유지비용은 S/W 비용의 10~15% 정도로 측정한다[15]는 연구 결과도 있어 개발단계에서 보안 취약점을 제거하지 않으면 S/W의 유지비용이 상당할 것으로 보인다.

취약점에 의한 공격에 대비하여 S/W회사에서는 취약점 패치를 꾸준히 하고 있으며, 마이크로소프트(MS), 구글(Google), 어베스트(Avast), 페이스북(Facebook) 등 주요 기업뿐만 아니라 한국인터넷진흥원(KISA)에서도 취약점 포상제도를 실시하고 있다. 또한 KISA는 무료 원격 웹 취약점 점검 서비스도 실시하고 있다.

취약점에 대한 패치가 이루어지지 않았을 경우에는 취약점을 악용한 제로데이 공격, APT 공격 등이 발생 할 수 있으며, 이로 인해 사이버테러 공격뿐만 아니라 개인정보유출이나 산업기밀유출 등의 사고로 이어지고 있는 것이 지금의 현실이다.

본 논문에서는 이러한 취약점으로 인한 손실을 추정하는 방법으로 질병 전파 모델인 SIR 모델을 응용하는 방안을 제시하고자 한다.

2. 관련 연구

소프트웨어 취약점(Software Vulnerability)이란, 일반적으로 소프트웨어 개발자가 개발

또는 유지보수 단계에서 의도하지 않은 형태로 사용되어 보안문제가 발생하는 경우를 말한다[9]. 취약점은 소프트웨어의 약점으로서, 소프트웨어 또는 이 소프트웨어가 처리하는 데이터의 무결성, 가용성, 또는 기밀성을 약화시키는 빌미를 해커에게 제공하게 된다. 취약성이 매우 큰 경우에 해커는 수중에 들어온 컴퓨터를 악용하여 사용자 몰래 임의 코드를 실행시킬 수도 있다[13, 16].

이러한 소프트웨어의 결함이나 시스템 설계상의 허점 또는 취약점이 공격자에 의해 악용되어 정보유출, 악성코드 유포 등 해킹사고를 유발하게 되는 것이다. 마이크로소프트의 보고서[9]에 따르면 전 세계 국가의 평균 악성코드 감염률과 비교하여 한국은 터키에 이어 두 번째로 높은 감염률을 보이고 있다.

전 세계 소프트웨어 업계 전반에 걸쳐 높은 심각도의 취약점(High)은 2013년 상반기에 비해 하반기에 조금 감소하였으며, 중간 심각도의 취약점(Medium)은 2013년 상반기에 비해 하반기에 상당히 증가하여 전체 59.3%를 차지하였다. 낮은 심각도의 취약점(Low)은 2013년 상반기와 하반기의 차이가 거의 없었다. 즉, 전체 취약점은 증가하였고 특히 중간 심각도의 취약점이 크게 증가하고 있는 것으로 나타났다[8].

컴퓨터 S/W에도 취약점이 있는 것처럼 우리 몸에도 취약한 부분이 있다. 특히 질병전파 모델이 컴퓨터 바이러스 전파 형태와 유사하며 이와 관련된 연구들이 많이 있다. 영국의 하머(W.H. Hamer)는 홍역의 유행에 관한 모델인 SI(Suspectible, Infectious)모델을 제시하였고, 로날드 로스(Ronald Ross)는 말라리아를 옮기는 기생충과 확산모델을 제시하였다. 이후 윌리엄 컬맥(William Kermack)과 앤더슨 맥켄드릭(Anderson McKendric)은 전염병이 유행하기 위한 초기 조건과 확산 정도를 예측하는 SIR(Suspectible, Infectious, Removed) 모델을 제시하였다[12].

이상구 외[12]는 SIR 기본모델에서 잠재기(Exposed)를 고려한 SEIR 모델을 활용하여 신종 인플루엔자의 확산에 대한 수학적 모델링을 하였다. 이때 S는 감염대상군, E는 잠재기, I는 감염군, R은 회복군이다.

Chen[1]에 따르면 SIS(Suspectible, Infectious, Suspectible)모델은 SI의 확장 모델로 감염된 후 치료된 노드가 재감염되는 경우를 고려한 모델이다.

질병 전파 모델을 웜, 바이러스 전파에 적용한 연구는 다음과 같다. 임재명, 윤종호[4]는 웜 공격과정에 대한 개선된 NS-2 통신망 시뮬레이션 모델인 AN-AN 모델을 구현하기 위하여 SIR 모델을 이용하였다. SIR 모델을 반영하여 DN-AN 모델에서 구현된 Message-Passing 에이전트와 Worm.tcl 프로그램을 수정한 시뮬레이터를 구현하였다.

Chen et al.[2]은 다른 감염 전파모델에서 보안패치 등 환경적인 요소를 고려하지 않는 등의 단점을 보완하기 위해 랜덤스캐닝 기법을 사용하여 전파되는 웜에 적용할 수 있는 AAWP(Analytical Active Worm Propagation) 모델을 제시하였다.

Zou et al.[17]은 code red worm의 확산을 분석하기 위해 기존의 감염 전파 모델에서 포함되지 않았던 사용자의 대응 활동과 트래픽 대량 발생으로 인한 과부하 및 처리 불능 등 두 개의 요소를 고려하여 Two factor worm model을 제시하였다.

한국정보보호진흥원[7]에서도 웜 바이러스의 전파 특성을 이해하기 위해 웜 전파 모델에 전염병 감염 모델을 적용하였다. 이러한 모델들은 주로 전파 속도, 전파 범위 등 전파되는 행위 자체에 포커스를 맞추고 있다.

본 논문에서는 질병 전파 모델을 응용하여 취약점으로 인한 경제적 손실을 측정하는 데 활용하는 방안을 제시하고자 한다.

3. 질병전파모델(SIR)과 악성코드 감염확산모델(VIR)의 비교

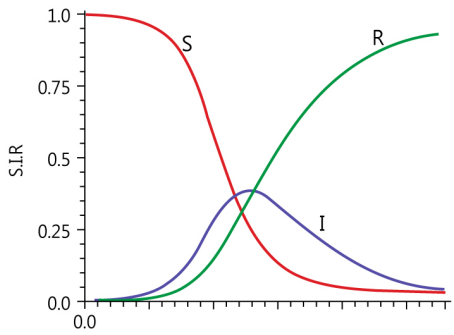
질병전파모델 중 하나인 SIR(Susceptible, Infectious, Removed)모델은 구성원을 Susceptible, Infectious, Removed의 세 가지 상태로 구분한다. Susceptible(감염대상군)은 전염되지 않았고 전염될 수 있는 상태의 비율이며, Infectious(감염군)는 전염되었고 다른 이를 전염시킬 수 있는 상태의 비율이고, Removed(회복군)는 전염 후 회복되었고 다시 전염되지 않는 상태의 비율이다[6, 14]. 이 모델의 상태는 다음과 같이 구분한다.

$$S \xrightarrow{\rho} I \xrightarrow{\alpha} R$$

ρ : rate of infection, α : recovery rate

S+I+R = 1

이때 감염된 개인의 접촉에 의한 질병 확산을 고려해야 하며, 개인이 질병에서 회복하고 내성을 얻을 수 있음을 고려해야 한다. Susceptible(감염대상군), Infectious(감염군), Removed(회복군)의 관계는 <Figure 1>와 같다.



〈Figure 1〉 Relation of S, I, R

여기에서 기본 번식 수(basic reproduction number)는

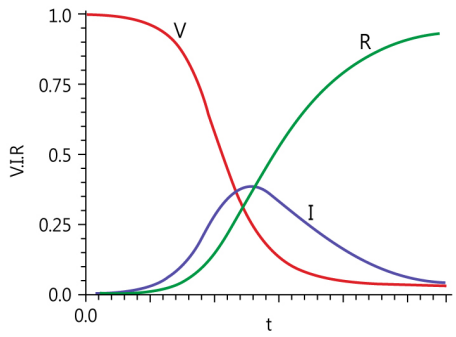
$$N_R = (\rho/\alpha) \qquad (1)$$

로 정의된다. 이 수는 전염 가능한 전체 인구에서 하나의 전염의 영향으로 인해 전염되는 숫자의 평균을 나타낸다. 이때 ρ는 전염된 비율이고, α는 제거된 비율이다. 예를 들어 천연두의 N_R은 3~5, 홍역의 N_R은 16~18, 말라리아의 N_R은 100 이상이다. N_R이 크면 감염률과 파급력이 크다는 것을 의미한다. N_R이 3~5로 작은 천연두는 백신 미접종 시 치사율 20~40%이며, N_R이 100 이상인 말라리아는 50~80%의 치사율을 갖고 있다.

SIR 모델을 악성코드 감염으로 응용하면 다음과 같이 정의할 수 있다. S/W 결함이나 시스템 설계 상의 취약점을 통해 악성코드에 감염될 수 있으며, 취약점이 공격자에 의해 악용되어 정보유출, 악성코드 유포 등 사고를 유발시키고, 패치를 통해 PC나 서버가 악성코드 감염에서 회복되는 것처럼 이를 SIR 모델과 마찬가지로 Vulnerable(취약군), Infectious(감염군), Recovered(회복군)의 세 가지 상태로 구분할 수 있다. 이때 S/W 취약점에 삽입된 악성코드에 의해 감염·확산되고, 이후 취약점

패치를 통해 PC가 악성코드 감염에서 회복되어 내성을 얻을 수 있음을 가정하여 고려하였다.

본 논문에서는 취약점에 의한 악성코드 감염 확산 모델인 VIR(Vulnerable, Infectious, Recovered)모델을 제시하고자 한다. Vulnerable(취약군)은 SIR 모델에서의 Susceptible (감염대상군)를 의미한다. 즉, 악성코드에 감염되지 않았으나 감염될 수 있는 상태로서 S/W에 취약점이 존재하는 상태를 말한다. Infectious (감염군)는 악성코드에 감염되었고 다른 PC나 서버를 감염시킬 수 있는 상태의 비율로 취약점에 의해 S/W에 악성코드가 삽입되었고 이로 인해 PC혹은 서버가 감염 될 수 있는 상태이다. Recovered(회복군)는 SIR 모델에서의 Removed(회복군)을 의미하며 악성코드에 감염 후 패치 되었고 다시 감염되지 않는 상태의 비율로 취약점을 패치하여 같은 취약점에 의해서는 다시 감염되지 않는 상태를 말한다.



〈Figure 2〉 Relation of V, I, R

시간 t에 따른 V, I, R의 변화를 나타내는 그래프는 SIR 모델의 그래프와 비슷한 형태로 나타날 것으로 추정한다. 이 모델의 상태 흐름도 다음과 같이 표현할 수 있다.

$$V \xrightarrow{\rho} I \xrightarrow{\alpha} R$$

ρ : rate of infection, α : recovery rate

V+I+R = 1

이때 기본 감염 수는 마찬가지로

$$N_R = (\rho/\alpha) \qquad (2)$$

로 나타낼 수 있으며, 여기서 ρ는 취약점에 의해 악성코드에 감염된 비율로 악성코드 감염률이고 α는 패치를 통해 취약점이 제거된 비율로 패치율이다. <Table 2>는 SIR 모델과 VIR 모델을 비교한 표이다.

4. 모델 적용 및 손실비용 추정

본 논문에서는 다음의 상황에 대해 VIR 모델을 적용하여, S/W 취약점으로 발생할 수 있는 경제적 손실비용을 추정하고자 한다.

〈Table 2〉 Comparison with SIR and VIR

	Epidemic	Malware	
N(Total)	the number of person	the numper of PC or server	N(Total)
S	rate of susceptible person	rate of vulnerable PC or server	V
I	rate of infected person	rate of infected PC or server	I
R	rate of recovered person	rate of recovered PC or server	R

국내 '한글 S/W'에 존재하는 취약점 중 KISA의 신규 취약점 신고제로 '**임의코드 실행 취약점**'이 발견되었고, 이를 보완한 최신버전으로 업데이트를 하여 보안조치 하였다.

VIR 모델 적용을 위해서는 몇 가지 전제조건이 필요하다. 우선 악성코드의 감염 대상인 국내에 있는 모든 PC의 수를 알아야 한다. 그리고 취약점이 발견되는 S/W들에 대한 악성코드 감염 비율을 파악하거나 취약점에 의해 악성코드에 감염된 PC의 수도 알아야 한다. 마지막으로 취약점이 발견된 S/W의 패치율 혹은 패치에 의해 복구된 PC의 수 등을 파악해야 한다.

손실 비용 측정 식은 다음과 같이 정의할 수 있다.

$$Loss = N \times (I-R) \times Value \times Weight$$

N : The number of total PC or server
I : rate of infection
R : rate of patch(recovered)
Value : value of PC or server
Weight : Weight of influence on vulnerability

위의 한글 S/W 상황에 대한 경제적 손실을 계산하기 위해 다음과 같이 파라미터 값을 추정하여 사용하였다. 국내 PC의 수(Total)는 23,000천여 대이다. 이는 미래에셋증권의 보고서 중 IDC의 자료 인용을 참고로 하여 추정하였다[5].

취약한 PC(Vulnerable)는 한글을 사용하는 PC의 비율이며

$$20,000천대/23,000천대 = 0.87 \quad (3)$$

로 87%이다. 이는 2009년 기준 한글 이용자가 2천만 명 수준으로 추산되었다는 보도 자료를 이용하였다[3].

감염된 PC(Infectious)는 한글의 취약점에 의해 악성코드가 삽입되어 감염된 PC의 비율로 추정할 수 있다. 악성코드에 의해 감염된 비율은 마이크로소프트의 보고서[8] 중 악성코드의 기본적인 감염률은 1,000대중 약 11.7대인 1.17%라는 결과가 있다. 본 논문에서는 이 값을 악성코드 감염률로 사용하고자 한다. 이 값을 국내 PC 수인 23,000천대에 적용하면 약 269,100대의 PC가 기본적으로 악성코드에 감염된다는 것을 알 수 있다.

패치 된 PC(Recovered)는 악성코드로 인해 감염된 PC중 보안 업데이트로 인해 패치 되어 회복된 PC의 비율이다. 이를 추정하기 위한 방안으로 한컴 회사의 홈페이지에 있는 패치의 업데이트 다운로드 수를 사용하였다. 해당 홈페이지에는 한글 관련 S/W 패치의 업데이트가 2010년 2월부터 2014년 5월까지 게시되어 있다. 특정한 하나의 패치에 대한 일자별 다운로드 건수를 확인 할 수 없어 정확한 추정을 하기에는 부족하기 때문에 본 논문에서는 한글 S/W 취약점 패치에 대한 평균 다운로드 건수를 계산하여 이를 패치율 값의 추정에 활용하고자 한다.

<Table 3>은 한컴 사의 S/W patch 다운로드 내용이다. 여기에는 한글뿐만 아니라 한컴 오피스 파일도 포함되어 있기 때문에 <Table 4>에 한글 S/W와 직접적으로 관련 있는 다운로드 건수만 별도로 선별하여 패치율 추정에 활용하였다.

〈Table 3〉 Hancom Patch Download List(2014. 7. 6)

Date	Hancom patch file	Hits	Download	Total Download
2010 02.01	Han/Word 2002 SE bundle patch file(Han/Word V3030)	52866	20586	32516
	Han/Word 97 to reinforce 2000 May patch	14309	5010	
	Hancom Nexcel 2005 patch for all users(Nexcel V6.7.5.333)	6572	2348	
	Hancom Slide 2005 update file(Slide V6.7.5.634)	2593	765	
	Hancom Office 2005_Hancom Nexcel 2005 patch for all users(Nexcel V6.7.7.333)	6957	2708	
	Hancom Office 2005_Hancom Slide 2005 update file(Slide V6.7.6.634)	4020	1099	
2010 03.02	Wordian for user Han/Word 2002 update file(all)-230MB	23530	8514	12989
	Hancom Note V1.5-(2003. 1. 14 reviced)	14076	4475	
2010 05.20	Han/Word PDF Converter 9.0 upgrade file	27613	6097	6097
2010 12.17	Hancom Slide 2007 update file(Slide .5.12.865)_win98, win2000 for users	16117	6235	11761
	Hancom Nexcel 2007 update file(Nexcel 7.5.12.726)_win98, win2000 for users	15693	5526	
2011 06.14	Hancom Office 2010 SE IME patch file	23334	6054	6054
2012 06.22	Hancom Han/Word 2007 update file(Han/Word 7.5.12.631)_win98, win2000 for users	12868	2047	25922
	Hancom Office 2005, Han/Word 2005 update file(Han/Word 6.7.10.1074)_win98, win2000 for users	6037	834	
	Han/Word 2004 update file(Han/Word 6.0.5.773)_win98, win2000 for users	2049	316	
	Han/Word 2002SE update file(Han/Word V5.7.9.3055)_win98, win2000 for users	3864	689	
	Hancom Office 2007 update file(Han/Word 7.5.12.631 etc.)_win98, win2000 for users	24568	22036	
2012 07.03	Hancom Office 2010 SE+ update file(Han/Word8.5.8.1256 etc.)_win98, win2000 for users	26843	22775	37988
	Hancom Office Han/Word 2010SE+Update file(Han/Word 8.5.8.1256)_win98, win2000 for users	12919	10751	
	Hancom Office Han/Cell 2010 SE+ update file(Han/Cell 8.5.8.1213)_win98, win2000 for users	4146	2223	
	Hancom Office Han/Show 2010 SE+ update file(Han/Show 8.5.8.1341)_win98, win2000 for users	2366	2239	
2012 09.21	Hancom Office 2010 ESD automatic update patch file download	21311	11225	11225
2014 05.27	Han/Word 2002SE update file(Han/Word 5.7.9.3079)	1123	1594	96814
	Han/Word 2004 update file(Han/Word 6.0.5.805)	374	416	
	Hancom Office 2005_Han/Word 2005, Han/Word 2005 update file (Han/Word 6.7.10.1107)	2407	2656	
	Hancom Slide 2007 update file(Slide 7.5.12.900)	556	585	
	Hancom Nexcel 2007 update file(Nexce l7.5.12.757)	661	727	
	Hancom Han/Word 2007 update file(Han/Word 7.5.12.699)	14741	18859	
	Hancom Office 2007 update file(Han/Word 7.5.12.699 etc.)	8720	8976	
	Hancom Office Han/Show 2010 SE+ update file(Han/Show 8.5.8.1480)	1485	1617	
	Hancom Office Han/Cell 2010 SE+ update file(Han/Cell 8.5.8.1336)	1284	1483	
	Hancom Office Han/Word 2010 SE+ update file(Han/Word 8.5.8.1422)	11595	15700	
	Hancom Office 2010 SE+ update file(Han/Word 8.5.8.1422 etc.)	16552	23636	
	Hancom Office Han/Word 2014 update file(Han/Word 9.0.0.1397)	4225	4212	
	Hancom Office 2014 update file(Han/Word 9.0.0.1397 etc.)	14423	16353	

〈Table 4〉 Hanword Patch Download List(2014. 7. 6)

Date	Hancom patch file	Download	Rate of patch($\hat{p}$)
2010 02.01	Han/Word 2002 SE bundle patch file(Han/Word V3030)	20586	0.08797
	Han/Word 97 to reinforce 2000 May patch	5010	0.02141
	Hancom Nexcel 2005 patch for all users(Nexcel V6.7.5.333)	2348	0.01003
	Hancom Slide 2005 update file(Slide V6.7.5.634)	765	0.00327
2010 03.02	Wordian for user Han/Word 2002 update file(all)-230MB	8514	0.03638
2010 05.20	Han/Word PDF Converter 9.0 upgrade file	6097	0.02606
2010 12.17	Hancom Slide 2007 update file(Slide .5.12.865)_win98, win2000 for users	6235	0.02665
	Hancom Nexcel 2007 update file(Nexcel 7.5.12.726)_win98, win2000 for users	5526	0.02362
2012 06.22	Hancom Han/Word 2007 update file(Han/Word 7.5.12.631)_win98, win2000 for users	2047	0.00875
	Hancom Office 2005, Han/Word 2005 update file(Han/Word 6.7.10.1074)_win98, win2000 for users	834	0.00356
	Han/Word 2004 update file(Han/Word 6.0.5.773)_win98, win2000 for users	316	0.00135
	Han/Word 2002SE update file(Han/Word V5.7.9.3055)_win98, win2000 for users	689	0.00294
	Hancom Office 2007 update file(Han/Word 7.5.12.631 etc.)_win98, win2000 for users	22036	0.09417
2012 07.03	Hancom Office Han/Word 2010SE+Update file(Han/Word8.5.8.1256)_win98, win2000 for users	10751	0.04594
2014 05.27	Han/Word 2002SE update file(Han/Word 5.7.9.3079)	1594	0.00681
	Han/Word 2004 update file(Han/Word 6.0.5.805)	416	0.00178
	Hancom Office 2005_Han/Word 2005, Han/Word 2005 update file(Han/Word 6.7.10.1107)	2656	0.01135
	Hancom Slide 2007 update file(Slide 7.5.12.900)	585	0.00250
	Hancom Nexcel 2007 update file(Nexce l7.5.12.757)	727	0.00311
	Hancom Han/Word 2007 update file(Han/Word 7.5.12.699)	18859	0.08059
	Hancom Office 2007 update file(Han/Word 7.5.12.699 etc.)	8976	0.03836
	Hancom Office Han/Word 2010 SE+ update file(Han/Word 8.5.8.1422)	15700	0.06709
	Hancom Office 2010 SE+ update file(Han/Word 8.5.8.1422 etc.)	23636	0.10101
	Hancom Office Han/Word 2014 update file(Han/Word 9.0.0.1397)	4212	0.01800
	Hancom Office 2014 update file(Han/Word 9.0.0.1397 etc.)	16353	0.06988
Average		7418.72	0.03170

패치율은 한글을 사용하며 악성코드에 감염된 PC의 수 대비 평균 패치 다운로드 수의 비율로 계산하였다. 이때 혼글 S/W를 사용하면서 패치를 적용하지 않아 악성코드에 감염된 PC의 수는 20,000천대 × 1.17%(기본 악성코드 감염률) = 234,000대 이다.

2010년 2월 게시된 패치에 대해 2014년 6월까지 하나의 패치에 대해 평균 7,419건의 패치가 이루어 진 것을 알 수 있다. 따라서 평균패치율은

$$\frac{7419\text{건}}{234\text{천대}} = 0.03170 \fallingdotseq 3.17\% \quad (3)$$

이다.

〈Table 5〉 Parameter for Estimation

	Malware	apply the Hanword S/W	
N(Total)	the number of PC or server	23 million	
V	rate of vulnerable PC or server	$\frac{20\,million}{23\,million}$ = 0.87	
I	rate of infected PC or server	0.0117 × V = 0.0102	ρ
R	rate of recovered PC or server	$\hat{p}$ × I = 0.0317 × I = 0.00032	α

PC 1대당 가치(value)는 통상적으로 PC 1대를 구매하는데 소요되는 값이기 때문에 1,000천 원으로 가정하였다. 따라서 훈글 S/W 취약점에 대한 손실비용 산출에 필요한 파라미터 값들은 <Table 5>와 같다.

ρ값은 전체 PC 대비 악성코드 감염율에 해당하고, α값은 전체 PC 대비 패치율에 해당한다. 훈글 S/W의 취약점에 대한 기본번식수(N_R)은 $N_R = (\rho/\alpha) = 0.0102/0.00032 = 31.875$이다.

SIR 모델에서 홍역의 N_R은 16~18, 말라리아의 N_R은 100 이상인 것과 비교하면 훈글 SW 취약점의 기본번식은 사람에게 있어서의 홍역 보다는 감염·전파력이 크고 말라리아 보다는 감염·전파력이 낮다는 것이라 할 수 있다.

본 논문에서 제시한 손실비용 추정식에서 취약점의 가중치는 VIR 모델의 N_R(기본 감염 수)을 사용하여 추정하였다. 기본 번식수가 크다는 것은 취약점을 이용하여 쉽게 공격이 가능하고 외부 위협으로부터 공격받을 시 감염·전파가 쉽게 된다는 것을 의미한다. 조직 내에서는 여러 가지 취약점에 대해 관리함으로써 N_R(기본 감염 수)값을 다양한 목적으로 활용할 수 있을 것으로 판단된다.

하나의 예시로 취약점에 따른 파급력과 감염정도를 나타내는 N_R(기본 감염 수)값을 통해 다음 <Table 6>과 같이 상, 중, 하의 3단계로 구분하여 각각 1, 2/3, 1/3으로 가중치를 적용하는 것도 하나의 방안이라고 할 수 있을 것이다. 이는 취약점의 파급력이 낮으면 손실에 미치는 영향이 상대적으로 낮고, 취약점의 파급력이 높으면 감염이 곧 바로 손실로 이어진다는 것을 의미한다.

〈Table 6〉 Example of Weight

Influence	N_R	Weight
high	$20 < N_R$	1
medium	$10 < N_R \leq 20$	2/3
low	$N_R \leq 10$	1/3

<Table 7>은 훈글 S/W의 취약점에 의한 손실비용 추정결과이다. 최종적으로 본 논문에서 제시한 S/W 취약점에 의한 손실비용 추정식에 훈글 S/W의 취약점 사례를 적용한 결과, 하나의 취약점으로 인해 약 2,272억 원의 손실비용이 발생할 수 있는 것으로 나타났다. 만일 취약점을 간과한다면 그에 대한 손실액이 발생 할 것이며, 신속한 취약점 대응으로 감염 PC에 대한 패치가 모두 이루어진다면 이러한 손실을 예방할 수 있을 것이라 할 수 있다.

〈Table 7〉 Estimating Loss

Loss = N × (I-R) × Value × Weight = 23 million × (1.02%-0.032%) × 1 milion KRW × 1 = 227.240 million KRW

5. 결 론

본 논문에서는 전염병 확산 모델인 SIR 모델을 응용하여 악성코드 확산에 적용하고자 VIR 모델을 제시하였고 이를 훈글 S/W 취약점에 의한 손실비용을 추정하는데 사용하였다. 보안 취약점에 대한 감염 시 손실을 추정하거나 측정한 논문을 찾아보기 어려운 실정에서 전염병 모델을 응용하여 수리적으로 S/W 취약점으로 인한 손실 비용을 산정한 것에 그 의의를 둘 수 있다.

VIR 모델에서는 PC나 서버가 악성코드에 감염되지 않았으나 감염될 수 있는 상태로 S/W에 취약점이 존재하는 Vulnerable(취약군) 상태, 악성코드에 감염되고 다른 PC를 감염시킬 수 있는 Infectious(감염군) 상태, 또한 악성코드에 감염 후 패치 되었고 같은 취약점에 의해서는 다시 감염되지 않는 Recovered(회복군) 상태로 구분하여 악성코드 감염이나 전파를 설명하였다.

VIR 모델을 효과적으로 활용하여 더욱 정확한 손실비용을 파악하기 위해서는 여러 가지 가정들이 존재한다. 예를 들어 악성코드의 감염 대상인 PC의 수 또는 서버의 수를 알아야 한다. 특정한 기업 같은 조직내에서는 중앙통제식 자산관리를 통해 이러한 내역을 파악할 수가 있기 때문에 조직내에서 활용하는 것은 상대적으로 쉬울 것으로 판단된다. 그러나 우리나라 국민들이 사용하는 PC용 S/W 취약점에 이를 적용하기 위해서는 국내의 모든 PC의 수, 취약점이 발견되는 S/W들에 대한 악성코드의 감염 비율 혹은 취약점에 의해 악성코드에 감염된 PC의 수를 알아야 한다. 또한 취약점이 발견된 S/W의 패치율 또는 패치에 의해 복구된 PC・서버의 수 등의 데이터들을 국가적으로 관리하여 파악하는 것이 병행되어야 한다.

본 논문에서는 우리나라 국민들이 가장 많이 사용하고 있는 훈글 S/W의 취약점이 발생하였을 때에 국가 전체적으로 어느 정도의 경제적 손실로 이어질 수 있는 가를 추정해 보았다. 그 결과 훈글 S/W의 취약점에 대한 패치가 신속히 이뤄지지 않으면 약 2,272억 원의 손실 비용이 발생할 것으로 예측되었다. 만일 훈글 S/W의 취약점을 간과한다면 그에 대한 손실액이 발생할 것으로 예상되며, KISA와 같은 전문기관 등에 의해 취약점이 신속하게 탐지・분석되어 발 빠르게 감염 PC에 대한 패치가 모두 이루어진다면 이러한 경제적 손실을 예방할 수 있을 것이라 판단되고, 이 값은 취약점 대응 노력의 가치로 인정받을 수 있을 것이라 판단된다.

본 논문은 S/W 취약점으로 인한 손실비용을 추정하기 위한 하나의 시도로서 의미를 가진다. 그러나 이를 실제 적용하는 과정에서 실측값들이 거의 없기 때문에 파라미터 값으로 여러 가정을 통해 추정한 제약점이 있다. 앞으로 이를 개선하기 위해서는 좀 더 객관적인 파라미터 추정방법들을 연구해 나갈 예정이다. 또한 S/W 회사들이 하나의 취약점

에 대해 일자별 패치 정보나 다운로드 정보를 관리하여 오픈한다면, 악성코드 감염 및 확산 모델을 보다 더 다양하게 적용할 수 있을 것이라 판단된다. 뿐만 아니라 국가 전체적으로 S/W 취약점에 대한 DB를 구축하여 이에 대해 상세히 관리해 나가고, 실시간 패치현황을 공유한다면 신종 취약점에 최대한 빠른 대응을 할 수 있을 것이고, 피해 손실이나 예방 대응효과 측정에도 다양하게 활용될 수 있을 것이라 판단된다.

아울러 감염율, 패치율, 기본 감염 수(N_R) 같은 값을 조직 내에서 관리한다면 보안대응을 위한 KPI로 활용할 수가 있고 상대적으로 높은 취약점을 우선 대응하도록 하는 전략수립 등 다양한 목적으로 활용될 수가 있을 것이라 판단된다. 앞으로 이러한 내용들은 지속적으로 연구를 추진할 예정이다.

References

[1] Chen, Z., "Worm propagation models," Mathematics Awareness Month : Mathematics and Internet Security Theme Essays, 2006.

[2] Chen, Zesheng, Lixin Gao, and Kevin Kwiat, "Modeling the spread of active worms," INFOCOM 2003, Twenty-Second Annual Joint Conference of the IEEE Computer and Communications, IEEE Societies, Vol. 3, IEEE, 2003.

[3] Lee, H. W., "On officeSW company beyond the Hanword," bloter.net, 2010. 03. 09, available : http://www.bloter.net/archives/26902.

[4] Lim, J.-M. and C.-H. Yoon, "Modeling and Network Simulator Implementation for analyzing Slammer Worm Propagation Process, Modeling and Network Simulator Implementation for analyzing Slammer Worm Propagation Process," Vol. 32, No. 5, pp. 277-285, 2007.

[5] Kim, J. Y. and Lee, S. H., "PC/Mobile Market," Mirae Asset, Company Insights, 2011.

[6] Kermack William O., and Anderson G. McKendrick, "Contribution to the mathematical theory of epidemics," Proc. of The Royal Society of London. Series A, Vol. 115, No. 700, 1927.

[7] Korea Information Security Agency, Development of Information Security Forecast Algorithm and Model, KISA-WP-2009-0025, 2009.

[8] Microsoft, Security Intelligence Report, Vol. 16.

[9] Microsoft, Security Intelligence Report Special Edition 10 Year Review, 2012.

[10] Ministry of public administration and security, SW security vulnerable point diagnosis Guide for E-Government SW development security diagnostician, 11-1311000-000395-14, 2012.

[11] NIST, The Economic Impacts of Inadequate Infrastructure for Software Testing, 2002.

[12] Lee, S. G., Ko, R. Y., and Lee, J. H., "Mathematical Modelling of the H1N1 Influ-

enza," Journal of the Korean Society of Mathematical Education Series E : Communications of mathematical education, Vol. 24, No. 4, pp. 877-889, 2010.

[13] Hwang, S.-O., "A Methodology for Security Vulnerability Assessment Process on Binary Code," JIWIT, Vol. 12, No. 5, pp. 237-242, 2012.

[14] Lim, S. S., Kwak, N. J., and Jung, K. M., "Tipping Point Analysis of SIR Model in Social Networks with Heterogeneous Contact Rates," 2011.

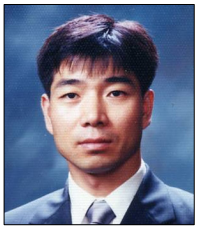
[15] Park, Y.-J. and Park, E.-J., "A Study on an Estimation of Adjusted Coefficient for the Maintenance of Information Security Software in Korea Industry," The Journal of Society for e-Business Studies, Vol. 16, No. 4, pp. 109-123, 2011.

[16] Yukyong Kim, and Doh, K.-G., "SOA Vulnerability Evaluation using Tun-Time Dependency Mesurement," The Journal of Society for e-Business Studies, Vol. 16, No. 2, pp. 129-142, 2011.

[17] Zou, Cliff Changchun, Weibo Gong, and Don Towsley, Code red worm propagation modeling and analysis, Proceedings of the 9th ACM conference on Computer and communications security, ACM, 2002.

저 자 소 개

김민정 (E-mail : korea.minjeong@gmail.com)
2003년~2007년 고려대 정보수학과 졸업 (이학사)
2013년~현재 상명대 지식보안경영학과 (석사과정)
관심분야 정보보호 정책, 개인정보보호, 산업보안



유진호 (E-mail : jhyoo@smu.ac.kr)
1988년~1992년 고려대 이과대학 수학과 (이학사)
1992년~1994년 고려대 일반대학원 통계학과 (이학석사)
2006년~2010년 고려대 정보경영공학전문대학원 정보경영공학과 (공학박사)
(세부전공 : 정보보호전공)
1993년~1999년 한국전자통신연구원(ETRI) 연구원
2000년~2004년 IBM Korea 차장(CRM/데이터마이닝 컨설턴트)
2004년~2013년 한국인터넷진흥원(KISA) 인터넷문화진흥단장
2013년~현재 상명대학교 경영학과 조교수
관심분야 정보보호, 개인정보보호, MIS, 인터넷윤리