국방 보안사고에 대한 행동 심리학적 분석 방법*†

박준정[1], 김광조[1) 2)]

카이스트 정보보호대학원[1)]/ 전산학과[1) 2)]

A Behavioral Psychological Analysis Research for Military Security Incidents*†

Joon-Jeong Park[1)], Kwangjo Kim[1) 2)]

Graduate School of Information Security[1)] / Dept. of Computer Science, KAIST[2)]

요 약

2013년 미국 NSA의 무차별적인 도·감청 사실을 폭로한 스노든 사건 이후 내부자(사람)에 의한 보안 취약점에 대한 관심이 폭발적으로 증가하였다. 하지만 사람의 심리와 행동에 대한 과학적인 연구 결과를 토대로 보안 취약점을 분석하고 근본적인 대책을 제시한 연구는 활발히 진행되지 못하였다. 특히, 국가안보의 핵심 축이면서 기밀자료를 다수 취급하고 있는 국방 분야에서 보안을 인간의 특성과 연계시킨 연구는 진행된 적이 없다.

국방망은 외부 인터넷과 물리적으로 완전히 분리되어 있으며, 외부인이 접근하기 극히 제한되는 등 국방 보안 환경은 고유한 특성을 보유하고 있다. 이러한 환경 하에서 발생한 보안사고 원인을 분석한 결과, '사람'이 가장 큰 문제였음을 다시 한 번 확인할 수 있었다.

이에 본고에서는 국방 분야 보안사고 중 이미 공개되어 있는 사례를 토대로 유형별 사고를 제시하고, 사실 관계를 바탕으로 전형적인 모델로 재정의한다. 사례별 행동 강화 요인과 약화 요인을 식별하고, 이 요인들이 보안사고와 연결되는 판단 및 행동에 어떤 영향을 미치는지에 대해 고찰하려고 한다.

이를 통해, 군에서 발생 가능성이 높은 보안사고자 행위 요인을 행동 심리학적 관점으로 분석하여 모델링하는 한편, 그에 따른 보안정책 방향을 설정하고 보안대책을 수립하는 것을 궁극적인 목표로 한다.

I. 서 론

2013년 미국 NSA의 무차별적인 도·감청 사실을 폭로한 스노든 사건 이후 내부자(사람)에 의한 보안 취약점에 대한 관심이 폭발적으로 증가하였다.

2014년 전 세계 IT 전문가 818명을 대상으로 한 설문조사 결과 응답자의 89%, 미국인 응답자의 93%가 '내부자 위협을 느끼고 있다'고 답변[1]하였다.

예측할 수 없는 사람의 행동이 보안 시스템을 무용지물로 만들 수 있기 때문에[2] 사람에 의한 보안 취약점은 최근 급부상하는 보안이슈 중 하나이다.

하지만 사람의 심리와 행동에 대한 과학적인 연구 결과를 토대로 보안 취약점을 분석하고 근본적인 대책을 제시한 연구는 활발히 진행되지 못하였다. 특히, 국가안보의 핵심 축이면서 기밀자료를 다수 취급하고 있는 국방 분야에서 보안을 인간의 특성과 연계시킨 연구는 진행된 적이 없다.

* 본 연구는 미래부가 지원한 2014년 정보통신·방송(ICT) 연구개발사업의 연구결과[1391104001, 생체모방 알고리즘을 활용한 통신기술 연구]로 수행되었습니다.

† This research was supported by the KUSTAR-KAIST Institute, KAIST, Korea.

국방망은 외부 인터넷과 물리적으로 완전히 분리[3]되어 있으며 외부인이 군 내부에 접근하기 극히 제한되는 등 고유한 국방 보안 환경 하에서 발생한 다양한 보안사고를 분석해 본 결과, '사람'이 가장 큰 문제였음을 다시 한 번 확인할 수 있었다.

이에 본고에서는 국방 분야 보안사고 중 이미 공개되어 있는 사례를 토대로 유형별 사고를 제시하고, 사실 관계를 바탕으로 전형적인 모델로 재정의한다. 사례별 행동 강화 요인과 약화 요인을 식별하고, 이 요인들이 보안사고와 연결되는 판단 및 행동에 어떤 영향을 미치는지에 대해 고찰하려 한다.

군에서 발생 가능성이 높은 보안사고자 행위 요인을 행동 심리학적 관점으로 분석하여 모델링하는 한편, 그에 따른 보안정책 방향을 설정하고 보안대책을 수립하는 것을 궁극적인 목표로 한다.

이를 위해, 제 2장에서는 보안 문제를 심리학적으로 접근하려고 했던 시도에 대해 살펴보고, 제 3장에서는 이미 알려진 국방 보안사고를 전형적인 유형으로 모델링 한 후 행동에 영향을 미치는 요인을 식별한다. 제 4장에서는 심리학적 연구 방법론에 대해서 논의한 다음, 마지막 제 5장에서는 연구가 완료되었을 경우 기대되는 효과에 대해 판단해 본 후 결론을 맺는다.

II. 관련 내용

2.1 관련 연구

Ryuichi Ogawa 등[4]은 APT 공격 시나리오를 설정한 후 공격자 역할을 수행할 피실험자를 대상으로 설문조사와 집단토론을 통해 공격 여부 인지와 공격 의도를 파악하는 연구를 진행하고 있다.

Youngsoo Kim 등[5]은 APT 공격자가 취할 수 있는 행위를 4단계로 분류하여 3.20 대란 공격자 행위에 적용한 연구를 하였다.

임채호 등[6]은 사이버범죄를 효과적으로 분석하고 대응하기 위해 심리적 관점에서 프로파일링 방안을 연구하였다.

2.2 한계 및 문제 제기

상기 연구들은 대부분 외부에서 발생하는 일반적인 공격 상황을 바탕으로 사이버 공간에서 공격자의 행위를 심리학적으로 분석하는데 큰 의미가 있다.

반면, 대부분의 보안사고가 내부자에 의해 발생하는 국방 보안 환경을 고려할 경우, 군 보안사고를 예방하기 위해서는 이에 특화된 행동요인과 보안행위와의 관계에 대한 연구를 진행하여야 할 필요가 있다.

III. 국방 보안사고 모델링 방안

3.1 제한사항

국방 분야 보안사고는 군 외부에 공개되는 경우가 많지 않아 정확히 파악할 수 없는 제한사항이 있다. 하지만 주요 보안사고들은 인터넷 등에 이미 공개되어 있기 때문에 본고에서는 이 사례만을 활용하여 대표적인 유형으로 4가지를 설정하였다.

3.2 공개된 국방 보안사고 사례 유형

(유형 1) 2014년 7월 현역장교들이 금품과 향응 등을 수수하고 방위력 개선사업 관련 기밀 다수를 무기중개인에게 불법 유출[7]하였다.

(유형 2) 2013년 10월 현역장교가 유명 SNS 서비스를 통해 간부들과 작전 관련 기밀을 공유하다 적발[8]되었다.

(유형 3) 2013년 1월 ~ 2014년 7월 간 외부 인터넷과 물리적으로 분리된 국방망에 바이러스 31,064건이 침입된 사실이 확인[9]되었다.

(유형 4) 2014년 1월 북한 해킹조직이 안보 관련 주요 인사를 대상으로 해킹메일을 다량 유포[10]하였으며, 국방부 출입기자 PC에서 악성코드 감염이 확인[11]되었다.

3.3 보안사고 재구성을 통한 모델링 예시

(유형 1) ~ (유형 4)에 해당하는 사례를 모두 모델링 할 수 있는데, 본고에서는 상기 방위력 개선사업 관련 기밀 유출사건(유형 1)을 토대로 모델링 한 예를 제시한다.

〈 상 황 〉
1. 방산업체 임원 A
   - 사업상 필요에 의해 기밀 수집 시도
2. 브로커 B
   - A로부터 기밀 불법 수집 제의 수락
   - 기밀을 취급하는 C에게 의도적으로 접근
3. 군 관계관 C
   - B로부터 기밀 유출 청탁 접수
   - 유출 여부에 대해 고민・판단

상기 상황에서 C의 기밀 유출 여부에 영향을 미치는 판단 과정을 세부 단계별로 살펴보면 Fig. 1.과 같다.

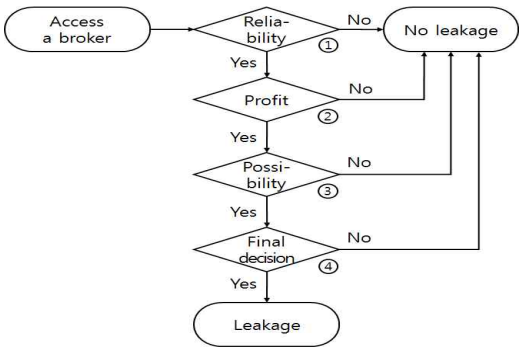

Fig. 1. Process that affect the military secrets leakage

3.4 단계별 행동 판단에 미치는 요인 판단

단계별 판단에 미치는 요인을 과학적으로 분석하기 위해 Table 1.과 같이 행동 강화요인(reinforcer)과 처벌요인(punisher)을 구분하여 제시한다.

Table 1. Factors in determining for each step

Step	Reinforcer	Punisher	Re-marks
1	confidence in the broker		
2	money, promotion, interpersonal relations	conscience, intensity of punishment, organizational culture, detecting probability	
3	expected ease of the acquisition	expected security countermeasures	
4	actual ease of the acquisition	actual security countermeasures	

상기 요인들의 선정에 대해서는 과거 유사한 기밀 유출 사례와 군사보안 전문가 자문 및 토의 등 다양한 방법을 통해 추가로 보완할 예정이다.

IV. 심리학적 연구 방법론[12]

심리학 연구에서 활용되는 다양한 방법론 중 본고에서 적용 가능한 방법을 위주로 살펴본다.

관찰법은 연구 대상자의 행동을 직접 관찰한 결과를 바탕으로 결론을 얻어내는 방법으로, 적절한 연구 대상자를 선정하는데 어려움이 있다.

면접법은 연구 대상자들을 1:1로 면담하여 심층적인 질문을 주고받는 방법으로, 면접의 특성상 대상자들이 솔직히 답변하지 않을 가능성이 상존한다.

질문지법은 대상자들이 질문지에 응답한 결과를 바탕으로 분석하는 방법으로, 다수의 사람들로부터 정보를 신속하게 수집하는데 특히 유리한 방법이다.

따라서 본고에서는 질문지법을 활용하여 기밀 유출 판단 단계에서 영향을 미치는 요인들을 고찰할 것이며, 심리학적 실험론 관련 문헌을 참고하고 해당 분야 전문가의 조언을 받아 질문지 문항을 개발할 예정이다.

V. 기대 효과 및 결론

다양한 보안위협에 개별 보안기술로 대응하는 것은 한계가 있을 수밖에 없다. 위험요인을 근본적으로 감소시키기 위해 의사결정 과정에서 이익과 손실이 미치는 영향[13]을 분석하는 등 인간의 기본적인 행동 매커니즘에 대한 이해가 유용할 수 있다는 점을 증명하는데 가치가 있다.

또한, 내부자 보안 위험이 기술보다는 사람의 문제[14]라는 전제를 바탕으로 각 개인이 자발적으로 판단하여 수행할 수 있는 행동들에 대한 연구[15]를 통해 국방 보안사고 관련 행동들을 분석해 볼 수 있을 것으로 기대된다.

결과적으로, 본 연구를 통해 사례별 보안 위협 행위들에 대한 강화 요인과 약화 요인을 추출하고 보안사고자 행위 패턴을 과학적으로 분석하여 보안정책 개선 및 다양한 보안대책 수립에 도움이 될 것으로 사료된다.

References

[1] Vormetric, "2015 Vormetric Insider Threat Report-Global Edition," Jan. 2015.

[2] 이수미, "휴먼팩터가 보안에 미치는 영향," Issue Report, 11(9), Financial Security Agency, June 2011.

[3] http://defence21.hani.co.kr/34228

[4] Ryuichi Ogawa *et al.*, "Case-based Psychological Analysis for Protecting Sophisticated Cyber-attacks," Proceedings of the 32nd Symposium on Cryptography and Information Security, Kokura, Japan, Jan. 2015.

[5] Youngsoo Kim and Ikkyun Kim, "Involvers' Behavior-based Modeling in Cyber Targeted Attack," Proceedings of SECURWARE 2014 : The Eighth International Conference on Emerging Security Information, Systems and Technologies, Lisbon, Portugal, Nov. 2014.

[6] Chaeho Lim *et al.*, "Profiling of Cyber-crime by Psychological View," *Journal of Korea Institute of Information Security and Cryptology*, 19(4), pp. 115-124, Aug. 2009.

[7] Prosecution Service, "http://www.spo.go.kr/seoul/notice/notice/notice01.jsp?mode=view&board_no=116&article_no=579011," July 2014.

[8] YTN, "http://www.ytn.co.kr/_ln/0103201310141055339751," Oct. 2013.

[9] Yonhap News, "http://www.yonhapnews.co.kr/bulletin/2014/10/08/0200000000AKR20141008079100043.HTML?from=search," Oct. 2014.

[10] Ministry of Science, ICT and Future Planning, "http://www.msip.go.kr/web/msipContents/contentsView.do?cateId=mssw311&artId=1213321," Jan. 2014.

[11] Yonhap News TV, "http://www.news-y.co.kr/MYH2014 0822016200038/," Aug. 2014.

[12] 김유진 등 공역, "심리학 개론," 형설출판사, Feb. 1984.

[13] R. West, "The psychology of security : why do good users make bad decisions?," Communications of the ACM, 51(4), pp. 34-40, Apr. 2008.

[14] 유우영, "내부자 보안 위협 관리," Proceedings of the 12th Conference on Defense Information Security and Cryptology, Seoul, Republic of Korea, Nov. 2014.

[15] 민경환 등 공역, "심리학 입문," 시그마프레스, Aug. 2011.