정보보호 위한 신기술 여기에 모였다

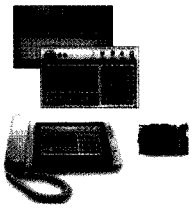
KISA 정보보호 연구성과물 전시 및 발표회 개최

지난 3월 10일 삼성동 코엑스 3층 컨퍼런스홀에서 KISA가 '정보보호 연구성과물 전시 및 발표회'를 가졌다. 그동안 KISA는 민간기업과 일반 사용자를 위한 침해사고 대응, 정보보호 인식제고, 정보보호 정책수립 기관으로서의 이미지가 강했던 것이 사실이다. 그런 KISA가 이번 발표회를 통해 정보보호 연구개발 분야에서도 중추적 역할을 하고 있음을 스스로 입증했다. 이날 발표회에서는 신규 융합서비스 보호기술, 인터넷 침해사고 대응기술, 개인정보 유출 방지기술 등 3개 분야의 10개 핵심기술 전시와 설명회가 460여명의 산·학·연 보안전문가가 참석한 가운데 성황리에 이뤄졌다. 기업 정보보호 담당자들에게는 최신 보안동향 및 기술에 대한 정보를 제공하고 보안 실무에 직접 적용 가능한 기술들이 선보인 이번 발표회의 주요 내용을 지면을 통해 소개해 본다.

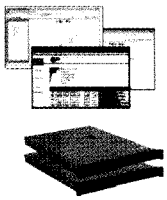
| 정보보호뉴스 취재팀 |

인터넷 전화 서비스 보호 위한 보안통신 기술

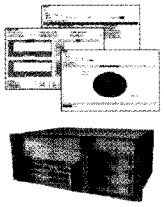
KISA가 이번 발표회를 통해 선보인 10개 중 2개의 기술은 VoIP 서비스를 위한 기술이었다. 최근 번호이동제 실시 및 행정 공공기관에서의 적용확대 정책에 따라 급속히 확산되고 있는 VoIP 서비스의 안전성을 위해 정책과 기술개발 등 종합적 예방책이 요구되고 있기 때문이다. 여기에 해당하는 연구결과는 종단간 암호통신 기능, VoIP 불법스팸 예방 및 피해 최소화를 위한 스팸대응 시스템, VoIP 서비스망 보호를 위한 보안세션 제어 시스템으로, 향후 보안기술 표준화 및 인터넷 전화 서비스와 관련된 정보보호 인식제고 측면에서 큰 의미가 있을 것으로 기대된다.



VoIP H/W 보안단말



VoIP 스팸대응시스템

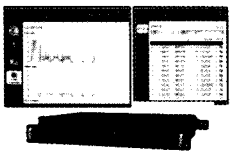


보안 세션제어시스템

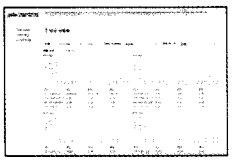
▲ 인터넷 전화 서비스 보호를 위한 보안통신 기술 ▲

인터넷전화 해킹 탐지 및 대응 기술

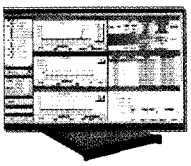
VoIP 서비스와 관련된 또 다른 기술인 인터넷전화 전용 방화벽은 인터넷전화 사용시 해킹으로 인한 과금 우회, 통화 방해 등 다양한 공격을 신속하게 탐지하고 차단하는 기술이다. 이미 지난 1월 산업체에 기술 이전돼 빠르면 4월 중 상용화 제품이 출시될 것으로 예상된다. 앞에서 소개된 보안통신 기술이 일반 사용자를 위한 것이라면, 인터넷전화 전용 방화벽은 인터넷전화 서비스 사업자와 기업을 위한 기술로 구분할 수 있다.



음성기반 SIP 침입방지기술



비정상 SIP 트래픽 모니터링 기술

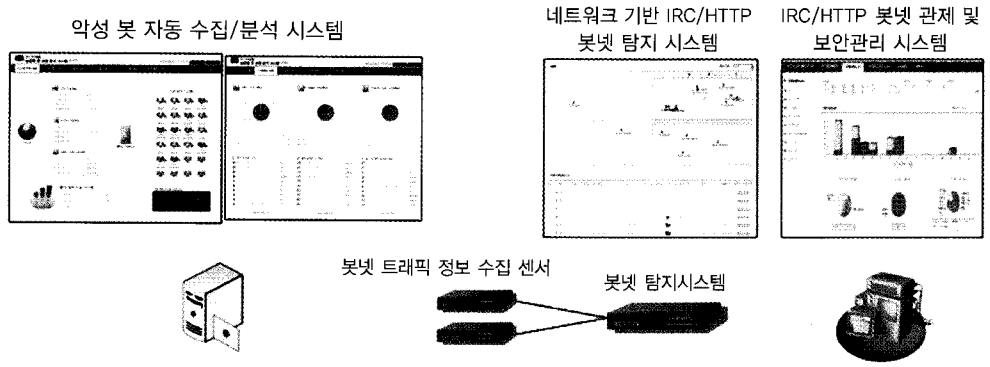


SIP 침입대응관리기술

▲ 인터넷전화 해킹 탐지 및 대응 기술 ▲

신종 봇넷 능동형 탐지 및 대응기술

분산서비스거부공격(DDoS), 스팸, 개인정보 탈취 등에 악용되는 봇넷은 향후 인터넷 환경의 최대 위협으로 손꼽히고 있다. 점점 지능화되는 신종 봇넷을 탐지하고 봇넷의 구성/분포/행동정보를 실시간으로 종합 관리하는 기술은 봇넷 대응을 위한 필수조건이다. KISA가 선보인 호스트 기반의 악성코드 능동형 탐지 및 대응기술과 네트워크 기반의 신종 봇넷 탐지기술, 실시간 봇넷 통합 관제 및 보안관리 기술은 향후 경제적 사회적 피해를 최소화하고 안전한 인터넷 서비스 환경을 조성하는데 큰 역할을 할 것으로 기대되고 있다. 특히, 국제적으로 연구 초기단계인 HTTP/P2P 봇넷 탐지/대응에 대한 기술선점 효과가 클 것으로 보인다.



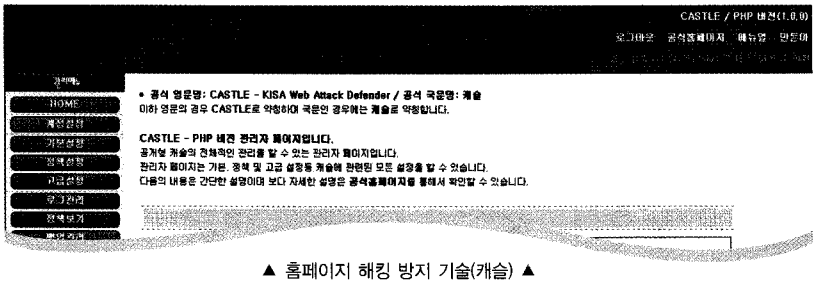
▲ 신종 봇넷 능동형 탐지 및 대응기술 ▲

홈페이지를 통한 악성코드 탐지 기술

홈페이지 해킹을 통한 악성코드 은닉 및 전파 피해를 최소화하기 위해서는 홈페이지 악성코드 탐지 시스템의 개발 및 운영이 필요하다. 이를 위해 개발된 악성코드 탐지기술은 홈페이지 소스 수집기능과 홈페이지 소스 분석 기능, 악성코드 점검 기능, 관리 기능을 구현한 것으로, 이미 지난 2008년 125,000여개 도메인에 대한 점검에도 이용돼 그 효과를 인정받기도 했다. 이 기술은 향후 악성코드에 대한 사전탐지 기능을 통해 악성코드에 대한 능동적인 대응책을 확보할 수 있을 뿐만 아니라, 악성코드 은닉 사이트의 자동발견 및 차단을 통해 2차 피해도 예방할 수 있을 것으로 예상된다.

홈페이지 해킹 방지 기술(캐슬)

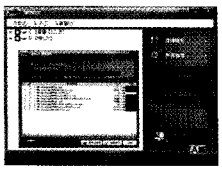
홈페이지 취약점은 상대적으로 낮은 수준의 기술로도 해킹에 악용이 가능하고, 또 많은 이용자들에게 악성코드를 전파하는 등 침해사고의 주요원인으로 지목되고 있다. 홈페이지 취약점을 보완하기 위해서는 취약점의 원인인 소스 수정이 필요하지만 대부분의 중소기업 홈페이지의 경우, 개발인력 미비로 해킹사고가 지속적으로 재발해 문제가 되고 있다. KISA가 개발한 홈페이지 해킹방지 기술(캐슬)은 홈페이지 주요 취약점 예방기술로, 최소한의 홈페이지 소스 수정만으로도 적용이 가능하다. 또한 정책 및 관리기능을 통해 유지보수가 편리하며, PHP, ASP, JSP와 같은 주요 웹 애플리케이션에도 적용할 수 있다



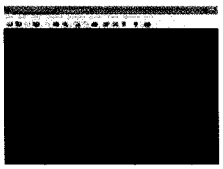
▲ 홈페이지 해킹 방지 기술(캐슬) ▲

홈페이지 해킹 경로 탐지 기술(휘슬)

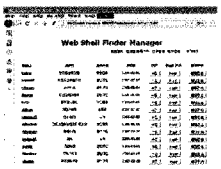
캐슬이 홈페이지 상의 취약점을 보완하는 기술이라면, 휘슬은 웹 서버 공격에 이용되는 웹쉘을 탐지해 대응하는 기술이다. 특히 웹쉘은 기존의 바이러스 백신 프로그램이 잘 탐지하지 못해 일반 서버 관리자들에게는 골칫거리였다. 이런 상황에서 개발된 휘슬은 웹쉘이 서버에 설치됐는지를 손쉽게 검색할 수 있으며, 관리자는 휘슬 관리 시스템을 통해 패턴, 배포업체, 점검결과를 관리해 안전한 서버 관리에 활용할 수 있다. 웹 서버에 대한 안전성이 지속적으로 제기되고 있는 가운데 휘슬은 국내 웹 서버 보안성 향상에 기여할 것으로 보인다.



윈도우 휘슬 프로그램

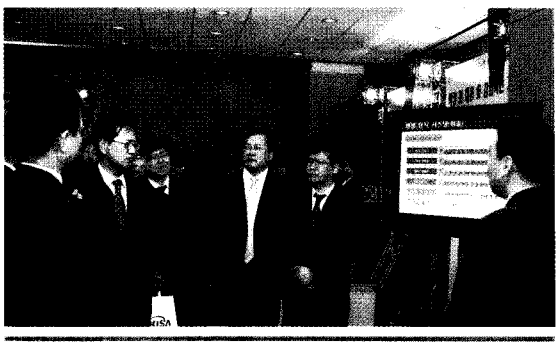


리눅스 휘슬 프로그램



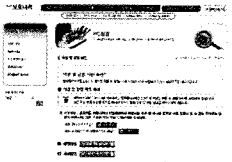
휘슬 관리 시스템

▲ 홈페이지 해킹 경로 탐지 기술(휘슬) ▲

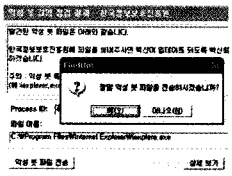


DNS 싱크홀 기반 악성봇 감염확인 기술(FindBot)

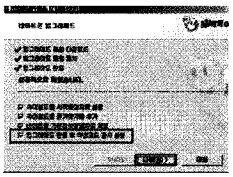
자신의 PC가 악성봇에 감염돼 공격에 악용된다는 사실을 모르는 사용자가 적지 않다. 악성 봇이 기존의 웜/바이러스와는 달리, 감염된 PC에는 특별한 피해를 주지 않아 사용자가 미처 알지 못하기 때문이다. 이런 상황에서 KISA가 일반 사용자도 손쉽게 악성봇 감염여부를 확인하고 무료백신을 통해 치료할 수 있도록 하는 기술을 개발했다. 악성봇 감염 확인 프로그램 FindBot은 사용자 PC에서 직접 악성봇 감염을 확인할 수 있는 소프트웨어로, 악성봇 감염 PC를 근본적으로 치료하고 보안 업데이트를 안내한다는 점에서 2차 피해를 차단하는 효과를 얻을 수 있다.



악성봇 감염확인 홈페이지



FindBot S/W

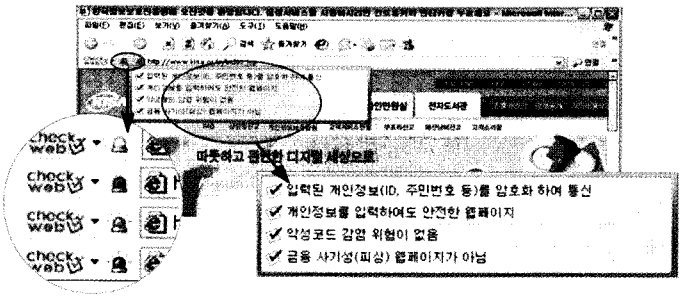


네이트온 악성코드 검사

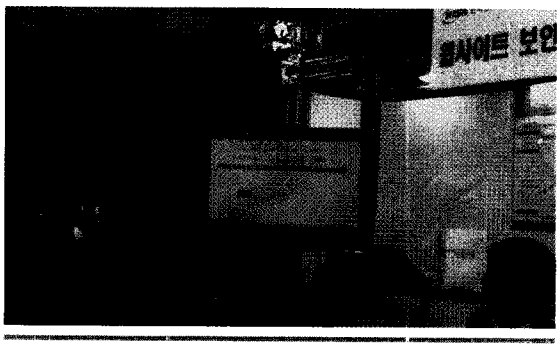
▲ DNS 싱크홀 기반 악성봇 감염확인 기술(FineBot) ▲

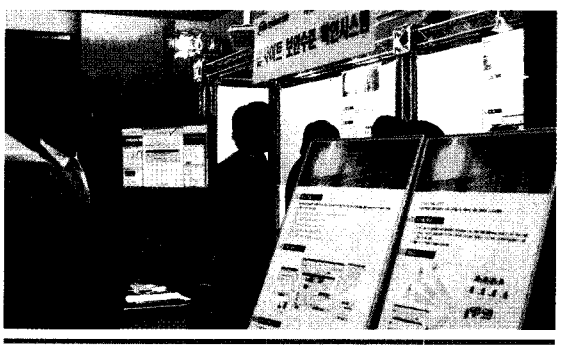
웹 사이트 보안수준 확인 시스템(Web Check)

최근 금융정보, 개인정보를 금융사기 목적으로 탈취하는 공격이 확산되면서 웹 이용자들의 불안감과 위험이 증대되고 있는 가운데, 웹 사이트 보안수준 정보를 확인할 수 있는 시스템도 이번에 선보였다. 웹 사이트 보안수준 확인 시스템 Web Check는 신뢰할 수 있는 웹 사이트의 URL과 IP를 기반으로 웹 사이트 화이트 리스트 DB를 구축해 관련 정보를 이용자에게 전달하는 것으로, 웹사이트를 방문했을 때 해당 웹사이트의 보안정책 준수 여부 및 신뢰도를 경광등과 설명창을 통해 알려주게 된다.



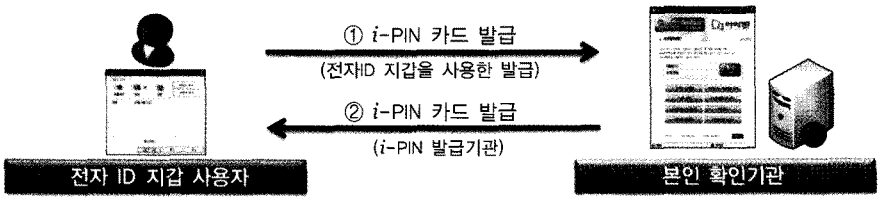
▲ 웹사이트 보안수준 확인 시스템(Web Check) ▲





전자ID지갑 기반의 온라인 본인확인시스템

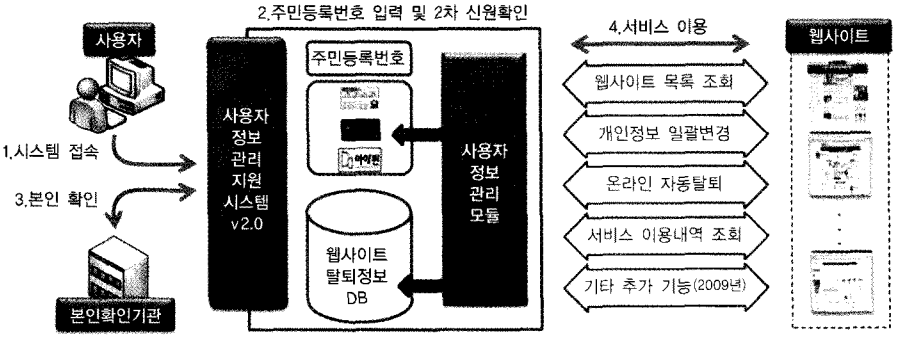
주민번호 노출에 따른 개인정보 침해사고가 증가함에 따라 인터넷 상에서 주민번호 없이 실명확인 가능한 아이핀을 개발·보급하고 있지만, 아이핀 사용자들은 본인확인기관 기억의 어려움과 패스관리의 불편함 등으로 이용확산이 원활하게 이뤄지지 않고 있다. 이런 문제를 해결하기 위해 KISA는 웹 사이트 인증정보를 사용자가 손쉽게 관리할 수 있는 전자ID지갑을 활용해 사용자 편의성을 증대시키고, 피싱, 파밍 공격에도 안전한 본인확인 시스템을 개발해 선보였다.



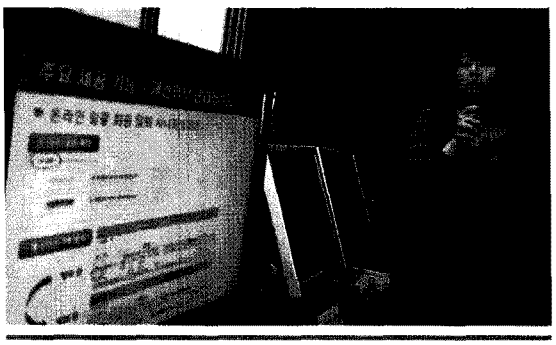
▲ 전자ID지갑을 이용한 아이핀 신규발급 과정 ▲

사용자 정보 관리지원 시스템

인터넷 이용의 증가로 수많은 웹사이트에서 사용자 개인정보가 분산 관리됨에 따라 사용자는 회원탈퇴 등을 위해 각 웹 사이트에 매번 직접 접속해야 하는 불편함이 있다. 또한, 개인정보 관리가 허술한 웹 사이트나 가입 후 이용하지 않는 웹 사이트 등에도 개인정보가 잔재해 개인정보 노출 위협이 증대되고 있다. 이러한 위협 및 사용자 불편을 최소화하기 위해 사용자 정보 관리지원 시스템은 사용자 이름 및 주민등록번호를 이용한 가입 웹 사이트 목록 조회 기능과 가입 웹 사이트 간 개인정보 일괄변경 기능을 제공한다.



▲ 사용자 정보 관리지원 시스템 기능 및 구성도 ▲



지난 2008년은 대규모 해킹·개인정보 유출 등 보안 사고로 얼룩진 한 해였다. 중국발 해킹으로 인해 국내 대표 오픈마켓 회원 1,000만명의 개인정보가 유출됐고, 포털 사이트의 고객 상담정보가 해커에 의해 탈취됐으며, 정유회사 고객정보 1,100여만건이 내부 직원에 의해 유출되는 등 다양한 형태의 보안 사고가 발생했던 한해였다.

지난 십여년에 걸쳐 진행된 정보화 혁명으로 인해, 거의 모든 정보들이 디지털화되고 인터넷을 통한 유통이 일반화되면서 정보보호 이슈는 날이 갈수록 심화되고 있는 실정이다. 인터넷이 우리 사회에 가져온 순기능은 형언할 수 없을 만큼 크지만 개인정보 침해를 비롯한 역기능 또한 심각한 수준에 이르고 있다. 향후 유비쿼터스 시대 도래 등과 더불어 다양한 개인 맞춤형 IT 서비스가 더욱 확산된다면 개인정보 보호와 프라이버시에 대한 이슈는 지금보다 더 첨예하게 대두될 것으로 예상된다. 더 많은 정보사회의 편익을 누리기 위해 개인정보의 적절한 수집과 활용은 계속될 것이기 때문이다. 그런 의미에서 개인정보보호는 고도 정보화 사회를 위한 기본 전제조건이자, 결정적인 신뢰요소다. 그리고 지금은 우리 사회의 개인정보보호 수준재고를 위해 모두의 지혜가 필요한 시점이다.

김인호 | SK텔레콤 IT보안팀 매니저 _ ino1170@sktelecom.com

선한 사마리아인과 정보보호

비즈니스 환경 변화와 정보보안 Risk 증대

여러 형태의 보안 위협은 기업·기관의 경영 활동에 있어 주요한 리스크(Risk) 중 하나가 되고 있다. 기업·기관이 해킹·고객정보 유출 등 보안 사고를 당하게 되면 피해 기업·기관은 수사기관의 조사 및 부정적 언론 보도로 인한 이미지 하락은 물론, 사안의 중요성에 따라 정부의 징계 및 형사처벌, 고객 집단소송 등 막대한 유무형의 피해에 직면하게 되는 것이 일반적인 현상이다. 또한 장기적으로는 고객이탈 및 매출 감소, 기업 브랜드 가치 훼손 등 보안 Risk가 악순환 형태로 지속·반복되며 피해가 확대되는 특징을 보이고 있다.

정보보안 사고 발생 시 기업/기관의 Risk 확대 과정

최근 해킹·고객정보 유출 등 정보보안사고 발생 시,
① 수사기관의 조사 → ② 언론노출 → ③ 정부의 징계 및 형사처벌(과태료/과징금) → ④ 고객 집단소송으로 인한 민사상의 책임 직면 → ⑤ 고객이탈 및 매출 감소 → ⑥ 기업 브랜드가치 훼손 등의 보안 Risk가 악순환 형태로 지속, 반복되며 피해가 확대되는 특징을 보이고 있음