Journal of the Korea Academia-Industrial cooperation Society
Vol. 24, No. 9 pp. 149-154, 2023

https://doi.org/10.5762/KAIS.2023.24.9.149
ISSN 1975-4701 / eISSN 2288-4688

자료교환체계 개선 및 OTP 다중인증을 통한 보안강화 메일시스템 구현

심호섭, 박만춘*
국방기술품질원

Application of Data Exchange System Improvement & OTP Multi-Factor Authentication for the Enhanced Security E-mail System

Hosup Shim, Manchun Park*
Defense Agency for Technology and Quality

요 약 IT 기술이 발달함에 따라 해킹 및 개인정보 유출과 같은 보안 사고가 지속적으로 일어나고 있다. 이는 국방기술품질원의 사내 전산메일의 경우에도 마찬가지로 예방적 차원의 대책 강구가 필요하였다. 이메일을 통한 기술자료 유통 시 '내외부 메일' 및 '자료교환시스템' 보안 강화가 필요해짐에 따라 기존 사용중이던 사내메일 시스템을 개선하여, '부서장 결재선 강화', '반출메일 암호화 설정', '다단계 로그인 인증 절차 도입' 등 보안 취약 및 위해 요소를 제거하였다. 물론 보안 측면만 강조해서는 시스템 사용자 입장에서 불편함을 감수해야만 하는 결과가 초래되는 경우가 발생하기도 하므로 이를 만회하기 위한 사용자 편의성 측면에서 보완적인 개선조치도 수행하였다. 성능이 업그레이드된 최신 이메일 솔루션, 키보드보안/모바일OTP/암호화 프로그램 등 보안 SW 적용, 표준기술(Non-Active X) 적용, 유관시스템 연동, 망연계 설치, 그리고 데이터 이관 및 검증 등을 거쳐 개선하였고, 보다 지능화되고 발전되어 가는 해킹기술 발전과 같은 보안 위협요소들로 인해 향후에도 지속적인 모니터링 및 이메일 보안기능 강화와 성능 업데이트가 이루어짐이 적절하다.

Abstract As advanced technology has developed recently, security problems such as hacking or personal information leakage are continuously and increasingly occurring. Accordingly, information systems in DTaQ are also affected by these threats and need to be prepared to respond to possible security problems. This would enable new DTaQ e-mail and data exchange systems to adopt technology standardization such as a non-active-X security enhancement and user-friendly function improvement. This would be helpful to eliminate a security-threat element and make a safe and user-friendly "e-working" environment. For example, the newest e-mail solution, keyboard security solution, mobile one-time password, and encoding program make the DTaQ e-mail and data exchange system not only improve security, but also strengthen the efficiency of its performance. Also, system improvement is conducted by related systems linkage, network connection, data transfer, tuning, etc. This study summarizes the major activities and achievements of adopting the new e-mail and data exchange system with a security solution, standardization of technology, etc.

Keywords : E-mail, Data Exchange, Security, OTP(One-Time Password), Authentication, Encoding, Decoding

*Corresponding Author : Manchun Park(Defense Agency for Technology and Quality)
email: mcpark@dtaq.re.kr
Received July 6, 2023 Revised August 3, 2023
Accepted September 1, 2023 Published September 30, 2023

1. 서론

해킹기술의 다변화, 고도화 및 대중화로 ID/PW 인증 방식의 안전성이 저하되고 있다[1]. 대부분의 회사는 해커로부터 정보자산을 보호하기 위해 각종 정보보호시스템을 도입·운영한다. 하지만 이메일을 통한 사회공학적 기법을 활용한 보안 위협이 날이 갈수록 점점 더 증가하고 있다. 최근에 통일부 사칭 '인권토론회 개최 안내', 국세청 사칭 '세무조사 출력요구 안내통지문' 등의 문구가 포함된 악성 메일이 유포되어 ID 및 비밀번호를 갈취당하는 피해가 발생하여 각별한 주의와 대비가 필요한 실정이다.

해킹기술의 발달로 보안장치를 우회하는 방법 등 정보보호시스템 운영상 취약점이 존재하게 된다. 침입방지시스템(IPS)은 정상적인 트래픽으로 위장 가능한 공격에 무방비하고, 침입차단시스템(Firewall)은 IP, Port 방식에 의한 사용자 중심의 보안정책 적용으로 FTP, Telnet등 내부자를 위해 허용된 서비스 접근 시 해킹이 가능하며, 침입탐지시스템(IDS)은 발견되지 않는 새로운 침입기법에 대응이 어려운 한계점을 지니고 있어 침입자가 정상적인 트래픽인 HTTP/HTTPS와 같은 트래픽으로 위장한 공격에 매우 취약한 실정이다.

이메일시스템의 경우에는 정상적으로 메일을 주고받기 위해서는 메일 운용에 필요한 SMTP, POP3 등 잘 알려진 포트를 정보보호시스템에 개방해 줄 수밖에 없다. 따라서 사이버 공격의 대부분이 이메일로부터 시작된다. 국방기술품질원의 이메일시스템은 장기사용에 따른 노후화로 인하여 각종 해킹 위협에 노출되어 있어, 이에 대한 보호대책 마련이 시급히 필요하다.

이메일시스템 보안 향상의 일환으로 기술자료 유통 시 '내외부 메일' 및 '자료교환시스템' 보안 강화가 필요해짐에 따라 '부서장 결재선 강화', '반출 메일 암호화 설정', '다단계 로그인 인증 절차' 등 각종 보안체계를 구축하여 비인가자의 무단 접속 차단 등 각종 취약요소를 제거하여 외부 해킹으로부터 중요자료가 유출되지 않도록 보안대책을 시급하게 마련해야 한다. 한편, 보안 측면만 강조해서는 시스템 사용자 입장에서 불편함을 감수해야만 하는 결과가 초래되는 경우가 발생하기도 하는데, 예를 들어, 사용자 보안 인증 강화를 위하여 모바일 OTP 인증수단을 도입하게 되면, 이에 따른 인증절차 추가로 인하여 이메일 사용자의 업무 절차 및 시간 증가와 같은 불편함을 초래하기도 한다. 이러한 불편함을 상쇄·만회할 수 있도록 사용자 편의성 측면에서, 내외부 메일/자료교환체계에서 외부에서 내부로 자료교환 시 '내부메일 이동' 기능, 내부에서 외부로 자료반출 시 파일 자동 복호화 기능개선 등을 통해 편리성도 고려해야만 한다. 종합하면 성능이 업그레이드된 최신 이메일 솔루션, 키보드보안/모바일 OTP/암호화 프로그램 등 보안 SW 도입과 동시에, 표준기술(Non-Active X) 적용, 유관시스템 연동, 망연계 설치, 그리고 데이터 이관 및 검증 등을 거쳐 보안성 향상된 이메일시스템을 구축하여 중요자료가 외부로 유출되지 않도록 보호대책을 강화하고자 한다.

2. 이론적 배경

신규 내외부 메일/자료교환체계를 구축함에 있어 요구성능을 만족시키고, 기존 시스템 운영환경과도 호환성이 보장되는 솔루션을 적용할 수 있도록 다음과 같이 OTP를 활용한 다중인증 이메일시스템이 필요하다.

2.1 신규 메일/자료교환체계 적용 방식

내외부 메일/자료교환체계의 보안강화를 위해 보안시스템 기반 파일전송 기능, 대용량 파일 암호화 기능 등을 적용하여, 사용자가 자료 반출시 임의로 승인권자를 변경하지 못하도록 1차/2차 승인권자 자동설정, 동일계정으로 로그인 될 경우 세션이 자동 종료되는 기능, 첨부파일 확장자 위변조를 탐지하여 업로드를 방지하는 기능과 키로깅 방지 보안프로그램(가상키보드), 다단계 인증 적용을 위한 보안프로그램(OTP), 자료 열람시 보안강화를 위한 보안메일(메일암호화) 적용 및 열람횟수를 제한하도록 구현하여 보안 취약요소를 제거할 수 있다.

내부망의 주요 Data를 보호하기 위하여 인터넷망과 네트워크를 물리적으로 완전히 분리하여 외부 접근 자체를 원천적으로 차단하여야 한다[2]. Fig. 1에서는 물리적으로 망분리되어 있는 네트워크 구성 내에서 구현하고자 하는 내외부 메일/자료교환체계의 목표구성도이다. 내외부 메일/자료교환체계는 망연동을 통하여 내외부 자료전송이 이루어지도록 하는 구조로 이루어진다.

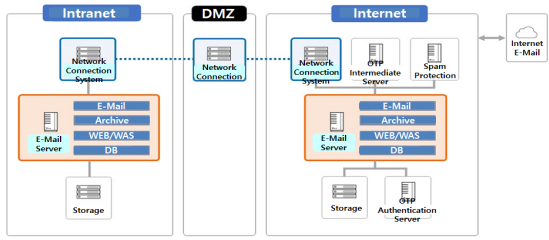

Fig. 1. Target system configuration diagram

2.2 유관시스템 연동 설계

보유한 인트라넷 서버를 해킹으로부터 보호할 수 있는 강력한 방법은 인터넷과 인트라넷을 물리적으로 분리하는 것이다[2]. 물리적으로 분리된 네트워크상에서 내부망의 자료를 외부로 안전하게 전송하기 위하여 여러가지 보안대책이 필요하다. 먼저 Fig. 3에서 보는 바와 같이 내부망에서 인터넷망으로 보내기 위한 메일 및 자료는 부서장의 승인을 받아야 전송되며, 특정 경로에 파일을 업로드 후 망연계에서 해당 파일을 가져갈 수 있도록 설계하여야 한다. 망연계에서는 해당 파일을 망전송 후 결과값을 다시 DB에 업데이트하는 방식이다. 연계구조는 '내부망 메일서버 ↔ 내부망 망연계서버 ↔ 망연계 ↔ 인터넷망 망연계서버 ↔ 인터넷망 메일서버'처럼 구성되어 있다. 인사DB 조직정보, SSO(Single Sign On) 서버, 포털, 전자문서 결재시스템, 메신저 등 내부 업무시스템과의 연동을 위하여 Table 1과 같은 연계 API를 통해 연계작업을 필요로 한다.

Table 1. System linked API

System	Linked API	Linked Contents
HR DB System	HR info. synchronization processing API	· Linkage between system & HR / Org. info. · Org. chart synchronization by batch process job · HR info. linkage / Group & private account
Business System	HR info. synchronization processing API	· User Info. / Org. chart linkage
SSO Server	SSO linkage	· Automatic authentication by SSO linkage · Automatic E-mail log-in by SSO linkage · Portal system log-in〉SSO server〉E-mail system log-in linkage
Portal System	E-mail linked API	· E-mail info. request API provision (# of unread E-email cases indication in portal main screen. · Linkage between posting of portal and E-mail system) · Send E-mail relay processing by SMTP (Simple Mail Transfer Protocol)
Messenger System	E-mail linked API	· Alarm for E-mail receipt confirmation · Pop-up display for read E-mail
Other Systems	SMTP	· Send E-mail relay processing by SMTP (Simple Mail Transfer Protocol)

2.3 키보드보안/OTP/암호화 등 보안기술

비인가자의 접근통제를 강화하기 위해서는 사용자 인증방식(OTP 인증)과 키보드보안 프로그램 등 보안 SW을 필수적으로 도입하여 위협요소를 제거하여야 한다.

먼저 OTP 인증 기술을 적용하기 위하여 OTP 인증서버, OTP 중계서버, OTP 모바일 앱 도입이 필요하다. 특징으로 시간동기방식, Multiple 인증방식을 제공하며, 통합인증 구현(WEB, CPN, VDI, 서버로그인 접근제어, 계정관리, DB접근 등) 인증 관련 컴플라이언스를 준수한다. 외부공격에 대한 안정성 확보를 위해 데이터 암호화, 통신구간 암호화 및 국정원 검증필 암호화 모듈이 적용된 인증수단을 도입하여야 한다.

공개키 기반 구조(Public Key)에서는 Fig.2에서 보는 바와 같이 암호화를 통하여 전송구간에서 시도하는 해킹을 무력화하여야 한다. Non-Active X 및 Non-Plugin 키보드 보안 기술 적용 및 터널링기법(E2E)으로 키보드입력 시점부터 서버 도착 시점까지 전체구간의 End-to-End 보안이 가능하다. 또한 키로깅, 캡쳐, 메모리 해킹, 네트워크 스니핑 등 다양한 키보드 해킹을 방지하고, 고속 Polling, BHO, 디버그 레지스터리 변조, Activity/Elite 등 키로거 대응이 가능하다. 다양한 OS와 멀티 브라우저를 지원한다[4].

Fig. 2. Keyboard security application

2.4 표준기술(Non-Active X)

Active X는 인터넷의 각종 서비스를 이용할 때 필요한 프로그램을 자동으로 편리하게 설치해 주지만 해커들의 악성코드 배포경로로 악용될 소지가 많아 보안에 매우 취약하다. 브라우저에 종속되지 않고 플러그인 방식 대신 웹에서 해당 프로그램을 실행하여 보안취약점을 제거할 수 있는 표준기술(Non-Active X) 적용이 필요하다.

Table 2에서 보는 바와 다양한 운영체제와 웹브라우저 환경(IE, Chrome, FireFox 등)에서 이용할 수 있어야 한다. IE11 기준으로 개발되어 별도의 호환성 설정없이 사용할 수 있도록 구현되어야 한다.

Table 2. Provide a variety of usage environment

Class	Operation Environment
OS	Windows, MacOS, Android, iOS
Web Browser	Internet Explorer, Edge, Chrome, FireFox, Safari, Opera

3. 적용결과

기술자료 유통 시 내외부 메일/자료교환체계 보안 강화가 필요해짐에 따라 '부서장 결재선 강화', '반출 메일 암호화 설정', '다단계 로그인 인증 절차 도입' 등 보안취약점 및 위해요소 제거를 추진하였다. 이밖에도 성능이 업그레이드된 최신 이메일 솔루션, 키보드보안/모바일 OTP/암호화 프로그램 등 보안 SW 적용, 표준기술(Non-Active X) 적용, 유관시스템 연동, 내외부 망연계 등을 통해 보안강화 및 기능개선을 하였다.

3.1 신규 메일/자료교환체계 연계로 보안강화

내부망에서는 인사DB에서 주기적으로 자동연동된 사용자 정보를 가지고, 포털계정으로 접속하면 SSO 통합인증을 통하여 내외부 메일/자료교환체계에 접속되어 메신저 및 포털시스템상에 메일 수신현황 또는 결재승인 알림이 표시되도록 연동하였다.

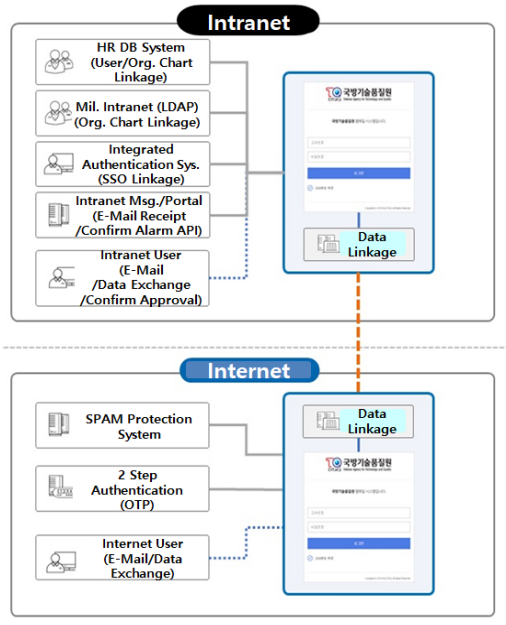

Fig. 3. E-mail / Data exchange system diagram

인터넷망에서는 Fig. 3과 같이 스팸메일차단시스템을 운영하여 유해성 메일을 필터링할 수 있도록 하였고, 메일 보안사고의 발생을 예방하고자, 2단계 인증수단인 모바일 OTP를 도입하여 비밀번호 유출, 무차별 대입공격(비밀번호 해킹) 등 시도가 발생하더라도 다중인증 체계를 구축하여 안전하게 메일시스템에 로그인할 수 있도록 보안을 강화하였다. 인터넷망에서 획득한 자료와 외부메일 수신자료는 내외부 메일/자료교환체계를 통하여 손쉽게 내부망으로 자료를 이동할 수 있도록 편의성을 향상시켰다.

국방기술품질원 사내 인터넷PC에서 메일시스템에 접속하기 위해서는 1단계로 사번/비밀번호 인증을 거친 후에 Fig. 4와 같이 모바일을 통한 2단계 OTP 인증을 받아야만 접속할 수 있도록 구축하였다.

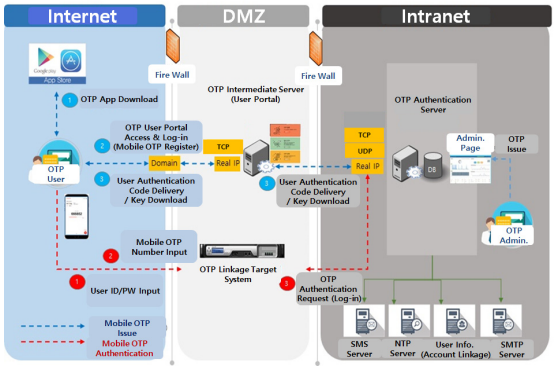

Fig. 4. OTP authentication network

3.1.1 내부망 웹메일 보안기능 강화

첫째, 인터넷 메일 및 기술자료 발송 시 자동으로 DRM(Digital Right Management, 디지털콘텐츠의 저작권을 보호하는 기술)이 해제되는 복호화 기술을 적용하여 DRM파일에 별도의 복호화 작업을 할 필요 없이, 암호화된 파일 그대로 첨부하여 발송시킬 수 있도록 사용자 편의성을 향상 시켰다. 이때 암호화는 PKI 및 DRM 방식을 적용하여 저장 및 전송되게 한다[5]. 둘째, 인터넷 메일 수신 시 내부망에서 본문 이미지화 변환 및 원문 미리보기 기능을 통해 외부 메일을 직접 열어보지 않더라도 미리 내용을 확인할 수 있게 되었다. 셋째, 내부망에서 인터넷망으로 메일 발송 시 2단계 인증(1차 결재자 및 2차 결재자 승인)을 통한 외부메일 송신으로 보안 절차를 단계적으로 강화하였다. 또한, 결재자의 보안성 검토 확인 기능이 추가되어 결재 승인이 이루어진 후 망연계를 통해 인터넷망으로 메일이 전송되도록 하였다. 넷째, 내부망에서 인터넷망으로 메일 발송 시 보안메일 및 대용량 첨부파일의 암호설정 기능을 추가하여 보안을 강화하였다.

3.1.2 인터넷망 웹메일 보안기능 강화

첫째, 2단계 인증(ID/PW (1단계), OTP (2단계) 인증)을 통해 로그인하도록 하여 인증 보안을 강화하였다. 이는 로그인시 ID/PW 외에 '일회용 인증번호(OTP)'를 같이 입력해야 로그인할 수 있는 이중 보안서비스로, ID/PW가 타인에게 노출되거나 이메일 계정이 해킹되어 탈취 비밀번호를 입력하여 접속시도를 하여도 메일계정 소유자의 휴대폰으로 전송되는 '일회용 인증번호(OTP)'를 모른다면 무단접속 불가하므로 강력한 로그인 인증수단을 제공하였다[6].

둘째, 메일 로그인 시 키보드보안을 통해 입력 시 보안을 강화하였다. 셋째, 인터넷에서 수신된 메일을 내부망으로 바로보내기 기능을 통하여 망분리 환경에서의 편리한 메일 사용 환경을 제공하였다. 넷째, 스팸/해킹 메일 발견 시 메일시스템 관리자에게 해당 메일이 바로 신고되도록 기능을 구현하였다.

3.2 유관시스템 연동구현을 통한 편리성 향상

인사DB 조직정보, SSO(Single Sign On) 서버, 포털, 전자문서 결재시스템, 메신저 등 내부 업무시스템과의 연동 구현을 위하여 Table 1과 같은 연계 API를 통해 연계작업을 수행하였다.

3.2.1 인사 DB 연동

내부망과 인터넷망 간 조직도 정보/사용자 계정 정보/결재자 정보를 주기적 배치처리(Batch Job Process)를 통하여 변경 사항을 정기적으로 처리되도록 하였다. 부서의 상위그룹 코드 및 부서명, 사용자 정보(직급, 이름, 부서 등) 등을 업데이트하기 위해 망연계 간 사용자 데이터 파일로 전송하는 구조이다.

3.2.2 SSO(Single Sign On) 연동

회사의 업무시스템은 업무 성격에 따라 다양한 웹 서비스를 제공하고 있다. 사용자들은 업무 처리를 위하여 여러 업무시스템을 접속할 때마다 서로 다른 방법으로 인증을 하고 있다. 이러한 불편한 점을 해결하기 위해서 포털에 SSO 기반의 인증체계를 도입하여 한 번의 포털 로그인으로 여러 업무시스템에 자동 로그인이 되도록 보안성 및 업무 효율성을 향상시켰다[3]. 포털에 로그인한 후 메일 링크버튼을 클릭 시 메일로 자동 로그인 처리되도록 하였다. SSO 인증 실패 시에는 메일 로그인 페이지로 이동되도록 하였다.

3.2.3 결재시스템, 포털 연동

결재시스템 및 포털 메인화면에 미확인 메일 건수 확인 기능, 게시판에서 메일보내기 기능을 제공하였다. 신규/미확인 메일 목록 제공 기능, 메일 목록 클릭 시 해당 메일보기 페이지로 팝업 제공 기능, 결재시스템의 공문 발송 메뉴 및 포털시스템의 게시판 메뉴에서 바로 메일 보내기 기능을 제공하여 사용자 편리성을 향상시켰다.

3.2.4 메신저 연동

사내 메신저에서 메일쓰기 바로가기 버튼 클릭 시 해당 페이지로 이동 기능, 신규 메일 수신 시 메신저 알림 팝업 기능, 메신저 알림 팝업 클릭 시 해당 메일보기 페이지로 이동 기능을 제공한다.

3.3 표준기술(Non-Active X) 적용

Active X 컨트롤을 사용하지 않는 드래그-드랍(Drag & Drop) 방식으로 파일을 첨부할 수 있도록 개선하여 보안에 취약한 Active X를 사용하지 않게 되어 보안 안전성을 확보하고, 표준기술 적용으로 다양한 이용환경을 제공받을 수 있게 되었다.

4. 결론

국방기술품질원 직원 내외부 메일/자료교환체계에 최신 성능을 보유한 강화된 보안기능 및 표준기술 적용으로 보안 위협요소 제거 및 업무환경 개선에 도움이 되고자 하였다. 제안된 신규 내외부 메일/자료교환체계의 구축으로 기술자료 반출시 첨부파일 암호화 설정과 열람 횟수 제한 기능을 제공하여 '안전메일' 기반을 마련하게 되었다. 개인인증/OTP로 허가된 사용자만 메일시스템에 접속하도록 보안을 강화하여 비인가자의 접속을 원천적으로 차단하였다. 또한, 메일 발송시 DRM 자동 복호화 적용으로 업무 효율성을 제고하는 등 사용자 편리성 측면에서도 개선이 이루어져 작업속도 향상 및 업무환경 개선에 이바지하게 되었다.

새로운 보안강화 기능 도입으로 인하여 시급한 보안 위협요소는 제거하였다. 하지만, 아무리 보안시스템을 강화하여도 사회공학적 기법을 활용한 악성메일 유포에 유연하게 대비하기 위해서는 국방기술품질원 차원의 '해킹메일신고 대응훈련'을 정기적으로 실시하여 출처가 불분명한 메일은 열람하지 않고 '신고'할 수 있도록 지속적

인 보안교육이 병행되어야 한다. 향후 발전방안으로는 서버 이중화 구성을 통하여 보다 안정적인 서비스를 제공하고 사이버공격으로부터 중요 업무자료가 유출되지 않도록 보안관제시스템과 연계하여 중앙에서 집중 보안관제하여 자료유출 사고를 방지할 수 있도록 발전시켜 나갈 계획이다.

References

[1] D. H. Choi, S. J. Kim, D. H. Won, "A technology analysis of One-Time Password and standardization trend", KICS, Vol.17, No.3, pp.12-17, Jun. 2007.

[2] Y. S. Han, J. S. Kim, "Data Exchange System Implementation for Data Transmission between Physically Disconnected Networks", Korea Information Processing Society, Vol.17, No.2, Nov 2010.

[3] W. S. Lee, "A Study on SSO (Single Sign On) using the standard API for the public institutions", Dept. of Computer Eng. Sungkyunkwan University, Apr 2015.

[4] G. O. Baik, C. H. Lim, J. G. Shon, "A Virtual Keyboard System for Preventing Keylogging", Journal of Security Engineering, Vol.7, No.4, pp.320, Aug 2010.

[5] S. S. Shin, K. H. Han, "A Implement of Web-Mail System based on Intranet", Journal of the Korea Academia-Industrial cooperation Society, Vol.12, No.5, pp.2346-2352, Nov 2011.

[6] S. H. Seo, C. Y. Choi, H. K. Choi, "Mobile Devices based OTP System for Two-Factor Authentication Services", The Korean Institute of Communications and Information Sciences, pp.133-134, 2012.

심 호 섭(Hosup Shim) [정회원]

- 2001년 2월 : 홍익대학교 금속재료공학과 (학사)
- 2002년 3월 ~ 2003년 8월 : 한국특허정보원 사원
- 2007년 8월 : 미국 미주리대학교 MBA (경영학석사)
- 2011년 3월 ~ 현재 : 국방기술품질원 연구원

〈관심분야〉
정보경영, 정보보호, 정보통신

박 만 춘(Manchun Park) [정회원]

- 1993년 2월 : 충남대학교 전산학과 (학사)
- 2013년 2월 : 한성대학교 국방경영학과 (석사)
- 1993년 4월 ~ 현재 : 국방기술품질원 연구원

〈관심분야〉
무기체계 SW, SW 품질관리, 테스팅