KR Maritime Cyber Security

News from KOREAN REGISTER

Mar 2019

Vol. 011

한국선급 활동

- 한화시스템과 사이버보안 및 ICT 기자재 공동연구에 대한 MOU 체결
- 씨드젠과 KR 사이버보안 e-learning 교육센터 운영에 대한 MOU 체결

실 사례로 살펴보는 OT 시스템 침투테스트

사이버 위협의 이해(OWASP Top 10)

모바일 보안 정책 수립 가이드라인

용어 설명

한국선급 활동

● 한화시스템과 사이버보안 및 ICT 기자재 공동연구에 대한 MOU 체결

한국선급과 한화시스템은 3월 14일 한화시스템 서울사업장에서 하태범 한국선급 연구본부장과 정석홍 한화시스템 사업본부장 등 양사 관계자가 참석한 가운데 '특수선용 사이버보안 및 ICT 기자재 공동 연구'를 위한 양해각서(MOU)를 체결했다.

이번 협약에 따라 양사는 한국선급의 사이버보안 인증 분야 역량과 한화시스템의 함정 시스템 통합 역량 및 군 통신망용 보안 솔루션 개발 경험을 바탕으로 특수선에 적용 가능한 사이버보안 규칙을 공동으로 연구한다. 또한 해사분야 맞춤형 보안 솔루션 개발을 통해 신규 사업 기회를 발굴하고, 전문 인력 양성, ICT 기자재 활용 부문 등에서도 협력해나갈 예정이다.

하태범 한국선급 연구본부장은 "한화시스템과의 공동 연구를 통해 선박 사이버보안 인증 역량을 한층 강화해나갈 것"이라고 하며 "앞으로 세계 해사업계에서 기술 리더십을 더욱 공고히 할 수 있을 것으로 기대한다"고 말했다

한화시스템은 종합 방산전자 전문기업으로서 함정의 두뇌에 해당되는 전투체계를 30여년간 국내 함정 및 잠수정 80여척에 성공적으로 공급하며, 우리 해군의 전력증강에 기여하고 있다. 또한 4차 산업혁명 기술 역량을 입증하는 무인 잠수정 및 무인 수상정 등 미래 해양무인체계 기술 및 장비를 개발하고 있으며, 군 통신망 전용 보안 솔루션을 제공하고 있다.

● 씨드젠과 KR 사이버보안 e-Learning 교육센터 운영에 대한 MOU 체결

한국선급은 3월 12일 정보보안 서비스 전문기업인 ㈜씨드젠과 사이버보안 이러닝(e-Learning) 교육센터 운영을 위한 양해각서(MOU)를 체결했다.

이번 협약 체결을 통해 양사는 사이버보안 e-Learning 교육센터 운영, 선박 사이버보안 온라인 교육 콘텐츠 개발 및 제공, 사이버보안에 대한 상호 기술자료 및 정보 교환 등 다양한 분야에서 협력하기로 하였다.

이날 협약식에서 김대헌 한국선급 디지털기술원장은 "정보보호 컨설팅 및 교육 서비스에 특화된 씨드젠과의 협약 체결을 통해 고객에게 보다 전문적인 서비스를 제공할 수 있을 것으로 기대한다"고 하며 "앞으로도 한국선급은 변화하는 산업 환경과 고객의 니즈에 맞춰 사이버보안 관련 기술 경쟁력을 강화하기 위해 노력할 것"이라고 밝혔다.

이번 MOU 체결을 통해 한국선급은 본부에서 진행하는 집체 교육과 별도로 온라인 교육을 필요로 하는 한국선급의 고객들에게 정보보호 일반 과정 및 심화 과정을 제공한다. 사이버보안 온라인교육은 한국선급 KR ACADEMY의 링크를 통하거나, KR 사이버보안 e-Learning 교육센터 (kr.islearning.kr) 를 통해 직접 신청할 수 있다.

씨드젠은 개인정보 및 정보보호 컨설팅, 정보보안 교육, 솔루션 개발, 정보보안 연구 등의 사업을 수행하는 정보보안 전문업체이며, 공공기관 및 산업분야의 400여개 기업을 대상으로 ISO 27001 및 정보보호 컨설팅을 수행한 바 있다.

실 사례로 살펴보는 OT 시스템 침투테스트

● 해운 분야를 위한 OT 시스템 침투 테스트의 필요성

국제 해운업계가 발표한 'Guidelines on Cyber Security onboard Ships(Rev.3)'에 따르면 선박은 다른 IT 시스템과 동일한 유형의 사이버보안 문제를 겪고 있다. 이 자료에는 선박의 IT 시스템 보안을 위한 규칙 및 지침이 포함되어 있으며, 올바른 절차를 따르지 않을 때 어떤 일이 발생하는지에 대한 예를 소개한다. 이 사례는 과거 배와 항만에서 발생한 사이버보안 사고이며 지금까지 공개적으로 드러나지 않은 사례이다.

특별히, 기존의 물리 보안에서 자주 언급되는 현안들이었던 해적, 화물 분실/탈취, 밀항/난민 등의 물리적 요인부터 시작하여 최근 새롭게 검토하고 있는 스마트 선박(Smart Shipping)에 적용되는 IoT, Embedded System 및 다양한 사이버 자산에 대한 Hacking까지 위협 범위가 넓어지는 양상이다.

이러한 변화 속에서 많은 선박 및 해양 쪽 산업 시설의 제어 시스템에서도 이러한 위협을 사전에 예방하고, 실제 침투 테스트(Pen-Testing)을 통해서 이러한 사이버 위협을 사전에 진단하고 대응하고자 하는 많은 기업과 기관들이 계속 증가되고 있다.

● O/T 진단 및 Red Teaming Project의 필요성

항만 및 선박에 대한 이해를 바탕으로 운영 환경(Operation Zone)에서 보안 점검이 수행되는 Red Teaming 프로젝트가 있다. Red Teaming 평가는 회사 내 보안팀에게 실제 IT 만이 아니라 OZ영역에서의 사이버 공격에 대처하는 실질적인 경험을 제공하는 데 중점을 둔다. 이러한 보안 진단 서비스를 통해 회사의 실제 운영 시스템이나 비즈니스에 피해를 입히는 공격을 회피하는 한편, 기존 및 지능형 공격자 Tactics, Techniques and Procedures (TTPs)를 사용하여 Red Teaming Project와 사내 보안팀이 준비한 목표를 위해 다양한 방법으로 진행된다.

아래 그림과 같이 기존의 Technology 영역에 대한 보안진단을 뛰어넘어 실제 운영 환경에 대한 이해를 통한 물리 침투를 수행하며, 소셜 엔지니어링 Hacking등을 이용하여 육상 및 해상에서 업무를 수행하는 내부 직원(해기사 포함)들에 대한 공격도 함께 진행하게 된다.

.

● **선박 보안진단 체크리스트**

구분	주요내용
비인가 사용	인가된 사용자만이 클라이언트의 서비스 및 자산에 연결할 수 있다. 그러나 클라이언트는 사이버 공격을 시작하기 위한 플랫폼으로 사용될 수 있다. 이는 인증을 우회해 익명의 사용자로 인터넷에 연결하여 수행된다.
사용자 데이터 스니핑 및 네트워크 패킷 수정	공격자가 패킷을 스니핑하거나 수정할 수 있으며 다른 사용자 데이터 (아이디, 비밀번호)를 훔칠 수 있다.
맬웨어 감염	공격자는 일반 사용자를 멀웨어 페이지로 리디렉션하고 연결된 휴대전화에 멀웨어를 설치할 수 있다. 이것은 Zero-day 취약점을 이용하여 이루어질 수 있다. 멀웨어가 피해자의 휴대전화에 성공적으로 설치되면 공격자 대상의 통화나 메시지를 쉽게 알 수 있다.
서비스 중단	공격자는 네트워크를 통해 선박 임베디드 시스템 취약점을 악용하여 서비스 중단을 초래할 수 있다. 클라이언트가 구축한 IoT 플랫폼 침투에 향후 사용되면 치명적인 피해를 발생할 수 있다.
외부 네트워크에서 OT 시스템 연결	위의 시나리오에서 공격자는 중요한 시스템에 직접 연결할 필요가 없다. 이것은 IP 주소만을 사용하는 외부 네트워크를 통해 OT Zone에 연결하여 수행 할 수 있다.
OT 네트워크 연결	무선, 블루투스, RF 등을 통해 시스템에 연결한다.
GPS 신호 공격	선박의 자동 조타키를 대상으로 GPS 스푸핑과 재밍한다.

● **자동 조타기 시스템에 대한 침투테스트 시나리오**

Project Name	Hacking for Autopilot Systems, Automatic Steering System in Marine industrial area.
Nature of Business	Auto-Pilot System on Ships (Under the NDA)
Period	6 Month
Service Provided / Job Scope	Phase 1: Black Box Pen-Testing Phase 2: 4 Things to hack While Using Auto-Pilot System on Ships (Auto-Pilot Hacking Check-List)  Phase 3: 0-day attack to GPS System and Auto-Pilot system + Source code Auditing. + UART Connected to Devices and we analysis their firmware. + JTAG Connected to Devices to log in their embedded Linux system as root privilege. Phase 4: Provide Documentation + Report of Pen-Testing (White, Black Box) each one. + Security Guide line for improve their systems. + Check list for their own Embedded System on Ships system when they planned to start their services. + Video Demo and Exploit Code and H/W Testing Devices. Phase 5: Reference News.

▪ 본 기사는 (㈜ NSHC & Shield Consulting co.,ltd 허영일 대표에 의해 작성되었습니다.

NSHC SECURITY는 ICS/SCADA(OT)사이버보안 분야에서 국내 및 아시아에서 유일하게 사이버 침투테스트 수행가능한 회사이며, 랜섬웨어, APT 공격과 같은 악성코드 분석 및 산업용 기기 대상 침투테스트 및 소스코드 진단을 수행하고 있다. SHIELD CONSULTING은 사이버보안에서 요구되는 물리적 보안(CCTV, 외부자 출입, 전자기기 반입 통제, 잠금장치) 컨설팅을 제공하고 있다.

사이버 위협의 이해(OWASP Top 10)

● 사이버 위협 이해하기

사이버 위협이란, 조직 운영, 조직 자산, 개인, 기타 조직 또는 국가에 대해 사이버 시스템을 통한 무단 액세스, 파괴, 공개, 정보 수정 또는 서비스 거부와 같은 잠재적으로 악영향을 미칠 수 있는 상황이나 사건을 의미한다. (출처 : NIST SP : 800-128)

사이버위협은 ICT 기술이 발전함에 따라 자산에 미치는 영향이 변화하므로 자산의 취약점을 파악하기 위해 주기적으로 목록화 할 필요가 있다.

● 한국선급 해상 사이버보안 시스템 인증 검사항목(CS1)

204.1 위험관리 : 내부 정보기술 및 운영기술 환경에 의한 영향을 미치는 외부 환경 요인을 위협으로 식별하고 목록화하여야 한다.

● OWASP Top 10

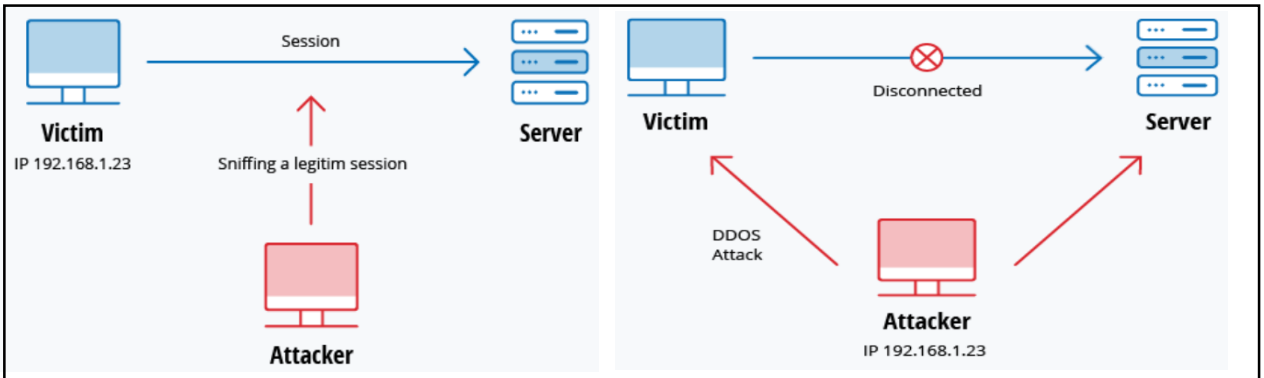
OWASP(Open Web Application Security Project)는 오픈소스 웹 어플리케이션 보안 프로젝트이다. 주로 웹에 관한 정보노출, 악성 파일 및 스크립트, 보안 취약점 등을 연구하며 웹 어플리케이션 취약점 중에서 빈도가 높고, 보안상 영향을 크게 줄 수 있는 10대 항목(OWASP Top 10)을 2004년, 2007년, 2010년, 2013년, 2017년 기준으로 발표하였다. 지난 1월 뉴스레터에 이어 '**A2 : 2017 – 취약한 인증**' 을 분석하고자 한다.

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – 인젝션	→	A1:2017 – 인젝션
A2 – 취약한 인증과 세션 관리	→	A2:2017 – 취약한 인증
A3 – 크로스 사이트 스크립팅 (XSS)	↘	A3:2017 – 민감한 데이터 노출
A4 – 안전하지 않은 직접 객체 참조 [A7 항목과 병합됨]	∪	A4:2017 – XML 외부 개체 (XXE) [신규]
A5 – 잘못된 보안 구성	↘	A5:2017 – 취약한 접근 통제 [합침]
A6 – 민감한 데이터 노출	↗	A6:2017 – 잘못된 보안 구성
A7 – 기능 수준의 접근 통제 누락 [A4 항목과 병합됨]	∪	A7:2017 – 크로스 사이트 스크립팅 (XSS)
A8 – 크로스 사이트 요청 변조 (CSRF)	☒	A8:2017 – 안전하지 않은 역직렬화 [신규, 커뮤니티]
A9 – 알려진 취약점이 있는 구성요소 사용	→	A9:2017 – 알려진 취약점이 있는 구성요소 사용
A10 – 검증되지 않은 리다이렉트 및 포워드	☒	A10:2017 – 불충분한 로깅 및 모니터링 [신규, 커뮤니티]

Ref. : OWASP Top 10 Project

● **OWASP 10대 위협 'A2 : 2017 – 취약한 인증'**

웹 애플리케이션에서는 로그인하는 대상이 사이트에 등록된 사용자가 맞는지, 아이디와 비밀번호를 이용하여 확인하는 인증 절차를 거친다. 이 인증 절차를 거쳐 사용자로 확인되면 웹 사이트에서 특정한 권한을 받는다. 또한 인증 후 페이지를 이동할 때는 로그인 상태를 유지하고, 일정 시간에 따라 접속을 초기화하기 위하여 세션을 생성한다. 그러나 인증 과정에서 결함이 발생하면 사용자의 계정 정보가 노출되고 공격자는 무차별 대입 공격 등을 통해 노출된 계정 정보로 로그인할 수 있다. 또한 세션 관리가 허술한 경우 공격자는 세션 아이디를 탈취하여 사용자의 권한을 획득하기도 한다. 공격자가 공격에 성공하면 인증 없이도 사용자 권한으로 웹 사이트의 서비스를 이용할 수 있게 된다. 아래는 세션 탈취로 인한 공격 시나리오를 나타낸다.



1. 클라이언트가 서버에 연결
2 공격자가 세션 탈취

3. 공격자가 클라이언트를 제어(DDOS 공격)
4. 공격자가 클라이언트와 서버의 연결을 끊음
5. 공격자가 클라이언트의 IP 주소로 변경
6.클라이언트의 시퀀스를 스푸핑
7. 서버는 클라이언트와 통신 중으로 생각

Ref. : https://blog.netwrix.com

취약점 확인 방법

인증과 관련된 공격으로부터 보호하기 위해서 사용자의 신원, 인증 및 세션을 관리하는 것이 매우 중요합니다.

만약 애플리케이션이 아래와 같을 경우 인증 취약점이 있을 수 있습니다.

- 공격자가 유효한 사용자 이름과 비밀번호를 가진 상태에서 계정 정보 삽입과 같은 자동화 공격을 허용합니다.
- 무차별 공격 또는 기타 자동화 공격을 허용합니다.
- "Password1" 또는 "admin/admin"과 같은 기본 암호, 약한 암호 또는 잘 알려진 암호를 허용합니다.
- 안전하지 않게 만들어진 "지식 기반 답변"과 같은 취약하거나 효과가 없는 자격 증명 복구나 비밀번호 복구를 허용합니다.
- 평문, 암호화되거나 취약한 해쉬 비밀번호를 사용합니다.(참조: A3:2017-민감한 데이터 노출)
- 다중 인증이 없거나 비효율적입니다.
- 세션 ID가 URL에 노출됩니다.(e.g., URL rewriting)
- 세션 ID를 제대로 무효화 시키지 않습니다. 로그아웃이나 비활성 기간 중에 사용자 세션 및 인증 토큰(특히 SSO(Single Sign On)토큰)이 제대로 무효화 되지 않습니다.

보안 대책

- 가능한 경우, 다중인증을 구현하여 자동화된 계정 정보 삽입, 무차별 공격, 탈취된 계정 정보 재사용 공격을 예방합니다.
- 특히 admin 계정의 경우 기본 계정 정보를 사용하여 제공하거나 배포하지 마십시오.
- 비밀번호를 생성하거나 변경할 때 최악의 Top 10000개 비밀번호 목록 이외로 설정하도록 하는 것과 같은 약한 비밀번호 검사를 구현하십시오.
- NIST 800-63 B's guidelines in section 5.1.1 for Memorized Secrets에 따라 암호 길이, 복잡성 및 순환 정책 또는 다른 최신 정책, 근거 기반 암호 정책을 조정합니다.
- 계정 열거공격에 대한 대비로 모든 결과에 대해 동일한 메시지를 사용하여 등록, 계정 정보 복구, API 경로를 강화하십시오.
- 로그인 실패에 대한 제한이나 시간 연기를 하십시오. 모든 실패에 대해 로그를 남기고 계정 정보 삽입, 무차별 공격, 다른 공격들이 탐지되면 관리자에게 알람이 오도록 설정하십시오.
- 로그인 이후에 예측 불허한 무작위 세션 ID를 생성하는 서버 측의 안전한 내장 세션 관리자를 사용하십시오. 세션 ID는 URL에 없어야 하며, 매우 안전하게 보관되어야 하고 로그아웃, 유휴 및 절대 시간 초과 이후 무효화되어야 합니다.

모바일 보안정책 수립 가이드라인

● **모바일 보안 정책의 필요성**

스마트폰과 같은 모바일 장비는 개인과 기업에서 활용도가 매우 높고 24시간 인테넷과 연결되어 있는 특성과 휴대성으로 새로운 보안 위협에 항상 노출되어 있다. 특히 무선랜(Wi-Fi) 및 블루투스 기능을 이용한 공중 무선랜 및 사설 무선랜 접속환경은 악성코드 유입이나 해킹 공격이 매우 용이하다. 따라서 개인적인 피해뿐만 아니라 기업정보의 유출을 방지하기 위해서는 모바일 보안 정책이 필요하다. 모바일 장비의 사용, 물리적 보호, 접근제어(VPN 포함), 암호화, 바이러스 정책, 내부 네트워크와 연결 보안정책에 대해 관리하여야 하며, 모바일 장비 사용자에 대한 보안교육을 정기적으로 실시하여야 한다. 또한 원격 작업 시 보안정책과 절차를 수립하여 공공망등을 경유하여 내부 네트워크 접속 시의 적절한 식별, 인증, 접근통제 대책을 마련하고 완료 시 접근권한, 장비 등을 회수 및 관리하여야 한다.

● **한국선급 해상 사이버보안 인증 검사항목(CS1)**

모바일 보안 정책(215.1) : 회사는 회사 모바일 기기 및 직원 소유의 모바일 기기 사용을 통제하기 위한 보안정책을 수립하야여 한다.

모바일 기기 관리(215.2) : 회사는 회사에서 이용 가능한 모바일 기기와 기능을 정의하고 사용 중인 기기를 식별하여야 한다.

무선 AP 접속 통제(215.4) : 회사는 임직원이 사용하는 모바일 기기가 악성코드 감염 또는 해킹에 악용되는 비인증 액세스 포인트(Rogue AP)에 접속하는 것을 예방하여야 한다.

● **스마트폰 사용자 수칙 [출처 : 한국인터넷 진흥원]**

1. 의심스러운 어플리케이션 다운로드 하지 않기
2. 신뢰할 수 없는 사이트는 방문하지 않기
3. 발신인이 불명확하거나 의심스러운 메시지 및 메일 삭제하기
4. 비밀번호 설정 기능을 이용하고 정기적으로 비밀번호 변경하기
5. 블루투스 기능 등 무선 인터페이스는 사용할 때만 ON
6. 이상증상이 지속될 경우 악성코드 감염여부 확인
7. 운영체제 및 백신프로그램을 항상 최신 버전으로 업데이트 하기
8. 스마트폰 플랫폼의 구조를 임의로 변경(탈옥등을 통한)하지 않기

● 모바일 보안 체크리스트 (예시)

구분	점검항목	결과(O/X)
모바일 단말기 보안	모바일 단말기 내 중요정보가 유출되지 않도록 단말기 잠금 기능을 상시 적용한다.	
	모바일 단말기의 취약성(예: 바이러스 및 악성코드의 취약성)을 주기적으로 점검하며, 운영체제 및 백신 프로그램을 항상 최신 버전으로 유지한다.	
	의심스러운 응용프로그램의 다운로드, 발신인이 불명확한 메시지 및 메일의 삭제, 신뢰성이 떨어지는 사이트의 방문을 금지한다.	
	모바일 단말기 접속제한을 위해 MAC이나 IP 통제 등 모바일 단말기 보호대책을 적용하며 모바일 단말기의 도난, 분실 시 지체없이 OOO팀으로 신고한다.	
	PC와 모바일 단말기 간의 동기화 시 악성코드가 모바일 단말기로 옮겨질 수 있으므로, PC에도 백신 프로그램을 설치하고 정기적으로 바이러스 검사를 수행한다.	
	모바일 단말기 내부운영 시스템의 설정을 임의로 개조하거나 플랫폼 구조를 임의로 변경하여 사용하지 않는다	
	모바일 단말기를 통한 업무처리 시 중요한 정보는 암호화하여 저장하며, 부득이한 경우 정보의 저장이 이루어지지 않도록 업무처리 종료 후 정보를 삭제한다.	
	서비스 사용자는 무선 통신 인터페이스의 이용 시 다음과 같은 보호 조치를 유지한다. 1. 블루투스 기능과 같이 안정성이 결여된 무선 인터페이스는 사용 시에만 활성화 하고, 업무처리 종류 후 비활성화 한다. 2. 신뢰할 수 없는 장소에서 무선망을 통한 결제, 기밀자료 열람 등 민감한 서비스를 이용하지 않는다. 3. 모바일 단말기에서 웹을 통하거나 응용프로그램 방식으로 민감한 서비스를 이용하는 동안 다른 프로세스 실행을 금지하고, 테더링 기능을 제한한다.	
모바일 업무 아키텍처 보안	무선 네트워크를 통해 전송되는 정보(고유식별정보, 비밀번호, 바이오정보 등)는 암호화하여 전송하고 전송구간에서 평문으로 노출되지 않도록 처리한다.	
	모바일 업무 서버로의 비정상적인 접속이 발생하거나 비정상 패킷이 송수신될 경우, 세션 강제종료 및 해당 로그 저장기능을 구현한다.	
	모바일 단말기에서 내부 모바일 업무 서버로의 직접연결은 차단하고, 외부망과 내부망은 분리한다.	
	모바일 업무 서버는 외부망 및 접속지점에 침입차단시스템, 유해 트래픽 탐지 시스템 등의 정보보호시스템을 구축, 운영한다. 해킹 및 비인가자의 접근 차단을 위해 침입차단시스템 구축 및 운영 비정상 트래픽 상시 모니터링을 위해 유해 트래픽 탐지시스템 구축 및 운영	
모바일 응용프로그램 보안	모바일 업무 시스템 접속을 위한 인증 및 패스워드 정책은 다음의 사항을 준수한다. 1. 비밀번호 설정기능을 이용하고, 정기적으로 비밀번호를 변경한다. 2. 사용자 인증은 ID/패스워드 방식을 기본으로 하며 서비스의 중요도에 따라 공인인증서 OTP, 생체인식 등 복합인증방식을 적용 할 수 있다.	
	중요자료는 모바일 단말기에 저장되지 않도록 하며, 서버에서 편집이 불가능한 형태로 변환하여 모바일 단말기에 전송되도록 하여야 한다.	
	모바일 업무 서버의 중요 설정정보나 불필요한 정보가 소스코드에 포함되지 않도록 응용프로그램을 구현한다.	
	사용자에게 입력받은 중요정보(로그인 비밀번호 등)에 대해 입력정보가 노출 또는 유출되지 않도록 반드시 인증을 거치도록 하여야 하며, 계정 발급 현황, 접속 로그 등을 남겨야 한다.	
	모바일 응용프로그램을 개발하여 업무에 사용할 경우, 반드시 보안성 검토를 수행하여 침해사고를 예방하여야 한다.	
	모바일 응용프로그램이 중요정보 또는 개인정보 등에 접속할 경우 반드시 사용자 인증을 거치도록 하여야 하며, 계정 발급 현황, 접속 로그 등을 남겨야 한다.	

용어 설명

- **OT(Operating Technology)** : 밸브, 펌프 등과 같은 물리적 장치의 직접 모니터링 또는 제어를 통해 물리적 프로세스의 변화를 감지하거나 일으키는 하드웨어 및 소프트웨어를 의미한다. 선박에서 OT 시스템은 추진시스템, 발전 및 배전, 조타, 항해, 통신, 화물 운영 등이 포함된다.
- **Zero-day 취약점** : 컴퓨터 소프트웨어의 취약점을 공격하는 기술적 위협으로 해당 취약점에 대한 대응방안이나 패치가 나오지 않은 시점에서 이루어지는 공격을 말한다. 1-day 취약점은 패치가 발표되었지만 검증 및 여러가지 사유로 인하여 패치를 적용하지 않은 시점에서 이루어지는 공격을 말한다.
- **무차별 대입공격(Brute Force Attack)** : 사용자에 대한 계정정보를 획득하기 위하여 비밀번호로 입력 가능한 모든 문자 조합을 입력하여 사용자의 계정과 비밀번호가 일치할 때까지 대입하는 공격이다. 사용자 비밀번호와 같이 비밀번호가 특정 패턴을 이루고 있을 경우에는 대입해야 할 값의 범위를 크게 줄일 수 있다. 이 경우 사전의 단어를 조합하여 대입하는 사전공격이 사용된다. 그러므로 비밀번호 패턴을 불규칙적으로 하고 자신의 개인정보와 연계되지 않도록 하는 것이 중요하다.
- **세션 탈취(Hijacking)** : 시스템에 접근할 적법한 사용자 아이디와 패스워드를 모를 경우 공격 대상이 이미 시스템에 접속되어 세션이 연결되어 있는 상태를 가로채기 하는 공격으로 아이디와 패스워드를 몰라도 시스템에 접근하여 자원이나 데이터를 사용할 수 있는 공격이다.
- **Rogue AP** : 비인증(Rogue) 액세스 포인트는 로컬 네트워크 관리자의 명시적인 허가 없이 보안 네트워크에 설치된 무선 액세스 포인트이다. 기업의 무선 랜 환경에서는 일반 사용자가 개인적으로 설치한 무선 AP를 통해 외부나 불법 침입자가 들어와 내부 직원과 같은 자격으로 모든 자원에 접근할 수 있으므로 적절한 규제가 필요하다.

KR Maritime Cyber Security
11