소프트웨어 보안

분석 설계 SW 보안강화

2. 보안 기능

소프트웨어 보안
소프트웨어 보안

보안 기능

1. 인증 대상 및 방식

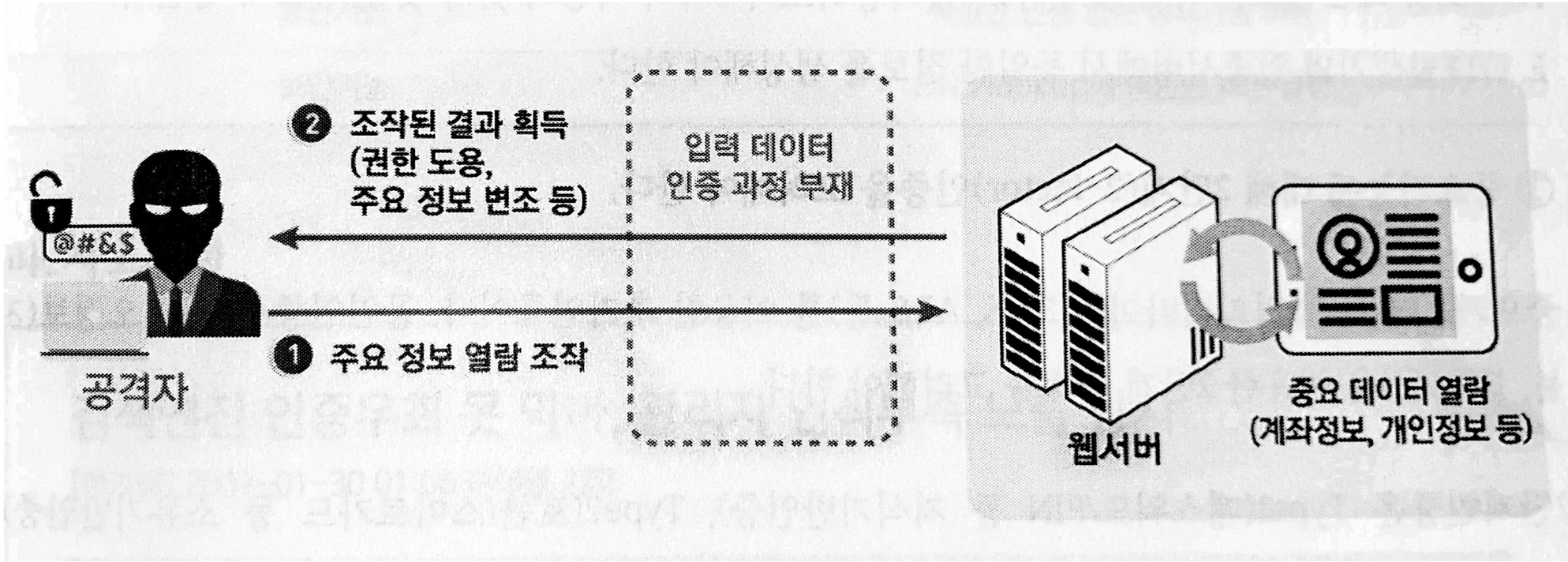
요구사항 분류	보안기능	요구사항번호	SR2-1
이름	인증 대상 및 방식		
설명	중요정보•기능과 인증방식을 정의하고, 정의된 중요정보 접근 및 중요기능 수행 허용을 위해 인증 기능이 우회되지 않고 수행될 수 있도록 설계해야 한다.		
요구사항내용	1. 중요기능이나 리소스에 대해서는 인증 후 정책이 적용되어야 한다. 2. 안전한 인증방식을 사용하여 인증우회나 권한 상승이 발생하지 않도록 해야 한다. 3. 중요기능에 대해 2단계(2-factor) 인증을 고려해야 한다.		

보안 기능

인증 대상 및 방식

취약점 개요

- 외부로 부터 중요기능이나 리소스를 요청하는 경우는 사용자 인증이 되었는지를 먼저 확인하지 않고 요청을 처리하는 경우 중요 정보나 리소스가 노출될 수 있다.



적절한 인증 없는 중요기능 허용

보안 기능

인증 대상 및 방식

소프트웨어 보안

설계시 고려사항

1. 중요기능이나 리소스에 대해서는 인증 후 사용 정책이 적용되어야 한다.
   - 분석단계에 분류된 중요기능에 대해 인증 후 사용이라는 보안 정책이 반드시 적용될 수 있도록 설계해야합니다.
   - 각각의 중요기능에서 인증을 요청하도록 구현하는 것은 쉽지 않지만, 시스템 설계시 중요기능을 분류하고 식별된 중요기능에 대해 일괄적으로 인증을 요구하도록 시스템을 설계한다. 이 경우 직접적으로 기능과 인증을 매핑시켜 처리하는 컴포넌트를 개발하거나, 인증기능을 제공하는 프레임워크 또는 라이브러리를 활용하여 중앙집중식 인증이 적용되도록 설계한다.
2. 안전한 인증 방식을 사용하여 인증우회나 권한 상승이 발생하지 않도록 해야 한다.

   인증 정보는 서버 측에 저장하는 인증이 필요한 기능이나 리소스에 접근을 시도할 때 서버에서 인증여부를 확인할 수 있도록 해야 한다.

보안 기능

인증 대상 및 방식

설계시 고려사항(계속)

2. (계속)안전한 인증 방식을 사용하여 인증우회나 권한 상승이 발생하지 않도록 해야 한다.

- 일회용 패스워드 사용시

- 일회용 패스워드를 적용하는 경우 타서비스나 시스템과의 연동이 보장되도록 설계해야 한다. 일회용 패스워드를 도입하는 경우 다음과 같은 규칙을 적용하여 설계한다.

① 일회용 패스워드는 시각정보, 이벤트정보, 질의-응답방식으로 취득한 정보를 이용해 생성할 수 있다.

② 시각정보기반의 연계정보는 특정 시간 동안만 유효하여야 하며, 이벤트/질의-응답방식을 사용할 경우에는 연계정보를 추측할 수 없도록 보호방안을 제공할 수 있어야 한다.

③ 일회용 패스워드에는 시간적 제한을 설정해야 한다.(금융영역에서는 30-60초)

④ 일회용 패스워드는 중복 및 유추가 불가능하도록 6자리 이상의 숫자 및 문자로 구성한다.

⑤ OTP발생기와 인증서버에서 동일한 정보를 생성해야 한다.

보안 기능

인증 대상 및 방식

설계시 고려사항(계속)

3. 중요기능에 대해 2단계(2-factor)인증을 고려해야 한다.
   - 중요기능에 대해서는 SMS ARS 와 같은 멀티디바이스를 이용하고 추가인증으로 공인인증서, 바이오정보(지문, 홍채 등)을 이용한 2단계 인증에 단계를 거치도록 설계하면 됩니다.
   - 2단계 인증의 경우 첫번째 유형으로 Type1(패스워드/PIN 등 지식기반인증), 두번째 유형으로 Type2(토큰/스마트카드 등 소유기반인증), 세번째 유형으로 Type3(지문/홍채 등 생체기반인증) 를 볼 수 있는데, 이중에서 2개 이상의 인증기법을 사용하도록 설계를 하는겁니다.

보안 기능

사고 사례(1)

검색엔진 인증우회 못막아, 관리자 인식부족 노출 방치

보안전문가들은 공공기관 사이트들이 로그인 절차를 갖추고 있음에도 개인정보가 노출된 것은 인증·권한확인 절차의 누락이 원인이라고 설명했다. 행정자치부처럼 비공개 문서의 내려받기가 가능했던 것도 홈페이지 내에 파일처리에 관한 인증·권한확인 절차를 두지 않았기 때문인 것으로 추정했다. 안철수연구소 여성구 전임컨설턴트는 "기술적인 측면에서 게시판의 '사용자 모드'로 내부 관리자만 접근이 가능하도록 하거나 쓰기, 수정, 보기 등의 각 단계마다 일일이 보안을 걸어 둬야 한다"며 "특히 관리자와 게시자만 볼 수 있게 만든 게시판의 경우에는 더욱 그렇다"고 말했다.

공공기관 관리자들의 개인정보 보호에 대한 인식 부족은 더 큰 문제라고 전문가들은 지적한다. 특히 노출빈도가 많은 민원게시판에는 민원인이 사실확인과 응답을 기대하며 주민등록번호와 휴대전화 번호 등을 무심코 올리는데, 이런 중요한 개인정보들을 민원접수 기관이 몇개월째 그대로 방치해둔 사례가 많았다. 개인정보보안연구소 킵스랩 백승호 대표는 "주민등록번호나 은행계좌번호와 같은 개인정보가 입력되었을 때는 다른 문자로 자동전환된다던지, 입력이 불가능하도록 하는 기술적 조치를 할 수도 있지만 개인정보 보호는 우선 관리자의 철저한 보호의지가 관건"이라고 말했다.

보안 기능

사고 사례(2)

코레일 홈피 보안 허술…비용 줄이려 보안코드 무시?

[JTBC] 입력 2016-10-12 21:42

코레일 '고객의 소리' 게시판에 글을 남기기 위해선 인증 과정을 거쳐야합니다.

이렇게 접속하는 방법을 정상 접근이라고 하는데, 코레일은 정상 접근에 대한 인증 절차만 만들고 인터넷 주소에 나타나는 고유 ID 숫자를 바꿔 접속하는 우회 접근에 대한 보안은 허술했습니다.

[보안업체 관계자 : 홈페이지를 요청하는 사람이 인증된 사람이냐를 확인해 줄 수 있는 3줄 정도의 시큐어 코딩만 들어갔어도 이런 문제가 생기지 않는데…]

인터넷 페이지가 넘어가는 전 과정과 민감정보에 보안 코드를 넣게 되면 서버의 처리 속도가 느려집니다.

보안 기능

소프트웨어 보안

2. 인증 수행 제한

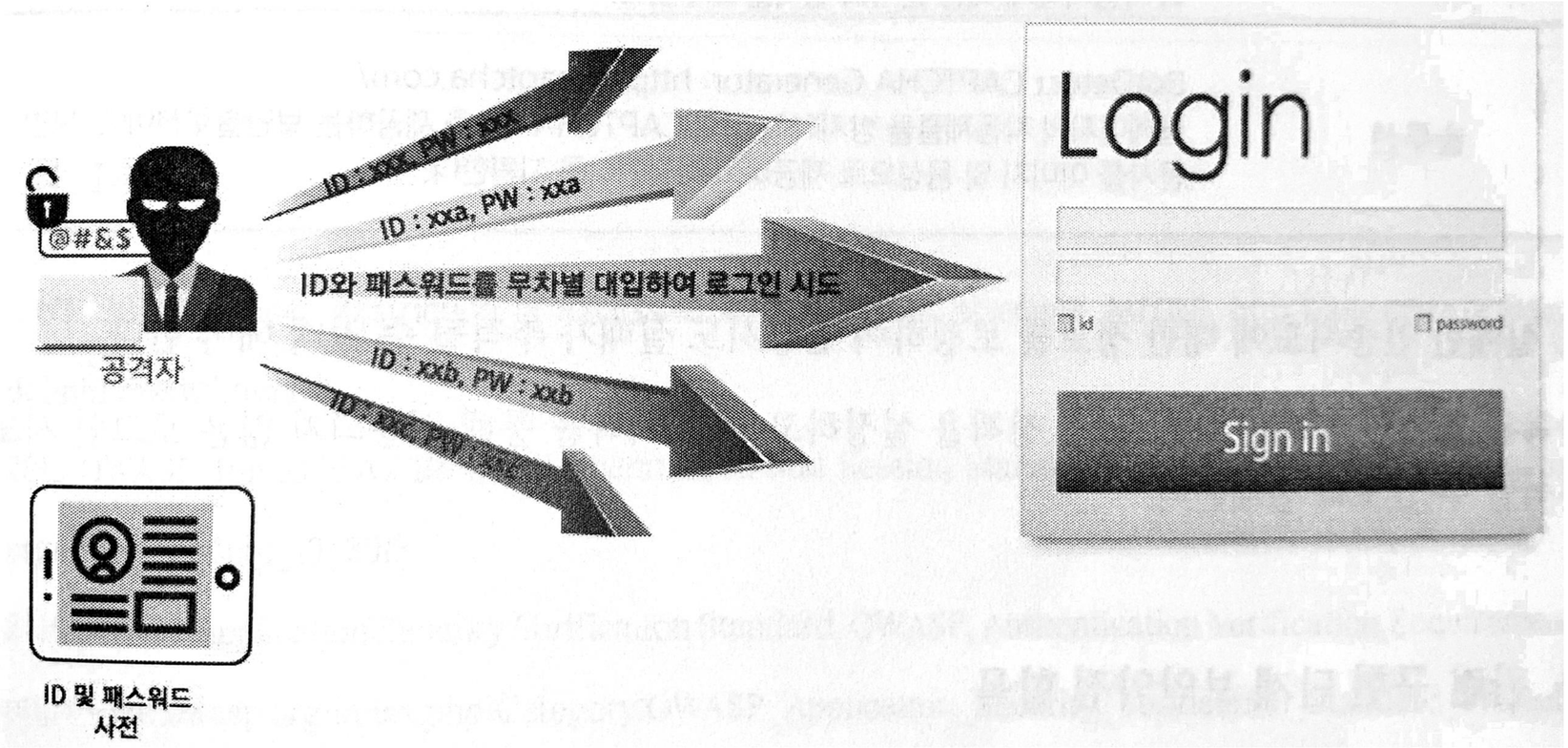
요구사항 분류	보안기능	요구사항번호	SR2-2
이름	인증 수행 제한		
설명	인증 반복시도 제한 및 인증실패 등에 대한 인증제한 기능을 설계해야 한다.		
요구사항내용	1. 로그인 기능 구현시, 인증시도 횟수를 제한하고 초과된 인증시도에 대해 인증제한 정책을 적용해야 한다. 2. 실패한 인증시도에 대한 정보를 로깅하여 인증시도 실패가 추적될 수 있게 해야 한다.		

보안 기능

인증수행 제한

취약점 개요

- 로그인 시도에 대한 횟수를 체크하지 않으면 로그인 시도 횟수가 초과되었을 때 계정에 대한 보호조치가 설정되어 있지 않은 경우 패스워드 무작위 대입공격이 시도될 수 있다.



반복된 인증시도 제한 기능 부재

보안 기능

인증수행 제한

소프트웨어 보안

설계시 고려사항

1. 로그인 기능 구현시, 인증시도 횟수를 제한하고, 초과된 인증시도에 대해 인증제한 정책을 적용해야 한다.
   - 로그인 시도횟수를 3-5번 이내로 제한하고 이를 초과하여 로그인에 실패하는 경우 추가 입력값을 요구하거나 계정잠금을 수행하도록 다음과 같은 메커니즘을 설계한다.

사용자 ID별, 세션ID별 로그인 횟수를 추적하기 위해 사용자 DB 테이블에 로그인실패횟수/계정잠금여부/마지막으로 성공•실패한 로그인 시간정보, 로그아웃한 시간정보들을 저장할 수 있도록 설계하여 일정횟수 이상 연속적으로 로그인 실패시 사용자ID와 패스워드 외의 추가적인 확인 정보를 저장하도록 한다.

보안 기능

인증수행 제한

소프트웨어 보안

설계시 고려사항(계속)

1. (계속)로그인 기능 구현시, 인증시도 횟수를 제한하고, 초과된 인증시도에 대해 인증제한 정책을 적용해야 한다.
   - 계정정보 입력시 자동입력 방지문자와 같은 장치를 마련하도록 설계한다.
   - 보안문자 이미지 생성 및 입력값과 보안문자를 비교하기 위해 다음과 같은 서비스나 솔루션의 사용을 고려할 수 있다.

자동 계정 생성 방지 기술

[CAPTCHA 기능을 제공하는 서비스 및 솔루션]

개발환경	활용가능한 서비스 및 솔루션
서비스	CAPTCHA 시스템의 일종으로 OCR 소프트웨어가 판독할 수 없는 글자이미지를 생성하여 사용자에게 해당 문자의 입력을 요구한다.
솔루션	웹페이지의 자동제출을 방지하기 위해 CAPTCHA 기능을 제공하는 보안솔루션이다. 보안 문자를 이미지 및 음성으로 제공하고 다중언어를 지원한다.

보안 기능

인증수행 제한

소프트웨어 보안

설계시 고려사항(계속)

2. 실패한 인증시도에 대한 정보를 로깅하여 인증시도 실패가 추적될 수 있게 해야 한다.
   - 반복된 로그인 실패에 대한 로깅 정책을 설정하고 로그 기록을 통해 허용되지 않은 로그인 시도를 분석할 수 있도록 설계한다.

보안 기능

인증수행 제한

소프트웨어 보안

사고 사례

유명 만화사이트, 로그인 취약점으로 개인정보 유출 위험

길민권 | 승인 2016.04.12 23:42

로그인시 팝업창에 아이디와 비밀번호 평문으로 노출

모 유명 만화사이트의 로그인 취약점으로 인해 평문 비밀번호가 그대로 노출되고 있으며 이로인해 회원들의 개인정보 유출로 이어질 수 있어 신속한 보안조치가 필요한 상황이다.

해당 취약점을 발견하고 데일리시큐에 제보한 김동채(동신대학교 정보보안학과) 제보자는 "해당 만화 사이트는 회원가입시 아이디를 요구하지만 비밀번호 입력 횟수에 제한이 없기 때문에 부르트 포스(Brute force) attack(무차별대입공격)으로 불법접근이 가능할 수 있다"며 "해당사이트에서 아이디로 사용되는 이메일 주소는 블로그나 SNS 등을 이용해 알아낼 수 있기 때문에 손쉽게 계정탈취로 이어질 수 있어 위험한 상황"이라고 설명했다.

보안 기능

3. 비밀번호 관리

요구사항 분류	보안기능	요구사항번호	SR2-3
이름	비밀번호 관리		
설명	안전한 비밀번호 조합규칙(비밀번호 길이, 허용문자 조합 등)을 설정하고, 안전한 저장 정책, 재설정 및 변경 정책, 패스워드 관리규칙(주기적 변경 등) 이 적용되도록 설계해야 한다.		
요구사항내용	1. 패스워드를 설정할 때 한국인터넷진흥원의 “암호이용안내서 " 의 패스워드 생성규칙을 적용해야 한다. 2. 네트워크를 통해 패스워드를 전송하는 경우 반드시 패스워드를 암호화하거나 암호화된 통신 채널을 이용해야 한다. 3. 패스워드 저장시, 솔트가 적용된 안전한 해시함수를 사용해야 하며, 해시함수 실행은 서버에서 해야 한다. 4. 패스워드 재설정/변경시 안전하게 변경할 수 있는 규칙을 정의해서 적용해야 한다. 5. 패스워드 관리 규칙을 정의해서 적용해야 한다.		

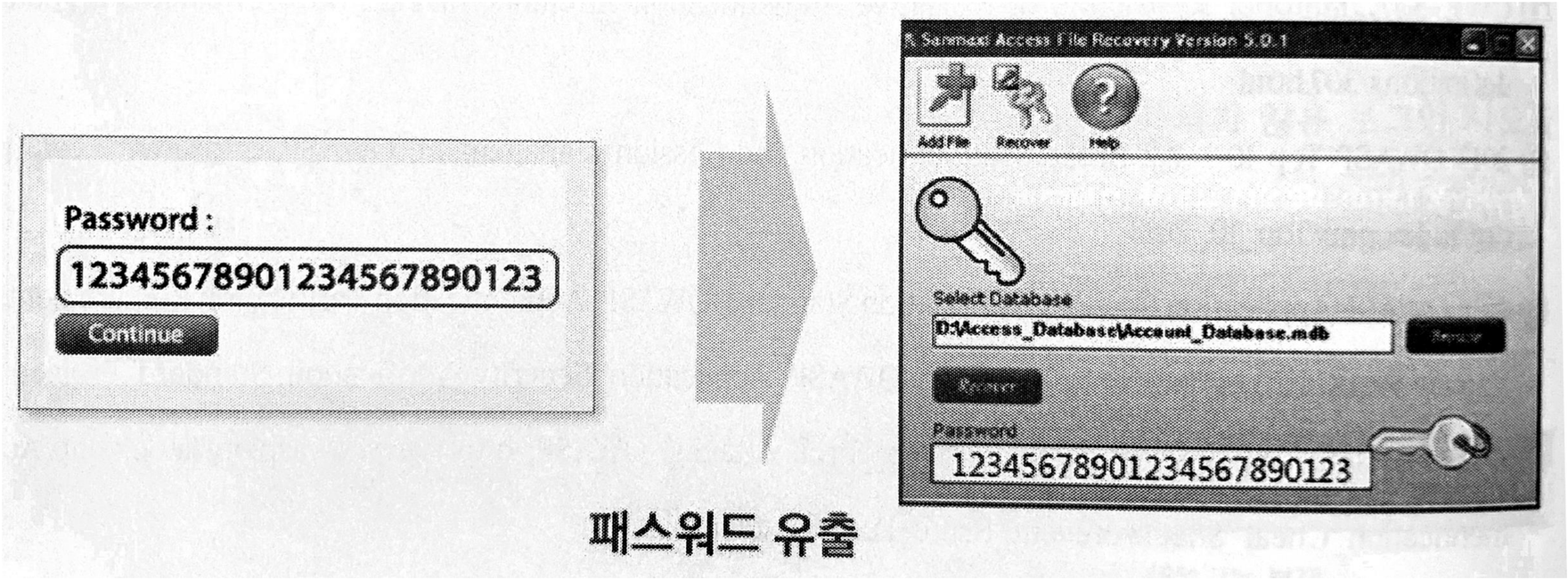
보안 기능

비밀번호 관리

소프트웨어 보안

취약점 개요

- 사례 1 : 취약한 비밀번호 사용
  - ❖ 회원가입 시에 안전한 패스워드 규칙이 적용되지 않아서 취약한 패스워드로 회원가입이 가능할 경우 무차별 대입공격을 통해 패스워드가 누출될 수 있다.



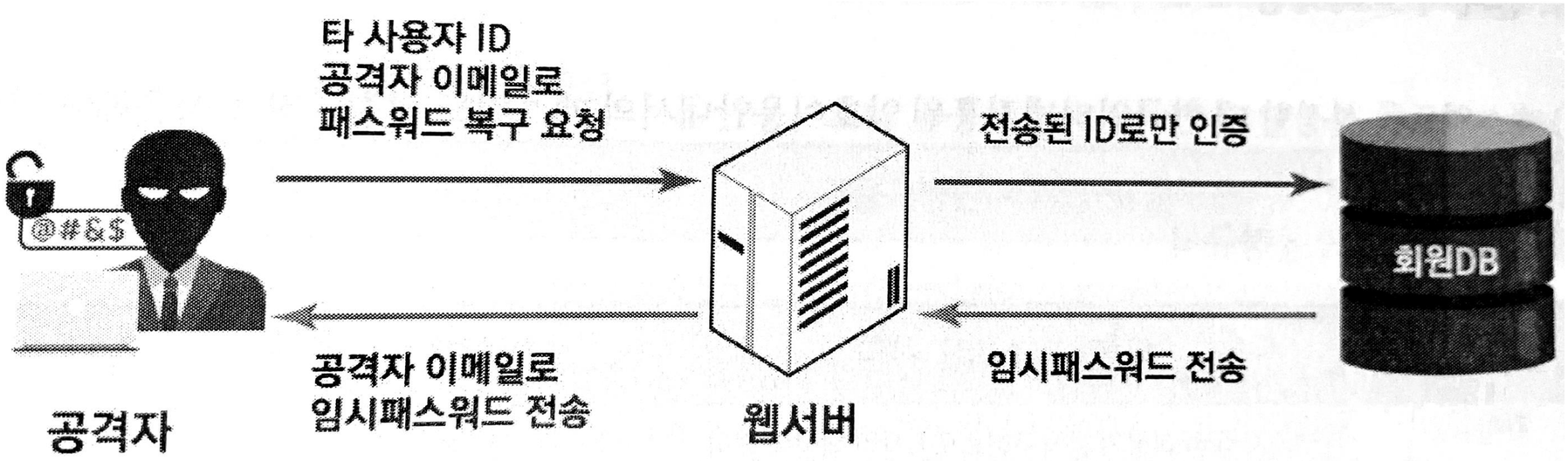
취약한 비밀번호 허용

보안 기능

비밀번호 관리

취약점 개요

- 사례 2 : 취약한 비밀번호 복구
  - ❖ 패스워드 복구 메커니즘(아이디/패스워드 찾기 등)이 취약한 경우 공격자가 불법적으로 다른 사용자의 패스워드를 획득, 변경, 복구할 수 있다.



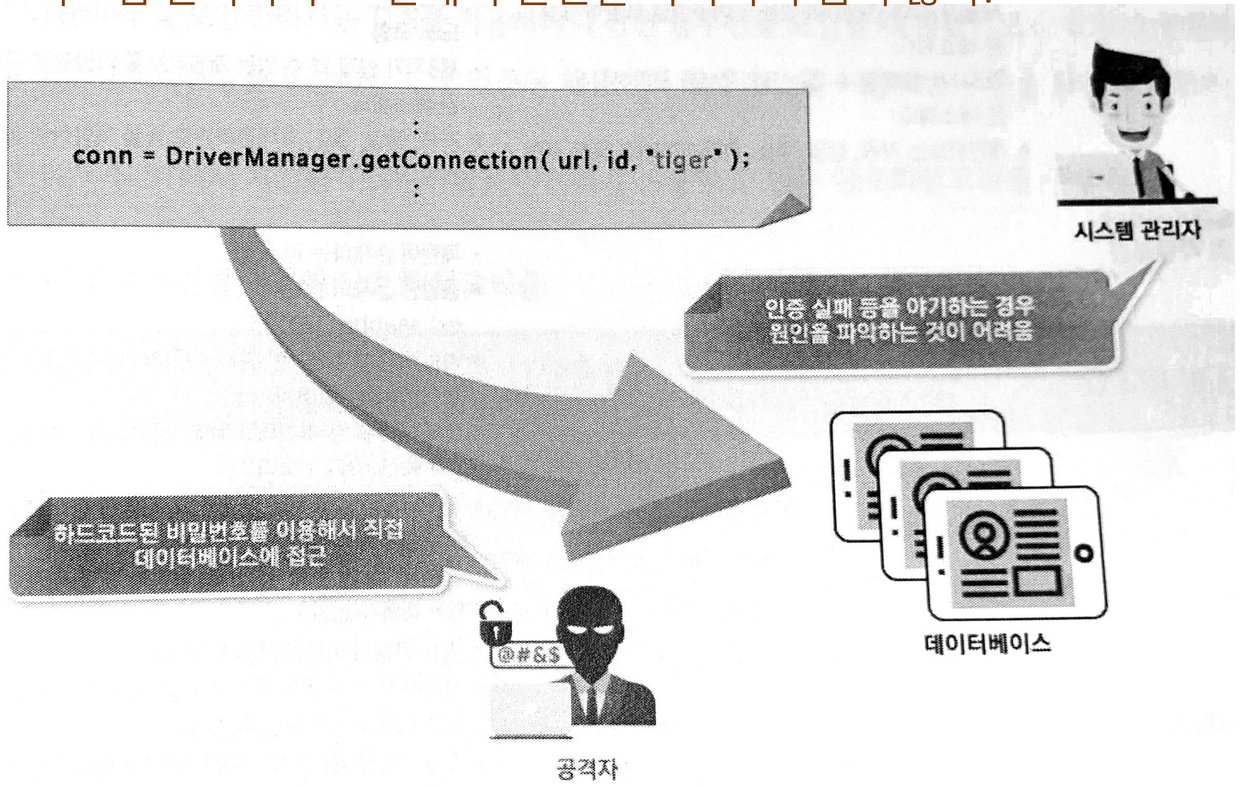
취약한 비밀번호 복구

보안 기능

비밀번호 관리

취약점 개요

- 사례 3 : 하드코드된 비밀번호
  - ❖ 프로그램 코드 내부에 하드코드된 패스워드를 포함하고, 이를 이용하여 내부 인증에 사용하거나 외부 컴포넌트와 통신을 하는 경우, 관리자 정보가 노출될 수 있어 위험하다. 또한, 코드 내부에 하드코드된 패스워드가 인증실패를 야기하는 경우, 시스템 관리자가 그 실패의 원인을 파악하기 쉽지 않다.



하드코드된 비밀번호

보안 기능

비밀번호 관리

소프트웨어 보안

설계시 고려사항

1. 패스워드를 설정할 때 ‘한국인터넷진흥원’ 암호이용안내서의 패스워드 설정규칙을 적용해야 한다.

[패스워드 설정규칙]

1. 문자구성 및 길이조건

안전한 패스워드 규칙	안전하지 않은 패스워드 규칙
• 3가지 종류 이상의 문자 구성으로 8자리 이상의 길이로 구성된 패스워드 • 2가지 종류 이상의 문자구성으로 10자리 이상의 길이로 구성된 패스워드 ❖ 문자 종류는 알파벳 대문자와 소문자, 특수기호, 숫자의 4가지임	• 2가지 종류 이하의 문자구성으로 8가지 이하의 길이로 구성된 패스워드 • 문자구성과 관계없이 7자리 이하 길이로 구성된 패스워드 ❖ 문자종류는 알파벳 대문자와 소문자, 특수기호, 숫자의 4가지임

보안 기능

비밀번호 관리

설계시 고려사항

[패스워드 설정규칙]- 계속

2. 특정정보이용 및 패턴조건

안전한 패스워드 규칙	안전하지 않은 패스워드 규칙
• 한글, 영어 등의 사전적 단어를 포함하지 않은 패스워드 • 널리 알려진 단어를 포함하지 않거나 예측이 어렵도록 가공한 패스워드 ❖ 널리 알려진 단어인 컴퓨터 용어, 기업 등의 특정명칭을 가공하지 않고 명칭 그대로 사용하는 경우 ❖ 속어, 방언, 은어 등을 포함하는 경우 • 사용자 ID와 연관성이 있는 단어구성을 포함하지 않은 패스워드 • 제3자가 쉽게 알 수 있는 개인정보를 포함하지 않은 패스워드 ❖ 개인정보는 가족, 생일, 주소, 휴대전화번호 등을 포함	• 한글 영어 등을 포함한 사전적인 단어로 구성된 패스워드 ❖ 스펠링을 거꾸로 구성한 패스워드도 포함 • 널리 알려진 단어로 구성된 패스워드 ❖ 컴퓨터 용어, 사이트, 기업 등의 특정 명칭으로 구성된 패스워드도 포함 • 사용자 ID를 이용한 패스워드 ❖ 사용자 ID 혹은 사용자ID를 거꾸로 구성한 패스워드도 포함 • 제3자가 쉽게 알 수 있는 개인정보를 바탕으로 구성된 패스워드 ❖ 가족, 생일,주소,휴대전화번호 등을 포함하는 패스워드

보안 기능

비밀번호 관리

소프트웨어 보안

설계시 고려사항

[패스워드 설정규칙]- 계속

2. 특정정보이용 및 패턴조건(계속)

안전한 패스워드 규칙	안전하지 않은 패스워드 규칙
	• 패턴이 존재하는 패스워드 ❖ 동일한 문자의 반복 ❖ 키보드 상에서 연속한 위치에 존재하는 문자들의 집합 ❖ 숫자가 제일 앞이나 제일 뒤에 오는 구성의 패스워드 • 숫자와 영문자를 비슷한 문자로 치환한 형태를 포함한 구성의 패스워드 • 영문자 “O”를 숫자 “0”으로 , 영문자 “I’”를 숫자 “1”로 치환 등의 패스워드 • 특정 인물의 이름을 포함한 패스워드 ❖ 사용자 또는 사용자 이외의 특정 인물, 유명인, 연예인 등의 이름을 포함하는 패스워드 • 한글발음을 영문으로, 영문단어의 발음을 한글로 변형한 형태의 패스워드 ❖ 한글의 “사랑“을 영어 “Sa Rang”으로 표기, 영문자 “LOVE”의 발음을 한글 ‘러브’로 표기

보안 기능

비밀번호 관리

소프트웨어 보안

설계시 고려사항

[패스워드 설정규칙]- 계속

3. 기타 조건

안전한 패스워드 규칙	안전하지 않은 패스워드 규칙
• 해당 시스템에서 사용자가 이전에 사용하지 않고 이전 패스워드와 연관성이 있는 단어구성을 포함하지 않은 패스워드	• 시스템에서 예제로 제시되는 패스워드 • 시스템에서 초기 설정된 패스워드 • 해당 시스템에서 사용자가 이전에 사용했던 패스워드

보안 기능

비밀번호 관리

설계시 고려사항(계속)

2. 네트워크를 통해 패스워드를 전송하는 경우 반드시 패스워드를 암호화하거나 암호화된 통신 채널을 이용해야 한다.
   - 웹브라우저와 같은 클라이언트와 웹서버 간의 통신이나 서버와 서버간의 통신 등 인터넷과 같은 공중망 환경에서는 패스워드와 같은 중요정보를 송수신하는 경우 보호대책이 필요하다. 이러한 보호대책으로 TLS, VPN 등과 같은 다양한 통신 암호기술을 적용할 수 있다.
   - 시스템관리자 및 보안관리자는 TLS를 적용하거나 관련 솔루션을 도입할 때 제품이 표준에 맞게 구현되었는지와 상호 호환성을 보장하는지 및 검증된 제품인지, 오픈소스를 이용하는지 등을 확인해야 한다.

TLS: Transport Layer Security

보안 기능

비밀번호 관리

설계시 고려사항(계속)

3. 패스워드 저장시, 솔트가 적용된 안전한 해시함수를 사용해야 하며, 해시함수 실행은 서버에서 해야 한다.
   - 패스워드는 복호화되지 않은 일방향 해시함수를 사용해서 암호화하여 저장해야 한다.

일방향 해시함수

일방향 해시함수는 수학적인 연산을 통해 원본 메시지를 변환하여 암호화된 메시지인 다이제스트를 생성한다. 원본 메시지를 알면 암호화된 메시지를 구하기는 쉽지만 암호화된 메시지로는 원본 메시지를 구할 수 없어야 하며 이를 ‘일방향성 ' 이라고 한다.

보안 기능

비밀번호 관리

설계시 고려사항(계속)

4. 패스워드 재설정/변경시 안전하게 변경할 수 있는 규칙을 정의해서 적용해야 한다.

- 패스워드 변경은 주기적인 변경과 분실시 재설정으로 나누어 볼 수 있다.

A. 주기적 패스워드 변경

- 사용자 및 관리자는 안전한 패스워드 관리를 위해 주기적으로 패스워드를 변경하여 패스워드의 노출 위협을 최소화하여야 한다. 일반적으로 사용자 패스워드 변경주기는 3개월에서 6개월 이하로 설정하는 것을 고려할 수 있다.
- 사용자는 자신의 패스워드가 제3자에게 노출되었을 경우 즉시 새로운 패스워드로 변경해야 한다. 패스워드 변경시 이전에 사용하지 않은 새로운 패스워드로 변경해야 하며, 이전의 패스워드와 연관성이 없어야 한다.

B. 패스워드 재설정

- 패스워드를 잊어버렸거나 분실하는 경우 패스워드 재설정이 필요하다. “패스워드 찾기” 기능구현시 I-pin 인증, 휴대전화 인증, 질의답변 검증 등을 통해 패스워드 재설정 권한을 확인하고 회원가입시 등록된 이메일 주소를 이용하여 패스워드를 재설정할 수 있는 링크를 전송한다. 사용자는 해당 링크를 클릭하여 자신의 패스워드를 재설정할 수 있도록 설계한다.

보안 기능

비밀번호 관리

설계시 고려사항(계속)

5. 패스워드 관리 규칙을 정의해서 적용해야 한다.

- 안전한 패스워드 관리를 위해 다음과 같은 항목을 고려한다.

A. 변경주기

- 패스워드는 3개월(또는 6개월)마다 주기적으로 변경하도록 한다.

B. 만료기간 설정

- 일정기간 시스템 사용자에 대해서는 패스워드 만료기간을 설정한다.
- 사용자 정보를 저장하는 DB테이블에 개인정보 변경주기를 추가한 뒤 일단위로 해당 필드가 업데이트 되도록 한다. 패스워드 기간이 만료되면 로그인시 사용자에게 패스워드 변경을 요청하고, 패스워드 변경시 개인정보 변경주기를 초기화하도록 한다.

C. 성공한 로그인 시간 관리

- 마지막으로 성공한 로그인 시간 정보를 관리해야 한다.
- 사용자 테이블에 마지막으로 로그인한 시간정보를 저장하고 사용자에게 알림으로써 계정도용 여부를 점검할 수 있도록 개발 가이드 구현 단계를 작성한다.

보안 기능

비밀번호 관리

설계시 고려사항(계속)

[참고] 패스워드 관리 주기

패스워드 생성

- 개인 패스워드는 사용자가 직접 생성하고 그룹 패스워드는 그룹의 장이 생성하여 구성원들에게 안전한 방법을 통해 전달 한다.

패스워드 사용

- 패스워드는 제 3자에게 노출되지 않도록 해야 하며, 자신의 패스워드와 관련된 정보 및 힌트를 제공하지 않아야 한다. 패스워드 변경주기는 3개월(또는 6개월)이다. 시스템 및 소프트웨어의 초기 패스워드는 설치 시 즉시 변경해야 한다.

패스워드 폐기

- 패스워드는 사용용도가 끝나거나 사용주기가 지난 경우 폐기한다. 인증 패스워드는 시스템 담당자가 사용자 계정의 삭제와 함께 폐기하고 암호화 패스워드는 사용자가 직접 폐기한다.

보안 기능

비밀번호 관리

소프트웨어 보안

사고 사례

가장 털리기 쉬운 패스워드 100선 공개, '내 비밀번호' 있나 확인하세요

[아시아경제 온라인이슈팀] 가장 털리기 쉬운 패스워드 100선이 공개됐다.

미국 패스워드관리업체 스플래시데이터는 '2014년 최악의 패스워드 25개' 명단을 발표했다. 이는 작년 한 해 동안 패스워드를 포함한 계정 정보가 인터넷에 유출된 사례 300만건을 조사한 결과다.

조사결과 '123456'과 'password'가 2년 연속으로 각각 1, 2위를 차지했다. 3~7위는 각각 '12345', '12345678', 'qwerty', '234567890', '1234' 등 자판에서 연속으로 나오는 키를 누르는 조합이었고, '1234567'(11위)도 마찬가지였다.

똑같은 숫자를 여러 차례 누르는 경우도 '111111'(15위), '696969'(22위), '123123'(23위) 등 흔했다.
'abc123'(14위)은 자판에서는 연속이 아니지만 알파벳 순서상으로 연속인 글자와 숫자를 누르는 조합이었다.

뜻이 있는 단어나 단문을 사용한 경우는 'baseball'(8위), 'dragon'(9위), 'football'(10위), 'monkey'(12위), 'letmein'(13위), 'mustang'(16위), 'access'(17위), 'shadow'(18위), 'master'(19위), 'michael'(20위), 'superman'(21위), 'batman'(24위), 'trustno1'(25위) 등이 있었다.

보안 기능

비밀번호 관리

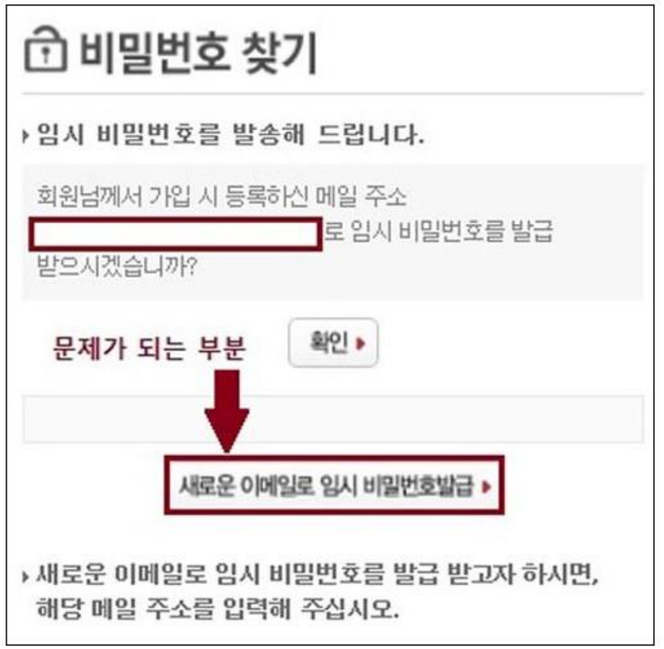
소프트웨어 보안

사고 사례(계속)

인터파크 오픈마켓에서 물건 팔려다 '탈탈'

해당 문제점을 제보한 유민상 씨는 "비밀번호를 찾다가 비밀번호를 찾는 방법 중 '등록한 e-mail 주소로 비밀번호 찾기' 부분에서 해킹의 위험이 있는 것을 발견해 제보하게 됐다"며, ""등록한 e-mail 주소로 비밀번호 찾기' 기능은 이름, 아이디, 메일주소만 알면 누구나 쉽게 임시비밀번호를 발급받을 수 있어 문제가 된다"고 전했다.

또한, 그는 "인터파크의 오픈마켓 판매자의 경우에는 이름과 메일주소가 그대로 노출돼 있고, 메일주소로 아이디를 유추할 수 있어 더욱 심각하다"며, "새로운 이메일주소로 임시 비밀번호를 발급하는 기능을 제거하거나 다른 방식으로 사용자 본인 확인 후 다른 이메일로 비밀번호를 전송할 수 있도록 해야 한다"고 전했다.



보안 기능

4. 중요자원 접근 통제

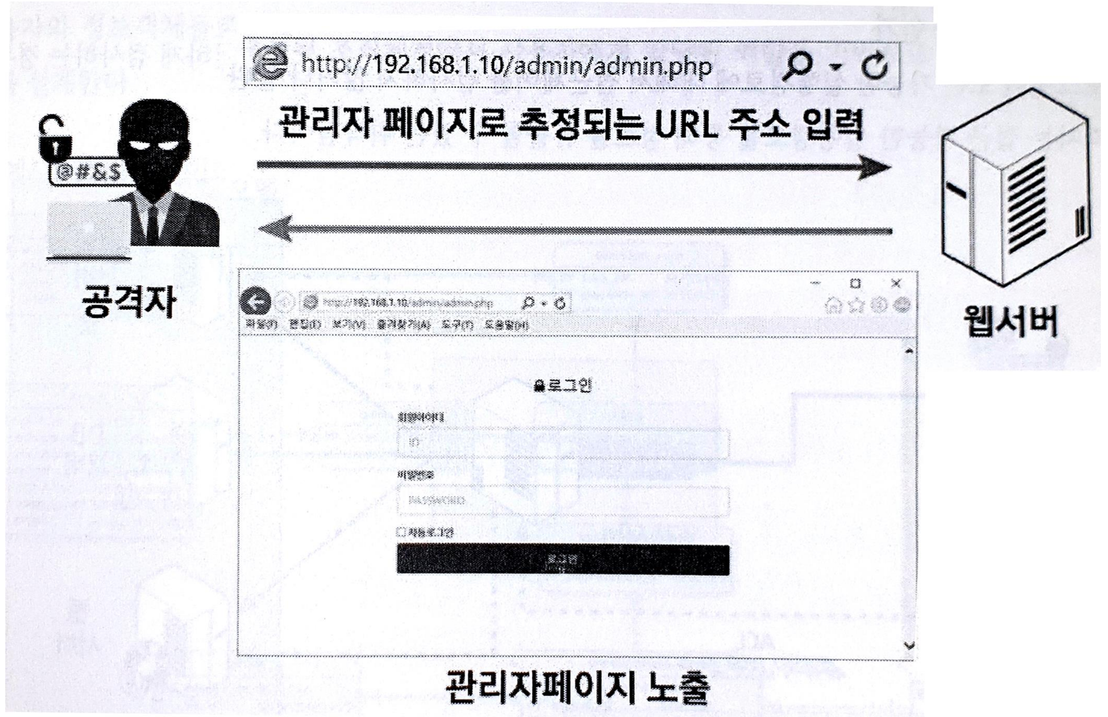
요구사항 분류	보안기능	요구사항번호	SR2-4
이름	중요자원 접근 통제		
설명	중요자원(프로그램 설정, 민감한 사용자 데이터 등) 정의하고, 정의된 중요자원에 대한 접근을 통제하는 신뢰할 수 있는 방법(권한관리 포함) 및 접근통제 실패 시 대응방안을 설계해야 한다.		
요구사항내용	1. 중요자원에 대한 접근통제 정책을 수립하여 적용해야 한다. 2. 중요기능에 대한 접근통제 정책을 수립하여 적용해야 한다. 3. 관리자 페이지에 대한 접근통제 정책을 수립하여 적용해야 한다.		

보안 기능

중요자원 접근 통제

취약점 개요

- 사례 1 : 관리자 페이지 노출
  - ❖ 관리자페이지가 인터넷을 통해 접근 가능할 경우, 공격자의 주 타겟이 되어, 공격자의 SQL 삽입, 무차별대입공격 등 다양한 형태의 공격의 빌미를 제공하게 되는 취약점이다.



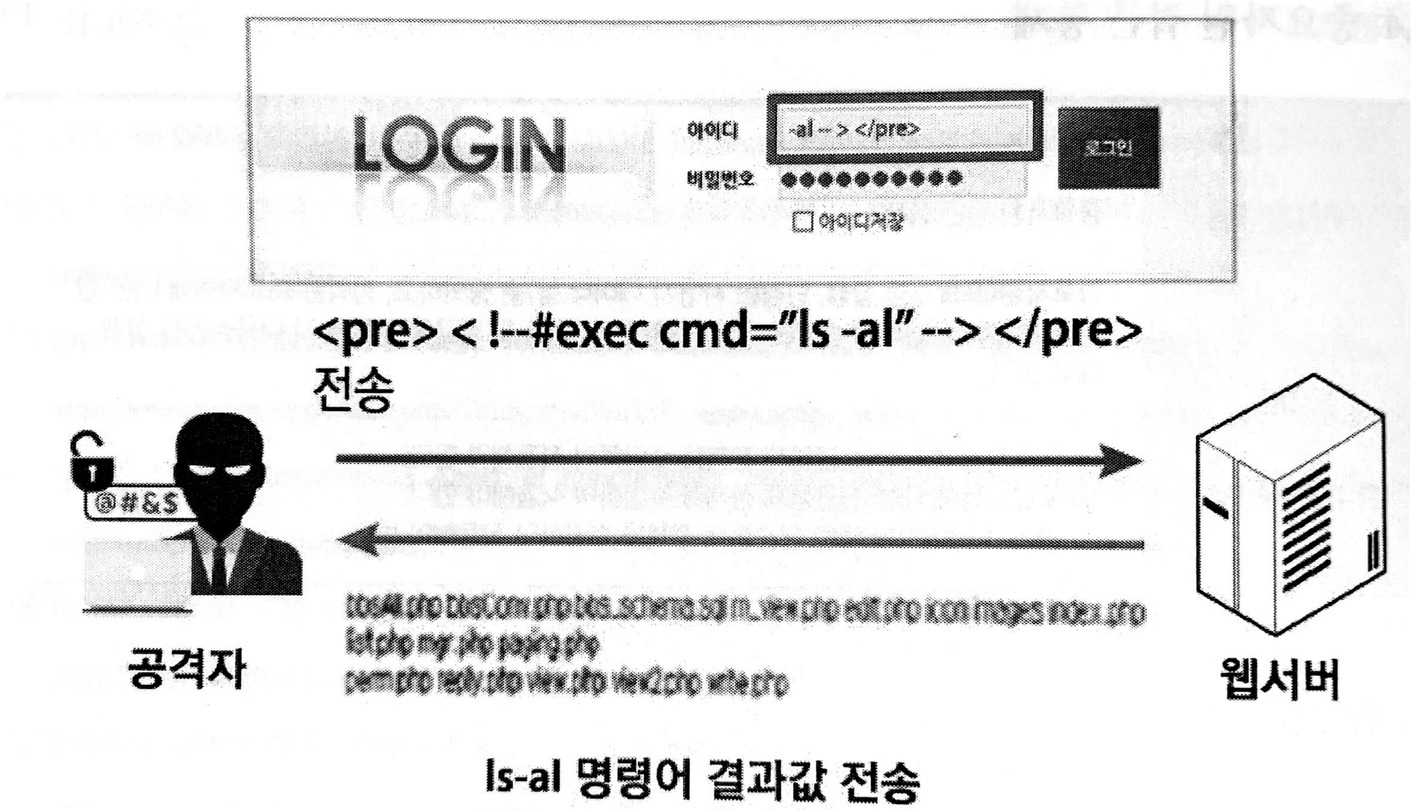
관리자페이지 노출

보안 기능

중요자원 접근 통제

취약점 개요

- 사례 2 : SSI 삽입
  - ❖ SSI(Server-side Includes)는 HTML 문서 내 변수 값으로 입력된 후, 이를 서버가 처리하게 되는데, 이 때 인젝션 명령문이 수행되어 서버 데이터 정보가 누출되는취약점이다.



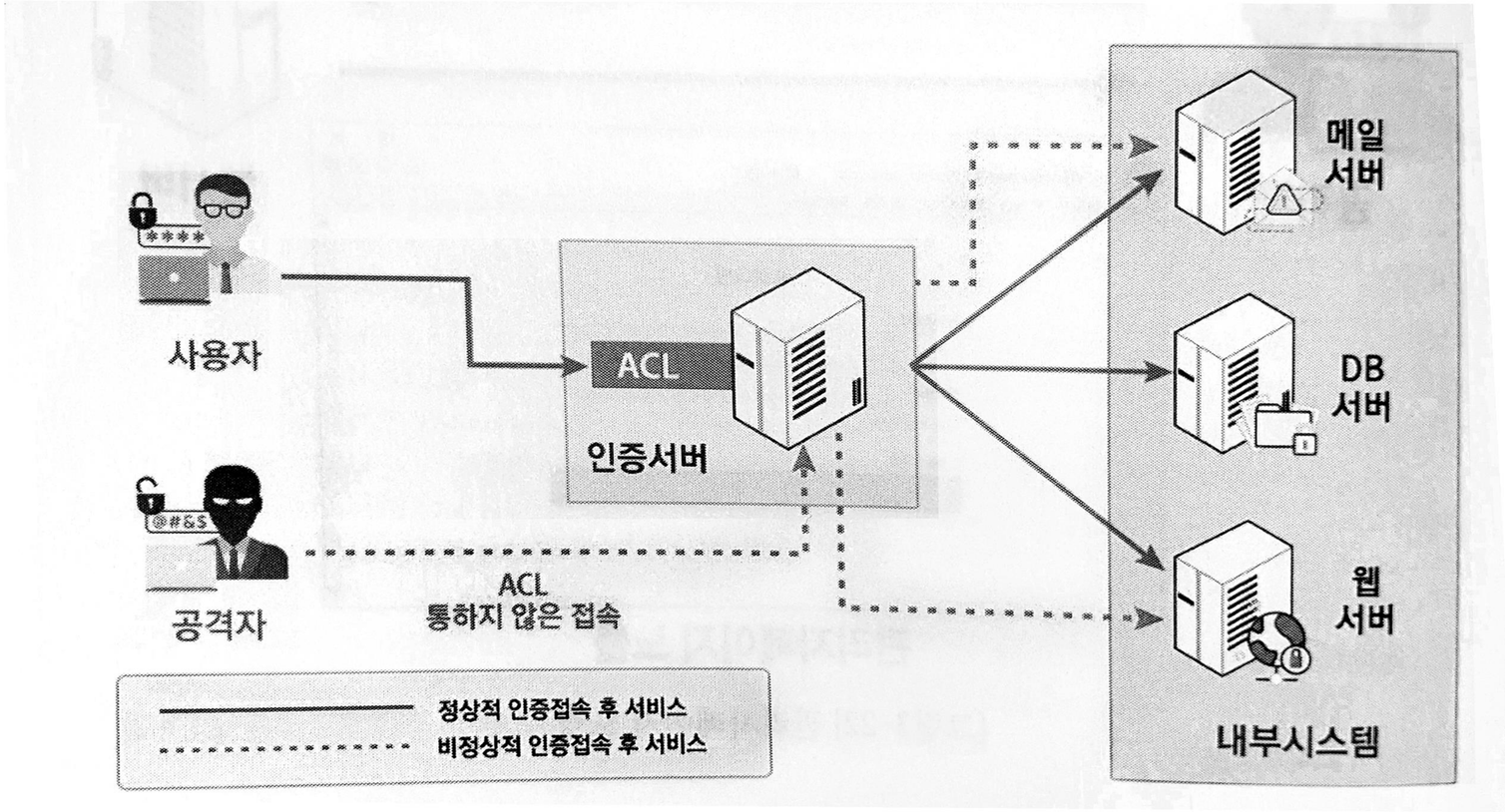
ls-al 명령어 결과값 전송

보안 기능

중요자원 접근 통제

취약점 개요

- 사례 3 : 부적절한 인가
  - ❖ 프로그램이 모든 가능한 실행경로에 대해서 접근제어를 검사하지 않거나 불완전하게 검사하는 경우, 공격자는 접근 가능한 실행경로를 통해 정보를 유출할 수 있는 취약점이다.



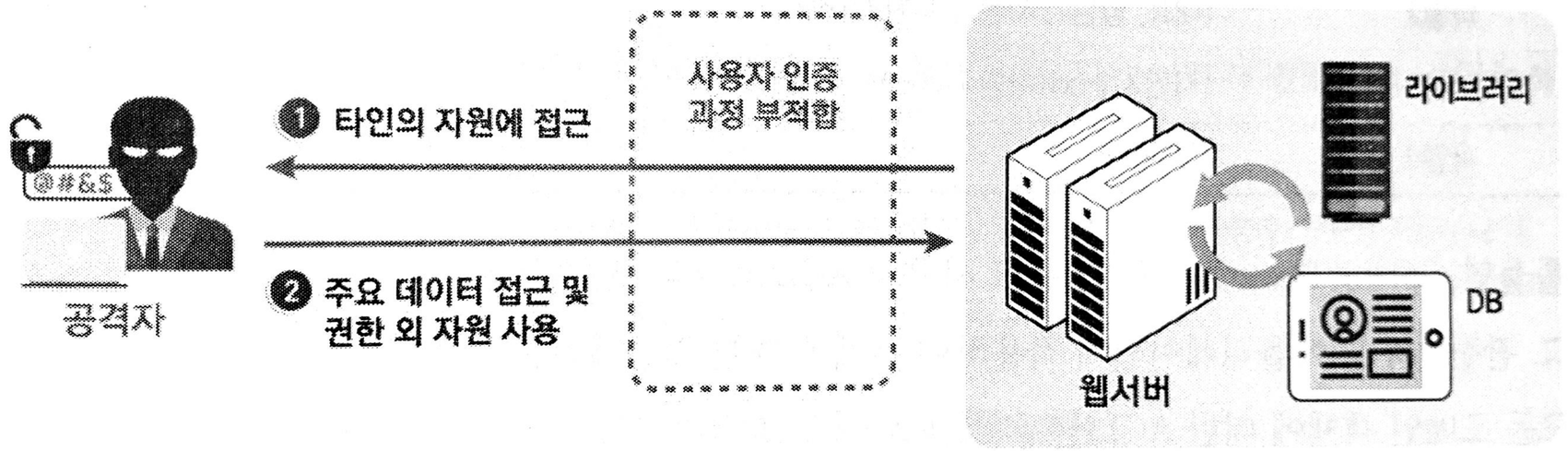
ls –al 명령어 결과값 전송

보안 기능

중요자원 접근 통제

취약점 개요

- 사례 4 : 중요자원에 대한 잘못된 권한 설정
  - ❖ SW가 중요한 보안관련 자원에 대하여 읽기 또는 수정하기 권한을 의도하지 않게 허가할 경우 권한을 갖지 않은 사용자가 해당 자원을 사용하게 될 수 있는 취약점이다.



중요한 자원에 대한 잘못된 권한 설정

보안 기능

중요자원 접근 통제

설계시 고려사항(1)

- RBAC(Role Based Access Controll ：역할기반 접근제어) 모델을 사용하여 기업, 정부 등 다수의 사용자와 정보객체들로 구성된 조직체계에서 사용자에게 할당된 역할을 기반으로 권한을 부여하도록 설계한다.
- 접근제어목록(Access Control List)을 구성하여 자원에 대한 접근 권한을 설정한다.
- 예를 들어, Spring Security 프레임워크 사용시 ACL 모듈을 추가할 수 있다. 다음과 같은 세 가지 ACL 관련 기능을 애플리케이션에 적용하여 객체에 대한 접근제어를 구현할 수 있다.
  1. 모든 도메인 객체에 대한 ACL 엔트리를 효과적으로 검색하고 수정한다.
  2. 메서드 호출에 앞서, 각 사용자가 객체에 대해 특정 작업을 수행할 권한이 있는지 검증한다.
  3. 메서드 호출이 끝난 후, 각 사용자가 객체(또는 반환되는 객체) 대해 특정 작업을 수행할 권한이 있는지 검증한다.

보안 기능

중요자원 접근 통제

소프트웨어 보안

설계시 고려사항(2)

1. 중요자원에 대한 접근통제 정책을 수립하여 적용해야 한다.
   - ❖ 중요자원에 대한 접근권한을 최소권한으로 설정한다.
   - ❖ 중요자원에 대한 접근 통제 정책을 설정하고, 사용자별 또는 그룹별 접근을 체크한다.

중요자원(파일, 프로세스, 메모리, 데이터베이스와 같은)에 대한 접근을 통제하기 위해 ACL 이나 RBAC을 적용하도록 설계한다. 접근통제 정책을 수립할 때는 최소권한의 원칙과 권한 분리 정책에 따라 자원에 대한 권한을 할당하고 자원에 대한 접근은 요구조건을 충족할 때만 허가하도록 설계해야 한다.

보안 기능

중요자원 접근 통제

소프트웨어 보안

설계시 고려사항(3)

2. 중요기능에 대한 접근통제 정책을 수립하여 적용해야 한다.

중요기능에 대한 접근 통제는 소프트웨어를 익명, 일반, 특권사용자와 관리자 영역으로 구분하여 역할기반 접근통제 정책 및 비즈니스 로직에 따라 접근통제가 실시되도록 다음과 같은 조건에 따라 설계한다.

- 중요기능에 대한 접근 권한은 최소한으로 설정한다.
- 중요기능에 대한 접근 통제 정책을 설정하고, 사용자별 또는 그룹별 접근을 체크한다.
- 프로그램에서 사용자 또는 자원에 대한 권한의 할당, 수정, 확인, 검사를 수행하여 의도치 않은 범위의 권한을 획득하지 않도록 한다.
- 파라미터 변조로 인증이 올바르게 수행되지 않을 수 있으므로 파라미터가 변조되지 않았는지 확인하는 절차를 구현한다.
- 상위권한을 사용해 수행되는 기능을 구현해야 하는 경우, 권한상승은 가능한 가장 마지막에 수행하고 수행종료 즉시 원상 복귀한다.

보안 기능

중요자원 접근 통제

설계시 고려사항(4)

3. 관리자 페이지에 대한 접근통제 정책을 수립하여 적용해야 한다.
   - 관리자 페이지의 URL은 쉽게 추측할 수 없도록 설정한다.
   - 관리자 페이지의 원격 연결시 암호화 통신 채널을 사용해야 한다.
   - 관리자페이지가 외부망에 있는 경우 IP 통제, 80번이 아닌 별도의 포트 사용, SSL 적용, 추가인증을 요구한다.
   - 관리자페이지가 내부망에 있는 경우 80번이 아닌 별도의 포트 사용, SSL 적용을 권고한다.

중앙집중화된 접근제어를 제공하는 라이브러리나 프레임워크를 사용하여 각 종류의 자원에 대한 접근을 보호할 수 있다.

보안 기능

중요자원 접근 통제

소프트웨어 보안

사고 사례(1)

[KT 개인정보 유출] KT, 같은 수법에 왜 또 당했나?

2년전 KT는 정보 유출 프로그램을 제작, 고객정보시스템을 조회하는 것처럼 꾸며 소량으로 고객정보를 가져가는 식으로 5개월간 870만건의 개인정보를 빼냈다.

6일 인천경찰청 광역수사대에 따르면 전문 해커 김모씨와 정모씨 등은 KT 홈페이지를 해킹해 KT 홈페이지에 로그인 후 개인정보를 빼내왔다.이들은 홈페이지 이용대금 조회란에 고유숫자 9개를 무작위로 자동 입력시키는 이 프로그램으로 KT 가입고객의 9자리 고유번호를 맞춰 개인정보를 탈취했다.

보안 기능

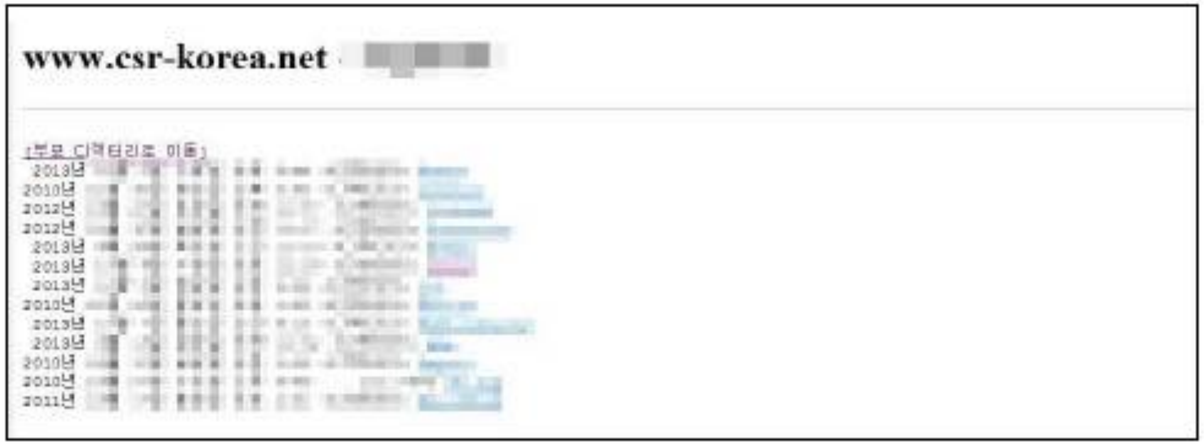
중요자원 접근 통제

소프트웨어 보안

사고 사례(2)

대한상의 '지속가능경영포털' 해외 해커 침입...보안 취약

[보안뉴스 김태형] 대한상공회의소 지속가능경영원에서 운영하고 있는 '지속가능경영포털 사이트(www.csr-korea.net)'가 해외 해커에 의해 침입 당한 흔적과 함께 디렉터리 리스팅 취약점과 파일 업로드 취약점이 발견됐다.



▲ 디렉토리 내부의 모든 파일이 보여지는 디렉토리 리스팅 취약점.

이 취약점은 디렉토리는 물론, 내부의 모든 파일들이 보이게 되어 공격자는 웹 어플리케이션의 구조를 파악해 민감한 정보가 포함된 설정 파일을 조회하거나 웹에 게시하지 않은 각종 파일을 유출할 수 있다.

보안 기능

5. 암호키 관리

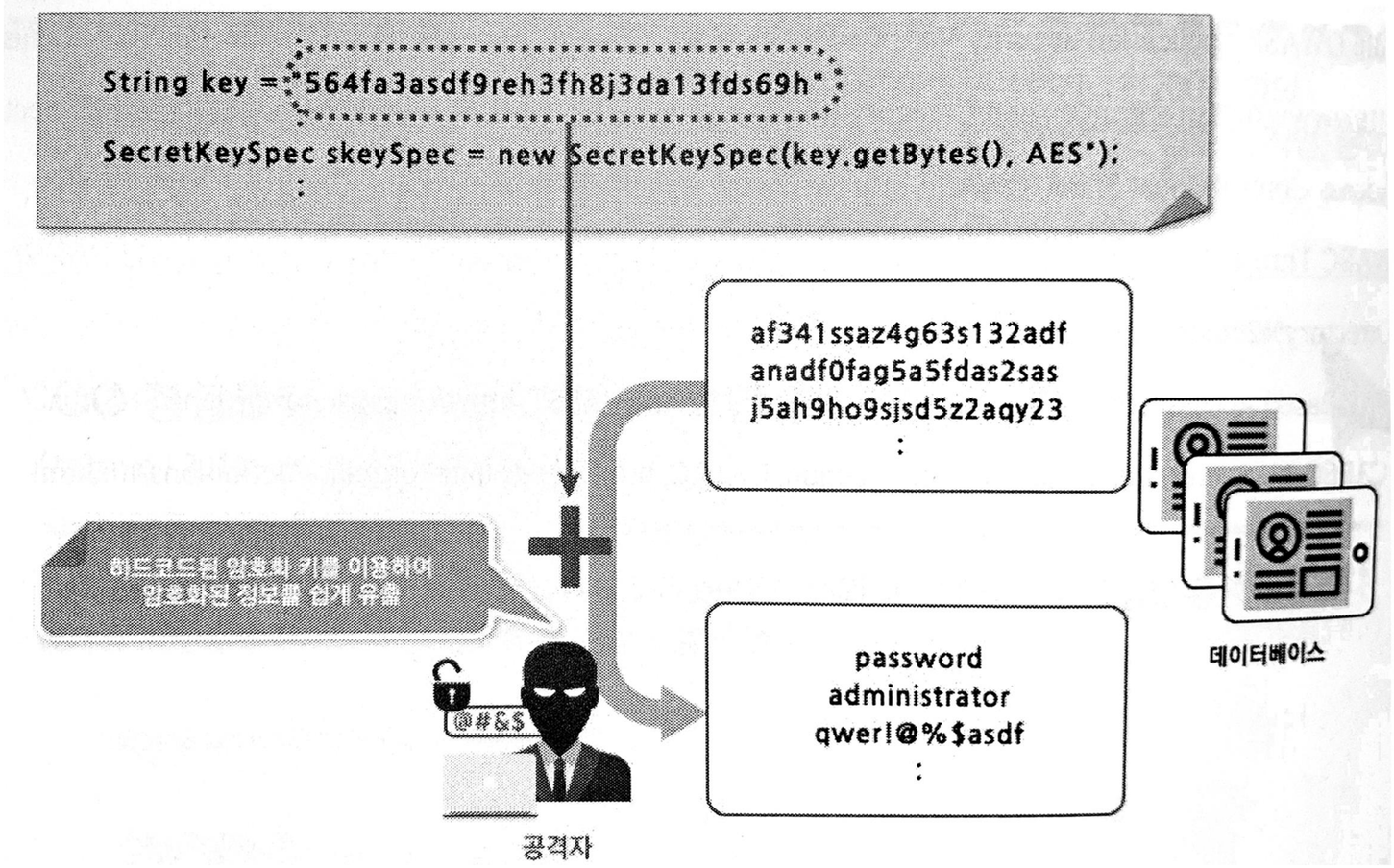
요구사항 분류	보안기능	요구사항번호	SR2-5
이름	암호키 관리		
설명	암호키 생성, 분배, 접근, 파기 등 안전하게 암호키 생명주기를 관리할 수 있는 방법을 설계해야 한다.		
요구사항내용	1. DB 데이터 암호화에 사용되는 암호키는 한국인터넷진흥원의 “암호이용안내서”에서 정의하고 있는 방법을 적용해야 한다. 2. 설정파일(xml, Properies)내의 중요정보 암호화에 사용되는 암호키는 암호화해서 별도의 디렉토리에 보관해야 한다.		

보안 기능

암호키 관리

취약점 개요

- 사례 1 : 하드코어된 암호키
  - ❖ 코드 내부에 하드코드된 암호화 키를 사용하여 암호화를 수행하면 암호화된 정보가 유출될 가능성이 높아진다.



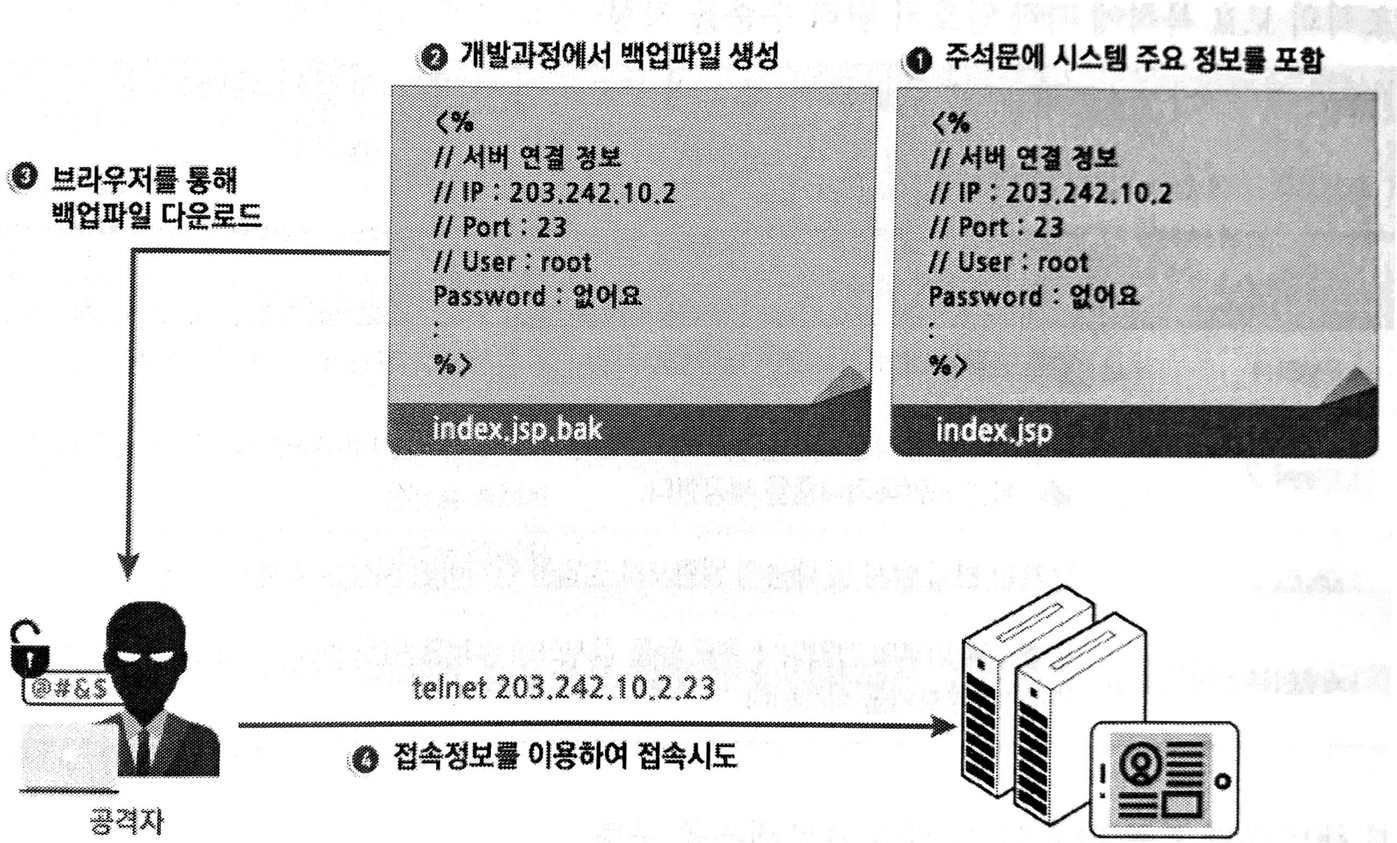
하드코드된 암호화 키

보안 기능

암호키 관리

취약점 개요

- 사례 2 : 주석문 안에 포함된 암호키
  - ❖ 주석문 안에 암호키에 대한 설명이 포함되어 있는 경우 공격자가 소스코드에 접근할 수 있다면 아주 쉽게 암호키가 노출될 수 있다.



주석문 안에 포함된 시스템 주요정보

보안 기능

암호키 관리

설계시 고려사항

1. DB데이터 암호화에 사용되는 암호키는 한국인터넷진흥원의 “암호이용안내서 " 에서 정의하고 있는 관리 방법을 적용해야 한다.

   A. 암호키 관리 규칙 생성시 고려사항

① DB 데이터 암호화에 사용되는 암호키는 데이터가 저장되는 데이터베이스와 물리적으로 분리된 장소에 별도로 보관한다.
② 암호화 키를 생성, 분배, 사용, 폐기하는 키의 생명주기관리를 위한 명시적인 암호화 정책을 적용한다.
③ 패스워드나 암호화키는 메모리에 저장하지 않는다.
④ 패스워드나 암호키가 메모리에 저장되어야 하는 경우 사용종료 후 메모리를 0으로 초기화 한다.
⑤ 암호키 생성 및 변경시 암호키에 대한 백업기능을 구현한다.
⑥ 대칭키 암호알고리즘에 사용되는 비밀키의 송신자 사용기간은 최대 2년, 수신자 사용기간은 최대 5년을 설정한다.
⑦ 공개키 암호알고리즘에서 사용되는 암호화 공개키는 최대 2년, 복호화 개인키는 최대 2년, 검증용 공개키는 최소 3년, 서명용 개인키는 최대 3년으로 설정한다.

보안 기능

암호키 관리

설계시 고려사항

1. (계속)DB데이터 암호화에 사용되는 암호키는 한국인터넷진흥원의 “암호이용안내서 " 에서 정의하고 있는 관리 방법을 적용해야 한다.

   B. 조직의 보호 목적에 따라 암호키 관리 수준을 지정

   NIST에서 제정한 FIPS 140-2의 레벨로써, 조직의 보호목적에 따라 적절히 채택한다.

[FIPS 140-2 레벨 분류]

레벨	내용
Level 1	암호모듈에 대한 기본적인 보안요구사항만을 충족하여 최소한의 보안을 제공한다.
Level 2	침입자의 불법적인 접근을 방지하고, 침입 이후에 변조를 나타내는 증거를 제공함으로써 물리적인 보안 메커니즘을 제공한다.
Level 3	강력한 변조 탐지 및 대응의 일환으로 침입을 감지하면서 저장된 키를 삭제한다.
Lever 4	암호모듈 외부의 전압이나 온도 등을 감지하여 수퍼쿨링(Supercooling) 등 환경의 이상 변화시, 암호키를 삭제한다.

보안 기능

암호키 관리

소프트웨어 보안

설계시 고려사항

1. (계속)DB데이터 암호화에 사용되는 암호키는 한국인터넷진흥원의 “암호이용안내서 " 에서 정의하고 있는 관리 방법을 적용해야 한다.

   c. 키 생명주기 기준 암호화 키 관리 프로세스를 구축

   - 키 생성 – 암호화키와 패스워드를 생성, 사용, 관리하는 사람 등을 명시하고 키를 생성하는데 사용하는 프로그램 등 어떠한 방법으로 생성하는지에 대한 절차를 명시한다.
   - 키 사용 – 암호화키와 패스워드를 어떠한 방법으로 사용하는지에 대한 절차, 생성한 키의 종류에 따른 변경주기, 인가된 사용자만 키에 접근할 수 있는 접근통제 방법 및 요구사항 등을 명시한다.
   - 키 폐기 – 키의 사용주기가 다 된 경우 및 사용 용도가 끝난 경우 등 생성한 키를 폐기하여야 하는 경우를 명시하고, 암호화키와 패스워드를 안전하게 폐기하는 절차 및 요구사항 등을 명시한다.

보안 기능

암호키 관리

설계시 고려사항

1. (계속)DB데이터 암호화에 사용되는 암호키는 한국인터넷진흥원의 “암호이용안내서 " 에서 정의하고 있는 관리 방법을 적용해야 한다.

   D. 키 복구 방안

   - 사용자 퇴사 등으로 인해 사용자 이외의 사람에게 키 복구가 필요한 경우, 암호화키는 정보보호담당자의 관리 하에 암호화키 관리대상 등에서 복구하고, 패스워드는 정보보호담당자가 임시패스워드를 발급하는 등 키 복구에 대한 방안을 마련하도록 한다.

보안 기능

암호키 관리

설계시 고려사항

1. (계속)DB데이터 암호화에 사용되는 암호키는 한국인터넷진흥원의 “암호이용안내서 " 에서 정의하고 있는 관리 방법을 적용해야 한다.

   E. 암호키 사용 유효기간

   - 암/복호화키의 사용이 일정시간을 넘은 경우 사용자 인터페이스를 통해 키 사용 기간이 경과했음을 알리고 새로운 키 생성을 권장하도록 설계한다. [표]는 NIST에서 권고하는 암호키 사용 유효기간이다.

키 종류		사용 유효기간	
		송신자 사용기간	수신자 사용기간
대칭키 암호 알고리즘	비밀키	최대 2년	최대 5년
공개키 암호 알고리즘	암호화 공개키	최대 2년	
	복호화 개인키	최대 2년	
	검증용 공개키	최소 3년	
	서명용 개인키	최대 3년	

보안 기능

암호키 관리

설계시 고려사항

2. 설정 파일(xml, Properties)내의 중요정보 암호화에 사용되는 암호키는 암호화해서 별도의 디렉터리에 보관해야 한다.
   - 설정파일내에 중요 정보 암호화에 사용된 암호키는 마스터키를 이용하여 암호화하여 별도의 디렉터리에 보관한다.

보안 기능

암호키 관리

사고 사례

보안업체 코드서명 정보 유출, 파장은?

모 보안 업체가 인터넷에서 자사 프로그램(보안 모듈)을 배포하는데 쓰는 일종의 인감 도장과 같은 성격의 코드 서명 정보가 유출돼 악성 프로그램 유포에 악용되는 사건이 벌어졌다.

일각에서는 이 사건이 보안회사를 통해 공격을 시도했다는 점에서 3.20 사이버테러 때와 유사하다는 분석이 나오고 있지만 현재로서는 공격자가 어떤 의도를 갖고 있는지 확신할 수 있는 단계는 아니란게 전문가들 설명이다.

공격자가 사이버테러 수준의 공격을 계획했는지, 특정 타깃을 노려 정보유출을 시도했는지, 금융정보를 빼내 돈을 벌려고 했는지 등에 대한 모든 가능성이 열려있는 상황이다. 현재 검찰에서 이 사건을 조사 중이다.

코드서명은 인터넷에 프로그램을 유포하기 위해 자사가 만든 것이 맞다는 것을 증명하기 위해 일종의 인감도장을 찍는 것과 같다. 이 과정에서 사용되는 것이 인증서와 개인키다. 이 사건의 경우 금융권 등 고객사에 제공하는 일부 보안모듈을 우리가 개발한 것이 맞다고 증명하는데 필요한 인감도장 정보(개인키)가 유출됐다.

코드서명 정보를 유출 당한 보안회사는 코드서명에 사용되는 개인키(온라인 상 인감도장 역할을 하는 정보)를 개발자들 PC에 저장해 사용해 왔다. 일부 개발자들 PC가 외부 공격자로 인해 악성코드에 감염되면서 이러한 개인키가 유출된 것이다.

공격자는 이 정보로 코드서명을 거쳐 악성 프로그램을 배포했다. 마치 실제 보안회사가 배포하는 것처럼 위장했다.

보안 기능

6. 암호연산

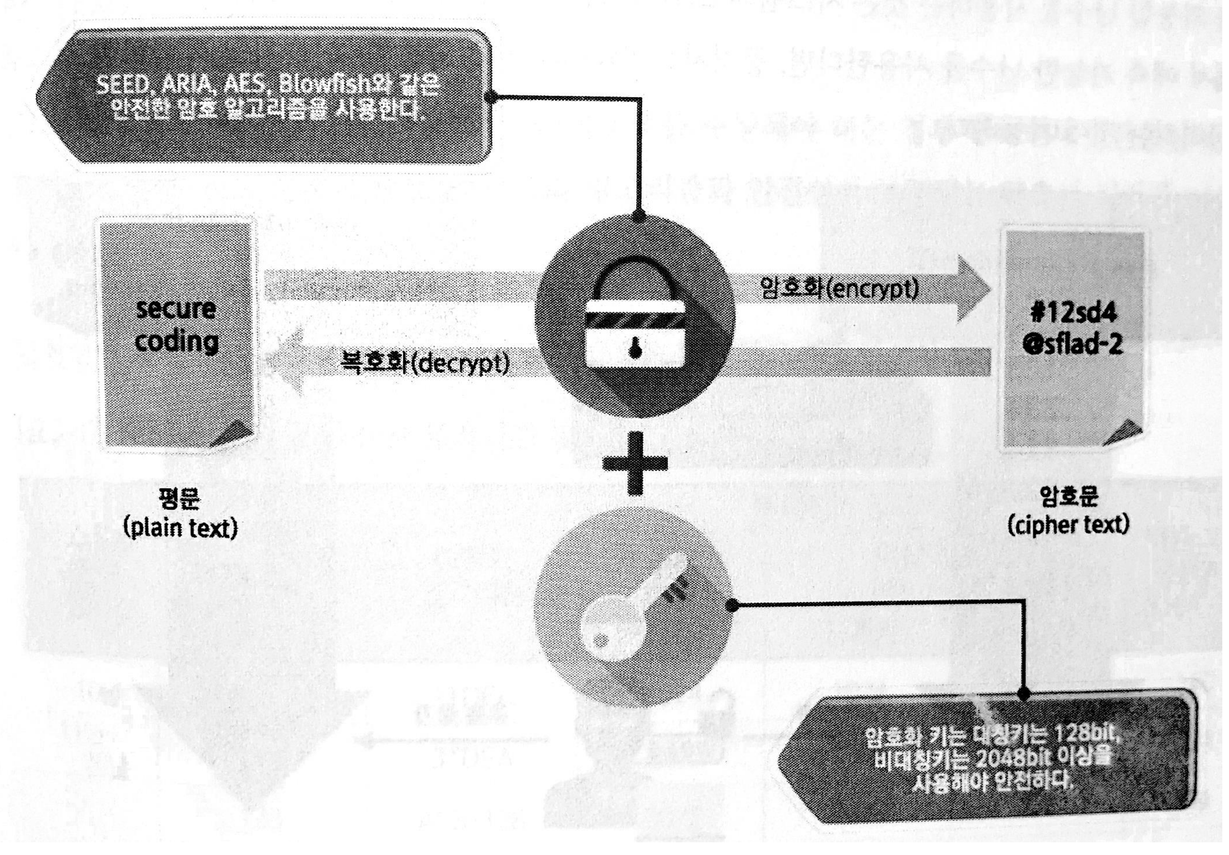
요구사항 분류	보안기능	요구사항번호	SR2-6
이름	암호연산		
설명	국제표준 또는 검증필 프로토콜로 등재된 안전한 암호 알고리즘을 선정하여 충분한 암호키 길이, 솔트, 충분한 난수값을 기반으로 암호연산 수행방법을 설계해야 한다.		
요구사항내용	1. 대칭키 또는 비대칭키를 이용해서 암/복호화를 수행해야 하는 경우 한국인터넷진흥원의 '암호이용안내서 ' 에서 정의하고 있는 암호화 알고리즘과 안전성이 보장되는 암호키 길이를 사용해야 한다. 2. 복호화되지 않은 암호화를 수행하기 위해 해시함수를 사용하는 경우 안전한 해시 알고리즘과 솔트값을 적용하여 암호화해야 한다. 3. 난수생성시 안전한 난수 생성 알고리즘을 사용해야 한다.		

보안 기능

암호 연산

취약점 개요

- 사례 1 : 취약한 암호알고리즘 사용
  - ❖ SW개발자들은 환경설정 파일이 저장된 패스워드를 보호하기 위하여 간단한 인코딩 함수를 이용하여 패스워드를 감추는 방법을 사용하기도 한다. 그렇지만, base64와 같은 지나치게 간단한 인코딩 함수를 사용하면 패스워드를 안전하게 보호할 수 없다.



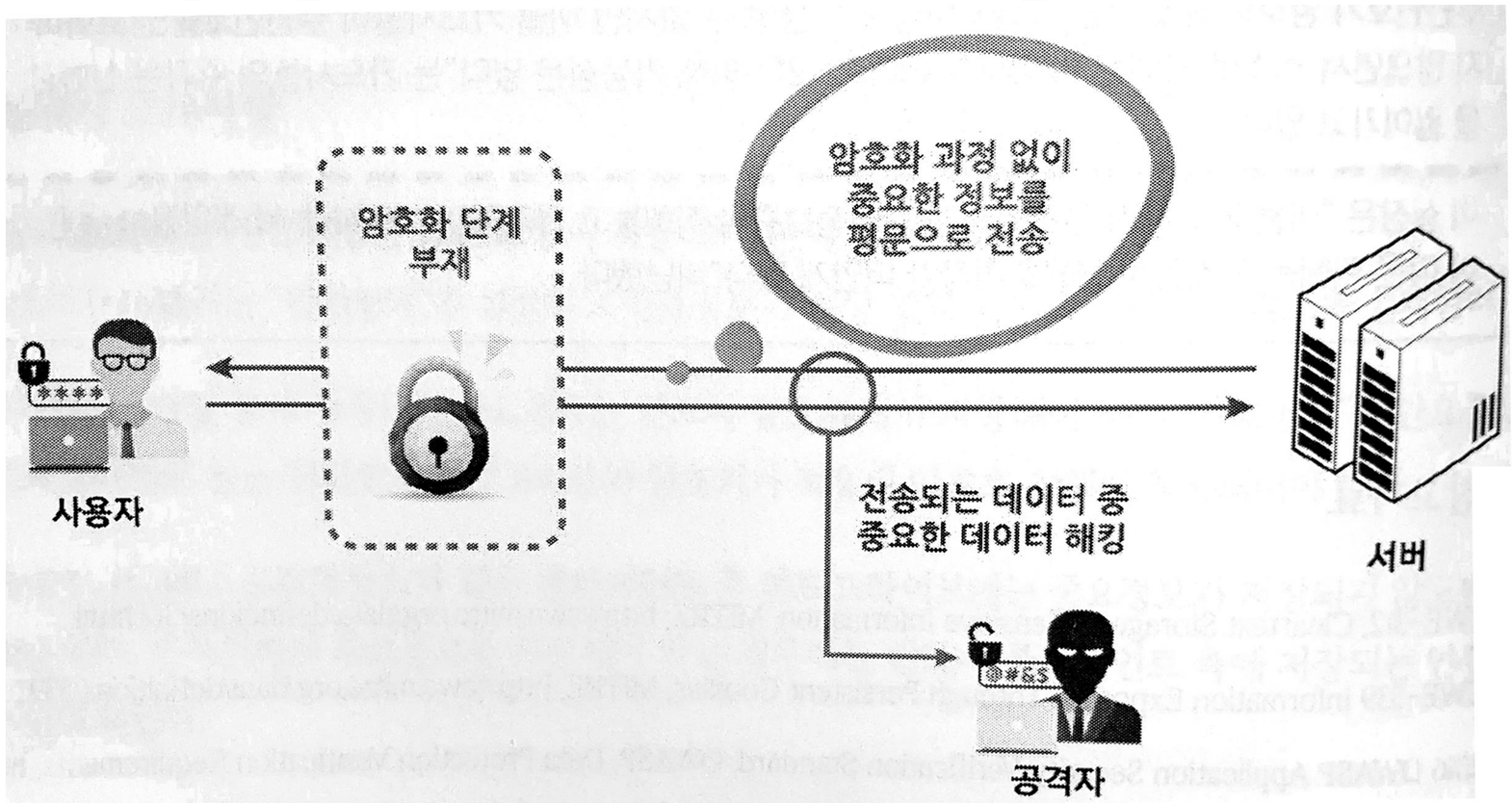
취약한 암호화 알고리즘 사용

보안 기능

암호 연산

취약점 개요

- 사례 2 : 충분하지 않은 키 길이 사용
  - ❖ 검증된 암호화 알고리즘을 사용하더라도 키 길이가 충분히 길지 않으면 짧은 시간 안에 키를 찾아낼 수 있고 이를 이용해 공격자가 암호화된 데이터나 패스워드를 복호화 할 수 있게 된다.



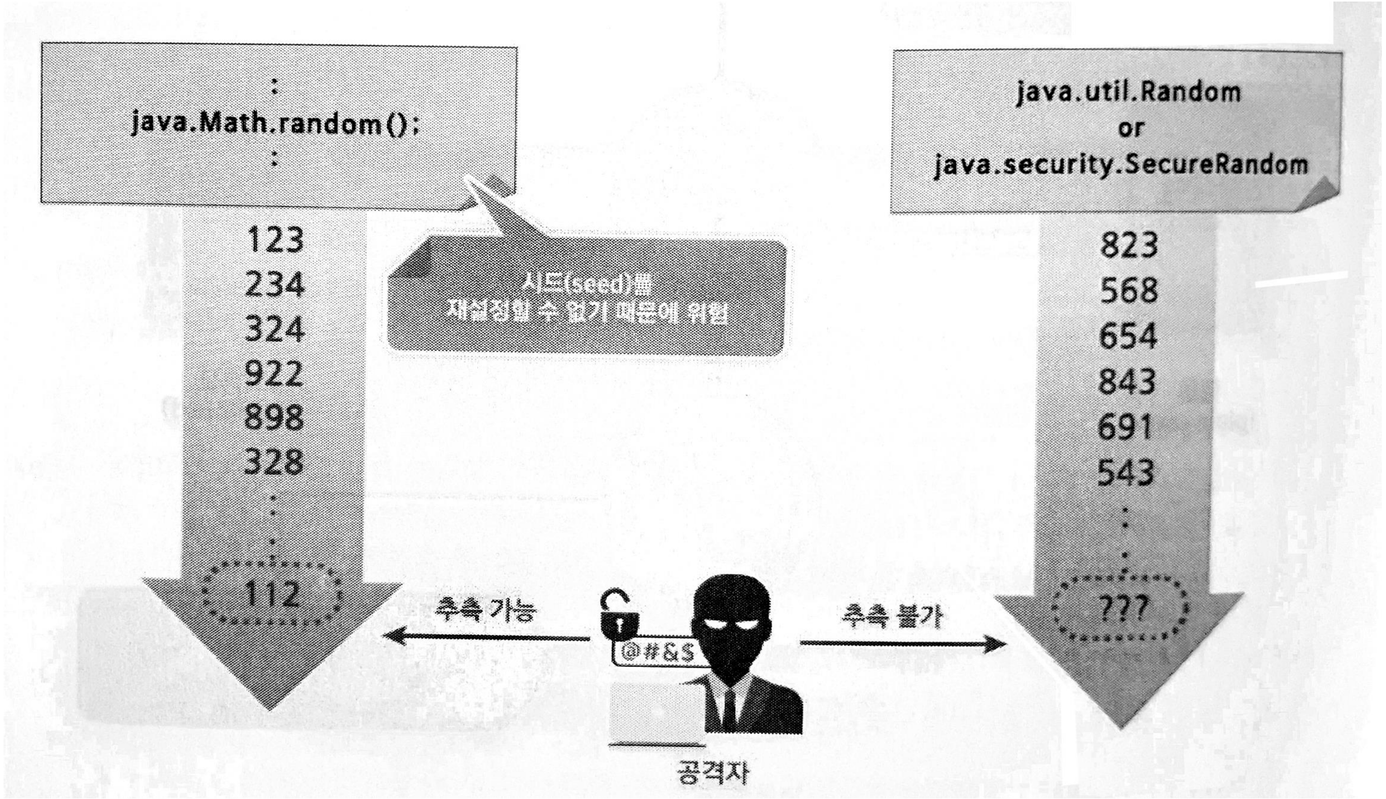
충분하지 않은 키 길이 사용

보안 기능

암호 연산

취약점 개요

- 사례 3 : 적절하지 않은 난수 사용
  - ❖ 예측 가능한 난수를 사용하는 것은 시스템의 보안약점을 유발한다. 예측 불가능한 숫자가 필요한 상황에서 예측 가능한 난수를 사용한다면, 공격자는 sw에서 생성되는 다음 숫자를 예상하여 시스템을 공격하는 것이 가능하다.



적절하지 않은 난수값 사용

보안 기능

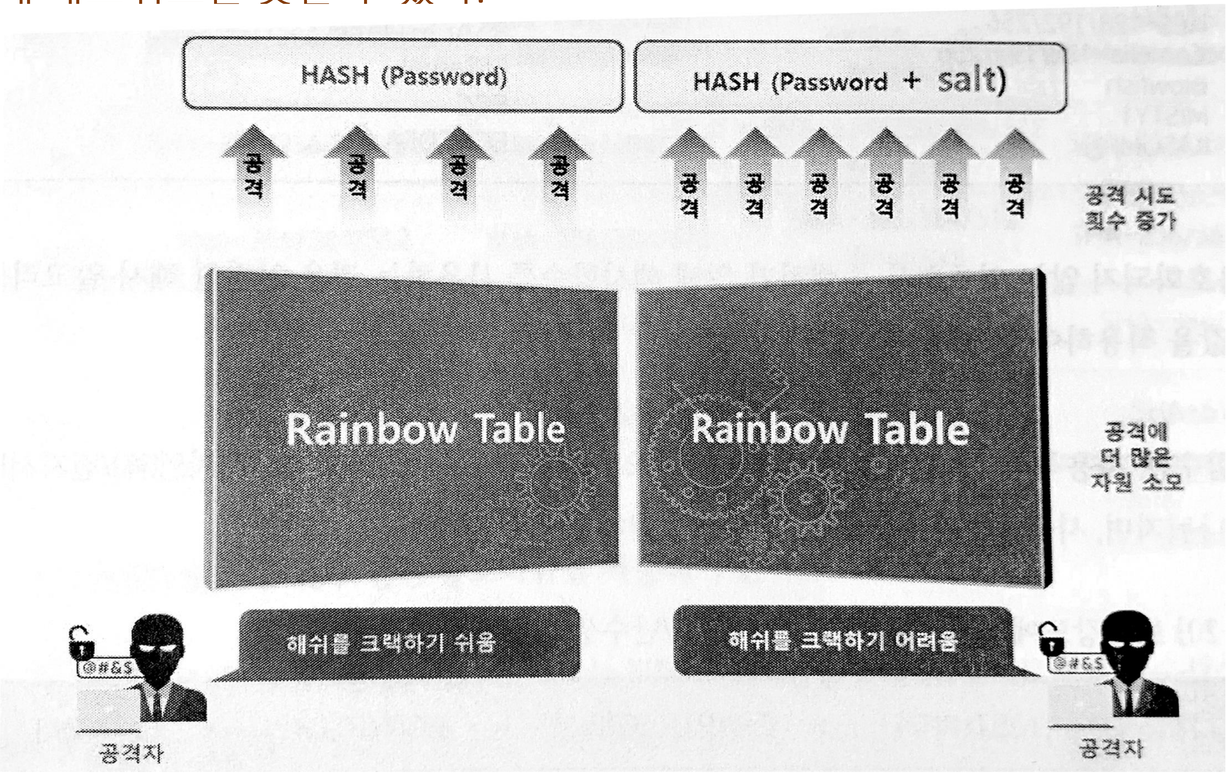
암호 연산

소프트웨어 보안

취약점 개요

- 사례 4 : 솔트 없이 사용하는 일방향 해시함수
  - ❖ 패스워드 저장시 일방향 해시함수의 성질을 이용하여 패스워드의 해시값을 저장한다. 만약 패스워드를 솔트(Salt)없이 해시하여 저장한다면, 공격자는 레인보우 테이블과 같이 가능한 모든 패스워드에 대해 해시값을 미리 계산하고, 이를 이용한 전수조사를 통해 패스워드를 찾을 수 있다.

레인보 테이블(rainbow table)은 해시 함수를 사용하여 변환 가능한 모든 해시 값을 저장시켜 놓은 표이다. 보통 해시 함수를 이용하여 저장된 비밀번호로 부터 원래의 비밀번호를 추출해 내는데 사용된다.



솔트 없이 일방향 해시함수 사용

보안 기능

암호 연산

설계시 고려사항

1. 대칭키 또는 비대칭키를 이용해서 암•복호화를 수행해야 하는 경우 한국인터넷진흥원의 “암호이용 안내서 " 에서 정의하고 있는 암호화 알고리즘과 안전성이 보장되는 암호키 길이를 사용해야 한다.

   ❖ 안전성이 보장되는 암호키 길이와 암호 알고리즘을 확인하고 사용하여야 한다.

NIST 알고리즘 안전성 유지기간 및 최소 키길이 권고

알고리즘 안전성 보장기간	보안 강도 (비트)	대칭키 알고리즘	비대칭키 알고리즘			타원•회귀 곡선기반(ex. ECD)
			인수분해 기반 (ex.RSA)	이산대수기반(ex. KCDSA)		
				공개키	개인키	
~ 10년	80	2TDEA	1024	1024	160	160
11년 ~ 30년	112	3TDEA	2048	2048	224	224
30년 ~	128	AES-128	3072	3072	256	256
	192	AES-192	7680	7680	384	384
	256	AES-256	15360	15360	512	512

보안 기능

암호 연산

설계시 고려사항

1. (계속)대칭키 또는 비대칭키를 이용해서 암•복호화를 수행해야 하는 경우 한국인터넷진흥원의 “암호이용안내서 " 에서 정의하고 있는 암호화 알고리즘과 안전성이 보장되는 암호키 길이를 사용해야 한다.

   ❖ 안전성이 보장되는 암호키 길이와 암호 알고리즘을 확인하고 사용하여야 한다.

국내외 사용 권고 알고리즘

대칭키 암호화 알고리즘	비대칭키 암호화 알고리즘
SEED	RSA
ARIA-128/192/256	KCDSA(전자서명용)
AES-128/192/256	RSAES-OAEP
Camelia-128/192/256	ElGamal
Blowfish	ECC
MISTY1	ECKCDSA 등
KASUMI 등	

보안 기능

암호 연산

설계시 고려사항

2. 복호화되지 않은 암호화를 수행하기 위해 해시함수를 사용하는 경우 안전한 해시 알고리즘과 솔트값을 적용하여 암호화 해야한다.
   - ❖ 해시함수는 사용목적에 따라 메시지인증/키유도/난수생성용과 단순해(메시지압축)/전자서명용으로 나눠지며, 사용목적과 보안강도에 따라 선택하여 이용하다.

보안 기능

암호 연산

설계시 고려사항

3. 난수 생성시 안전한 난수 생성 알고리즘을 사용해야 한다.
   - ❖ 국가정보원 “암호알고리즘 검증기준 V2.0“ 또는 FIPS 140-2 인증을 받은 암호모듈의 난수생성기와 256비트 이상의 시드를 사용하여 난수를 생성한다. 난수의 무작위성을 보장하기 위해 이전 난수생성 단계의 결과를 다음 난수생성 단계의 시드로 사용하는 의사난수 생성기를 이용한다.

사고사례

인터넷뱅킹에도 쓰는 암호화 기술 보안 '우려'

SHA1 암호화 알고리즘 보안성 취약

국내 주요 인터넷뱅킹 사이트를 포함해 대부분 암호화 통신을 제공하는 웹사이트가 지원하는 암호화 알고리즘(SHA1)이 이르면 올해 말부터 심각한 보안문제에 노출될 수 있는 것으로 나타났다.

이러한 SHA1이 두 가지 서로 다른 정보를 입력했을 때, 같은 해시값을 만들어 낼 수 있는 시점이 온다는 것이다. 이를 악용한 공격을 '충돌공격(collision attack)'이라고 부른다. 이런 시점이 되면 더이상 SHA1을 활용한 해시값은 안전하다고 보기 어렵다.

앞서 MD5라는 암호화 알고리즘 역시 SHA1과 같은 용도로 활용됐었지만 이란을 대상으로 한 미국, 이스라엘 첩보기관이 수행한 사이버첩보활동에 악용된 '플레임(Flame)' 악성코드가 이러한 MD5에 대한 충돌공격을 활용해 각종 정보를 수집하는데 악용됐다

보안 기능

소프트웨어 보안

7. 중요 정보 저장

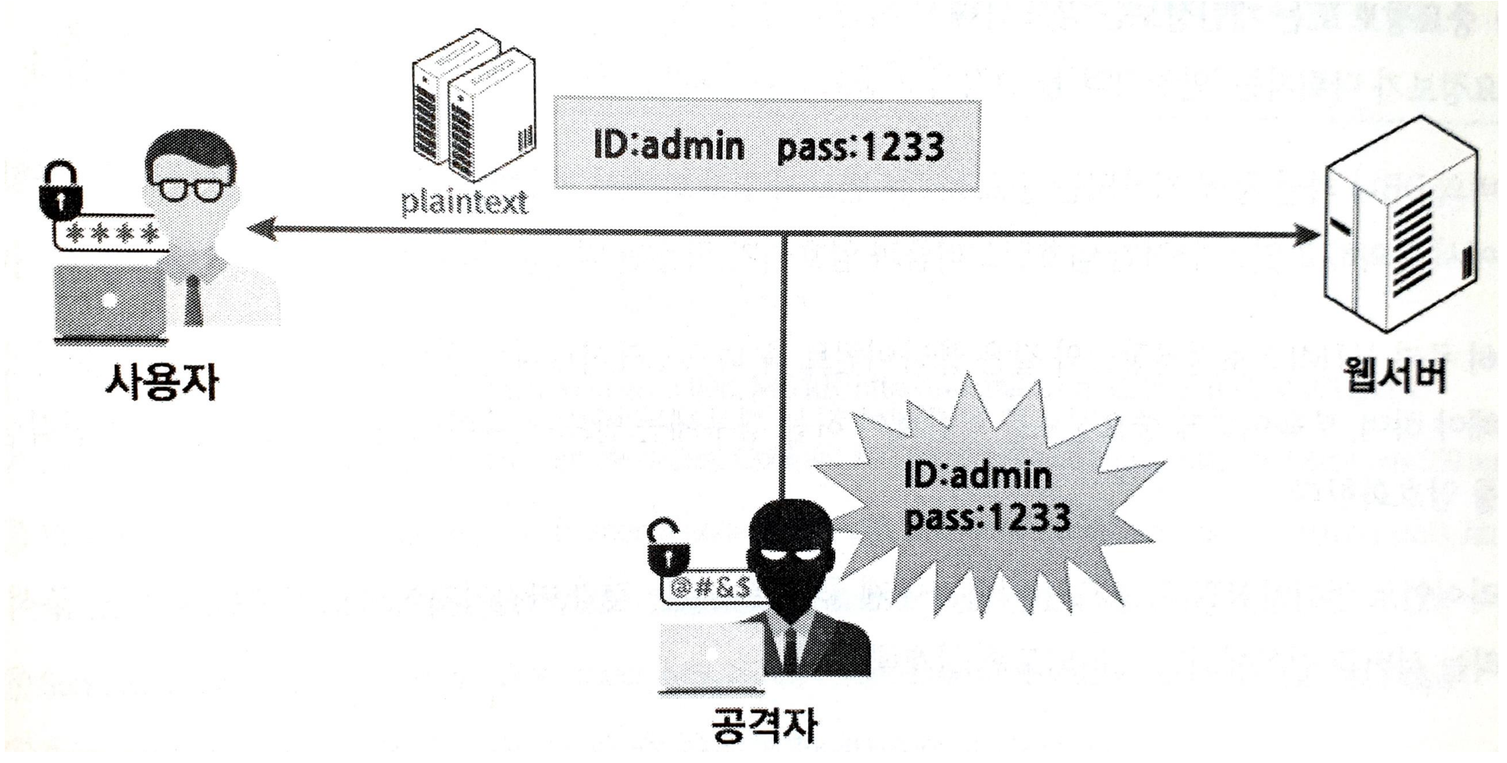
요구사항 분류	보안기능	요구사항번호	SR2-7
이름	중요 정보 저장		
설명	중요정보(비밀번호, 개인정보 등) 저장시 안전한 저장 및 관리방법을 설계해야 한다.		
요구사항내용	1. 중요정보 또는 개인정보는 암호화해서 저장해야 한다. 2. 불필요하거나 사용하지 않은 중요정보가 메모리에 남지 않도록 한다.		

보안 기능

중요 정보 저장

취약점 개요

- 사례 1 : 중요정보 평문저장
  - ❖ 메모리나 디스크에서 처리하는 중요데이터(개인정보, 인증정보, 금융정보)가 제대로 보호되지 않을 경우, 보안이나 데이터의 무결성을 잃을 수 있다. 특히 프로그램이 개인정보, 인증정보 등의 사용자 중요정보 및 시스템 중요정보를 처리하는 과정에서 이를 평문으로 저장할 경우 공격자에게 민감한 정보가 노출될 수 있는 취약점이다.



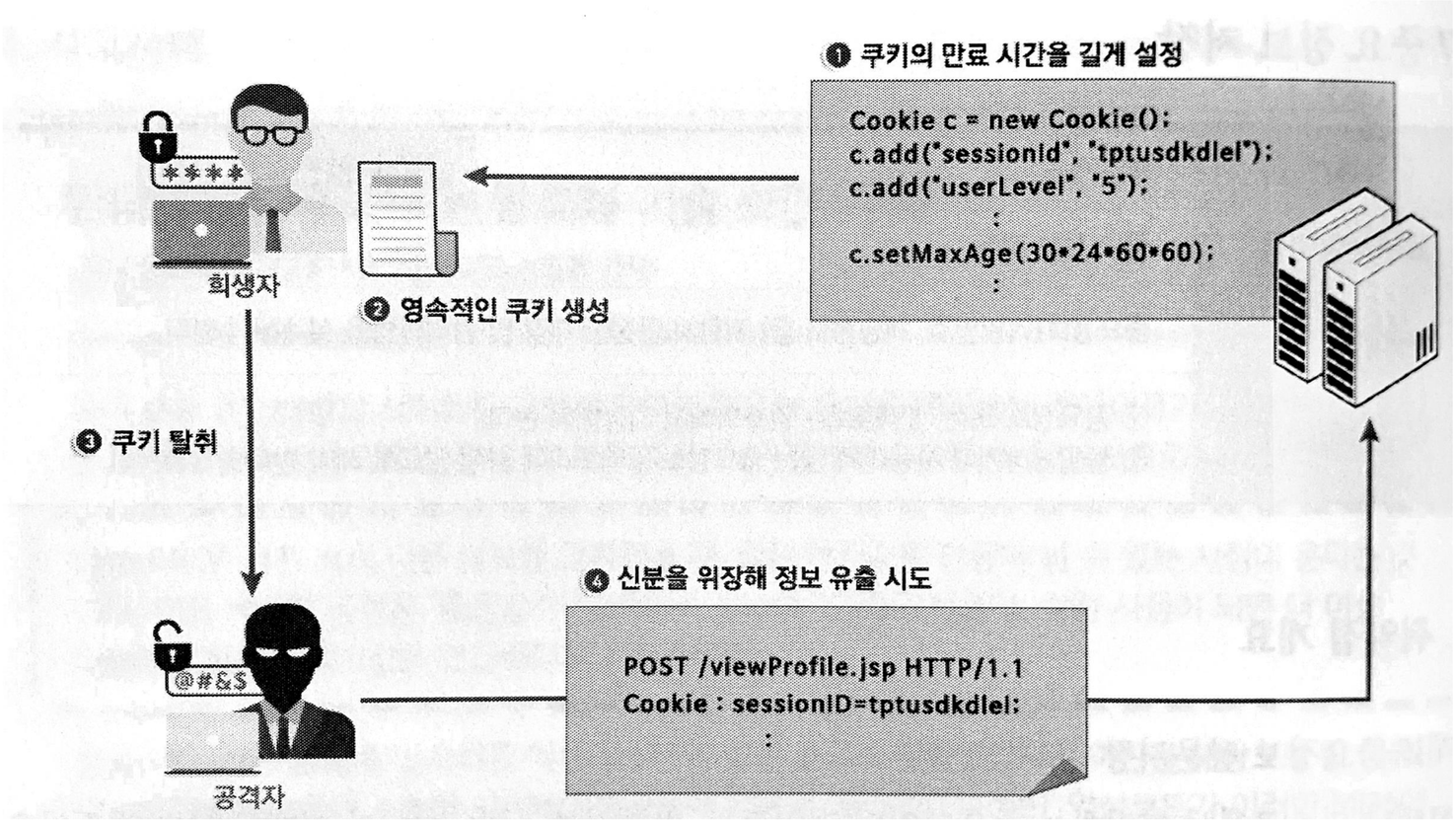
중요정보 평문저장

보안 기능

중요 정보 저장

취약점 개요

- 사례 2 : 사용자 하드디스크에 저장된 쿠키를 통한 정보노출
  - ❖ 개인정보, 인증정보 등이 영속적인 쿠키에 저장된다면 공격자는 쿠키에 접근할 수 있는 보다 많은 기회를 가지게 되며, 이는 시스템을 취약하게 만든다.



사용자 하드디스크에 저장되는 쿠키를 통한 정보노출

보안 기능

중요 정보 저장

설계시 고려사항

1. 중요정보 또는 개인정보는 암호화해서 저장해야 한다.
   - ❖ 중요정보가 다뤄지는 “안전영역 " 을 설정하고 중요정보가 해당 영역 외부로 누출되지 않도록 설계한다.
   - ❖ 서버의 DB나 파일 등에 저장되는 중요정보는 반드시 암호화해서 저장해야 하며 “암호연산“ 보안요구항목에서 정의하고 있는 안전한 암호알고리즘과 암호키가 적용된 암호화 정책이 적용되어야 한다.
   - ❖ 특히 쿠키, HTML5 로컬저장소와 같은 클라이언트 측 하드드라이브에는 중요정보가 저장되지 않도록 설계해야 하며, 부득이하게 중요정보를 저장해야 하는 경우에는 반드시 클라이언트 측에 저장되는 민감정보를 암호화한다.
   - ❖ 클라이언트 언어인 HTML 코드는 사용자에게 공개되어 있는 것과 마찬가지이므로 중요한 로직 및 주석처리는 서버측 언어에서만 처리되도록 설계해야 한다.

보안 기능

중요 정보 저장

설계시 고려사항

2. 중요정보가 메모리에 남지 않도록 해야 한다.
   - ❖ 개인정보 또는 특정 금융정보를 처리하는 기능 구현시 더 이상 필요하지 않은 데이터에 대해 메모리를 초기화하여 중요데이터가 메모리에 남지 않도록 시큐어코딩 규칙을 정의한다.
   - ❖ 특히 민감한 정보를 포함하는 페이지는 사용자 측 캐싱을 비활성화 하도록 제한적인 캐시정책을 수립하여야 하며, 부득이 캐싱을 해야 하는 경우 캐싱되는 정보는 암호화하여 저장하도록 설계한다.
   - ❖ 인증정보와 같은 민감한 정보를 포함하는 웹 폼을 구현하는 경우 자동완성 기능을 비활성화 하도록 시큐어코딩 규칙을 정의한다.

보안 기능

중요 정보 저장

소프트웨어 보안

사고 사례

KB·롯데·NH농협카드, 주민번호 암호화 안해

사상 최악의 개인정보 유출 사태를 촉발시킨 KB국민카드와 롯데카드, NH농협카드가 주민번호를 암호화 하지 않아 2차 피해에 심각하게 노출된 것으로 드러났다.

주민번호가 암호화돼 있으면 유출되더라도 도용할 수 없지만 이들 카드사들이 주민번호를 암호화하지 않으면서 스스로 사태를 확대시킨 셈이고 "2차 피해 가능성은 없다"는 카드사들의 주장은 신빙성을 잃어가고 있다.

23일 금융감독원과 금융권에 따르면 KB국민카드와 롯데카드, NH농협카드는 주민번호를 암호화하지 않았다.

보안 기능

소프트웨어 보안

8. 중요 정보 전송

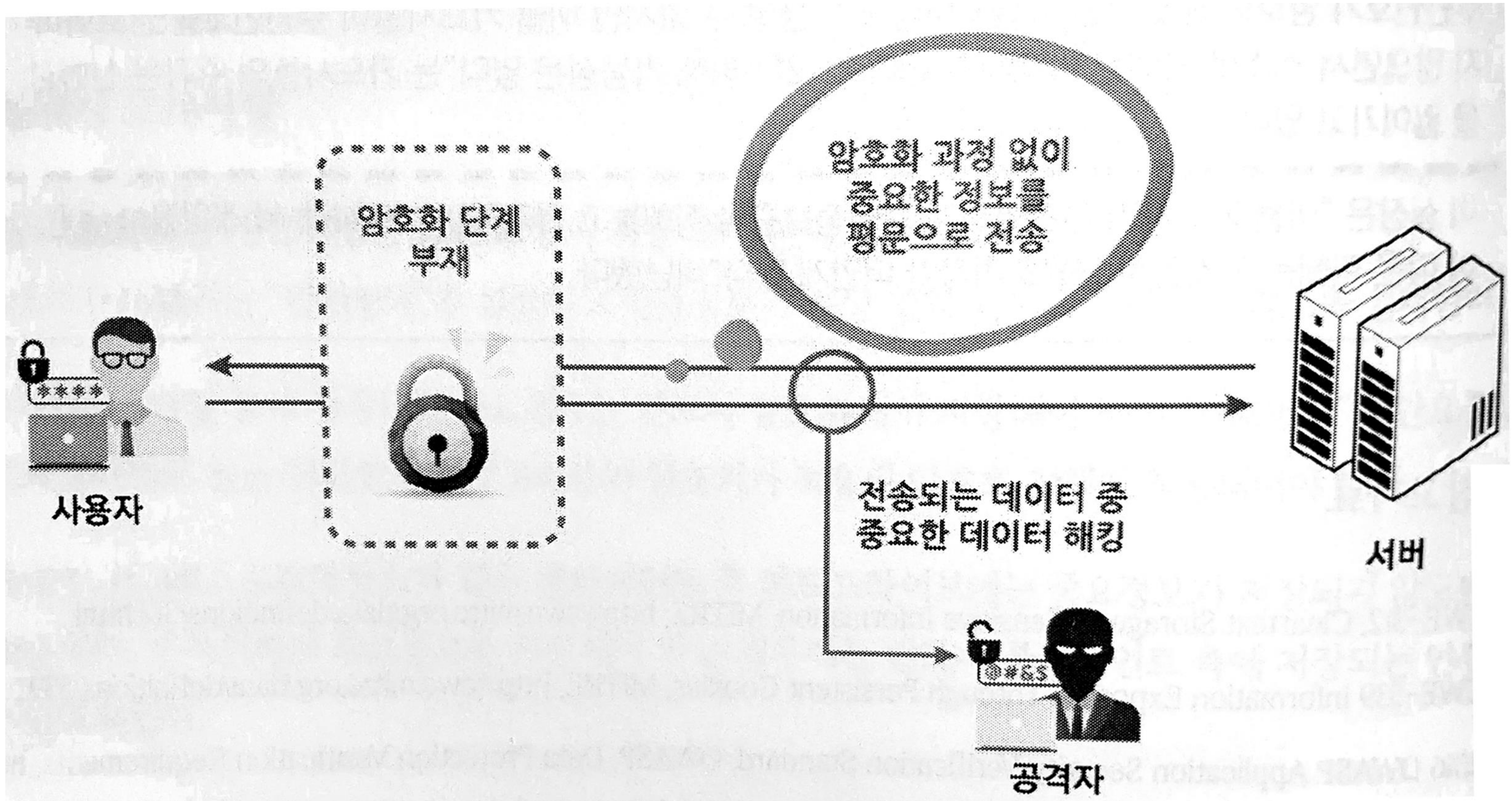
요구사항 분류	보안기능	요구사항번호	SR2-8
이름	중요 정보 전송		
설명	중요정보(비밀번호, 개인정보 등) 전송시 안전한 전송방법을 설계해야 한다.		
요구사항내용	1. 인증정보와 같은 민감한 정보 전송시 안전하게 암호화해서 전송해야 한다. 2. 쿠키에 포함되는 중요정보는 암호화해서 전송해야 한다.		

보안 기능

중요 정보 전송

취약점 개요

- 프로그램이 보안과 관련된 민감한 데이터를 평문으로 송•수신할 경우, 통신채널 스니핑을 통해 인가되지 않은 사용자에게 민감한 데이터가 노출될 수 있다.



중요정보 평문전송

보안 기능

중요 정보 전송

설계시 고려사항

1. 인증정보와 같은 민감한 정보 전송시 안전하게 암호화해서 전송해야 한다.
   - ❖ 분석단계에서 정의된 중요정보를 네트워크를 통해 전송해야 하는 경우 안전한 암호모듈로 암호화한 뒤 전송하거나 안전한 통신 채널을 사용하도록 설계한다. 안전한 암호화는 “암호연산“ 요구항목을 충족시키는 암호화 알고리즘이나 암호키를 사용한다.
   - ❖ 웹 애플리케이션 설계시 클라이언트에서 서버로 전달되는 데이터(hidden 필드, Ajax 변수, 쿠키, 헤더 값) 또는 클라이언트로 전달되는 데이터(HTTP 응답헤더 포함) 중 불필요하게 많은 데이터가 전송되지 않도록 설계한다.

2. 쿠키에 포함되는 중요정보는 암호화해서 전송해야 한다.
   - ❖ 쿠키에는 중요정보가 포함되지 않도록 설계해야 하지만 부득이 쿠키에 중요정보가 포함되어야 하는 경우에는 반드시 세션쿠키로 설정되어야 하며 전달되는 중요정보는 반드시 암호화해서 전송해야 한다.

보안 기능

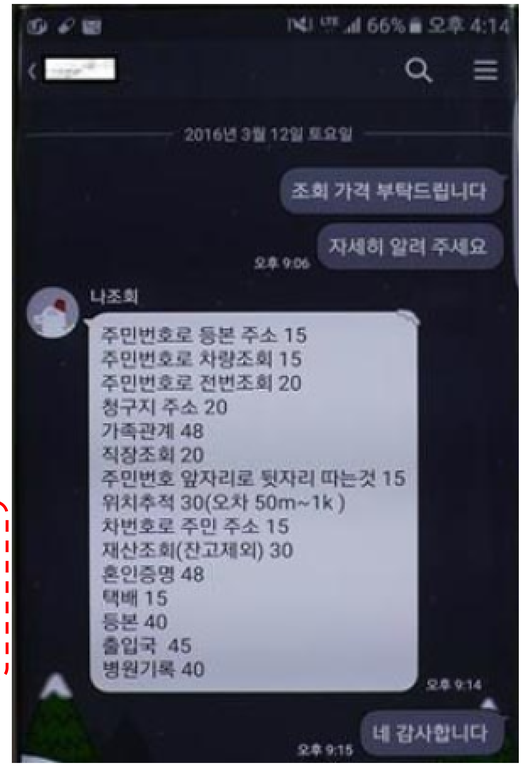
중요 정보 전송

소프트웨어 보안

사고 사례

경찰, 이통사 위치정보 서버 해킹해 판매한 일당 검거

또한 이들에게 위치정보 추적과 미행 등을 의뢰한 의뢰인 34명도 불구속 입건했다. 의뢰인 34명 중 약 80%는 외도가 의심되는 배우자의 사생활 뒷조사를 위해 의뢰했고 기타 채권·채무자나 헤어진 여자친구의 소재를 파악해 달라는 의뢰도 있었다.



(자료 : 서울지방경찰청 제공)

홍씨는 2014년 9월 18일부터 올해 5월 26일까지 647회에 걸쳐 개인정보를 판매해 2억7477만원 상당의 부당이득을 챙긴 혐의를 받고 있다. 또 해커 김모(27·구속)씨는 피처폰(일반 휴대전화)의 취약점을 이용해 SKT의 위치정보 서버 주소(URL)를 획득하고 데이터(패킷) 분석·송수신 프로그램을 이용해 추적한 위치정보를 홍씨에게 건당 30만원에 넘겼다. SKT의 위치정보 서버는 위치정보를 암호화하지 않은 평문으로 전송한 것으로 논란이 될 것으로 보인다.

다른 이통사들은 특정 IP에서만 위치정보를 조회할 수 있도록 제한하고 위치정보가 조회됐을 때 이용자에게 그 사실을 문자로 통보해 왔다. 하지만 SKT는 경찰로부터 범죄에 이용됐다고 통보받은 6월 초까지 이와 같은 체계가 없었던 것으로 밝혀졌다. 이에 대해 경찰은 관리 소홀 등 이통사의 책임 여부에 대해서도 조사하고 있다.