정보 윤리 소책자

간단한 비밀번호로 중대한 사건!

【 목표와 포인트】

1. 패스워드의 중요성과 그 결정 방법에 대해 이해한다.

   - 패스워드가 해킹 당하면 어떤 피해를 입을 가능성이 있는지 이해한다.
   - 패스워드는 보통 어떤 방법으로 해킹 당하는지 이해한다.
   - 안전한 패스워드를 어떻게 정하는지 이해한다.

2. 시스템적으로 좋은 패스워드를 선정해도 약점이 있으면 해킹 당한다. 소셜엔지니어링이나 다른 시스템간에 같은 패스워드를 설정하는 문제에 대해 이해한다.


해라 유 이화
이화~
과제는 끝났어?
비밀번호는
어떻게 됐어?
이제 집에
가려구
아니, 아직 다
안 됐는데
오늘은 끝~~
다행이네...
근데 꽤 쉬운
비밀번호를
한거 아냐?
그럴리가
없지~
괜찮아~ 난
비밀번호를
잊을일이
없어~
아..
재발급은 됐는데...
이화도 조심하는게 좋을꺼야..


그래? 근데 자주
있는 일이,
자기 생일이나
전화번호나..
그리고...
ID랑 비밀번호를
똑 같이 한다거나..
그게..
ID를
알아내면
비밀번호도
...
혹시
이화~
너 비밀
번호가...
생일이라던가?!


그....
그건...
아냐!!
음... 그래도
조심해야할꺼야~!
안녕~~


아무래도
비밀번호는
변경해야겠다
123456778
*****
ID또는 비밀번호가
틀렸습니다.
OK


아...
뭐야~
방금전까진
됐었는데!
아...
비밀
번호는
맞는데!
뭐지.
ID또는 비밀번호가
틀렸습니다
아...
아...
나도
정보센터에
가야만
하나....
아...
없어져..


긴급호출
경제학부
리카학생
실례합니다~
방금 비밀번호를
쓸 수 없게
됐는데요..


잠깐
안으로
들어
오시겠어요?
아..
이화씨
네?
무슨일...
무슨일
이세요??


이화 학생?
자..
앉으세요~
네..
방금전에
이화학생 ID를
정지 시켰어요.
네!?
정.지.
라구요?
무슨 말씀
이세요?
사실, 방금전에 삼우교육대학교에서
연락이 왔어요. 이상한 불법엑세스가
있다는 연락이 와서 조사를 해보니,
이화 학생의 ID가 쓰였어요.
그래서 일단 정지를 시켰습니다.
불법
엑세스요
?!
무슨
말씀인지
잘모르겠
어요..


이화 학생이
한게 아니라면
누군가가
학생 ID를
도용한거네요..
이화학생의
ID와
비밀번호를
훔쳐서
악용한것
같아요.
세..
ID가
도용
됐다구요?
어머..
이호양..
사태가 꽤
심각한 것
같아요?


접수처
ID나 비밀번호가 적힌 종이를 잃어버렸다거나.. 뭔가 짐작되는 일은 없어요?
특히 없는데요
쉬운 비밀번호였다거나 다른사람에게 가르쳐준적은?
아.. 그건..
역시..
누군가가 이화학생 ID를 사용해서 메일이나 파일을 읽어 봤을지 몰라요.
사실은 이틀전쯤에 같은 시간에 다른 두 기계에서 ID가 이용된 기록이 있어요.
아.. 그런일이... 저 어떻게 해야하죠?


이런경우엔.. 자기뿐만 아니라 다른 사람들에게도 피해를 주고 있어요..
네트워크를 사용할땐 ID와 비밀번호를 잘 관리해야돼요..
그리고 이화학생 메일이나 파일 등에 문제는 없는지 확인해 보세요
그앞이었 고로일록 리으러는도 !
네~ 조심하겠습니다
이호양.. 이번 사건은 비밀번호를 도용당한게 원인이네요... 비밀번호는 잘 관리해야죠..


네~
잘 알겠습니다!
그럼, 문제하나 내볼까요?
둘 중에 어떤 비밀번호가 좋을까요?
rika1130
R1i3A1KO
맞춰 보세요
음...
아래쪽 같은데요?
딩동~
비밀번호기 도용될 수 있는 방법을 알아보면,
우선 개인적인 정보에서 예를 들어 ID나 이름, 생일 등이 있어요.
생일은 학생증이나 블로그 같은곳에서 알아낼지도 모르죠..
또한, 사전에있는 단어를 추측해서 비밀번호가 될 가능성이 있는것을 조합해 보는 경우도 있어요
그러니까.. 좋은 비밀번호 설정은...
개인적인 정보는 사용하지 않고
사전에 있는 단어는 쓰지 않는다!
그리고 길고 대문자와 소문자 숫자를 섞어서 쓰는것입니다.
그래서 위쪽의 비밀번호는 적당하지 않아요
rika -> 이화의 이름


알고는 있었는데요. 제가.. 건망증이 심해서 외우기 쉽게 ID와 똑같이...
안돼! 안돼!
자기 비밀번호나 그 힌트는 다른 사람에게 알려주면 안 돼요! 예를들어, 정보센터에서 시스템장애로 인해 비밀번호 재설정 하니까 알려달라고 하면 어떻게 해야할까요?
센터직원이면.. 알려줄것 같은데..
그건.. 안 되는 거죠?
맞아요!! 절대로 가르쳐 주면 안 돼요!
시스템장애인척하며 비밀번호를 알아내는 방법 등으로 비밀번호를 부정하게 취득하는 수법을 소셜엔지니어링 (Social Engineering) 이라고 해요.

용어 【자료】

정보보안

조직이 가지고 있는 여러 가지 정보를 안전하게 관리하기 위한 규칙을 어떻게 만들까를 생각한다. 정보를 안전하게 지키려면 조직으로서 정보취급방법규칙을 결정하여 의사소통을 도모하는 것이 반드시 필요하다. 또, 다수의 멤버가 있는 경우에는, 지켜야 할 규칙들을 문서로 만들 필요가 있다. 정보보안대책에서는 정보보안대책 본연의 자세에 대한 조직으로서 대책(방침이나 목표)을 결정하여 거기에 따른 자세한 규칙을 순서대로 정해서 문서화 한다.

암호

특정인에게만 전하기 위해, 그 특정인 이외에는 아무도 모를 듯 한 방법으로 전하고 싶은 것을
나타내는데 그것을 암호라고 한다. 암호 전의 메시지를 평문, 암호화한 후의 메시지를 암호화라고 부른다. 또, 암호문을 원래 메시지로 돌아가는 것을 복호화라고 한다. 암호화나 복호화를 할 때는 키가 필요하지만 이 키가 공통인 것을 공통키 암호(대상키 암호, 비밀키 암호), 짝을 이루는 다른 키를 사용하는 것을 비대칭키 암호(공개키 암호) 라고 한다.

소셜 엔지니어링

사람의 허점을 노려서 패스워드 등을 부정하게 취득하는 방법. 본편에서는 시스템관리자로 가장하여 패스워드를 묻기 시작하려고 하는 예를 들었지만, 그 이외에도 여러 가지 수법이 있으므로 주의해야 한다. 예를 들면, 보안에서 유명한 기업으로 가장해, “보안에 관계된 중요한 일이므로 이 URL에 접근해 주세요. 첨부파일를 읽어주세요.” 등과 메일을 보내 가짜 사이트로 유도하는 예도 있다. 다른 확실한 수단을 이용하고, 그 정보가 사실인지, 아이디나 패스워드 등의 정보를 정말로 넣을 필요가 있는지 등, 침착하게 판단해야 한다.

부정접근행위금지 등에 관한 법률

인증정보의 부정취득을 막기 위해, 2001년에 시행되었다. 타인의 아이디로 무단 로그인을 하면, 그 밖에 아무것도 하지 않고 로그인 한 것만으로도 법률위반이 된다. 무단 로그인을 당한 쪽은 피해자이지만, 그 아이디로 이루어진 행위에 의해, 가해자로도 될 수 있다. 간편한 패스워드는 피할 것. 친구 사이 아이디를 빌려 쓰는 것도 엄금한다.

패스워드 관리

우리는 오늘날의 정보사회에서 여러 가지 시스템으로 아이디나 패스워드를 이용하고 있다. 아이디와 패스워드의 관리 방법은 각 시스템에 따라 다르지만, 정보보안대책을 정한 신뢰할 수 있는 기관에서는, 본인만 알 수 있게 암호화되고 관리되고 있다. 그러나 그렇지 않은 수상한 시스템이 존재하는 것도 사실이다. 각 아이디의 중요성의 차이를 생각하지 않고, 무엇이든지 같은 패스워드를 설정하면 관리가 잘된 시스템으로부터 패스워드가 뚫리게 되므로 주의해야 한다.

인터넷 이용 시, 패스워드 [재사용]이 대다수

2011년 6월 16일 갱신　ITmedia

http://www.itmedia.co.jp/news/1106/16/news024.html

유출된 약 4만 명의 이용자계정을 분석한 결과, 동일한 사용자라고 판단되는 2천개 이상의 계정 중 92% 이상이 두 가지 경우에 동일한 암호를 재사용하고 있었다. 또 다른 유출 데이터에서 일반 전자메일 계정이 있는 88건을 추출하였고 이중 70%의 사용자가 동일한 암호를 재사용하고 있었다. 분석 결과, 암호에 포함된 문자열을 확인하고 숫자, 대문자, 소문자 등을 조합하고, 소문자 같은 한 종류만을 이용한 암호를 설정한 경우가 절반 가까이 있었다. 자세한 내용은 위를 참조한다. 당신은 괜찮습니까?

인터넷 서비스 부정 이용 (정보처리추진기구보안센터 2012년 1월)

정보처리추진기구 시큐리티센터는 2011년을 정리하며 인터넷 서비스 부정 이용을 다루었다. 부정 이용의 원인으로는 바이러스 감염이나 피싱 등이 있으며, 피해 확대의 원인으로는 동일한 ID와 패스워드의 재사용이 거론되고 있다.

앞으로는 패스워드를 재사용하는 사람을 대상으로, 지금까지는 표적이 되지 않았던 무료 서비스를 포함하여, ID, 패스워드 재사용을 하지 않기, 쉬운 암호 사용 안 하기 등을 안내할 예정이다.

인터넷에서의 암호【암호화】

암호는 훨씬 예전부터 누군가에게 비밀의 메시지를 보내기 위한 것 등에 사용되어 왔다.

제2차세계대전에서 암호해독의 역사는 상징적인 것이다. 오늘날 인터넷상에서는 정보를 안전하게 교환하는 것 등에 암호가 사용되고 있다. 공개키 암호 등 암호방식의 대책은 생략하지만 본편에 있듯이 패스워드의 암호화와 통신의 암호화의 차이를 생각해보자. 당연 이야기지만, 패스워드는 시스템 상에서 보존되고 있는데 비해, 통신에서는 상대가 존재하여 상대에게 메시지를 전할 필요가 있다.

패스워드 암호화

입력한 문자열을 시스템 상에 보존하고 있는 것과 비교하여 인증을 실시한다. 구체적으로는 패스워드로 입력한 문자열을 요약함수 등을 사용해 요약한 값과 인증 서버상의 패스워드 요약값을 비교한다. 요약 값으로부터 원래로 되돌리지 못하고, 또, 다른 문자열로부터 똑같은 요약 값을 만드는 것은 더없이 곤란한 방식을 사용한다.

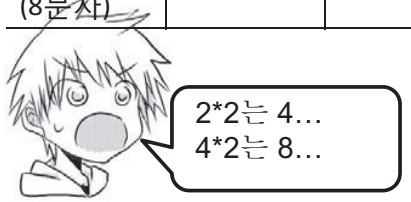
통신의 암호화

신용카드암호를 온라인 쇼핑몰 사이트에서 입력하는 경우 등에서는 안전하게 통신을 하는 것이 필요하다. 인터넷 상에서는 제3자의 통신 데이터가 도청될 가능성이 있기 때문에 도청되어도 해독할 수 없게 메시지를 암호화한다. 물론, 통신상대에게 도착한 시점에서 그 메시지를 복원(복호화) 한다.

당신의 패스워드는 숫자만으로 되어있지는 않겠지요?

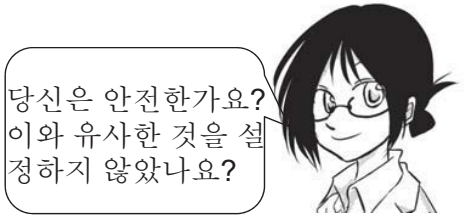
패스워드는 대문자, 소문자, 숫자 등을 혼재시키는 것이 좋다. 패스워드를 은행의 비밀번호등과 같이 생각해서 숫자만으로 설정한 사람은 패스워드를 변경하도록 하는 것. 만약, 1초에 10만 번의 빠르기로 패스워드를 생성하고 해독을 시도했다고 가정하면 각각 어느 정도의 시간에 모든 패스워드를 시험할 수 있을까. 아래와 같이 공란에 계산결과를 넣어보자. 물론, 이것들은 단순한 기준에 지나지 않지만 대문자. 소문자. 숫자를 조합하는 중요성을 생각해 보는 것이 필요하다.

	숫자	영어 (소문자)	전체영어	영어와 숫자
문자의 종류	10	26	52	62
2문자 조합	10＊10	26＊26	52＊52	62＊62
4문자 조합	10^4 1만	26^4 약 46만	52^4 약 730만	62^4 약 1480만
8문자 조합	10^8 1억	26^8 약 2100억	52^8 약 50조	62^8 약 220조
16문자 조합	10^{16}	26^{16}	52^{16}	62^{16}
해독시간 (4문자)	0.1초	약 5초		약 150초
해독시간 (8문자)	약 17분	약 24일	약 17년	



취약한 ID와 패스워드 【유출정보의 분석 등으로부터】

정보유출피해가 있었던 패스워드를 분석한 결과이다. 공격자를 유인하기 위해서 일부러 취약한 시스템을 인터넷 상에 두어, 공격자의 공격수법을 조사한 것 도 있다. 이러한 공격자는 보통, 리카가 걱정하는 것 같이 개인적인 메일이나 파일을 읽는 것에 목적이 없다. 해킹한 아이디와 패스워드를 이용하여 연쇄적인 부정 이용을 하는 것으로, 개인의 경우에는 금전을 노리거나 기업 등에 대해서는 정보를 노리거나 한다. 또한 봇(bot)이라고 불리는 컴퓨터 바이러스 장치 네트워크를 통해 감염된 컴퓨터를 조종하거나 가짜 웹사이트를 구축하기도 한다. 이것은 암호를 도난 당하는 것으로 가해자가 될 가능성을 의미하고 있다.
비록 시스템에 중요한 데이터가 없다 하더라도 쉬운 설치 암호를 설정하지 말라는 것이다. 공격자에게 공격 당한 암호의 예는 다음과 같다.



취약한 패스워드의 예

ID와 같은 패스워드

123456, password, 0, 1, qazwsx, admin, test, 123qwe, 1qaz2wsx, qwerty, 123qaz, 1234, 12345, psswd, 123, 이와 같은 조합, 등