5.8 사이버 보안

개요

인터넷은 여러 보안 위협으로 가득 차있습니다. 그 중 한가지 큰 위협은 **사이버 공격**으로, 해커가 악의적인 목적으로 컴퓨터 시스템과 네트워크를 대상으로 공격을 시도하는 것입니다.
사이버 보안은 시스템과 관련 있는데 웹사이트와 사용자가 사이버 위협에 스스로 더 잘 대처할 수 있도록 하는 것을 말합니다.
사용자는 더 안전한 비밀번호를 사용하고 스팸 메일을 보지 않는 등 다양한 방법으로 그들 스스로 사이버 위협을 방어해야 합니다.

핵심개념

* 사이버 공격
* 사이버 보안
* 피싱
* 이중 인증
* SSL

비밀번호

많은 사람들이 비밀 번호를 쉽게 기억하기 위하여 서로 다른 웹사이트에서 같은 비밀번호를 사용합니다. 하지만 이것은 보안 위협을 많이 받도록 하는 원인이 됩니다. 만약 해커가 하나의 웹사이트에서 여러분의 비밀번호에 대한 접근 권한을 획득하면, 여러분이 가입한 모든 웹사이트의 비밀번호를 알고 접속할 수 있습니다. 이런 상황을 방지하기 위하여 비밀번호 관리자는 여러분이 입력하는 비밀번호를 암호화시켜 저장하기도 합니다.

해커는 다양한 방법으로 비밀번호 획득을 시도할 수 있습니다. 그들은 가능한 사용자의 아이디와 비밀번호 조합을 수 백만 번 시도합니다. 따라서 보안을 강하하기 위해서 더 길고 복잡한 비밀번호를 사용해야 합니다.

또한 해커는 사용자에게 일반적인 **회사를 사칭하는 메일을 보내고 링크로 접속하는 것을 유도하여 사용자의 비밀번호와 민감한 정보를 요청**하는 **피싱 공격(phishing)**도 할 수 있습니다.

구글, 페이스북과 같은 몇몇 서비스는 비밀번호 도용 방지 수단으로 **이중 인증**을 제공합니다. 이중 인증을 사용하면 로그인하기 위해 사용자 아이디와 비밀번호를 사용하는 것은 물론 다른 정보도 필요로 합니다. 예를 들면 웹사이트에서 여러분 휴대폰에 인증코드를 보내 로그인할 때 입력하게 합니다. 이중 인증을 사용할 때의 보안 이점은 누군가가 여러분의 비밀번호를 얻게 되더라도 휴대폰에 전송되는 인증코드를 알 수 없어 여러분 계정에 접근할 수는 없다는 것입니다. 하지만 만약 휴대폰을 잃어버렸거나 휴대폰의 신호가 없으면 여러분은 계정으로 접속할 수 없게 되기 때문에 로그인이 불편해질 수도 있습니다.

보안 소켓 계층

HTTPS(HTTP Secure)는 HTTP와 **보안 소켓 계층(SSL)**이라고 불리는 기술을 결합한 인터넷 통신 프로토콜입니다.
SSL을 사용하는 웹사이트는 각각 인증서를 갖고 있는데 이것은 웹사이트에 접근하려는 사용자에게 제공됩니다. **인증서는 웹 브라우저에게 웹 서버로 보내진 요청을 어떻게 암호화했는지 말해주는 공개키를 포함**합니다. 웹 서버는 **암호화된 요청을 해독하는 다른 키인 비밀키**를 갖고 있습니다.

그 외의 사이버 공격

해커는 사이버 공격을 수행하기 위하여 다양한 기술을 활용합니다. 웹 서버와 사용자 사이에는 DNS 서버와 라우터 등으로 악성 코드를 보내 https://를 http://로 바꿀 수 있습니다. 그 결과 사용자가 봤을 때는 정상적인 사이트이지만 실제로는 그렇지 않은 사이트로 변경됩니다. 이러한 방법을 **중간자 공격**이라고 합니다.

세션 하이재킹은 웹사이트에 접속할 때 자동적으로 만들어지는 임시파일로 사용자의 정보가 담겨있는 **쿠키**를 얻기 위해 상대방의 네트워크 트래픽을 관찰하고, 상대방의 HTTP 헤더에 쿠키를 사용하여 상대방을 다른 사람으로 생각하도록 웹 서버를 속이는 기술입니다.