ICT 0514

Security

Security는 굉장히 중요한 문제. 현재 Security에 대한 문제는 잘 해결되고 있는가

IoT가 급성장하면서 IoT를 공격하는 프로그램이나 소프트웨어들도 급증했다. 600% 정도 급증한 것으로 나타남.

직접 공격을 하는게 아니라 다른 사람의 컴퓨터를 이용해서 Hop을 하면서 몇 단계를 거치기 때문에 Origin을 찾기가 굉장히 어렵다.

모바일 보안 위협이 지속적으로 증가하는 추세. Coin mining – 코인 채굴 공격이 2017년에 85배 급증. 훔친 처리 능력과 클라우드 CPU사용량을 이용하여 암호 화폐를 채굴.

공격의 71%가 스피어 피싱으로 시작

합벅적인 소프트웨어 패키지에 악성 코드를 심는 소프트웨어 업데이트 공급망 공격 – 최대 200% 증가.

기밀성, 무결성, 가용성, 인증, 부인방지, 접근제어, 추적불가능, 익명성, 확장성, 실시간성

사이버 공격의 목적

정보를 퐘한 재산탈취 및 주요 시설 파괴가 목적. 사이버공격은 사이버를 활용해서 행하는 공격. 주로 정부기관에서 시작하는 경우가 많다. (사이버 전쟁은 암암리에 지금도 진행중이다.) 정부기관에서 87% 이상이 비롯된다.

우리나라는 1~2년마다 대규모로 사이버 공격에 의한 피해가 많다.

주로 발표는 북한의 소행이라고 하지만, 정확한 Origin을 알기에는 굉장히 어려움이 따른다.

코드에 나오는 특수한 패턴 등을 보고 파악하곤 한다.

병원 – 원격으로 정보송수신도 가능하지만 원격으로 제어하는 것도 가능하다.

약물투여나 심박기 등을 제어 가능 -> 윤리적인 문제로 번지는 경우가 많다.

GPS를 해킹하는 것은 굉장히 쉬운 일이다. – 인공위성 3개에서 오는 신호를 가지고 거리를 측정한 다음에 원을 그려서 측정 - > 오차범위가 몇십M밖에 되지 않음.

옆에서 가짜 신호를 보내면 오동작하는 경우가 생김 -> 비행기에 문제가 생길 경우 심각한 피해를 입힐 수 있다.

GPS는 미국에서 만든 기술. 민간용이 있고 군사용이 있다. 군사용은 훨씬 정밀하다. 축구공 크기의 오차도 구분해 낼 수 있는 정도.

현재 드론의 보안수준 – 간단한 해킹 공격만으로도 쉽게 뚫릴 수 있을 정도.

헬스케어

정보유출, 정보 위변조, 랜섬웨어의 3가지 유형으로 범죄가 일어날 수 있다.