정보보호개론

교과 소개

1. 정보보호와 암호기술

정보보호(information security)와 관련하여 바이러스(virus), 스파이웨어(spyware), 백신(vaccine), 피싱(phising), 스팸 메일, 해킹, 침입탐지 및 예방(intrusion detection, prevention), 분산 서비스 거부 공격(distribued denial-of-service attack), 방화벽(firewall) 등의 용어를 대중 매체를 통해 많이 접할 수 있다. 이들 용어 외에도 인증서(certificate), 전자 서명(digital signature), 비트코인(bitcoin), 블록체인(blockchain), 대체 불가능 토큰(NFT, Non-fungible token) 등과 같은 용어도 접할 수 있다. 이 교과에서는 전자와 관련된 정보보호 기술은 다루지는 않는다. 대신 후자 등과 같이 **암호기술**(cryptography)을 사용하는 정보보호 기술을 다룬다. 물론 최근 악성 소프트웨어 중 랜섬웨어는 전자와 관련된 것이지만 암호기술을 원래 목적과 다르게 공격에 활용하고 있다.

암호기술은 디지털 세계에서 정보보호 서비스를 제공하기 위해 사용하는 도구 집합(tool-kit)을 말한다. 하지만 정보보호 서비스를 제공하기 위해 사용하는 모든 기술을 암호기술이라 하지 않는다. 정보보호 서비스를 제공하기 위해 디지털 정보에 직접 적용하는 수학적 이론에 바탕을 두고 있는 알고리즘과 이를 응용한 프로토콜을 암호기술이라 한다.

우리가 IT 기술 좁게는 컴퓨팅 기술을 학습할 때 그 기술이 등장한 배경이나 그 기술을 활용하는 환경을 이해할 필요가 있으며, 급속하게 발전하는 IT 기술을 고려하였을 때 IT의 최근 트랜드를 이해할 필요가 있다. 현재 제4차 산업혁명이라는 것이 화두이다. 쉽게 이해하면 오래전부터 언급된 유비쿼터스 시대의 보편화 및 지능화이다. 유비쿼터스는 5A(any where, any time, any device, any network, any service)로 설명되는 컴퓨팅 환경으로 언제, 어디서나, 어떤 장치를 사용하여 어떤 네트워크이든지 원하는 서비스를 받을 수 있는 환경을 말한다. 사물인터넷(IoT, Internet of Things)이 현실화되면서 초연결 시대로 접어들고 있으며, 5A가 더는 미래의 이야기가 아니라 오늘의 현실이 되고 있다. 유비쿼터스의 또 다른 특징은 내재성(pervasive)이다. 우리가 인식하지 않더라도 지능적으로 현재 상황을 인지(context-aware)하여 서비스가 이루어지는 시대가 되고 있다. 네트워크 환경도 점점 전부 인터넷 통신 기술을 사용하는 환경으로 변하고 있다. 이를 “All IP 시대”라 한다.

오늘날 IT 기술의 또 다른 중요한 특징은 융합이다. 더는 학문의 경계를 논하기 어렵게 되었다. 특정 제품이 특정 공학 분야의 전유물이던 시대는 끝났다. 이제 자동차는 기계공학 분야로 제한되지 않고, 전자공학 더 나아가 컴퓨터공학 분야로 전환되고 있다.

이와 같은 컴퓨팅 환경의 변화는 정보보호의 중요성을 더욱 높이고 있다. 정보화는 우리 삶의 편리성에 획기적 변화를 가져오고 있지만 정보화는 보안 위협에도 매우 의미심장한 변화를 초래한다. 이와 같은 위협을 대처하지 못하면 보안 수준은 정보화 때문에 오히려 낮아질 수 있다. 예를 들어 영상 통화는 원격에서 서로의 얼굴을 보면서 대화를 할 수 있도록 해주지만 거꾸로 우리도 모르게 우리 사생활이 노출될 수 있는 위험도 있다. 또 앞서 소개한 랜섬웨어처럼 정보보호 기술이 오히려 공격 기술로 활용할 수 있고, 범죄 목적으로 사용할 수 있다.

이처럼 IT 기술의 발달은 순기능만 있지 않고 역기능도 존재할 수밖에 없다. 특히, 초연결 시대에 개인 프라이버시 침해는 더욱 심해지고 있다. 이를 극복하기 위해 다양한 기술이 연구되고 있으며, 법률도 제정되고 있다.

하지만 IT 기술의 발달은 공격 기술의 발달을 의미한다. 이 때문에 공격이 쉬워지고, 피해 전파 속도나 공격의 파급 효과도 매우 커지고 있다. 또 사이버 공격의 경로가 PC, 스마트폰과 같은 기존 컴퓨팅 장치로 제한되지 않고, 냉장고, 로봇청소기, 자동차 등 다양한 스마트 기기와 제품이 대상이 되고 있다. 따라서 이를 방어하고 방지하기 위한 기술 개발이 매우 중요한 시대이다. 4차 산업혁명 시대에 필요한 각 종 서비스를 실현할 수 있는 기술은 있지만 그 서비스에 필요한 보안 요구사항을 충족할 수 없다면 그 서비스는 실제 도입되기 어렵다. 서비스 신뢰의 핵심은 보안이다.

이 교과에서 다루는 암호기술 측면에서 보면 학문적 공간에서만 멈물던 여러 기술이 최근에 실제 서비스에 많이 적용되고 있다. 이것은 컴퓨팅 기술과 암호기술에 대한 이론이 발전하여 충분히 효율적으로 또 안전하게 적용할 수 있는 기술이 되었기 때문이다. 특히, 블록체인과 암호화폐가 큰 학문적, 사회적 관심을 받음에 따라 더 발전된 암호화폐를 실현하기 위해 논문에서만 존재하였던 많이 기술이 서비스에 직접 구현되어 대중 앞에 모습을 나타내고 있다. 이것은 암호기술이 한 단계 더 발전하는 계기가 되고 있으며, 암호기술이 대중과의 거리가 가까워지는 계기도 되고 있다. 또 한편으로 정보보호 기술이 정보 서비스의 올바른 동작을 위해 필수 요소가 됨에 따라 이들 서비스에 필요한 여러 암호기술에 대한 표준이 갱신되고 새롭게 제정되고 있다. 이 표준은 경쟁을 통해 보통 채택되며, 이 경쟁 과정에서 기술은 한 단계 더 발전하게 되는 효과가 있다. 이와 같은 표준은 서비스 안전성에도 큰 기여를 한다.

2. 정보보호 분야

정보보호 분야는 다양하게 분류할 수 있지만 크게 프로그램 보안, 시스템 보안, 네트워크 보안, 응용 보안, 기타 보안으로 분류하여 생각해 볼 수 있다. 프로그램 보안은 설치된 또는 실행 중인 소프트웨어의 허점을 활용한 공격을 방어하는 기술을 말하며, 공격자가 활용할 수 있는 허점이 없도록 소프트웨어를 강건하게 구현하는 기술과 기존 소프트웨어의 허점을 발견하는 기술로 나눌 수 있다. 이때 전자를 방어 프로그래밍(defensive programming), 안전 프로그래밍(secure programming)이라 한다. 정보보호에서 허점을 발견하는 이유는 이를 이용하여 공격하는 것이 아니라 보완하여 공격에 활용될 수 없도록 하는 것이다.

시스템 보안은 시스템 침입에 성공한 공격자의 악의적인 행동으로부터 시스템을 보호하는 기술을 말한다. 이를 위해 공격자가 활용할 수 있는 시스템의 허점을 발견하는 기술과 공격자가 침입에 성공하였을 때 이에 대응하는 기술이 필요하다. 후자를 침입 탐지와 예방 기술이라 한다. 네트워크 보안은 크게 통신 트래픽 및 통신 메시지의 내용을 분석하여 공격에 대응하는 기술과 통신 프로토콜에 암호기술을 추가하여 공격자가 존재하더라도 프로토콜이 목적을 달성할 수 있도록 하는 기술로 나눌 수 있다. 이 경우 항상 프로토콜이 목적을 달성할 수 있도록 하는 것은 가능하지 않으므로 누구든지 프로토콜의 수행을 통해 부당한 이득을 얻지 못하도록 하는 것이 목표이다.

응용 보안은 각 응용의 기능 요구사항이나 보안 요구사항을 충족하기 위해 사용하는 보안 기술을 말한다. 예를 들어 전자선거는 일인일표, 비밀성, 매표방지 등의 요구사항이 충족되어야 하며, 이와 같은 요구사항을 충족시키기 위해 암호기술을 사용할 수 있다. 이 외에 컴퓨터 포렌식, 정보보호 정책, 정보보호 관련 법률, 정보보호 윤리, 정보보호 교육 등 앞서 언급한 보안 분야로 분류되지 않는 것도 있다. 현재 범죄 수사에서 정보기기에 대한 포렌식은 과학 수사에서 없어서는 안 될 요소가 되었다. 이 교재에서 다루는 암호기술은 통신 프로토콜의 보호와 응용 보안에 주로 사용한다.

3. 정보보호 핵심 서비스와 암호기술의 예

정보보호의 3대 핵심 서비스라 하면 비밀성, 무결성, 가용성을 말하며, 4대 핵심 서비스라 하면 여기에 인증이 추가된다. 이 4가지 중에 비밀성, 무결성, 인증은 주로 암호기술을 사용하여 제공한다. 따라서 이와 같은 측면에서 보면 암호기술이 매우 중요한 정보보호 기술 중 하나라는 것을 알 수 있다.

암호기술은 우리가 생각하였을 때 하기 힘든 것들을 가능하게 해준다. 예를 들어 원격에 있는 두 사용자가 네트워크를 통해 동전 던진기를 하고 싶다고 하자. 언뜻 생각하면 참여자가 정직하게 행동하지 않고 상대방을 속일 수 있기 때문에 원격에 있는 두 사용자 간의 동전 던지기를 할 수 없다고 생각할 수 있다. 하지만 암호기술을 사용하면 원격에서 두 사용자가 동전 던지기를 할 수 있다. 일반적인 동전 던지기는 상대방이 지켜보는 가운데 이루어지기 때문에 던지는 사람이나 맞히는 사람이나 속이는 것이 어렵다. 하지만 원격에서 이루어질 경우 던지는 사람은 쉽게 던지기의 결과를 속일 수 있으므로 이를 못하게 하는 장치가 필요하다. 다음 두 가지 특성을 만족하는 함수가 있으면 원격에 있는 서로 신뢰하지 않는 두 사용자가 동전 던지기를 할 수 있다.

- 특성 1. 모든 정수 x에 대해 $f(x)$를 계산하는 것은 쉽지만 $f(x)$로부터 그것의 원상을 얻는 것은 계산적으로 불가능[1](computationally infeasible)해야 한다. 특히, 원상이 짝수인지 홀수인지 구분할 수 없어야 한다.
- 특성 2. $x \neq y$이자만 $f(x) = f(y)$인 정수쌍 (x, y)를 찾는 것은 계산적으로 불가능해야 한다.

이와 같은 특성을 만족하는 함수 f가 있으면 다음과 같이 동전 던지기가 가능하다.

- 단계 1. A는 매우 큰 정수 x를 임의로 선택하여 $f(x)$를 계산하여 $f(x)$를 B에게 전달한다.
- 단계 2. B는 $f(x)$의 원상이 짝수인지 홀수인지 추측하여 그 결과를 A에게 전달한다.
- 단계 3. A는 단계 1에서 선택한 x를 B에게 전달한다.
- 단계 4. B는 x가 $f(x)$의 올바른 원상인지 확인한다.

위 과정을 간단히 분석하여 보자. B는 $f(x)$로부터 x에 대한 어떤 정보도 얻을 수 없다면 단계 2에서 A의 선택을 맞힐 확률은 50%이다. 이것은 특성 1 때문에 만족된다. A는 $f(x) = f(y)$인 하나는 짝수이고, 하나는 홀수인 서로 다른 두 수 x와 y를 찾을 수 있다면 단계 3에서 항상 자신이 유리한 값을 주어 B가 틀리도록 할 수 있다. 하지만 이것은 특성 2 때문에 가능하지 않다. 따라서 이와 같은 함수만 있으면 불가능한 것처럼 생각한 동전 던지기를 원격에서 할 수 있다. 실제 이와 같은 특성을 만족하는 함수가 존재하며, 이 교재를 통해 배우게 된다.

동전 던지기에서 사용하는 f 함수는 암호기술에서는 암호알고리즘(cryptograhic algorithm)으로 분류되며, 동전 던지기처럼 암호알고리즘을 이용하는 프로토콜을 암호프로토콜(cryptograhic protocol)이라 한다. 암호기술이라는 도구 집합은 암호알고리즘과 그것을 응용한 암호프로토콜로 구성되어 있다.

연습문제

1. 과거 컴퓨터가 없던 시대를 상상해 보자. 디지털 정보를 사용하지 않는 시대에 정보를 보호하기 위한 메커니즘을 생각하여 보자. 다음 각 상황에서 사용한 정보보호 방법을 제시하시오.
   ① 두 사람의 대화 내용을 다른 사람은 알 수 없도록 하고 싶다.
   ② 종이에 적혀 있는 정보를 권한이 있는 사람만 볼 수 있도록 제한하고 싶다.
   ③ 종이에 서술된 내용에 특정 사람이 동의하고 있다는 것을 확인하고 싶다.
   ③ 종이에 적혀 있는 정보가 변조되지 않았다는 것을 확인하고 싶다.
   ⑤ 현재 대화하고 있는 상대방의 신원을 확인하고 싶다.
2. 동전 던지기 단계 1에서 A가 매우 큰 정수를 임의로 선택한다. 만약 A가 선택하는 정수의 범위가 제한적이면 어떤 문제가 발생하는지 설명하시오.
3. 동전 던지기에서 사용한 함수 f의 출력은 균일하게 분포되어야 한다. 즉, x가 주어졌을 때 $f(x)$가 특정 출력값을 가질 확률은 출력의 범위가 n일 때 $1/n$이어야 한다. 사용하는 함수 f가 이 조건을 만족한다고 하였을 때, $f(x)$ 출력의 범위가 작으면 특성 2를 제공할 수 없다. 그 이유를 설명하시오.

[1]계산적으로 불가능하다는 것은 얻는 방법이 전혀 없다는 것이 아니라 현재의 컴퓨팅 파워를 이용하여 지금까지 알려진 가장 최선의 방법을 사용하더라도 결과를 얻기 위한 너무 많은 비용(시간, 돈)이 소요되어 의미가 없다는 것을 의미함