정 보 보 호 학 회 지
제 32 권 제6호, 2022. 12

양자컴퓨팅 시대를 대비하기 위한 암호화 선제대응력(Crypto-Agility) 도입 방안

박 종 욱*, 백 선 엽*, 장 상 운*, 한 상 윤*

요 약

양자컴퓨팅 시대가 도래하면 현재까지 안전하다고 여겨지는 암호 알고리즘이 쉽게 해독될 수 있다. 이에 대비하기 위해 NIST에서는 PQC 알고리즘 개발 프로젝트를, 한국에서는 KpqC 프로젝트를 통해 양자컴퓨팅 대응 암호 알고리즘을 개발하고 있다. 양자컴퓨팅 시대에 안전한 새로운 암호 알고리즘 개발도 중요하지만, 암호취약점 발견이 일상이 될 경우 시스템 변경을 최소화하면서 기존 암호 알고리즘을 신규 암호 알고리즘으로 대체할 수 있는 암호화 선제대응력(Crypto Agility)에 대한 준비도 필요하다. 본 논문에서는 기존 시스템의 영향을 최소화하면서 암호 관련 요소들(암호 알고리즘, 암호 파라미터, 암호 프로토콜 등)을 대체하기 위해 필수적인 암호화 선제대응력 요구사항을 제안하고, 이를 실행하기 위해 정책기관에서 추진되어야 할 실행항목을 제시한다.

Ⅰ. 서 론

정보보안시스템은 응용 서비스와 운영 환경에 따라 암호 알고리즘과 프로토콜이 결정된다. 실시간으로 관리되는 서비스 운영에 비교하여 암호기능에 대한 우선순위는 낮아 현실에서는 대부분 한번 설정하고 잊어버리는(set and forget) 형태로 관리되고 있다. 게다가 사용자들은 응용 서비스나 시스템에 어떤 방식의 암호 알고리즘과 프로토콜이 적용되었는지 대부분 관심이 없다.

한편, 정보보안시스템은 암호 알고리즘과 프로토콜 뿐만 아니라 이를 구현하면서 발생할 수 있는 다양한 암호 취약점들로부터 위협을 받고 있다. SHA-1 알고리즘은 이미 2010년 초 취약하다고 밝혀졌고, 구글 연구원들은 2017년 최초의 충돌 쌍을 발견했다[1]. 무선랜 프로토콜인 WEP, WPA, WPA2에 대한 취약점과 블루투스 프로토콜에 대한 Blueborne 취약점 등도 발표되었다[2,3]. 대표적인 보안 라이브러리인 OpenSSL에서는 HeartBleed, POODLE Attack 등의 메이저 취약점이 매년 발견되고 있다[4,5]. 기존 사례에서 살펴볼 수 있듯이 정보보안시스템은 시간이 지나면 취약점이 발견될 수 있으며, 이러한 취약점들은 암호화되어 전송되는 정보의 안전성을 위협한다.

특히, 수학적 난제에 기반한 공개키 암호 알고리즘은 컴퓨터 연산 속도가 증가하면서 시간이 지날수록 취약해진다. 최근 급속히 발전하고 있는 양자컴퓨팅 기술은 중첩/얽힘과 같은 양자 현상을 사용하여 연산 속도를 획기적으로 증가시켰고, 기존 암호 알고리즘의 안전성을 더욱 위협하고 있다. Shor 알고리즘은 양자컴퓨터를 이용하여 RSA와 같은 인수 분해 문제의 복잡도에 의존하는 암호시스템을 해독할 수 있다고 알려졌다[6]. 또한, Shor 알고리즘을 수정하면 이산 로그 문제도 해결할 수 있어서 DH, ECDH 등의 키교환 프로토콜과 ElGamal, ECC 등의 비대칭 암호 알고리즘, DSA, ECDSA 등의 전자서명 알고리즘들에 대한 위협이 증가하고 있다. Grover 알고리즘은 양자컴퓨팅을 활용해 데이터베이스 내 특정 조건에 해당하는 항목을 빠르게 찾을 수 있어 AES 등의 대칭키 암호 알고리즘의 안전성을 1/2로 감소시킬 수 있다[7].

[표 1]은 암호 알고리즘 종류와 키길이 변화에 따라 일반컴퓨팅과 양자컴퓨팅에서의 안전성을 비교한 결과를 나타낸다.

양자컴퓨팅 업계에서는 2030년에 공개키 암호 해독이 가능한 양자컴퓨터가 상용화될 것으로 예상한다.

* 한국전자통신연구원 부설연구소 (책임연구원, khspjw@nsr.re.kr, 책임연구원, sybaek@nsr.re.kr, 책임연구원, jsw@nsr.re.kr, 실장, syhan@nsr.re.kr)

〔표 1〕 암호 알고리즘 안전성 비교

암호 알고리즘	키길이	안전성	
		일반컴퓨팅	양자컴퓨팅
RSA	1024	80	0
	2048	112	0
ECC	256	128	0
	384	256	0
AES	128	128	64
	256	256	128

암호 알고리즘과 프리미티브에 의존하고 있는 현대 암호시스템은 양자컴퓨팅의 등장으로 인하여 안전성에 상당한 위협을 받고 있다.

이를 해결하기 위해 기존 암호 알고리즘을 대체할 수 있도록 양자 내성 암호 알고리즘 개발이 추진되고 있다. 대표적으로 한국의 KpqC, 미국 NIST의 PQC(Post-Quantum Cryptography) 프로젝트가 현재 진행 중이다[8,9]. 이와 함께, 레거시 알고리즘 및 프로토콜, 인증서 등을 사용하던 시스템은 양자 내성 암호로의 전환을 준비해야 한다. 새로운 암호 알고리즘 개발도 중요하지만, 암호 취약점 발견이 일상화될 경우 시스템 변경을 최소화하면서 기존보다 안전한 새로운 암호 요소를 신속히 적용하기 위해 시스템 차원의 암호화 선제대응력(Crypto-Agility)에 대한 준비도 필요하다.

본 논문에서는 암호화 선제대응력의 정의와 속성에 대하여 설명하고, 현재까지 암호화 선제대응력과 관련된 연구 동향을 살펴본다. 또한, 암호화 선제대응력 도입을 위한 준비사항을 설명하고, 이를 바탕으로 도입 요구사항 및 제도화 방안 등을 제시한다.

Ⅱ. 암호화 선제대응력 정의 및 속성

2.1. 정의

암호화 선제대응력이란 시스템 내부 구조에 많은 변화를 가져오지 않고, 새로운 암호 알고리즘 및 프리미티브로 신속하게 대체할 수 있는 것을 의미한다. 정보보안시스템은 설계와 표준, 구현 기술 등에 암호화 선제대응력을 반영해야 한다[10]. 현재 많이 사용하는 TLS/SSL 암호 프로토콜은 안전성을 강화하기 위해 암호 알고리즘 또는 프리미티브를 협상하는 방식을 활용하는데, 이는 암호화 선제대응력의 일부 속성으로 간주할 수 있다. 2.2절에서는 현재 인프라를 연속적으로 유지하면서, 새로운 암호 방식으로 손쉽게 전환하도록 암호화 선제대응력의 기본 속성을 설명한다.

암호화 선제대응력이 반영되지 않은 시스템은 암호 관련 취약점이 발견되더라도 취약점 대응에 많은 시간이 소요될 뿐만 아니라 보호해야 할 정보가 외부 공격에 쉽게 노출될 수도 있다. 반면에 암호화 선제대응력이 반영된 시스템은 암호기능을 변경하여 공개된 암호 취약점에 대하여 즉각적으로 대응하고, 앞으로 발생할 것으로 예상되는 암호 알고리즘 취약점을 사전에 방지할 수 있다. 양자 내성 암호 알고리즘의 경우에도 새로운 취약점이 언제든 발견될 수 있으므로 양자 내성 암호 알고리즘을 탑재하는 정보보안시스템도 암호화 선제대응력을 필수적으로 적용해야 한다.

2.2. 속성

정보보안시스템에 새로운 암호기능을 추가하거나 기존 암호기능을 삭제하게 되면, 서비스 운용, 시스템 호환, 기술 구현 등의 다양한 문제가 발생할 수 있다. 따라서 암호기능 구현은 독립성을 유지하는 모듈 방식으로 이뤄져야 한다. 암호화 선제대응력을 지원하기 위한 암호기능 모듈의 기본 속성을 확장성, 상호운용성, 비가역성, 자발성으로 정의했다.

2.2.1. 확장성

확장성은 시스템의 암호화 선제대응력을 달성하기 위해 제일 중요한 속성이다. 최초 설계에서 선택한 암호 알고리즘 또는 프로토콜 등은 시간이 지남에 따라 취약해진다. 따라서 시스템은 새로운 암호 알고리즘과 프로토콜 추가가 가능해야 하고, 키길이 조절, 새로운 암호 프리미티브의 추가 또는 변경, 암호 구현을 위한 다양한 기능의 조합 등을 지원해야 한다.

암호화 선제대응력을 위한 암호기능 확장은 암호 알고리즘이 구현된 소프트웨어 또는 하드웨어의 업데이트를 통해 이뤄진다. 업데이트는 독립적인 모듈 형태로 진행되어 업데이트로 인하여 다른 암호기능 요소에 영향을 끼치지 않아야 한다.

암호기능 구현 방식에 따라 확장성을 위해 다음과 같은 사항이 고려한다. 새로운 암호 알고리즘을 탑재하거나, 암호키의 길이를 확장하기 위해서는 장치의

메모리 공간에 여유분이 필요하다. 이 경우, 취약성으로 인하여 쓸모가 없어진 기존 암호 알고리즘 또는 키, 인증서 등의 정보를 삭제하여 메모리 공간을 추가로 확보하여 활용할 수 있다. FPGA 기반의 하드웨어 가속기 기반으로 운용되는 시스템은 펌웨어를 업데이트하여 새로운 암호 알고리즘을 추가할 수 있어야 한다. ASIC 형태의 하드웨어 가속기는 암호 모듈 형태로 기존의 시스템에 쉽게 정합될 수 있도록 통신 인터페이스와 연동 소프트웨어 라이브러리 등의 표준화가 필요하다. 마지막으로 암호 통신 프로토콜은 새로운 암호 알고리즘 및 암호 프리미티브에 대한 협상이 가능해야 하고, 새로운 방식의 암호 통신 프로토콜로의 기능 업데이트도 지원해야 한다.

2.2.2. 상호운용성

시스템은 동일 시스템 또는 이기종 시스템과 암호기능을 호환하여 사용하는 상호운용성을 제공해야 한다. 암호기능은 특정 소프트웨어와 하드웨어의 종류 또는 버전에 종속되지 않아야 하고, 현재 시스템이 보유하고 있는 암호 알고리즘과 프리미티브를 조합하여 상대 시스템이 활용하는 암호 프로토콜과 연동될 수 있어야 한다.

암호화 선제대응력의 상호운용성을 달성하기 위해 첫 번째로 협상에 사용되는 데이터 포맷에 대한 표준이 필요하다. 일반적으로 데이터 교환에 많이 사용되는 JSON (JavaScript Object Notation) 또는 XML (eXtensible Markup Language) 등의 형식을 활용하여 시스템 간의 암호 관련 정보를 공유할 수 있다.

두 번째로 시스템 간 암호기능 정보를 공유하는 방식에 대한 표준화가 필요하다, 정보에 포함될 주요 내용으로 암호 프로토콜명과 버전 정보, 암호 알고리즘과 프리미티브 등을 포함한다. 공유한 정보를 통해 상대방의 암호 능력을 확인하고, 안전한 암호 기법을 선택할 수 있다.

세 번째로 현재는 정의되지 않았지만, 미래에 활용할 수 있는 암호기능들을 고려하여 추가로 확장하는 방법을 고려해야 한다. 이를 위해서는 암호 협상 과정에서 기존에 알려지지 않은 암호기능들을 지원하는 개념을 반영해야 한다. 전송되는 암호기능 정보량은 줄이고, 협상 과정을 간결화시켜 성능 지연을 최소화하는 방안도 고려해야 한다.

마지막으로 시스템 간의 암호 통신 세션 수립뿐만 아니라, 상대 시스템의 암호기능 취약점 정보에 대해 전달할 수 있어야 한다. 일종의 암호 취약점 경고 메시지를 전달하여 상대가 안전한 암호 알고리즘 또는 프리미티브로 업데이트할 수 있도록 해야 한다.

2.2.3. 비가역성

암호화 선제대응력을 위해 시스템은 비가역성의 속성을 갖춰야 한다. 암호화 선제대응력에 따라 새로운 암호 알고리즘 또는 파라미터를 업데이트하면, 시스템은 취약하다고 알려진 이전 암호 방식을 사용하면 안된다. TLS 프로토콜에서 BEAST, CRIME 공격들은 안전하지 않은 암호 알고리즘 협상을 통해 시스템을 장악할 수 있었고, POODLE 공격은 fallback attack으로 프로토콜 버전을 낮춘 뒤 해당 버전에 포함된 취약점을 활용해 공격을 수행했다. 따라서, 소프트웨어 또는 하드웨어 형태의 암호기능 모듈이 새롭게 변경된 시스템에서는 버전 정보 및 무결성 검증 등을 통해 이전 버전의 암호기능 모듈을 재사용할 수 없어야 한다. 소프트웨어 모듈은 관리자 수준에서 접근이 가능한 공간에 버전 정보를 저장하여, 사용자 수준에서 버전 정보 수정 자체가 불가능해야 한다. 비가역성을 제공하기 위해 쓰기만 가능하고 삭제 불가능한 메모리를 활용을 고려해야 한다. 또한, 최신 소프트웨어 버전 번호로 업데이트만 가능한 rollback prevention 기술 등을 활용해 소프트웨어 버전을 이전으로 되돌리는 것도 방지할 수 있다.

2.2.4. 자발성

일반적으로 시스템 업데이트는 사용자가 수동으로 수행하거나 업데이트 설정 정보를 이용하여 수행한다. 하지만, 암호화 선제대응력이 적용된 시스템은 취약한 상태에 노출되어 있는지를 판단하고, 이를 해결하는 방안을 찾아 대응하는 자발성을 확보해야 한다. 암호화 선제대응력이 적용된 시스템은 암호 취약점에 대한 정보를 관리 서버와 연결되어 취득하거나 암호 통신 세션을 수립하는 다른 시스템 또는 장비로부터 획득할 수 있어야 한다.

관리 서버는 실시간으로 암호 취약성에 대한 정보를 업데이트한다. 다양한 종류의 장비들은 서버에 주기적으로 접속하거나 푸시 알람 등을 이용하여 관리

서버부터 안전한 암호 알고리즘과 비밀키 길이 등의 암호 정보를 확인하고, 최신 정보로 업데이트해야 한다. 획득된 정보를 바탕으로 암호 취약성 진단을 수행하고, 시스템에서 취약한 요소가 발견되면, 새로운 암호 체계를 활용하거나 업데이트 서버로부터 검증된 암호 모듈 라이브러리를 수신해 변경한다.

암호 통신 세션 수립 시, 상대방으로부터 암호 취약성 정보를 획득하여 자신의 취약성 여부를 확인한 뒤, 취약하다고 판단되면 업데이트 서버로부터 시스템 업데이트를 진행한 후에 암호 통신 세션을 다시 수립할 수 있다. 이 경우, 통신 세션을 수립하는 시스템 또는 장비로부터 인증된 암호기능 라이브러리를 획득도 가능하다. 예를 들어, A 단말이 AES 알고리즘만 가지고, B 단말이 인증된 ARIA 알고리즘 기능을 포함하고 있으면, A 단말은 B 단말이 ARIA 알고리즘을 요청할 수 있다. 두 단말이 상호 인증이 수행되었다면, B 단말이 A 단말로 ARIA 알고리즘을 전달하고, ARIA 알고리즘으로 암호 통신 세션을 수립할 수 있다.

Ⅲ. 암호화 선제대응력 사례 및 연구 동향

3.1. 기존 사례

암호화 선제대응력은 오래전부터 암호 커뮤니티 내에서 거론된 개념이었지만, 앞에서 언급된 모든 속성을 지원하지 않았다. TLS/SSL 표준과 X.509 디지털 인증서 표준이 대표적인 사례다.

TLS 프로토콜이 암호 전송을 위한 통신 세션을 수립하는 과정은 다음과 같다. 첫째, CipherSuite 공유를 통해 장비에서 지원하는 암호 후보군(키공유/기밀성/무결성 암호 알고리즘 종류, 운용모드, 키길이 등)을 상호 확인한다. 둘째, 암호 후보군에서 실제 암호 세션에서 운용하는 키공유/기밀성/무결성 알고리즘 등을 선택하고 두 장비가 이에 대한 협의를 마친다. 이후, 선택된 알고리즘을 활용하여 전송 데이터 암호기능을 수행하는 상호운용성을 포함한다. TLS 절차는 데이터 전송을 위한 암호 세션 수립 시, 취약하다고 알려진 암호 알고리즘은 후보에서 배제하고 안전한 암호 알고리즘을 적용하기 쉽다. 하지만, 암호기능 설정에 응용 서비스가 직접 알고리즘 및 파라미터를 결정해야 한다. 따라서 서비스 개발자가 현재 사용 중인 암호 안전성을 전문가 수준으로 이해하고, 시스템 운영자는 취약해진 알고리즘 및 프로토콜에 대한 정보를 실시간으로 확인해 시스템 설정에 반영해야 한다. 또한, 하위 호환성 유지로 인하여 취약하다고 알려진 알고리즘 또는 프로토콜을 즉시 삭제하는 것도 현실적으로 쉽지 않다.

X.509 디지털 인증서는 버전 정보, 인증서 고유 일련번호, 인증서 서명 알고리즘, 서명값, 인증서 해시값, 발행기관, 유효기간(시작 및 종료), 주체의 정보, 주체의 공개키 알고리즘 및 공개키 정보를 포함한다. ASN.1 표기 형식을 활용하며 확장 필드를 통해 추가적인 정보를 포함하는 점에서 상호운용성을 포함하고 있다. 인증서의 경우, 유효기간이 존재하며, PKI 구조로 인하여 rootCA 인증서가 갱신되면 이로부터 서명되어있는 하위 단계의 인증서들은 새롭게 인증서를 받아야 한다. 그렇지 않으면 모든 시스템은 멈춰야 한다. 기존 시스템에서는 새로운 알고리즘을 지원하지 않기 때문이며 시스템 마이그레이션도 동일한 이유로 쉽지 않다. 이를 해결하기 위해 ISARA, Cisco, CableLabs, DigiCert 등은 레거시 알고리즘과 퀀텀 세이프 암호 알고리즘을 모두 지원하는 하이브리드 디지털 인증서를 개발하고 있다[11]. 사용자는 하이브리드 root 인증서를 받고, 하이브리드 엔드 엔티티 인증서를 요구하여 서버에 접속하는 방식을 사용한다. 이처럼 암호화 선제대응력을 도입하기 위해서는 새로운 인증서 발급 등의 관리 기법이 필요하다.

3.2. 관련 연구 동향

3.2.1. 해외 공공기관

양자컴퓨팅 시대에 대비하여 취약한 공개키 암호 알고리즘 등을 단시간에 교체하는 것은 많은 문제를 발생시킬 수 있다. 이를 해결하기 위한 암호화 선제대응력 관련 프로젝트가 NIST 산하 NCCOE에서 2022년부터 추진되고 있다[12]. “Migration to Post-Quantum Cryptography 프로젝트는 다양한 유형의 조직, 자산 및 지원 기술에 걸쳐 취약한 알고리즘에서 PQC 알고리즘으로 마이그레이션하기 위한 연구 항목을 다음과 같이 제시한다.

- 공개키 알고리즘의 활용 식별
- 레거시 알고리즘의 존재 확인
- 암호 프로토콜 종속성 식별
- 소프트웨어를 통한 업데이트 가능 여부 판단

- 보호되고 있는 정보의 민감성 식별
- 마이그레이션 중에 상호운용성을 유지 필요성 식별
- 개발자와 사용자의 프로세스 및 절차 업데이트
- 새로운 프로세스 및 절차 테스트 및 검증

영국의 사이버안전센터 NCSC에서는 프로토콜 설계 원칙에서 프로토콜 관련 프로젝트를 추진할 때 업데이트를 쉽게 하고, 운영 중지를 방지하며, 취약점 대응을 빠르게 할 수 있도록 암호화 선제대응력을 강조하고 있다[13]. 프랑스의 ANSSI에서는 양자 내성 암호 천이에 관한 견해에서 암호화 선제대응력의 구현이 역호환성 등의 이유로 쉽지 않지만, 양자컴퓨팅 위협에 대응하는 데 필요하며, 향후 제품의 위험편익분석에 중요한 요소로 고려해야 한다고 밝히고 있다[14].

3.2.2. 연구 및 산업계

암호화 선제대응력과 관련된 연구 동향을 살펴보면 2018년 Hannse Mehrez 등이 암호화 선제대응력을 보유한 시스템이 보유해야 할 특성으로 확장성, 상호호환성, 유연성, 가역성 등 10개 항목을 제시하였다[15]. 2019년 Olaf Grote 등은 양자컴퓨팅 공격에 대응하기 위해 양자 내성 암호 알고리즘뿐만 아니라 모든 보안 프로토콜도 암호화 선제대응력을 보유해야 한다고 강조했다[16]. 2021년 Chujiao Ma 등은 암호화 선제대응력 측면에서 위협 평가 모델(Crypto Agility Risk Assessment Framework)을 제안하고, 양자컴퓨팅 위협 대응에 암호화 선제대응력이 결여될 때 발생할 수 있는 위협을 분석하고 평가하는 방법을 설명했다[17].

산업계에서는 암호화 선제대응력을 도입하기 위한 도구를 다음과 같이 개발하고 있다. 기관에서 운영하는 암호자산을 관리해주는 암호자산 목록관리(Crypto Inventory) 도구를 여러 업체에서 개발하고 있다. 또한 Cryptosense社는 암호자산을 제어하고 관리할 수 있는 Cryptosense Analyzer Platform 개발을 [18]. Infosec社에서는 암호자산, 인증서, 키 등을 관리할 수 있는 Cryptographic Agility Management Platform과 암호자산을 찾고 위협단계를 분석하여 실행 우선순위를 찾아주는 AgileSec Analytics를 개발하였다. 또한, 최신 표준알고리즘을 응용프로그램에 쉽게 적용할 수 있는 AgileSec SDK 등의 암호화 선제대응력 관련 제품을 선보였다[19]. SENETAS社에서는 암호화 선제대응력이 탑재된 하드웨어 암호장비를 개발하였고[20], Cryptomathic社에서는 키관리시스템에 암호화 선제대응력 기능을 탑재한 Crypto Service Gateway를 개발하고 있다[21]. 미국을 중심으로 암호화 선제대응력 관련 프로젝트 및 연구, 기술 개발 등이 다양하게 추진되고 있지만, 국내에서는 암호화 선제대응력 관련 연구 및 관련 기술 개발은 미진하다.

Ⅳ. 암호화 선제대응력 적용 대상 및 도입 시나리오

4.1. 적용 대상 식별

정보보안시스템에서는 암호 알고리즘, 암호 프로토콜, 암호 파라미터, 암호 모듈, 인증서 등에 암호화 선제대응력 적용이 필요하며, 시스템에 따라 적용 대상이 축소되거나 확장될 수 있다. 암호화 선제대응력 적용 대상들은 앞에서 언급한 확장성, 상호운용성, 비가역성, 자발성의 속성을 포함하도록 설계해야 한다.

4.1.1. 암호 알고리즘

암호 알고리즘은 암호기능 구현에 필수다. 자료의 기밀성 또는 무결성을 지원하기 위해 활용되는 암호 알고리즘은 일반적으로 소프트웨어나 하드웨어 모듈 형태로 구현되어 동작한다. 레거시 암호 알고리즘이 취약하다고 여겨지면, 안전하다고 보장된 새로운 알고리즘으로 즉각적인 변경이 가능해야 하고, 기존 암호 알고리즘의 사용은 중단해야 한다. 따라서, 모든 시스템은 자발적으로 암호 알고리즘을 안전한 알고리즘과 취약한 알고리즘으로 분류할 수 있어야 하고, 취약한 알고리즘 사용은 금지한다. 미래에 사용할 수 있는 예비 암호 알고리즘에 대한 개념도 고려할 수 있다. 상호운용성을 제공하도록 암호 알고리즘을 새롭게 추가하는 방식과 알고리즘 취약성 검증 기법 등에 대한 논의가 앞으로 필요하다.

4.1.2. 암호 프로토콜

암호 프로토콜은 데이터 저장, 데이터 통신, 서명, 인증 등에 활용된다. 상호운용성을 위해 암호 프로토콜 표준화가 필요하고 시스템들은 자신뿐만 아니라 상대 시스템의 프로토콜명과 프로토콜 버전 정보를 확인할 수 있어야 한다. 데이터 저장 프로토콜은 기존 암호 알고리즘에서 새로운 암호 알고리즘의 변환을 지원해

야 한다. 데이터 통신 프로토콜은 통신하는 시스템의 암호 관련 정보(Cryptographic Capability)를 교환하고, 암호 통신 세션을 안전하게 수립하는 방식을 지원해야 한다. 서명 및 인증 프로토콜은 새로운 암호 알고리즘의 변환에 따라 재서명 방식과 신규 인증 메커니즘을 지원하는 방안을 고려해야 한다. 현재 사용하는 암호 프로토콜이 취약하다고 여겨지면, 보유하고 있고 취약하지 않은 암호 프로토콜로 변경하거나 업데이트 서버로부터 받은 새로운 프로토콜을 적용한다. 모든 시스템은 자발적으로 암호 프로토콜을 검증하고, 취약하다고 판단된 프로토콜은 사용을 금지해야 한다. 암호 프로토콜에 대해 취약성을 평가하고 결과를 공유하는 방안과 프로토콜 업데이트 메커니즘 등에 대해 추가적인 논의가 필요하다.

4.1.3. 암호 파라미터

암호 파라미터는 암호 알고리즘이 정해진 이후에 설정되는 키길이, 오프셋, 운용 방식 등에 대한 정보를 의미한다. 양자컴퓨팅으로 인하여 암호 안전성이 낮아짐에 따라 유사한 안전성을 유지하기 위해서 대칭키 알고리즘은 기존 키길이의 2배 이상을 증가시켜야 한다고 알려져 있다. 암호화 선제대응력을 도입하기 위해서는 암호기능과 관련된 암호 파라미터를 정의하고, 상호운용성을 고려하여 파라미터(키길이 등)을 증가시킬 수 있는 방식을 고려해야 한다. 자발적인 암호 취약성 진단에 따라 안전성을 위해 증가된 키길이는 정해진 이후로 축소되지 않도록 관리해야 한다.

암호 알고리즘, 암호 프로토콜, 암호 파라미터를 합쳐 본 논문에서는 암호자산으로 표기한다.

4.1.4. 암호 모듈

암호 모듈은 암호기능을 수행하는 중요 요소이다. 주로 소프트웨어 라이브러리 형태, 펌웨어 또는 하드웨어 방식으로 개발되어 정보보안시스템에 적용된다. 암호화 선제대응력을 도입하기 위해서는 각 모듈 형태로 최대한 업그레이드가 손쉬운 방식을 고려해야 한다. 특히 펌웨어 또는 하드웨어 방식의 암호모듈의 경우 업그레이드가 쉽지 않고 오래동안 사용할 수 있기 때문에 양자 컴퓨팅 위협을 고려하여 개발되어야 한다. 암호화 선제대응력을 포함하는 암호 모듈에 대한 자가 검증, 상호운용성, 확장성, 비가역성 등이 정의되어야 하며, 이에 대한 구현 및 평가 방식에 대해 논의가 필요하다.

4.1.5. 정보 자산

암호 알고리즘의 대상이 되는 정보 자산에 대해 다음과 같은 속성을 파악해야 한다. 양자 컴퓨팅 공격 시점이후 까지 보호되어야할 자산인지 판단하기 위해 자산의 수명주기를 결정해야 하며, 새로운 암호 알고리즘으로 교체시 폐기 또는 재암호화가 필요한지 판단하기 위해 자산의 중요도를 분류해야 한다.

4.1.6. 정보보안시스템

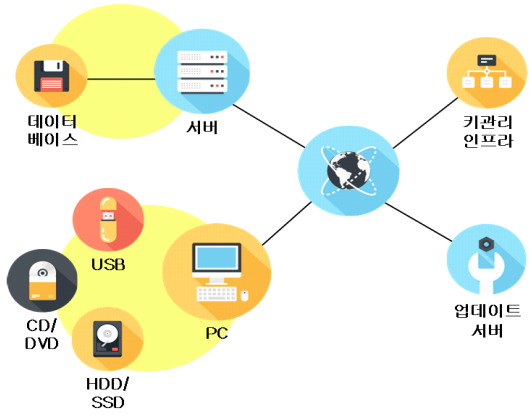
정보자산에 대한 보호대책을 제공하는 정보보안시스템은 암호자산이 변경될 경우 영향을 받을 수 밖에 없다. 따라서 정보보안시스템과 암호자산에 대한 정보를 유지해야 하며, 정보자산 변경에 따라 정보보안시스템의 업데이트가 용이할 수 있도록 검토가 필요하다.

4.1.7. 공개키 관리 시스템

공개키 관리 시스템에서 중요한 부분은 공개키 알고리즘과 인증서이다. 현재 운용하고 있는 공개키 알고리즘을 새로운 알고리즘을 대체할 수 있도록 새로운 인증 메커니즘, 체계 구성에 대한 논의가 필요하다. 또한 기존 PKI 구조에서 발행된 인증서는 새로운 PQC 환경에서 호환이 되지 않을 수 있다. 이를 해결하기 위해 앞에서 언급한 바와 같이, 하이브리드 디지털 인증서가 제안되었다. 암호화 선제대응력을 도입하기 위해서는 기존 인증서와 새롭게 정의될 인증서를 구분하고, 인증서 정보에 따라 새로운 알고리즘을 적용할 수 있는 방식을 고려해야 한다.

4.2. 암호화 선제대응력 도입 시나리오

암호자산(암호 알고리즘 또는 프로토콜 등)이 양자컴퓨팅 등의 위협에 취약해졌다고 가정하고, [그림 1]과 같이 중요 데이터를 저장하는 정보보안시스템에서의 암호화 선제대응력 속성 도입 시나리오를 다음과 같이 제안한다.



〔그림 1〕 데이터 저장 시스템 구성도

- **1단계** : 현재 저장장치(데이터베이스, USB, HDD/SSD, CD/DVD)에 보호 대상으로 관리되는 정보자산을 계속해서 보호해야 할 필요가 있는지, 폐기해도 되는지를 검토한다. 또한 보호하는 정보자산의 재암호화가 필요한지를 검토한다.
- **2단계** : 시스템(서버, PC)에서 취약한 암호자산을 식별하여 취약점 보완 방식을 결정하고, 업데이트를 수행한다. 새로운 암호자산을 개발하는 경우는 암호화 선제대응력을 온전히 반영해 설계해야 하며, 취약한 하위 버전 암호자산 사용을 금지한다. 정보자산의 재암호화를 수행하는 경우. 복호화된 평문이 외부에 노출되지 않아야 한다. 포렌식 등의 외부 공격에 대응하기 위해 복호화된 평문은 램디스크 또는 안전한 하드웨어 보안 모듈 등에 임시로 저장하는 방안의 적용을 검토한다. 인증, 서명 등을 위해 공개키 알고리즘을 사용한다면, 키관리 인프라의 업데이트를 별도로 검토한다.
- **3단계** : 데이터 저장을 위해 시스템의 암호자산이 업데이트될 경우, 암호자산뿐만 아니라 시스템의 업데이트도 추가로 필요한지 검토한다. 필요하다면 최소한의 노력과 비용을 들여 업데이트할 수 있도록 필요한 조치를 수행한다.

위의 내용을 정리하면 [표 2]와 같다.

〔표 2〕 데이터 저장 시스템의 암호화 선제대응력 도입

단계	확인사항
1	- 정보자산 식별 - 재암호화 필요성 식별
2	- 암호자산 식별 - 취약한 암호자산 대책 수립 - 취약한 암호자산 업데이트 - 취약한 공개키 인프라 대책 수립
3	- 시스템 업데이트 대책 수립 - 시스템 업데이트

Ⅴ. 암호화 선제대응력 요구사항 및 제도화 제안

암호화 선제대응력 도입을 실행하기 위해 정보보안 시스템을 운용하는 실행기관과 제도적, 정책적으로 지원하는 정책기관에 따라 요구사항을 구분할 수 있다. 실행기관은 암호자산, 정보자산의 목록을 관리하고, 암호자산을 포함하고 있는 정보보안시스템을 관리해야 한다. 정책기관은 장기간 사용하는 장치의 선제 대응, 새로운 블록/해시 알고리즘 대응, 공개키시스템 대응 등을 반영하여 암호화 선제대응력 도입 정책을 수립해야 한다.

5.1. 실행기관의 암호화 선제대응력 요구사항

5.1.1. 암호자산 목록관리

기관에서 운영하는 암호자산의 문제점을 식별하고 필요한 대책을 세우기 위해 가장 기본이 되는 요소는 암호자산에 대한 목록화이다. 기관에서 운영하는 암호 알고리즘과 이를 활용하고 있는 프로토콜, 응용프로그램뿐만 아니라 암호 목적, 운용모드, 키 종류 및 용도 등을 포함하는 암호자산을 목록화하여 관리해야 한다. 기관에서 운영하는 암호자산에 대한 목록화를 수동으로 하지 않고 도구를 이용하여 관리할 수 있도록 산업계의 도구 개발 추진 동력을 제공할 수 있도록 관계기관의 제도적 지원이 필요하다.

5.1.2. 정보자산 목록관리

양자컴퓨팅 위협에 기관에서 보유하고 있는 정보자산을 식별해야 한다. 암호 정보를 저장하고 해독이 가능한 시점에 복호화하는 “steal now, decrypt later” 공

격에 노출될 수 있는 정보자산을 목록화해야 한다. 암호된 정보자산에 접근이 쉽고, 일정 시간이 지나서 해독되어도 문제 소지가 있는 정보자산을 목록화해야 한다. 이런 정보자산은 양자 위협에 대응할 수 있는 암호 알고리즘으로 즉시 대체가 필요하다.

다음으로 정보자산에 대한 접근이 쉽지 않은 자산에 대해 사이버 위협에 대한 Michele Mosca 이론에 해당하는 취약한 자산을 목록화해야 한다. 즉 X는 정보자산을 안전하게 보관해야 하는 기간으로, Y는 양자컴퓨팅 대응 암호 알고리즘으로 대체하기 위해 소요되는 시간으로, Z를 양자컴퓨팅 공격 시점으로 가정할 때 X + Y > Z가 되는 정보자산을 목록화해야 한다.

5.1.3. 암호화 선제대응력 관리시스템 구축

암호화 선제대응력 관련 정보를 업데이트하고, 암호화 선제대응력을 적용하는 장치가 활용할 수 있도록 암호화 선제대응력 관리시스템을 구축해야 한다. 네트워크에 연결된 장치가 암호화 선제대응력 관리 서버에 접속하여 암호기능에 사용할 수 있거나 불가능한 암호 알고리즘 및 파라미터 정보를 획득할 수 있도록 지원한다. 실행기관의 관리시스템 운영 기준을 제시하며 제도적으로 지원할 수 있는 정책개발도 필요하다.

5.1.4. 정보보안시스템 업그레이드 대비

현재 대부분의 정보보안시스템은 암호 알고리즘을 하드코딩된 형태로 구현하고 있다. 따라서 새로운 암호 알고리즘으로 변경할 경우, 정보보안시스템의 변경이 필요하며, 시스템의 업그레이드에 문제가 없도록 선제 조치가 필요하다.

5.1.5. 데이터 재암호 대비

정보자산을 새로운 알고리즘으로 재암호를 하기 위해서는 기존 알고리즘으로 평문화한 후 새로운 알고리즘으로 재암호해야 한다. 서비스에 지장을 최소화하면서 재암호할 수 있는 대책을 수립해야 한다. 특히 해시된 데이터베이스에 대해서는 추가적인 검토가 필요하다.

5.2. 정책기관의 암호화 선제대응력 요구사항

5.2.1. IoT 및 RoT 장치 선제 대응

펌웨어 또는 하드웨어 암호모듈 형태로 운영되는 IoT 장치 또는 RoT(Root of Trust) 장치는 설치된 후 5년 이상의 기간에 사용되며 set and forget 형태로 운영되는 경우가 많다. 또한 취약점이 발견되어도 패치 등의 대책을 조치하기가 쉽지 않은 환경에서 대부분 운영된다. 따라서 새로운 양자컴퓨팅 위협에 대응하기 위해 기관에서 운영하는 IoT 및 RoT 장치에 대한 목록을 관리해야 하며, 위협에 대응하는 대책을 수립해야 한다. 향후 보급이 예정된 장치의 경우에는 새로운 양자 내성 암호 알고리즘으로 천이가 쉽도록 암호화 선제대응력 기능을 보유하도록 관련 정책을 수립해야 한다.

5.2.2. 블록암호 알고리즘 키길이 및 해시 알고리즘 출력 길이 상향

기존 블록 암호 알고리즘의 경우 양자컴퓨팅 공격에 키 길이의 안전성이 1/2로 감소하며, 해시 알고리즘도 안전성이 1/2로 감소한다. 따라서 정보자산의 유효기간을 고려하여 블록 암호 알고리즘의 키 길이를 256비트 이상으로 변경해야 하며, 해시 알고리즘도 SHA의 경우 512 비트로 출력 길이를 상향해야 한다.

5.2.3. 정보보안시스템의 암호화 선제대응력 도입

현재 대부분의 정보보안시스템은 암호 알고리즘을 하드코딩된 형태로 구현하고 있어 새로운 암호 알고리즘으로 변경할 경우, 응용프로그램 변경도 필요하며, 많은 시간과 예산이 요구된다. 양자컴퓨팅 시대에는 지금보다 많은 암호 알고리즘 취약점이 도출되고, 빈번하게 암호 알고리즘 변경이 발생할 수 있다. 따라서 암호 알고리즘이 변경되더라도 정보보안시스템의 수정이 필요 없는 암호 알고리즘 연동 추상화 기법[22] 등을 도입하여 정보보안시스템이 암호화 선제대응력 기능을 보유할 수 있도록 CC 평가제도 등의 보완이 필요하다.

5.2.4. 공개키 관리시스템 대책 수립

공개키 암호 알고리즘을 주로 이용하는 PKI(공개키 관리시스템)가 양자컴퓨팅 공격에 가장 취약하며, 암호화 선제대응력을 도입하기 위해서 먼저 공개키 인프라에 사용되는 인증서, 키, 알고리즘 등에 대한 목록을 관리해야 한다. 둘째, 양자컴퓨팅 위협에 대응할 수 있도록 양자 내성 인증서를 현재 시스템과 호환성을 고려하여 운영할 수 있도록 대책을 수립하여야 한다. 셋째, 양자 내성 시스템으로 교체하기 위해 서비스 연속성을 보장하기 위한 대책을 수립해야 한다.

5.3. 암호화 선제대응력 관련 제도화

기관에서 효율적으로 양자컴퓨팅 위협에 대응하는 암호화 선제대응력을 도입하기 위해 가장 중요한 부분은 관련 기술 개발, 도입 및 운영을 제도적으로 뒷받침하여야 한다. 암호화 선제대응력 도입을 위해 정책기관에서 우선하여 추진되어야 할 암호화 선제대응력 관련 실행 항목을 다음과 같이 제안한다.

첫째, 암호화 선제대응력 기술에 대한 표준화 및 기술 개발을 지원할 수 있도록 기술 개발 및 표준화 관련 예산 반영을 추진한다. 둘째, 암호자산 및 정보자산에 대한 목록화를 의무화하도록 정보보안관리에 관련 내용 제도화를 추진한다. 셋째, 암호 기능이 탑재된 정보보안시스템에 암호화 선제대응력 관련 기능을 탑재하도록 CC 평가제도 등의 보완을 추진한다. 넷째, 공개키 관리시스템의 인증서, 암호 알고리즘, 키 등에 대한 목록화와 시스템에 암호화 선제대응력이 도입되도록 제도화한다. 다섯째, 취약점에 대한 패치가 어려운 펌웨어/하드웨어 형태의 정보보안시스템은 사용기간을 고려하여 암호화 선제대응력을 필수적으로 탑재하도록 관련 제도의 보완을 추진한다.

Ⅵ. 결 론

양자컴퓨팅 시대에는 현재 사용하는 암호 알고리즘의 안전성을 보장할 수 없다. 이런 상황이 도래하면, 많은 정보가 취약해지고, 서비스 중단이 발생할 수 있으며, 암호 알고리즘, 응용프로그램, 프로토콜 등을 대체하기 위해서도 많은 예산과 시간, 노력이 필요하다. 이를 해결하기 위해 암호화 선제대응력에 대하여 정의하였다. 또한, 기관이 적용 대상을 분석하여 취약한 부분을 사전에 대책을 수립할 수 있도록 암호화 선제대응력 도입 준비사항을 제안하였다. 마지막으로 실행기관 및 정책기관에서 필요한 요구사항을 분류하였고, 제도화가 필요한 항목을 제시하였다. 이를 기반으로 암호화 선제대응력이 많은 시스템에 반영될 수 있도록 관련 기술 연구 및 개발이 활발하게 추진되기를 기대한다.

참 고 문 헌

[1] Google Blog, “Announcing the first SHA1 collision,” https://security.googleblog.com/*2017/02/announcing-first-sha1-collision.html*, February 2017.

[2] Mathy Vanhoef and Frank Piessens, Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2,” *In Proceedings of the 2017 ACM Computer and Communication Security(CCS),* pp1313-1328, Dallas, Tx, USA, November 2017

[3] Ben Seri and Gregory Vishnepolsky “Blueborne - A New Class of Airborne Attacks That Can Remotely Compromise Any Linux/IoT Device,” *Black Hat Europe 2017,* London,UK, December 2017

[4] Neel Mehta, “The Heartbleed Bug,” *CVE-2014-0160*, April 2014

[5] Bodo Möller, Thai Duong and Krzysztof Kotowicz, “This POODLE Bites: Exploiting The SSL 3.0 Fallback,” *CVE-2014-3566*, September 2014

[6] Peter W Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” *SIAM Journal on Computing 26.5*, pp.1484-1509, 1997

[7] Lov K. Grover, “A fast quantum mechanical algorithm for database search,” In *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing(STC)*, pp.212-219, New York, NY, USA, July 1996

[8] 양자내성암호연구단, *https://kpqc.or.kr*

[9] NIST Post-Quantum Cryptography Project, *https://csrc.nist.gov/projects/ post-quantum-cryptograp*

hy

[10] Willian Barker, William Polk and Murugiah Souppaya, “Getting Ready for Post-quantum Cryptography: Exploring Challenges Associated with Adoption and Using Post-Quantum Cryptographic Algorithms“, *NIST CSWP 15,* April 2021

[11] Panos Kampanakis, Peter Panburana, Ellie Daw and Daniel Van Geest, “The Viability of Post-Quantum X.509 Certificates,” *IACR Cryptology ePrint*, January 2018

[12] NIST NCCOE, “Migration to Post-quantum Cryptography”, https://www.nccoe.nist.gov/*sites/default/files/2022-07/pqc-migration-project-description-final.pdf*

[13] NCSC UK, “Protocol Design Principles”, *https://ncsc.gov.uk/whitepaper/protocol-design-principles, NCSC UK Whitepaper*, December 2020

[14] ANSSI, “ANSSI views on the Post-Quantum Cryptography transition”, *https://ssi.gouv.fr/en/publications/anssi-technical_position_paper-post_quantum_cryptography_transition, ANSSI Technical Position Papers*, January 2001

[15] Hassane Aissaoui Mehrez and Othmane El Omri, “The Crypto Agility Properties”, *In Proceedings of The 12th International Multi-Conference on Society, Cybernetics and Informatics (IMSCI)*, pp.99-103, Orlando, FL, USA, July 2018

[16] Olaf Grote, Andreas Ahrens and César Benavente-Peces, “A Review of Post- Quantum Cryptography and Crypto-agility Strategies”, I*n Proceedings of 2019 International Interdisciplinary PhD Workshop (IIPhDW)*, pp115-120, Wismar, Germany, May 2019

[17] Chujiao Ma, Luis Colon, Joe Dera, Bahman Rashidi, and Vaibhav Garg “CARAF: Crypto Agility Risk Assessment Framework”, *Journal of Cybersecurity,* vol. 7, no 1. pp. 1-11, May 2021

[18] Cryptosense, “Cryptosense Analyzer Platform”. *https://cryptosense.com/analyzer*

[19] Infosec Global, “Control Your Cryptography With Crypto Agility Management”, *https://infosecglobal.com*

[20] Senetas, “Bringing Agility to Cryptography“, *https://www.senetas.com/cybersecurity-challenges/why-encrypt/crypto-agility*

[21] Cryptomathic, “CSG Overview”, *https://www.cryptomatic.com/products/key-management/crypto-service-gateway*

[22] Tyson Macaulay and Richard Henderson, “C*r*yptographic Agility in Practice-emerging use-case,” *https://assets.website-files.com/612fec6a451c71c9308f4b69/614b712e53ce8f7fad0c3c4a_ISG_AgilityUseCases_Whitepaper-FINAL.pdf*, Infosec Global Whitepaper, 2019

〈저자소개〉

박 종 욱 (Jong Wook Park)

정회원

1986년 2월 : 경북대학교 전자공학과 졸업

1988년 2월 : 경북대학교 전자공학과 석사

2001년 8월 : 경북대학교 전자공학과 박사

1988년 2월~2000년 1월 : 국방과학연구소 연구원

2000년 2월~현재 : ETRI부설연구소 책임연구원

<관심분야> 블록체인, AI 보안, 암호검증

백 선 엽 (Seon Yeob Baek)

종신회원

2003년 2월 : KAIST 전기 및 전자공학과 졸업

2010년 1월 : KAIST 전기 및 전자공학과 박사(석박통합)

2010년 2월~11월 : KAIST 전기 및 전자공학과 포닥

2010년 12월~현재 : ETRI부설연구소 책임연구원

<관심분야> AI 보안, 인증, 네트워크 보안, 무선통신

장 상 운 (Jang Sang-Woon)

정회원

2002년 2월 : 고려대학교 수학과 졸업

2004년 2월 : 고려대학교 정보보호대학원 석사

2004년 2월~현재 : ETRI부설연구소 책임연구원

<관심분야> 암호구현 및 분석, 암호모듈 검증

한 상 윤 (Sang Yun Han)

정회원

2002년 2월 : 홍익대학교 전자전기공학 학사

2004년 2월 : 포항공과대학교 정보보안 석사

2004년 2월~현재 : ETRI부설연구소 실장

<관심분야> 암호검증, 정보보호, 암호