물리적 복제방지 기능(PUF) 보안 요구사항 국제 표준화 현황

강유성 (ETRI 책임연구원, youskang@etri.re.kr)

1. 머리말

IT 보안기술에 대한 보안성 평가기준 및 시험방법에 관한 국제표준화를 담당하고 있는 표준그룹은 ISO/IEC JTC 1/SC 27/WG 3(이하 SC27/WG3)이다. 제56차 SC 27/WG 3회의는 2018년 4월 중국 우한에서 개최되었으며, 연 2회(4월, 10월) 대면회의를 개최하고 있다. 이 표준그룹은 CC(Common Criteria)와 CMVP(Cryptographic Module Validation Program)에서 참고할 보안성 평가기준을 논의하고 있으며 시장에서의 파급력이 큰 표준문서를 만들고 있다.

2. 회의 주요 결과

암호키를 사용하는 디지털 디바이스가 암호키를 안전하게 생성하고 사용하고자 할 때, 기술적인 해결책이 될수 있는 주요 기술 중 하나가 물리적 복제방지 기능(PUF, Physically Unclonable Function)을 이용하는 것이다. 이는 하드웨어 기반의 해결책으로 기술적 완성도가 높을 경우 그 활용도가 매우 큰 기술이다.

SC27/WG3에서는 하드웨어 기반의 키은닉 핵심기술이라 할 수 있는 PUF 기술과 WBC 기술에 대한 보안 요구사항 및 평가/시험 방법에 대한 표준화가 활발하게 진행되고 있다. 이번 회의에서는 PUF 보안 요구사항 표준인 ISO/IEC 20897-1 CD 투표 결과와 PUF 보안성 시험/평가 방법 표준인 ISO/IEC 20897-2 WD 코멘트 내용을 중심으로 표준화 논의가 진행되었다. <표 1>은 해당 기술에 대한 표준화 현황을 요약한 것이다.

<표 1> SC27/WG3 키은닉 핵심기술 표준화 현황

[2018년 4월]

문서	제목	현 단계	에디터
ISO/IEC 20897-1	Security requirements, test and evaluation methods for physically unclonable functions for generating non-stored security parameters – Part 1: Security requirements	2nd CD	· Sylvain Guilley(프랑스 Secure-IC) · Soshi Hamaguchi(일본 Cosmos) · 강유성(한국 ETRI)
ISO/IEC 20897-2	Security requirements, test and evaluation methods for physically unclonable functions for generating non-stored security parameters – Part 2: Test and evaluation methods	2nd WD	· Soshi Hamaguchi(일본 Cosmos) · 강유성(한국 ETRI) · Sylvain Guilley(프랑스 Secure-IC)

※ WD(Working Draft): 작업 초안(위원회 승인 받기 전, 작업반이 작성중인 문서)

※ CD(Committee Draft): 위원회 초안(위원회 승인은 받았으며, 국가 투표를 진행하는 문서)

ISO/IEC 20897-1 표준은 PUF 출력이 가져야 할 주요 보안 요구사항에 대해 PUF 출력의 Reliability와 Entropy 중심으로 보안 요구사항을 정의하여 2018년 6월 22일까지 두 번째 CD 문서를 만들어서 제출한 후 CD 투표를 진행하기로 결정되었다. PUF 보안성에 대한 시험/평가 방법을 정의할 ISO/IEC 20897-2는 두 번째 WD를 2018년 6월 22일까지 작성하여 전문가 의견 수렴을 위해 SC27/WG3에서 회람될 예정이다.

3. 맺음말

하드웨어 기반의 키은닉 핵심기술인 PUF 기술은 아직 숙성도가 낮고 시장의 신뢰도도 낮은 상황이다. 그러나 이러한 기술들이 처음 기대했던 성능이 만족될 경우 그 활용 가치는 매우 크고 시장의 요구가 기하급수적으로 커질 것으로 예상된다.

ISO/IEC 20897-1 표준에서는 PUF 보안 요구사항 자체를 표준화하고 있으므로 기술장벽과 관련이 없지만, ISO/IEC 20897-2 표준은 Reliability, Uniqueness, Unpredictability, Diffuseness 등의 보안 요구사항에 대한 계산식과 테스트 방법이 제시되면서 성능의 차이를 객관적으로 비교할 수 있는 근거를 제시하고 있다. 비록 표준문서가 구체적인 판단 기준을 제시하지는 않더라도 구체적인 계산식의 제시는 기술력과 관련된 문제가 될 수 있으므로 우수한 성능의 PUF 생산 기업에게 유리한 표준이 될 수 있다. 하지만 중장기적인 관점에서 보면, PUF를 사용하고자 하는 시장에 객관적 성능 측정 방안을 제시하여 시장 활성화를 촉진한다는 긍정적인 측면도 존재한다.

따라서, 비록 현재 PUF 기술이 숙성도가 낮고 현재의 시장 요구가 적더라도 미래의 키은닉 기술 시장 활성화를 위해 주요 후보인 PUF 기술의 보안 요구사항 정의 및 시험/평가 방법 표준화에 관심을 가지고 적극 참여하여 시장이 필요로 하는 기술로 표준화를 유도하는 것이 바람직할 것으로 판단된다.