情 報 保 護 學 會 誌
第 14 券 第 5 號, 2004. 10

IT 보안기술 국제표준화
- ISO/IEC JTC1/SC27 WG2 28차 싱가포르 회의 활동을 중심으로-

장 청 룡*, 천 동 현**, 차 재 현***

요 약

ISO/IEC JTC1/SC27의 WG2는 정보보안기술을 위한 관련 메커니즘의 표준을 만드는 Working Group이다. 본 고에서 소개하는 28차 싱가포르회의(2004. 4) 이전에 개최된 21차 동경회의(2000. 10)와 22차 오슬로회의(2001. 4)에 대해서는 동 학회지 제11권 1호(2001년 2월)와 제11권 3호(2001년 6월)를 참고하고, 23차 서울회의와 WG2 중 블록암호 표준화 동향에 대해서는 제11권 6호(2001년 12월), 24차 베를린회의(2002. 4)에 대해서는 제12권 2호(2002. 4)를 참고하기 바란다. 본 고에서는 금년 4. 19(월)~23(금)에 걸쳐 싱가포르 Conrad Continental Singapore에서 개최된 제 28차 WG2 회의의 활동 결과를 소개하고, 아울러 암호알고리즘의 표준화 정책변경으로 지난 2000년부터 SEED의 국제표준 채택까지의 표준화 활동을 정리하고 향후 차세대 암호 기법의 국제표준화를 위한 제언을 한다. 또한 이번 회의 기간 중 아시아권 보안 기술 및 제품의 보급 확산을 위한 RAISS(Regional Asia Information Security Standards) 포럼의 동향과 대응방안에 대하여 제안한다.

Ⅰ. 서 론

금번 SC27/WG2 싱가포르 회의(2004. 04. 19(월)~4. 23(금))에는 한국대표로 ISO/IEC JTC1/SC27 한국대표 기관인 기술표준원 담당관을 비롯하여 5명이 참석하였고, WG1에 2명, WG3에 3명 등 총 10명이 참석하였다. WG2 회의에는 영국 2명, 미국 2명, 일본 8명, 벨기에 2명, 캐나다 1명, 스웨덴 1명, 남아공 1명, 싱가포르 2명, 독일 1명, 중국 2 등 총 27명이 참석하였으며 지금까지 국제회의에 모습을 보이지 않았던 중국이 참석하였다.

회의는 WG2 Convener인 M. DeSoete(벨기에)가 주재하였으며 그녀가 SC27의 Vice-chair로 자리를 옮김에 따라 이번 회의까지 임기를 마치고 차기 회의부터 일본의 K. Naemura가 WG2 convener 역을 맡게 되었다.

이번 회의는 특별히 우리나라가 동경회의(2000. 10)에 128비트 블록암호알고리즘 후보로 SEED를 제안한 이래 3차 CD에 수용된 SEED를 표준안에 수용하는가의 여부에 대한 각 회원국들로부터의 투표 결과를 심의하고 이의 결과에 따라 최종 블록암호알고리즘을 결정하는 회의였다.

이를 위하여 지난 파리회의(2003. 10) 이후의 캐나다, 일본 등의 관계자들과 수차례의 e-mail 교신, 직접 면담 등을 통하여 SEED에 대한 국제표준화의 지지를 요청하여 상호 굳건한 협력을 하는 방향으로 의견을 모았다. 더욱이, 회의현장에서도 지지 약속 회원국은 물론 개최국인 싱가포르 대표로부터도 지지를 받아내어 우리나라의 SEED를 찬성 7, 반대 2로 최종위원회문서(FCD)에 수용시킬 수 있었다[17, 19].

또한, 패스워드 기반의 키 설정 프로토콜에 관하여 우리나라가 제안한 2개의 기법(AMP와 C2C PAKA) 중 AMP만이 1차 CD에 수용되었다. 아울러 디지털 서명기법 중 메시지 복원기법의 ECKNR 기법이 1차 CD에 수용되었으며 부가형 기법으로는 KCDSA와 EC-KCDSA, 그리고 식별자 기반 기법인 IBS-2가 계속해서 2차 WD

* 경동대학교 컴퓨터미디어공학부(crjang@kl.ac.kr)
** 한국정보보호진흥원 전자거래보호단 암호인증기술팀(dhcheon@kisa.or.kr)
** 산업자원부 기술표준원 (chajh@ats.go.kr)

에 수용될 수 있게 되었다[16, 18, 20].

본 고에서는 II절에 금년 4월 싱가포르에서 개최된 ISO/IEC JTC1/SC27 WG2의 활동을 소개하고, III절에서는 암호화 알고리즘의 국제표준화 정책변화로 지난 2000년부터 블록암호의 표준화를 위하여 노력한 결과 최종위원회문서까지 수용된 SEED TFT의 활동 및 이의 추진을 위하여 ISO/IEC 18088-1의 표준 선정 기준인 Annex A에 의거한 SEED의 justification을 항목별로 정리하였다. 아울러, IV절에서는 같은 회의기간 중 싱가포르에서 제안한 아시아권 보안 기술 및 제품의 보급 확산을 위한 RAISS(Regional Asia Information Security Standards) 포럼의 진행사항을 소개한다. V절에서는 국제 수준의 평가결과를 요구하는 부문에서의 활동을 위한 제언을 중심으로 결론을 정리하였다.

II. WG 2 28차 싱가포르회의 주요 논의 사항

1. 3차 CD18033-3(Encryption algorithms - Part 3: Block cipher)에 대한 논의[17, 19]

가. 검토문서:

- o SC27 N3752, Text of 3rd CD
- o SC27 N3901rev1, Summary of Voting, Revised summary of voting on selection of algorithms to IS 18033-3 Information technology - Security techniques of - Encryption algorithms - Part 3: Block cipher
- o SC27 N3899rev1, Summary of voting for 3rd CD

나. 회의 진행 : 에디터 Chikazawa(일본 미쓰비시)

- o 회의 첫날 우리나라에서 SC27 사무국으로 송부한 투표 문건이 접수되지 않음을 발견하여 즉시 한국에서 준비한 관련 문서들을 포함시켜 개정판을 배포하였다.
- o 다음날 회의에서 의장이 64비트건과 128비트건을 하나씩 별도로 처리하는 것으로 진행하였다.
- o 캐나다 측에서 3차 CD문서에 대한 반대투표의 의견을 개진하였다. 특히 투표처리의 적용을 서신투표에서 JTC 1 DIRECTIVES(4th EDITION)의 CLAUSE 12.6(과반수 투표에 과반수 찬성)로의 적용에 대하여 투표일 현재 31개 회원국에서 15개국 투표하여 찬성, 반대 및 기권이 각각 9:2:4로 투표결과가 되어 만약 CAST-128이 현 문서에 포함되지 않을 경우 엄격히 규정의 적용하던지 아니면 투표자체를 무력화 시키려고 하였다.

〈표 1〉 FCD 18033-3에 포함된 블록암호

구분	제안국	알고리즘명
64 비트	미국	TDEA
	일본	MISTY1
	캐나다	CAST-128
128 비트	미국	AES
	일본	Camellia
	한국	SEED

- o 에디터 및 WG2 Convener의 중재로 현재의 투표결과 CAST-128과 SEED는 찬성과 반대가 각각 9:2와 6:2(회의에서 싱가포르의 찬성 1표 추가로 7:2)로 투표 회원국 과반수 이상이 찬성하여 해당 표준후보 모두를 현 3차 CD에 포함시키기로 하고 이를 최종 CD(FCD)로 진행시키기로 하였다.
- o 주요 결의사항 : 〈표 1〉과 같이 3차 CD에 포함된 6개의 블록암호를 모두 FCD에 포함하여 진행하기로 하였다.
- o Annex E의 ASN.1 표기에 관한 미국의 편집의견이 수용되었다.
  - 본문은 single space로 편집되어야 한다.(현재는 double space임)
  - 본문은 현재 (ASN.1 comment delimiter)인 two dash characters를 single non ASCII, hard dash로 자동 변환시키는 'smart-dash feature'에 의하여 영향을 받아 의의수정이 요구된다.
  - ASN.1의 폰트는 'Courier New Font'로 처리한다.

2. 3차 WD11770-4(Key Management - Part 4: Mechanism based on weak secrets)에 대한 논의[20]

가. 검토문서:

- o SC27 N3894, Summary of NB Comments, Summary of NB Comments on document SC27 N 3741 - ISO/IEC 3rd WD11770-4 - Information technology - Security techniques of - Key Management - Part 4: Mechanism based on weak secrets

나. 회의 진행 : 에디터(L. Chen, 영국 HP)

- o C2C-PAKA: 1차 CD에 수용되지 않았다

- 퀘벡회의(2003. 4)에서 논의를 시작하였으나 이에 대한 공격 가능성이 파리회의(2003. 10)에서 논의되어 이의 안전성을 한국의 제안자와 에디터 간에 논의하였다. 이의 최종판이 현재 논문 심의중이며 최종 5월 10일 확정 예정이라 설명하였다(e-amil 서신에 대하여 최근 메일 답신이 Chen에게 전달되지 않아 직접 전달함).
- 이와 같은 형태의 제안은 미숙한 제안으로 인식되었으며 또한 관련 자료의 검토 또한 각 회원국에서 이해 부족으로 안전성 및 인지도가 낮아 기각 처리되었다.

o AMP : 1차 CD에 수용되었다.
- 구현 사례: PASSWORD 생성, 알고리즘 자체에 대한 구현 사례에 대한 기고를 일본측에서 요청하였다.
- WU[98]기법에 대한 문서의 안전성 공격에 대한 의견을 제시하여 현재 표준안에 수용된 SRP3을 SRP6로 대체시키자는 의견을 제시하였다. 에디터는 이의 이해를 하고 있으나 참여 회원국 대표들은 이에 대한 이해 부족으로 검토를 위한 문서의 접근은 IEEE회원가입으로 제한되는 바, 이의 관련 최근 문서(IEEE 1363.2, WU[02])를 에디터와 회의 참여 전문가들에게 배포해 줄 것을 요청하여 이를 한국 NB에서 준비하여 배포하기로 하였다.

3. 1차 WD9796-3(9796-3 1차 개정, Digital signature schemes giving message recovery - Part 3: Discrete logarithm based mechanisms)에 대한 논의

가. 검토문서:

o SC27 N3891, Summary of NB Comments, Summary of NB Comments on document SC27 N3731 - ISO/IEC 1st WD 9796-3 - Information technology - Security techniques of -Digital signature schemes giving message recovery - Part 3: Discrete logarithm based mechanisms

나. 회의 진행 : 에디터(A. Miyaji, 일본 JAIST)

o ECKNR : 1st CD에 수용되었다.
- 현 WD에 수용되어 있지 않음을 지적하여 이를 수용하기로 하였다.
- 모든 기법들에 대한 ASN. 1 모듈을 본 표준안의 부기에 수용하기로 하였다.
- 모든 기법들에 대하여 일반 유한체, 유한체 상에서의 타원곡선 및 둘 모두에 사용됨을 표현하는 주석을 포함시키기로 하였다.

4. 1차 WD14888-3(14888-3 1차 개정, Digital signature schemes with appendix - Part 3: Discrete logarithm based mechanisms)에 대한 논의

가. 검토문서

SC27 N3893, Summary of NB Comments, Summary of NB Comments on document SC27 N3737 - ISO/IEC WD 14888- 3 - Information technology - Security techniques of -Digital signature with appendix - Part 3: Discrete logarithm based mechanisms

나. 회의 진행

공동 에디터(이필중, 한국 포항공대, L. Chen, 영국 HP)

o KCDSA, EC-KCDSA 및 IBS-2 : 2차 WD에 수용되었다.

5. 제안 신규 과제 연구

가. 생체 데이터의 인증에 관한 연구 기간이 필요함을 인식하여 P. Griffin을 라포타로 임명하고 관련 기고 요청을 각 회원국에 2004. 8. 1까지 배포하기로 함(Resolution 6). 또한 이와 연계하여 SC17 WG3와의 Liasion officer를 L. Yih로 임명하였다(Resolution 21).

나. 객체 식별자(object identifiers)와 ASN.1 Syntex에 관한 연구 기간이 필요함을 인식하여 P. Griffin을 라포타로 임명하고 각 회원국에 관련 기고를 요청하기로 하였다(Resolution 19).

6. 암호알고리즘 등록(IS 9979)에 대한 회원국 의견 수렴

o Future of the Register of Cryptographic Algorithm

The Register of Cryptographic Algorithms was initially set up at a time when ISO/IEC

had resolved that it would not standardize encryption techniques. The register, online at www.isoregister.com, allows non- standardized encryption algorithms to be given an agreed name. However, since the register was initially set up under the terms specified in ISO/IEC 9979, ISO/IEC policy has changed, and the multi-part international standard ISO/IEC 18033 covering encryption techniques is now nearing completion. In addition, ISO/IEC 9979 will be subject to a review in 2005.

The near-completion of ISO/IEC 18033 suggests that now is an appropriate time to review the future of the register. National Bodies are therefore requested to respond to the following question so that appropriate decisions can be made.

1. would the NB object if the register is closed to new entries, i.e. the addition of new algorithms to the register is no longer possible?(SC27 N4022, 2004. 4. 22 문서에는 삭제됨)
2. Would the NB object if the register ceased to exit(and ISO/IEC 9979 is withdrawn)?

o 현재 18033이 FCD를 걸쳐 2005년까지 표준화가 완료될 예정이므로 과연 IS 9979에 등록되어 있는 암호알고리즘들에 계속적인 추가등록이 과연 적절한가에 대한 회원국들의 의견을 수렴하고 있다. 따라서, 최근 표준화중인 알고리즘들은 아직 등록이 안된 상태여서 표준 수용 관계국들과의 협의를 통하여 상기 사항을 결정할 예정이지만 본 투표에는 개인적으로는 반대할 이유는 없다고 사료된다.

III. 국제 표준화를 위한 SEED TFT의 활동과 제언

1. SEED TFT의 국제표준화 활동[1,2,3,4,5,6,7,8,9]

런던 회의(20차 SC27 WG2 회의, 2000. 4)에서 암호알고리즘의 신규과제 논의에 대하여 KISA의 후원으로 한국정보보호학회 회원들이 주축이 된 암호알고리즘 TFT가 결성되었다. 당시 산업계 단체표준인 SEED를 포함한 암호알고리즘에 대한 국제표준화 후보 공모와 이에 따른 공청회를 통하여 동경회의에 SEED를 포함한 3개의 국내 개발 알고리즘을 후보로 제안하였다. 이후 오슬로 회의와 서울회의를 거쳐 SEED만이 작업문서(WD)에 수용되었다. 이를 위하여 TFT에서는 국제회의를 통하여 지적된 사항과 SEED의 개발 당시 안전성 검증 자료를 제외한 성능평가 자료가 미비하여 TFT 참여위원과 국내 전문가들의 헌신적인 봉사로 ISO/IEC 18033-1 Annex A의 표준암호 선정기준에 의거 알고리즘 분석서, 소프트웨어 평가자료와 하드웨어 평가자료(ASIC (Application Specific Integrated Circuit) 혹은 FPGA (Field Prgrammable Gate Array), IC 카드 환경) 등을 준비하여 관련 국제회의에 지속적으로 기고하였다. 특히, 투표문건에 대하여는 우리와 입장이 유사하거나 혹은 우리를 이해할 수 있는 회원국 전문가 및 대표들과 e-mail 교신, 해당국의 직접 방문 등을 통하여 한국측 제안의 정당성을 홍보하여 그들로부터 긍정적인 지지를 받아내었다.

이러한 국제 활동을 크게 국제적 평가 전문가들과의 협력과 국제표준화 회의 활동으로 나누어 설명하기로 한다. 국제 평가 기관인 NESSIE에 대하여는 중간결과 발표회의 참여와 참여기관 중 하나인 런던대학 관계자와의 협력 증진, KISA에서 과제 책임자의 초청을 통한 협력 증진 그리고 CRYPTREC에서의 SEED 평가를 위한 이의 주관 정부기관 관계자와의 상호 방문을 통한 협력 등에 의하여 SEED가 국제적 평가기관들로부터 안전성과 성능 측면에서 공인된 결과를 얻을 수 있었다. 이러한 결과들은 국제 표준화 회의 참여 및 이를 위한 기고에서 각 회원국들을 이해시킬 수 있는 훌륭한 자료가 되었다.

한편, 국제회의에 대한 대응의 위하여 기술표준원이 운영하는 전문위원회에서 예상되는 문제점에 대한 충분한 논의를 거쳐 회의에 임하였음에도 불구하고 국제회의 현장에서 특정한 문제에 대하여 참여 회원국 대표들을 이해시키기 위한 문서의 준비에 따른 현장에서의 유연한 대처 능력의 발휘와 이의 문서 등록을 통하여 향후 활용할 근거 자료의 확보가 필요하다. 그리고 투표문건에 대하여는 회의 현장에서 회원국들의 지지 확보와 반대 회원국의 설득 등을 통한 우호세력 확보를 위하여 관련 회원국 대표와 해당 프로젝트 에디터와의 지속적인 협조 관계 유지가 필요하다. 이는 국제회의의 지속적인 참여와 회원국 대표간의 상호 협력을 전제로 이루어 질 수 있으며 이를 위하여 우리나라에서도 표준화 과제 발굴과 에디터를 육성·지원하는 방안이 강화되어야 할 것이다.

2. SEED의 국제표준 선정 기준에 대한 정당화

본 절에서는 ISO/IEC 18033-1의 Annex A(Criteria for inclusion of ciphers in this International Standard)에 있는 표준 선정을 위한 각 항목별 정당성을 정리한다.

2.1 안전성 : 알려진 다양한 공격, 안전성의 증명, 널리 알려진 평가기관으로부터의 평가

o SEED는 128비트 블록 크기와 128비트의 고정된 키 길이를 갖는 안전성이 우수한 Feistel 구조의 대칭키 블록암호알고리즘으로 안전성 분석을 위하여 국내 암호전문가들에 의한 기존의 다양한 공격에 대한 평가결과를 제시하였으나 알고리즘 제안(2000. 9) 당시 NESSIE(2000.3 ~ 2000. 9)와 CRYPTREC(2000. 6. 13 ~ 7. 초)의 평가에 응모하지 못하여 제 3의 평가기관에서의 평가결과가 없다는 지적을 회원국들로부터 받았다. 그러나, 일본의 CRYPTREC에서의 안전성 평가(2002. 2)과 NESSIE의 성능평가 결과(2003. 2)에 의해 어느 정도 회원국들에게 우수함이 인지되었다.

2.2 다양한 플랫폼에서의 성능 :

o SEED의 설계 당시 AES의 기준으로 TDEA 보다 좋은 성능을 고려하였으며 하드웨어 구현 성능에 대한 검토가 미진하였다. 즉 하드웨어 설계시 면적, 게이트 수, 소모 전력 등에 대한 자료의 분석이 미진하였다. 또한 소프트웨어 구현에서도 C, JAVA 등의 언어와 8비트 마이크로프로세서, PC, 워크스테이션 등 다양한 환경에서의 구현결과를 확보하는 것이 미진하였다. 그러나, NESSIE의 성능평가 결과(2003. 2) 중 일부 항목이 후보 알고리즘과의 비교에서 다소 유리한 점 등이 어느 정도 회원국들에게 인지되었다[7,17].

2.3 라이센싱 문제

o SEED는 개발 당시 글로벌 시대에서 인터넷을 기반으로 하는 안전한 전자상거래의 활성화가 목적이었기 때문에 특허권을 등록하지 않았으며, 이의 개발과 보급을 주관해온 한국정보보호진흥원은 SEED를 사용하는 자에게 국내·외를 차별하지 않고 알고리리즘 사용에 대한 어떤 대가도 요구하지 않음을 강조하였다.

2.4 성숙도

o SEED는 '99년 개발완료 이후 바로 정보통신단체표준으로 채택되었고 아울러 2004년 10월 현재 780개의 국내·외 산업계, 학계 및 연구기관에 배포되어 사용되고 있다. 또한, 세계적으로 국내 인터넷 보급률이 1위임을 인식시키고 이를 기반으로 하는 증권거래, 전자상거래, e-cash, 교통카드 등의 비밀성 서비스에 활용되고 있음을 강조하였다[17].

2.5 공인기관으로부터의 인정 수준

o SEED는 '97년부터 한국정보보호센터 주관으로 개발 및 자체 평가를 통하여 안전성과 성능 측면에서 우수한 것으로 판단되어 정보통신단체표준(TTAS.KO-12.004(1999. 9))으로 채택되었으며, 국제적 수준으로 활용할 만한 가치가 있는 표준 후보로 ISO/IEC JTC1/SC27 동경회의(2000. 10)에 제안되었다. 이후 CRYPTREC의 평가(2002. 2)에서 안전성에서는 문제가 되지 않으나 부분키생성 알고리즘에서 특정키 패턴이 생성됨을 지적받았으며 전반적으로는 키의 전수조사만이 유일한 공격이라는 안전성 평가결과를 얻

〈표 2〉 NESSIE의 블록암호 S/W 성능 평가 결과

순번	Platform	AES	SEED	Camellia
1	PIII/Win Visual C 6.0	23/23/497 주)	57/57/446	65/65/411
2	PII/Win Visual C 6.0	22/23/612	56/56/447	64/64/479
3	PIV/Linux Northwood gcc 2.95.2	26/26/1329	63/63/467	71/72/535
4	AMD Duron Win XP VC 7.0(.NET)	32/35/500	52/51/410	68/68/330
5	Alpha Cc	17/17/493	44/44/358	48/48/287
6	Sun/Sparc V9 450 MHz gcc 3.0.4+3.2.1	31/29/684	35/35/381	49/49/375
7	Sun/Sparc 248MHz gcc 2.95.3	31/31/705	36/36/447	55/55/352
8	Sun 333MHz gcc 3.2.1	29/30/655	39/37/396	51/51/381

주 : 암호화/ 복호화/ 키 설정 시간, 단위 [cycles/byte]

었다. 또한, PC 기반(Pentium III급 @650MHz) 성능측면에서는 다소 느린(moderate slow) 등급의 평가를 받았다. 그러나, NESSIE의 다양한 플랫폼(Pentium III급 ~ SUN @333MHz)에서의 S/W 성능 평가(2003. 2)에서는 ISO/IEC JTC1/SC27 128비트급 최종 후보들의 평가에서 Camellia 보다 우수한 성능을 보이는 것으로 평가를 받았다[8,15,17].

2.6 채택 수준

o SEED는 국내의 산업표준으로 뿐만 아니라 국제적으로 이를 채택하여 소프트웨어 및 하드웨어로 구현되어 다양하게 제품으로 사용되고 있다. 최근, ISO/IEC JTC1/SC27 싱가포르회의에서 최종위원회문서에 수용됨에 따라 이를 채택하여 유통 및 저장정보에 대한 보호와 프라이버시 보호를 위한 비밀성 서비스에 다양하게 채택되어 질 것으로 전망된다[5, 16, 19]

2.7 표준화될 후보 알고리즘 개수의 최소화

o 이에 대해서는 제안 초기부터 많은 논란을 가지고 있었다. a)항에서는 두 개 이상에 대한 예외로서 계산량과 하드웨어 공간 등 구현상에서의 차별화, 적용 환경에서의 특별한 차별화 등일 경우와 b)항에서는 공격 등 안전성 측면에서 다른 설계 원칙을 적용한 경우로 대안적 성격으로 후보를 복수화 한다는 것이었다. 표준안에 각 회원국의 제안 후보의 수용은 서울회의(2001. 10)에서 안전성에 문제가 없는 것은 모두 작업문서에 수용하는 것으로 결의하였다. 그러나, 퀘벡회의(2003. 4)부터 표준 수용 후보의 개수에 대한 최소화를 위하여 투표를 하기로 하였다. 결국, 싱가포르회의(2004. 4)에서 64비트급 3개(TDEA, MISTY1, CAST-128)와 128비트급 3개(AES, Camellia, SEED)가 최종위원회문서에 수용되었다[16, 19].

Ⅳ. RAISS 포럼

지난 ISO/IEC JTC 1/SC27 싱가포르회의에서 본 회의와는 별도로 아시아 지역의 보안기술 및 제품에 대한 개발 촉진 및 보급 확산을 위한 논의를 하기 위한 준비로서 싱가포르 보안기술 위원회 위원장인 Meng-Chow Kang(Chair, Security & Privacy Standards Technical Committee, ITSC, Singapore, mengchow@acm.org)명의의 "RAISS (Regional Asia Information Security Standards) Forum"의 제안이 있었다. 이에 JTC1/SC27 회의기간 중 4월 22일 저녁에 제안국인 싱가포르, 한국, 일본, 호주, 말레이시아, 중국 등 관심 전문가들이 20여명 참석하였다. 이 회의의 주요 논의사항은 다음과 같다:

1. 의제의 선정

o 아시아 지역에서 보안기술의 개발 및 제품화의 수준이 차별화되었음을 인식하고, 이에 따라 선도 그룹과 후발 그룹간의 보안 표준분야의 채택과 전개에 관한 기술력, 경험 등이 공유될 수 있는 논의의 장 마련을 통해 그 격차를 해소하는 방안 모색
o 선도 그룹에게는 표준의 개발 방향과 대상을 발굴할 수 있는 기회를 제공

2. 참여 기관

o 후원 기관 : 정부, 민간 업체
o 참여 회원 : 민간 업체의 참여 장려

3. RAISS 포럼의 목표

가. 지역 경제체제들의 보안표준 개발, 채택 및 전개 활동에 관한 지식 공유 및 경험 습득을 위한 포럼의 지원
나. 아시아 지역에서 국제 보안표준의 개발 및 보급을 더욱 효과적으로 하기 위해 지역적인 협력을 위한 포럼을 구성하고 지역 기구들을 위한 포럼에서 다음과 같은 사항을 지원:
  o 지역적 보안표준의 요구사항 및 방향 설정
  o 표준의 구현 및 사용상의 연동성 및 호환성을 진흥시키기 위한 지역적 합의 혹은 이해

4. 업무 추진 방법

상기 목표를 달성하기 위하여 세부 실행 프로그램을 기획하고 추진하기 위한 아시아 지역 표준화 기구의 주요 정책 결정자와 리더들로 구성되는 조직 위원회를 구성한다.

이를 위한 초기 단계의 목표는 다음과 같다:

1) 초기 포럼의 지속적인 발전을 모색하고 이 지역에서의 검토와 합의를 이루는 관점에서 본 포럼의 초기 단계 목표 확인
2) 관련 기고의 제출 요청, 본 포럼의 운영을 위한 기금의 확보 등을 포함하는 초기 포럼을 위한 프로그램 개발

3) 행사장 선정, 계획, 참가 요청, 발제자 및 특별 초대자 초청 등을 포함한 초기 포럼 행사의 조직
4) 포럼 멤버 혹은 참여자들과 함께 본 포럼의 최종 목표와 비전의 개발 및 향후 계획의 개발

5. 향후 추진

본 포럼은 다양한 형식의 회의를 통하여 지역내 보안 표준 기구들의 적극적인 참여와 정보 공유를 통하여 목표를 달성하도록 한다.

6. 최근 동향 및 대응

최근 싱가포르에서 접수된 서신에 의하면 온라인 토론방(http://groups.msn.com/RAISSForum)의 개설로 한국의 참여를 권유하고 있다. 또한, 금년 11월 19일 동경에서 1차 RAISS 포럼을 일본정부의 후원에 의하여 개최될 예정이다.

한편, 싱가포르 회의에서 언급된 한국(KISA)의 보안 보증(CC) 워크숍에 관한 관심을 표명하며 만약 동경회의에서 본 포럼의 일환으로 이를 개최시 적극 지원을 하겠다고 하였다.

더욱이, 싱가포르는 본 포럼의 종신적 사무국 운영을 제안하였다. 아울러, 본 포럼의 회칙(Terms of Reference for RAISS Forum)을 1차 동경회의에서 결정하고자 하고 있다.

본 포럼에의 한국 참여는 아시아권 시장에 대한 일본의 독주를 견제하고 중국의 움직임에 대한 대응을 위하여 산학연관이 협력하여 체계적으로 추진하여야 할 것이다. 또한, 싱가포르는 사무국 유치라는 카드를 사용할 것이기 때문에 이에 대한 대비가 필요하다. 즉, 종신적 사무국보다는 임기적 사무국 운영이 당분간 유지됨이 바람직하다. 또한 기술 개발에 대한 제안으로 전자상거래 결재 등에의 PKI 솔루션, 암호화 제품으로 우리의 강점을 정리한 대비가 필요할 것이다. 더욱이, IT839 전략 추진에 따른 보안 기술 개발 및 제품화를 위한 항목 선정도 적절할 것이다.

아울러, 이러한 포럼을 통하여 특정 보안제품에 대한 적합성 및 상호운용성 검증을 위한 시험 플랫폼의 운용과 이들 결과의 발표도 하나의 이슈가 될 수 있을 것이다.

V. 결 언

본 고에서는 SEED를 비롯한 국내 개발 알고리즘에 대하여 ISO/IEC JTC1/SC27/WG2 28차 싱가포르회의 활동들과 SEED와 같은 국제 평가를 통한 표준 제안 후보의 표준 선정시의 국내외 활동과 이를 위한 제언을 하였다. 아울러, 최근 아시아권 지역의 보안 기술 및 제품의 보급 확산을 위한 RAISS 포럼 동향 및 이의 대응 방안도 정리하였다.

이번 SC27/WG2 싱가포르 회의를 통하여 SEED의 최종위원회문서 수용 등은 국제표준화 활동의 좋은 성과의 하나이며 이는 국내 암호기술 수준의 국제화를 위한 진일보의 계기가 되어 보안기술 분야에서 국제적 위상을 제고할 수 있게 되었다.

금년 10월회의를 통하여 SEED는 최종국제표준안(FDIS, final DIS)으로, AMP와 복원형 디지털 서명의 ECKNR 기법 은 최종위원회문서로 진행될 예정이다. 그리고 부가형 디지털 서명 기법인 KCDSA와 EC-KCDSA, 그리고 식별자 기반 기법인 IBS-2는 1차 CD문서로 진행될 것이다.

이와 같은 국제표준화 활동을 모델로 앞으로 차세대 암호알고리즘이 개발될 경우에는 이의 글로벌 이용을 전제로 개발 목표 또는 적용 분야를 차별화하고 안전성 평가를 위한 다양한 공격에 대한 자체 분석은 물론 이들에 대한 공개 검증을 위하여 제 3의 평가 기관 또는 주요 국제 학술기관에 의해 평가를 받아야 할 것이다. 아울러, 성능평가의 경우도 소프트웨어 구현 환경별(PC급, 워크스테이션급, 하이-엔드 플랫폼, C, Java 등의 구현 언어) 평가, 하드웨어 환경(IC 카드, FPGA 등)에서의 구현 면적, 전력 소모 등을 고려한 성능평가가 지금까지 공개된 우수한 국제표준 후보들과 비교하여 이루어져야 한다. 그리고, 이러한 결과들은 공개매체인 웹 등을 통한 홍보가 필요할 것이다. 아울러, 국제 표준화를 위하여 표준화 대상의 발굴과 이에 따른 프로젝트 에디터의 육성 및 지원 또한 중요한 과제이다.

아울러, RAISS 포럼 활동에도 적극 참여하여 국제시장 진출을 위한 국산제품의 수출 경쟁력 확보 방안의 수립과 후진 개발도상국들에게 IT 및 관련 보안 기술과 솔루션의 소개를 통한 국제 협력에도 노력을 기울여야 하겠다.

참고문헌

[1] 이홍섭 외, "정보보호기술개발 - 128비트 블록 암호알고리즘 (SEED) 개발 및 분석 보고서 (http://www.kisa.or.kr/technology/sub1/128-seed.pdf)", 한국정보보호센터, 1998. 12
[2] 박성준, "국내 표준 블록 암호알고리즘(SEED) 활

용방법", 제4회 정보보호 심포지움(SIS '99), 한국정보보호센터, pp. 575~599, 1999. 4.
[3] 장청룡 외, "SEED의 ISO/IEC 국제표준화 추진", 한국정보보호진흥원, 2001. 11
[4] 장청룡, "블록 암호 SEED의 국제표준화", 경동논총, 경동대학교 대학교육문화원, 2003. 12.
[5] 정보통신단체표준(TTA.KO-12.0004), http://www.kisa.or.kr/evaluation/webdriver?MIval =hh_3_tta.
[6] SEED, http://www.kisa.or.kr/seed/index.html,
[7] B. Preneel, B. Van Rompay, S. B. Ors, A. Biryukov, L. Granboulan, E. Dottax, M. Dichtl, M. Schafheutle, P. Serf, S. Pyka, E. Biham, E. Barkan, O. Dunkelman, J. Stolin, M. Ciet, J-J. Quisquater, F. Sica, H. Raddum, M. Parker, "Performance of Optimized Implementations of the NESSIE Primitives", NESSIE, February 20th, 2003.
[8] CRYPTREC, 暗號技術評價報告書(2002年度) (CRYPTREC Report 2002), http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/doc/c02_2 .pdf
[9] NESSIE project description, http://www.cosic.esat.kuleuven.ac.be/ nessie/.
[10] ISO/IEC JTC1/SC27 , "ISO/IEC 9979 Register of Cryptographic Algorithms", http://www.din.de/ni/sc27/doc7.html#9979
[11] ISO/IEC JTC1/SC27, "A Call for Contributions to a New Work Item Proposal on "Encryption Algorithms", ISO/IEC JTC1/SC27 N2477, 1999. 12.
[12] ISO/IEC JTC1/SC27, "Summary of Voting on JTC1 N6009(SC27 N2488), Proposal for a New Work Item Proposal on Encryption Algorithms(JTC1 N6112)", ISO/IEC JTC1/SC27 N2521, 2000. 3.
[13] ISO/IEC JTC1/SC27, "National Body Contributions on NP 18033 "Encryption Algorithms" in response to SC27 N2563 (ATT. 3 Korean Contribution)", ISO/IEC JTC1/SC27 N2656r1 (n2656_3.zip), 2000. 10.
[14] ISO/IEC JTC1/SC27 ," Resolutions of the 21st meeting of SC 27/WG 2", ISO/IEC JTC1/SC27 N2720(SC27/WG2 N463), 2000. 10.
[15] ISO/IEC JTC 1/SC 27, "Third Party Evaluation on SEED by CRYPTREC", ISO/ IEC JTC 1/SC 27 N3213, 2002. 4.
[16] ISO/IEC JTC1/SC27, "Resolutions of the 28th meeting in Singapore of SC 27/WG 2", ISO/ IEC JTC1/SC27 N4026, 2004. 4.
[17] ISO/IEC JTC1/SC27, "Summary of Voting on Selection of Algorithms to ISO/IEC 18033-3 Information technology -Security techniques - Encryption Algorithms-Part 3: Bloch ciphers", ISO/IEC JTC1/SC27 N3901rev1 att2 (Juastification for Inclusion of SEED in ISO/ IEC 18033-3), 2004. 4.
[18] ISO/IEC JTC1/SC27, "Disposition of comments received on document SC27 N3737rev1 - ISO /IEC 1st WD 14888-3, IT security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms (revision)", ISO/IEC JTC1/SC27 N3968, 2004. 4.
[19] ISO/IEC JTC1/SC27, "Dispositions of comments received on document SC27 N3752 ISO/IEC 3rd CD 18033-3 - IT Security techniques - Encryption algorithms - Part 3: Block ciphers, ISO/IEC JTC1/SC27 N3978, 2004. 5.
[20] ISO/IEC JTC1/SC27, "Disposition of comments received on document SC27 N3741 ISO/IEC 3rd WD 11770-4 - IT Security techniques - Key management - Part 4: Mechanisms based on weak secrets(ref. document Summary of Voting SC27 N3894), ISO/IEC JTC1/SC27 N3970, 2004. 5.

〈著 者 紹 介〉

장 청 룡 (Chung-ryong Jang)
종신회원

1980년 2월 : 성균관대학교 전자공학과 졸업
1986년 8월 : 연세대학교 대학원 전자공학과 석사
1994년 2월 : 성균관대학교 대학원 정보공학과 박사
1979년 12월 ~ 1983년 12월 : 한국전자통신기술연구소(현, ETRI), 연구원
1984년 1월 ~ 1997년 1월 : 한국통신 연구개발본부 선임연구원
1997년 3월 ~ 현재: 경동대학교 컴퓨터미디어공학부 부교수
관심분야 : 보안제품 시험, 통신망 보호, 블록암호

천 동 현(Donghyeon Cheon)
종신회원

1995년 2월 : 고려대학교 수학과 이학사
1997년 8월 : 고려대학교 대학원 수학과 이학석사
2001년 2월 : 고려대학교 대학원 수학과 이학박사
1999년 9월~2001년 8월 : 고려대학교 기초과학연구소 연구원
2001년 9월~현재 : 한국정보보호진흥원 암호인증기술팀 선임연구원
〈관심분야〉 암호학, 정보보호

차 재 현(Jae-hyeon Cha)

1985년 2월 : 한양대학교 전자계산학과 석사
2002년 2월 : 숭실대학교 컴퓨터학과 공학박사
1982년~산업자원부 기술표준원 보안기술연구관