CENTER FOR INFORMATION SECURITY TECHNOLOGIES

Global KU Frontier Spirit

KOREA UNIVERSITY

고려대학교 정보보호연구원

CIST LETTER

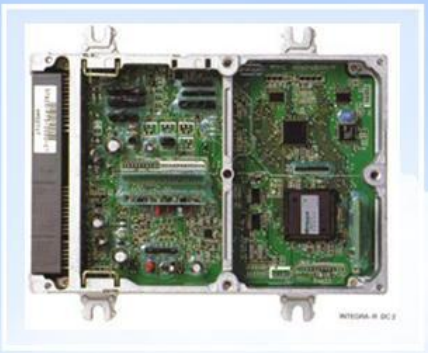
No. 18, February 2011

Contents

자동차는 과연 안전한가?

최근의 자동차는 사용자들에게 편리한 기능을 고루 갖추며 출시되고 있다. 우리가 익히 알고 있는 ABS(Anti-lock Brake System)부터 자동주차시스템에 이르기까지 많은 기능들이 점차 자동차에 탑재되고 있다. 이제는 자동차를 단순한 기계로 보기보단 전자제품으로 보는 것이 오히려 더 어울릴 정도로 자동차와 IT기술이 점차 결합되고 있는 것이다. 앞으로는 가솔린 대신에 전기를 동력원으로 하는 전기자동차의 시대가 올 것이다. 그렇게 된다면 자동차는 이전 세대의 자동차와는 다른 완벽한 하나의 전자제품으로 봐도 무방할 것이다.

하지만 자동차 내부에는 이미 예전부터 전자제품이 장착되어 쓰이고 있었다. 바로 ECU(Electronic Control Unit)이다. ECU는 자동차 내부에 장착된 여러 전자기기들을 제어하기 위한 장치로 컴퓨터에 비유하자면 CPU에 해당된다. 고급차량일수록 고급 기능들이 많이 구현되어 있고 ECU 또한 많이 장착되어 있다.



<ECU의 내부 구조>

이러한 ECU들은 CAN(Controller Area Network)이라는 프로토콜을 이용해 서로 정보를 교환한다. 하지만 이 CAN을 통해 전송되는 데이터를 외부에서 송/수신 할 수 있는 방법이 존재한다. 바로 자동차 진단을 위해 존재하는 OBD-Ⅱ(On Board Diagnostic) 포트를 통해 가능하다. OBD-Ⅱ포트는 자동차 핸들의 하단 부분에 존재하며 OBD케이블과 관련 프로그램만 있으면 누구나 쉽게 데이터를 송/수신 할 수 있다.

하지만 ECU는 서로 간에 메시지를 주고받을 때 인증과정이 전혀 없고 메시지는 평문으로 전송되는 등 보안에 매우 취약한 구조를 갖고 있다. 그렇기 때문에 사용자의 입력이 없이도(ex: 엑셀 밟기 등) 자동차를 제어하는 공격이 가능하다. OBD-Ⅱ 포트를 통해 수집된 데이터를 분석하여 원하는 기능의 메시지를 정확히 ECU에 전송한다면 자동차의 제어가 가능해진다.

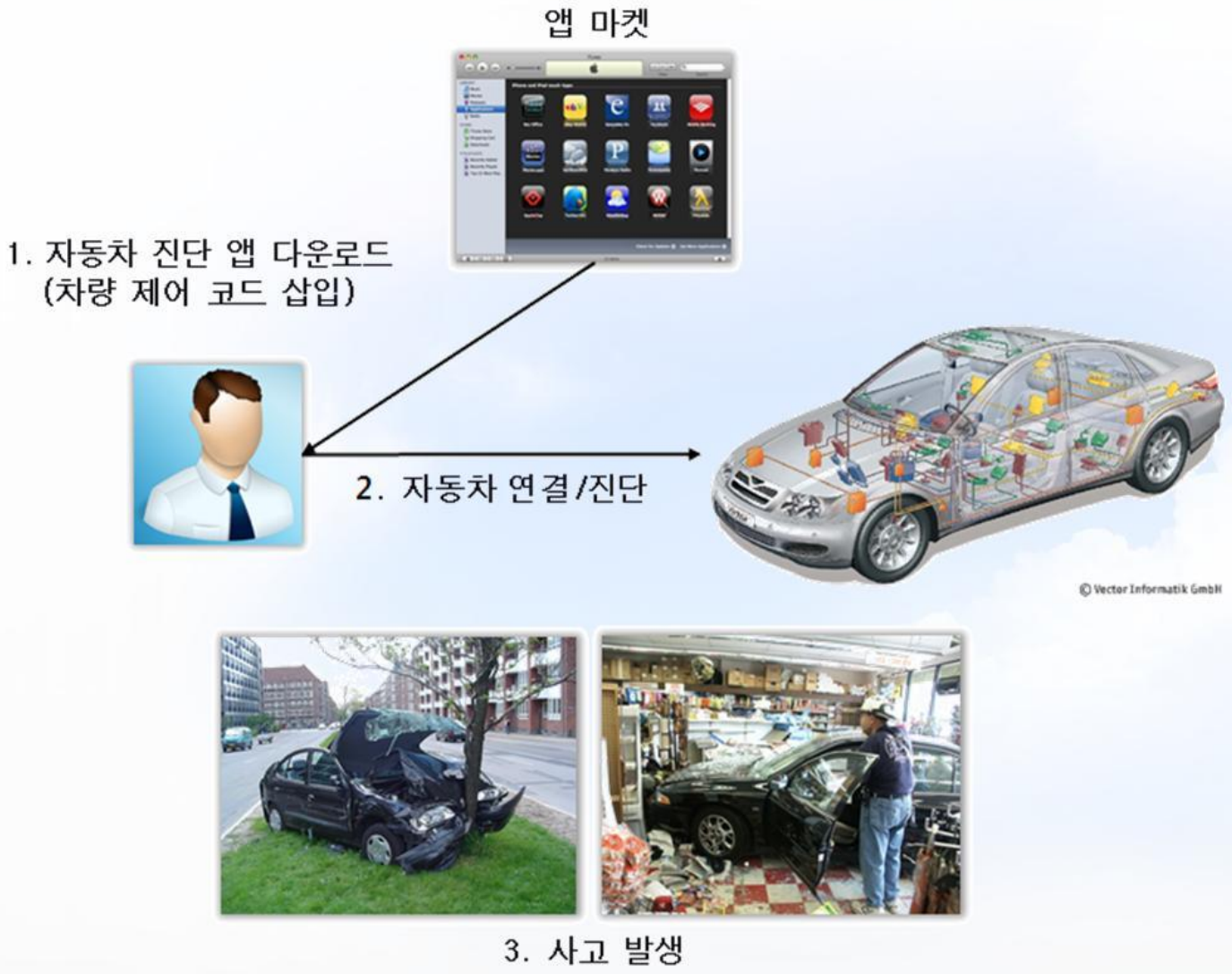
CAN 프로토콜의 메시지 규격은 표준이다. 하지만 메시지의 내용은 CAN을 운영하는 각 제조업체 별로 규정하기 나름이다. 이 메시지의 내용은 제조업체 별로 다르고, 차종별로 다르며, 같은 차종이라도 옵션에 따라 다르다. 그렇기 때문에 CAN 데이터 패킷을 분석하는 것은 쉽지 않은 일이다. 하지만 불가능한 것도 아니다. 문제는 ECU에 전혀 보안 메커니즘이 없다는 것이다.

우리 정보보호연구원에서는 국내 최초로 이러한 취약점을 이용하여 실제 국내 차량을 대상으로 차량 제어공격에 성공한 바 있다.

운전자가 없는 상태에서 엑셀을 구동시켜 시속 220Km까지 엔진을 구동시키고, VDC 기능을 끈 상태에서도 VDC 기능이 작동하게 하는 등의 공격을 성공하였다. 이 공격은 자동차 내부에서 OBD포트와 노트북을 연결하고 외부의 스마트폰에서 노트북에 메시지를 보내는 시나리오였다. 하지만 실생활에서 발생 가능한 시나리오 또한 존재한다.

국내 K자동차의 한 모델은 출시와 함께 스마트폰과 자동차 진단 앱, 스마트폰과 연동되는 OBD 무선포트를 제공하고 있다. 이 앱에 차량제어코드를 삽입 한다면 운전자는 주행 중에 자동차가 급발진하는 등의 사고를 당할 수가 있다. 다음의 그림은 이러한 시나리오를 도식화 한 것이다.

지금까지 자동차의 취약점에 대해 간단히 알아보았다. 현재까지 우리는 자동차와 IT를 별개의 도메인으로 생각해왔다. 하지만



<자동차 보안 사고 시나리오>

자동차와 IT는 융합되어가고 있으며 그 속에서 보안이라는 이슈 또한 생겨나고 있다. 게다가 기존의 IT 서비스 환경에서의 보안과 달리 자동차에서의 보안은 한 번의 사고가 인명까지 앗아갈 수 있는 매우 큰 영향력을 가지고 있다. 이는 앞으로 자동차보안도 보안전문가가 가져가야 할 영역임을 말해주고 있다.

김윤규
(박사 19기)
임베디드보안 연구실

2010 US DC3 Digital Forensics Challenges 우승

안녕하세요. 저는 디지털포렌식연구센터 석사17기 한지성입니다. 저는 작년 2010년 12월 1일, 기분 좋은 소식을 듣게 되었습니다. 미국 국방부 산하의 사이버범죄센터(DC3: DOD Cyber Crime Center)가 주최한 '2010 Digital Forensics Challenges'에서 저희 디지털포렌식연구센터가 'DFRC'라는 팀 이름으로 우승을 차지하였습니다. 이는 2009년에 개최된 같은 대회에 이어 2년 연속 우승이기에 더욱 특별합니다.

이번 대회는 총 53개 국가의 1,010개 팀이 참가하여 최종적으로 71개 팀만이 보고서를 제출하였는데, 작년에 44개 팀만이 최종 보고서를 제출한 것에 비해 경쟁률이 올랐다는 것을 보여준다고 할 수 있습니다.

시상은 총 11개 부문에 대해 이루어졌습니다. 우선 크게 International 부문과 U.S., 그리고 U.S. Academic으로 나뉩니다. 그리고 각 분류 내에서 미영주권자 여부 및 신분(Non-US, Commercial, Civilian 등)에 따라 세부 시상이 주어졌습니다.

저희 DFRC는 'Non-US Only'에게 주어지는 'Prize IMPACT'를 수상하였습니다. 또한 3,297점으로 가장 높은 점수를 기록하여 'Grand Champion'도 수상하였습니다.

대회 방식은 각각 다른 배점이 된 총 22개의 과제를 정해진 시간 동안 해결하여 보고서를 제출하는 형태로 이루어졌으며, 윈도우즈 레지스트리, 파일 포맷, 패킷 분석, 소프트웨어 역공학, 스테가노그래피, 패스워크 크래킹 등 다양한 주제로 과제가 구성되었는데, 특별히 그 전 대회와 크게 달랐던 점은 도구 개발 과제들이 큰 배점을 가지고 있어 총점에 큰 영향을 준다는 것입니다.

저희 디지털포렌식 연구실에서는 그동안 실제 디지털포렌식 수사에 사용하기 위한 도구 개발을 많이 수행해왔기 때문에, 득점에 있어 가장 유리할 수 있지 않았나 싶습니다.

2010 DC3 Challenge Stats - Winner's Circle

Out of the total 11 awarded prizes by DC3, SANS, IMPACT, EC-Council, JHU/CyberWatch, and the Cyber Security Challenge UK, the winners of the 2010 DC3 Digital Forensics Challenge are:

Award	Team Name	Country	Score
Overall			
• Grand Champion	DFRC	South Korea	3,297
International			
• Prize IMPACT (Non-US Only)	DFRC	South Korea	3,297
• Prize ECC - Commerical	LittleTree	South Korea	1,791
• Prize ECC - Civilian	Williams Twins Forensics	United States	1,470
• Prize UK Challenge (UK Only)	Mine Inc.	United Kingdom	352
U.S.			
Prize DC3 (U.S. Only)	Williams Twin Forensics	United States	1,470
• Prize ECC - U.S. Government	LBPDCCID	United States	409
• Prize ECC - U.S. Military	Batcheej	United States	88
U.S. Academic			
• Prize SANS - U.S. Undergraduate	Team Name	United States	1,129
• Prize SANS - U.S. Graduate	WriteBlockers	United States	988
• Prize SANS - U.S. High School	Crash Override	United States	361
• Prize JHU/CyberWatch - U.S. Community Colleges	PWNsauce	United States	84

<2010 DC3 DFC 우승자 발표 내용 – 밑줄 친 부분이 디지털포렌식연구센터>

많은 도전 과제들 중 쉽게 해결되는 과제들도 있는 반면에, 끝까지 해결하지 못할 수도 있는 과제들도 있습니다. 말 그대로 'Challenge'이기 때문에 해결하기 힘들거나 불가능한 문제가 있을 수 있습니다. 바로 이러한 점이 대회 참가자들을 가장 괴롭힙니다. 과연 시간을 투자해도 될 문제인지 아닌지 판단하는 것 역시 대회의 승패를 가르는 중요한 문제입니다. 저희는 제한된 시간 안에 문제 해결을 위한 연구가 불가능하다고 판단되는 일부 과제는 과감하게 제외하고, 그 이외에는 모두 해결함으로써 고득점을 얻을 수 있었다고 생각합니다.

DC3 디지털 포렌식 챌린지는 디지털 포렌식을 연구하는 사람들에게 대회 이상의 의미가 있습니다. 기존의 다른 대회처럼 주최측이 문제를 만들면 도전자들이 정답을 찾아내는 방식이 아닌, 아직 학술·기술적으로 해결되지 않은 문제들을 통해 디지털 포렌식 분야에서 앞으로 연구해 볼만한 가치가 있는 과제들을 제시한다는 점에서 큰 의미를 찾고 싶습니다. 이번 대회의 경우에는 '가상 환경 데이터 복구' 및 'Shadow Volume Copy 데이터 추출' 등의 제시된 도전 과제를 해결하고 이에 대한 연구 논문이 나와 학술적으로도 큰 성과가 있었습니다.

올해 2011년에도 디지털포렌식연구센터의 선·후배들이 팀을 구성하여 3회 연속 우승을 노립니다. DC3 디지털 포렌식 챌린지는 전 세계의 디지털 포렌식 전문가 및 기업들이 우승을 놓고 다투는 만큼 우리 CIST에도 큰 영광이 되는 세계 무대입니다. CIST 내의 많은 연구원 및 교수님들의 응원이 큰 힘이 됩니다. 많은 관심과 격려 부탁드리겠습니다.

끝으로 2010년 대회의 우승을 위해 많은 도움과 격려를 주신 이상진 교수님을 비롯하여 문제 해결에 도움을 준 연구원들, 그리고 우리 팀원들인 변근덕, 유병영, 이경식 연구원에게 진심을 담아 감사의 마음과 수고의 박수를 전달하고 싶습니다.

디지털포렌식 연구실

2010 DC3 DFC
우승 팀원


변근덕
(박사 11기)


유병영
(석사 17기)


이경식
(석사 17기)


한지성
(석사 17기)

CIST 주요 학회 일정

학회명	장소	일시	학회 설명
NDSS Symposium 2011	San Diego, USA	6~9 February	Annual Network & Distributed System Security Symposium
FSE 2011	Lyngby, Denmark	13~16 February	International Workshop on Fast Software Encryption
CT-RSA 2011	San Francisco, USA	14~18 February	Cryptographers' Track - RSA Conference
FC 2011	St. Lucia	28 February ~ 4 March	Financial Cryptography and Data Security
PKC 2011	Taormina, Italy	6~9 March	International Conference on Practice and Theory in Public Key Cryptography
SAC 2011	Taichung, Taiwan	21~24 March	Symposium On Applied Computing
ASIACCS 2011	Hong Kong	22~24 March	ACM Symposium on Information, Computer and Communications Security
TCC 2011	Providence, USA	28~30 March	Theory of Cryptography Conference
WIAMIS 2011	Delft, Netherlands	13~15 April	International Workshop on Image Analysis for Multimedia Interactive Services
EUROCRYPT 2011	Tallinn, Estonia	15~19 May	-
IH 2011	Prague, Czech Republic	18~20 May	Information Hiding Conference
IEEE Symposium on Security and Privacy 2011	Oakland, USA	22~25 May	-
ADFSL 2011 Conference	Richmond, USA	25~27 May	Conference on Digital Forensics, Security and Law
IEEE/SADFE 2011	Oakland, USA	26 May	International Workshop on Systematic Approaches to Digital Forensic Engineering in conjunction with IEEE Security and Privacy Symposium
ACNS 2011	Nerja, Spain	7~10 June	International Conference on Applied Cryptography and Network Security

주요 학회 일정

CIST

학회명	장소	일시	학회 설명
ACISP 2011	Melbourne, Australia	11~13 July	Australasian Conference on Information Security and Privacy
ICME 2011	Barcelona, Spain	11~15 July	IEEE International Conference on Multimedia and Expo
DFRWS 2011	LA, USA	1~3 August	Digital Forensics Research Conference
USENIX Security 2011	San Francisco, USA	10~12 August	USENIX Security Symposium
CRYPTO 2011	Santa Barbara, USA	14~18 August	International Conference on Cryptology Organized by the International Association for Cryptologic Research
WISA 2011	Jeju Island, Korea	22~24 August	Workshop on Information Security Applications
MobiCom 2011	Las Vegas, USA	19~23 September	International Conference on Mobile Computing and Networking
CHES 2011	Tokyo, Japan	25~28 September	Workshop on Cryptographic Hardware and Embedded Systems
FDTC 2011	Tokyo, Japan	29 September	Workshop on Fault Diagnosis and Tolerance in Cryptography
MM&Sec 2011	Buffalo, USA	29~30 September	ACM Workshop on Multimedia and Security
CCS 2011	Chicago, USA	17~21 October	ACM Conference on Computer and Communications Security
PQCrypto 2011	Taipei, Taiwan	29 November ~ 2 December	International Workshop on Post-Quantum Cryptography
ASIACRYPT 2011	Seoul, Korea	4~8 December	International Conference on the Theory and Application of Cryptology and Information Security
HIS 2011	Melaka, Malaysia	5~8 December	International Conference on Hybrid Intelligent Systems
ESCAR 2011	Germany	미정	Embeded Security in Cars Conference

입사 및 발령 소식

박사 1기	이현숙	2011년 1월	삼성전자 입사
박사 9기	윤택영	2010년 7월	한국전자통신연구원(ETRI) 입사
박사 9기	임선희	2010년 7월	한국전자통신연구원(ETRI) 입사
박사 9기	장남수	2010년 8월	세종사이버대학교 교수 부임
박사 11기	김범한	2010년 9월	삼성전자 입사
박사 11기	이준호	2010년 11월	삼성전자 입사
박사 12기	이제상	2010년 11월	삼성전자 입사
박사 15기	임경수	2010년 하반기	한국전자통신연구원(ETRI) 입사
박사 17기	오영우	2011년 2월	문화체육관광부 기획조정실 기획행정관리담당관 발령
석사 10기	김일중	2010년 하반기	SC제일은행 입사
석사 15기	김연수	2010년 하반기	LG CNS 입사
석사 15기	이진경	2010년 하반기	한국인터넷진흥원(KISA) 입사
석사 15기	최용석	2010년 하반기	경찰청 사이버테러대응센터 입사
석사 16기	He Fei	2010년 하반기	STX조선 입사
석사 17기	정석재	2010년 12월	대우증권 입사
석사 17기	김아름	2011년 1월	한국국방연구원(KIDA) 입사
석사 17기	이경식	2011년 1월	국방과학연구소(ADD) 입사
석사 17기 (금융 1기)	설희경	2011년 1월	롯데정보통신 입사
석사 17기 (금융 1기)	유지영	2011년 1월	이글루 시큐리티 입사
석사 17기 (금융 1기)	유숙현	2011년 1월	소프트포럼 입사
석사 17기 (금융 1기)	김강석	2011년 2월	국민은행 입사
석사 17기 (금융 1기)	김태형	2011년 2월	BC카드 입사
석사 17기 (금융 1기)	엄지원	2011년 2월	BC카드 입사

입사 및 발령 소식

석사 17기 (금융 1기)	이호근	2011년 2월	LG전자 입사
석사 17기 (금융 1기)	정상각	2011년 2월	안철수연구소 입사
석사 17기 (금융 1기)	양대욱	2011년 3월	한화S&C 입사
석사 17기 (금융 1기)	최승현	2011년 3월	롯데정보통신 입사

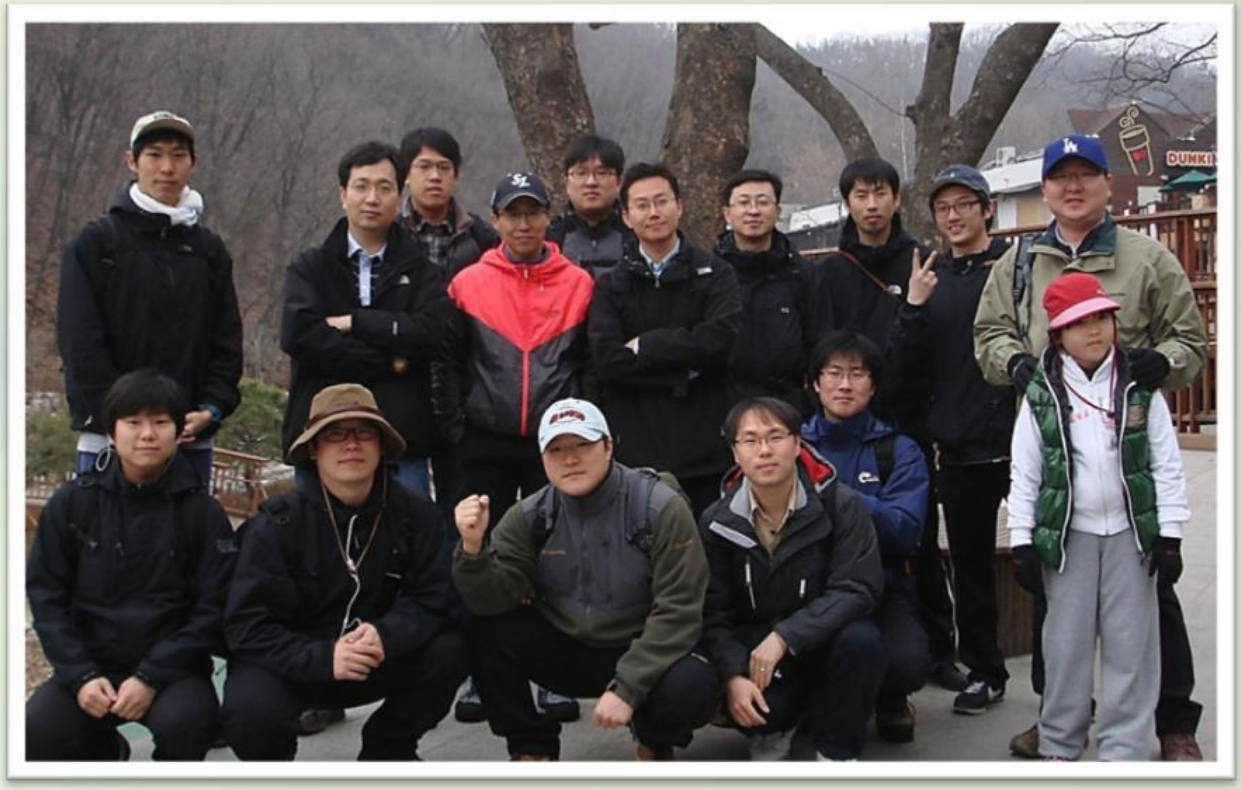
결혼 및 출산 소식

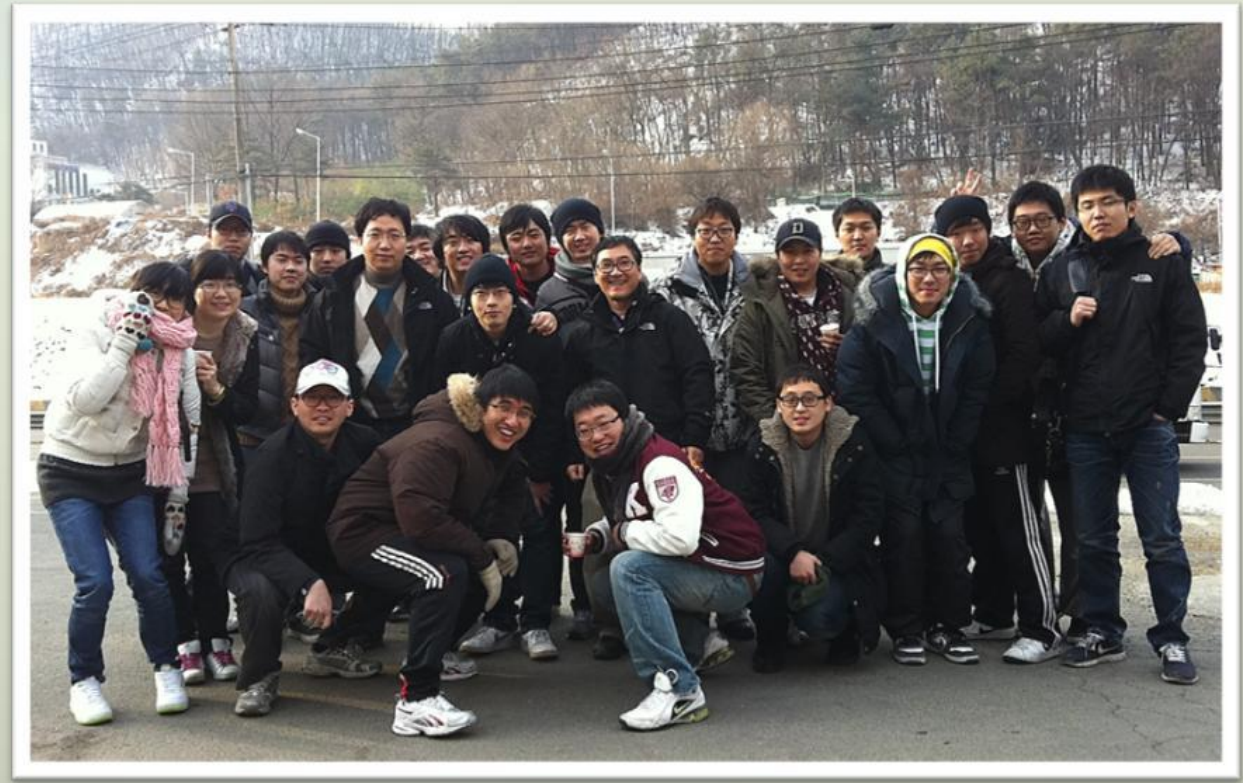
박사 3기	손태식	2011년 1월 결혼
박사 5기	김 역	2010년 12월 결혼
박사 7기	최은영	2010년 10월 결혼
박사 9기	임선희	2010년 12월 결혼
박사 11기	이준호	2011년 3월 결혼(예정)
박사 11기	정기태	2010년 9월 득녀
박사 12기	이제상	2010년 10월 결혼
박사 14기	이진태	2010년 10월 득녀 (저작권위원회 재직)
박사 14기	이진태	2010년 12월 결혼 (한국인터넷진흥원 재직)
박사 15기	임경수	2010년 하반기 득녀
박사 16기	김기탁	2010년 11월 결혼
석사 2기	김종현	2011년 2월 결혼
석사 4기	김구일	2010년 9월 결혼
석사 9기	김보만	2010년 하반기 결혼
석사 12기	권혁돈♡박은경	2010년 12월 결혼
석사 15기	이동찬♡박한나	2010년 10월 결혼
석사 16기	최중영	2011년 2월 득녀
석사 17기 (금융 1기)	김강석	2011년 2월 결혼

공개키암호 연구실

금융보안 연구실

대칭키암호 연구실





디지털포렌식 연구실

멀티미디어보안 연구실

무선모바일보안 연구실

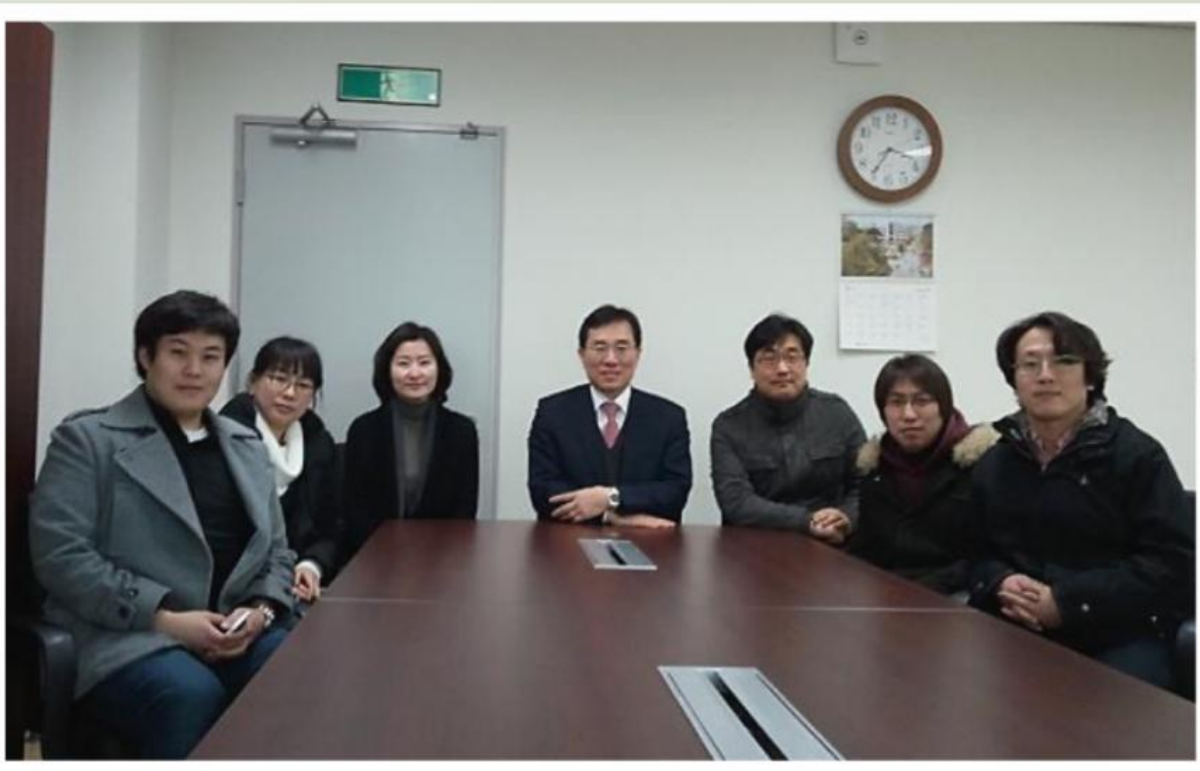
시스템네트워크보안 연구실

암호프로토콜 연구실

양자암호 연구실

온라인컨텐츠보안 연구실

임베디드보안 연구실



정보보호정책 연구실

프라이버시향상기술 연구실

Korea University

Center for Information Security Technologies

CIST Letter
No. 18 February 2011

국번:3290

정보보호대학원 학사지원부	미래융합기술관 615호	4251~3
정보보호대학원 원장실	미래융합기술관 614호	4044
정보보호연구원 사무실	미래융합기술관 613호	4256
학사지원부/CIST (FAX)	02) 928-9109	

임종인 교수님 연구실	미래융합기술관 611호	4891
이동훈 교수님 연구실	미래융합기술관 612호	4892
이상진 교수님 연구실	미래융합기술관 609호	4893
홍석희 교수님 연구실	미래융합기술관 203B호	4894
김형중 교수님 연구실	미래융합기술관 610호	4895
정익래 교수님 연구실	창의관 716호	4896
김휘강 교수님 연구실	창의관 811B호	4898
윤석구 교수님 연구실	창의관 809C호	4770
문종섭 교수님 연구실	(녹지)생명공학관 231A호	4750
양형진 교수님 연구실	(녹지)생명공학관 233호	3972

공개키암호 연구실	(구)연수관 105호	4756
금융보안 연구실	미래융합기술관 203A호, 과학도서관 405호	3881/4999
대칭키암호 연구실	(구)연수관 104호	4763
디지털포렌식 연구실	(녹지)생명공학관 136호, 학군단 4호	4276/4738
멀티미디어보안 연구실	(구)연수관 102호, 103호	4764/4998
무선모바일보안 연구실	(녹지)생명공학관 142B호	-
보안하드웨어 연구실	(구)연수관 101호	4763
시스템네트워크보안 연구실	(녹지)생명공학관 135호	4749/3998(F)
암호프로토콜 연구실	(녹지)생명공학관 138호	4259
양자암호 연구실	(녹지)생명공학관 231A호	4750
온라인컨텐츠보안 연구실	창의관 811C호, (녹지)생명공학관 142A호	3521
임베디드보안 연구실	미래융합기술관 607호	4997
정보보호정책 연구실	미래융합기술관 606호	4996
정보은닉 연구실	학군단 3호	4293
프라이버시향상기술 연구실	(녹지)생명공학관 140호	4258

One Stop Center	4092
자연계 총부무 (우편물 관리)	4026
주차 관리	4362

http://www.korea.ac.kr http://cist.korea.ac.kr

발행인 : 임종인
편집인 : 정익래

고려대학교
KOREA UNIVERSITY

Korea University 정보보호연구원
CIST Center for Information Security Technologies