등록 안내

Ⅰ. 사전등록

1. 등록 기간 : ~ 4월 23일(일) 까지

2. 등록 방법 : 학회 홈페이지(itfe.or.kr) 행사페이지를 통해 온라인 신청 후 등록비 결제

3. 결제 방법 및 증빙서류 발급 안내

※ 계좌이체 : 신한은행 100-025-389176 (예금주 : 한국정보통신설비학회)
☞ 사업자등록증 업로드 필수. 등록시 기재하신 이메일 주소로 전자계산서가 발급됩니다. (계좌이체 및 현금결제 시에만 발급 가능)

※ 카드결제 : 학회 홈페이지에서 온라인 결제(비회원 포함)
☞ 온라인결제 : 홈페이지 > 마이페이지 > 나의 결제내역에서 영수증 출력 가능 (비로그인 시 정보 확인이 어려워 출력 불가능하니 꼭 로그인 후 등록하여 주세요.)

※ 참석확인증 : 행사가 끝난 후 신청자 메일로 송부.

Ⅱ. 등록비

구분	사전등록	현장등록
회원	150,000원	180,000원
일반	200,000원	230,000원
학생(학부생, 대학원생)	100,000원	130,000원

※ 비회원은 일반으로 등록하셔야 하며, 이후 행사에 2023년도 회원자격을 부여합니다.

행사장 안내

aT센터 4층 창조룸 Ⅱ

서울특별시 서초구 강남대로 27, (양재동 232 aT센터)
(지하철 신분당선 양재시민의숲역 하차, 4번 출구 방향)
Tel. 02-6300-1114

※ **주차안내**
유료주차만 가능합니다.
주차비 : 1시간 4,200원, 1일 주차(24시간) 36,000원

< 후원 안내 >
① Gold(후원 500만원) : 자료집 광고게재 및 3인 학회등록비 면제
② Silver(후원 300만원) : 자료집 광고게재 및 2인 학회등록비 면제
③ Bronze(후원 150만원) : 자료집 광고게재 및 1인 학회 등록비 면제

◎ 문의처(한국정보통신설비학회 사무국)
주소 : (08302) 서울시 구로구 가마산로26길 5 로제리움2차 908호
전화 : 02-851-4001
이메일 : itfe@itfe.or.kr
홈페이지 : www.itfe.or.kr

초대인사말

정보통신분야에 종사하시는 귀하 및 귀사의 무궁한 발전을 기원합니다.
한국정보통신설비학회에서 2023년도 춘계세미나를 개최합니다.
올해는 우리사회의 다양한 분야에 걸쳐 이슈가 되고 있는 '융합보안'이라는 주제로 이 분야 최고의 전문가와 정책 관계자들을 모시고 여러분들을 초대합니다.

이번 춘계세미나에서는 오전세션에서는 산업제어시스템분야의 보안기술에 대한 소개, 디지털헬스케어 보안모델, 실제 적용되고 있는 블록체인기반 저작권 보호기술을 다루어보고, 오후세션에서는 캠퍼스네트워크 보안, 네트워크및 보안가상화, 하드웨어 공급망 보안등 다양한 융합분야에서 적용가능한 보안기술을 소개하고, 사례중심으로 토의할 계획을 가지고 있습니다.

본 춘계세미나를 통해 융합보안 보안 위협, 모델, 그리고 사례에 대한 최근 국내/외의 다양한 사례와 중요 이슈들을 토론하는 장으로 마련하였사오니 정보통신분야에 종사하시는 많은 분들의 참여와 관심을 부탁드립니다.

2023년 4월

www.itfe.or.kr
ISSN 2384-3284

한국정보통신설비학회
2023 정보통신설비 춘계세미나
"네트워크 융합 보안 세미나"

2023년 4월 27일(목) 13:00~18:00

aT센터 4층 창조룸 Ⅱ

주최 (사)한국정보통신설비학회

주관 (사)한국정보통신설비학회, 한국정보보호학회 융합보안연구회

후원 롯데정보통신, 쌍용정보통신, 올포랜드, 파이오링크, 네이버시스템, 대영유비텍, 대보정보통신

프로그램위원장 김기형 교수(아주대학교)

사단법인 한국정보통신설비학회
Korea Institute of Information & Telecommunication Facilities Engineering

2023 정보통신설비 춘계세미나 프로그램

시 간	강 연 제 목	연사(소속)
Session 1.		
13:00~13:40	IEC 624443 제어시스템 보안 표준과 인증	한근희 교수 (고려대학교)
13:40~14:20	저작권보호를 위한 블록체인기반 파일관리	강민수 부장 (시큐에버)
14:20~15:00	디지털헬스케어 보안모델 및 보안실증	백종현 연구위원 (한국인터넷진흥원)
Break Time (15:00 ~ 15:20)		
Session 2.		
15:20~16:00	캠퍼스 네트워크 보안과 관리의 중요성	석상찬 차장 (파이오링크)
16:00~16:40	네트워크 및 보안 가상화	최동영 이사 (진인프라)
16:40~17:20	하드웨어 공급망 위협과 대응방안	이중희 교수 (고려대학교)
기념식		
17:20~17:30	환영사	최 경 강원대 교수 한국정보통신설비학회장
17:30~18:00	경품추첨 및 단체사진 촬영	
폐 회(18:00)		

Session 1.

시간	내 용
13:00 ~ 13:40	 **한근희 교수(고려대학교 정보보호대학원)** • IEC TC 65 WG 10 산업제어시스템 보안 워킹그룹 전문위원 • 행정안전부, 국가정보자원관리원 사이버안전과장 • 드림시큐리티, 안철수연구소 부사장 • LG U + 인터넷기술팀장 • 한국전자통신연구원 **IEC 624443 제어시스템 보안 표준과 인증**

시간	내 용
13:40 ~ 14:20	 **강민수 부장(시큐에버)** • 15년 IT 영업 경력 • 다수의 네트워크, 인프라환경, 정보보안솔루션 통합 SI사업 진행 • 2015~2016 00방호부대 통제실 인프라 구축 사업 총괄 진행 • 2016~2017 00자산신탁 인프라 고도화 사업 총괄 진행 • 2018~2019 00POS 신규 네트워크 패쇄망 구축 사업 총괄 진행 • 2020~2021 환경부 소속기관 망분리 3단계 사업 총괄 진행 • 2020~2021 식품안전정보원 위탁판매시스템 인프라구축 사업 컨소시엄 • 블록체인 기반 파일관리 프로젝트 수행 중 **저작권보호를 위한 블록체인기반 파일관리** 점점 다양해지는 악성코드 및 해킹, 랜섬웨어에 대응하기 힘들어지는 상황에 대한 국가적 관심이 대두되고 있는 시기에 미래지향적 기술인 블록체인 기술을 이용하여 파일을 관리하는 기술이 접목된다면 파일에 대한 신뢰를 상승시킬 수 있고, 모든 파일 정확성에 대한 구성원 간의 합의를 통해 검증된 트랙잭션을 영구적으로 기록되어 변경시킬 수 없으므로 보안이 더욱 강화됩니다. 또한, 분산원장 기술을 이용하여 시간 낭비를 최소화 할 수 있습니다. 이와 더불어 보안전자지갑을 통한 저작권자의 저작권보호를 위한 매개체가 될 수 있습니다. 이러한 기술적 요소들을 바탕으로 저작권보호와 파일에 대한 강화된 보안 기술을 공유하며 소개하고자 합니다. 저작권보호, 보안강화, 파일관리를 균형적으로 다룰 수 있는 방안과 활성화를 위한 앞으로의 방향, 나아가 블록체인 기반 플랫폼 성장에 의견을 나누고자 합니다.

시간	내 용
14:20 ~ 15:00	 **백종현 연구위원(한국인터넷진흥원)** • 2015~2016년 KISA 융합보안연구팀장 • 2017~2018년 KISA 차세대인증보안팀장 • 2019~2023년 KISA 융합보안정책팀장 • 2017~2019년 TTA TC5 TG501 의장 • 2009~현재 ITU-T SG17 IoT 보안 분과 의장 **디지털헬스케어 보안모델 및 보안실증** 2019년 4월 세계 최초 5G 네트워크 상용화를 기점으로 디지털헬스케어를 포함한 다양한 융합산업이 급속도로 확산되기 시작하였으며, 코로나 19 바이러스의 확산으로 비대면 진료의 수요가 급증하면서 안전한 디지털헬스케어 서비스 제공을 위한 보안의 수요도 증가하기 시작했다. 정부에서도 디지털헬스케어 보안에 대한 중요성을 인식하고 '20년부터 디지털헬스케어 디바이스 및 서비스의 보안강화를 위한 사업을 지속적으로 추진하고 있다. 본 발표에서는 디지털헬스케어 디바이스 및 서비스에 대한 보안 위협을 분석하고 해당 위협에 대응하기 위한 보안 기술, 제품 및 솔루션 등을 제시하는 디지털헬스케어 보안 모델에 대해 설명하고, 해당 보안모델을 실제 디지털헬스케어 서비스에 적용하여 실증한 결과에 대해서도 소개한다.

Session 2.

시간	내 용
15:20 ~ 16:00	 **석상찬 차장(파이오링크)** • 현재 파이오링크 TiFRONT사업실 교육/보건 담당 영업 • 한드림넷 기술지원 SE **캠퍼스 네트워크 보안과 관리의 중요성** - 캠퍼스 네트워크는 인가/비인가 사용자가 혼합된 네트워크 - 네트워크 관리자는 불특정 다수가 접속되는 네트워크 환경 관리에 많은 어려움이 있음 - 불특정 다수가 접속되는 환경을 간편하고 효율적으로 관리할 수 있는 방안 제시

시간	내 용
16:00 ~ 16:40	 **최동영 이사(진인프라 기술지원그룹 그룹장)** • 1999~2006 : ㈜컴네트플러스 삼성반도체(기흥) 사업장 Network 구축 및 운영 • 2008~2015 : 진인프라(구 넷케이티아이) 네트워크 필드 엔지니어 • 2015~현재 : 진인프라(구 넷케이티아이) 기술지원그룹 네트워크기술부/정보보안기술부 총괄담당 **네트워크 및 보안 가상화** 클라우드가 대중화 되면서 완성도 높은 다양한 제품을 바탕으로 서버와 스토리지의 가상화는 성과를 내고 있습니다. 하지만 아직까지 네트워크/보안에 대한 가상화는 대형고객사를 제외하고 대중화가 되지 못하고 있습니다. 네트워크 분야에서 가장 화두가 되고 있는 SDN(Software Defined Networks)에 대해서 간략하게 소개하고 가상화에서 요구되는 기능과 시장동향을 설명하고자 합니다. 보안 가상화는 다양한 보안 솔루션증 가장 기본이라 할 수 있는 방화벽의 가상화 구현방식에 대해서 설명드리겠습니다.

시간	내 용
16:40 ~ 17:20	 **이중희 교수(고려대학교)** • 2019~현재 고려대학교 정보보호대학원 조/부교수 • 2014~2019 University of Texas at San Antonio 조교수 • 2003~2008 삼성전자 연구원 **하드웨어 공급망 위협과 대응방안** 국제 분업이 활발한 하드웨어(반도체) 산업은 하나의 제품을 생산하기 위해 여러 나라에 흩어진 여러 기업이 참여하게 된다. 참여 기업들이 동일한 국가 또는 유사한 제도권 아래 운영되고 있으면 상호 신뢰를 바탕으로 협업을 할 수 있지만, 제도가 다르거나 적대적인 관계에 있는 국가의 기업과는 신뢰를 바탕으로한 협업이 어렵다. 신뢰를 바탕으로 협업을 하더라도 부정행위를 기술적으로 탐지할 수 있는 방법은 여전히 필요하다. 본 발표에서는 하드웨어 공급망에서 발생할 수 있는 부정행위와 이에 대한 기술적 대응방안을 설명한다.