고려대 블록체인연구소를 가다

보안 취약점, 사전에 분석·방지한다

블록체인 기술은 4차 산업혁명 기술 중 하나의 옵션이 아닌, 다양한 산업 분야에 걸쳐 기반이 되는 플랫폼의 역할을 할 것으로 전망되고 있다. 그리고 금융, 의료, 물류, 공공서비스 등 분야를 점차 넓혀가며 사회시스템 전반을 변화시키고 있다. 이러한 시대적 흐름에 발맞춰 블록체인 기술에 대한 현황을 명확하게 인식하고 비즈니스적 활용을 고취하고자 설립된 고려대학교 블록체인연구소는 현재 6개 연구센터를 중심으로 블록체인 기반기술, 법률·제도, 비즈니스 모델, 의료·물류 정보 등을 연구 중이다. 고려대 블록체인연구소는 체계적이고 긴밀한 산학협력 프로그램(실버, 골드, 플래티늄)을 운영하며, 산학협력 간담회를 통해 산업현장의 니즈를 파악하고, 연구 개발을 통해 기술이전과 컨설팅을 제공하는 등 블록체인 관련 기술의 핵심 개발뿐 아니라 실질적인 활용을 위한 노력을 아끼지 않고 있다. 이에 〈공학저널〉은 매호 고려대 블록체인연구소에서 블록체인 분야 연구를 진행 중인 연구소를 탐방하고 있다. 9월호에서는 블록체인 기술을 활용한 보안 기술을 연구 중인 고려대학교 컴퓨터학과 이희조 교수(**사진**)를 만났다.

〈편집자 주〉

INTERVIEW

고려대학교 컴퓨터학과 **이희조** 교수

블록체인 보안 분야 어떠한 연구를 진행 중인지

해킹과 악성코드 등 보안사고의 90%는 소프트웨어 내 존재하는 보안 취약점을 이용한 공격이라는 US-CERT 보고가 있듯 보안 취약점을 사전에 탐지해 제거하는 것은 사고 예방에 매우 중요한 부분입니다. 블록체인 또한 소프트웨어로 구동되기 때문에 마찬가지로 보안 취약점이 없어야 예정된 기능이 정상적으로 동작할 수 있게 됩니다. 저희 연구그룹은 보안 취약점 자동분석 기술에 대한 연구를 진행해 오고 있으며, 2019년부터는 과기정통부 산하 정보통신기획평가원(IITP)의 지원으로 '블록체인 플랫폼 보안취약점 자동분석 기술' 에 관한 연구를 진행하고 있습니다. 블록체인 플랫폼 보안에 관한 세계 최고 수준의 기술 개발에 도전하는 '혁신도약형' 사업으로 지정돼 수행 중에 있습니다. 본 연구는 블록체인 플랫폼을 애플리케이션, 시스템, 네트워크 3개 분야로 구분해 총 9개의 기술을 개발하고, 이를 보안취약점 자동분석 서비스 'IoTcube'에 공개하는 방식입니다. 이를 통해 블록체인 개발자 및 스타트업 등 누구나 인터넷에서 손쉽게 전문적인 보안 취약점 분석을 할 수 있도록 공개서비스를 제공하고 있습니다.

블록체인 오픈소스로 인한 코드 재사용이 발생시키는 보안 문제점은 무엇인지

비트코인 소스코드가 라이트코인, 대시코인

등의 다른 블록체인 프로젝트에서 많은 부분 재사용되고 있듯, 블록체인 소프트웨어들 간의 코드 재사용 비율이 높다는 점은 보안성 관점에서 주목할 만합니다.

블록체인 소프트웨어의 내부 구조를 보면, 이전에 개발된 다른 블록체인 소프트웨어를 재사용하는 부분 외에도, DB, 암호화, 파서, 압축등을 위해 다양한 오픈소스 소프트웨어를 포함하고 있습니다. 이런 현상이 발생하는 데에는, 주된 블록체인 프로젝트를 오픈소스로 개발하고 또한 오픈소스로 공개하는 등 상호 재사용비율을 높이는 것이 원인이 되고 있습니다. 오픈소스로 공개하고 코드를 재사용하는 것은 현재의 소프트웨어 개발 트랜드로 그 자체에는 문제가 없으나, 보안을 고려한 소프트웨어 개발, 코드 관리를 해야 하는데 간과될 경우들이 문제가 되고 있습니다.

이러한 위협을 예방하기 위해 우리 연구팀은 시스템 레벨에서의 '블록체인 프로젝트 내의 취약 코드 탐지'와 '블록체인 프로젝트 내의 타사 오픈소스 구성요소 탐지'의 크게 두 가지 보안성 검증 기술을 연구하고 있습니다. 또한 블록체인 프로젝트가 타사 오픈소스 코드 베이스의 일부만 수정해서 재사용하더라도 정확하게 식별해내는 CENTRIS 기술을 연구 중에 있습니다. 언급한 두 가지 기술을 도입한다면 실제로 블록체인 프로젝트 코드 베이스에 포함된 취약 코드들을 탐지·패치 할 수 있고, 취약점을 내포하고 있거나 라이선스 충돌 가능성이 존재하는 타사 오픈소스 구성 요소의 식별 후 바로 패치 업데이트와 같은 적절한 조치를 취할 수 있어, 블록체인 서비스의 보안성 검증을 지원할 수 있을 것으로 기대합니다.

이와 관련 최근 성과 또는 이슈가 있다면

블록체인 기술 중 스마트 컨트랙트는 한 번 설치되면 수정하기 어렵고, 주로 금전과 관계된 민감도 높은 데이터를 취급하기에, 실행에 문제가 발생하면 큰 손실로 이어질 수 있다는 특성이 있습니다. 따라서 스마트 컨트랙트는 일반적인 프로그램보다도 보안성과 안전성이 강조돼야 하는데, 현존하는 안전성 검증 도구는 취약점 검출의 정확도와 성공율 부분에서 널리 활용되기에는 부족합니다. 우리 연구팀은 기존 도구 대비 높은 정확도를 가진 검증 자동화 기술인 'VeriSmart'를 개발해 최근 최고 권위를 인정받는 IEEE S&P 2020에 발표했습니다. 알고리즘은 소프트웨어로 구현돼 오픈소스로도 공개됐으며, 보안취약점 자동분석 플랫폼인 'IoTcube'에 탐재돼 스마트계약 코드를 넣으면 취약점 여부를 바로 확인해 보는데 즉시 사용해 볼 수 있도록 공개하고 있습니다.

포스트코로나의 장기적 영향에 따라 비대면 기술이 조명되는 가운데 블록체인 기술은 어떤 영향을 끼칠 것이라 예상하는지

최근 DID 기술의 다양한 적용시도를 통해 알 수 있듯이, 비대면이 일상화되는 새로운 세상에서 블록체인 기술은 과정의 투명성을 높이고, 중앙 집중으로 인한 비효율을 제거해 궁극적으로 우리가 보다 윤택한 삶을 누리는데 일조하리라 생각합니다. 다만 블록체인 역시 소프트웨어로 개발되는 기술이므로, 소프트웨어 보안을 더욱 철저히 대비해야 합니다. 소프트웨어 보안은 취약점이 없는 소프트웨어를 개발하는 것에서 시작할 수 있으며, 스마트 컨트랙트 뿐만 아니라 어플리케이션, 시스템, 네트워크 등 블록체인 서비스를 구성하는 전 단계의 소프트웨어에서 보안관리를 기반으로 합니다. 이를 위해서는 개발단계의 보안 내재화가 필요합니다. 여기에는 설계단계의 보안 아키텍쳐 구성, 개발 시작전 오픈소스 관리체계 점검, 시큐어 코딩 규칙 준수 외에 정적분석을 통한 CVE 취약점 점검 및 퍼징 기술 등을 활용한 동적분석 등이 포함될 수 있으며, 일부 단계에서는 보안 테스팅이나 검수를 위해 오픈소스나 상용 도구들을 활용하여 쉽게 실행할 수 있습니다.

향후 계획이 있다면

블록체인은 최신 기술의 발전과 시장에 따라 급변하고 있습니다. 자동 취약점 분석기술을 기반으로 하는 블록체인 플랫폼 보안 기술 역시 Go, Python 등 언어 확장과 하이퍼레저를 포함한 다양한 시스템과 소프트웨어에 적용 가능하도록 유연성을 넓히고자 합니다. 또한 우리 연구팀의 연구를 통해 개발된 기술이 실제 산업현장에서도 잘 활용돼 보다 안전한 블록체인 서비스 환경을 구축하는데 일조하는 것이 보안기술을 연구하는 연구자의 역할이라고 생각합니다. IoTcube를 통한 오픈 서비스를 통해 사용자에 검증된 기술을 국내외 학술연구망, 해외 오픈 프로젝트, 공공선도사업 등 다양한 블록체인 서비스에 적용하는데 적극 협력하도록 하겠습니다.

김하늬 기자 hani@