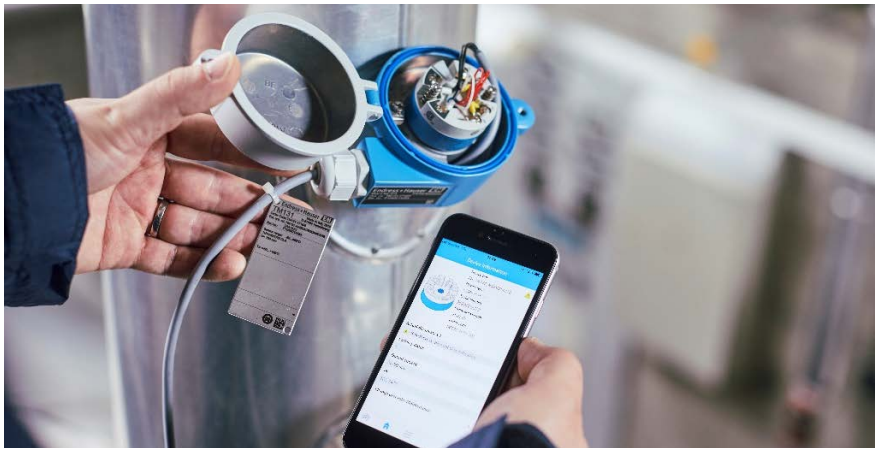
엔드레스하우저가 개발한 안전한 블루투스 연결 솔루션

프로세스 산업을 위한 안전한 저전력 기술

CPace 프로토콜을 사용하는 안전한 엔드레스하우저 블루투스 저전력 연결 솔루션의 장점:

- 블루투스 계기 사용 시 CPace 프로토콜을 통해 플랜트의 가용성, 시간 효율성 및 보안성 향상
- PAKE 프로토콜을 사용하여 암호 길이와 복잡한 PKI(공개 키 인프라) 사용 가능 여부와 상관없이 산업 플랜트에서 안전하게 암호 사용
- 단일 프로토콜만 검증하기 때문에 계기 유형 및 전력 사양에 상관없이 사용 가능
- 비대칭 암호화 방식을 사용하여 피싱 및 중간자 공격(man-in-the-middle attack) 방지
- 일반적인 다른 솔루션보다 강력한 보안 실현(예: 미리 공유한 키) – IETF에서 엔드레스하우저 솔루션 권장



블루투스 보안 문제의 해결 프로세스 산업의 전 분야에서 현장 계기에 대한 편리한 무선 액세스에 관심을 갖는 오퍼레이터가 점점 많아지고 있습니다. 그러나 계기에 원격으로 액세스하는 경우가 늘어나면서 심각한 보안 위험도 함께 증가하고 있습니다.

또한 산업용 사물 인터넷(IoT)의 발전으로 프로세스 제어 구성요소들이 더욱 밀접하게 상호 연결되고 있습니다. 이러한 현장 계기에는 내부 또는 외부 인력에 의한 정기적인 설치, 모니터링 또는 정비가 필요합니다. 오늘날 안전한 암호 기반 사용자 인증은 특히 블루투스 같은 무선 인터페이스가 탑재된 계기를 사용하고 있지만 플랜트 오퍼레이터가 복잡한 PKI(공개 키 인프라)를 관리할 자체 보안 부서를 아직 만들지 못한 경우에 중요한 역할을 수행하고 있습니다.

산업 환경에서는 소비자 도메인보다 훨씬 더 높은 보호 수준이 필요하고 블루투스의 내장 메커니즘이 이를 고려하기 때문에 엔드레스하우저는 CPace라는 솔루션을 핵심 구성요소로 사용하여 암호를 보호하는 추가적인 보안 계층을 개발했습니다. CPace는 블루투스 페어링 단계에서 일어나는 악명 높은 공격들을 방지합니다.

암호 보호는 매우 어렵기 때문에 엔드레스하우저의 CPace는 독일 ID 카드에 사용되는 PACE 방식에서 파생된 강력한 PAKE 기술을 이용합니다.

사용자에게 편리한 암호 길이로 보안 구축 기존의 보안 솔루션에는 인증서와 PKI 또는 긴 암호 키(예: “X4RTQ 4KPKM PTWXS 3BP4Z C66D5 RRJ26”)가 필수입니다. CPace는 사용자가 상대적으로 짧은 암호를 지정한 경우에도 오프라인 암호 공격을 방지하기 때문에 계기에 대한 블루투스 연결이 항상 안전합니다. PAKE 프로토콜에 사용된 비대칭 암호화 덕분에 보안 계층은 암호화 길이와 무관하게 구축되었습니다.

뿐만 아니라, 현장 계기의 제한된 리소스 때문에 SRP나 PACE 같은 프로

Endress+Hauser

People for Process Automation

토콜을 사용해 암호를 검증할 경우 1분 이상의 로그인 지연이 발생할 수 있지만, 엔드레스하우저의 CPace는 보안 등급을 낮추지 않고도 암호 검증 중의 최대 로그인 지연을 2초 이하로 유지합니다.

이제 복잡한 보안 인프라와 길고 어려운 액세스 암호 없이도 보안을 실현할 수 있기 때문에 실제 보안과 사용 편의성이 향상됩니다.

인터넷 표준 기구도 인정한 CPace

2018년, 인터넷 표준 기구 IETF는 암호 기반 로그인을 개선한 보안 솔루션의 필요성을 인식했고, 2019년 IETF의 암호화 전문가 그룹 CFRG에서 보안 분석 및 선정 프로세스를 실시했는데, 여러 후보 프로토콜을 대상으로 종합적인 보안 분석을 수행한 결과 엔드레스하우저의 솔루션 CPace를 최종적으로 선정했습니다("인터넷 프로토콜에서 사용 권장").

뿐만 아니라, 2016년 독일 뮌헨에 있는 프라운호퍼 AISEC 연구소는 엔드레스하우저 블루투스 보안 확장 기능의 보호 수준을 "높음"으로 분류했습니다.

다음과 같은 해커도 공격에 성공하지 못합니다.

- 몇 주에 걸쳐 공격을 시도하는 해커
- 전자, 암호화 및 부채널 공격에 대한 전문 지식을 보유한 해커
- 전체 시스템에 대한 내부 정보를 보유한 해커
- 모든 무선 인터페이스에 완전한 액세스 권한을 가진 해커

블루투스 저전력 솔루션 및 CPace를 통한 안전한 연결

현재 블루투스 연결 기능이 있는 모든 엔드레스하우저 계기가 지원됩니다.

PAKE와 IETF란 무엇인가요?

PAKE(Password Authenticated Key Exchange, 암호 인증 키 교환)는 해커가 해킹 툴을 사용해 암호에 대한 오프라인 공격을 감행하지 못하도록 암호를 통한 액세스 인증을 검증하는 프로토콜 그룹입니다(예: 블루투스 인터페이스가 있는 현장 계기).

IETF(Internet Engineering Task Force, 인터넷 엔지니어링 태스크 포스)와 IRTF(Internet Research Task Force, 인터넷 리서치 태스크 포스)는 인터넷 백본, LAN 인프라 그리고 인터넷 브라우저 같은 응용 프로그램에서 사용되는 TCP/IP, TLS, IPSEC 등의 프로토콜을 비롯하여 인터넷에 대한 표준을 관리하는 기관입니다. IETF 내에서 표준 내 암호화 보안 분석은 IRTF 산하 CFRG(Crypto Forum Research Group, 암호화 포럼 리서치 그룹)의 소관입니다.

지속 가능한 임업으로부터 제공받은 종이로 친환경적 생산 및 인쇄

www.kr.endress.com

IN01194S/46/KO/01.21

Endress+Hauser
People for Process Automation