Standards bei Internet-Sicherheit

Categories : Messtechnik

Date : 24. November 2020

Die Kryptographie-Arbeitsgruppe der Internet Standardisierungs-Organisation IETF (Internet Engineering Task Force) hat das von Endress+Hauser entwickelte CPace-Protokoll als empfohlenes Verfahren für den Einsatz in Internet-Standards ausgewählt. Das Protokoll CPace ging nach umfangreichen Sicherheitsanalysen als Sieger aus einem Wettbewerb mit Einreichungen von Mitarbeitenden namhafter Firmen hervor.
Der sichere Zugriff auf Feldgeräte hat bei Betreibern in allen Zweigen der Prozessindustrie höchste Priorität. Moderne Anlagen enthalten Hunderte bis Tausende Mess-, Steuer- und Regelgeräte, auf die immer häufiger aus der Ferne zugegriffen werden muss. Zudem müssen Feldgeräte regelmäßig installiert, kontrolliert oder gewartet werden. Die sichere passwortbasierte Authentifizierung der Nutzer, vor allem bei Geräten mit digitalen Datenschnittstellen, spielt dabei heutzutage eine besondere Rolle.

Sicherheit trotz benutzerfreundlicher Passwortlängen

Für den Einsatz von Bluetooth-Kommunikation im Industrieumfeld identifizierten die Security-Experten von Endress+Hauser den Bedarf für einen zusätzlichen Schutz und entwarfen hierzu eine Lösung namens CPace. CPace gehört zur Klasse der PAKE-Verfahren (Password-authenticated key exchange). Sie kommt unter anderem auch im deutschen Personalausweis zum Einsatz, um das kryptographische Sicherheitsniveau weitgehend von der Passwortlänge zu entkoppeln. CPace bietet dabei den Vorteil, dass die Leistung selbst kleinster Feldgeräte ausreicht, um die Geräte und damit die Industrieanlagen bestmöglich vor Cyber-Angriffen zu schützen. Gleichzeitig stößt die Lösung auf hohe Akzeptanz bei Anwendern, da das Sicherheitsniveau auch ohne lange Passwörter erreicht wird.
„Wir haben nach einer eigenen Lösung gesucht, um einen sicheren Verbindungsaufbau mit den Geräten zu schaffen, weil bisherige Verfahren, mit adäquatem Security Niveau für Industrieanwendungen aufgrund der beschränkten Ressourcen ausschieden. Eine Passwort-Überprüfung hätte eine Login-Verzögerung von zwei Minuten und mehr bedeutet“, sagt Endress+Hauser-Projektleiter Dr. Björn Haase.

CPace macht es Angreifern schwer

Die Sicherheit der PAKE-basierten Lösung mit Bluetooth-Technologie von Endress+Hauser, wurde bereits 2016 durch ein Review des Fraunhofer-Instituts für Angewandte und Integrierte Sicherheit (AISEC) bestätigt. Das Schutzniveau des Endress+Hauser-Sicherheitslayers, dessen Kernkomponente jetzt für den Einsatz im Internet-Umfeld ausgewählt ist, wurde als „hoch“ eingestuft.

PAKE

Password-authenticated key exchange bezeichnet eine Gruppe von Protokollen, die ein Passwort zur Zugangsberechtigung verifizieren, ohne dabei einem Angreifer mit Hacker-Werkzeugen Offline-Angriffe auf das Passwort zu ermöglichen.

PACE

Das PAKE-Protokoll PACE (Password-authenticated connection establishment) ist ein passwortbasiertes Authentisierungs- und Schlüsseleinigungsverfahren, welches vom deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) für den Einsatz im neuen Personalausweis entwickelt wurde.

CPace

Composable password-authenticated connection establishment ist die Weiterentwicklung des PACE-Verfahrens des BSI durch Endress+Hauser und passt dieses auf die begrenzten Rechenressourcen von kleinen Feldgeräten an.

IETF

Die Internet Engineering Task Force (Internettechnik-Arbeitsgruppe) ist eine offene, internationale Freiwilligenvereinigung von Netzwerktechnikern, Herstellern, Netzbetreibern, Forschern und Anwendern, welche die Standardisierung des Internets organisiert und sich mit der technischen Weiterentwicklung des Internets befasst. Die Mitglieder erstellen technische Dokumente, die Nutzung, Weiterentwicklung und Verwaltung des Internets beeinflussen. Insbesondere kümmert sich die IETF um die Standardisierung der im Internet eingesetzten Kommunikationsprotokolle und Kryptographieverfahren