Einführung in die Kryptographie: Methoden und praktische Anwendungen

Praxisnahe Übersicht: Methoden und Anwendungen der Kryptographie

Beginn:
13.11.2025 - 09:00 Uhr

Ende:
14.11.2025 - 16:30 Uhr

Dauer:
2,0 Tage

weitere Termine

Ostfildern

Veranstaltungsnr.: **36257.00.001**

Leitung

Dr. Julian Liedtke
TRUMPF SE + Co. KG

Alle Referent:innen

Präsenz
EUR 1.310,00
(MwSt.-frei)

Mitgliederpreis
EUR 1.179,00
(MwSt.-frei)

in Zusammenarbeit mit:

GESELLSCHAFT FÜR INFORMATIK

BESCHREIBUNG

Security in Produkten stützt sich insbesondere in der Umsetzung technischer Anforderungen. Fehler, falsche Entscheidungen, unzureichende Kenntnisse öffnen potenziellen Angreifern Möglichkeiten (und seien sie noch so klein) Sicherheitsziele zu kompromittieren und Werte zu verletzen/zerstören. In diesem Kurs werden praxisnah die Methoden der Kryptographie vorgestellt und deren Vor- und Nachteile evaluiert.

Ziel der Weiterbildung

- Überblick über Methoden und Algorithmen der Kryptographie kennenlernen
- Bewusstsein bekommen, wann welche Methoden eingesetzt werden
- Hilfen zur Bewertung von Kryptographie kennen
- Anwendungsfälle exemplarisch kennenlernen
- Unterschiede von funktionaler Sicherheit und Security kennen
- Risikobegriff kennen

IMMER TOP!

Unser Qualitätsversprechen

Seit über 65 Jahren gehört die Technische Akademie Esslingen (TAE) mit Sitz in Ostfildern – nahe der Landeshauptstadt Stuttgart – zu Deutschlands größten Weiterbildungs-Anbietern für berufliche und berufsvorbereitende Qualifizierung im technischen Umfeld. Unser Ziel ist Ihr Erfolg. Egal ob Seminar, Zertifikatslehrgang oder Fachtagung, unsere Veranstaltungen sind stets abgestimmt auf die Bedürfnisse von Ingenieuren sowie Fach- und Führungskräften aus technisch geprägten Unternehmen. Dabei können Sie sich stets zu 100 Prozent auf die Qualität unserer Angebote verlassen. Warum das so ist?

PROGRAMM

1 | Einführung

- Motivation, Anwendungsfälle
- Historie der Kryptographie

2 | Symmetrische Kryptosysteme

- Anwendungsfeld und Einsatzmöglichkeiten
- Auswahl eines für den Use-Case passenden Kryptosystemes
- Vor- und Nachteile, Einordnung und mögliche Alternativen
- Vernam Verschlüsselung
- Brute Force Attack
- Chosen-Plaintext Attack (CPA)
- Chosen-Ciphertext Attack (CCA)
- Stream Ciphers
- Block Ciphers
- Block Cipher Modes (ECB, CBC, CTR)
- Stream Ciphers
- Advanced Encryption Standard (AES)
- Pseudo-Random Functions (PRF)

3 | Hash Funktionen & Message Authentication Codes (MACs)

- Anwendungsfeld und Einsatzmöglichkeiten
- Auswahl eines für den Use-Case passenden Verfahrens
- Vor- und Nachteile, Einordnung und mögliche Alternativen
- Preimage Resistance
- Collision Resistance
- Message Authentication Codes mittels Hashes (Encrypt-then-MAC)

4 | Asymmetrische Kryptosysteme & Digitale Signaturen

- Anwendungsfeld und Einsatzmöglichkeiten
- Auswahl eines für den Use-Case passenden Verfahrens
- Vor- und Nachteile, Einordnung und mögliche Alternativen
- Zahlentheoretische, schwierige Probleme
- RSA Verschlüsselung
- Digitale Signaturen
- Diffie-Hellman (DH) Schlüsselaustausch
- Public-Key Infrastructures (PKIs)

5 | Anwendungen

- TLS
- Block Chain

Alle Themenblöcke werden mit Beispielen und Anwendungsfällen aus der Praxis sowie interaktiven Übungen durchgeführt.

TEILNEHMER:INNENKREIS

- Produktentwickler (System, Software, Hardware) im Umfeld der Sicherheit (i.S. der Security)
- Projektleiter mit der Verantwortung für die Produktsicherheit ihrer zu entwickelnden Produkte
- Manager, Interessenvertreter zum Erwerb von Bewusstsein für technische Anforderungen zur Absicherung der Produktsicherheit
- Rollenverantwortliche wie Security Engineer zum Erhalt von Basiskenntnissen und Umsetzung von Kryptographie in praktischen Anwendungsfällen.

REFERENT:INNEN

Dr. Julian Liedtke

Dr. Julian Liedtke ist Experte für Cybersicherheit mit Schwerpunkt auf Cyber Resilience Act und Network and Information Security (NIS-2, ISO 27001). Als Cyber Security Coordinator verantwortet er die Umsetzung und Einhaltung wichtiger Sicherheitsregulierungen. Seine Aufgaben umfassen die Koordination von Sicherheitsmaßnahmen und die Entwicklung von Strategien zur Cyberresilienz. Im Jahr 2024 schloss er seine Promotion in Informatik ab, was seine akademische Expertise unterstreicht. Seine Kombination aus wissenschaftlicher Ausbildung und praktischer Erfahrung macht ihn zu einem gefragten Spezialisten. Dr. Liedtke trägt maßgeblich zur Weiterentwicklung von Sicherheitskonzepten in der digitalen Infrastruktur bei.

Dr. Thomas Liedtke

Dr. Thomas Liedtke ist
- seit vielen Jahren Mitglied der deutschen DIN-AK-Spiegelgruppe, welche für die Definition ISO/SAE 21434, ISO/PAS 5112 und weitere Cybersecuritystandards verantwortlich ist
- Mitglied des intacs Advisory Boards und Leiter der SPICE Cybersecurity Arbeitsgruppe Leiter der ZVEI Arbeitsgruppe Datensicherheit im Automobil
- Leadauditor für CSMS; ISMS; TISAX
- Berater für die Implementierung der Cybersecurity in Unternehmen

Publikationen
- Informationssicherheit: Möglichkeiten und Grenzen; SpringerLink publisher: link.springer.com/book/10.1007/978-3-662-63917-7
- The New Cybersecurity Challenges and Demands for Automotive Organisations and Projects – an Insight View link.springer.com/chapter/10.1007/978-3-031-42307-9_21

Weitere Veranstaltungen

Sicherheitsgerichtete Systeme entwickeln

VERANSTALTUNGSORT

Technische Akademie Esslingen
An der Akademie 5
73760 Ostfildern
Die TAE befindet sich im Südwesten Deutschlands im Bundesland Baden-Württemberg – in unmittelbarer Nähe zur Landeshauptstadt Stuttgart. Unser Schulungszentrum verfügt über eine hervorragende Anbindung und ist mit allen Verkehrsmitteln gut und schnell zu erreichen.

GEBÜHREN UND FÖRDERMÖGLICHKEITEN

Die Teilnahme beinhaltet Verpflegung sowie ausführliche Unterlagen.

Preis:
Die Teilnahmegebühr beträgt:
1.310,00 € (MwSt.-frei)

Fördermöglichkeiten:
Bei einem Großteil unserer Veranstaltungen profitieren Sie von bis zu 70 % Zuschuss aus der ESF-Fachkursförderung.
Bisher sind diese Mittel für den vorliegenden Kurs nicht bewilligt. Dies kann

verschiedene Gründe haben. Wir empfehlen Ihnen daher, Kontakt mit unserer Anmeldung aufzunehmen. Diese gibt Ihnen gerne Auskunft über die Förderfähigkeit der Veranstaltung.

Weitere Bundesland-spezifische Fördermöglichkeiten finden Sie hier.

Inhouse Durchführung:
Sie möchten diese Veranstaltung firmenintern bei Ihnen vor Ort durchführen? Dann fragen Sie jetzt ein individuelles Inhouse-Training an.

Weitere Termine und Orte

Datum	Lernsetting & Ort	Preis
Beginn: 23.04.2026 Ende: 24.04.2026	Ostfildern	EUR 1.310,00