VDI Wissensforum

Seminar

inklusive Quizzes und Gruppendiskussionen

Grundlagen der Cybersecurity - Kryptographie für Einsteiger

Die Top-Themen:

- **Symmetrische Kryptographie und Hashfunktionen**
- **Asymmetrische Kryptographie mit Schwerpunkt auf RSA, Diffie-Hellman und Elliptischer-Kurven-Kryptographie**
- **Post-Quantum-Kryptographie im Kontext der Bedrohungen durch Quanten-computer**
- **Grundprinzipien der Kryptographie: Kerckhoffs' Prinzip und One-Time Pad**
- **Praktische Anwendungen von Kryptographie**

Termine und Orte

26. und 27. März 2024
Freising

23. und 24. Juli 2024
Online

19. und 20. November 2024
Düsseldorf

Einstieg in Kryptographie - praxisnah und anwendungsori-entiert!

Ihr Trainer
Dr. Tobias Oder, Security Archi-tect, Alter Solutions Deutschland GmbH, Düsseldorf

Veranstaltung der VDI Wissensforum GmbH
Jetzt online anmelden!
www.vdi-wissensforum.de/01SE197
Telefon +49 211 6214-201 • Fax +49 211 6214-154

Bildquelle: © iStock_solarseven

Allgemeine Informationen

Zielsetzung

Cybersecurity ist eine der wichtigsten Herausforderungen unserer Zeit, da unsere Abhängigkeit von digitalen Systemen exponentiell wächst. Cyberangriffe können schwerwiegende wirtschaftliche, politische und persönliche Konsequenzen haben, wodurch der Schutz unserer Daten und Infrastrukturen von entscheidender Bedeutung ist, um die Stabilität und Sicherheit unserer Gesellschaften zu gewährleisten. Die ständige Entwicklung von Angriffsmethoden erfordert kontinuierliche Anstrengungen, um den Schutz vor Cyberbedrohungen aufrechtzuerhalten.

In unserem VDI-Seminar lernen Sie, die Sicherheitsziele von Kryptographie zu verstehen, die Relevanz standardisierter Kryptographie zu erkennen und gängige kryptographische Algorithmen kennenzulernen. Sie werden in der Lage sein, Angriffe auf kryptographische Algorithmen nachzuvollziehen und zu erkennen.

Darüber hinaus zeigen wir Ihnen, wie Sie Kryptographie in der Praxis einsetzen können und vermitteln Ihnen ein Verständnis für verschiedene Anwendungsfälle. Nach dem Besuch des Trainings werden Sie in der Lage sein, zukünftige Bedrohungen, wie Quantencomputer, einzuschätzen und zu mitigieren.

Nach jedem größeren Themenblock sind kleine Diskussionsrunden vorgesehen, in denen verschiedene Fragen gemeinsam erörtert werden.

Zielgruppe

Das Training richtet sich an:
- Anwender von Kryptographie
- Entwickler von sicherheitsrelevanten Produkten und Komponenten
- Systemarchitekten von vernetzten Systemen
- Anwender von Kommunikationsprotokollen
- Administratoren von Netzwerken und IT-Infrastruktur
- Datenschützer / Datenschutzbeauftragte

Seminarmethoden

Wir bitten Sie um die Mitnahme eines Notebooks, da das browserbasierte Tool Mentimeter zum Einsatz kommt. Eine Installation von Software ist nicht erforderlich.

Das Training wird durch interaktive Elemente wie Quizzes und Gruppendiskussionen aufgelockert.

Veranstaltungsdokumentation
Jeder Teilnehmer erhält eine Dokumentation wie Präsentationsunterlagen, Handbuch o.ä. und eine VDI Wissensforum-Teilnahmebescheinigung.

Seminarleitung

Dr. Tobias Oder, Alter Solutions Deutschland GmbH, Düsseldorf

Dr. Tobias Oder promovierte 2019 an der Ruhr-Universität Bochum im Fachbereich IT-Sicherheit. Seine aus 26 Publikationen mit über 1000 Zitierungen bestehende Forschung konzentrierte sich auf die praktische Realisierbarkeit von quanten-resistenter Kryptographie auf eingebetteten Systemen. Seit 2020 ist er als Security Architekt in der Automobilindustrie tätig und übte zwischen 2020 und 2023 weitere Lehrtätigkeiten an der Wilhelm-Büchner Hochschule aus.

Inhouse-Seminar

Dieses Seminar können Sie auch als firmeninterne Schulung buchen:

Wir erstellen Ihnen gerne ein individuelles Angebot. Rufen Sie uns an.

Frau Angela Bungert/Herr Jens Wilk
Tel.: +49 211 6214-200, E-Mail: inhouse@vdi.de
Herr Heinz Küsters
Tel.: +49 211 6214-278, E-Mail: kuesters@vdi.de

Weitere interessante Veranstaltungen

Automotive Systems Engineering kompakt
03. und 04. April 2024, Form eines Online-Seminars
13. und 14. November 2024, Form eines Online-Seminars

Datenkommunikation im Fahrzeug
10. und 11. April 2024, Frankfurt am Main
04. und 05. September 2024, Form eines Online-Seminars

Model-Based Systems Engineering kompakt
16. und 17. April 2024, Form eines Online-Seminars
20. und 21. August 2024, Form eines Online-Seminars

Seminarinhalte

1. Tag 09:00 bis 17:00 Uhr

Symmetrische Kryptographie und Hashfunktionen

Historische Chiffren
- Was bedeutet Kryptographie?
- Substitutionschiffren
- Enigma

Grundprinzipien der Kryptographie
- Sicherheitsziele von Kryptographie
- Kerckhoffs' Prinzip
- One-Time Pad

Stromchiffren
- LFSRs (Linear Feedback Shift Registers)
- ChaCha20 Algorithmus

Blockchiffren
- Unterschiede zu Stromchiffren
- Modulararithmetik und endliche Körper
- Advanced Encryption Standard
- Modes of Operation
- Message Authentication Codes

Symmetrische Kryptanalyse
- Wie kann man symmetriche Chiffren brechen?
- Wann gilt eine Chiffre als „gebrochen"?
- Brute-Force Angriffe
- Differezielle Kryptanalyse
- Lineare Kryptanalyse

Hashfunktionen
- Sicherheitseigenschaften von Hashfunktionen
- SHA-2 Algorithmus
- SHA-3 Algorithmus

2. Tag 08:30 bis ca. 16:30 Uhr

Asymmetrische Kryptographie

Grundlagen der asymmetrischen Kryptographie
- Unterschiede zur symmetrischen Kryptographie
- Digitale Signaturen

RSA
- Faktorisierungsproblem
- Mathematische Grundlagen
  - » Eulers Phi Funktion
  - » Erweiterter Euklidischer Algorithmus
- RSA-Algorithmus
- Primzahltests
- Binäre Exponentation

Diffie-Hellman-Schlüsselaustausch
- Diskretes Logarithmus Problem
- Vergleich mit dem Faktorisierungsproblem
- Zyklische Gruppen
- Diffie-Hellman-Protokoll

Elliptische-Kurven-Kryptographie
- Mathematische Grundlagen von elliptischen Kurven
  - » Definition von elliptischen Kurven
  - » Arithmetische Operationen auf elliptischen Kurven
  - » Das diskrete Logarithmus Problem auf elliptischen Kurven
- Unterschiede zu RSA und Diffie-Hellman

Post-Quantum-Kryptographie
- Quantencomputer als Bedrohung
- NIST Standardisierungsprozess
- Gitter-basierte Algorithmen
- Hash-basierte Algorithmen

Praktische Anwendung
- Public Key Infrastructures
- Transport Layer Security

VDI Wissensforum

Seminar:
Grundlagen der Cybersecurity - Kryptographie für Einsteiger

Jetzt online anmelden
www.vdi-wissensforum. de/
01SE197

Einstieg in Kryptographie praxisnah und anwendungsorientiert!

VDI Wissensforum GmbH | VDI-Platz 1 | 40468 Düsseldorf | Deutschland

Sie haben noch Fragen?
Kontaktieren Sie uns einfach!

VDI Wissensforum GmbH
Kundenzentrum
Postfach 10 11 39
40002 Düsseldorf
Telefon: +49 211 6214-201
Telefax: +49 211 6214-154
E-Mail: wissensforum@vdi.de

www.vdi-wissensforum.de

✓ Ich nehme wie folgt teil (zum Preis p. P. zzgl. MwSt.):

Seminar		
☐ **26. und 27. März 2024** **Freising** (01SE197001)	☐ **23. und 24. Juli 2024** **Online** (01SE197701)	☐ **19. und 20. November 2024** **Düsseldorf** (01SE197002)
EUR 1.840,-	EUR 1.840,-	EUR 1.840,-

23S01EM30

☐ Ich bin VDI-Mitglied und erhalte **pro Veranstaltungstag EUR 50,- Rabatt** auf die Teilnahmegebühr: VDI-Mitgliedsnummer*_____

*Für den VDI-Mitglieder-Rabatt ist die Angabe der VDI-Mitgliedsnummer erforderlich.

Meine Kontaktdaten:

Nachname _____ Vorname _____

Titel _____ Funktion/Jobtitel _____ Abteilung/Tätigkeitsbereich _____

Firma/Institut _____

Straße/Postfach _____

PLZ, Ort, Land _____

Telefon _____ Mobil _____ E-Mail _____ Fax _____

Abweichende Rechnungsanschrift _____

_____

Datum Unterschrift

Teilnehmer mit einer Rechnungsanschrift außerhalb Deutschlands, Österreichs oder der Schweiz bitten wir, mit Kreditkarte zu zahlen. Bitte melden Sie sich über www.vdi-wissensforum.de an. Auf unserer Webseite werden Ihre Kreditkartendaten verschlüsselt übertragen, um die Sicherheit Ihrer Daten zu gewährleisten.

Die allgemeinen Geschäftsbedingungen der VDI Wissensforum GmbH finden Sie im Internet: www.vdi-wissensforum.de/de/agb/

Veranstaltungsort(e)
Freising: Mercure Hotel München Freising Airport, Dr.-von-Daller-Str. 1-3, 85356 Freising, Tel. +49 8161/532-0, E-Mail: ha0q8-sb@accor.com
Online: online, Tel. +49 211/6214-201, E-Mail: wissensforum@vdi.de
Düsseldorf: NH Düsseldorf City Nord, Münsterstr. 232-238, 40470 Düsseldorf, Tel. +49 211/239486-0, E-Mail: nhduesseldorfcitynord@nh-hotels.com

Im Veranstaltungshotel steht Ihnen ein begrenztes **Zimmerkontingent** zu Sonderkonditionen zur Verfügung. Bitte buchen Sie Ihr Zimmer frühzeitig per Telefon oder E-Mail direkt bei dem Hotel mit dem Hinweis auf die „VDI-Veranstaltung". Weitere Hotels in der Nähe des Veranstaltungsortes finden Sie auch über unseren kostenlosen Service von HRS, www.vdi-wissensforum.de/hrs

HRS Das Hotelportal

Leistungen: Im Leistungsumfang sind die Pausengetränke und an jedem vollen Veranstaltungstag ein Mittagessen enthalten. Ausführliche Veranstaltungsunterlagen werden den Teilnehmern am Veranstaltungsort ausgehändigt.

Exklusiv-Angebot: Als Teilnehmer dieser Veranstaltung bieten wir Ihnen eine 3-monatige, kostenfreie VDI-Probemitgliedschaft an (dieses Angebot gilt ausschließlich bei Neuaufnahme).

Datenschutz: Die VDI Wissensforum GmbH verwendet die von Ihnen angegebene E-Mail-Adresse, um Sie regelmäßig über ähnliche Veranstaltungen der VDI Wissensforum GmbH zu informieren. Wenn Sie zukünftig keine Informationen und Angebote mehr erhalten möchten, können Sie der Verwendung Ihrer Daten zu diesem Zweck jederzeit widersprechen. Nutzen Sie dazu die E-Mail Adresse wissensforum@vdi.de oder eine andere der oben angegebenen Kontaktmöglichkeiten.
Auf unsere allgemeinen Informationen zur Verwendung Ihrer Daten auf https://www.vdi-wissensforum.de/datenschutz-print weisen wir hin.
Hiermit bestätige ich die AGBs der VDI Wissensforum GmbH sowie die Richtigkeit der oben angegebenen Daten zur Anmeldung.

Ihre Kontaktdaten haben wir basierend auf Art. 6 Abs. 1 lit. f) DSGVO (berechtigtes Interesse) zu Werbezwecken erhoben. Unser berechtigtes Interesse liegt in der zielgerichteten Auswahl möglicher Interessenten für unsere Veranstaltungen. Mehr Informationen zur Quelle und der Verwendung Ihrer Daten finden Sie hier: www.wissensforum.de/adressquelle

Mit dem FSC® Warenzeichen werden Holzprodukte ausgezeichnet, die aus verantwortungsvoll bewirtschafteten Wäldern stammen, unabhängig zertifiziert nach den strengen Kriterien des Forest Stewardship Council® (FSC). Für den Druck sämtlicher Programme des VDI Wissensforums werden ausschließlich FSC-Papiere verwendet.

FSC www.fsc.org
MIX
Papier aus verantwortungsvollen Quellen
FSC® C124933