SEMINARBESCHREIBUNG

PKI, CA, https – Zertifikats- und Public-Key-Infrastrukturen verstehen

KURZBESCHREIBUNG

SSL/TLS und Datensicherheit durch verschlüsselte Kommunikation sind heute fast eine Selbstverständlichkeit – zumindest sollten sie es sein. Sie haben aber nur Erfolg, wenn sie bequem genutzt werden können und "einfach so" funktionieren. Wie Verschlüsselung in der Praxis funktioniert und was man dazu benötigt, lernen Sie in diesem Seminar. Neben den Grundlagen der symmetrischen und asymmetrischen Verschlüsselung lernen Sie ihre Anwendung im Rahmen von gebräuchlichen Public-Key-Verfahren kennen. Darüber hinaus widmen wir uns den unterschiedlichen Zertifikats- und Schlüssel-Formaten und stellen exemplarisch Tools zu ihrer Analyse und Erstellung vor.

IHR NUTZEN

Sie lernen die Grundlagen und Begriffe der gängigen Verschlüsselungsmechanismen kennen.

Sie können Schlüssel(paare), Zertifikatsanträge und Zertifikate erstellen, bearbeiten und verwenden und mit Zertifikatsketten umgehen.

SCHWERPUNKT

Der Schwerpunkt des Seminars liegt auf Public-Key-/X509-Zertifikaten für die Absicherung der TLS-, Internet- und Mailkommunikation.

ZIELGRUPPE

Alle, die Zertifikate und PKI jetzt und in Zukunft installieren und betreiben und für die Sicherheit verantwortlich sind.

THEMEN

Kryptographische Grundlagen
- Terminologie
- Hash, Message Authentication Code, MD5, SHA

Symmetrische Verschlüsselung

Asymmetrische Verschlüsselung
- Public Key, Private Key
- Eigenschaften und Funktionalitäten eines Schlüsselpaares
- Sicherheitsziele
- Abgrenzung PSK vs. PKI

RSA, Diffie-Hellman

Vom Public Key zum Zertifikat

Komponenten einer PKI
- Zertifikatsanforderungen, Zertifikate, Zertifizierungsstellen, Zertifikatsketten
- X.509, Zertifikatsformate, PEM, DER, PKCS#7, PKCS#12
- Subscriber, Relying Party

Verschlüsselte Kommunikation, Server- und Client-Authentifizierung
- SSL/TLS, https, OpenSSL, XCA

ARD-CA

Abgrenzung gegenüber PGP

TERMINE

20.07.20, 09:00 - 21.07.20, 16:30
Online
Preis: 1.140 EUR

DAUER

2 Tage

TEILNEHMERZAHL

16

INHALTLICH VERANTWORTLICH

Olaf Schott
E-Mail o.schott@ard-zdf-medienakademie.de
Telefon +49 911 9619-478
Telefax +49 911 9619-299

KONTAKT

Anette Barth
E-Mail a.barth@ard-zdf-medienakademie.de
Telefon +49 911 9619-251
Telefax +49 911 9619-199

SEMINARNUMMER

31 552