Verschlüsselung mit Zertifikaten und TLS/SSL 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.

HINWEIS

Falls die Veranstaltung als Webinar durchgeführt wird, stellen wir die Übungsrechner per Anydesk zur Verfügung, Anleitungen und Zugangsdaten dazu erhalten Sie rechtzeitig vor dem Webinar. In diesem Fall empfehlen wir zur Teilnahme einen PC mit 2 Bildschirmen.

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 TLS/SSL-basierte Verschlüsselung jetzt und in Zukunft installieren und betreiben und für 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. Public/Private Key

RSA, Diffie-Hellman

Vom Schlüsselpaar zum Zertifikat
- Zertifikatsanforderungen, Zertifikate, Zertifizierungsstellen, Zertifikatsketten
- X.509, Zertifikatsformate, PEM, DER, PKCS#7, PKCS#12
- Subscriber, Relying Party
- Public Key Infrastructure (PKI)

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

ARD-CA

Abgrenzung gegenüber PGP

TERMINE

Aktuell sind keine Termine verfügbar.

INHALTLICH VERANTWORTLICH

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

KUNDENSERVICE

Anette Barth
E-Mail: kundenservice@ard-zdf-medienakademie.de
Telefon: +49 911 9619-251

SEMINARNUMMER

31 512