

Szkozenie: Capstone Courseware 562 Securing Java Web Services



DOSTĘPNE TERMINY

2025-06-02 | 5 dni | Virtual Classroom
2025-06-16 | 5 dni | Warszawa / Wirtualna sala

Cel szkolenia:

Ten zaawansowany kurs wprowadza programistów Java do kluczowych koncepcji i technologii dla rozwoju bezpiecznych usług internetowych i zabezpieczania architektury oprogramowania dla przedsiębiorstw. Choć konsensus formowania, i standardy zostały w dużej mierze ukształtowane, jest to nadal szeroka i wymagająca dziedzina. Skupiamy się na kilku dobrze zdefiniowanych metodach kryptografii: XML, WS-Security i WS-SECURITYPOLICY standardy i zabezpieczenia Markup Language Asercje lub SAML. Poruszamy także XACML dla polityki autoryzacji i na relacjach zaufania i Federacjach - nie tylko przewidziane przez SAML ale również poprzez specyfikacje WS-Trust i WS-Federation.

Podejścia te nie pokrywają się, a w naszych głównych przykładach prezentujemy jedną, spójną historię zapewnienia poufności, integralności, niezaprzeczalności, autentyczność użytkownika i odpowiedniego zezwolenia żądania z mieszanką polityki badawczej WS-Security, SAML, a nawet jakąś aplikacją kodowaną podpisem cyfrowym. Mamy również zbadać web-aplikacje SAML, dogłębną analizę tożsamości Single Sign-On i federacje tożsamości.

Dla celów praktycznych oczywiście zależy od konkretnej platformy, którą jest Java EE, zdecydowana większość treści kursu uczy interoperacyjnych specyfikacji i będzie równie przydatne dla programistów pracujących na innych platformach obsługujących web-service, takich jak .NET - lub do tych, którzy pracują z wieloma platformami, a muszą zrozumieć interoperacje w szczegółach, które mogą być nie potrzebne w strategii wdrażania. W rzeczywistości są dostępne modyfikacje, które zasadniczo pomijają Java, które przylegają ściślej do XML.

Cel szkolenia:

- Zrozumienie unikalnych wyzwań związanych z zapewnieniem interoperacyjności usług opartych na XML.
- Zastosowanie standardów W3C do cyfrowego podpisywania i szyfrowania XML fragmenty i dokumenty.
- Zrozumienie znaczenia specyfikacji WS-Security interoperably Secure Messaging.
- Korzystanie state-of-the-art narzędzi do konfiguracji lub wdrożenia podpisu, szyfrowania i różne treści nagłówka WS-Security dla Java Web Services.
- WSS-Drive implementacje z dokumentów WS-SECURITYPOLICY.

- "Vouch for" poręczenie za użytkownika między domenami w celu uzyskania zezwolenia na żądania bez poświadczeń udostępniania.
- Wymiana informacji zabezpieczeń między serwerami, aplikacjami i komponentami, z wykorzystaniem twierdzenia SAML i modeli protokołów.
- Zrozumieć rolę w zarządzaniu politykami XACML i podejmowanie decyzji.
- Zrozumieć architektury WS-Trust i WS-Federation dla rozwijania relacji zaufania, które umożliwiają usługi federacyjne i architektury zorientowane na usługi.
- Budowanie aplikacji internetowych, które uczestniczą w federacji SAML i Single Sign-On.

Plan szkolenia:

- Zabezpieczanie Service-Oriented Enterprise
 - Zabezpieczenia dla Web Services
 - Zagrożenia
 - Bramki-CIA
 - Poziomy rozwiązania: W3C, OASIS, Java EE
 - Scenariusz: Secure Multi-Party Conversation
 - Kryptografia
 - WS-Security i WS-SecurityPolicy
 - Scenariusz: Information Security Sharing
 - SAML i XACML
 - Scenariusz: Wiele domen użytkownika
 - Scenariusz: Single Sign-On
 - Technologia Stacks: WS-Federation i Liberty Alliance
 - WS-I Basic profil bezpieczeństwa
- Bezpieczeństwo w transporcie
 - Use Case: bezpieczny transport
 - Http schematy uwierzytelniania
 - HTTP BASIC
 - DIGEST-HTTP
 - Zabezpieczenie Web-Service URLs
 - HTTPS
 - Wsparcie JAX-WS
 - Oś Wsparcia
- Podpis XML
 - Use Case: niezaprzeczalność
 - XML Digital Signature

- Kryptografia Backgrounder
- Canonical XML
- Otoczki, kopertowanie i odłączone Podpisy
- SignedInfo i Referencje
- Java Cryptography Architecture
- Keystores
- Dlaczego nie wystarczą klucze
- Certyfikaty X.509 i łańcuchy certyfikatów
- KeyStore API
- Java API XML Digital Signature
- Kroki do Szyfrowania i deszyfrowania zawartość XML
- JAX-WS Handlers wiadomość
- Foiling the Man in the Middle
- XML Encryption
 - Przypadek użycia: Poufność
 - XML Encryption
 - EncryptedData
 - Element vs Content Encryption
 - Key Wrapping
 - The Java Rozszerzenia kryptograficzne
 - Apache XML Bezpieczeństwo
 - Kroki do szyfrowania i deszyfrowania zawartości XML
 - Wybór Algorytmy i rozmiary kluczy
- WS-Security
 - Przypadek użycia: Bezpieczna wymiana wiadomości
 - Przypadek użycia: Logowanie użytkownika
 - The Specyfikacja WS-Security
 - Security Token Rodzaje
 - Znaczniki czasu
 - Nazwa Tokens
 - Podpis i szyfrowanie
 - Narzędzia dla WS-Security
 - XWSS i JAAS
 - Foiling Replay Attacks
- WS-SecurityPolicy
 - Przypadek użycia: Udostępnianie metadanych

- WS-Policy
- Znormalizowana vs kompaktowa forma
- Policy Attachment
- Polityka Scopes
- WS-SecurityPolicy
- Protection Asercje
- Token Asercje
- Wspieranie i powoływanie Tokenów
- Powiązania
- Metro i WSIT
- Wdrażanie odwołania
- Integracja strukturą zabezpieczeń
- Wprowadzenie do SAML
 - Historia SAML
 - Twierdzenia
 - Protokoły
 - Powiązania
 - Profile
 - Korzystanie OpenSAML
 - SAML i Web Services
- Twierdzenia SAML
 - Przypadek użycia: "vouching" Użytkownika
 - Szablony odrzucenia
 - Rozszerzalność
 - Twierdzenia i Tematy
 - NameID Rodzaje
 - Warunki
 - Ptwierdzenie tematu
 - Potwierdzenie Metody
 - AuthntStatement
 - Authentication Konteksty
 - AttributeStatement
 - Attribute Profiles
 - AuthzDecisionStatements
 - Akcje i dowody
 - WS-Security i tokeny SAML

- OpenSAML modele odrzucenia
- Tworzenie obiektów XML
- Marshalling i Unmarshalling
- SAML protokół
 - Przypadek użycia: wsteczne Kwerendy
 - żądania, Zapytania i odpowiedzi
 - Status i StatusCode
 - AuthnQuery
 - AttributeQuery
 - AuthzDecisionQuery
 - Pozostałe żądania i rodzaje reakcji
 - OpenSAML wzór protokołu
 - SAML i XML Signature
 - SAML Encryption i XML
- XACML
 - Przypadek Użycia: Back-Channel autoryzacji
 - Przypadek Użycia: zasady autoryzacji udostępnianie
 - Polityki, zestawy polityk i cele
 - Zasady
 - Połączenie algorytmów
 - Policy Context
 - Request i typy reakcji
 - Profil SAML z XACML
 - Autoryzacji decyzje poprzez XACML
- Zabezpieczanie usług Federated
 - Publish, Find, Bind ... Execute!
 - UDDI
 - WS-BPEL
 - Problem zaufania
 - WS-Trust
 - The Security Service token
 - Messaging Model: RST i RSTR
 - Klucze pochodne
 - WS-SecureConversation
 - Secure Conversation Metrics
 - WS-Federation

- Value Proposition
- Powiązania SAML
 - Przypadek użycia: Mówić "przez" Przeglądarkę
 - Wiązanie SOAP
 - SAML przez HTTP
 - Browser jako Messenger
 - Redirect, POST i powiązania Artefaktów
 - PAOS Binding
 - Wiązanie URI
- Federated Identity
 - Co to jest federacja?
 - Problemy dla Identity Federation
 - SAML 2,0 Federacje
 - Single Sign-On
 - Account Linking and Persistent Pseudonimy
 - Chwilowe Pseudonimy
 - Mapowanie nazw ID
 - Federation Termination
 - OpenSSO
 - Fedlets

Wymagania:

- Solidne doświadczenie programowania Java jest niezbędne, kurs 103 [Java Programming](#) zapewnia doskonale przygotowanie.
- Doświadczenie w rozwoju **Java Web services** jest również wymagane: ćwiczenia przyjmują zrozumienie zarówno **SAAJ** i **JAX-WS**. Kurs 561 [Developing SOAP Web Services in Java](#) jest bardzo wskazany.
- Kursanci powinni być w stanie czytać i pisać XML płynnie, i mieć trochę znajomości XML Schema. Rozważ kursy 501 [Introduction to XML](#) i 517 [XML Schema](#).

Poziom trudności



Certyfikaty:

Uczestnicy szkolenia otrzymują certyfikat sygnowany przez firmę Capstone Courseware.

Prowadzący:

Certyfikowany wykładowca Capstone Courseware.