Zijn Uw webapplicaties wel veilig?

Transfer Café December 2014

Spreker(s) : Peter de Vaal, Martin Hol

Datum : 15 december 2014

E-mail : pdevaal@transfer-solutions.com, mhol@transfer-solutions.com

TRANSFER

Onderwerpen

- Veilige communicatie: SSL
- Netwerkarchitectuur: Aanbevelingen
- Java: Is het veilig?
- Identity Management

TRANSFER

VEILIGE COMMUNICATIE: SSL

TRANSFER

Cryptografie voor het web

- Garantie voor privacy
  - Versleuteling van gegevens over het netwerk
  - Authenticatie: Ken de andere partij
- Versleuteling
  - De zender versleutelt de gegevens
  - De ontvanger ontsleutelt
- Authenticatie
  - Server
  - Gebruiker of client
  - (Vendor van) Client software
- SSL / TLS is de(!) standaard

TRANSFER

Cryptografie: Algoritmen

- Hash
  - onomkeerbare encryptie. Bijv: MD5, SHA
  - Gebruik: Digitale handtekening voor een certificaat
- Symmetric Key
  - 1 sleutel voor de/encryptie. Bijv. (3)DES, AES
  - Gebruik: Versleutelen dataverkeer
- Asymmetric Key Pair:
  - 2 sleutels voor de/encryptie. Bijv. RSA, ECC
  - Gebruik: Uitwisselen symmetric key
    Validatie certificaten

TRANSFER

Cryptografie: Certificaten

- Server certificaat
  - Authenticatie van de server
- Client certificaat
  - Authenticatie van de “gebruiker”
- Code Signing certificaat
  - Authenticatie van (gedownloade) *client* software
- Self-signed certificaten
  - Met tooling zelf geproduceerde certificaten
  - Worden nooit per definitie vertrouwd
  - Zelf root CA plaatsen op clients
  - Nooit voor internet/extranet gebruiken!

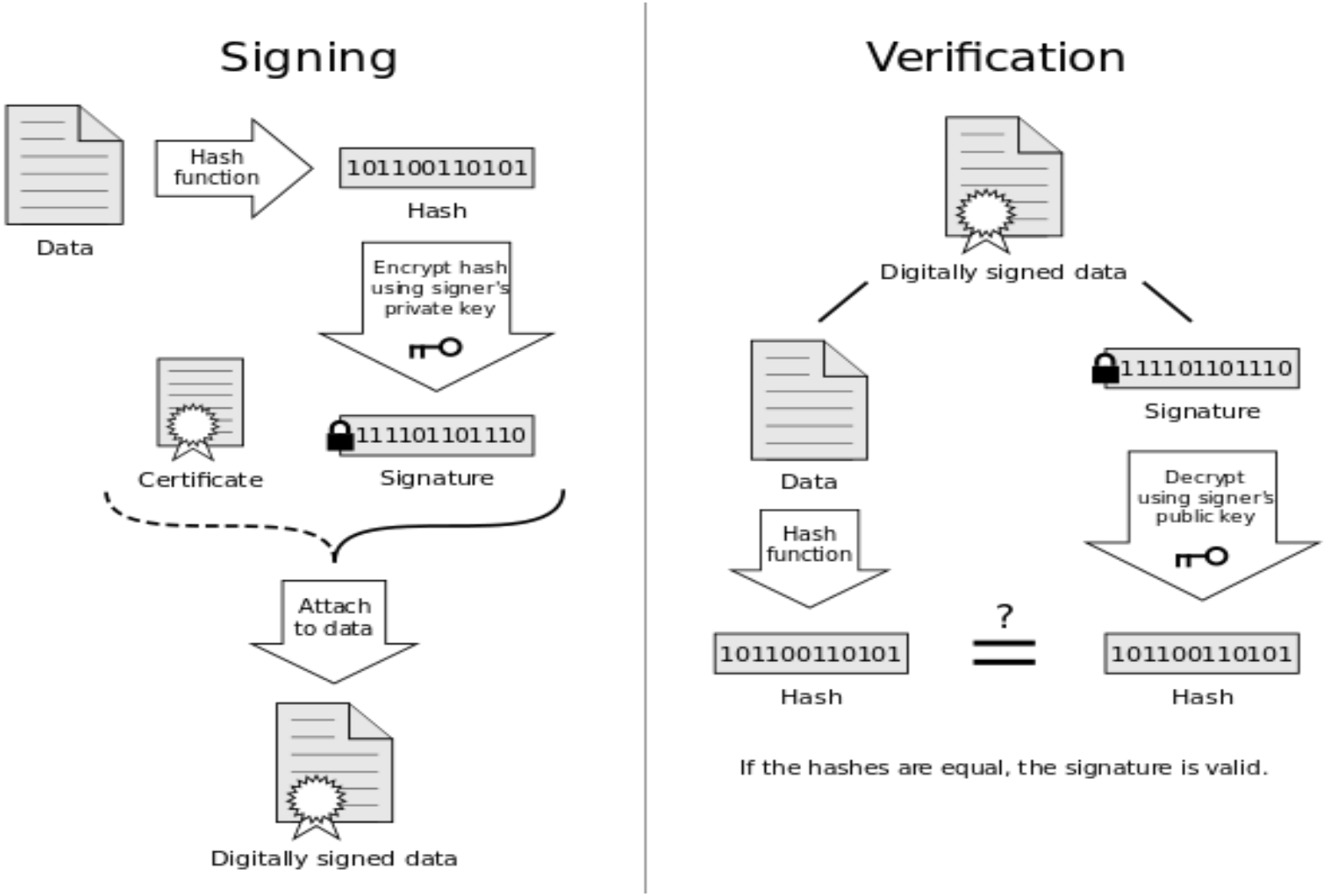
TRANSFER

PKI: Public Key Infrastructure

- Private en Public Key (Asymmetric key pair)
  - Op zichzelf geen bewijs van authenticiteit
- Digital Certificate
  - Authenticiteit van de public key

TRANSFER

Authenticatie (1)



Authenticatie (2)

- Controle Certification Path
  - (a.k.a. Certificate Chain)
- Certificate Authority (CA)
  - Top van de hierarchie
  - CA's Trust Anchor (Self-Signed Root Certificate) is aanwezig in de Truststore van de validator
  - Voorbeelden: VeriSign, Thawte, GlobalSign
- Mogelijk een aantal Intermediairs

TRANSFER

SSL/TLS: Protocol

- SSL: Secure Sockets Layer
  - Protocol toevoeging aan standaard protocols zoals: TCP/IP, HTTP, LDAP, SMTP etc.
  - Doel: dataversleuteling en authenticatie
  - Versies: 1.0, 2.0 en 3.0, allen van vorige eeuw
- TLS: Transport Layer Protocol
  - Nieuwe naam voor SSL, zelfde principe
  - Versies: 1.0 (1999), 1.1 (2006), 1.2 (2008) 1.3 (specificatie fase, okt 2014)
  - TLS 1.0 verschilt weinig van SSL 3

TRANSFER

SSL/TLS: Protocol

- 1. Handshake (cipher negotiation)
  - Bepalen van algoritmen en parameters (Cypher)
  - Server authenticatie
  - Client genereert shared key en wisselt deze uit
- 2. Authenticatie
  - Enkelzijdig: Alleen server authenticeert zich
  - 2-zijdig: Zowel client als server authenticeert zich
  - Root CA certificaat (trust) nodig op client
    - Browsers bevatten root CA van alle bekende CAs
    - Niet-browser clients: Moeten zelf root CA plaatsen
- 3. Communicatie middels shared keys

TRANSFER

SSL/TLS: Tools

- Beheer van certificates, keys, csr’s:
  - OpenSSL (incl. TLS)
  - JDK's Keytool
  - Div. grafische tools (Bijv. KeyStore Explorer)
  - Oracle: orapki, wlst, kss://

- Online Tools: https://www.sslshopper.com
  - Check CSR
  - Check Certificate
  - Check Site
  - Certificate Format Converter

TRANSFER

Certificaten: Formaten

- Certificate Formats
  - PEM (Base-64, handig mee te nemen)
  - DER (Digitaal)
- Certificate File formaten:
  - *.CRT
  - *.CER
  - *.KEY
  - *.P7B
  - ~~*.PEM~~

TRANSFER

Certificate stores

- Tweeledig gebruik:
  - Identity Keystore: Bevat authenticatie keys
  - Trust Keystore: Bevat CA certificaten
    - Bijv. *cacerts* (truststore van de JRE)
  - Goede praktijk: Deze varianten altijd scheiden
- Java Keystore (*.jks)
- PKCS12
- Oracle Wallet
  - Beheer: orapki (commandline), Wallet Manager (9i, 10g, 11g), WLST, Enterprise Manager (12c)

TRANSFER

Ontwikkelingen

- SSLv3 Einde, POODLE attack
  - Browser ondersteuning SSLv3:
    - Firefox: verwijderd per december 2014
    - Chrome, Safari: Alleen fall-back
    - IE: Disabled
    - Oudere browserversies blijven kwetsbaar!
  - Oracle Middleware: SSLv3 verwijderd in 12c
- TLS 1.0: Ook gekraakt (8 dec 2014)
  - Minder kwetsbaar dan SSLv3
  - Maar moet zo snel mogelijk uitgeschakeld worden
- SHA1 -> SHA2
  - Nederlandse Overheid vereist SHA2

TRANSFER

“This seems like a good moment to reiterate that *everything* less than TLS 1.2 with an AEAD cipher suite is cryptographically broken”

https://www.imperialviolet.org/2014/12/08/poodleagain.html

TRANSFER

Oracle WebLogic

- Certicom SSL-implementatie
  - Verouderde default implementatie t/m 11G
  - Geen SHA2
  - Desupported in 12C

- JSSE
  - In 12C de enige implementatie
  - In 11G enige optie voor “Clients” van SHA2 WebSites
    - WebServices
    - Oracle Service Bus

TRANSFER

Oracle Webtier

- Oracle HTTP Server 11g
  - Ondersteuning van SSLv3 en TLS 1.0
- Oracle WebCache 10g/11g
  - Ondersteuning van SSLv3 en TLS 1.0
  - 10g: clientHello v2 niet standaard ondersteund
- Oracle HTTP Server 12c
  - Ondersteuning van TLS 1.0, 1.1 en 1.2
  - SSLv3 verwijderd

TRANSFER

Beveiliging oudere servers met TLS 1.2

- Oracle 10g en 11g producten ondersteunen geen TLS 1.2
- Oplossing: Oracle HTTP Server (OHS) 12c
  - Zet dit product in als reverse proxy
  - Routeer naar OHS11g …
  - … of gebruik als vervanger van OHS 11g en routeer direct naar WebLogic 11g

TRANSFER

NETWERKARCHITECTUUR

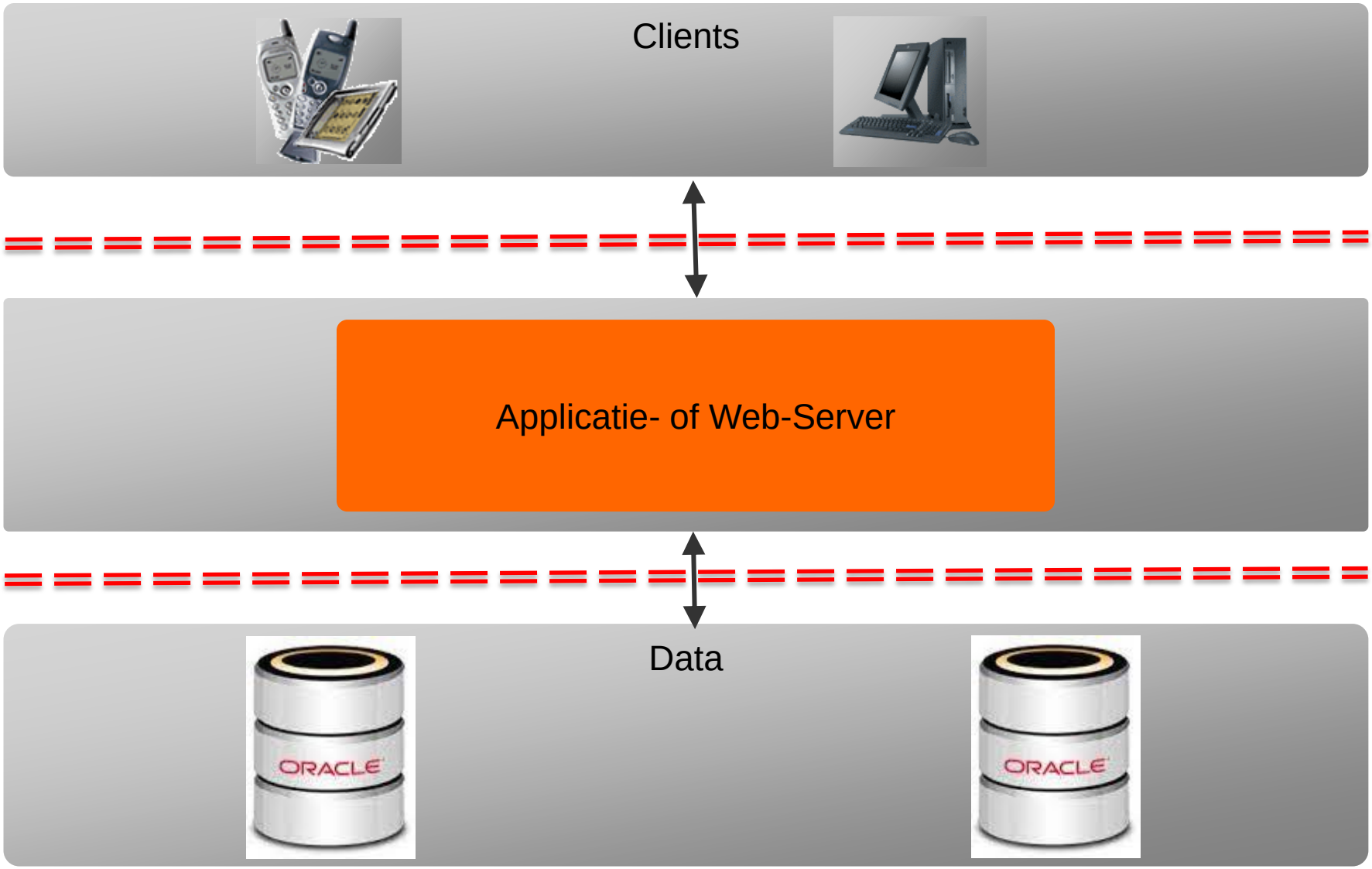
TRANSFER

Uw netwerk en het web

- Netwerk zones:
  - Internet
  - DMZ
  - Applicatie zone
  - Data zone
  - Intranet: Gebruikers/kantoor zone
  - Extranet: Toegang tot het intranet via internet via VPN en/of SSL authenticatie
- Tussen alle zones staan firewalls

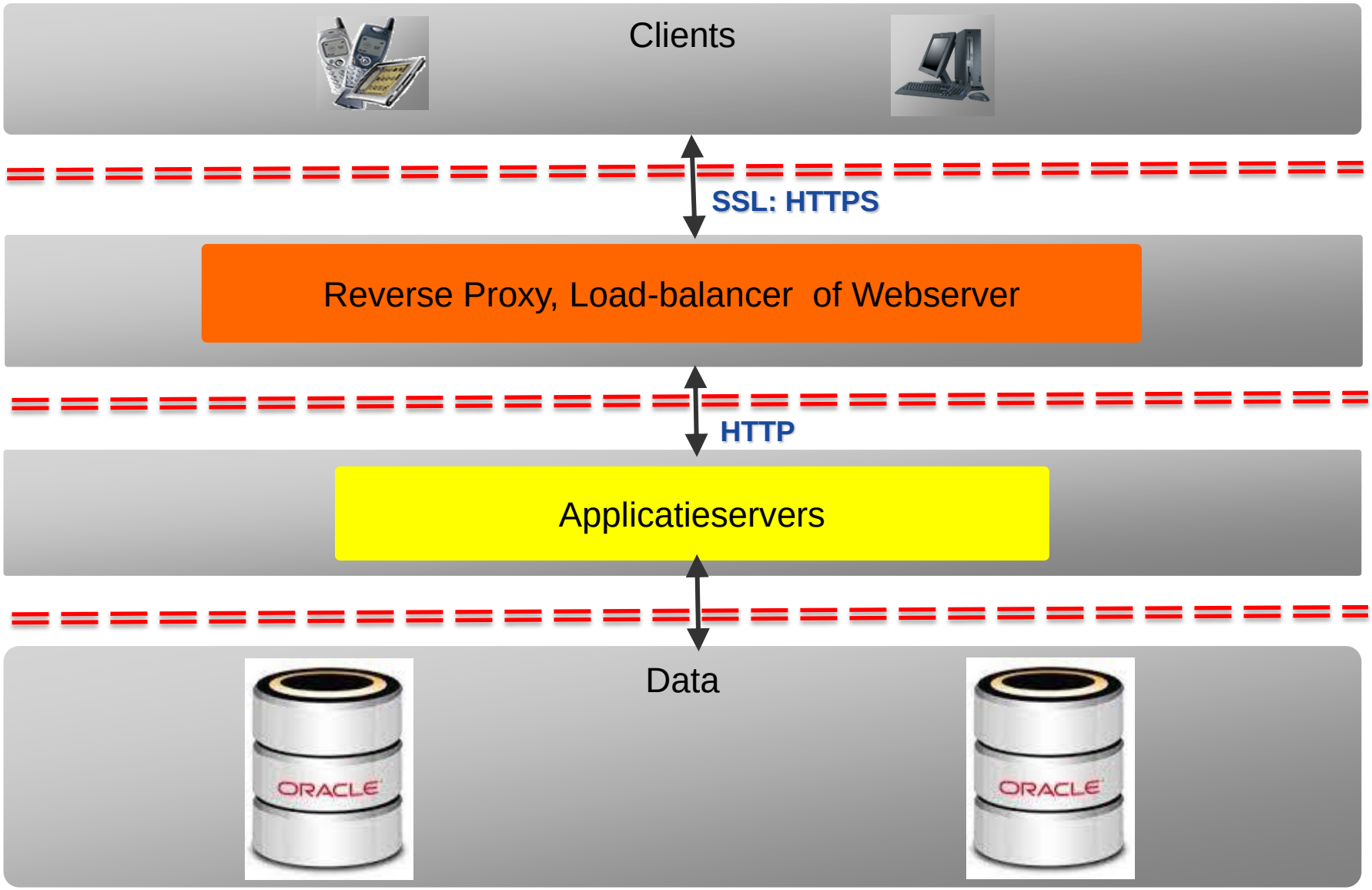
TRANSFER

Klassieke 3-lagenarchitectuur



TRANSFER

Meer-lagenarchitectuur met DMZ



TRANSFER

Voor een veilig intranet

- Toegang vanaf internet uitsluitend via DMZ
  - Geef nooit rechtstreeks toegang tot servers in intranet zones
  - Open uitsluitend standaard poorten: 80 en 443
  - Vermijdt andere poorten, zoals LDAP(s), zoek alternatieven via HTTPS (bijv. webservices)
- Toegang vanaf LAN (kantoor netwerk)
  - Bij voorkeur via DMZ, evt. via applicatiezone
  - Geen rechtstreekse toegang tot datazone!

TRANSFER

Wel of niet SSL?

- Altijd SSL tot DMZ
- SSL tussen interne zones:
  - Altijd waar wachtwoorden over het netwerk gaan (LDAP, SSO)
  - Verder niet nodig voor de meeste toepassingen
  - Geeft alleen enorme overhead (performance, configuratie inspanning, dure consultants, slecht of niet gedocumenteerde architectuur, verlopende certificaten etc. etc.)
  - SSL NOOIT door ontwikkelaars laten implementeren. Gebruik alleen standaard technologie!

TRANSFER

JAVA EN VEILIGHEID

TRANSFER

Is Java nu veilig of niet?

- Java werd gezien als grootste lek in beveiliging
  - Is dit altijd zo, of in bepaalde situaties?
- Sinds Java 7 update 40 is Java “veilig”
  - Maar blijf nieuwe updates installeren
  - Gebruik geen oude Java versies meer op clients
- 3 typen gebruik van Java:
  - Runtime voor toepassingen op client
  - Runtime voor applicatieservers
  - Applicaties vanaf internet via browser of Java webstart

TRANSFER

Java op de client

- Java Applicaties op een client
  - Gebruikt de Java Runtime Engine (JRE)
  - Applicaties zijn zelf geïnstalleerd
  - Applicaties hebben vaak geen internetverbinding
  - Je hebt dus zelf controle over veiligheid

TRANSFER

Java op de server

- Java Applicatieserver
  - Uitvoerend hart van de applicatieserver
  - Die is meestal afgeschermd met firewalls
  - Toegang vanaf internet via een DMZ
  - Toegang naar internet via een proxyserver
  - Je hebt veiligheid zelf in de hand

TRANSFER

Java via internet

- Rich User Interface Internet toepassingen (RUI)
  - Werken via de webbrowser of Java Webstart
  - Maakt gebruik van de Java plug-in van de browser, en een op de client geïnstalleerde JRE naar keuze
  - Programmacode komt van de webserver via internet
  - De webbrowser plug-in is toegangspoort tot de client
  - Programmas geven (soms) volledig toegang tot de client aan de server
  - Zonder extra maatregelen dus erg onveilig!
  - Java plug-in versies van voor 7 update 40 dus NIET MEER GEBRUIKEN op clients!
  - Oudere JREs mogen nog wel aanwezig zijn, maar de browser moet altijd de nieuwste plug-in versie hebben

TRANSFER

Wat zijn de maatregelen voor RUIs?

- Vanaf Java 7 update 40:
  - Moet alle programmacode van een digitale handtekening voorzien zijn, gezet met een geldig CA certificaat
  - Moet in de manifest file van de applicatie de rechten van de applicatie aangegeven zijn
  - Kan in de manifest file aangegeven worden vanaf welk internetdomein de applicatie uitgevoerd mag worden

TRANSFER

Wat zijn de gevolgen hiervan?

- Internetsites met niet vertrouwde Java RUIs kunnen niet meer gestart worden
  - Er kunnen in het Java controlpanel uitzonderingen opgenomen worden, maar telkens moet deze opnieuw bevestigd worden bij opnieuw starten
  - Dit voorkomt onbedoeld starten van malafide Java software via de browser
- En Uw eigen RUI software?
  - Voorbeeld is: Oracle Forms applicaties
  - Ook die moet dus van een handtekening voorzien worden

TRANSFER

Wat te doen met 3rd party software?

- Leverancier vragen om een gesignde versie
  - Is vaak niet mogelijk of kost geld
- Oude Java versie (6) plug-in blijven gebruiken
  - Zeer af te raden
  - De webbrowser en dus de Java plug-in heeft toegang tot Internet. Met Java 6 plug-in is het risico groot dat malafide sites door gebruikers bezocht worden en schade veroorzaken
- Gebruik maken van een Deployment Rule Set
  - Hiermee kan de desktopbeheerder het gebruik van (websites met) RUIs reguleren

TRANSFER

Deployment Rule Set

- File met regels over toegang tot RUIs
  - Beschrijft uitzonderingen per applicatie, zoals toegang zonder signature, toegang met oudere JRE etc.
  - XML file ingepakt in een JAR file
  - De JAR moet gesigned zijn
  - Wordt geplaatst op de client
  - Dus gedistribueerd door desktopbeheerder

TRANSFER

Hoe beheer ik mijn DRS?

- Java SE Advanced (of Suite) licentie
  - Java 8 SE Advanced Beheertool
  - Beheer van alle Java applicaties en RUIs op clients in een organisatie
  - Eenvoudig beheer van de DRS en automatisch pushen naar clients
  - Kan ook DRS voor Java 7 clients maken

TRANSFER

Kan ik self-signed certificaten gebruiken?

- Java RUIs met self-signed certificaten
  - Was de standaard t/m Java 6
  - Oracle Forms had hier een utility voor (sign_webutil.sh)
  - In Java 7 wordt self-signed niet meer geaccepteerd
  - Work-around:
    - Voeg het root CA toe aan de cacerts file van de JRE
    - Dit moet voor alle clients gedaan worden

TRANSFER

IDENTITY MANAGEMENT

TRANSFER

Identity Management: Doel

- Authenticatie van gebruikers
- Toegangscontrole
- Beheer van identiteiten en authorisaties (Identity Governance)

TRANSFER

Belangrijkste software

- Directory Services: LDAP
  - Voorbeelden:
    - Microsoft Active Directory
    - Oracle Internet Directory
    - Oracle Unified Directory
  - Doel: Authenticatie m.b.v. username/password
- Single Sign On services
  - Voorbeelden:
    - Oracle Access Manager
    - IBM Tivoli Webseal
  - Doel: Centrale authenticatie en toegangscontrole

TRANSFER

Authenticatie met een wachtwoord

- Wachtwoord policies
  - Vereisten aan formaat: Controle op gebruik hoofdletters, leestekens, bestaande woorden etc.
    - Te veeleisend is onveiliger dan zonder voorwaarden: veel mensen gaan het wachtwoord oipschrijven
    - Redelijke voorwaarden: Minimum lengte 6, Minimaal 1 hoofdletter en 1 cijfer
  - Geldigheidsduur: Na hoeveel tijd vernieuwen
    - Te kort is onveiliger dan geen: veel mensen gaan het wachtwoord opschrijven
    - Redelijke termijn: 4 maanden

TRANSFER

Andere authenticatie methoden

- SSL certificaat
- Token (RSA)
- Hardware: TouchID, irisscan etc.
- Externe authenticatie, bijv. Facebook, Google, Apple
- Multi-level authenticatie:
  - Combinatie van authenticatiemethoden
  - evt. afhankelijk van de situatie

TRANSFER

Best Practices

- Single Sign On
  - Alleen als toegang tot vele toepassingen nodig is, bijv. vanuit en bedrijfsportaal
  - Via Windows Native Authentication: Alleen voor vaste werkplekken in kantooromgeving (uitstervend?)
- Gebruik standaard inlogfaciliteit
  - Bouw niet voor elke applicatie een inlogscherm
  - Oracle: Gebruik OPSS framework
  - Authenticeer tegen LDAP, niet tegen database of XML files

TRANSFER

Oracle producten

- Directory Servers
  - Oracle Internet Directory
    - Betrouwbaar, maar vereist Oracle DB
  - Oracle Virtual Directory
    - Vereist andere DS en/of DB. Geeft flexibiliteit
  - Directory Server Enterprise Edition
    - SUN product, wordt nog veel gebruikt
  - Oracle Unified Directory
    - Beoogde opvolger van alle voorgaande
    - Werkt met embedded Berkeley DB
    - Is Java SE based, toegang via WebLogic (ODSM)
    - Ongeevenaarde performance
    - Nog niet alle Oracle producten zijn gecertificeerd

TRANSFER

Oracle producten

- Oracle Platform Security Services (OPSS)
  - Standaard component van Fusion Middleware
  - In WebLogic licentie
  - Authenticatie
  - Keystore Management
  - log-in
  - federatie (SAML)

TRANSFER

Oracle producten

- Oracle Access Management
  - Zeer veelzijdig product
  - Enige concurrent van IBM Tivoli Access Manager
  - Dure licentie
  - Basic licentie als onderdeel van iAS, Forms-Reports en WebLogic Suite licenties, maar enorme installatie overhead voor dat doel
- Oracle Identity Manager
  - Identity Governance
  - Vereist SOA Suite voor workflow
  - Alleen voor corportae Identity Management (>10.000 werknemers)

TRANSFER

CONSULTING | MANAGED SERVICES | EDUCATION

WWW.TRANSFER-SOLUTIONS.COM