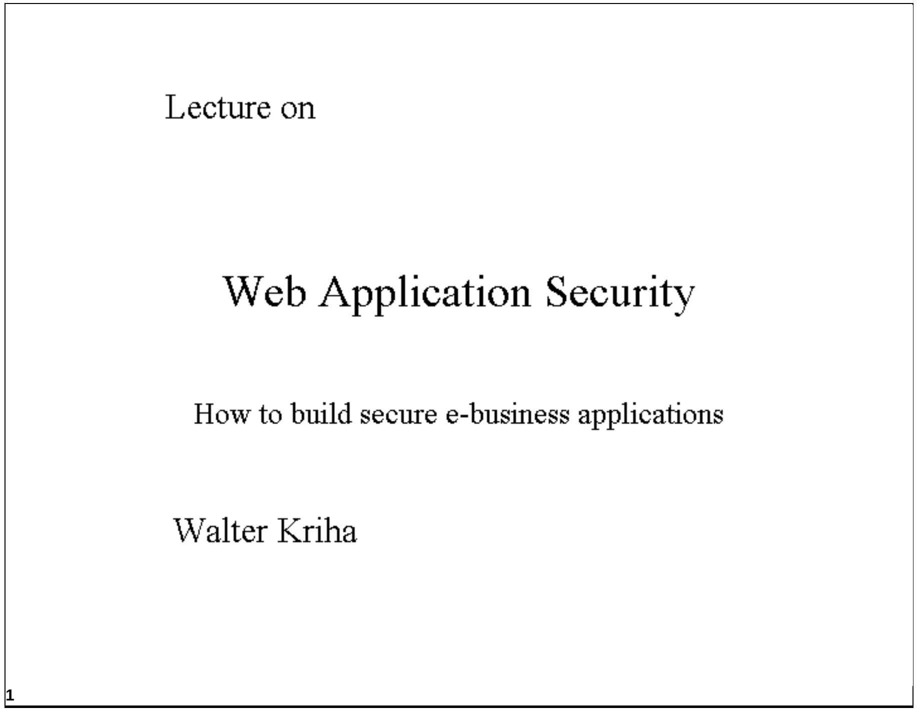
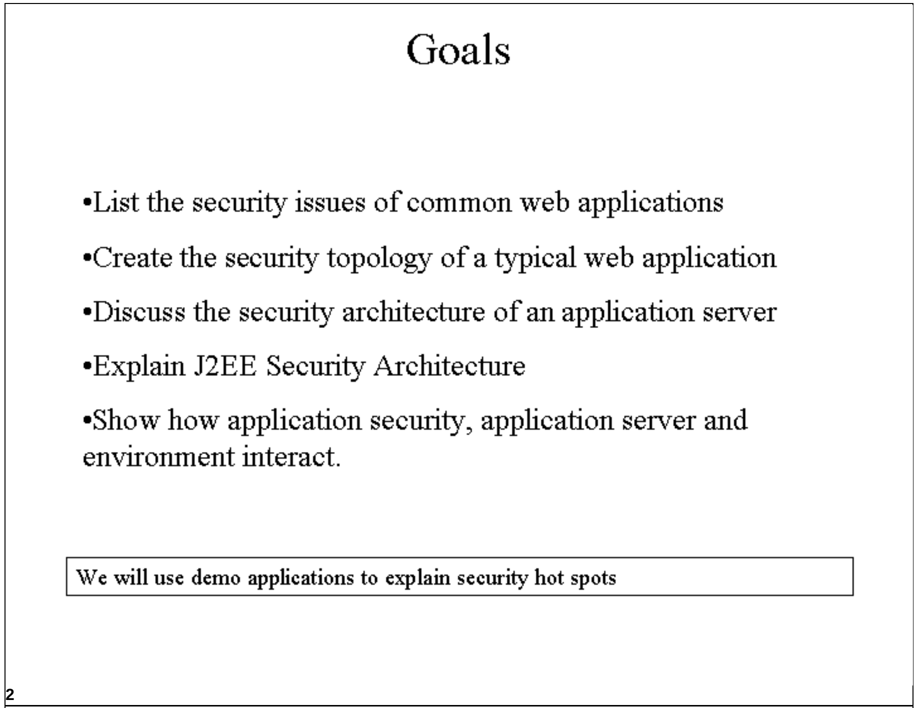


Lecture on

Web Application Security

How to build secure e-business applications

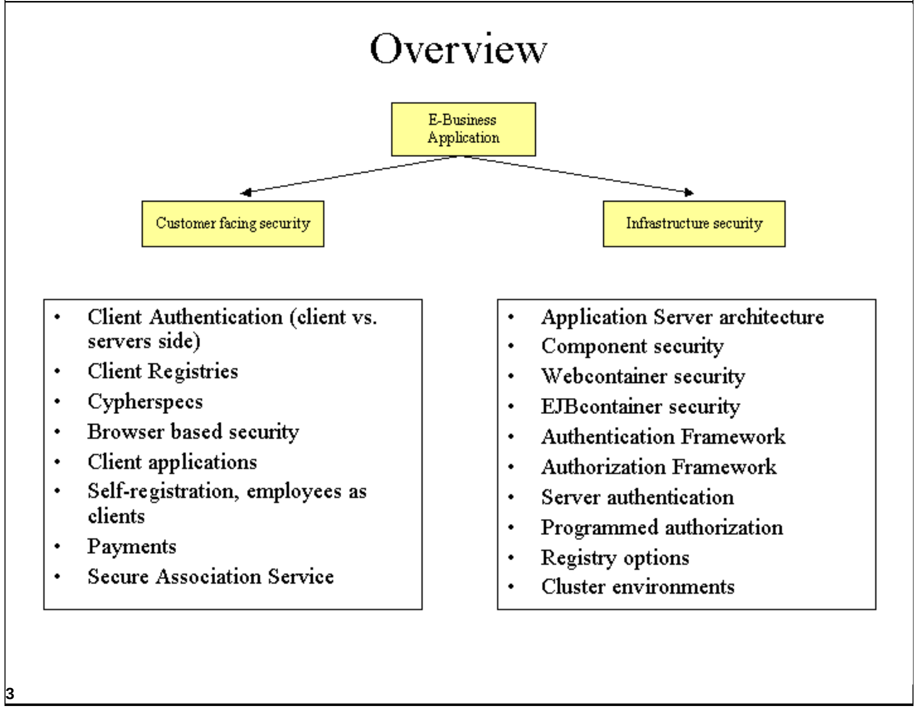
Walter Kriha



Goals

- List the security issues of common web applications
- Create the security topology of a typical web application
- Discuss the security architecture of an application server
- Explain J2EE Security Architecture
- Show how application security, application server and environment interact.

We will use demo applications to explain security hot spots



Overview

- Client Authentication (client vs. servers side)
- Client Registries
- Cypherspecs
- Browser based security
- Client applications
- Self-registration, employees as clients
- Payments
- Secure Association Service

- Application Server architecture
- Component security
- Webcontainer security
- EJBcontainer security
- Authentication Framework
- Authorization Framework
- Server authentication
- Programmed authorization
- Registry options
- Cluster environments

Mechanisms and Technologies

- Java Authentication and Authorization Service (JAAS)
- Java Secure Sockets Extension (JSSE)
- Servlet Security
- Enterprise Java Beans Security
- Public-Key Cryptography Standards (PKCS)
- Java Cryptography Architecture (JCA) and Java Cryptography Extension (JCE)

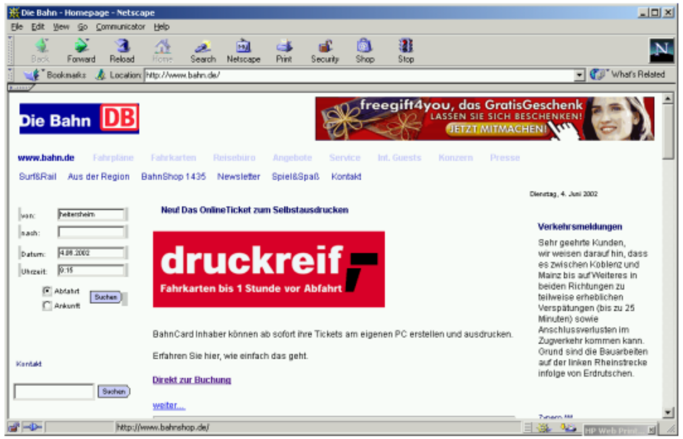
We will not delve into the details of JCA and JCE because the principles should be well known from Security I. But we will look at the others and especially at the role they play in securing an e-business application. An excellent (and short) introduction is: „Security challenges for Enterprise Java in an e-business environment" by Koved et.al. (see resources)

Advanced Infrastructure Architecture

- Single-Sign-On (SSO)
- LDAP based user registries
- User profiles and personalization
- Clustering and virtual servers

Each of these technologies presents a challenge for application builders. We will show how a SSO environment could be built, the problems behind a central user management, how we can achieve personalized services and finally how to do all this FAST by introducing a clustering architecture.

A typical e-business scenario


Die Bahn - Homepage - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: http://www.bahn.de/
What's Related
Die Bahn DB
freegift4you, das GratisGeschenk
LASSEN SIE SICH BESCHENKEN!
JETZT MITMACHEN!
www.bahn.de Fahrpläne Fahrkarten Reisebüro Angebote Service Int. Guests Konzern Presse
Surf&Rail Aus der Region BahnShop 1435 Newsletter Spiel&Spaß Kontakt
druckreif
Fahrkarten bis 1 Stunde vor Abfahrt
Suchen
Kontakt
Suchen
http://www.bahnshop.de/

Dienstag, 4. Juni 2002

von: heitersheim
nach:
Datum: 4.06.2002
Uhrzeit: 9:15
● Abfahrt
○ Ankunft

Neu! Das OnlineTicket zum Selbstausdrucken

BahnCard Inhaber können ab sofort ihre Tickets am eigenen PC erstellen und ausdrucken.

Erfahren Sie hier, wie einfach das geht.

Direkt zur Buchung

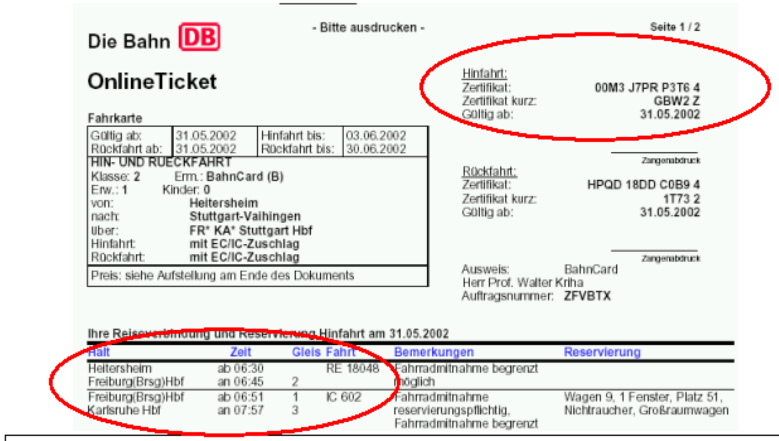
weiter...

Verkehrsmeldungen

Sehr geehrte Kunden, wir weisen darauf hin, dass es zwischen Koblenz und Mainz bis auf Weiteres in beiden Richtungen zu teilweise erheblichen Verspätungen (bis zu 25 Minuten) sowie Anschlussverlusten im Zugverkehr kommen kann. Grund sind die Bauarbeiten auf der linken Rheinstrecke infolge von Erdrutschen.

www.bahn.de, the bahn portal, offers online-tickets as a new service. Customers can print their own tickets and make reservations up to one hour before travel begins. A bahncard and a valid major credit card are requirements. Users need to register for that service and provide registration data.

The online ticket as a crypto problem (1)



- Bitte ausdrucken -

Seite 1 / 2

OnlineTicket

Fahrkarte

Gültig ab: Rückfahrt ab:	31.05.2002 31.05.2002	Hinfahrt bis: Rückfahrt bis:	03.06.2002 30.06.2002

HIN- UND RUECKFAHRT
Klasse: 2 Erm.: BahnCard (B)
Erw.: 1 Kinder: 0
von: Heitersheim
nach: Stuttgart-Vaihingen
über: FR* KA* Stuttgart Hbf
Hinfahrt: mit EC/IC-Zuschlag
Rückfahrt: mit EC/IC-Zuschlag

Preis: siehe Aufstellung am Ende des Dokuments

Hinfahrt:
Zertifikat: 00M3 J7PR P3T6 4
Zertifikat kurz: GBW2 Z
Gültig ab: 31.05.2002

Zangenabdruck

Rückfahrt:
Zertifikat: HPQD 18DD C0B9 4
Zertifikat kurz: 1T73 2
Gültig ab: 31.05.2002

Zangenabdruck

Ausweis: BahnCard
Herr Prof. Walter Kriha
Auftragsnummer: ZFVBTX

Ihre Reiseverbindung und Reservierung Hinfahrt am 31.05.2002

Halt	Zeit	Gleis	Fahrt	Bemerkungen	Reservierung
Heitersheim Freiburg(Brsg)Hbf	ab 06:30 an 06:45	 2	RE 18048	Fahrradmitnahme begrenzt möglich	
Freiburg(Brsg)Hbf Karlsruhe Hbf	ab 06:51 an 07:57	1 3	IC 602	Fahrradmitnahme reservierungspflichtig, Fahrradmitnahme begrenzt	Wagen 9, 1 Fenster, Platz 51, Nichtraucher, Großraumwagen

The conductor inserts the „bahncard into a handheld terminal and reads in the number from the magnetic strip. The ticket contains so called „Zertifikat" information which is also entered. The system sends back the actual travel data which the conductor compares with the printed document. The ticket contains no credit card information. How does the DB prevent abuse of self-made tickets?

The online ticket as a crypto problem (2)

The challenge:

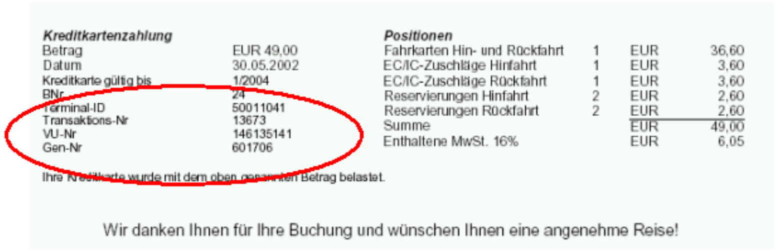
- Any number of copies can be made
- A ticket is valid a couple of days on many different trains on the same route.
- Several people could use ticket copies at the same time
- The ticket could be manipulated in arbitrary ways (e.g. an cheap certificate copied into an expensive ticket)
- People could claim „un-used" tickets by showing new copies without invalidation stamps (which the conductors usually add)

The response:

- An online invalidation through the conductor prevents re-use or concurrent use of used tickets. Daily batch runs could not prevent concurrent use by different travelers
- Certificates guarantee that a ticket has not been manipulated. Requires conductors to compare display information with travel data on ticket.
- The stamps attached by the conductors are merely a sign for colleagues that certain checks have already been performed. Real invalidation is done online.

There are certainly more ways to abuse the system but given the number of tickets and the considerable improvement for travellers this risk seems to be acceptable. The bahn has also taken measures like increasing the fee for returned (unused) tickets enormously. What do you think – is an online ticket theoretically safer than an old-fashioned ticket or not? The above creates security for the bahn: no abuse of tickets. But where did YOUR security go with respect to unused tickets? An unused ticket used to be defined as a ticket without imprints from conductors. But ALL online tickets can be printed again without such imprints. Can you still prove that you did not travel? Will the IRS („Finanzamt") accept online tickets as proof of expenses that occurred?

Interesting back matter



Kreditkartenzahlung	
Betrag	EUR 49,00
Datum	30.05.2002
Kreditkarte gültig bis	1/2004
BNr	24
Terminal-ID	50011041
Transaktions-Nr	13673
VU-Nr	146135141
Gen-Nr	601706

Positionen			
Fahrkarten Hin- und Rückfahrt	1	EUR	36,60
EC/IC-Zuschläge Hinfahrt	1	EUR	3,60
EC/IC-Zuschläge Rückfahrt	1	EUR	3,60
Reservierungen Hinfahrt	2	EUR	2,60
Reservierungen Rückfahrt	2	EUR	2,60
Summe		EUR	49,00
Enthaltene MwSt. 16%		EUR	6,05

Ihre Kreditkarte wurde mit dem oben genannten Betrag belastet.

Wir danken Ihnen für Ihre Buchung und wünschen Ihnen eine angenehme Reise!

Looks like there are a lot of legacy transaction systems involved in generating an online ticket. All these numbers could be keys into different systems for which the portal is merely a frontend. A typical portal problem.

Required Business Organisation

- Conductor training
- Mobile online terminals
- Help Desk for ticket cancellation, change etc.

So far I have noticed the following with respect to the business organization behind online tickets:

-Some conductors do check those tickets using their online terminals, some don't.

-Sometimes a ticket gets checked twice and sometimes not at all (meaning no online check. Instead a conductor looks at the ticket and just imprints it without really checking the validity)

-On certain routes the tickets are never checked through online validation (especially on short trips with local trains)

- If have not tried cancellation of tickets but the web page already says that regular bahn offices will not take unused tickets back.

The rest of the portal

-Train schedule

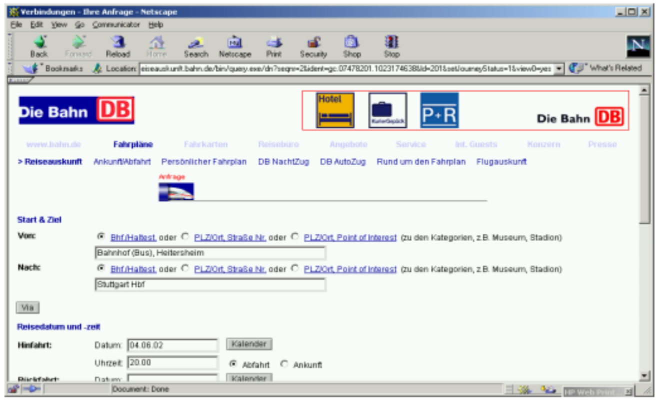
- Registration

-login procedure and personalization

-other services like credits, travel office etc.

In a typical portal manner www.bahn.de offers a lot more than just the online ticket service. Hint: before you start to analyse a portal, change the cookie settings in your browser to „ask for confirmation before allowing cookie" and watch the URL input line carefully to see the differences in page references, e.g. when you are redirected to different hosts etc. Do this BEFORE first contact. This way you can trace state handling by the web application running the portal.

Train schedule


Verbindungen - Ihre Anfrage - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: eiseauskunft.bahn.de/bin/query.exe/dn?seqnr=2&ident=gc.07478201.1023174638&ld=201&sel/ourneyStatus=1&view0=yes
What's Related
Die Bahn DB
Hotel
P+R
Die Bahn DB
www.bahn.de Fahrpläne Fahrkarten Reisebüro Angebote Service Int. Guests Konzern Presse
> Reiseauskunft Ankunft/Abfahrt Persönlicher Fahrplan DB NachtZug DB AutoZug Rund um den Fahrplan Flugauskunft
Anfrage
Document: Done

Start & Ziel

Von: ● Bhf/Haltest. oder ○ PLZ/Ort, Straße Nr. oder ○ PLZ/Ort, Point of Interest (zu den Kategorien, z.B. Museum, Stadion)

Bahnhof (Bus), Heitersheim

Nach: ● Bhf/Haltest. oder ○ PLZ/Ort, Straße Nr. oder ○ PLZ/Ort, Point of Interest (zu den Kategorien, z.B. Museum, Stadion)

Stuttgart Hbf

Via

Reisedatum und -zeit

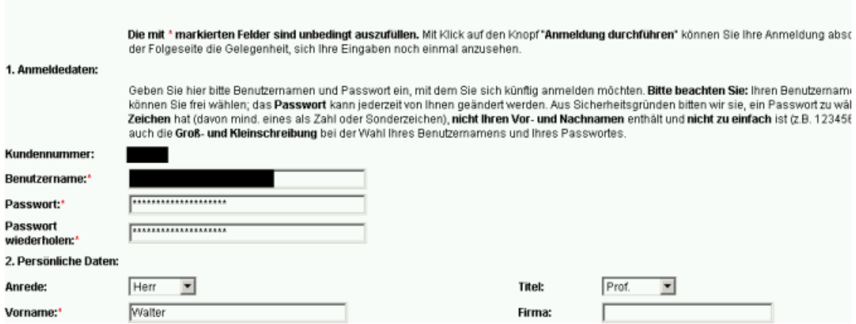
Hinfahrt: Datum: 04.06.02 Kalender

Uhrzeit: 20.00 ● Abfahrt ○ Ankunft

Rückfahrt: Datum: Kalender

The train schedule service runs on a different host and has been offered long before the online ticket. This means that the bahn had to integrate different services to allow booking of online tickets after regular train information queries.

User Registration



Die mit * markierten Felder sind unbedingt auszufüllen. Mit Klick auf den Knopf "Anmeldung durchführen" können Sie Ihre Anmeldung absc der Folgeseite die Gelegenheit, sich Ihre Eingaben noch einmal anzusehen.

1. Anmeldedaten:

Geben Sie hier bitte Benutzernamen und Passwort ein, mit dem Sie sich künftig anmelden möchten. **Bitte beachten Sie:** Ihren Benutzernam können Sie frei wählen; das **Passwort** kann jederzeit von Ihnen geändert werden. Aus Sicherheitsgründen bitten wir sie, ein Passwort zu wäl **Zeichen** hat (davon mind. eines als Zahl oder Sonderzeichen), **nicht Ihren Vor- und Nachnamen** enthält und **nicht zu einfach** ist (z.B. 123456 auch die **Groß- und Kleinschreibung** bei der Wahl Ihres Benutzernamens und Ihres Passwortes.

Kundennummer: [redacted]

Benutzername:* [redacted]

Passwort:* ********************

Passwort wiederholen:* ********************

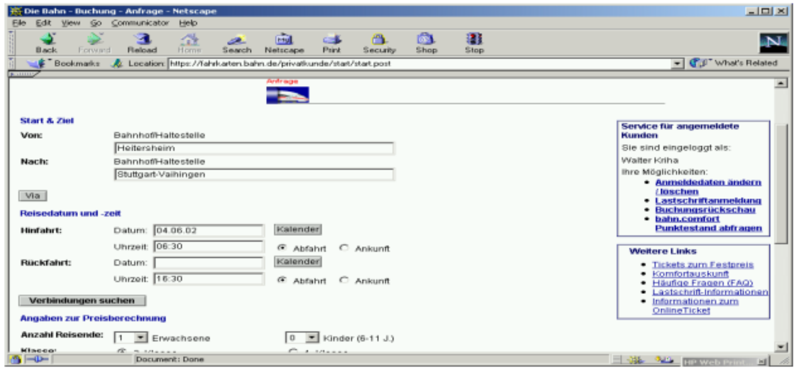
2. Persönliche Daten:

Anrede: Herr Titel: Prof.

Vorname:* Walter Firma:

Users are required to register. They can chose their own user id (if still available) and also a password. All user data are transmitted using SSL, including credit card and bahncard information.

Personalized Information


Die Bahn - Buchung - Anfrage - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: https://fahrkarten.bahn.de/privatkunde/start/start.post
What's Related
Anfrage
Document: Done

Start & Ziel

Von: Bahnhof/Haltestelle

Heitersheim

Nach: Bahnhof/Haltestelle

Stuttgart-Vaihingen

Via

Reisedatum und -zeit

Hinfahrt: Datum: 04.06.02 Kalender

Uhrzeit: 06:30 ● Abfahrt ○ Ankunft

Rückfahrt: Datum: Kalender

Uhrzeit: 16:30 ● Abfahrt ○ Ankunft

Verbindungen suchen

Angaben zur Preisberechnung

Anzahl Reisende: 1 Erwachsene 0 Kinder (6-11 J.)

Service für angemeldete Kunden

Sie sind eingeloggt als:

Walter Kriha

Ihre Möglichkeiten:

- Anmeldedaten ändern / löschen
- Lastschriftanmeldung
- Buchungsrückschau
- bahn.comfort Punktestand abfragen

Weitere Links

- Tickets zum Festpreis
- Komfortauskunft
- Häufige Fragen (FAQ)
- Lastschrift-Informationen
- Informationen zum OnlineTicket

After login the system shows a certain route that a customer can select as default, e.g. if somebody travels frequently along the same route. This reduced the time needed to perform a ticket purchase considerably. But this requires the portal to hold customer preferences. Old purchase can be looked up any time.

Other services

financial services (credits etc.)

Travel office (flights, cars etc.

Die Bahn DB
Für 99 € zur Weltgartenschau "Floriade"
ICE International nach Holland

Those services are performed by other companies or affiliates. This means that customer data needs to be exchanged, especially identification and credit card information. Please note that the travel office on the right side asks for a userid and password again – something clearly not optimal. Portals usually want to provide so called Single Sign-On: a customer registers once and can then use other services as well (if authorized of course). If other businesses are involved there is now a problem of trust between the bahn portal and those businesses with respect to authentication of users.

Possible extensions to the bahn portal

Company accounts:

- Can the travellers delegate the booking to their HR office?
- How can companies define certain company wide standards for travel and location booking?
- Can companies get an account just like users? E.g. to book online tickets for employes which need to go on business trips?
- Can those companies register several people with the right to perform bookings?
- Can these people share travel information?

Public kiosks:

- Can the travellers book such online tickets from public kiosks, e.g. in super markets?

If these become requirements on day – is the web application security able to deal with it? Company accounts with delegation of rights require fine-grained authorizations and access rights. It is quite hard to extend a system that has been built without the notion of company accounts to suppurt them suddenly. The same is true if the input device changes: Does your application have a concept of „location"? E.g. to schedule different session timeout for home browsers vs. public kiosks?

Some thoughts on the business ideas

- The bahncard seems to become the major anchor for all customer related information.
- This goes together with a major PR campaign by the bahn to foster the collection of „bonus points" when the bahncard is show during regular ticket buying.
- The bahncard is not shareable, another hint at its possible quality as a primary key.

Over the next slides we will challenge these assumptions and see what it would mean for our web application architecture. We will try to make a case for separating authentication, authorization and customer segmentation as much as possible from our system to be independent if those things change.

The bahncard – a problem?

The online ticket service seems to be bound to the bahncard number.

- **What happens now with all the bahn employees that want to make a private trip? Do they suddenly all need bahncards simply because the online ticket service needs it?**
- **What happens if one of these days the bahn decides it must make the bahncard shareable? How would this affect the overall authentication and authorization process?**

The web application behind bahn.de

Client side:

- Authentication against portal
- Secure transport of client data to the portal and back.

Server side:

- Authentication against client
- Secure transport of client data to the portal and back.
- Session state handling (http and https)
- Secure transport of information WITHIN portal components
- Authorization and access control
- User registries
- Personalization
- Load-balancing
- Single Sign-On

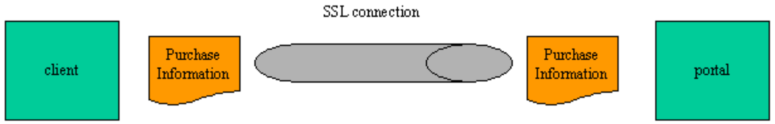
Of course we do not know how bahn.de has been built. For now we just assume that it has been built using a J2EE based web application server with several additional components like security server, reverse proxies, user registries etc. But before we delve into the technical details a word on security requirements is in order.

Client side security requirements

Train schedule	public, http
Registration	confidential, https
Login data	confidential, https
Purchase of ticket	integrity, confidential, https, proof of purchase

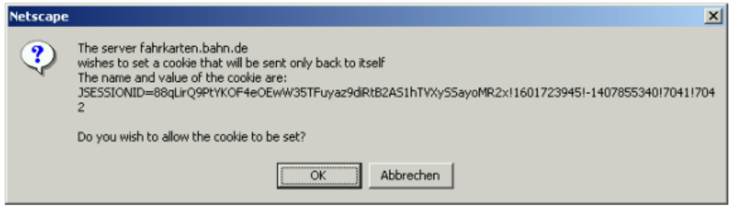
For a first guess at client side security it is usefull to list the information categories and their security requirements which play a role on the client. Most of it is quite standard nowadays. The userid/password mechanism where users can pick their own data requires a pre-established trust e.g. through the previous purchase of a bahncard etc. There might be a window of opportunity if copied bahncard and credit card information is used. Before the victim notices the bills coming in the attacker has long travelled. But this would require a faked bahncard as well.

Passwords, SSL and non-repudiation



SSL does NOT provide non-repudiation on object level. It is a secure transport but after leaving the transport, objects are unprotected. This has nothing to do with SSL using a client certificate to authenticate the client as well. To achieve proof-of-purchase the client would have to digitally sign the purchase request. Used together with encryption the client wouldn't even need an SSL session to transmit the signed purchase request. In our case the bahn decided not to create the PKI infrastructure necessary for the client to sign the purchase request. Since the password is also shared there is little that would proof that a certain request comes from a certain client.

Session State Handling (1)



The server fahrkarten.bahn.de
wishes to set a cookie that will be sent only back to itself
The name and value of the cookie are:
JSESSIONID=88qLirQ9PtYKOF4eOEwW35TFuyaz9diRtB2AS1hTVXySSayoMR2x!1601723945!-1407855340!7041!7042

Do you wish to allow the cookie to be set?

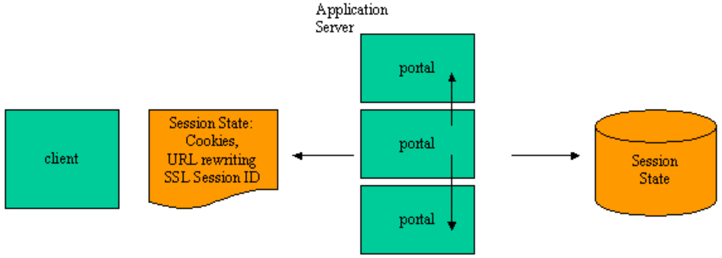
Bahn.de uses cookies to store session state. Strictly speaking session state is part of the information on the client and needs to be secured properly. Cookies are not safe with respect to replay attacks from copies. Cookies over SSL sessions are a little bit better but still a security problem. What happens to existing cookies when the web application switches into SSL mode?

URL rewriting suffers from the problem that only dynamic pages can support it. Any access to a static page in between would lose the session data completely.

High security applications will use the SSL Session ID as the anchor of a client session and tie session information in a database to it.

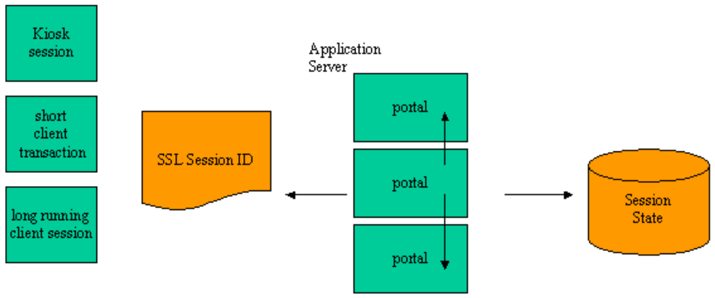
A highly secure environment will not allow cookies to be set by web applications. An intermediate like a reverse proxy can filter all cookie set requests and tie all session information to the SSL Session ID.

Session State Handling (2)



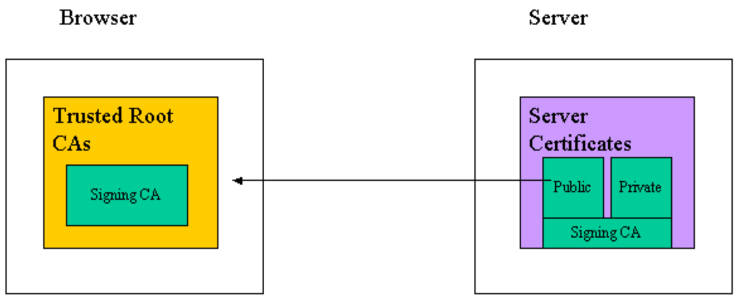
An application server that keeps state becomes a problem for load-balancing or fail-over: Since the session state is only available within the application server all client requests after the first one need to be routed to the same server (server affinity)– thus effectively undermining load-balancing. If the server crashes, the client session is lost. Cookies, URL rewriting or the SSL Session ID are all ways to make the application server stateless again. The session state can also be stored in a database with cookies or Session IDs as keys. This solution even provides fail-over: a crashed session can be resumed by a different application server. Another alternative is to use a special protocol that allows session information to be replicated across application servers.

Session Timeouts



The setting of session timeouts is critical to prevent session takeover or abuse. Unfortunately a portal needs to support different types of applications with different timeout requirements. E.g. a financial advisor package may need timeouts of several hours while a fast e-banking transaction may only require 10 minutes. Special care must be exercised to synchronize session timeouts across components e.g. intermediates like reverse proxies, web-servers and application servers. Services need to get an update if a session is closed to do resource cleanup.

Server authentication



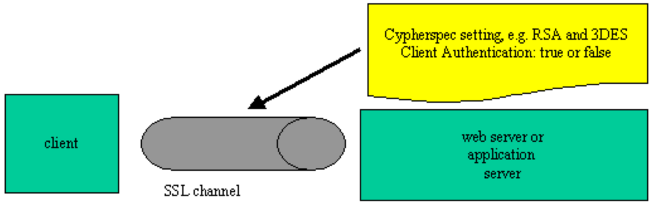
The server needs a PUBLIC certificate from a well-known certificate authority. This public certificate is sent to the browser during the handshake phase of an SSL connection initiation. The browser needs a so called root certificate from the SAME CA where the server got his public certificate. If such a root certificate is available at the browser it can use the public key from the root certificate to validate the public certificate from the server. Otherwise it can still accept the public server certificate but it cannot validate it. This is usually the only place where we will work with real public certificates within the complex structure of a web application. Internal connections will be secured by home-made certificates.

A Certificate Signing Request

1. Create key database to store certificates (pw protected)
2. Create certificate request (supply fully qualified domain name or whatever the target CA wants.)
3. Copy CSR (cert. signing req.) over to CA.
4. Receive .arm file from your CA.
5. Place your now signed certificate into your key database

The exact procedure depends on your choice of tool, e.g. JSSE tools or special web server certificate tools. Please verify the received signed certificate before placing it into your key database.

SSL configuration issues


Cypherspec setting, e.g. RSA and 3DES
Client Authentication: true or false
client
SSL channel
web server or application server

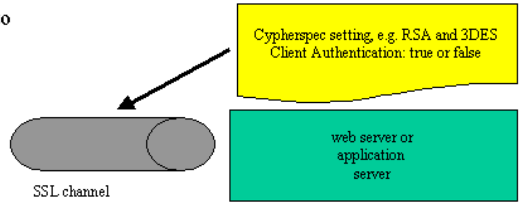
It is the responsibility of the web or application server to set the proper settings with respect to ciphers and client authentication. Beware the defaults: most systems come with settings that will allow basically any form of cipher to be used fo SSL, effectively disabling encryption.

And client authentication needs to be requested from the server or it won't happen – allowing e.g. certain man-in-the-middle attacks.

The problem of defaults exists in almost every server side software: we will find it again if we look at default authorization in LDAP, default security settings in application servers etc.

Testing SSL Configuration

Change your SSL3 settings in your browser to a different cipher specification and try to connect to the web server


Cypherspec setting, e.g. RSA and 3DES
Client Authentication: true or false
web server or application server
SSL channel

After changing your browser settings you should no longer be able to establish an SSL session with the web server because you do not share at least one common cipher specification. BTW: did you ever adjust your browser settings for reasonable cipher specs with respect to SSL?

Building the distributed trusted computing base

The next session will deal exclusively with the server side infrastructure for a large scale web application. We will deal with authentication and authorization frameworks, container security, security services, personalization and Single Sign-on issues.

Resources (1)

- Security challenges for Enterprise Java in an e-business environment, L Koved et.al, http://www.research.ibm.com/journal/sj/401/koved.html
- Introduction to JAAS and Java GSS-API Tutorials http://java.sun.com/j2se/1.4/docs/guide/security/jgss/tutorials/
- For information on the Pluggable Authentication Module, see http://java.sun.com/products/jaas/.
- V. Samar and C. Lai, “Making Login Services Independent of Authentication Technologies,” http://java.sun.com/security/jaas/doc/pam.html. Explains the reasons for an open, externalized authentication framework
- Keith Smith, SSL/TLS in WebSphere: Usage, Configuration and Performance (very good guide to configure component security using SSL connections between all parts)

Resources (2)

- Object Management Group (www.omg.org) Security Service Specification version 1.7, March 2001, 434 pages. Security for adults. Go there for detailed definitions of delegation, distributed security threats, distributed trusted computing base, principals and credentials etc.
- Chandra Kopparak, Load balancing Servers, Firewalls and Caches. Explains how load-balancing, session state handling and security are intertwined. Perfect and short. With clear ip-packet information that shows wherever DNAT or SNAT etc. are performed to achieve load-balancing.