

INFORMATION SECURITY DECISIONS

Hosted by  

# How to Overcome Web Services Security Obstacles

**Dick Mackey**  
SystemExperts Corporation

---

---

---

---

---

---

---

---

INFORMATION SECURITY DECISIONS

Hosted by  

## Agenda

- Introduction to Web Services
- Web Services threats
- Web Services security standards
- What's here today
- What you can do to secure your Web Services

---

---

---

---



---

---


---

---


INFORMATION SECURITY DECISIONS

Hosted by  


## Why Web services?



Display information meant for Web browsers and humans

← Traditional Web → 

Web Services:  
Programmatic Access  
Remote Procedures  
(e.g., Get\_Schedule (person, month, sched);

← SOAP → 

---

---

---

---



---

---

---

---

INFORMATION SECURITY DECISIONS

Hosted by  

## The good and the bad

- Web services are growing in popularity for B2B applications
- The good:
  - Interoperable across platforms and implementations
  - Can be written in many languages – Perl, Java, C, C#, VB...
  - Standard / non-proprietary
  - Building blocks for larger systems
- The bad: convenience leads to security issues

---

---

---

---

---

---



---

---

---

---

INFORMATION SECURITY DECISIONS

Hosted by  

## What are Web services?

- Remote Procedure Call (RPC) services (mostly)
- Offered through web servers / app servers
- Designed to build modular distributed systems
- Extensible (not as "brittle" as previous systems)
- Provide well-defined, language-independent interfaces
- Support standard wire protocols (XML/SOAP)
- Services define interfaces (WSDL)
- Services advertise (UDDI)

---

---

---

---

---

---



---

---


---

---

INFORMATION SECURITY DECISIONS

Hosted by  

## Web services model



```

sequenceDiagram
    participant Client
    participant Server as TToDoService
    Client->>Server: getToDoByDayRequest(day)
    Server-->>Client: getToDoByDayResponse(day)
  
```

---

---

---

---

---

---



---

---

---

---

INFORMATION SECURITY DECISIONS

Hosted by  

## WSDL and SOAP

- **Web Services Definition Language (WSDL)**
  - XML definitions of interfaces
  - Describes SOAP operations or documents to exchange
    - Types
    - Parameters
    - Messages
    - RPCs
- **Simple to build both clients and servers**
  - Can generate stubs or just look at the definition and code accordingly
  - Apache Axis allows you to write a Java class, drop it in a directory, and go
- **Tools support dynamic invocation of operations based on interface definition**

---

---

---

---

---

---



---

---

---

---

INFORMATION SECURITY DECISIONS

Hosted by  

## UDDI

- Universal Description, Discovery, and Integration
- Provides a place to register and find interfaces/services
- UDDI is a web service itself
- Allows services to advertise
- Provides info about your services

---

---

---

---

---

---



---

---

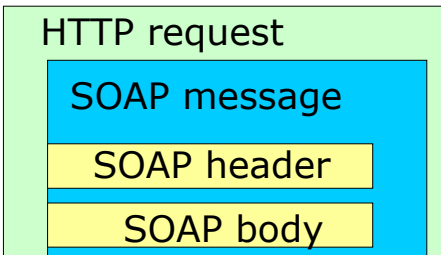
---

---

INFORMATION SECURITY DECISIONS

Hosted by  

## SOAP message anatomy



```

graph TD
    HTTP[HTTP request] --- SOAP[SOAP message]
    SOAP --- SOAP_HEADER[SOAP header]
    SOAP --- SOAP_BODY[SOAP body]
  
```

---

---

---

---

---

---



---

---

---

---

INFORMATION SECURITY DECISIONS

Hosted by  

## SOAP request

```
<?xml version='1.0' ?> <env:Envelope
  xmlns:env="http://www.w3.org/2003/05/soap-envelope" > <env:Header>
<t:transaction xmlns:t="http://thirdparty.example.org/transaction"
  env:encodingStyle="http://example.com/encoding"
  env:mustUnderstand="true" >5</t:transaction> </env:Header>
<env:Body>
<m:chargeReservation env:encodingStyle="http://www.w3.org/2003/05/soap-
encoding" xmlns:m="http://travelcompany.example.org/">
<m:reservation xmlns:m="http://travelcompany.example.org/reservation">
  <m:code>FT35ZBQ</m:code> </m:reservation>
<o:creditCard xmlns:o="http://mycompany.example.com/financial">
<n:name xmlns:n="http://mycompany.example.com/employees"> Dick Mackey
  </n:name>
<o:number>123456789099999</o:number>
<o:expiration>2005-02</o:expiration></o:creditCard>
</m:chargeReservation>
</env:Body></env:Envelope>
```

---

---

---

---

---

---

---

---



---

---

---

---

INFORMATION SECURITY DECISIONS

Hosted by  

## SOAP response

```
<?xml version='1.0' ?>
<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-
envelope" >
<env:Header> <t:transaction
  xmlns:t="http://thirdparty.example.org/transaction"
  env:encodingStyle="http://example.com/encoding"
  env:mustUnderstand="true">5</t:transaction></env:Header>
<env:Body>
<m:chargeReservationResponse
  env:encodingStyle="http://www.w3.org/2003/05/soap-encoding"
  xmlns:m="http://travelcompany.example.org/">
<m:code>FT35ZBQ</m:code>
<m:viewAt> http://travelcompany.example.org/reservations?code=FT35ZBQ
  </m:viewAt>
</m:chargeReservationResponse>
</env:Body>
</env:Envelope>
```

---

---

---

---

---

---

---

---



---

---

---

---

INFORMATION SECURITY DECISIONS

Hosted by  

## Why are Web services dangerous?

- They use web servers and their protocols are allowed through firewalls
- They are flexible and powerful
  - Messages can include attachments (selectively processed)
  - Messages can include attacks at internal weaknesses
  - They are so easy to implement they tempt developers to deploy indiscriminately
- They often do not get the scrutiny web sites do

---

---

---

---

---

---

---

---

---

---

---

---

INFORMATION SECURITY DECISIONS

Hosted by  

## Developing Web services

- There are a variety of tools for developing Web Services
  - Apache Axis
  - Microsoft .NET
  - Sun JaxRPC
- All are interoperable
- All are securable
  - WS Security is available in most environments
  - Apache WSS4J
  - Microsoft .NET Web Service Extensions (WSE)
  - Sun's WS Security for JaxRPC

---

---

---

---



---

---

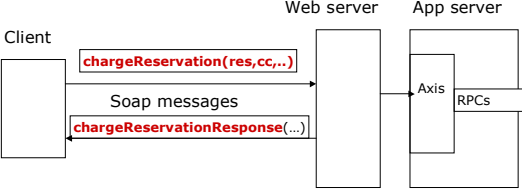
---

---

INFORMATION SECURITY DECISIONS

Hosted by  

## Web services implementation



Web services run inside servlets in an App server

---

---

---

---



---

---

---

---

INFORMATION SECURITY DECISIONS

Hosted by  

## How to make WS safer

- Be aware of threats
- Authenticate connections or methods
- Encrypt sensitive data
- Separate sensitive web services from others
- Take web services seriously: code carefully and avoid mistakes

---

---

---

---


---

---

---

---

INFORMATION SECURITY DECISIONS

Hosted by  

## WS-security

- Defines how authentication and crypto information is carried by SOAP
- Provides authorization support
  - **Claims can be signed**
  - **Authorization can be specific to a domain**
- Supports multiple authentication methods
- Supports multi-party transactions

---

---

---

---



---

---

---

---

INFORMATION SECURITY DECISIONS

Hosted by  

## WS-security (cont.)

- WS-Security defines how security tokens can be included in SOAP messages
  - **XML elements appear in SOAP headers**
  - **Elements define tokens like username, signature**
- Supports tokens for various authentication mechanisms
  - **Kerberos**
  - **Username and password**
  - **Public key**
  - **SAML Tokens**
- Supports confidentiality, authenticity, and integrity of SOAP messages
  - **Message digest**
  - **Digital signature**

---

---

---

---



---

---

---

---

INFORMATION SECURITY DECISIONS

Hosted by  

## Related security specifications

- Secure conversation
  - **Builds on WS-Security to support SSL-like negotiation of conversations**
- WS-Trust
  - **Establishes framework to process security tokens**
  - **Which tokens should a party trust?**
- WS-Federation
  - **Establishes a framework for supporting multiple security domains**
  - **Example: Healthcare, physician, insurance company, pharmacy**

---

---

---

---



---

---

---

---

INFORMATION SECURITY DECISIONS

Hosted by  

## How are WS used today?

- Companies like Google and Amazon support search interfaces
- Travel agencies use WS for pricing
- Many organizations use WS for internal client / server applications – it’s getting to be the method of choice
- Financial organizations use it to support security operations (single sign-on) and partner interactions

---

---

---

---



---

---

---

---

INFORMATION SECURITY DECISIONS

Hosted by  

## What organizations do today

- Most offer unauthenticated services to the public
- When security is necessary, most organizations use SSL (transport security)
- Application authentication
  - **Username and passwords over SSL**
  - **Client side certificates with SSL**
- We haven’t seen anyone using WS-Security (yet)
- SAML is being used for Federation
  - **Multi-company single sign-on**
  - **Authorization**

---

---

---

---



---

---

---

---

INFORMATION SECURITY DECISIONS

Hosted by  

## What can you do?

- Decide what you need to support
  - **Point-to-point authentication (SSL or WS-Security)**
  - **Multi-party or end-to-end (WS-Security or SAML)**
  - **Federation (SAML or WS-Security)**
- Consider building security into the application
  - **Implementations of WS-Security are popping up from Sun, Apache, IBM, Oracle...**
  - **Look into SAML for Federation**
- **Firewall and border products can be useful**
  - **Firewall vendors are building products to look inside SOAP messages to find large attachments and provide direct authentication**
  - **CA Netegrity’s TransactionMinder supports security at the boundary**
  - **DataPower**

---

---

---

---



---

---

---

---

INFORMATION SECURITY DECISIONS

Hosted by  

## In closing

- Web Services are here to stay
- Be careful what you export to the masses
  - **Web services require the same or greater scrutiny as other web interfaces**
- Use solutions that match your development environment
- If buying WS products, make sure you don't leave gaps in your protection
- Be ready to adopt more closely coupled security mechanisms as they become available.

---

---

---

---



---

---

---

---

INFORMATION SECURITY DECISIONS

Hosted by  

## Audience Response

- **Questions?**

---

---

---

---

---

---

---

---