Web Services Security: a preliminary study using Casper and FDR

E. Kleiner and A.W. Roscoe

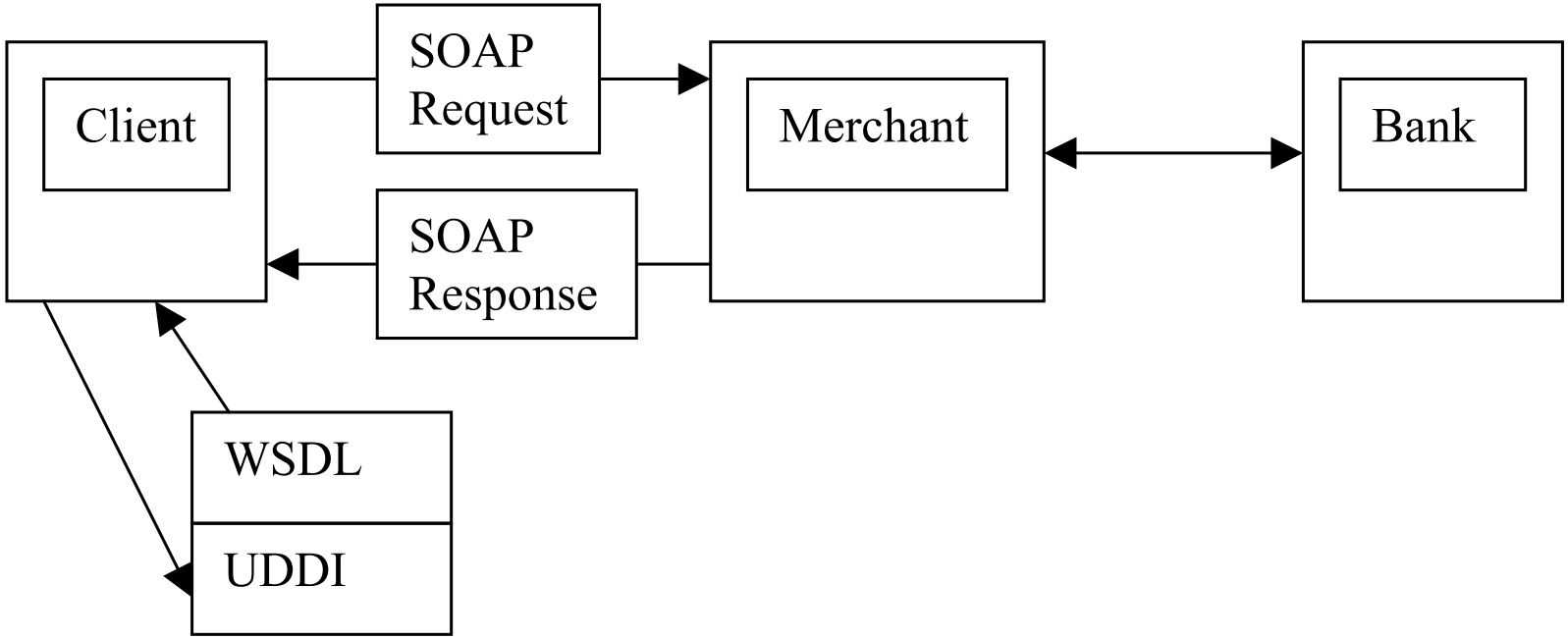
Web Services - a quick overview

Web Services is an XML-based architecture that was developed in order to make the coupling between distributed components looser.

SOAP was defined by Microsoft and DevelopMentor to provide a way to envelop information using XML to exchange it between different computing systems.

With the growth of the popularity and importance of the Web Services architecture, more and more standards have been defined for extending the functionality and for dealing with different concerns.

Web Service - An example implementation



SOAP request example

```
<soap:Envelope xmlns:soap="http://www.w3.org/2001/12/soap-envelope">
   <soap:Header>
   </soap:Header>
   <soap:Body xmlns:Merchant="http://www.merchant.com/buying">
     <Merchant:Buy>
       <Merchant:Item> BasketBall </Merchant:Item>
       <Merchant:Price> 100 </Merchant:Price>
       <Merchant:Bank> HSBC </Merchant:Bank>
     <Merchant:Buy>
   </soap:Body>
 </soap:Envelope>
```

SOAP response example

```
<soap:Envelope xmlns:soap="http://www.w3.org/2001/12/soap-envelope">
   <soap:Header>
   </soap:Header>
   <soap:Body xmlns:Merchant="http://www.merchant.com/Schema">
     <Merchant:BuyResponse>
       <Merchant:Return> Completed successfully</Merchant:Item>
     </Merchant: BuyResponse >
   </soap:Body>
 </soap:Envelope>
```

Web Services Security - an overview

Problems with securing web services with a secure transport layer (ex. SSL):

- SOAP is not bound to a specific transport layer.
- The message is protected only in a secure channel.
- The secure transport layer does not support intermediaries.
- Inefficiency.

Web Services Security specification

Was initially proposed by Microsoft in October 2001.

Defines elements to incorporate security tokens within a SOAP message.

XML-Signature and XML-Encryption are used for achieving integrity and confidentiality for the security tokens.

Message M - taken from an Oasis proposed protocol

```
<Envelope>
 <Header>
  <Security mustUnderstand="1">
   <BinarySecurityToken ValueType="x509v3" Id="myCert"> BV1
   </BinarySecurityToken>
   <Signature>
    <SignedInfo>
     <CanonicalizationMethod Algorithm=.... />
     <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig\#rsa-sha1"/>
     <Reference URI="#body">
      <Transforms>
       <Transform Algorithm=.... />
      </Transforms>
      <DigestMethod Algorithm=... />
      <DigestValue> BV2 </DigestValue>
     </Reference>
    </SignedInfo>
    <SignatureValue> BV3 </SignatureValue>
    <KeyInfo>
     <SecurityTokenReference>
      <Reference URI="#myCert" />
     </SecurityTokenReference>
    </KeyInfo>
   </Signature>
```

```
      <EncryptedKey>
        <EncryptedMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
        <KeyInfo>
          <SecurityTokenReference>
            <KeyIdentifier ValueType="X509v3"> BV4
            </KeyIdentifier>
          </SecurityTokenReference>
        </KeyInfo>
        <CipherData>
          <CipherValue> BV5 </CipherValue>
        </CipherData>
        <ReferenceList>
          <DataReference URI="#enc" />
        </ReferenceList>
      </EncryptedKey>
    </Security>
  </Header>
  <Body  Id="body">
    <EncryptedData Id="enc" Type="http://www.w3.org/2001/04/xmlenc#content">
      <EncryptedMethod Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc" />
      <CipherData>
        <CipherValue> BV6 </CipherValue>
      </CipherData>
    </EncryptedData>
  </Body>
</Envelope>
```

Modelling WS-Security

Construct a mapping ϕ from SOAP messages to Casper input, such that if a WS-security protocol contains the messages $m_1, m_2..., m_n$ then,

1. If an attack is found on $\phi(m_1), \phi(m_2), ..., \phi(m_n)$ then a corresponding attack can be reproduced on $m_1, m_2..., m_n$.
2. If an attack exists on $m_1, m_2, ..., m_n$ then it also exists on $\phi(m_1), \phi(m_2), ..., \phi(m_n)$

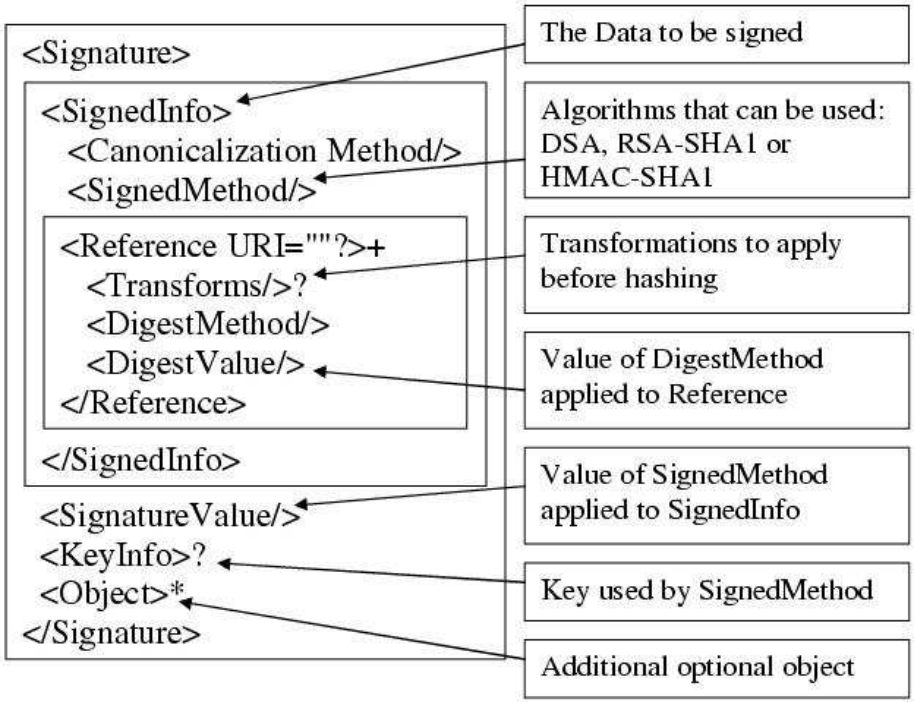
The more important of the above properties is (2), since we definitely do not want to generate a false "proof" of correctness using the translation.

Any attack found by Casper can be translated back to make sure it is really present in the original protocol.

Applying ϕ on a `Security` element

$$\phi(\langle Security\rangle ... \langle /Security\rangle) =$$
$$\phi(\langle BinarySecurityToken\rangle ... \langle /BinarySecurityToken\rangle),$$
$$\phi(\langle EncryptedKey\rangle ... \langle /EncryptedKey\rangle), \phi(\langle Signature\rangle ... \langle /Signature\rangle)$$

Applying ϕ on a `Signature` element



$$\phi(\langle Signature\rangle ... \langle /Signature\rangle) = \{\phi(\langle Reference ...\rangle ... \langle /Reference\rangle), \ldots$$
$$\phi(\langle Reference ...\rangle ... \langle /Reference\rangle) ...\}_{\phi(\langle KeyInfo\rangle ... \langle /KeyInfo\rangle, SIG)}$$

Demonstrate the complete derivation of $\phi(M)$

$\phi(M)$

$\Rightarrow \phi(\langle\text{Header}\rangle...\langle/\text{Header}\rangle),\phi(\langle\text{Body}\rangle...\langle/\text{Body}\rangle)$

$\Rightarrow \phi(\langle\text{Security}\rangle...\langle/\text{Security}\rangle),\phi(\langle\text{Body}\rangle...\langle/\text{Body}\rangle)$

$\Rightarrow \phi(\langle\text{BinarySecurityToken}\rangle...\langle/\text{BinarySecurityToken}\rangle)$,
$\phi(\langle\text{EncryptedKey}\rangle...\langle/\text{EncryptedKey}\rangle)$, $\phi(\langle\text{Signature}\rangle...\langle/\text{Signature}\rangle)$,
$\phi(\langle\text{Body}\rangle...\langle/\text{Body}\rangle)$

$\Rightarrow \phi(\langle\text{EncryptedKey}\rangle...\langle/\text{EncryptedKey}\rangle)$, $\phi(\langle\text{Signature}\rangle...\langle/\text{Signature}\rangle)$,
$\phi(\langle\text{Body}\rangle...\langle/\text{Body}\rangle)$

$\Rightarrow \phi(\langle\text{ReferenceList}\rangle...\langle/\text{ReferenceList}\rangle,\{\text{K}\})$, $\{\text{K}\}_{\phi(\langle\text{KeyInfo}\rangle...\langle/\text{KeyInfo}\rangle,\text{ENC})}$,
$\phi(\langle\text{Signature}\rangle...\langle/\text{Signature}\rangle)$, $\phi(\langle\text{Body}\rangle...\langle/\text{Body}\rangle)$

$\Rightarrow \phi(\langle\text{DataReference URI=\#enc }/\rangle,\{\text{K}\})$, $\{\text{K}\}_{\phi(\langle\text{KeyInfo}\rangle...\langle/\text{KeyInfo}\rangle,\text{ENC})}$,
$\phi(\langle\text{Signature}\rangle...\langle/\text{Signature}\rangle)$, $\phi(\langle\text{Body}\rangle...\langle/\text{Body}\rangle)$

$\Rightarrow \text{Context(enc,\{K\})}$, $\{\text{K}\}_{\phi(\langle\text{KeyInfo}\rangle...\langle/\text{KeyInfo}\rangle,\text{ENC})}$, $\phi(\langle\text{Signature}\rangle...\langle/\text{Signature}\rangle)$,
$\phi(\langle\text{Body}\rangle...\langle/\text{Body}\rangle)$

$\Rightarrow \text{Context(enc,\{K\})}$, $\{\text{K}\}_{\phi(\langle\text{SecurityTokenReference}\rangle...\langle/\text{SecurityTokenReference}\rangle,\text{ENC})}$,
$\phi(\langle\text{Signature}\rangle...\langle/\text{Signature}\rangle)$, $\phi(\langle\text{Body}\rangle...\langle/\text{Body}\rangle)$

$\Rightarrow \text{Context(enc,\{K\})}$, $\{\text{K}\}_{\phi(\langle\text{KeyIdentifier}\rangle...\langle/\text{KeyIdentifier}\rangle,\text{ENC})}$,
$\phi(\langle\text{Signature}\rangle...\langle/\text{Signature}\rangle)$, $\phi(\langle\text{Body}\rangle...\langle/\text{Body}\rangle)$

$\Rightarrow \text{Context(enc,\{K\})}$, $\{\text{K}\}_{\text{PK(B)}}$, $\{\phi(\langle\text{Reference URI=\#body}\rangle...\langle/\text{Reference}\rangle)\}$,

$\{\phi(\langle \text{KeyInfo}\rangle \ldots \langle/\text{KeyInfo}\rangle), \text{SIG}\}, \phi(\langle \text{Body}\rangle \ldots \langle/\text{Body}\rangle)$

$\Rightarrow \text{Context}(\text{enc}, \{\text{K}\}), \{\text{K}\}_{\text{PK(B)}},$
$\{\phi(\langle \text{DigestMethod} \ldots /\rangle)(\phi(\text{body}))\}_{\phi(\langle \text{KeyInfo}\rangle \ldots \langle/\text{KeyInfo}\rangle, \text{SIG})}, \phi(\langle \text{Body}\rangle \ldots \langle/\text{Body}\rangle)$

$\Rightarrow \text{Context}(\text{enc}, \{\text{K}\}), \{\text{K}\}_{\text{PK(B)}}, \{\text{sha1}(\phi(\text{body}))\}_{\phi(\langle \text{KeyInfo}\rangle \ldots \langle/\text{KeyInfo}\rangle, \text{SIG})},$
$\phi(\langle \text{Body}\rangle \ldots \langle/\text{Body}\rangle)$

$\Rightarrow \text{Context}(\text{enc}, \{\text{K}\}), \{\text{K}\}_{\text{PK(B)}},$
$\{\text{sha1}(\{\text{Body}\}_{\phi(\langle \text{EncryptedData Id=“enc”}\rangle \ldots \langle/\text{EncryptedData}\rangle)})\}_{\phi(\langle \text{KeyInfo}\rangle \ldots \langle/\text{KeyInfo}\rangle, \text{SIG})},$
$\phi(\langle \text{Body}\rangle \ldots \langle/\text{Body}\rangle)$

$\Rightarrow \text{Context}(\text{enc}, \{\text{K}\}), \{\text{K}\}_{\text{PK(B)}}, \{\text{sha1}(\{\text{Body}\}_{\text{K}})\}_{\phi(\langle \text{KeyInfo}\rangle \ldots \langle/\text{KeyInfo}\rangle, \text{SIG})},$
$\phi(\langle \text{Body}\rangle \ldots \langle/\text{Body}\rangle)$

$\Rightarrow$
$\text{Context}(\text{enc}, \{\text{K}\}), \{\text{K}\}_{\text{PK(B)}},$
$\{\text{sha1}(\{\text{Body}\}_{\text{K}})\}_{\phi(\langle \text{SecurityTokenReference}\rangle \ldots \langle/\text{SecurityTokenReference}\rangle, \text{SIG})},$
$\phi(\langle \text{Body}\rangle \ldots \langle/\text{Body}\rangle)$

$\Rightarrow \text{Context}(\text{enc}, \{\text{K}\}), \{\text{K}\}_{\text{PK(B)}}, \{\text{sha1}(\{\text{Body}\}_{\text{K}})\}_{\phi(\langle \text{Reference URI=\#myCert} \ldots /\rangle, \text{SIG})},$
$\phi(\langle \text{Body}\rangle \ldots \langle/\text{Body}\rangle)$

$\Rightarrow \text{Context}(\text{enc}, \{\text{K}\}), \{\text{K}\}_{\text{PK(B)}}, \{\text{sha1}(\{\text{Body}\}_{\text{K}})\}_{\text{SK(A)}}, \phi(\langle \text{Body}\rangle \ldots \langle/\text{Body}\rangle)$

$\Rightarrow \text{Context}(\text{enc}, \{\text{K}\}), \{\text{K}\}_{\text{PK(B)}}, \{\text{sha1}(\{\text{Body}\}_{\text{K}})\}_{\text{SK(A)}}, \{\text{Body}\}_{\text{K}}$

$\Rightarrow \{\text{K}\}_{\text{PK(B)}}, \{\text{sha1}(\{\text{Body}\}_{\text{K}})\}_{\text{SK(A)}}, \{\text{Body}\}_{\text{K}}$

Oasis proposed protocol

1. A→B: `M`
2. B→A: `M'`

After applying ϕ to both of the messages we get the following protocol.

1. MSG 1 .A→B : $\{K\}_{PK(B)}$, $\{sha1(\{Body\}_K)\}_{SK(A)}$, $\{Body\}_K$
2. MSG 2. B→A : $\{K2\}_{PK(A)}$, $\{sha1(\{Body2\}_{K2})\}_{SK(B)}$, $\{Body2\}_{K2}$

An attack

Using FDR the following authentication attack was found.

1. MSG 1. $\mathrm{I} \rightarrow \mathrm{Bob} : \{\mathrm{K}\}_{\mathrm{PK(Bob)}}, \{\mathrm{sha1}(\{\mathrm{Body}\}_{\mathrm{K}})\}_{\mathrm{SK(I)}}, \{\mathrm{Body}\}_{\mathrm{K}}$
2. MSG 2. $\mathrm{Bob} \rightarrow \mathrm{I} : \{\mathrm{K2}\}_{\mathrm{PK(I)}}, \{\mathrm{sha1}(\{\mathrm{Body2}\}_{\mathrm{K2}})\}_{\mathrm{SK(Bob)}}, \{\mathrm{Body2}\}_{\mathrm{K2}}$
3. MSG 1. $\mathrm{Alice} \rightarrow \mathrm{I}_{Bob} : \{\mathrm{K3}\}_{\mathrm{PK(Bob)}}, \{\mathrm{sha1}(\{\mathrm{Body3}\}_{\mathrm{K3}})\}_{\mathrm{SK(Alice)}}, \{\mathrm{Body3}\}_{\mathrm{K3}}$
4. MSG 2. $\mathrm{I}_{Bob} \rightarrow \mathrm{Alice} : \{\mathrm{K2}\}_{\mathrm{PK(Alice)}}, \{\mathrm{sha1}(\{\mathrm{Body2}\}_{\mathrm{K2}})\}_{\mathrm{SK(Bob)}}, \{\mathrm{Body2}\}_{\mathrm{K2}}$

Future work

- Present a complete proof of ϕ's properties.
- We are interested in "internalising" potential intermediaries in order to be able to model and check protocols with arbitrary number of intermediaries.
- We will need to study what precise inferences we can draw for the WS-Security implementation in cases where Casper either finds no attacks on a small model or proves a protocol more generally.

Thanks!