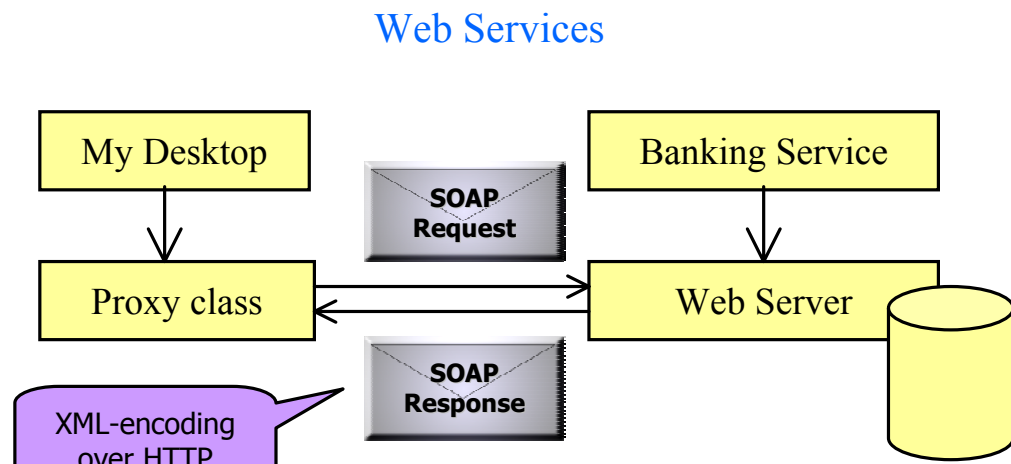


Security Abstractions for Web Services

Riccardo Pucella (Cornell University) and Andy Gordon (Microsoft Research)



Security Choices

- SSL transport
 - Encrypts all traffic between client and server
 - Firewall cannot monitor messages
 - Routers cannot forward messages
- Application-level, or do-it-yourself security

Declarative Security

[van Doorn et al, 1996]

Alternative

- SOAP-level security
- Avoids problems with SSL
 - Avoids dependency on HTTP

Translation to Cryptyc

- (Cryptyc = Spi-calculus + correspondence assertions)
- Translate object calculus expressions into Cryptyc
 - Implement abstraction using protocols
 - Web service invocation = exchange of 4 messages
 - Prove that translated expressions type-check
 - Cryptyc type theory ensure security guarantees [Gordon, Jeffrey, 2001]



Object Calculus Formalization

Values $u, v ::= x \mid null \mid new\ c(v_1, \dots, v_n) \mid p$
 Bodies $a, b ::= v \mid let\ x = a\ in\ b \mid if\ u=v\ then\ a\ else\ b \mid v.f \mid v.l(u_1, \dots, u_n) \mid w.l(u_1, \dots, u_n) \mid q[a]$
 Operational semantics $a \rightarrow^p b$

Captures the essence of C# + Security annotations

C# + Security Annotations

```
class BankingService {
    Identity CallerId;

    [WebMethod]
    [SecurityLevel(Level=AuthEnc)]
    public int Balance (int account) {
        if (account==12345 &&
            CallerId=="Alice")
            return 100
        else
            ...
    }
}
```

Caller/callee authentication
 integrity
 at-most-once semantics
 encryption (secrecy)

caller

Protocols Implementing Abstractions

p invoking $l(u_1, \dots, u_n)$ on web service w owned by q with result r :

$p \rightarrow q$	$CertEK_p$
$p \leftarrow q$	$CertEK_q, \{nK\}_{EK_p, nq}$
$p \rightarrow q$	$\{w, p, t, K, nK\}_{EK_q, np}, \{l(u_1, \dots, u_n), t, nq\}_K$
$p \leftarrow q$	$\{r, t, np\}_K$

Visual Studio .NET Implementation

```
<?xml version='1.0' encoding='utf-8'?>
<soap:Envelope xmlns:soap='http://schemas.xmlsoap.org/soap/envelope/'
  xmlns:xsi='http://www.w3.org/2001/XMLSchema-instance'
  xmlns:xsd='http://www.w3.org/2001/XMLSchema'>
  <soap:Header>
    <DSHeader xmlns='http://tempuri.org/'>
      <callerid>Alice</callerid>
      <calleeid>Bob</calleeid>
      <np>13</np>
      <nq>-1</nq>
      <signature>4E:00:6F:00</signature>
    </DSHeader>
  </soap:Header>
  <soap:Body>
    9D:8F:95:2B:BC:60:B1:73:A7:C4:82:F5:39:20:97:F7:69:71:66:
    D3:A3:A0:90:B9:9B:FE:71:0A:65:C1:EF:EE:99:CB:4D:8A:40:37:
    CA:1E:D0:03:50:34:76:8C:E3:F3:30:DD:C9:34:19:D4:04:CB:39:
    ...
  </soap:Body>
</soap:Envelope>
```