

Biztonságos SOAP vs. Python

avagy ki hajol le a szappanért

Veres-Szentkirályi András
vsza@silentsignal.hu

budapest.py
2012-02-29

SOAP



<http://www.flickr.com/photos/pollas/4454688806/>

SOAP biztonság – jelszavas auth: UsernameToken

```
<soap:Envelope xmlns:soap="...">
  <soap:Header>
    <wsse:Security xmlns:wsse="..." xmlns:wsu="..."
      soap:mustUnderstand="1">
      <wsse:UsernameToken wsu:Id="UsernameToken-3">
        <wsse:Username>admin</wsse:Username>
        <wsse:Password Type="...#PasswordDigest">
          fTI7fNcwD69Z3d0T1bYfvSbQPb8=</wsse:Password>
        <wsse:Nonce EncodingType="...#Base64Binary">
          1DLfpq3fLJ508Dlnr4blQ==</wsse:Nonce>
        <wsu:Created>2011-05-05T17:20:22.319Z</wsu:Created>
      </wsse:UsernameToken>
    </wsse:Security>
  </soap:Header>
  <soap:Body>
    ...
  </soap:Body>
</soap:Envelope>
```

SOAP biztonság – időbélyegzés

```
<soap:Envelope xmlns:soap="...">
  <soap:Header>
    <wsse:Security xmlns:wsse="..." xmlns:wsu="..."
      soap:mustUnderstand="1">
      <wsu:Timestamp wsu:Id="TS-3">
        <wsu:Created>2012-02-27T15:54:28.096Z</wsu:Created>
        <wsu:Expires>2012-02-27T15:59:28.096Z</wsu:Expires>
      </wsu:Timestamp>
      ...
    </wsse:Security>
  </soap:Header>
  <soap:Body>
    ...
  </soap:Body>
</soap:Envelope>
```

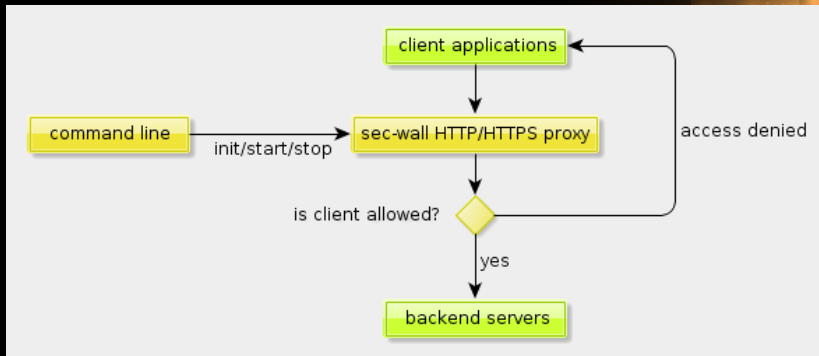
SOAP biztonság – aláírás

```
<wsse:Security mustUnderstand="true"><s:Signature xmlns:s="...">
  <s:SignedInfo>
    <s:CanonicalizationMethod Algorithm=".../xml-exc-c14n#" />
    <s:SignatureMethod Algorithm=".../xmldsig#dsa-sha1" />
    <s:Reference URI="#id-581ce77d-1483-4362-ab5b-95ebf814c75f">
      <s:Transforms><s:Transform Algorithm=".../xml-exc-c14n#" />
      </s:Transforms>
      <s:DigestMethod Algorithm=".../xmldsig#sha1" />
      <s:DigestValue>...DBC0g=</s:DigestValue>
    </s:Reference> ...
  </s:SignedInfo>
  <s:SignatureValue>...NvMQ1EA==</s:SignatureValue>
  <s:KeyInfo><wsse:SecurityTokenReference>
    <s:X509Data><s:X509IssuerSerial>
      <s:X509IssuerName>CN=Arena</s:X509IssuerName>
      <s:X509SerialNumber>1321699512</s:X509SerialNumber>
    </s:X509IssuerSerial></s:X509Data>
  </wsse:SecurityTokenReference></s:KeyInfo>
</s:Signature></wsse:Security>
```

SOAP biztonság – E2E titkosítás

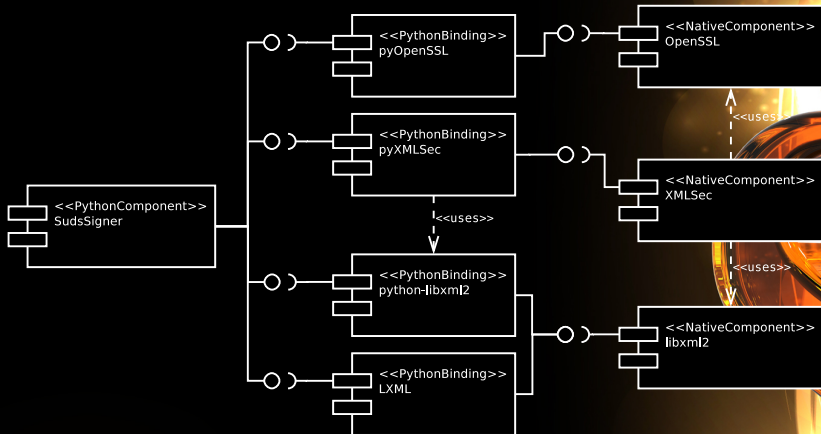
„Jager, Tibor and Juraj, Somorovsky –
How to break XML encryption”,
CCS '11 Proceedings of the 18th ACM conference
on Computer and communications security,
ACM New York, ISBN 1-450-30948-6

Python szerver megoldás – sec-wall



<http://sec-wall.gefira.pl/>

Python kliens megoldás – SUDS



Összefoglalás

- ▶ SUDS: funkcionálisan teljes kliens implementáció
- ▶ sec-wall: részleges szerver implementáció
- ▶ szabad szoftveres projektek, contributions welcome
- ▶ flamebait: életképes a Python – SOAP páros?



Köszönöm a figyelmet!

<https://github.com/dnet>

<http://silentsignal.hu>