

BitFlip: Determine a Data's Signature Coverage from within the Application

OWASP 23.06.2010 Henrich C. Pöhls Institute of IT-Security and Security Law University of Passau, Germany hp@sec.uni-passau.de +498515093217

Copyright © The OWASP Foundation Permission is granted to copy, distribute and/or modify this document under the terms of the OWASP License.

The OWASP Foundation

me, myself and this talk

- ► M.Sc. Information Security from Royal Holloway
- Diplom Informatik from University of Hamburg
- Currently PhD student at University of Passau



ReSCUe IT:

- General: IT supported robust & secure Supply Chains
- Our Goal: Legally compliant & manageable integrity and authenticity statements for the data

Institute of IT-Security and Security Law

Henrich C. Pöhls



Outline

Problem & Motivation

■ BitFlip Approach

■ What BitFlip is not ...

■ What BitFlip can do ... example XML-wrapping

■ Conclusion

Institute of IT-Security and Security Law

Henrich C. Pöhls



Problem: Message Security Layer vs. Application Layer

Design is layered

Application Layer

- Application logic works on data
- Data comes in by message
 - Application extracts data from message
- Security layer protects message (or part thereof)
 - Signed messages are verified before given to app.

Layered Security:

interlinking between layers must stay "in-sync"





Example: XML SOAP message security

Available security mechanism for SOAP messages:

- WS-Security (Tokens ...)
- XML Signature (and Encryption)
- Security checks considered "good practice":
- well defined XML schema
- rigorous schema validation
- validity check of signing public-key
- enforce strict security policies



Henrich C. Pöhls



Example: XML SOAP message security

Available security mechanism for SOAP messages:

- WS-Security (Tokens ...)
- XML Signature (and Encryption)
- Security checks considered "good practice":
- well defined XML schema
- rigorous schema validation
- validity check of signing public-key
- enforce strict security policies
- ... but attacks on real world web services happen.





Authenticate not just the message, but everything that is used to determine the meaning of the message.

Ferguson and Schneier



Henrich C. Pöhls



```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds=
<soap:Header>
<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-ws
<soap:Body Id="1">
<nds:return_hash> <!--Optional:-->
<nds:name>?fffd g</nds:name>
</nds:return_hash>
</soap:Body>
</soap:Header>
<soap:Body>
<nds:return_hash> <!--Optional:-->
<nds:name>evilHomer</nds:name>
</nds:return_hash>
</soap:Body>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#"><SignedInfo>
<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-2/
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<Reference URI="#xpointer(id('1'))"><Transforms>
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<DigestMethod
```

Algorithm="http://www.w3.org/2000/00/xmldsig#sha1"/~DigestValue>zci/05E3D6E

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds=
<soap:Header>
<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-ws
<soap:Body Id="1">
<nds:return_hash> <!--Optional:-->
<nds:name>?fffd g</nds:name>
</nds:return_hash>
</soap:Body>
</soap:Header>
<soap:Body>
<nds:return_hash> <!--Optional:-->
<nds:name>evilHomer</nds:name>
</nds:return_hash>
</soap:Body>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#"><SignedInfo>
<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-2/
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<Reference URI="#xpointer(id('1'))"> Transforms>
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<DigestMethod
```

Algorithm="http://www.w2.org/2000/00/xmldsig#sha1"/~DigestValue>zgi/05E3D6I

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
```

<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds= <soap:Header>

<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-ws

<soap:Body Id="1"> <nds:return_hash> <!--Optional:--> <nds:name>?fffd g</nds:name> </nds:return_hash> </soap:Body> <nds:return_hash> <!--Optional:--> <nds:return_hash> <!--Optional:--> <nds:name>evilHomer</nds:name> </nds:return_hash> </soap:Body>

<Signature xmlns="http://www.w3.org/2000/09/xmldsig#"><SignedInfo>

<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20

<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>

<Reference URI="#xpointer(id('1'))"> (Transforms>

<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/> <DigestMethod

Algorithm="http://www.w2.org/2000/00/xmldsig#sha1"/~DigestValue>zoi/05E2D6I

<?xml version="1.0" encoding="UTF-8" standalone="no"?>

<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds= <soap:Header>

<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-ws

<soap:Body Id="1"> <nds:return_hash> <!--Optional:--> <nds:name>?fffd g</nds:name> </nds:return_hash>

</soap:Body>

</soap:Header>

<soap:Body>

<nds:return_hash> <!--Optional:-->

<nds:name>evilHomer</nds:name>

</nds:return_hash>

</soap:Body>

<Signature xmlns="http://www.w3.org/2000/09/xmldsig#"><SignedInfo>

<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20

<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>

<Reference URI="#xpointer(id('1'))"> (Transforms>

<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/> <DigestMethod

Algorithm="http://www.w2.org/2000/00/xmldsig#sha1"/~DigestValue>zgi/05E3D6I

<?xml version="1.0" encoding="UTF-8" standalone="no"?>

<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds= <soap:Header>

<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss

<soap:Body Id="1"> <nds:return_hash> <!--Optional:--> <nds:name>?fffd g</nds:name>

- </nds:return_hash>
- </soap:Body>

</soap:Header>

<soap:Body>

<nds:return_hash> <!--Optional:--> <nds:name>evilHomer</nds:name> /

</nds:return_hash>

</soap:Body>

<Signature xmlns="http://www.w3.org/2000/09/xmldsig#"><SignedInfo>

<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-2/

<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>

<Reference URI="#xpointer(id('1'))"> Transforms>

<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/> <DigestMethod

Algorithm_"http://www.w2.org/2000/00/zmldsig#sha1"/5_DiggstValue>zoi405E2D6

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
```

<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds= <soap:Header>

<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-ws <soap:Body Id="1">

<nds:return_hash> <!--Optional:-->

<nds:name>?fffd g</nds:name>

</nds:return_hash>

</soap:Body>

</soap:Header>

<soap:Body>

<nds:return_hash> <!--Optional:-->

<nds:name>evilHomer</nds:name>

</nds:return_hash>

</soap:Body>

<Signature xmlns="http://www.w3.org/2000/09/xmldsig#"><SignedInfo>

<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-2001/REC-xml-c140/REC-xml-c140-2001/REC-xml-c14n-2001/REC-xml-c140/REC-xml-c140/RE

<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>

<Reference URI="#xpointer(id('1'))"><Transforms>

<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/> <DigestMethod

Algorithm="http://www.w3.org/2000/00/xmldsig#sha1"/~DigestValue>zgi/05E3D6L

SOAP message example is from:

Meiko Jensen Ruhr Universität Bochum

<?xml version="1.0" encoding="UTF-8" standalone="no"> <soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds="ht <soap:Header>

<wse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-w <soap:Body Id="1">

<nds:return_hash><!--Optional:->

<nd column (in the second secon

Signaturewieurou Angonumi nup.//www.wo.org/2000/07/Annusig#15a-511a1 // <Reference URI="#xpointer(id('1'))"><Transforms>

Chrene Content and Content

Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>zcj495F3P6R1C ZW5Tybl01u0BGmB3Z9IJ4mlXwBcQhBuGc0IPobt3E10sMSIcGVd7X3gzjynhdTYyC 5mRp5GvrDk/659Nu+xk=</SignatureValue>KeyInfo><X509Data><X509SubjectNan CBMDYmF5MQswCQYDVQQHEwJwYTEQMA4GA1UEChMHcHJpdmF0ZTELM BAMTB61hdHQwHhcNMTAwNTE4MTA1MDA4WbcNMTAwODE2MTA1MDA4







<?xml version="1.0" encoding="UTF-8" standalone="no"> <soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds="ht <soap:Header>

<wse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-w <soap:Body Id="1">

<nds:return_hash><!--Optional:->

<nd column (in the second secon

Signaturewieurou Angonumi nup.//www.wo.org/2000/07/Annusig#15a-511a1 // <Reference URI="#xpointer(id('1'))"><Transforms>

Chrene Content and Content

Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>zcj495F3P6R1C ZW5Tybl01u0BGmB3Z9IJ4mlXwBcQhBuGc0IPobt3E10sMSIcGVd7X3gzjynhdTYyC 5mRp5GvrDk/659Nu+xk=</SignatureValue>KeyInfo><X509Data><X509SubjectNan CBMDYmF5MQswCQYDVQQHEwJwYTEQMA4GA1UEChMHcHJpdmF0ZTELM BAMTB61hdHQwHhcNMTAwNTE4MTA1MDA4WhcNMTAwODE2MTA1MDA4







<?xml version="1.0" encoding="UTF-8" standalone="no"> <soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds="ht <soap:Header>

<wse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-w <soap:Body Id="1">

<nd:return_hash><!--Optional:->

<nd:return_hash> <!--Option
</p>
<sid: name>?fffd g</nds:nam
</p>
<sid: return_hash>
</sid: sid: return_hash>

<2001</p>

Signature/returned Augonatini – http://www.woorg/2000/07/Augostg#15a-Sulat // <Reference URI="#xpointer(id('1'))"><Transforms>

<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/></T <DigestMethod

Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>zcj495F3P6R1C ZW5Tybl01u0BGmB3Z9IJ4mlXwBcQhBuGc0IPobt3E10sMSIcGVd7X3gzjynhdTYyC 5mRp5GvrDk/659Nu+xk=</SignatureValue><KeyInfo><X509Data><X509SubjectNan CBMDYmF5MQswCQYDVQQHEwJwYTEQMA4GA1UEChMHcHJpdmF0ZTELM BAMTB61hdHQwHhcNMTAwNTE4MTA1MDA4WhcNMTAwODE2MTA1MDA4 BitFlip: controlled change of single character



<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/></T <DigestMethod

Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>zcj495F3P6R1C ZW5Tybl01u0BGmB3Z9UJ4mlXwBcQhBuGc0IPobt3E10sMSIcGVd7X3gzjynhdTYyC 5mRp5GvrDk/659Nu+xk=</SignatureValue><KeyInfo><X509Data><X509SubjectNan CBMDYmF5MQswCQYDVQQHEwJwYTEQMA4GA1UEChMHcHJpdmF0ZTELM BAMTBG1hdHQwHhcNMTAwNTE4MTA1MDA4WhcNMTAw0DE2MTA1MDA4



Institute of IT-Security and Security Law



<?xml version="1.0" encoding="UTF-8" standalone="no" >-<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds="ht <soap:Header>

<wse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-w <soap:Body Id="1">

<ndsreturn_hash> <!--Optional:->

<nd column line column

Signature/returned Augonaum – http://www.woorg/2000/07/Augostg#15a-sna1 // <Reference URI="#xpointer(id('1'))"><Transforms>

<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/></T <DigestMethod

Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>zcj495F3P6R1C ZW5Tybl01u0BGmB3Z9IJ4mlXwBcQhBuGc0IPobt3E10sMSIcGVd7X3gzjynhdTYyC 5mRp5GvrDk/659Nu+xk=</SignatureValue>KeyInfo><X509Data><X509SubjectNan CBMDYmF5MQswCQYDVQQHEwJwYTEQMA4GA1UEChMHcHJpdmF0ZTELM BAMTB61hdHQwHhcNMTAwNTE4MTA1MDA4WhcNMTAwODE2MTA1MDA4 BitFlip: controlled change of single character <?xml version="1.0" encoding="UTF-8" standalone="no">>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds="ht <soap:Header>

<wse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-w <soap:Body Id="1">

<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/></T</p>

Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>zcj495F3P6R1C ZW5Tybl01u0BGmB3Z9IJ4mlXwBcQhBuGc0IPobt3E10sMSIcGVd7X3zgiynhdTYyC 5mRp5GvrDk/659Nu+xk=</SignatureValue><KeyInfo><X509Data><X509SubjectNan CBMDYmF5MQswCQYDVQQHEwJwYTEQMA4GA1UEChMHcHJpdmF0ZTELM BAMTBG1hdHQwHhcNMTAwNTE4MTA1MDA4WhcNMTAwODE2MTA1MDA4





Institute of IT-Security and Security Law



<?xml version="1.0" encoding="UTF-8" standalone="no" >-<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds="ht <soap:Header>

<wse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-w <soap:Body Id="1">

Signature/neurod Argonalmi – nup//www.woorg/2000/07/Annusig#isa-sita1 // <Reference URI="#xpointer(id('1'))"><Transforms>

<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/></T <DigestMethod

Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>zcj495F3P6R1C ZW5Tybl01u0BGmB3Z9IJ4mlXwBcQhBuGc0IPobt3E10sMSIcGVd7X3gzjynhdTYyC 5mRp5GvrDk/659Nu+xk=</SignatureValue><KeyInfo><X509Data><X509SubjectNan CBMDYmF5MQswCQYDVQQHEwJwYTEQMA4GA1UEChMHcHJpdmF0ZTELM BAMTB61hdHQwHhcNMTAwNTE4MTA1MDA4WhcNMTAwODE2MTA1MDA4 BitFlip: controlled change of single character <?xml version="1.0" encoding="UTF-8" standalone="no"?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds="hi <soap:Header>
<wses:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-w <soap:Body Id='1'>
<nds:retum hash><!-->

<nd:name>?fffd g</nds:name>
</so
</so
return_hash> <!--Option
</so
</cd>

chaname>?fffd g</nds:name
</so
</pre>
chaname>?fffd g</nds:name
</pre>
carreturn_hash> -2001

<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/></T</p>

Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>zcj495F3P6R1C ZW5Tybl01u0BGmB3Z9IJ4mlXwBcQhBuGc0IPobt3E10sMSIcGVd7X3gzjynhdTYyC 5mRp5GvrDk/659Nu+xk=</SignatureValue><KeyInfo><X509Data><X509SubjectNan CBMDYmF5MQswCQYDVQQHEwJwYTEQMA4GA1UEChMHcHJpdmF0ZTELM BAMTB61hdHQwHhcNMTAwNTE4MTA1MDA4WbcNMTAwODE2MTA1MDA4

Signature Verification





Henrich C. Pöhls



<?xml version="1.0" encoding="UTF-8" standalone="no" >-<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds="ht <soap:Header>

<wse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-w <soap:Body Id="1">

Signature/recurod Argonann- http://www.woorg/2000/07/Annusig#isa-sha1 //
<Reference URI="#xpointer(id('1'))"><Transforms>

<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/></T <DigestMethod

Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>zcj495F3P6R1C ZW5Tybl01u0BGmB3Z9IJ4mlXwBcQhBuGc0IPobt3E10sMSIcGVd7X3gzjynhdTYyC 5mRp5GvrDk/659Nu+xk=</SignatureValue><KeyInfo><X509Data><X509SubjectNan CBMDYmF5MQswCQYDVQQHEwJwYTEQMA4GA1UEChMHcHJpdmF0ZTELM BAMTB61hdHQwHhcNMTAwNTE4MTA1MDA4WhcNMTAwODE2MTA1MDA4 BitFlip: controlled change of single character <?xml version="1.0" encoding="UTF-8" standalone="no">
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds="ht
soap:Header>
<wses:Security xmlns:wsee="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-w
<soap:Body Id='1'>
<mses:Security xmlns:wsee="http://docs.oasis-open.org/wss/2004/01/oasis-2004/01-wss-w
<soap:Body Id='1'>
<mses:Security xmlns:wsee="http://docs.oasis-open.org/wss/2004/01/oasis-2004/01-wss-w
<soap:Body Id='1'>
<mses:Security xmlns:wsee="http://docs.oasis-open.org/wss/2004/01/oasis-2004/01-wss-w
<soap:Body Id='1'>
<mses:Security xmlns:wsee="http://docs.oasis-open.org/wss/2004/01/oasis-2004/01-wss-w
<soap:Body Id='1'>
</mses:Security xmlns:wsee="http://docs.oasis-open.org/wss/2004/01-wss-w
</mses:Security xmlns:wsee">soap:Body Id='1'>
</mses:Security xmlns:wsee="http://docs.oasis-open.org/wss/2004/01-wss-w
</mses:Security xmlns:wsee">soap:Body Id='1'>
</mses:Security xmlns:wsee
</mses:Security xmlns:wsee="mainto-open.org/wss/2004/

<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/></T <DigestMethod

Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>zcj495F3P6R1C ZW5Tybl01u0BGmB3Z9IJ4mlXwBcQhBuGc0IPobt3E10sMSIcGVd7X3gzjynhdTYyC 5mRp5GvrDk/659Nu+xk=</SignatureValue><KeyInfo><X509Data><X509SubjectNan CBMDYmF5MQswCQYDVQQHEwJwYTEQMA4GA1UEChMHcHJpdmF0ZTELM BAMTBG1hdHQwHhcNMTAwNTE4MTA1MDA4WhcNMTAwODE2MTA1MDA4

Signature Verification





Henrich C. Pöhls







Henrich C. Pöhls



<?xml version="1.0" encoding="UTF-8" standalone="no" >-<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds="ht <soap:Header>

<wse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-w <soap:Body Id="1">

Signature/returned Argonaum – http://www.woorg/2000/07/Annusig#isa-shat // <Reference URI="#xpointer(id('1'))"><Transforms>

<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/></T <DigestMethod

Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>zcj495F3P6R1C ZW5Tybl01u0BGmB3Z9IJ4mlXwBcQhBuGc0IPobt3E10sMSIcGVd7X3gzjynhdTYyC 5mRp5GvrDk/659Nu+xk=</SignatureValue><KeyInfo><X509Data><X509SubjectNan CBMDYmF5MQswCQYDVQQHEwJwYTEQMA4GA1UEChMHcHJpdmF0ZTELM BAMTB61hdHQwHhcNMTAwNTE4MTA1MDA4WhcNMTAwODE2MTA1MDA4 BitFlip: controlled change of single character <?xml version="1.0" encoding="UTF-8" standalone="no">
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds="ht
soap:Header>
<wses:Security xmlns:wsee="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-w
<soap:Body Id='1'>
<mses:Security xmlns:wsee="http://docs.oasis-open.org/wss/2004/01/oasis-2004/01-wss-w
<soap:Body Id='1'>
<mses:Security xmlns:wsee="http://docs.oasis-open.org/wss/2004/01/oasis-2004/01-wss-w
<soap:Body Id='1'>
<mses:Security xmlns:wsee="http://docs.oasis-open.org/wss/2004/01/oasis-2004/01-wss-w
<soap:Body Id='1'>
<mses:Security xmlns:wsee="http://docs.oasis-open.org/wss/2004/01/oasis-2004/01-wss-w
<soap:Body Id='1'>
</mses:Security xmlns:wsee="http://docs.oasis-open.org/wss/2004/01-wss-w
</mses:Security xmlns:wsee">soap:Body Id='1'>
</mses:Security xmlns:wsee="http://docs.oasis-open.org/wss/2004/01-wss-w
</mses:Security xmlns:wsee">soap:Body Id='1'>
</mses:Security xmlns:wsee
</mses:Security xmlns:wsee="mainto-open.org/wss/2004/

<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/></T <DigestMethod

Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>zcj495F3P6R1C ZW5Tybl01u0BGmB3Z9IJ4mlXwBcQhBuGc0IPobt3E10sMSIcGVd7X3gzjynhdTYyC 5mRp5GvrDk/659Nu+xk=</SignatureValue><KeyInfo><X509Data><X509SubjectNan CBMDYmF5MQswCQYDVQQHEwJwYTEQMA4GA1UEChMHcHJpdmF0ZTELM BAMTBG1hdHQwHhcNMTAwNTE4MTA1MDA4WhcNMTAwODE2MTA1MDA4

Signature Verification VERIFIED





Henrich C. Pöhls



<?xml version="1.0" encoding="UTF-8" standalone="no"?> <?xml version="1.0" encoding="UTF-8" standalone="no"?> <soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds="http://www.w3.org/2003/05/soap-envelope" xmlns:nds="http://www <soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds="http://www.w3.org/2003/05/soap-envelope" xmlns:nds="http://www <soap:Header> <soap:Header> <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-w <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-w <soap:Body Id="1"> <soap:Body Id="1"> <nds:return hash> <!--Optional:--> <nds:return_hash> < !--Optional:--> <nds:name>?fffd g</nds:name> </nd </so **return_hash> <!--Option</pre> BitFlip: and name>?fffd g</nds:nam sidename>?fffd A</nds:nam</pre> controlled i:return_hash> <Si <catherefore a contract of the second s -2001 -2001 change of ICINICUIOU //IZOTIUIIII- IIUU.//WWW.WJ.012/2000/07/AIIII03/2#18a-501a1 // <Re <Reference URI="#xpointer(id('1'))"><Transforms> <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/></T <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/></T single <DigestMethod <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>zcj495F3P6R1C Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>zcj495F3P6R1C ZW5Tybl01u0BGmB3Z9IJ4mlXwBcQhBuGc0IPobt3E10sMSIcGVd7X3gzjynhdTYyC ZW5Tybl01u0BGmB3Z9IJ4mlXwBcQhBuGc0IPobt3E10sMSIcGVd7X3gzjynhdTYyQ character 5mRp5GvrDk/659Nu+xk=</SignatureValue><KeyInfo><X509Data><X509SubjectNan 5mRp5GvrDk/659Nu+xk=</SignatureValue><KeyInfo><X509Data><X509SubjectNan CBMDYmF5MQswCQYDVQQHEwJwYTEQMA4GA1UEChMHcHJpdmF0ZTELM CBMDYmF5MQswCQYDVQQHEwJwYTEQMA4GA1UEChMHcHJpdmF0ZTELM BAMTBG1hdHQwHhcNMTAwNTE4MTA1MDA4WhcNMTAwODE2MTA1MDA4 BAMTBG1bdHOwHbcNMTAwNTE4MTA1MDA4WbcNMTAwODE2MTA1MDA4 **Result:** character covered Signature Signature Verification Verification VERIFIED



Henrich C. Pöhls



```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds=
<soap:Header>
<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-ws
<soap:Body Id="1">
<nds:return_hash> <!--Optional:-->
<nds:name>?fffd g</nds:name>
</nds:return_hash>
</soap:Body>
</soap:Header>
<soap:Body>
<nds:return_hash> <!--Optional:-->
<nds:name>evilHomer</nds:name>
</nds:return_hash>
</soap:Body>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#"><SignedInfo>
<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-2/
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<Reference URI="#xpointer(id('1'))"><Transforms>
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<DigestMethod
```

Algorithm="http://www.w3.org/2000/00/xmldsig#sha1"/~DigestValue>zci/05E3D6L

xml version="1.0" encoding="UTF-8</th <th>3" standalone="no"?></th> <th></th>	3" standalone="no"?>				
<soap:envelope td="" xm<="" xmlns:soap="http://ww</td><td>w.w3.org/2003/05/soap-envelope"><td>lns:nds=</td></soap:envelope>	lns:nds=				
<soap:header></soap:header>					
<wsse:security 1"="" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss</td></tr><tr><td><soap:Body Id="></wsse:security>				Not covered by Signature	
<nds:return_hash> <!--Optional:--></nds:return_hash>	Covered by Signature				
<nds:name>?fffd g</nds:name>					
	XML file is corrupt				
	Signature couldn't be found				
<soap:body></soap:body>	Internals from JAVA verify process:				
<nds:return_hash> <!--Optional:--></nds:return_hash>	javax.xml.crypto.dsig.XMLSignature				
<nds:name>evilHomer</nds:name>	Marshal Exception				
	Nullpointer while				
	unmarsnaling				
<signature xmlns="http://www.w3.org/2000/09/xmldsig#"><signedinfo></signedinfo></signature>					
<canonicalizationmethod 09="" 2000="" algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20</td></tr><tr><td colspan=5><SignatureMethod Algorithm=" http:="" www.w3.org="" xmldsig#rsa-sha1"=""></canonicalizationmethod>					
<reference uri="#xpointer(id('1'))"><transforms></transforms></reference>					
<transform algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"></transform> <					
<digestmethod< td=""></digestmethod<>					
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/> <digestvalue>zci495F3P6R</digestvalue>					

xml version="1.0" encoding="UTF-8<br <soap:envelope docs<="" http:="" th="" xmlns:soap="http://ww
<soap:Header>
<wsse:Security xmlns:wsse="><th>8" standalone="no"?> /w.w3.org/2003/05/soap-envelope" xmlns: s.oasis-open.org/wss/2004/01/oasis-200401</th><th>nds=</th></soap:envelope>	8" standalone="no"?> /w.w3.org/2003/05/soap-envelope" xmlns: s.oasis-open.org/wss/2004/01/oasis-200401	nds=		
<soap:body id="1"> <nds:return_hash> <!--Optional:--> <nds:name>?fffd g</nds:name></nds:return_hash></soap:body>	Not covered by Signature Covered by Signature			
 	XML file is corrupt Signature couldn't be found			
 <soap:body> <nds:return_hash> <!--Optional:--> <nds:name>evilHomer</nds:name> </nds:return_hash> </soap:body>	Internals from JAVA verify process: javax.xml.crypto.dsig.XMLSignature Marshal Exception Nullpointer while unmarshaling			
<signature xmlns="http://www.w3.org/2000/09/xmldsig#"><signedinfo> <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20</td></signedinfo></signature>				

<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/> <Reference URI="#xpointer(id('1'))"><Transforms>

<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/><DigestMethod</td>

Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>zci495F3P6R

xml version="1.0" encoding="UTF-8"<br <soap:envelope no"?="" xmlns:soap="http://www</th><th>standalone="> .w3.org/2003/05/soap-envelope</soap:envelope>	e" xmlns:nds=					
<soap:header></soap:header>						
<wsse:security 1"="" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss</td></tr><tr><td><soap:Body Id="></wsse:security>						
<nds:return_hash> <!--Optional:--> <nds:name>?fffd g</nds:name> </nds:return_hash> 	Application logic extracts: soap:Envelope\soap:Body \nds:return_hash\nds:name = "evilHomer"					
<soap:body></soap:body>	BitFlip Test on:					
<nds:return_hash> <!--Optional:--></nds:return_hash>	soap:Envelope\soap:Body					
<nds:name>evilHomer</nds:name>	\nds:return_hash\nds:name					
	= not covered					
<signature xmlns="http://www.w3.org/2000/09/xmldsig#"><signedinfo></signedinfo></signature>						

<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20 <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>

<Signature/vietnou Argonum= "http://www.w5.org/2000/09/xmidsig#rsa-shar"
<Reference URI="#xpointer(id('1'))"><Transforms>

<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/><DigestMethod</td>

Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>zci495F3P6R

What BitFlip does NOT and can NOT offer ...

BitFlip does not do "positive verification":

no assurance that the parts that seem covered are secured against all kinds of attacks

does not check for exploits in the signature verification process

■ is not a "fuzzer"





What BitFlip does ...

- detects absence of integrity protection ("white spots")
- works independently of signature verification process ("black-box")
- implemented on application level
 - application controlled
 - ▶ use same "parser logic" to select flipping data
- absence can be detected by a single "flip"
 - overhead of one additional signature verification





BitFlip: Conclusion

- Allows Applications to test if Signature Verification Process covers the data the application logic extracted
- Independent of Verification Process (black-box)
 - Full Verification not necessary if no black-box
- Tool to evaluate the Verification Process
 - detect errors during application design
 - testing the layers below before application roll-out
 - re-run tests after changes to the policy or the verification process



Henrich C. Pöhls

