Technologien & Sicherheitsaspekte im Cloud Computing

Jörg Schwenk
Horst Görtz Institute
Ruhr-University Bochum

München, 4. Februar 2010

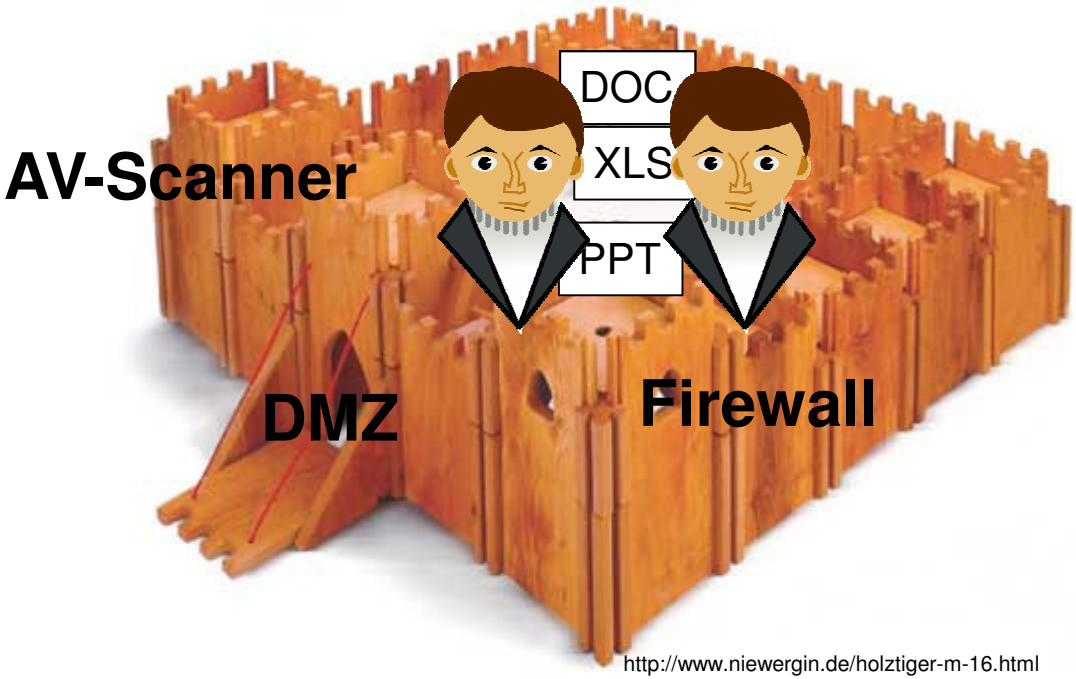
Überblick

1. Die wirklichen Bedrohungen im Cloud Computing
2. Der Webbrowser als universelle Client-Software in der Cloud
3. Webservices: Die Sprache der Cloud
4. Single Sign On
5. Ausblick: Was noch zu tun ist

hgi
Horst-Görtz Institut
für IT Sicherheit

Die wirklichen Bedrohungen im Cloud Computing

Heute: Daten und Nutzer innerhalb der Burgmauern



http://www.niewergin.de/holztiger-m-16.html

Horst-Görtz Institut für IT Sicherheit

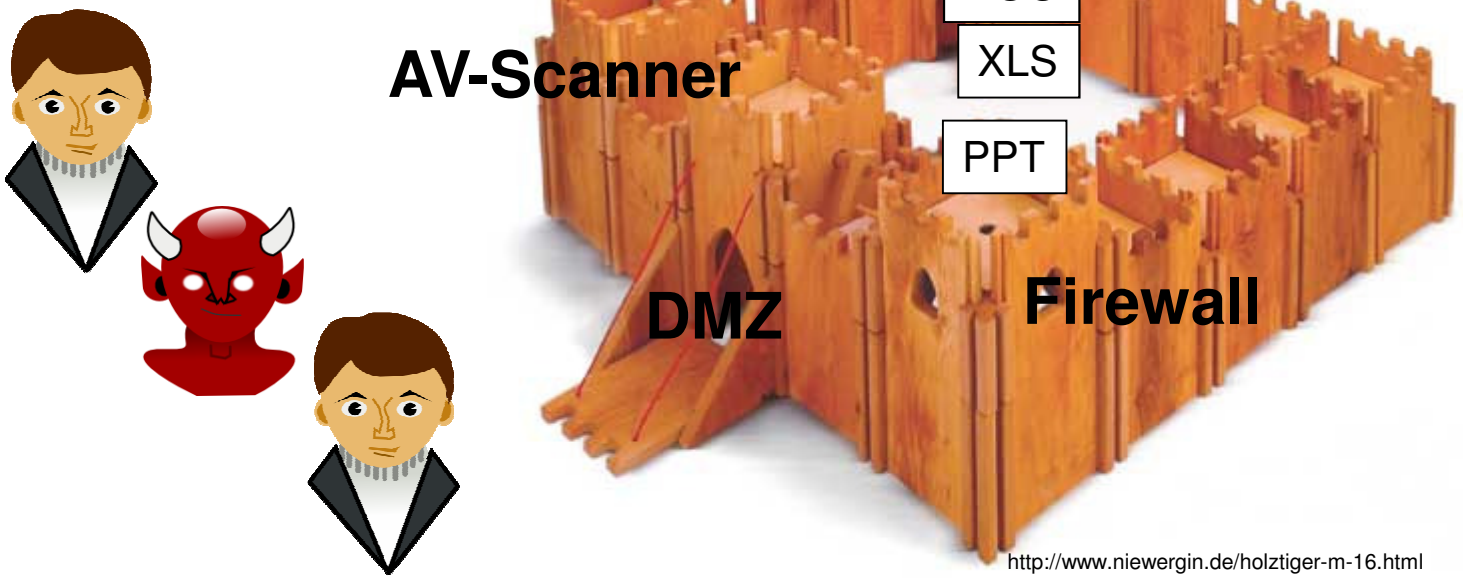
Die wirklichen Bedrohungen im Cloud Computing

Heute: Daten und Nutzer innerhalb der Burgmauern

- Physikalischer Zugang zum Intranet wird immer stärker reglementiert (z.B. Deaktivierung von USB)
- Firewalls, DMZ, etc. schützen die Daten vor externem Zugriff
- AV-Scanner und IDS spüren unerwünschte Eindringlinge auf
- Schwache Authentifikation (Passwörter) im Intranet
- Zugang für Außendienstmitarbeiter über starke, schwer zu konfigurierende Techniken (IPSec-VPN, OTP, ...)

Die wirklichen Bedrohungen im Cloud Computing

Cloud Computing: Nutzer und Angreifer außerhalb der Burg



http://www.niewergin.de/holztiger-m-16.html

Die wirklichen Bedrohungen im Cloud Computing

Cloud Computing: Nutzer und Angreifer außerhalb der Burg

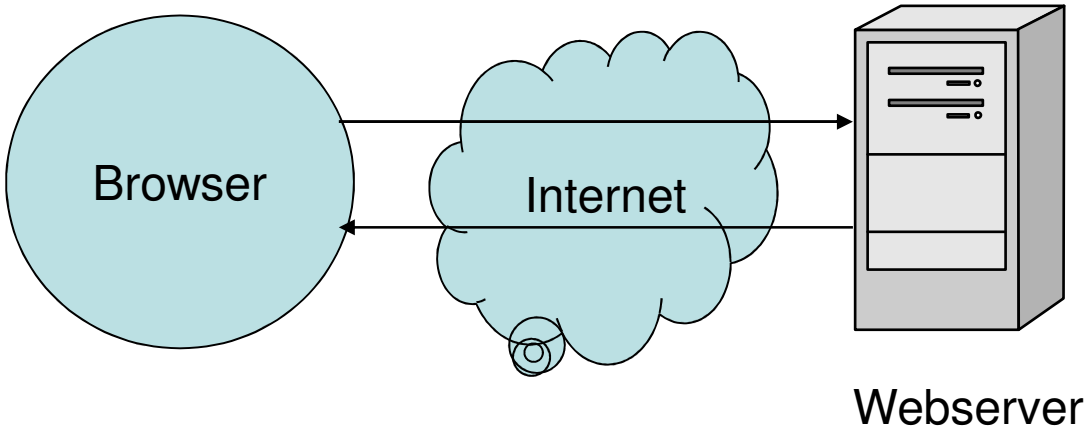
- Gleicher physikalischer Zugang zum „Intranet“ der Cloud für Nutzer und Angreifer
- Firewalls, DMZ, etc. schützen die Daten nicht mehr vor externem Zugriff
- Sicherheit der Daten im Cloud RZ: Verträge, SLAs
- Zugang für alle Mitarbeiter (und alle Angreifer) über (schwache?) leicht zu konfigurierende Techniken (Passwörter, Single-Sign-On, ...)
- Sicherheit der Identität = Sicherheit der Daten

Überblick

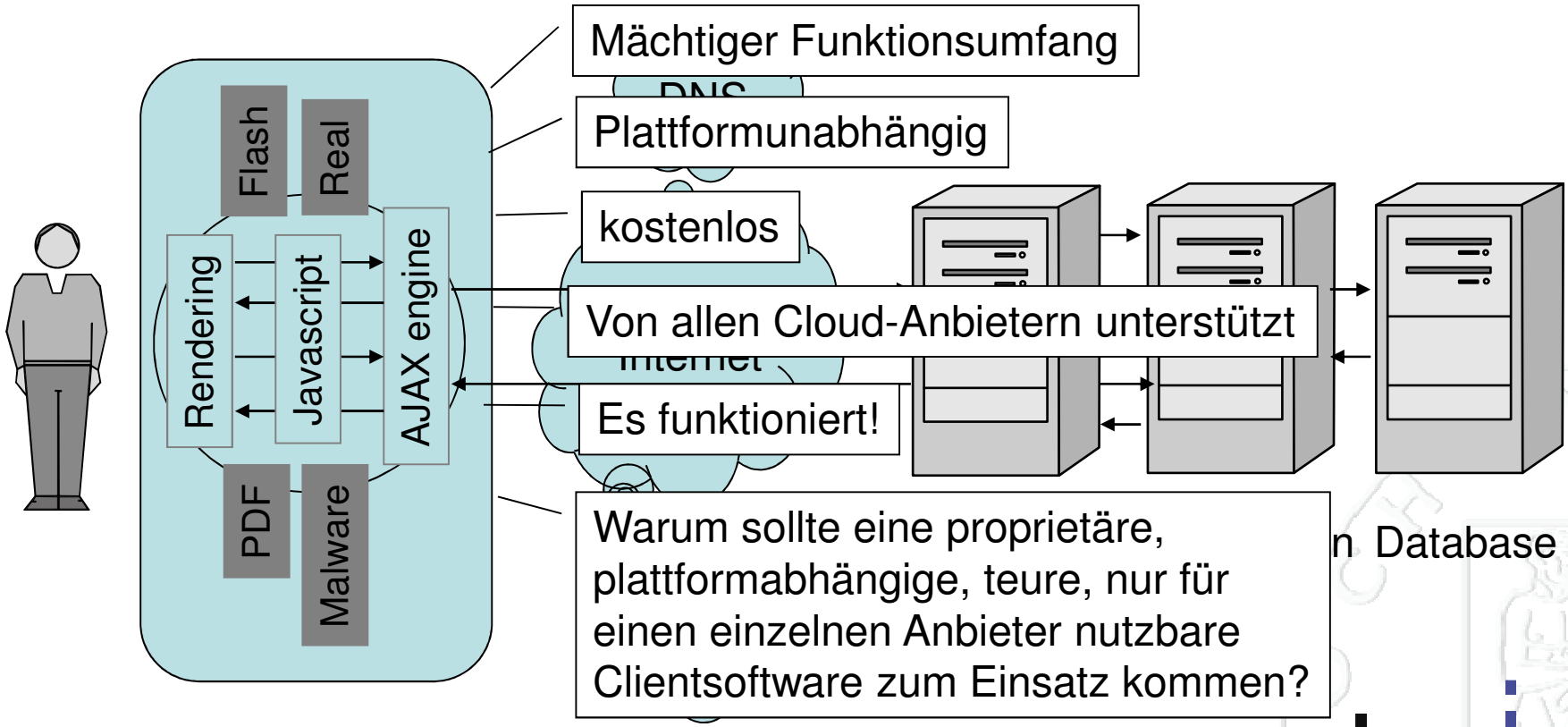
1. Die wirklichen Bedrohungen im Cloud Computing
2. Der Webbrowser als universelle Client-Software in der Cloud
3. Webservices: Die Sprache der Cloud
4. Single Sign On
5. Ausblick: Was noch zu tun ist

hgi
Horst-Görtz Institut
für IT Sicherheit

Der Webbrowser als universelle Client-Software in der Cloud



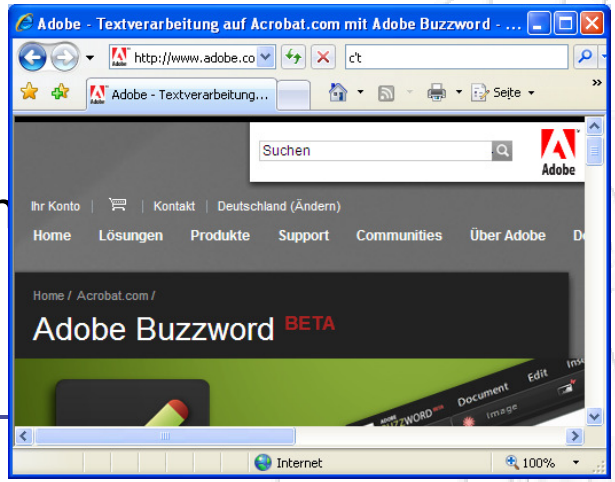
Der Webbrowser als universelle Client-Software in der Cloud



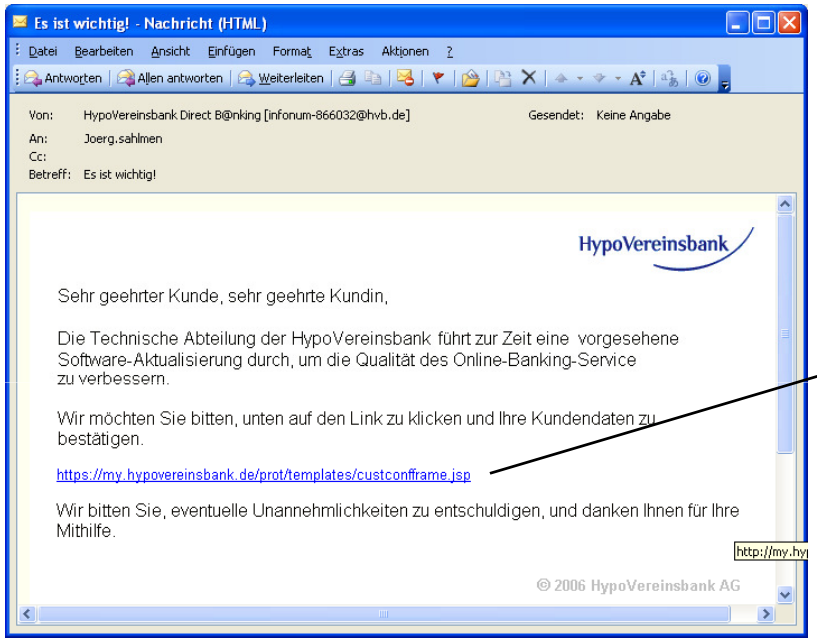
Horst-Görtz Institut für IT Sicherheit

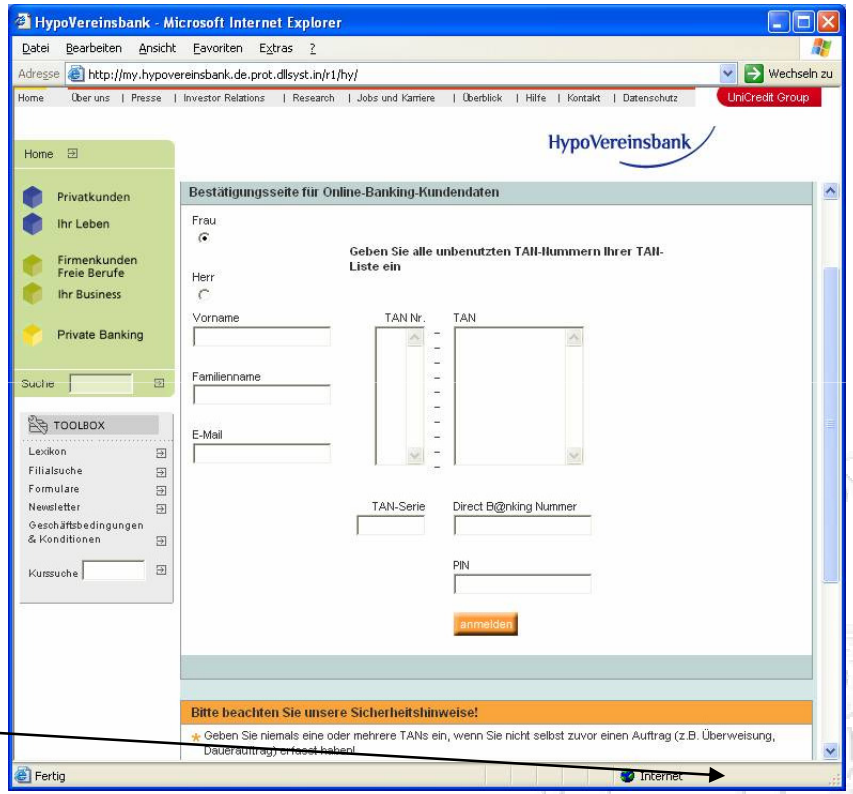
Browser-basierte Anwendungen

- Web 2.0
  - Soziale Netzwerke: StudiVZ, Youtube, XING, …
  - Neue Anwendungen: Google Maps, …
  - Viel Javascript-Code + XMLHttpRequest: AJAX
- SaaS (Software as a Service)
  - Klassische Desktop-Anwendungen jetzt im Browser
  - Z.B. MS Word → Adobe Buzzword
  - Browser in der Rolle des Betriebssystems
- SOA (Service Oriented Architecture)
  - Neues Paradigma für Serveranwendungen
  - Browser ist zentrale Clientsoftware



Why Phishing Works



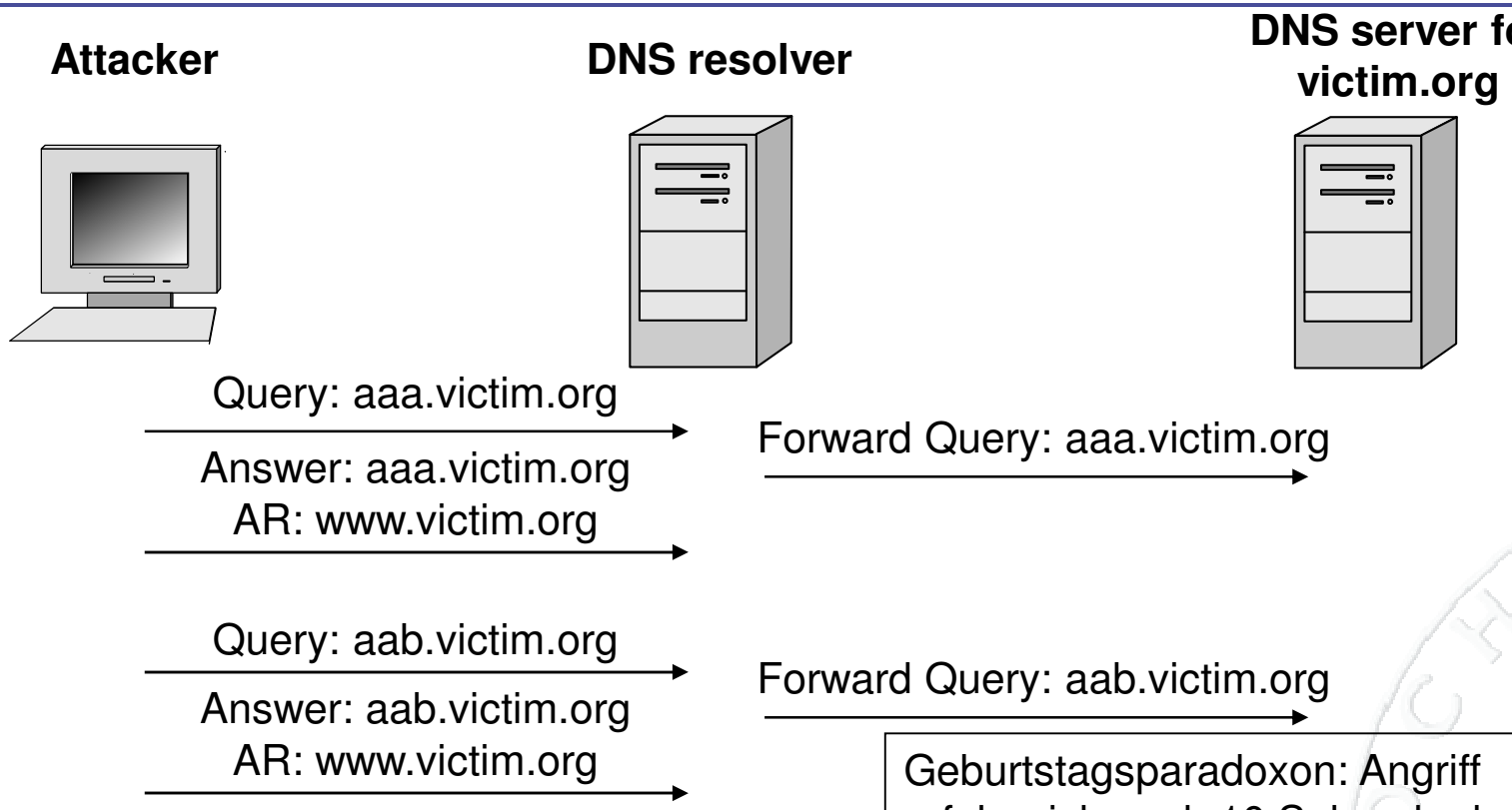


Schlosssymbol für SSL fehlt, aber das stört keinen Nutzer!

Fazit: Klassische PKI hilft nicht!

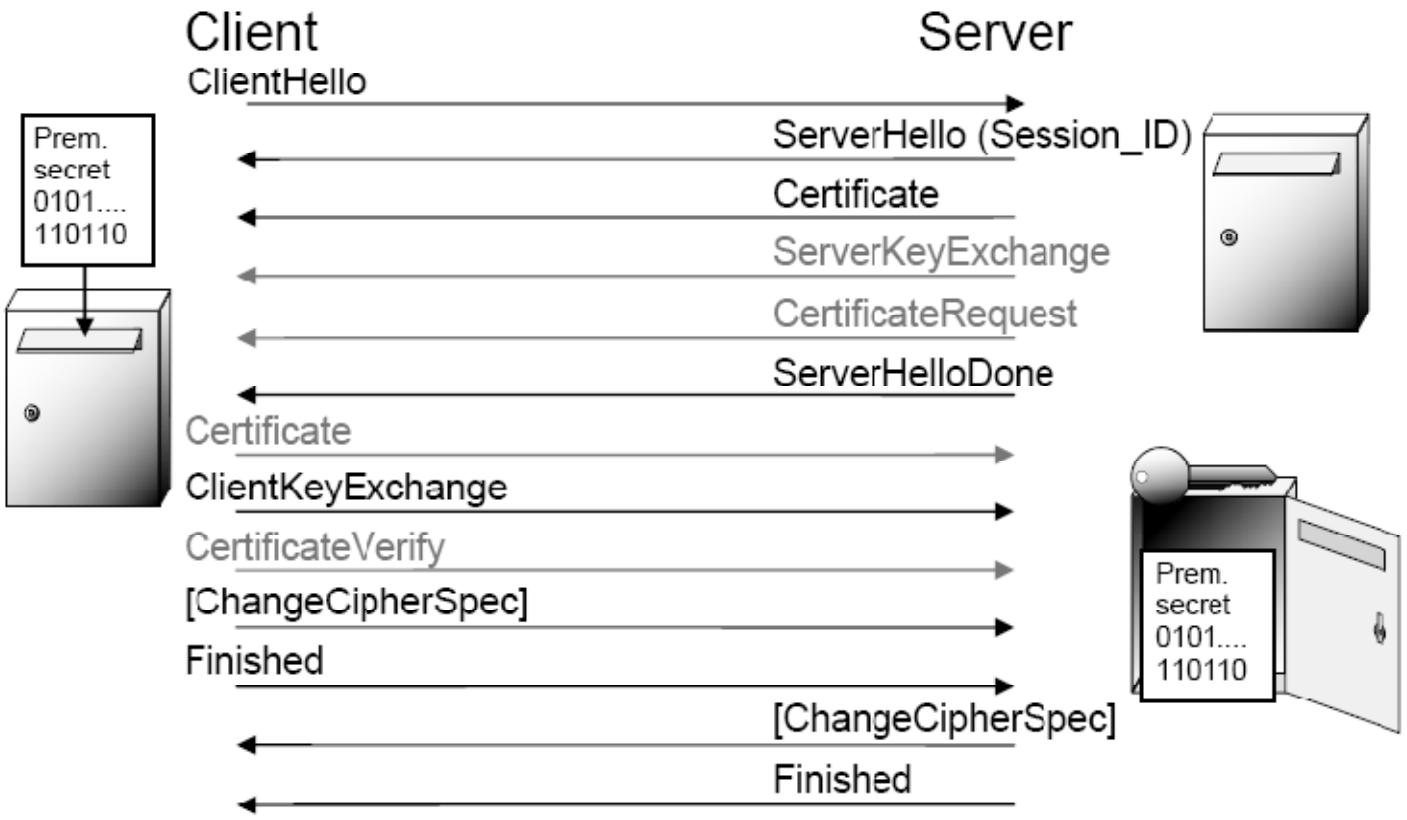
hgi
Horst-Görtz Institut
für IT Sicherheit

DNS Cache Poisoning: Dan Kaminski (Black Hat 2008)



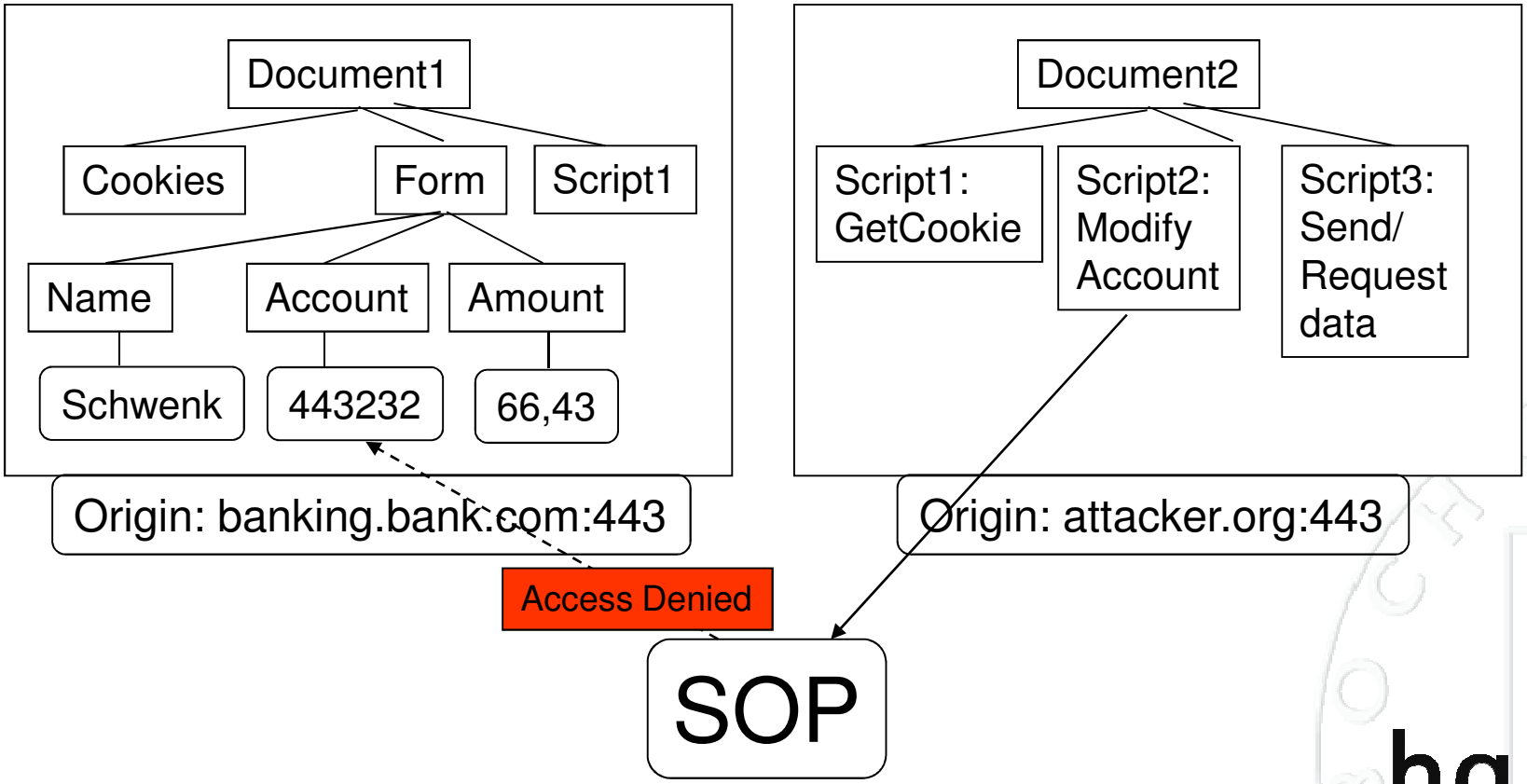
Fazit: DNS hilft nicht!

Sicherheitsmechanismen: SSL/TLS



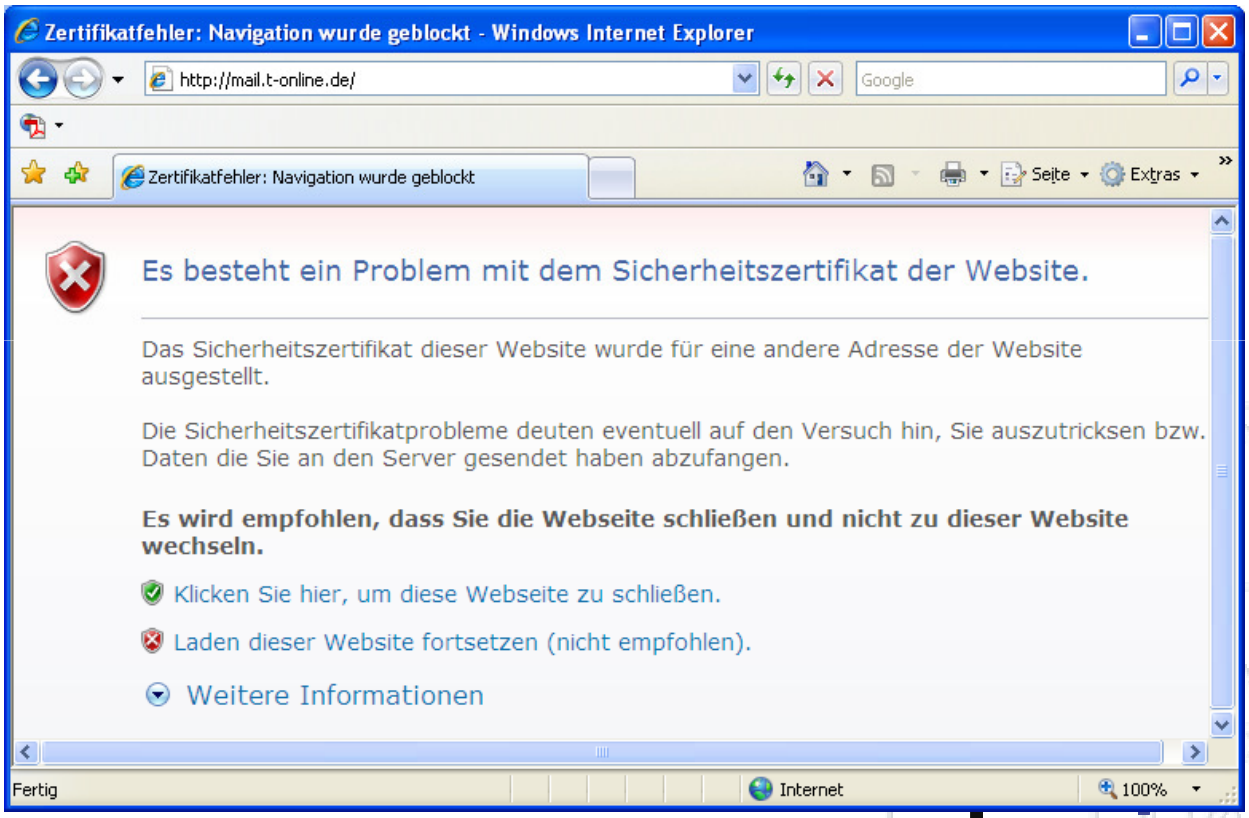
Letzter kryptographischer Angriff: Bleichenbacher 1998.

Sicherheitsmechanismen: SOP (Same Origin Policy)



Sicherheitsmechanismen: SOP and SSL

- Keine direkte Interaktion zwischen SSL und SOP
- Nutzer wird gezwungen, Sicherheits-entscheidungen zu treffen



hgi
Horst-Görtz Institut
für IT Sicherheit

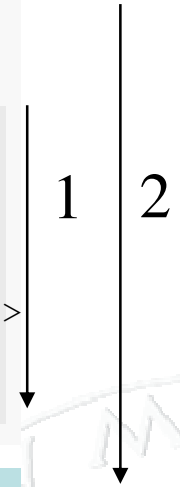
Überblick

1. Die wirklichen Bedrohungen im Cloud Computing
2. Der Webbrowser als universelle Client-Software in der Cloud
3. Webservices: Die Sprache der Cloud
4. Single Sign On
5. Ausblick: Was noch zu tun ist

hgi
Horst-Görtz Institut
für IT Sicherheit

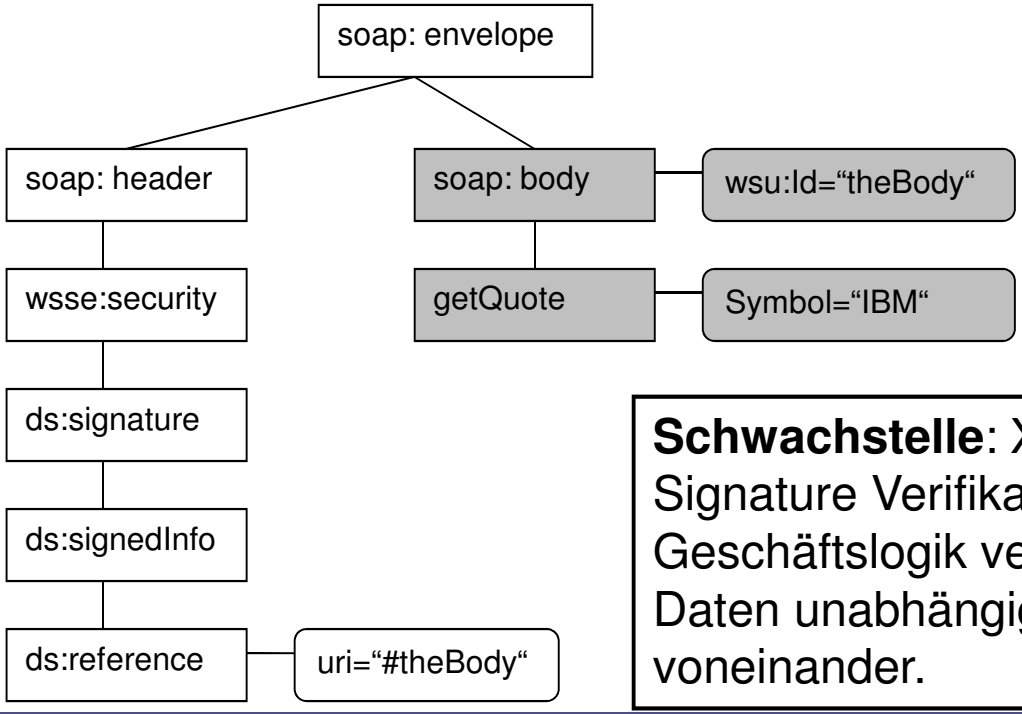
XML Signature

```
<Signature Id="MyFirstSignature" xmlns="http://www.w3.org/2000/09/xmldsig#">
  <SignedInfo>
    <CanonicalizationMethod Algorithm="..."/>
    <SignatureMethod Algorithm="..."/>
    <Reference URI="..../">
      <Transforms>
        <Transform Algorithm="..."/>
      </Transforms>
      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <DigestValue>j6lwx3rvEPO0vKtMup4NbeVu8nk=</DigestValue>
    </Reference>
  </SignedInfo>
  <SignatureValue>MC0CFFrVLtRlk=...</SignatureValue>
  <KeyInfo>
    <KeyValue>
      <DSAKeyValue>
        <P>...</P><Q>...</Q><G>...</G><Y>...</Y>
      </DSAKeyValue>
    </KeyValue>
  </KeyInfo>
</Signature>
```



XML Wrapping Attacks (McIntosh and Austel 2005)

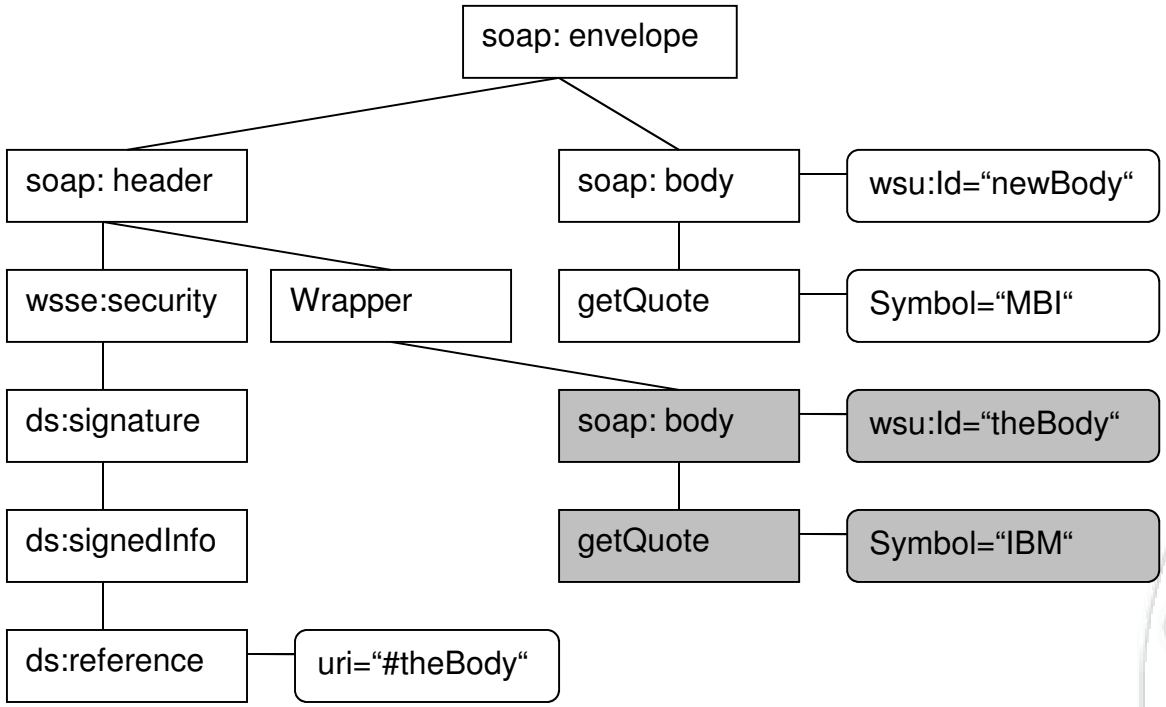
Das Originaldokument: Der SOAP Body ist signiert und wird über das `wsu:id` Attribut referenziert; die Signaturprüfung gibt nur einen Booleschen Wert (TRUE/FALSE) zurück.



Schwachstelle: XML Signature Verifikation und Geschäftslogik verarbeiten Daten unabhängig voneinander.

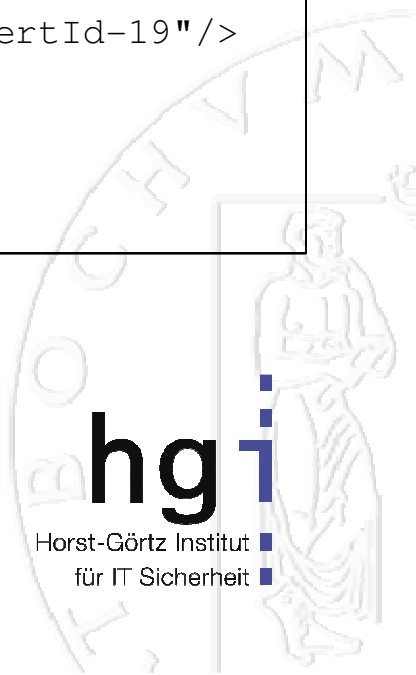
XML Wrapping Attacks (McIntosh and Austel 2005)

Das modifizierte Dokument: Die gleichen Daten sind signiert und referenziert über das `wsu:id` Attribut, aber der SOAP Body wurde verändert.



Fehlerhafte Signaturverifikation in der Amazon Cloud

```
<soapenv:Envelope>
  <soapenv:Header>
    <wsse:Security>
      <wsse:BinarySecurityToken wsu:Id="CertId-19">...
      <ds:Signature>
        <ds:SignedInfo>...
          <ds:Reference URI="#id-17547166">...
          <ds:Reference URI="#Timestamp-7461949">...</ds:SignedInfo>
        <ds:SignatureValue>...</ds:SignatureValue>
        <ds:KeyInfo>
          <wsse:SecurityTokenReference><wsse:Reference URI="#CertId-19"/>
          </wsse:SecurityTokenReference></ds:KeyInfo>
      </ds:Signature>
    </wsse:Security>
  </soapenv:Header>
  <soapenv:Body wsu:Id="id-17547166">
    <ec2:DescribeImages>
      ...
    </ec2:DescribeImages>
  </soapenv:Body>
</soapenv:Envelope>
```



hgi
Horst-Görtz Institut
für IT Sicherheit

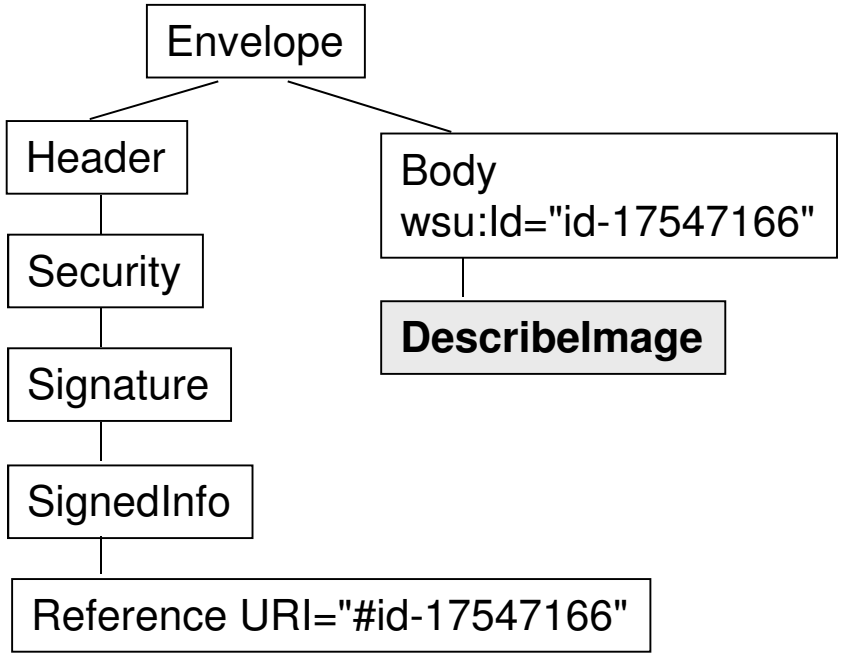
Fehlerhafte Signaturverifikation in der Amazon Cloud

```
<soapenv:Envelope>
  <soapenv:Header>
    (<!-- same header as original message -->)
     ...
     <ds:Reference URI="#id-17547166">...
     ...
  </soapenv:Header>
  <soapenv:Body wsu:Id="id-17547166">
    <ec2:RunInstances>
      ...
    </ec2:RunInstances>
  </soapenv:Body>
  <soapenv:Body wsu:Id="id-17547166">
    <ec2:DescribeImages>
      ...
    </ec2:DescribeImages>
  </soapenv:Body>
</soapenv:Envelope>
```

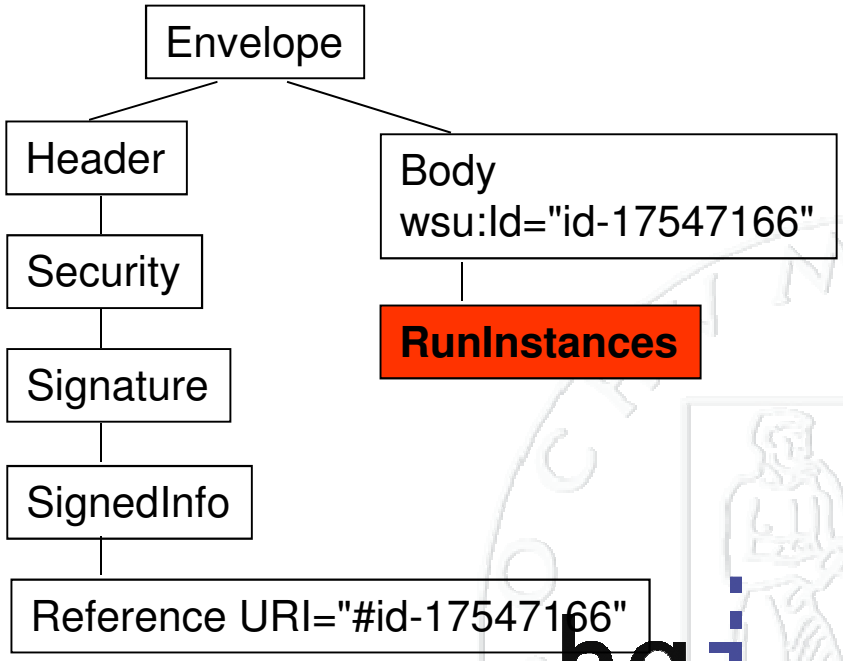
N. Gruschka, L. Lo Iacono, Vulnerable Cloud: SOAP Message Security Validation Revisited, IEEE ICWS 2009

Fehlerhafte Signaturverifikation in der Amazon Cloud

Wie die Signaturverifikation (DOM) die (XML-)Welt sieht



Wie die Geschäftslogik (SAX) die (XML-)Welt sieht



Fehlerhafte Signaturverifikation in der Amazon Cloud

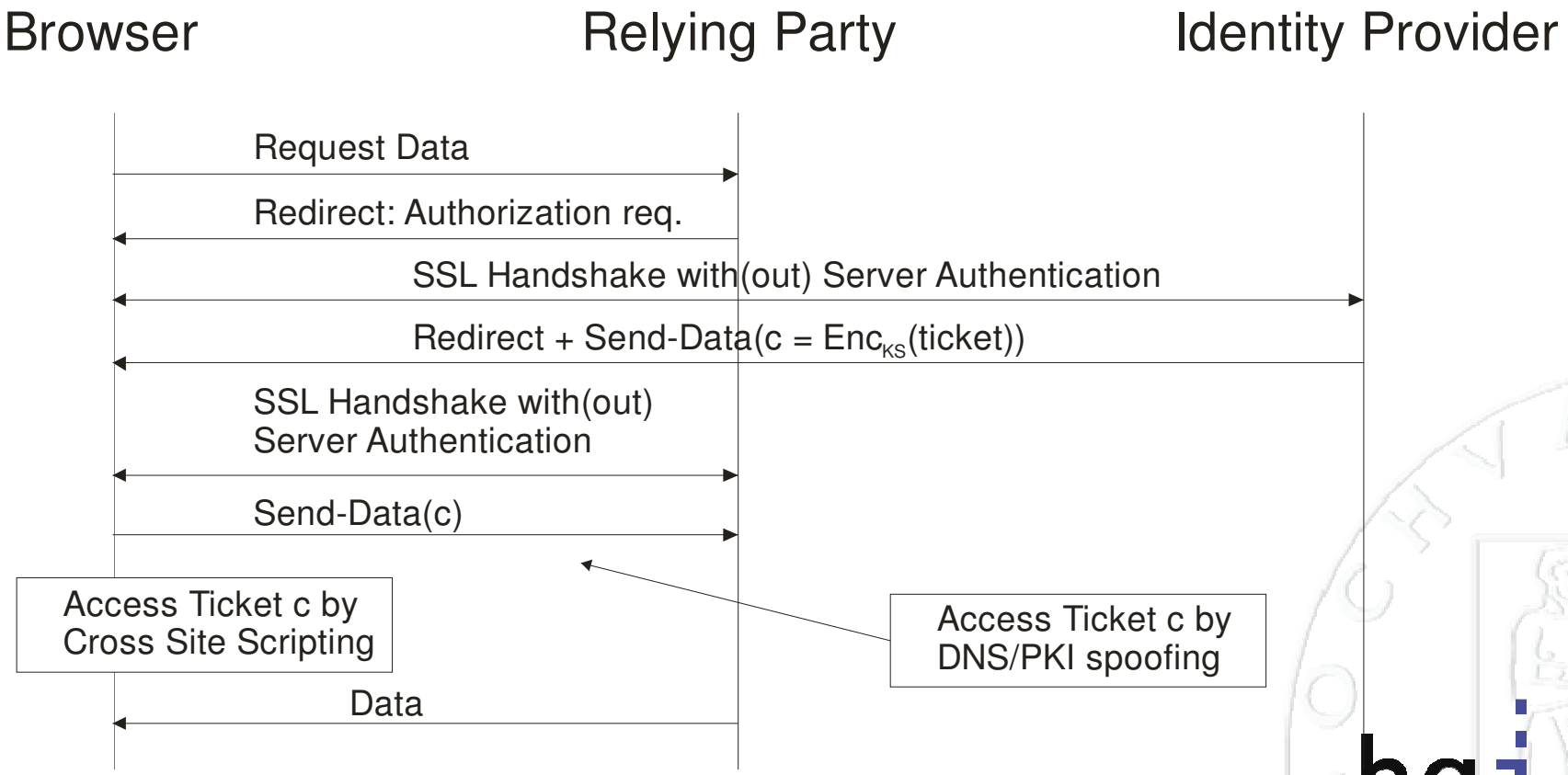
- Signaturverifikation verwendet DOM:
  - Zuerst wird der erste Body in den Hauptspeicher geladen
  - Dann wird der zweite Body in den Hauptspeicher geladen: da er ein identisches ID-Attribut besitzt, wird der erste Body mit dem zweiten überschrieben
  - Somit sind die tatsächlich signierten Daten geladen, und die Signaturverifikation ist erfolgreich
- Businnes Logic verwendet SAX:
  - BL wartet auf den Event, dass der Body der SOAP-Nachricht geladen wird.
  - Sobald dieser Event eintritt, werden die Daten verarbeitet, in diesem Fall die nicht signierten Daten.
  - Tritt der gleiche Event zum zweiten Mal auf (der Original-Body wird geladen), wird er ignoriert.

Überblick

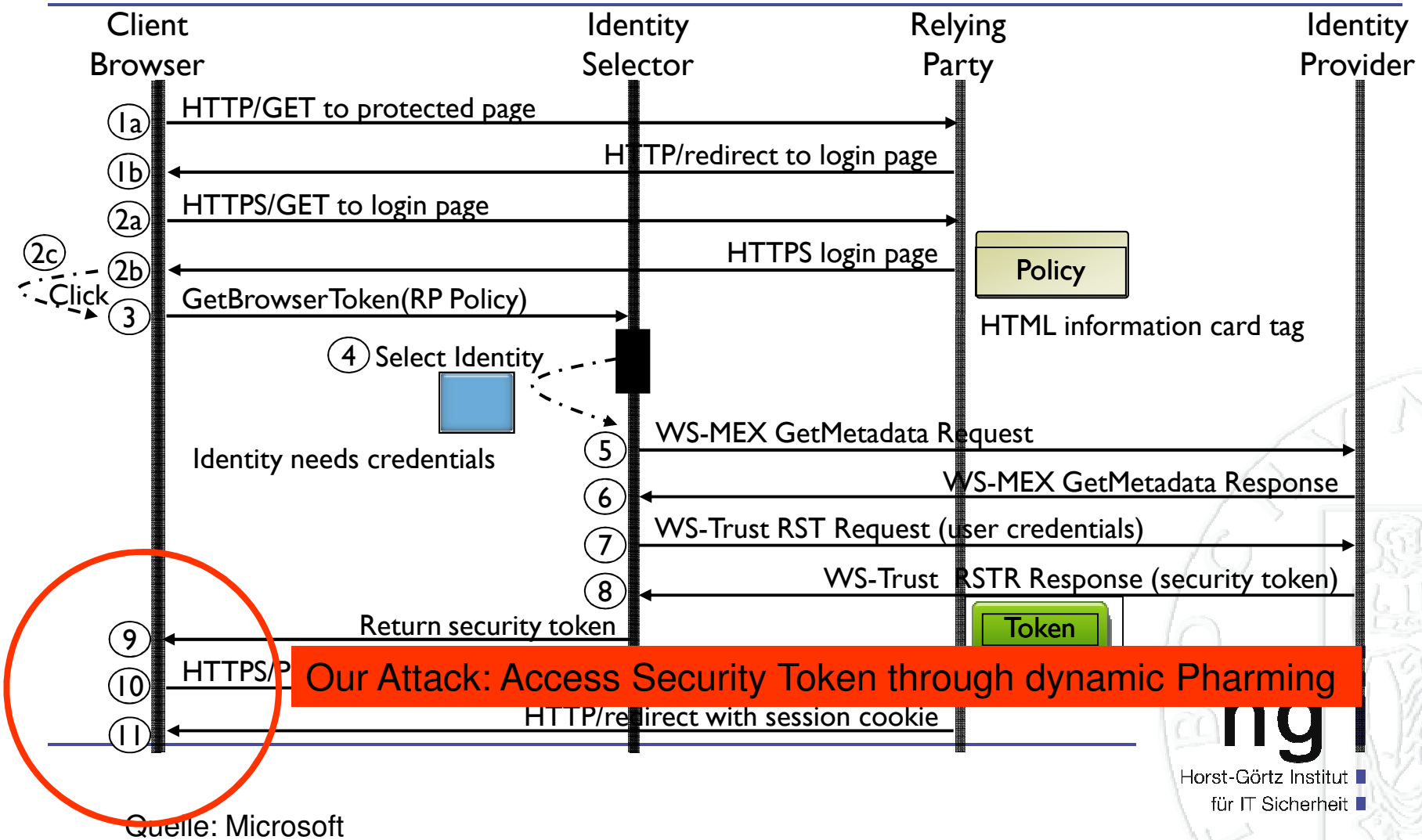
1. Die wirklichen Bedrohungen im Cloud Computing
2. Der Webbrowser als universelle Client-Software in der Cloud
3. Webservices: Die Sprache der Cloud
4. Single Sign On
5. Ausblick: Was noch zu tun ist

hgi
Horst-Görtz Institut
für IT Sicherheit

MS Passport: Generische Schwachstelle

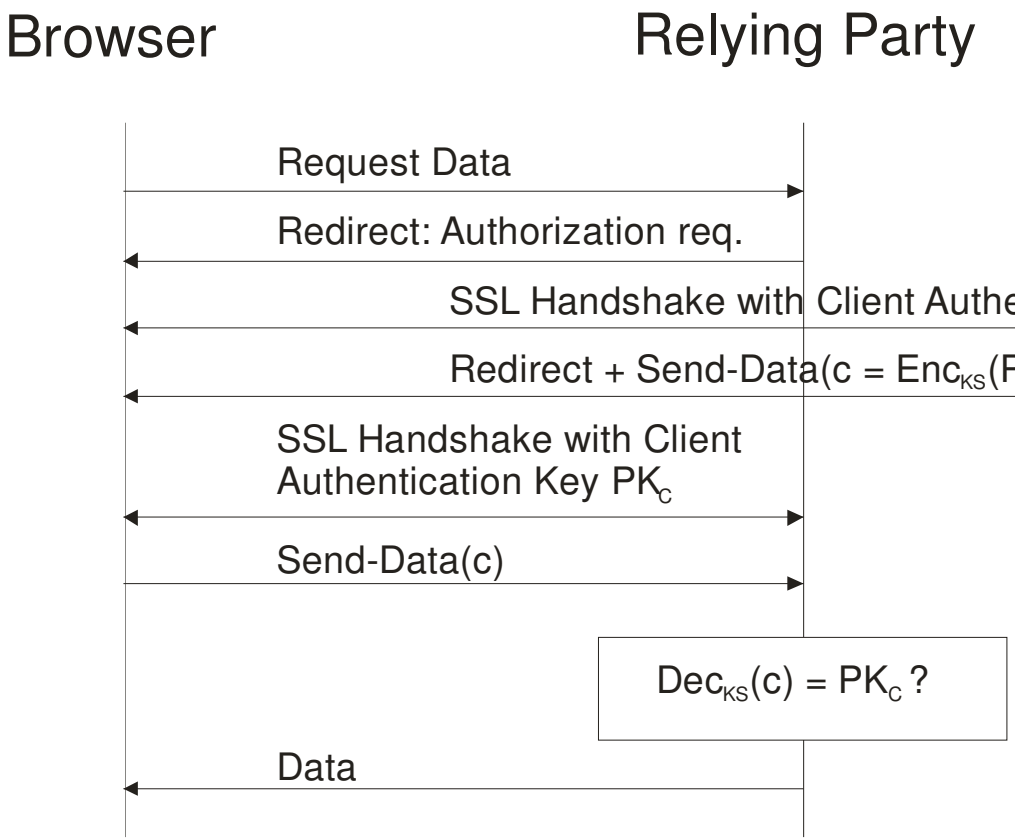


MS Cardspace



Quelle: Microsoft

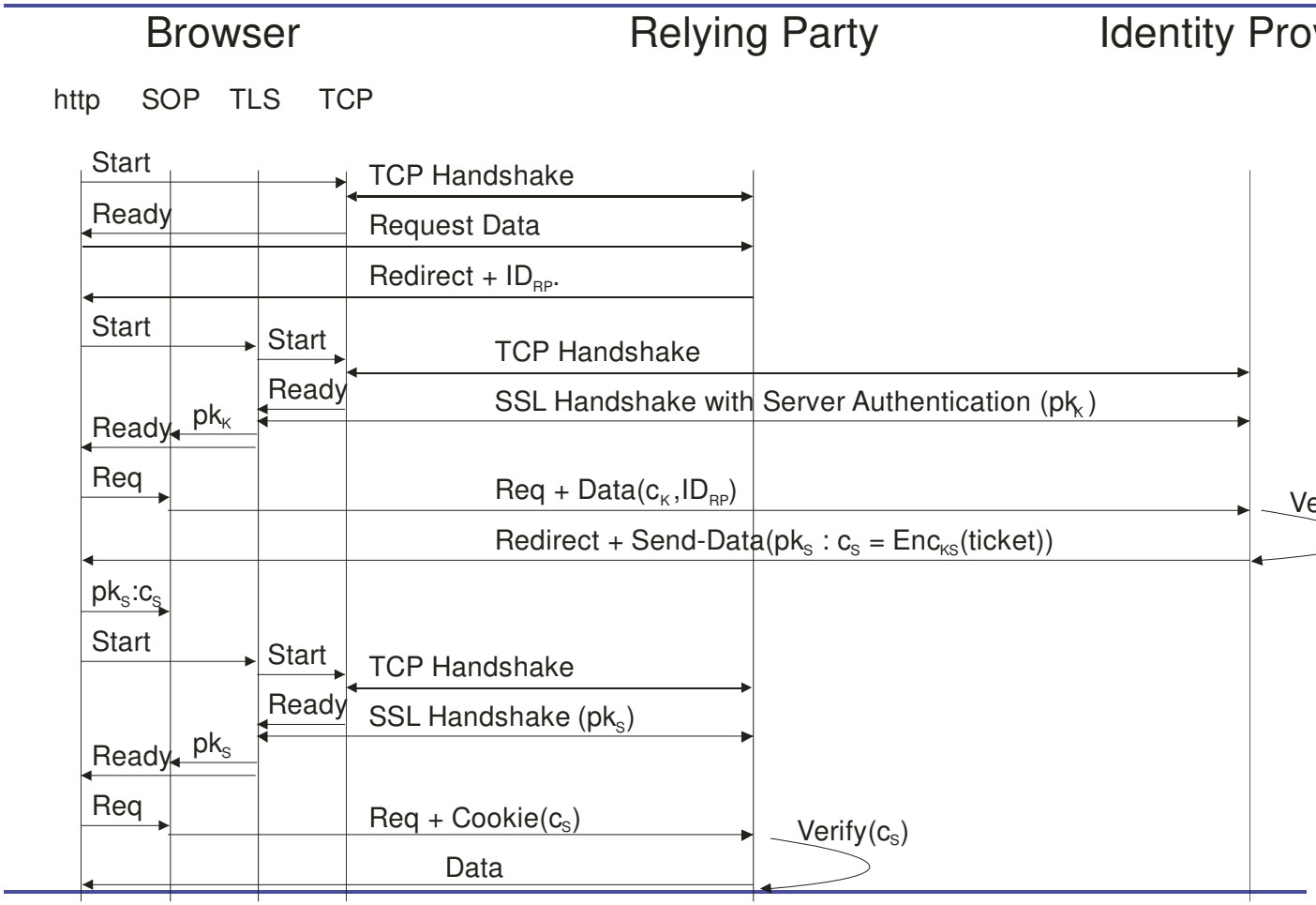
Lösung 1: Wiedererkennen des Browsers



Token c kann immer noch mittels XSS oder DNS/PKI Spoofing gestohlen werden ... **aber es ist jetzt an den Browser gebunden!**

N. KLINGENSTEIN. SAML V2.0 Holder-of-Key Web Browser SSO Profile. Working Draft 11, 11.01.2009.

Lösung 2: Wiedererkennen des Servers



Überblick

1. Die wirklichen Bedrohungen im Cloud Computing
2. Der Webbrowser als universelle Client-Software in der Cloud
3. Webservices: Die Sprache der Cloud
4. Single Sign On
5. Ausblick: Was noch zu tun ist

hgi
Horst-Görtz Institut
für IT Sicherheit

Ausblick: Was noch zu tun ist

- Neue Paradigmen für Browser-Sicherheit:
  - Kopplung von SSL/TLS und SOP
  - SSL-Client-Zertifikate, SSL/TLS ohne PKI
- WS-Security:
  - Integration bekannter Schutzmaßnahmen gegen Wrapping-Attacken in die Produkte
  - Verbesserung der Performanz von XML Signature und XML Encryption
  - Erweiterung aller Standards auf mehr als zwei Parteien
  - Model-Driven WS-Security
- Integration von Browser und XML, z.B. SAML SSL Client Certificate Profile

Veröffentlichungen

- Sebastian Gajek, Mark Manulis, Ahmad-Reza Sadeghi, Jörg Schwenk: Provably Secure Browser-Based User-Aware Mutual Authentication over TLS. ASIACCS'08
- Detlef Hühnlein, Bud Brugger, Jörg Schwenk: TLS Federation - a Secure and Relying-Party-Friendly Approach for Federated Identity Management. CAST Biosig 2008
- Sebastian Gajek, Lijun Liao, Jörg Schwenk: Stronger TLS Bindings for SAML Assertions and SAML Artifacts. ACM SWS'08
- Sebastian Gajek, Tibor Jager, Mark Manulis, and Jörg Schwenk. A browser-based kerberos authentication scheme. ESORICS'08
- Sebastian Gajek, Mark Manulis, and Jörg Schwenk. Enforcing user-aware browser-based mutual authentication with strong locked same origin policy. ACISP'08
- Sebastian Gajek. A universally composable framework for the analysis of browser-based protocols. ProvSec'08, volume 5324 of LNCS, pages 313-328. Springer, 2008.
- Sebastian Gajek, Mark Manulis, Olivier Pereira, Ahmad-Reza Sadeghi, and Jörg Schwenk. Universally composable analysis of tls. ProvSec'08, volume 5324 of LNCS, pages 283-298. Springer, 2008.
- Florian Kohlar, Jörg Schwenk, Meiko Jensen, and Sebastian Gajek. Secure Bindings of SAML Assertions to TLS Sessions. In Proceedings of the Fifth International Conference on Availability, Reliability and Security (ARES), Krakow, Poland, 2010
- Meiko Jensen, Lijun Liao, and Jörg Schwenk. The Curse of Namespaces in the Domain of XML Signature. In Proceedings of the ACM Workshop on Secure Web Services (SWS), Chicago, Illinois, U.S.A., 2009
- Meiko Jensen, Jörg Schwenk, Nils Gruschka, and Luigi Lo Iacono. On Technical Security Issues in Cloud Computing. In Proceedings of the IEEE International Conference on Cloud Computing (CLOUD-II), Bangalore, India, 2009.
- Sebastian Gajek, Meiko Jensen, Lijun Liao, and Jörg Schwenk. Analysis of Signature Wrapping Attacks and Countermeasures. In Proceedings of the 7th IEEE International Conference on Web Services (ICWS), Los Angeles, USA, 2009.

Fragen?

joerg.schwenk@rub.de

www.hgi.rub.de

www.nds.rub.de

hgi
Horst-Görtz Institut
für IT Sicherheit