RUHR-UNIVERSITÄT BOCHUM

Cloud Computing, Webservices und HTML5: Was ist noch sicher?

Prof. Dr. Jörg Schwenk, Lehrstuhl für Netz- und Datensicherheit

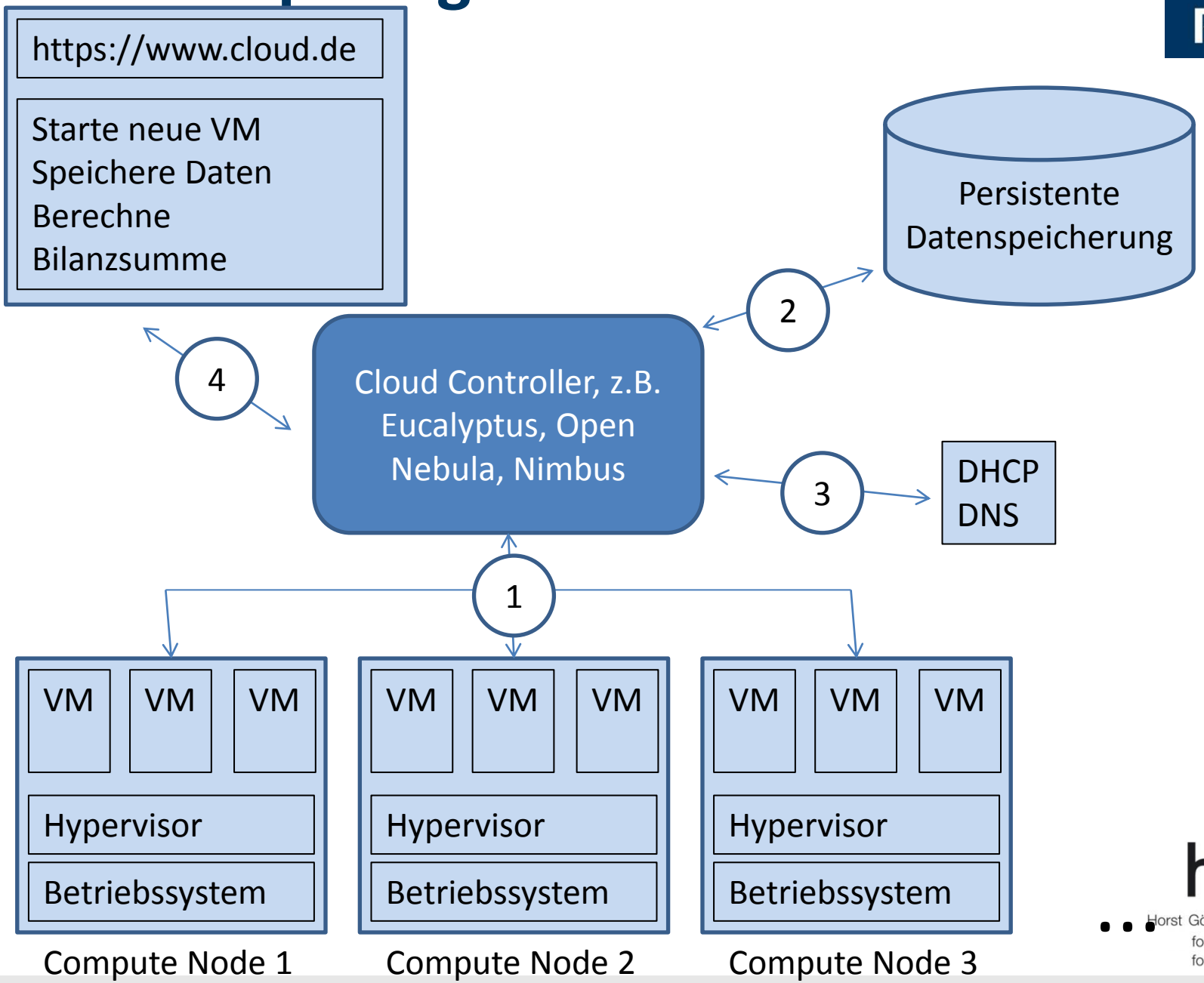
München, 29. März 2012

Horst Görtz Institute for IT-Security

Gliederung

- Cloud Computing: Architekturübersicht
- Amazon AWS: SOAP-, REST- und Browser-basiertes Kontrollinterface
- SOAP: XML Signature Wrapping
  - Exkurs: SAML
- REST: Schwachstellen bei Google und Facebook
- HTML5: XSS and Scriptless Attacks

Cloud Computing: Architekturübersicht



Cloud Computing: Architekturübersicht

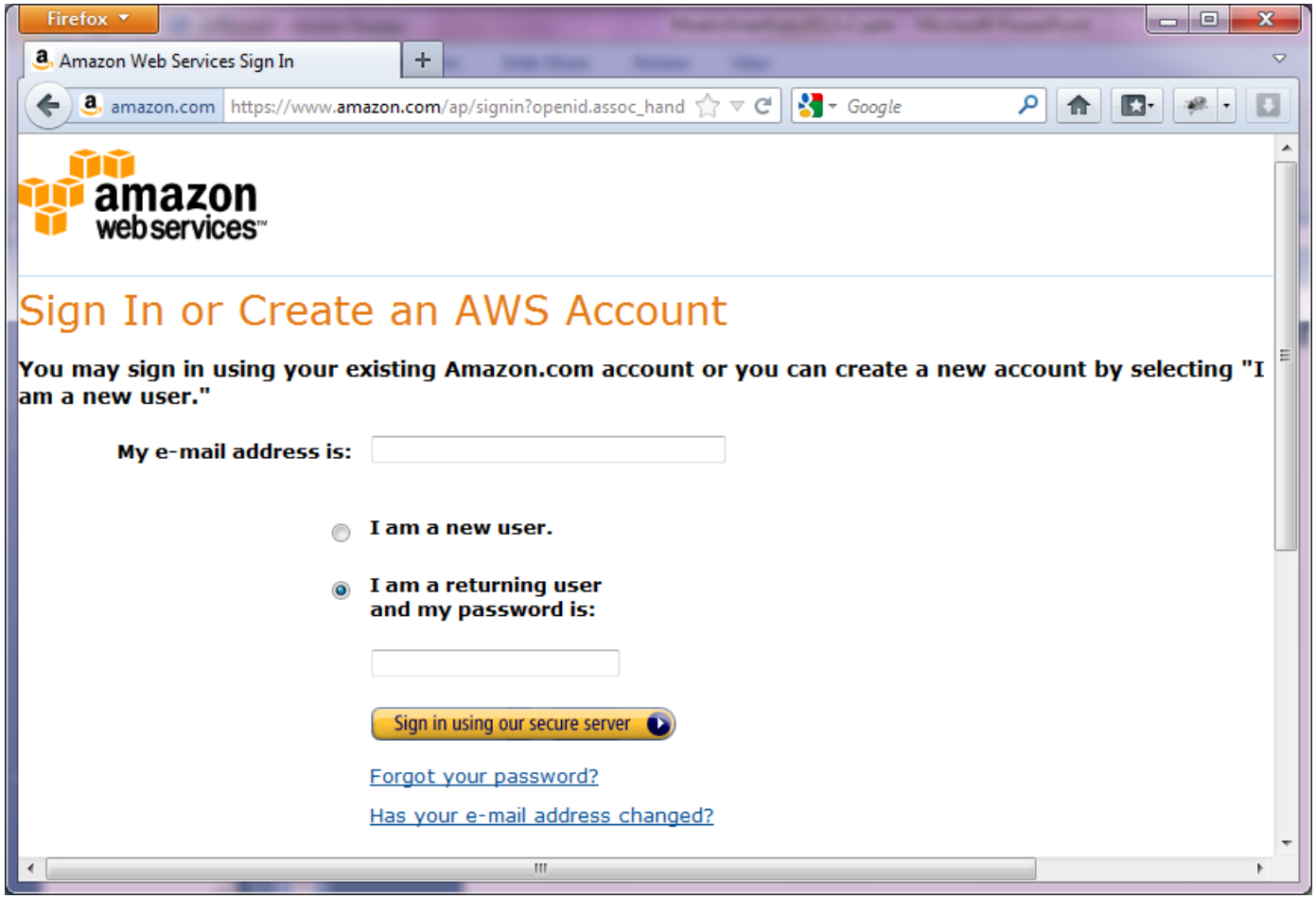
- Gute Einführung in IaaS:
  - Peter Sempolinski and Douglas Thain: A Comparison and Critique of Eucalyptus, OpenNebula and Nimbus, University of Notre Dame
- Schnittstelle 1 (Virtualisierung) stand bisher im Fokus der Untersuchungen
- Wir untersuchen die wesentlich kritischere Schnittstelle 4

Cloud Computing: Architekturübersicht

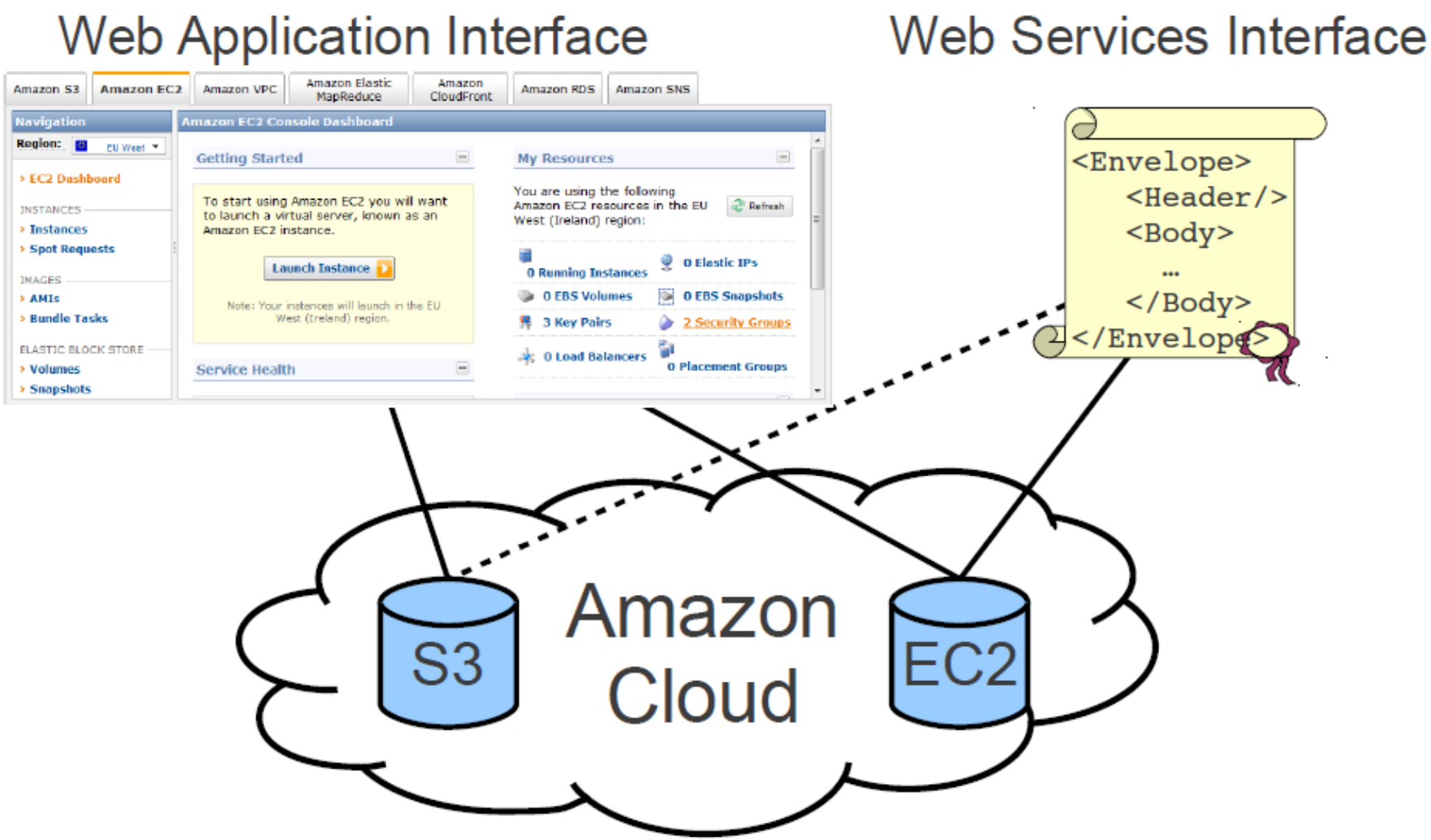
- NIST “Essential Characteristics” für Cloud Computing:

- *On-demand self-service*
  - *Auch die Authentifizierung von Nutzern und der Schutz der Daten muss im “On-demand self-service” erfolgen*
- *Broad network access*
- *Resource pooling*
- *Rapid elasticity*
- *Measured Service*

Cloud Computing: AWS erfüllt die Kriterien

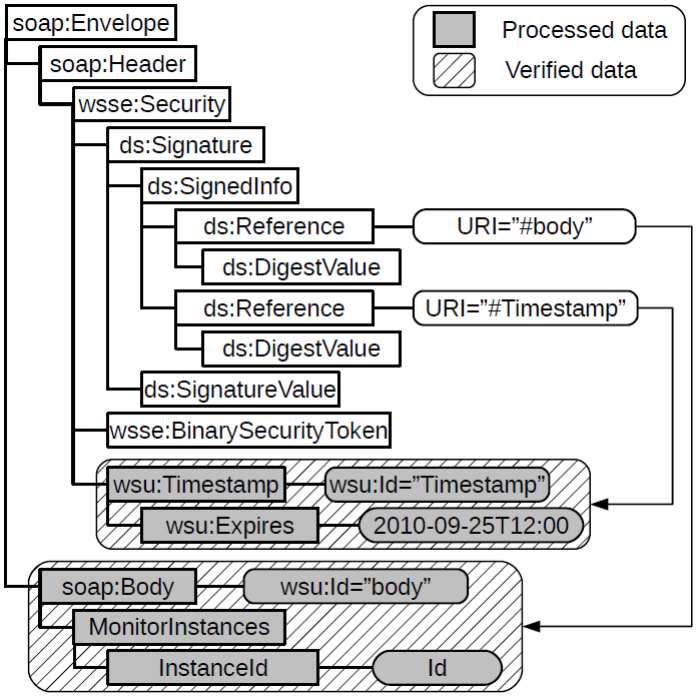


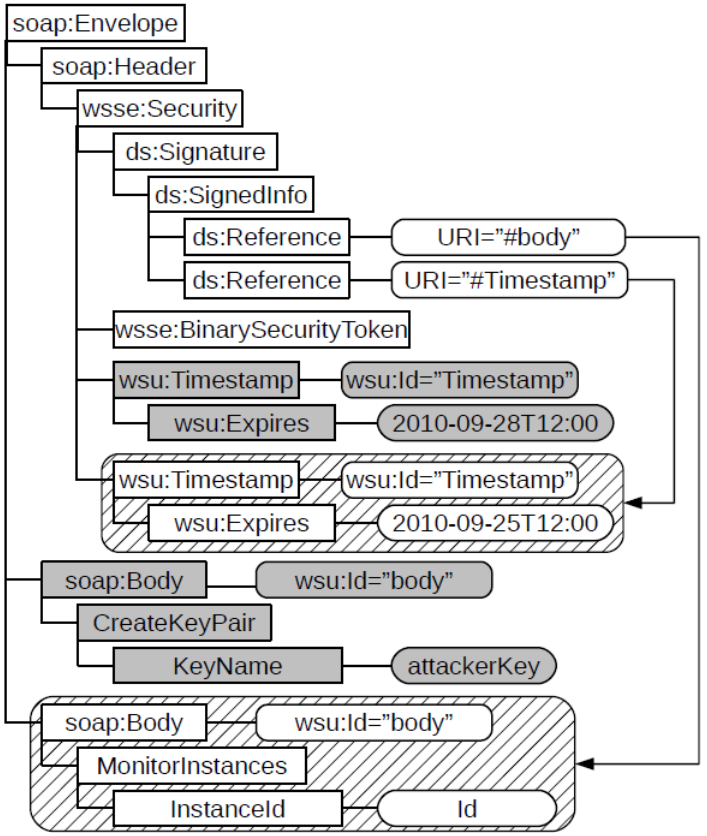
Amazon AWS: Überblick



Amazon AWS und Eucalyptus: SOAP

- XML Signature Wrapping, auch für Eucalyptus (private Cloud)





Exkurs: SAML
Wo wird SAML eingesetzt?

Microsoft® Office 365

SuisseID

amazon web services™

Der neue Personalausweis

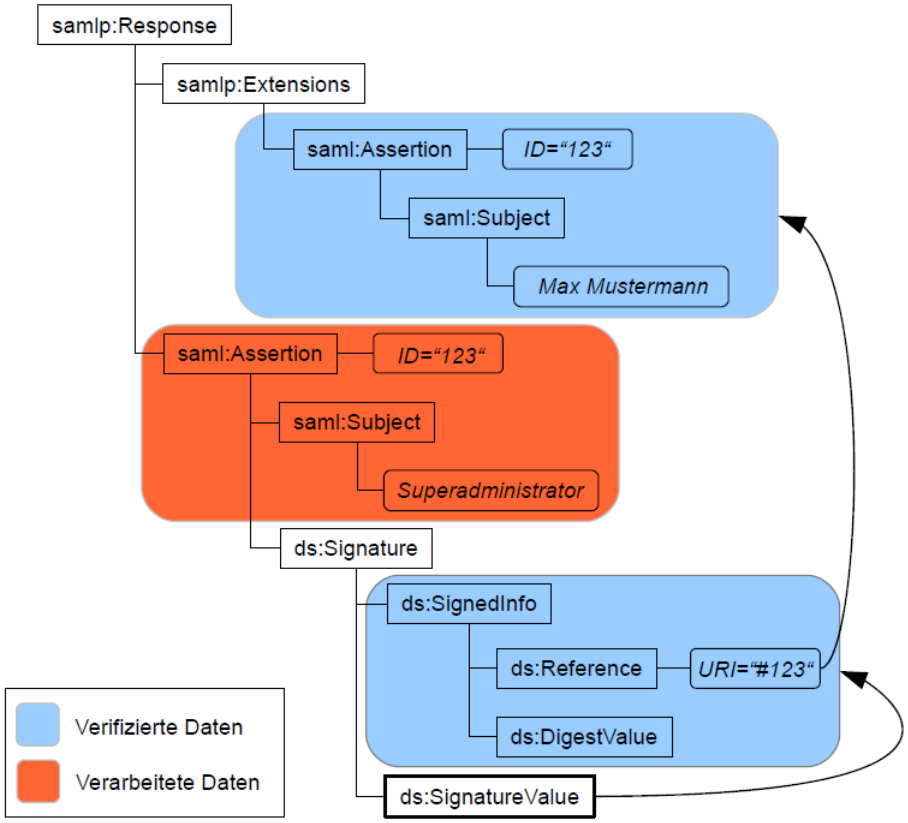
salesforce

Shibboleth®

hgi
Horst Görtz Institute for IT-Security

Exkurs: SAML
XML Signature Wrapping

- Wir konnten 11 von 14 SAML-Frameworks brechen
- Beispiel: OpenSAML/ Shibboleth



REST: Schwachstellen bei Google und Facebook

- Rui Wang, Shuo Chen, XiaoFeng Wang: Signing Me onto Your Accounts through Facebook and Google: a Traffic-Guided Security Study of Commercially Deployed Single-Sign-On Web Services. IEEE S&P 2012
- REST wenig standardisiert
- Artikel deckt Sicherheitsprobleme zwischen IdP und RP auf

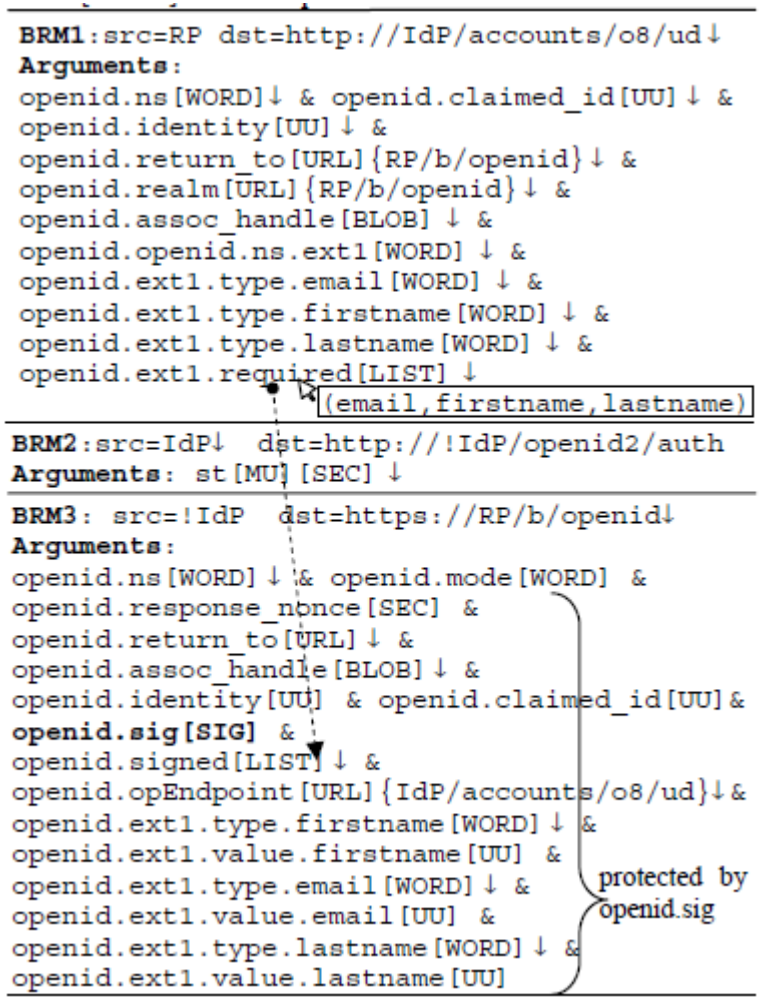
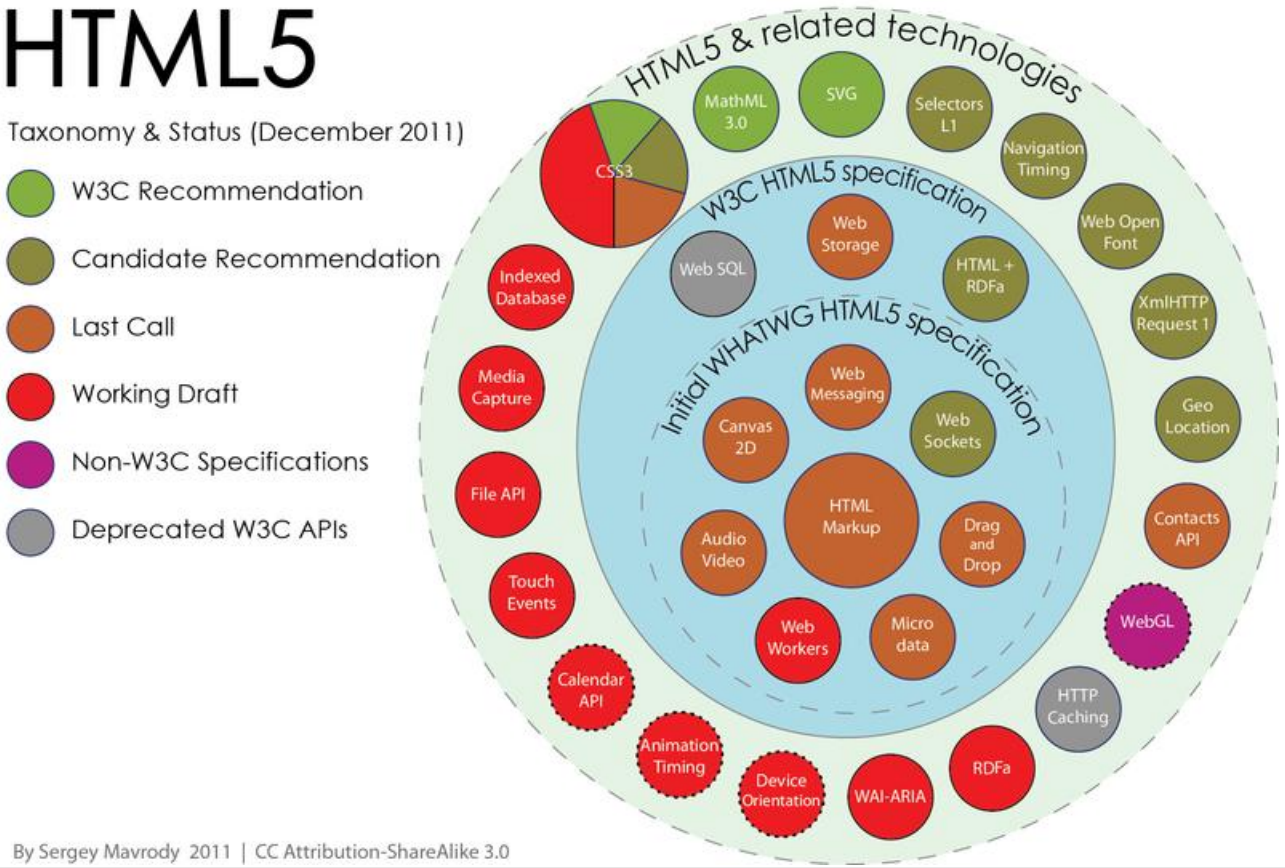


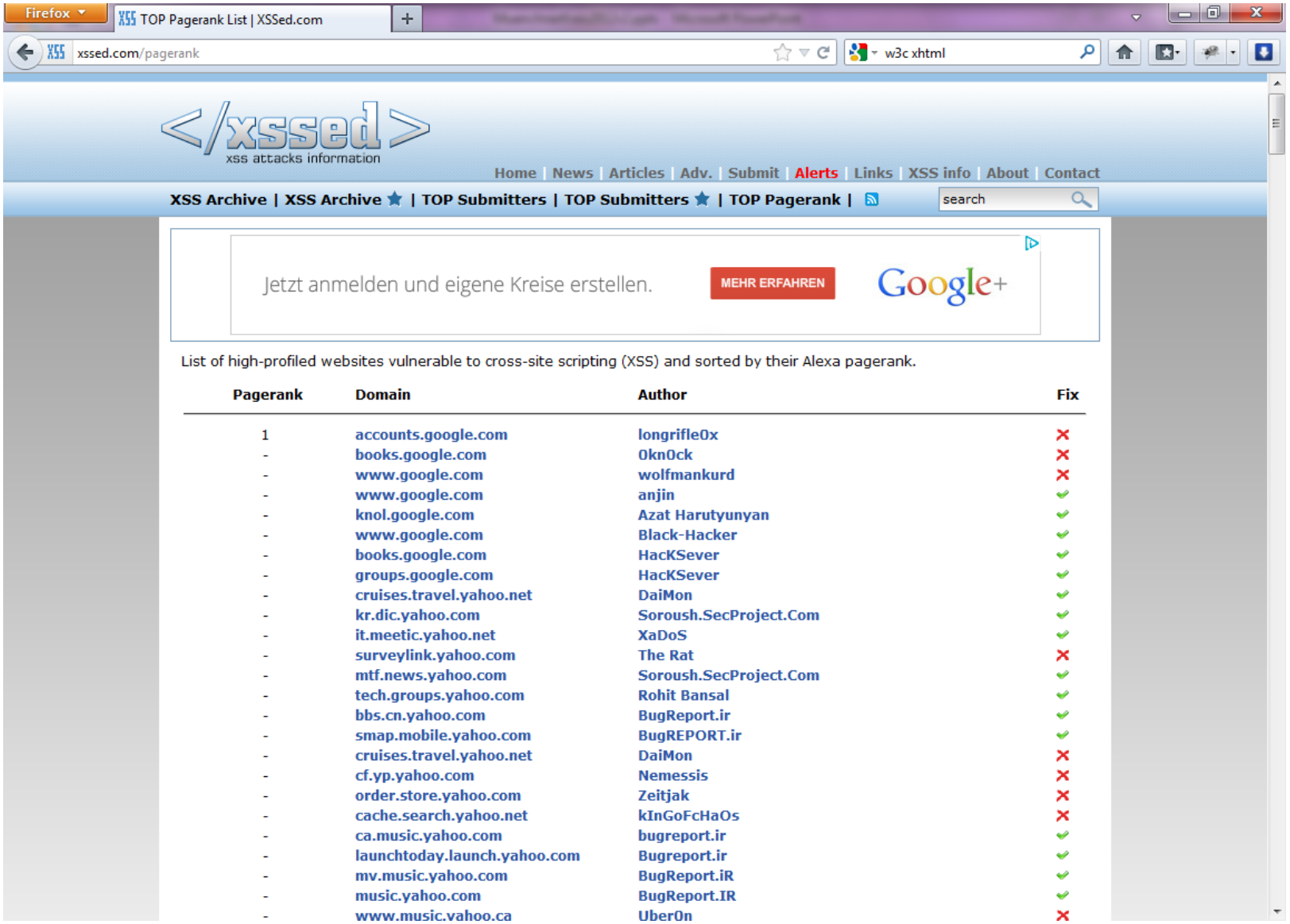
Figure 8: GoogleID+Smartsheet trace for scenario (A)

HTML5: XSS and Scriptless Attacks

- World Wide Web Consortium (www.w3.org) konnte sich mit XHTML nicht durchsetzen
- Web Hypertext Application Technology Working Group (WHATWG), gegründet 2004, standardisiert HTML5

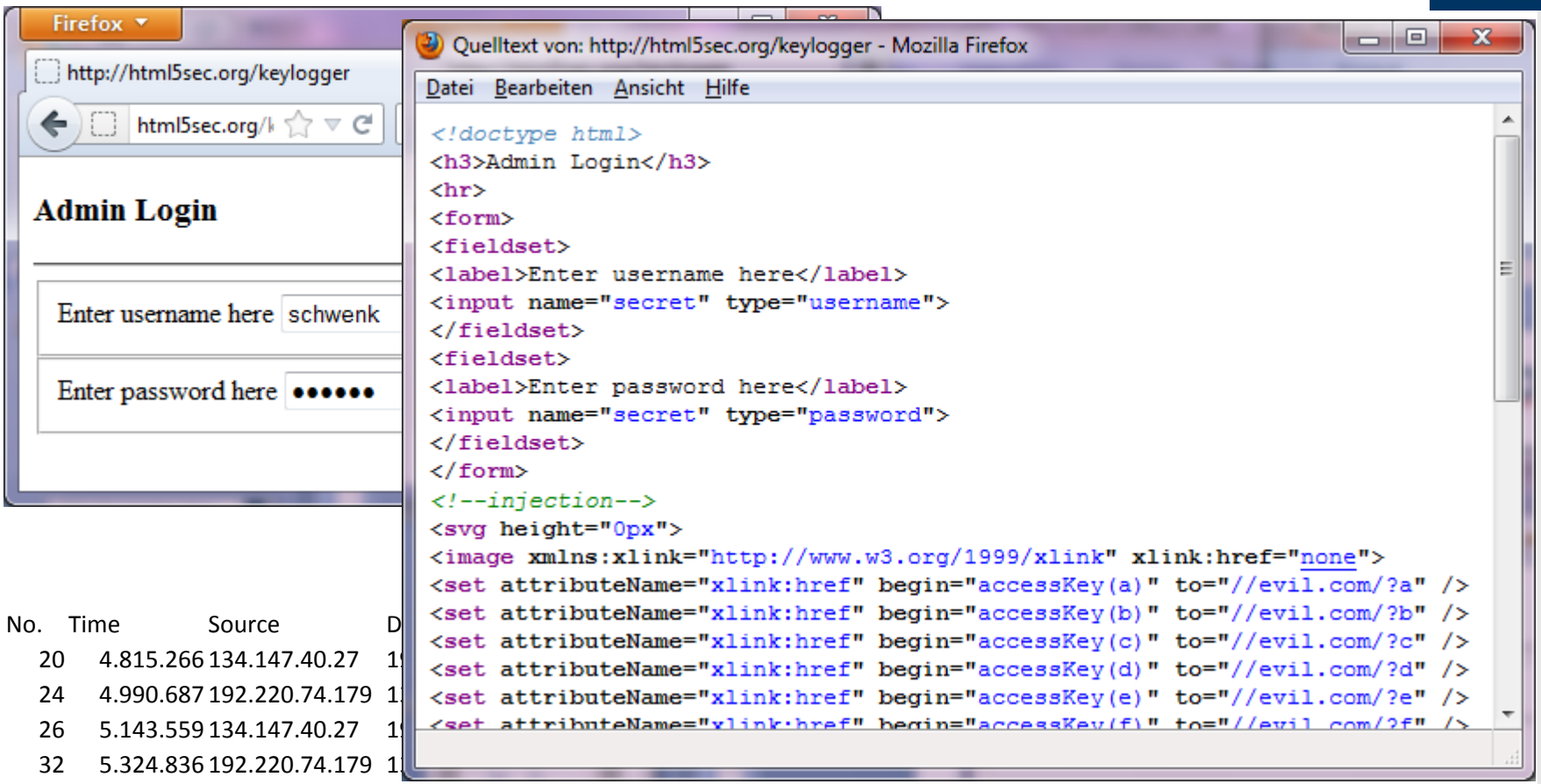


HTML5: XSS and Scriptless Attacks



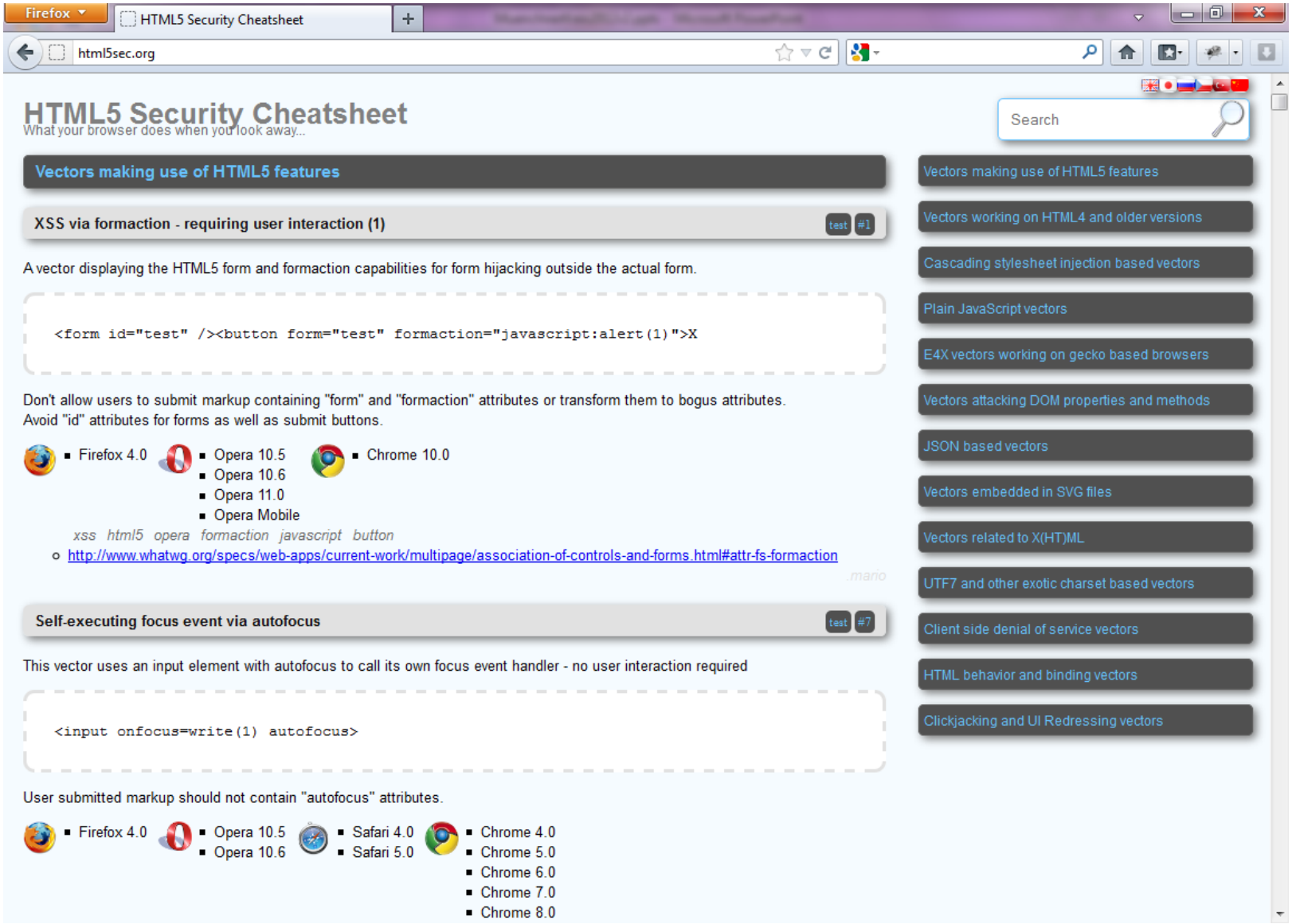
Pagerank	Domain	Author	Fix
1	accounts.google.com	longrifle0x	✗
-	books.google.com	0kn0ck	✗
-	www.google.com	wolfmankurd	✗
-	www.google.com	anjin	✓
-	knol.google.com	Azat Harutyunyan	✓
-	www.google.com	Black-Hacker	✓
-	books.google.com	HacKSever	✓
-	groups.google.com	HacKSever	✓
-	cruises.travel.yahoo.net	DaiMon	✓
-	kr.dic.yahoo.com	Soroush.SecProject.Com	✓
-	it.meetic.yahoo.net	XaDoS	✓
-	surveylink.yahoo.com	The Rat	✗
-	mtf.news.yahoo.com	Soroush.SecProject.Com	✓
-	tech.groups.yahoo.com	Rohit Bansal	✓
-	bbs.cn.yahoo.com	BugReport.ir	✓
-	smap.mobile.yahoo.com	BugREPORT.ir	✓
-	cruises.travel.yahoo.net	DaiMon	✗
-	cf.yp.yahoo.com	Nemessis	✗
-	order.store.yahoo.com	Zeitjak	✗
-	cache.search.yahoo.net	kInGoFcHaOs	✗
-	ca.music.yahoo.com	bugreport.ir	✓
-	launchtoday.launch.yahoo.com	Bugreport.ir	✓
-	mv.music.yahoo.com	BugReport.iR	✓
-	music.yahoo.com	BugReport.IR	✓
-	www.music.vahoo.ca	UberOn	✗

HTML5: XSS and Scriptless Attacks



No.	Time	Source	D			
20	4.815.266	134.147.40.27	1			
24	4.990.687	192.220.74.179	1			
26	5.143.559	134.147.40.27	1			
32	5.324.836	192.220.74.179	1			
36	5.553.898	134.147.40.27	192.220.74.179	HTTP	GET /?c HTTP/1.1	
41	5.734.461	192.220.74.179	134.147.40.27	HTTP	HTTP/1.1 200 OK (text/html)	
43	5.940.252	134.147.40.27	192.220.74.179	HTTP	GET /?r HTTP/1.1	
47	6.114.131	192.220.74.179	134.147.40.27	HTTP	HTTP/1.1 200 OK (text/html)	
56	6.393.312	134.147.40.27	192.220.74.179	HTTP	GET /?e HTTP/1.1	
61	6.564.836	192.220.74.179	134.147.40.27	HTTP	HTTP/1.1 200 OK (text/html)	
64	7.293.367	134.147.40.27	192.220.74.179	HTTP	GET /?t HTTP/1.1	
69	7.464.361	192.220.74.179	134.147.40.27	HTTP	HTTP/1.1 200 OK (text/html)	

HTML5: XSS and Scriptless Attacks



Fazit: Hoher Forschungs- und Entwicklungsbedarf

- Bewährte Technologien wie Firewalls werden nutzlos
- SOAP und SAML
  - XML Signature Wrapping: sichere Implementierung wurde im BSI-Projekt XSpRes entwickelt
  - XML Encryption: CBC-Modus gebrochen, GCM wird neu standardisiert
- REST
  - Standardisierung erforderlich
- XSS und HTML5
  - XSS ein ungelöstes Problem; neuer Lösungsansatz: JSAgents
  - HTML5: Scriptless Attacks!