Security Aspects in Web 2.0 Mashup Systems

Alexander Ritt

Philipp Hörtler

Overview

- Introduction
  - What is Web 2.0
  - What are Mashup Systems
- Mashup Systems in Detail
- Risks
  - Web 2.0
  - Mashup Systems
  - Examples
- Conclusion

Introduction

- Difference Web 1.0 and Web 2.0
- Rapid Expansion of Web 2.0
- Web Services and Web 2.0
- SOA

Introduction – *What is Web 2.0*

- Definition:
  - Web 2.0
- Mashups
  - Google Maps
  - Amazon
- Social Networks
  - MySpace
  - Facebook

Introduction – *What are Mashup Systems*

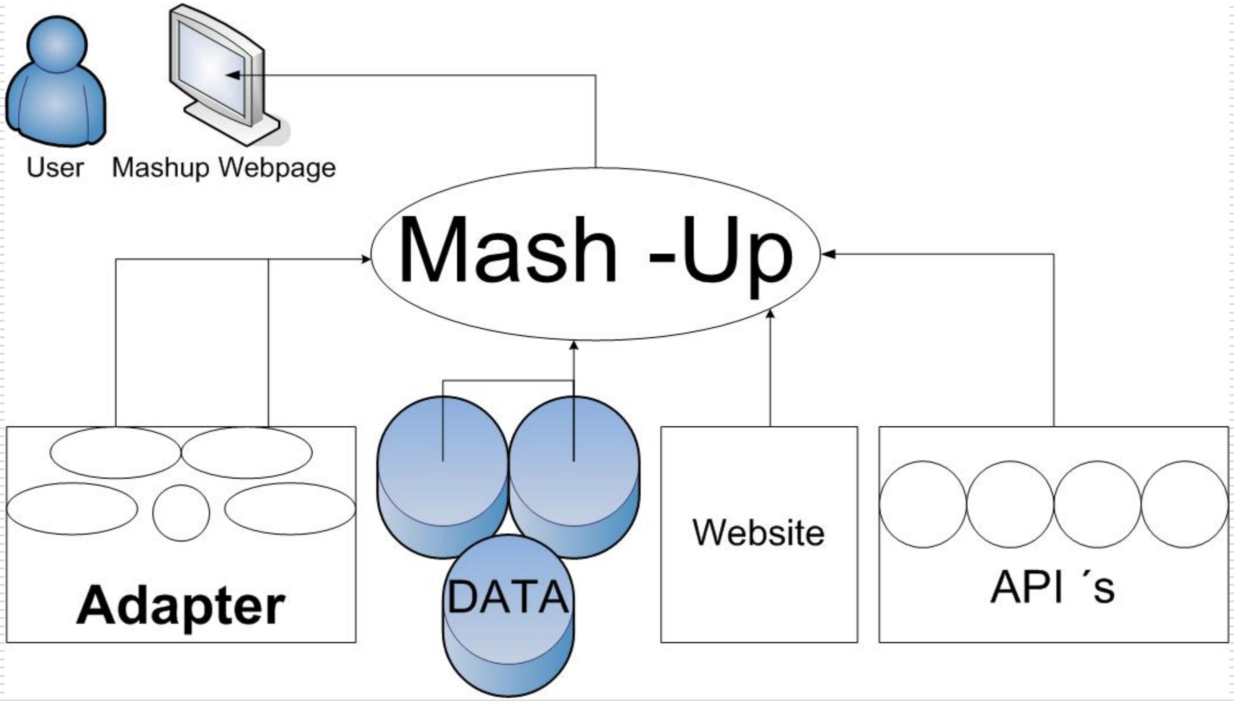
- The term mashup
- Mashups use standard API´s
- Mashups work together with SOA´s
- Combining data and services

Mashup Systems in Detail

- The power of mashups
- Three main types of mashups
  - Better interface (navigation, more responsive) for data from mostly one source
  - Combining data from different sources to get more relevant information
  - Combining data from different sources and presenting with a better interface

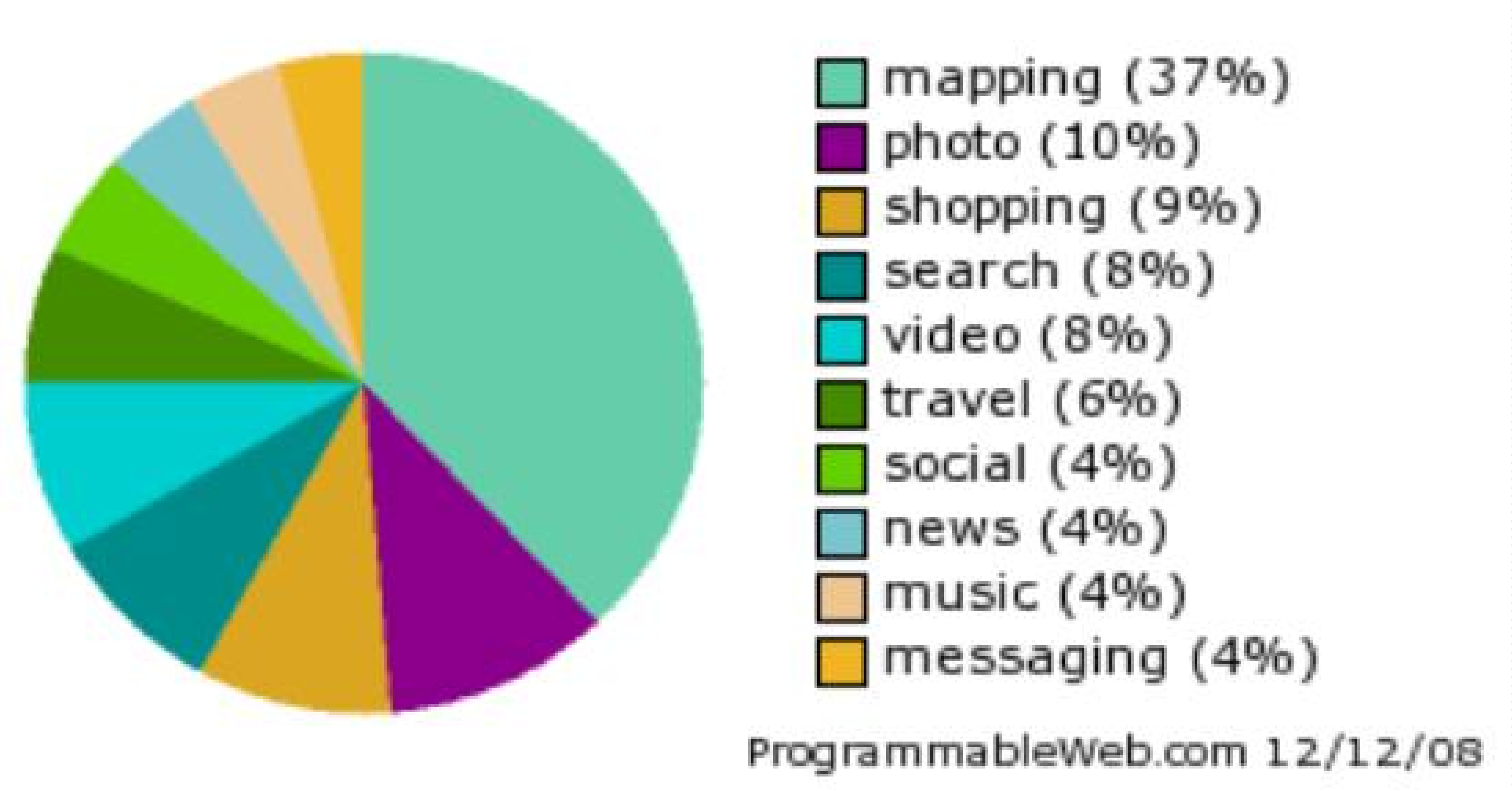
Mashup Systems in Detail

- □ Clientside Mashups
- □ Serverside Mashups



Mashup Systems in Detail

- Mashup Categories



ProgrammableWeb.com 12/12/08

Mashup Systems in Detail

- The most common Mashup Systems
  - Housing Maps (Craigslist + GM)
  - Fishing Solution (anglers fish information + GM)
  - Roadwatch (speed cameras + GM)
  - Wikis
  - Blogs
  - Studivz, YouTube, Amazon, Flickr, ...

Risks

- Most common and well known attack strategies
  - Cross-site-scripting (XSS)
  - Cross-site-request-forgery (CSRF)
- Many new risks resulting of new architecture and technologies

Risks – *Web 2.0*

- Correctness of dynamic and multiauthored information (Wikis)
- Validation of provided custom content
- Vulnerabilities or malicious code resulting of uploading custom files (YouTube, MySpace)

Risks – *Web 2.0*

- Examples
  - The Samy Worm hit MySpace
    JavaScript code that loads into a browser and infects visited MySpace pages
  - The Yamanner Worm was spammed to Yahoo!
    When *opening the attachment the worm sends a copy to the whole contact lists*

Risks *– Mashup Systems*

- Web 2.0 mashups rely on AJAX *poses a avriety of risks for end-users including*
  - XSS
  - CSRF
  - JSON Hijacking
  - ...

Risks *– Mashup Systems*

- Social networking/media sites provide APIs to access user informations
  - May expose user credentials and other sensitive data (including passwords, emails, ...)
  - Minimize the exposure of user information

Risks *– Mashup Systems*

- Combining services
  - Google Maps + GPS System
  - + list of restaurants, shopping centres, patrol stations, …
- Combining existing information
  - Google (Search engine, gMail, G-Docs)
  - StudiVZ, Flickr, MySpace
  - Amazon, eBay

Risks *– Examples*

- Geo-tracking
  - People search
- Combining Data
  - Google + Amazon + Yahoo
- Web 2.0 Hacking with Firefox Plugin
  - Firebug and Source Code

Conclusion

- Web 1.0 developing into Web 2.0
- 1000 new mashups every 6 months
- Correctness of data?
- Nice Features, but dont combine all!

Security Aspects in Web 2.0 Mashup Systems

Thank you for your attention!