

# Language-based web application security

Andrey Chudnov  
Department of Computer Science

## Sources of insecurity

Communication	Applications often use unencrypted communications. Even encrypted communications can be compromised by man-in-the-middle attacks
Storage	Many web applications store private data on the server side (e-mail, calendars etc.). This data is as secure as service providers' own data.
Server-side software	Server-side software often (~80%) has bugs that allow successful attacks on information.
Mashups	It's hard for the user to check if proper communication encryption is done, if the authentication credentials and private data are not abused.
JavaScript	Any web page could contain a program in JavaScript. This allows for interactive (Web 2.0) applications, but is also a major source of risk in form of JavaScript worms, e.g. Same (Facebook), Yamanner (Yahoo) etc.
Users	Most of the users are known to make poor security decisions, especially, on the Web where security risks are not apparent.

## Research results

Information flow analysis in presence of:

- Interactions with the browser
- Dynamic code evaluation

## Possible applications

- A more secure web browser
- Static code analysis tools for JavaScript

# Information flow

