

MOTIVATION

Studying web security

Large-scale data collection: **existing solutions**
 (millions of websites, distributed crawls)



Analysis tools: **no comprehensive solutions**
 (ad hoc approaches, duplicated efforts)



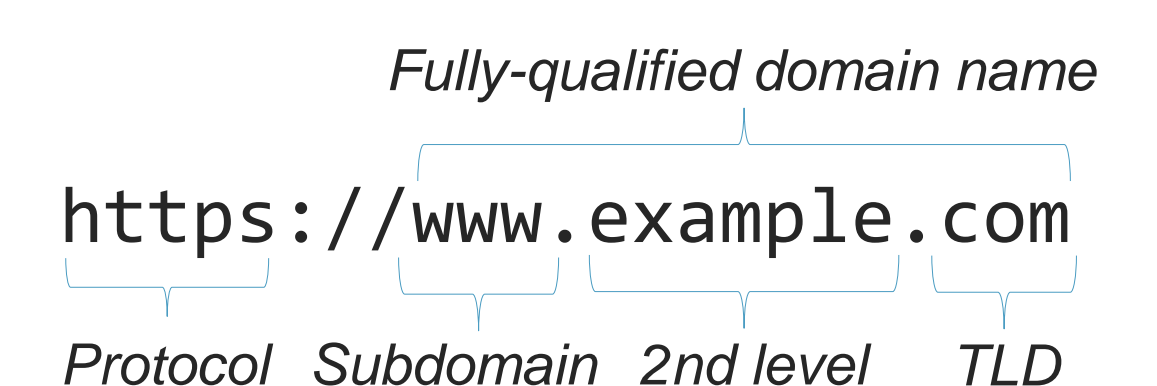
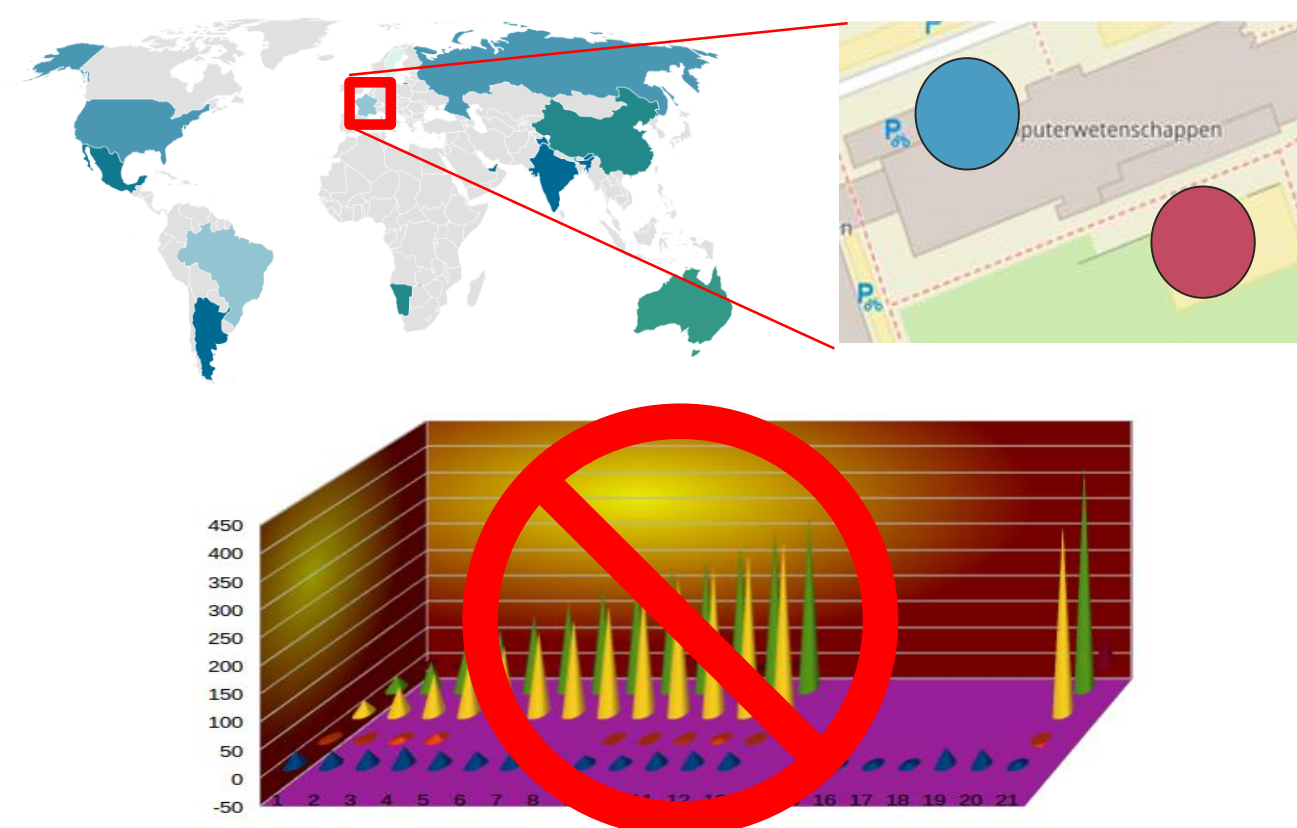
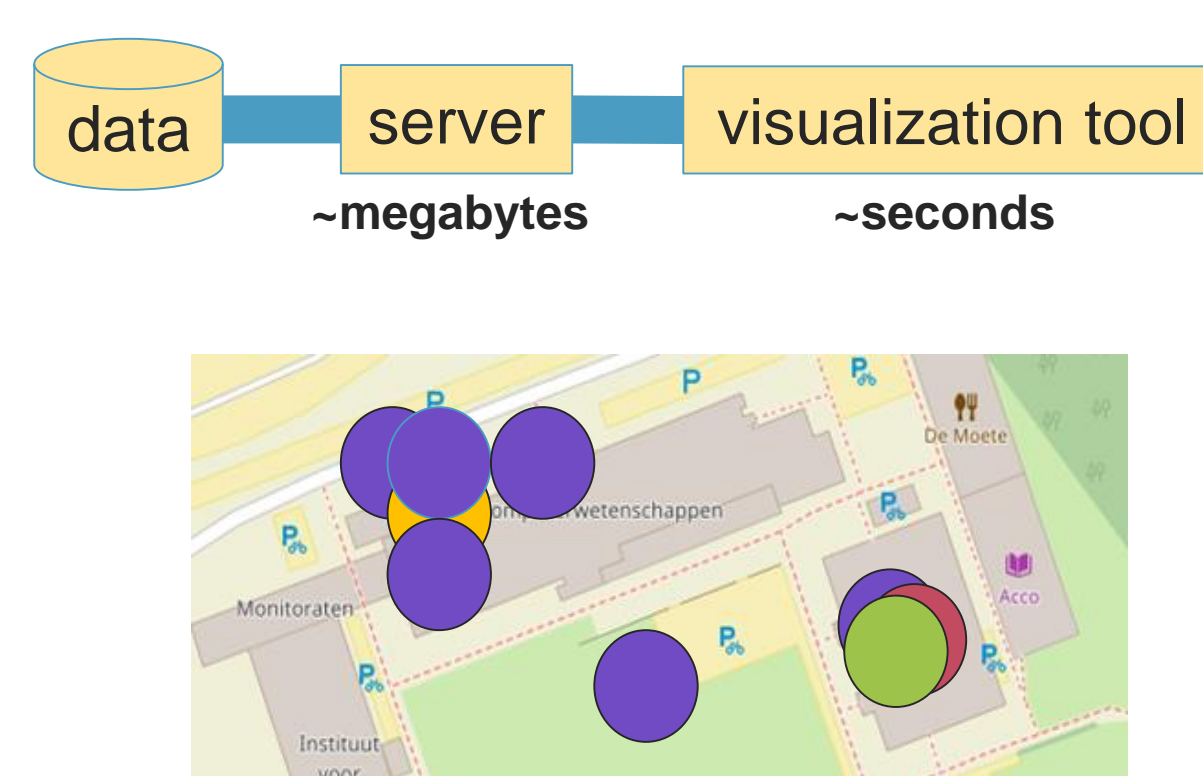
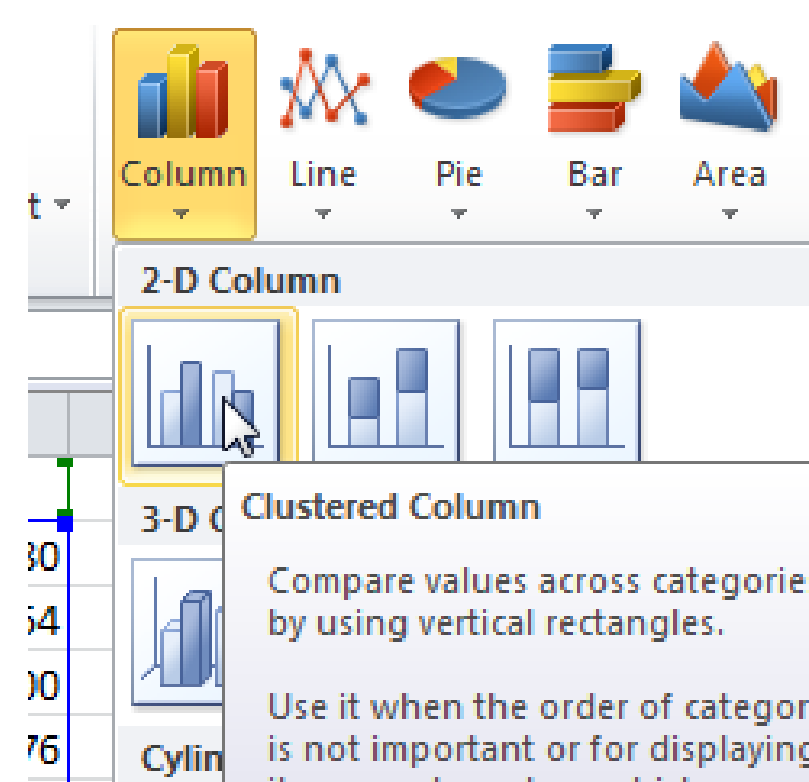
Visual analytics [2]

- › Visualization: leverage processing power of human perception
- › Interaction: encourage data exploration

- +** Analyze data & get insights › more **accurately** › more **efficiently** › on a **larger scale**
- Security analysts: unfamiliar → reluctant to adopt visualizations [1]

Goal: create tailored solution that › addresses the challenges in analyzing web security data
 › facilitates visual exploration for security analysts

CHALLENGES



Separation of data and visualization

- › Difficult to create visualization
- › Heterogeneous data sources

Scalability

- › Data processing
- › Visual representation

Exploration

- › Overview → details
- › Avoid misrepresentation

Web security data

- › Specific types/structures
- › Public data sources

DESIGN

Data abstraction

- › Add context to data
- › Transform data into standard format

Aggregation

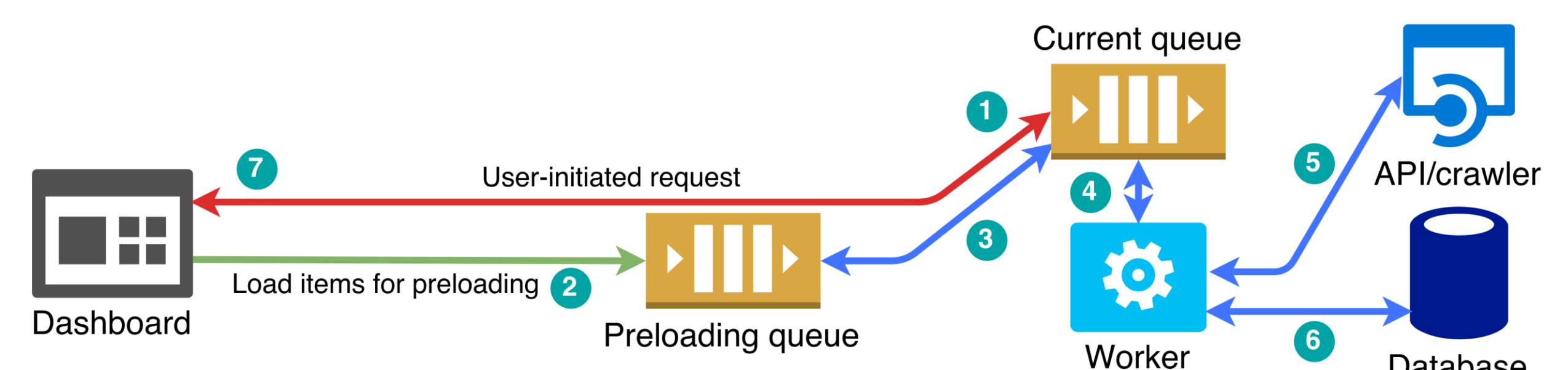
- › By default & early on
- › On structures in web: e.g. IP → AS

Interactive visualization

- › Automated creation
- › Multiple linked charts

Integration with public and collected data

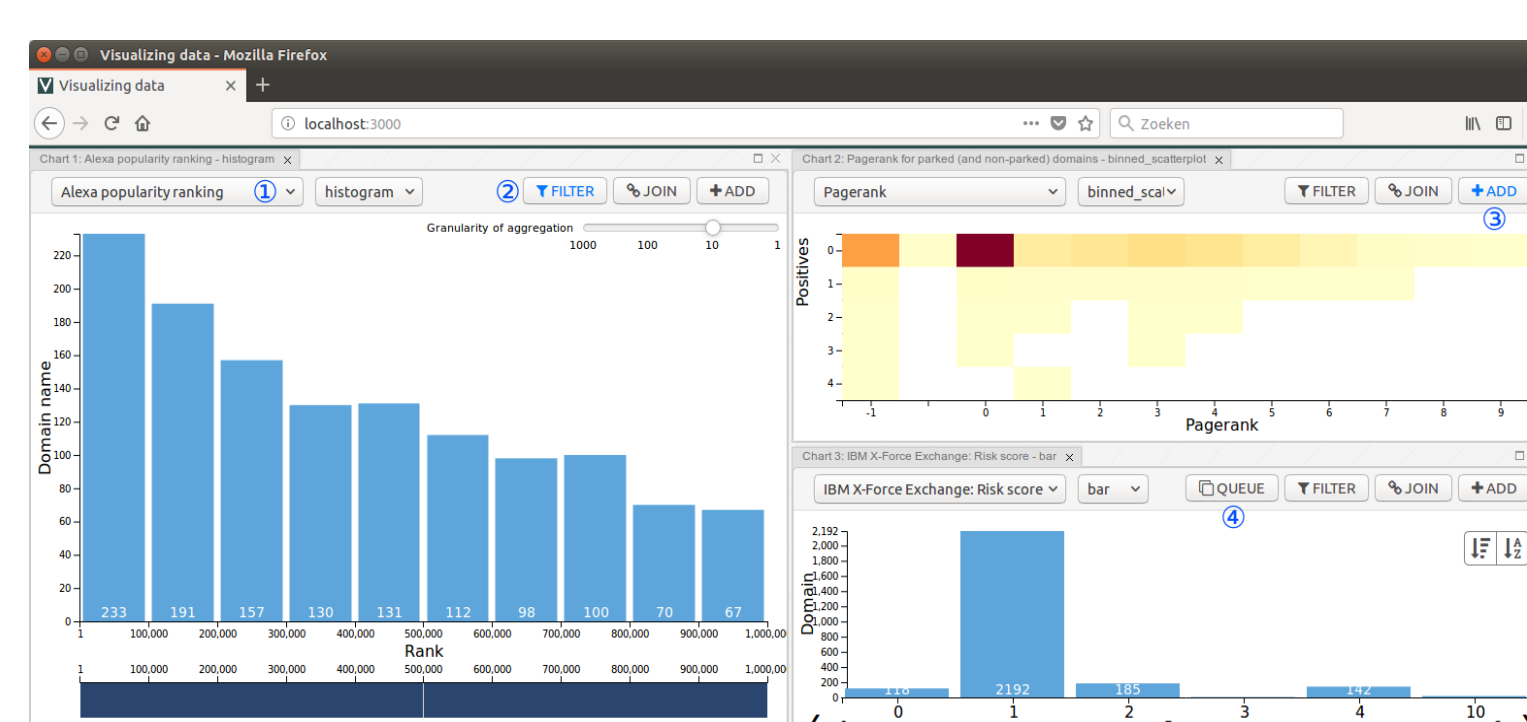
- › Background data preloading
 - › Public APIs
 - › Web crawlers (e.g. DNetCrawl)
- › Explore & combine interactively



CONCLUSION & FUTURE WORK

Visual analytics: **beneficial** to web security, if **challenges** are addressed

- › Prototype implementation of design
- › To improve: data access + analytics
- › Future: release to researchers/analysts



REFERENCES

1. Fink et al., *Visualizing cyber security: Usable workspaces*. Proc. VizSec, pp. 45-56, 2009.
2. Thomas and Cook, *Illuminating the Path: The Research and Development Agenda for Visual Analytics*, 2005.