UNIVERSITAS SCIENTIARUM SZEGEDIENSIS
UNIVERSITY OF SZEGED
Department of Software Engineering

The Security History of the WebKit Browser Engine

Renáta Hodován

Outline

- Motivation
- Background
- Analyzing the statistics
- Future work

WebKit

- Web browser engine
- Powers several desktop browsers...
  - Apple Safari
  - Google Chrome
  - Etc.
- … and mobiles
  - iPhone
  - Android
  - MeeGo

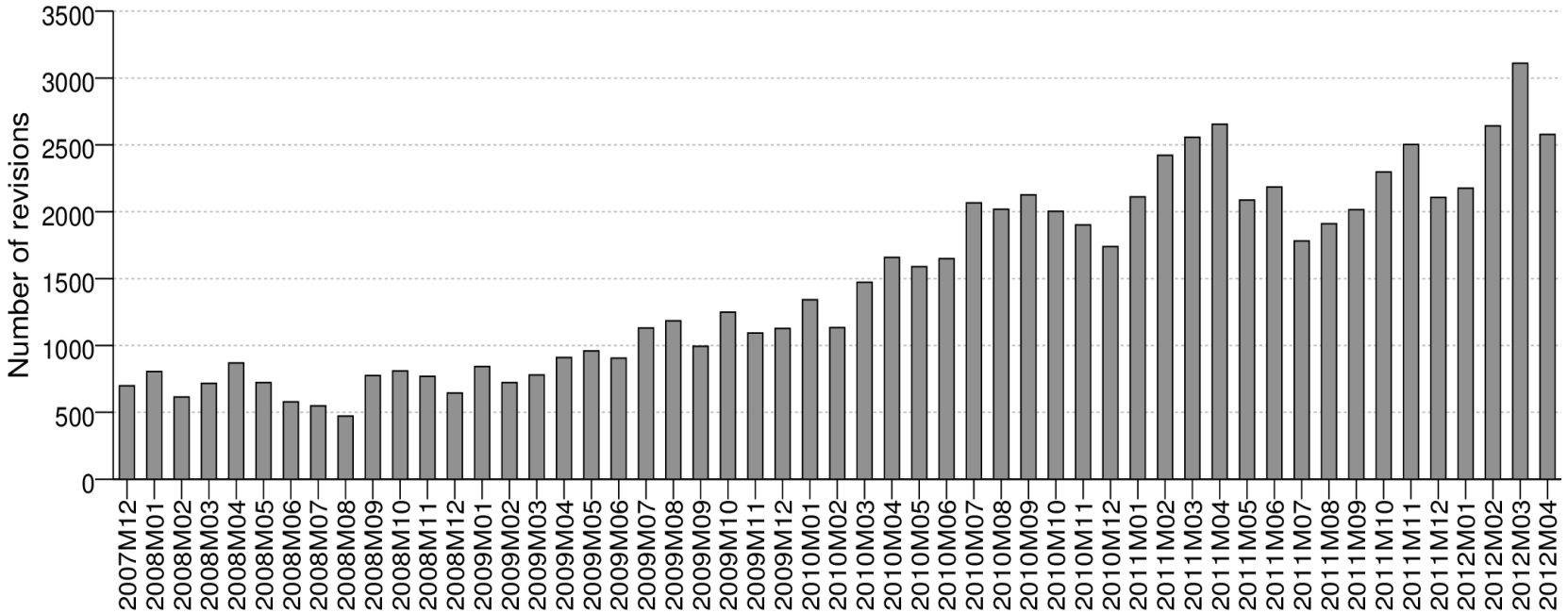
WebKit

- Open Source Project
- Bugs and requests are logged in a public Bugzilla
- Three types of bugs:
  - WebKit
  - Inspector
  - Security

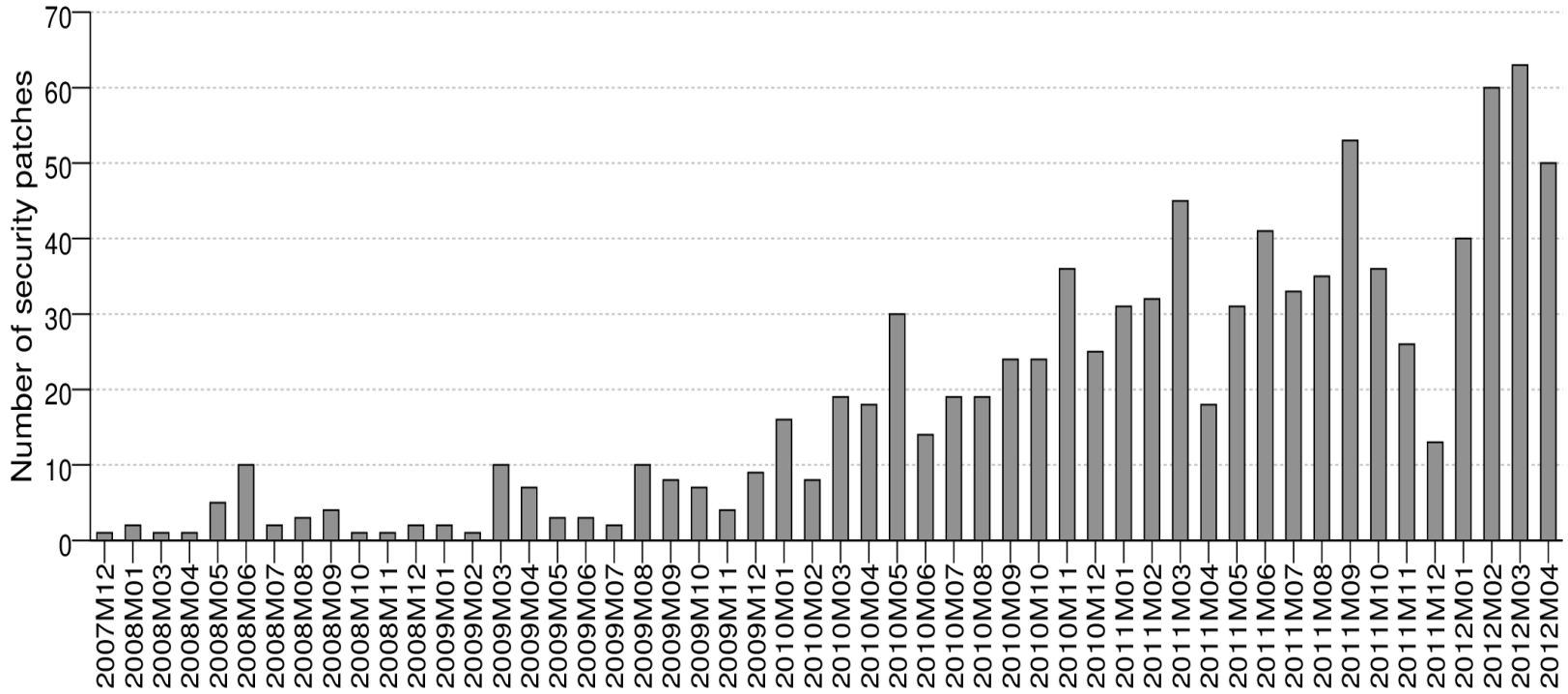
Security Bugs

- Officially: not publicly accessible
- In practice: the fixed bugs are deducible
  - Not violating any rules
  - Publishing the method would be still unethical
  - Presenting the statistical summary is permitted

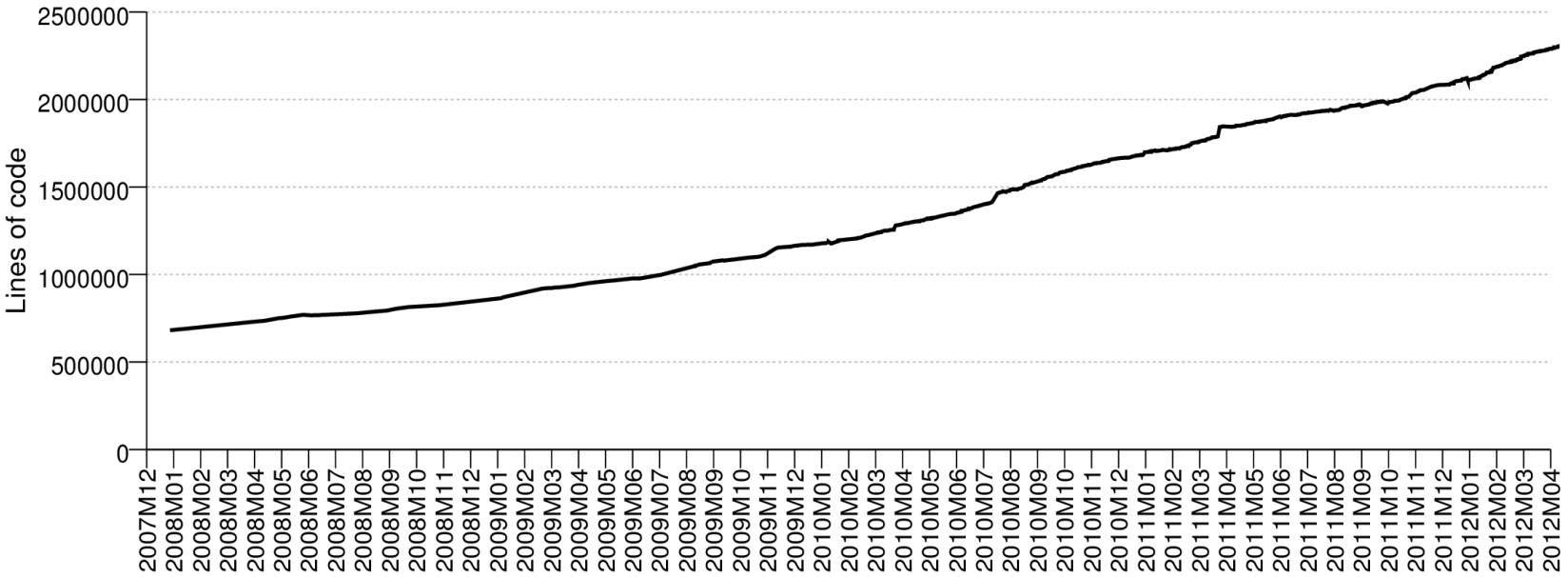
All Committed Revisions



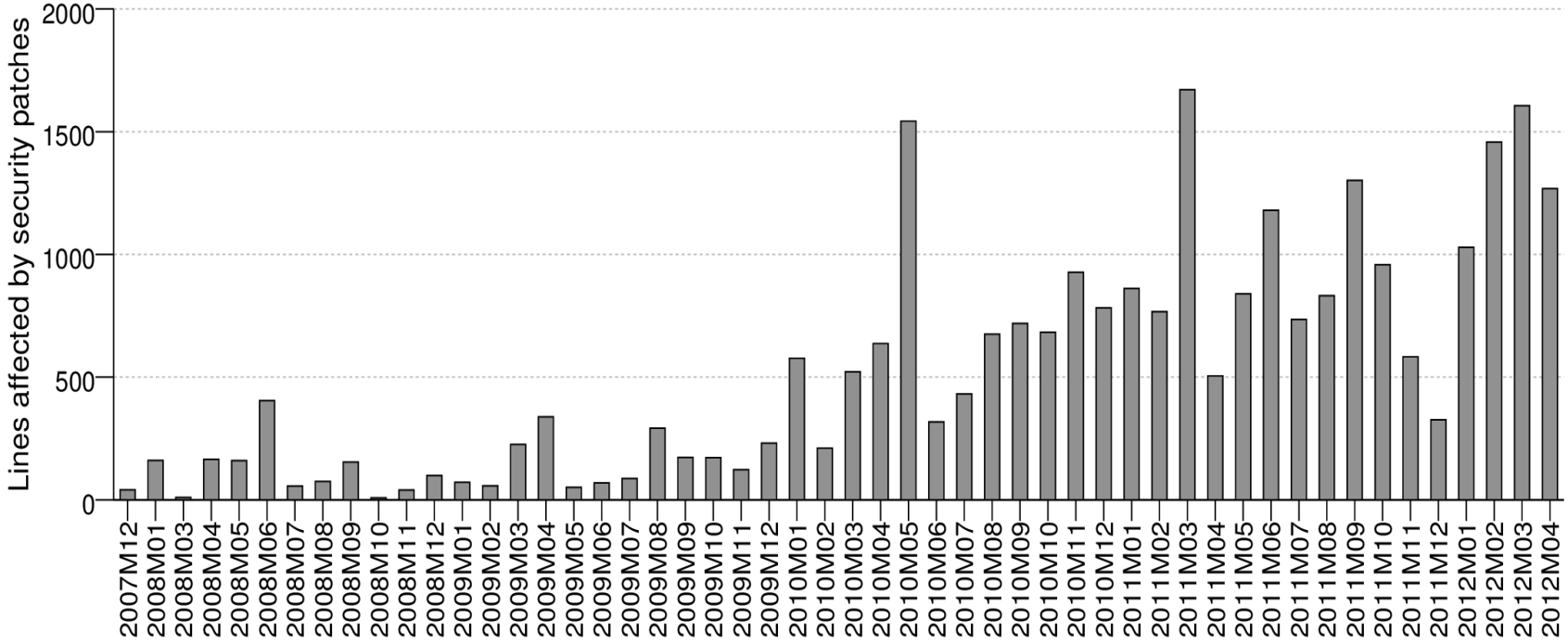
Committed Security Bug Fixes



Code Size Over Time



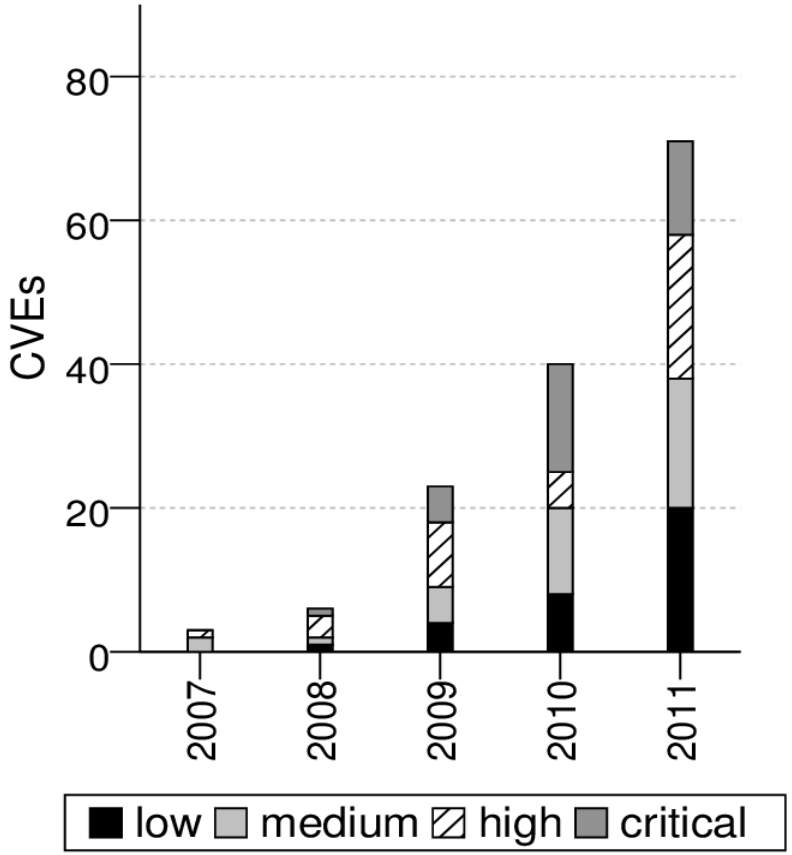
Changed Lines In Security Revisions



CVE

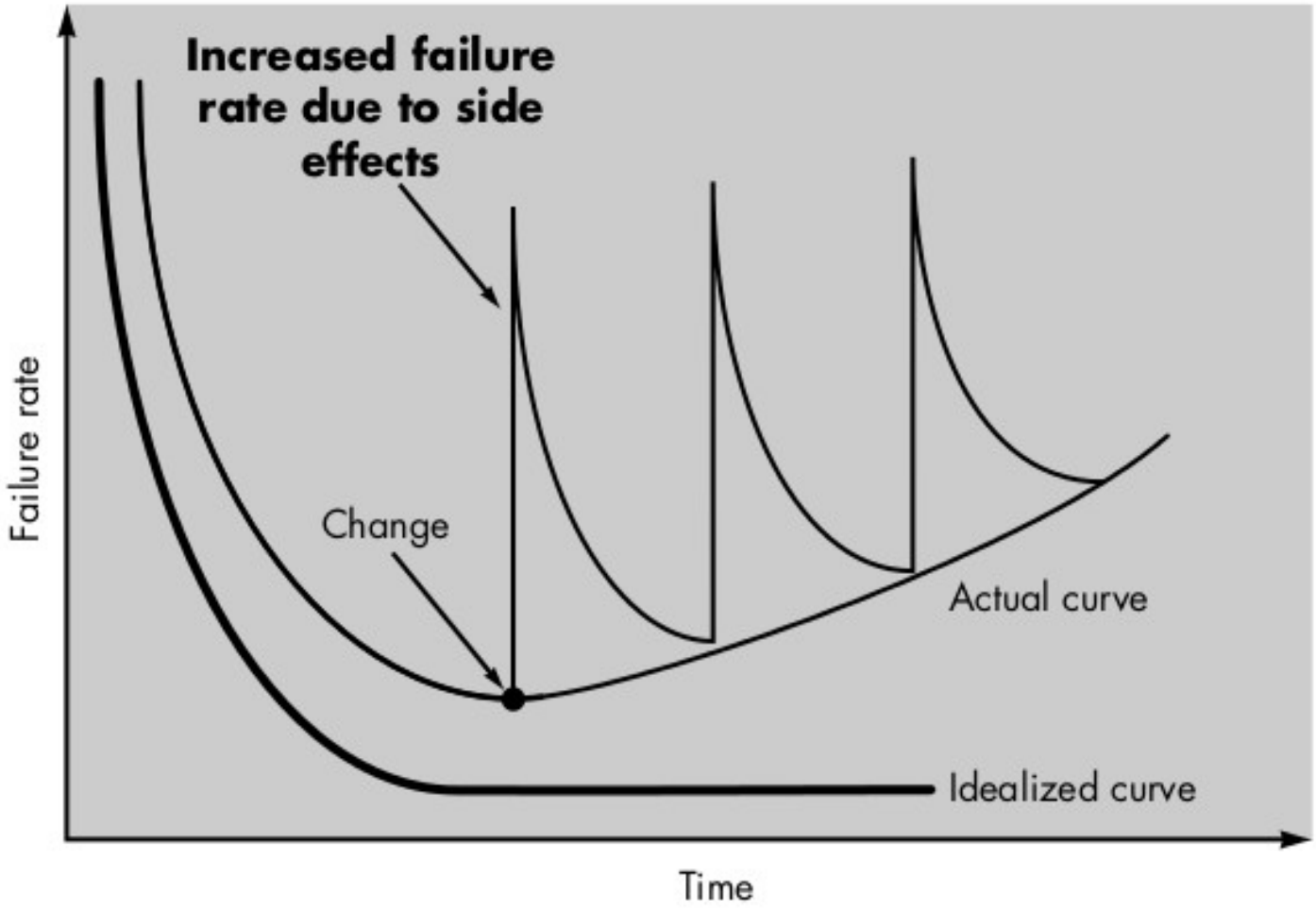
- Common Vulnerabilities and Exposures
- Provides a reference-method for publicly known information-security vulnerabilities.
- Maintained by MITRE Corporation
- Easy to filter for target
- Contains entries about WebKit from 2007

WebKit CVEs



UNIVERSITAS SCIENTIARUM SZEGEDIENSIS
UNIVERSITY OF SZEGED
Department of Software Engineering

Aging of a Software



Roger S. Pressman, Ph.D., Software Engineering A Practitioner's Approach

Summary

- Given a relatively big database of security bugs (~1000 entry)
- Relation between:
  - Speed of development
  - The size or the complexity of the code
  - The needed security fixes
- The determined trends are alarming

Future work

- Further analysis of the database
  - Looking for “Bad Smells”
- Defining “attack surface” for web browsers
- Applying these metrics for different browsers or revisions
- Sandboxing
  - SUID
  - seccomp filter

Thank you for your attention!

Acknowledgement

The publication/presentation is supported by the European Union and co-funded by the European Social Fund.

Project title: “Broadening the knowledge base and supporting the long term professional sustainability of the Research University Centre of Excellence at the University of Szeged by ensuring the rising generation of excellent scientists.”

Project number: TÁMOP-4.2.2/B-10/1-2010-2012