Plan4bugs: An Empirical Study of Bug Fixing Activities for Software Security Maintenance

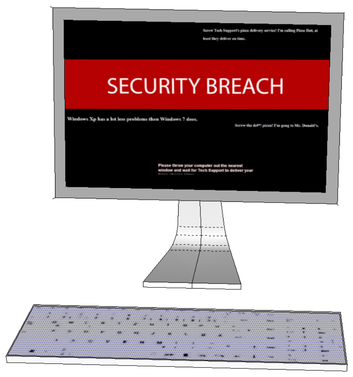
The Open University
Centre for Research in Computing

Saad Bin Saleem, Dr. Yijun Yu, Professor Bashar Nuseibeh, Professor Anne De Roeck

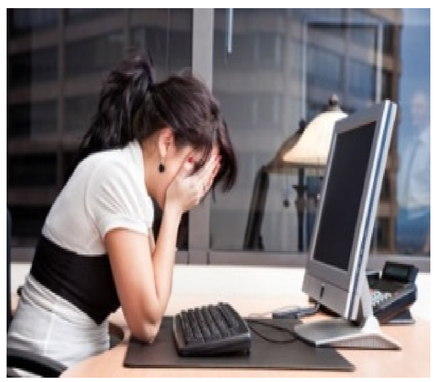
Introduction

Security attacks on software systems are common due to rapid growth of the internet and collaborative computing. They need to be fixed quickly by developers to deter the harm.

Security attack



Developer's response

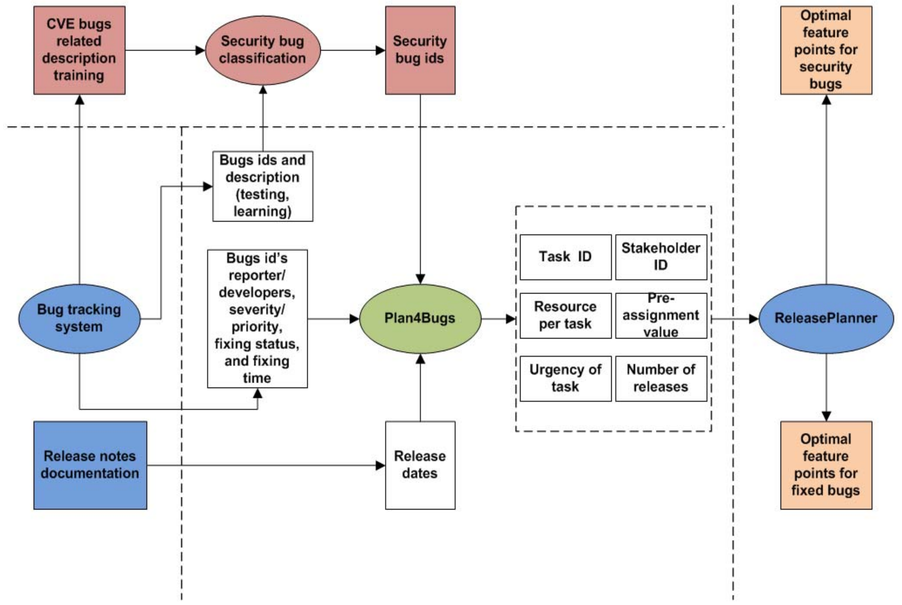


Problem

It is a practical challenge for **developers** to quickly fix the high priority **security bugs** within time and **resource constraints** in response to a **security attack**. Therefore, the following research question is addressed to measure and compare the security bug fix time.

RQ: Under tight schedule and resource constraints, what is the optimal time to fix high priority security bugs compared to fixing the other bugs?

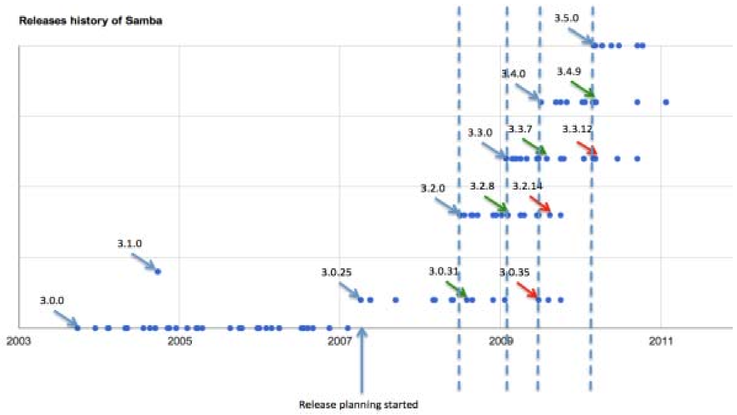
Technical Solution



To answer the research question, first a **security bug classifier** is developed**,** which uses textual descriptions of bugs to classify security and non-security bugs. Then, a toolkit **plan4bugs** is developed to turn the bug fixes data into inputs for the ReleasePlanner.

ReleasePlanner is an Industrial tool which is used to measure the bug fix time of all and security bugs only. The outputs of ReleasePlanner also helped us to compare the security and the others bug fix time.

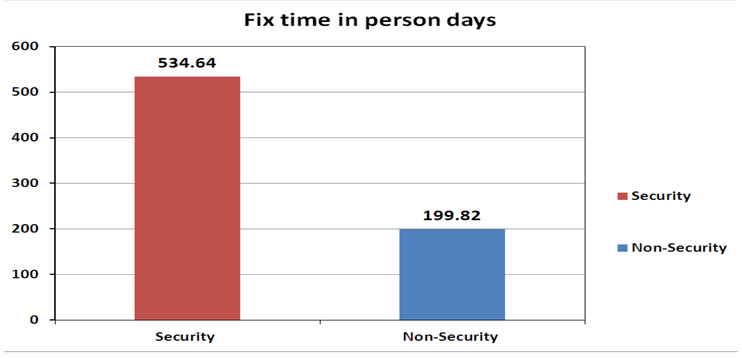
Case Study



The results are based on the Samba case study, the data was collected from Samba Bugzilla using technical solution.

Findings

The average bug fix time for security bugs is 167% longer than the other bug fix average time. The frequent reopening of security bugs than the other bugs is reason of this higher percentage.



To contact and download the papers visit **::** http://crc.open.ac.uk/People/s.b.saleem