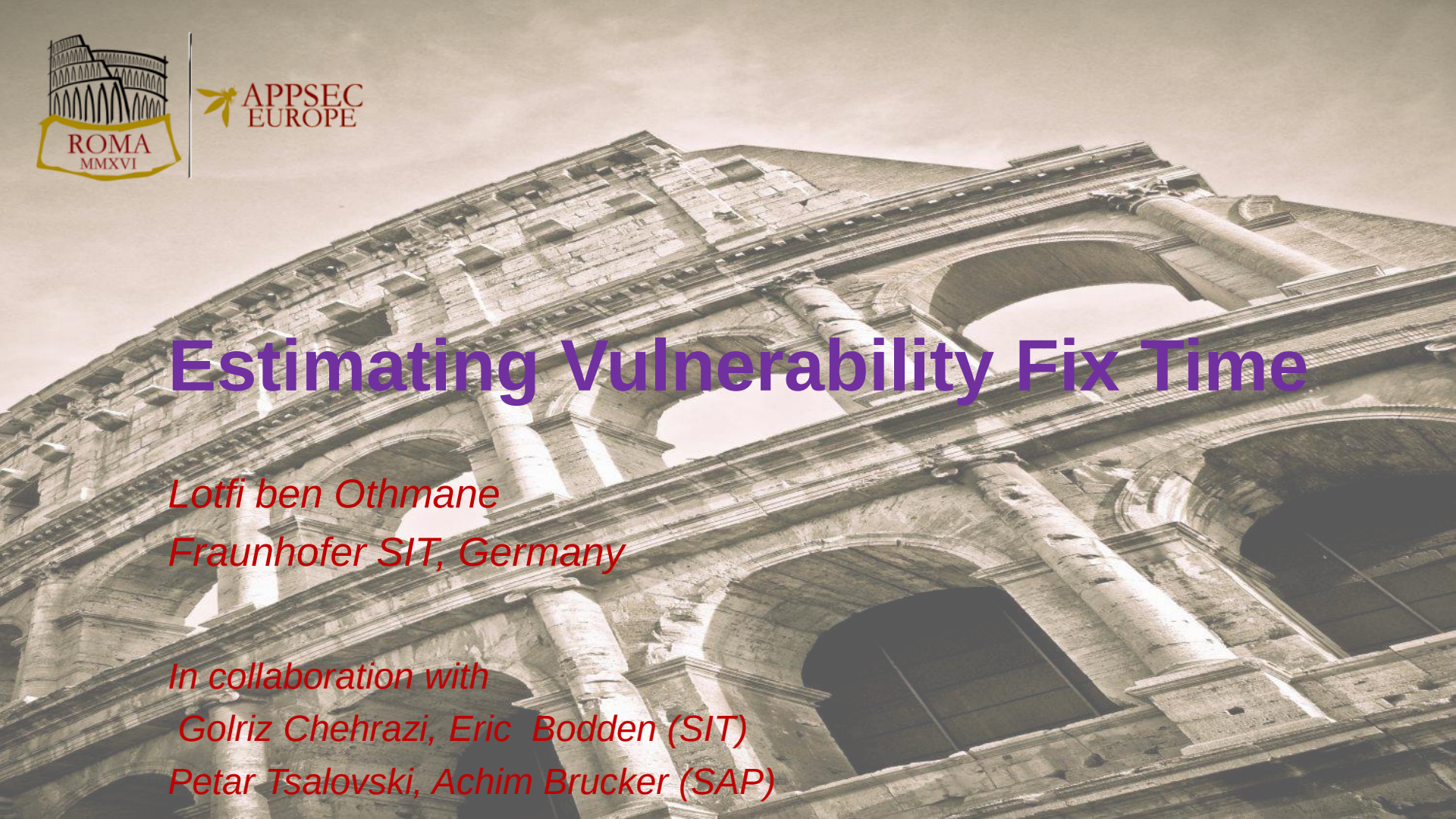


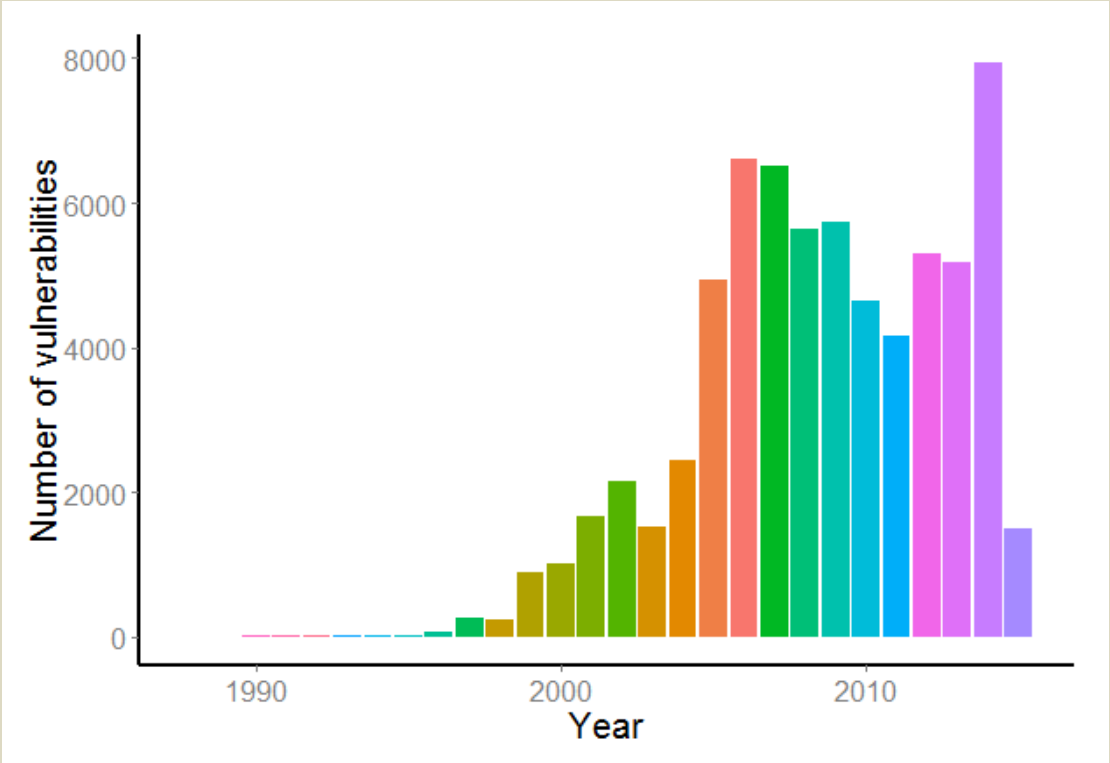
Estimating Vulnerability Fix Time

Lotfi ben Othmane
Fraunhofer SIT, Germany

In collaboration with
Golriz Chehrazi, Eric Bodden (SIT)
Petar Tsalovski, Achim Brucker (SAP)

Software Vulnerabilities

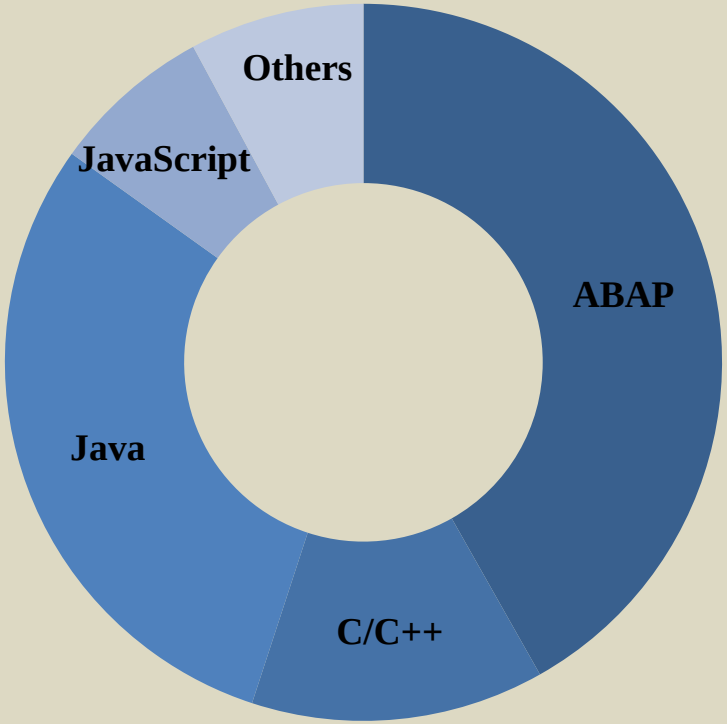
Up to 23.3.2015



ROMA MMXVI

APPSEC EUROPE

Security Testing at SAP



Language	Tool	Vendor
ABAP	CVA (SLIN_SEC)	SAP
C/C++	Coverity	Coverity
JavaScript, Ruby	Checkmarx	Checkmarx
Others	Fortify	HP

- Mandatory since 2010 for all products
- Multiple billons lines analyzed
- Constant improvements:
  - tool configuration
  - new tools and methods

The Problem

Challenge: Predict the cost of fixing a given security vulnerability

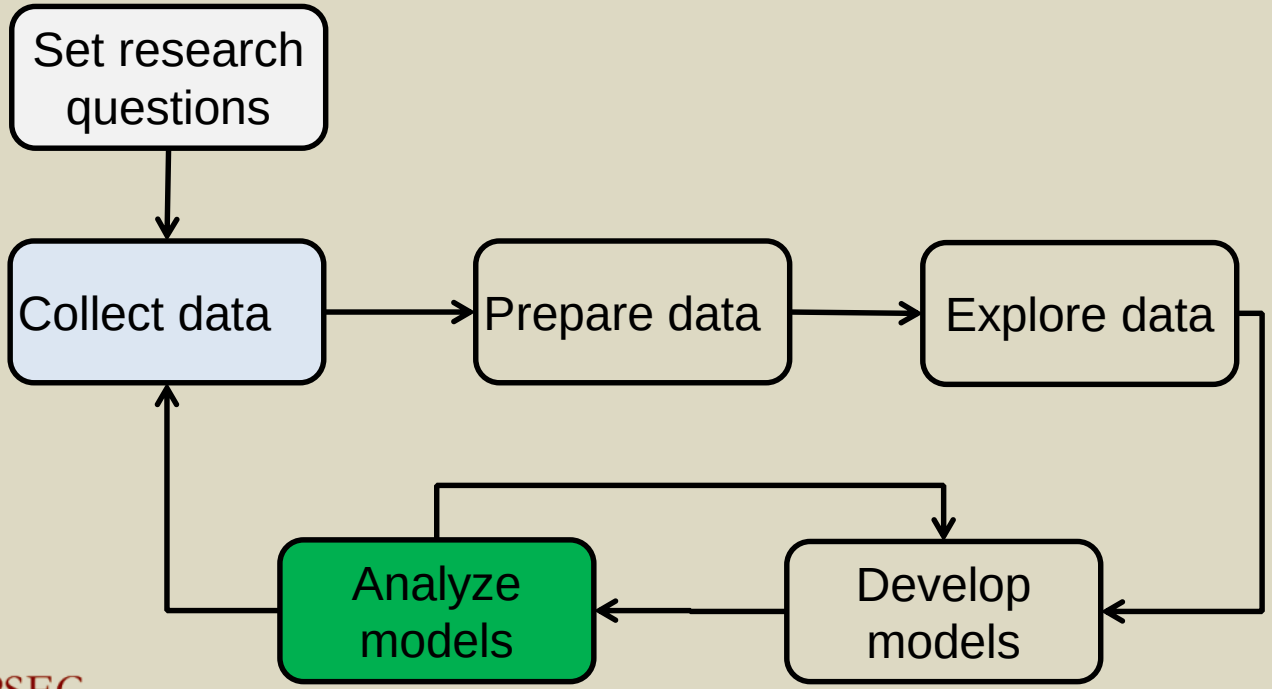
$\Rightarrow$ Predict the duration of fixing security vulnerabilities?

Let vul_fix_time = f (x_1, …….x_j)

Given collected attributes x_i?

Find out f

Research Method



ROMA MMXVI

APPSEC EUROPE

Data-Sets

1. Static analysis data of ABAP code (Data-set 1)
2. Static analysis data of Java and C Code (Data-set 2)
3. Security messages (Data-set 3)

4. Descriptive components data
5. Descriptive projects data

Extended Data-sets

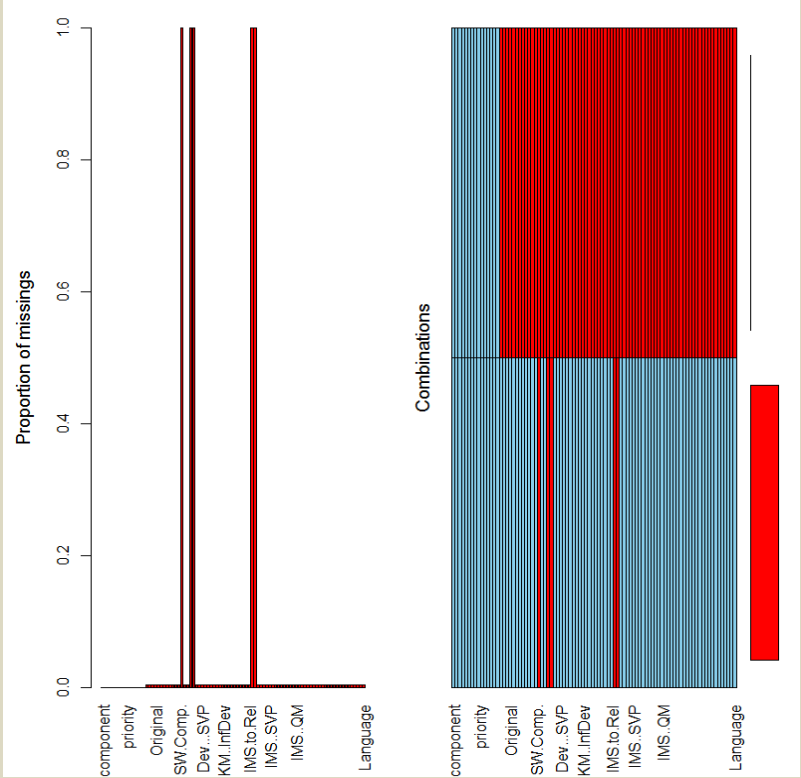
1. Pre-release issues data related to projects
   → Extension of Java- and C-issues

2. Post-release issues data related to components
   → Extension of security messages

APPSEC EUROPE

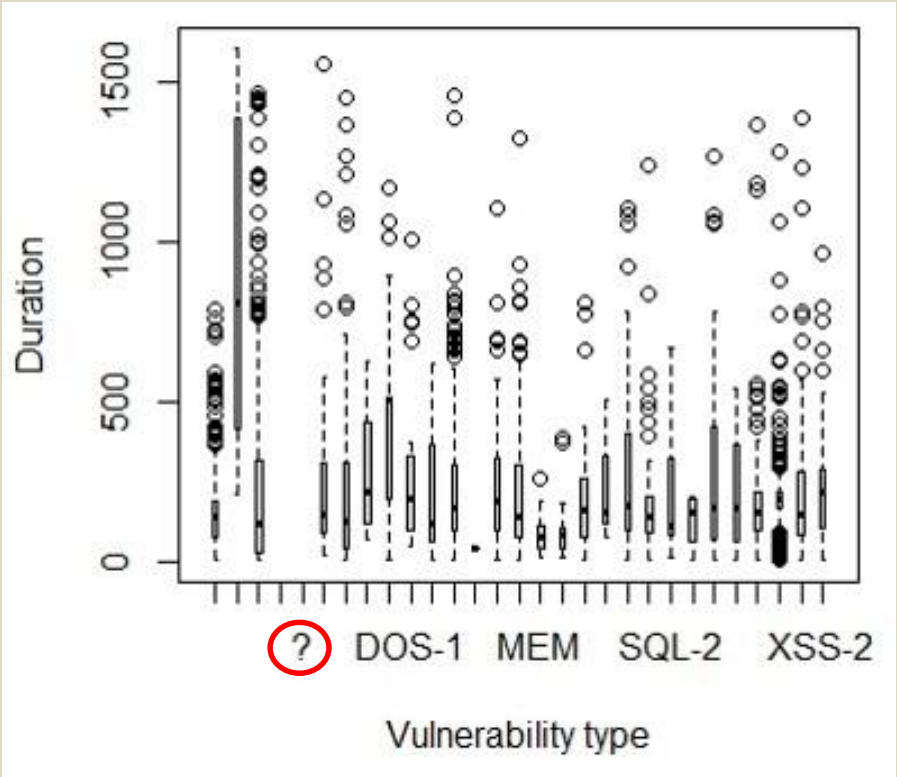
Data Preparation

- Data cleaning
- Data transformation



Data Exploration

Understand the data



ROMA MMXVI

APPSEC EUROPE

Regression Methods

1. Linear Regression (LR)
2. Tree-based regression (RPART)
3. Neural-networks regression (NN)

Used Metrics

1. Prediction accuracy
    1. Coefficient of determination
    2. Prediction level (PRED) <= 25% error
    3. Akaike Information Criterion – rate of info. Loss
2. Factors importance

Results

Output of data analysis

1. Prediction value
2. Accuracy of the prediction model
3. Most influencing factors

Prediction Models (Parts)

Message source	Coef.
(Intercept)	249.17
Code scan tool	-50.04
Central security department	-38.05
Customers	-60.68
Ext. research organizations	-102.78
Int. development departments	-12.21
Test services	-124.74
Validation services	-21.88

84) vulnerabilitytype=,&OTHER,ACI-1,CDR-1,INF-1,MAC-1,MEM,XSS,XSS-2 270 5063771.00 286.53700

168) Component=AP-RC-ANA-UI-XLS,BC-BSP,BC-CST-DP,BC-CST-IC,BC-CTS-SDM,BC-CTS-TMS,BC-DOC-HLP,BC-DOC-TTL,BC-I18,BC-JAS-ADM-MON,BC-JAS-DPL,BC-SEC,BC-SEC-DIR,BC-SRV-ARL,BC-SRV-FSI,BC-UPG-SLM,BC-UPG-TLS-TLJ,BC-WD-CMP-FPM,BC-XI-CON-AXS,BC-XI-IBD,BC-XI-IBF,BI-BIP-AUT,BI-OD-STW,BI-RA-WBI,BW-BEX-OT-MDX,CA-GTF-IC-BRO,CA-GTF-IC-SCR,CA-GTF-RCM,CRM-BF,CRM-BF-SVY,CRM-CIC,CRM-IC-EMS,CRM-IC-FRW,CRM-IPS-BTX-APL,CRM-ISA,CRM-ISA-AUC,CRM-ISE,CRM-LAM-BF,CRM-MD-PRO,CRM-MKT-DAM,CRM-MKT-MPL,CRM-MSA,FS-CM,FS-SR,IS-A-DP,IS-U-CS-ISS,LO-AB-BSP,LO-GT,MFG-ME,MOB-APP-EMR-AND,PA-GE,PLM-PPM-PDN,PLM-WUI-RCP,PSM-GPR-SN,SBO-INT-B1ISN,SCM-EWM-RF,XAP-IC-IDM,XX-PROJ-CDP-TEST-296 119 1015233.00 205.82350 *

169) Component=AP-CFG,AP-LM-MON-HC,AP-LM-SUP,AP-RC-ANA-RT-MDA,AP-RC-RSP,AP-RC-UIF-RT,AP-SDM-EXC,BC-CCM-MON-OS,BC-CCM-SLD-JAV,BC-CST,BC-CUS-TOL-CST,BC-DB-ORA-INS,BC-DOC-TER,BC-ESI-WS-ABA,BC-ESI-WS-JAV-RT,BC-FES-BUS-RUN,BC-JAS-ADM-ADM,BC-JAS-COR,BC-JAS-SEC-UME,BC-MID-RFC,BC-SEC-SAL,BC-SRV-COM,BC-SRV-COM-FTP,BC-SRV-KPR-CS,BC-SRV-MCM,BC-SRV-SSF,BC-WD-ABA,BC-WD-

ROMA MMXVI

APPSEC EUROPE

Accuracy of Prediction

Metric / DS	Residual	AIC	PRED
ABAP	LR(0.526)	LR (122465)	LR (31.81%)
C++ Java Cov./Fort.	LR (0.461)	LR (334565)	NN (33.81%)
Ext. C++ Java	LR (1)	RPART(463)	LR (100%)
Sec msg	LR (0.944)	RPART(6507)	RPART (34.71%)
Ext. sec msg	LR (0.909)	RPART(6421)	NN (65.05%)

Factor Importance

Factors for data-set 3

Factor	Metric
Component	2.83
Processor	2.75
Reporter	1.78
Vulnerability type	0.83
Source	0.46
CVSS score	0.02

Factor for data-set 1

Factor	Metric
Project ID	0.27
Vulnerability name	0.09
Vulnerability count	0.07
Priority	0.01

Factor for data-set 2

Factor	Metric
Scan status	0.96
Project name	0.73
Vulnerability name	0.51
Priority	0.30
Scan source	0.25
Vulnerability count	0.08
Folder name	0.08

Factor Importance

Factors for extended data-set 3

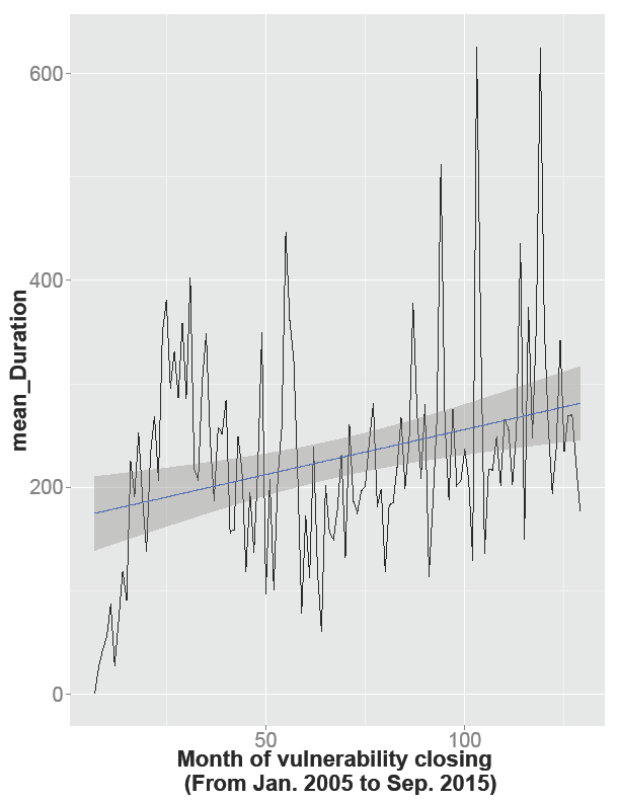
Factor	Metric
Processor	2.98
Component	2.94
Reporter	1.69
Dev_comp_owner	1.27
Dev_prod_owner	1.09
Vulnerability type	0.60
Priority	0.06

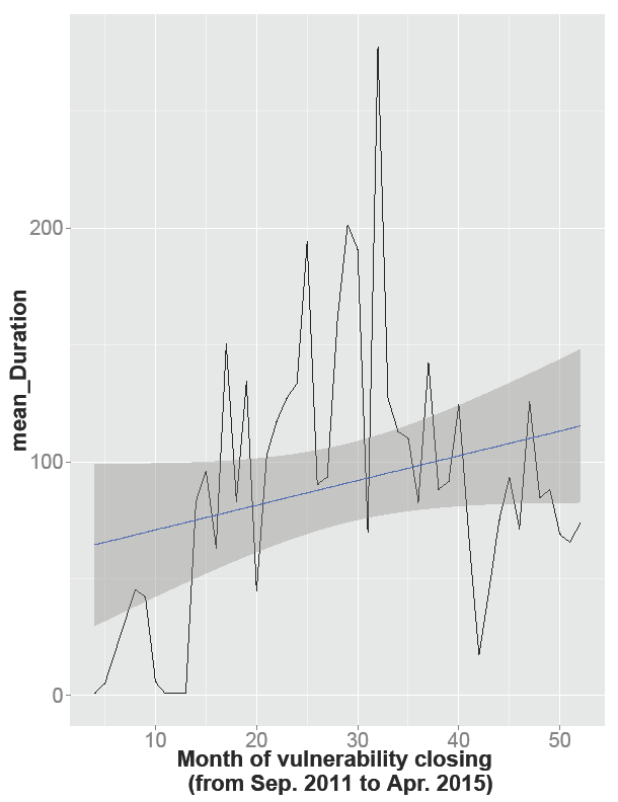
Factors for extended data-set 2

Factor	Metric
FixToRelease_period	0.95
Dev_period	0.68
Int_prg_name	0.68
Prg_lead_resp	0.68
Risk expert	0.68
FoundToRelease_period	0.41
Vulnerability name	0.48
Vulnerability count	0.08
Folder name	0.04
Priority	0.02

Evolution of The Average VFT

Sec. messages





Fort./Cov.

Use of The Results

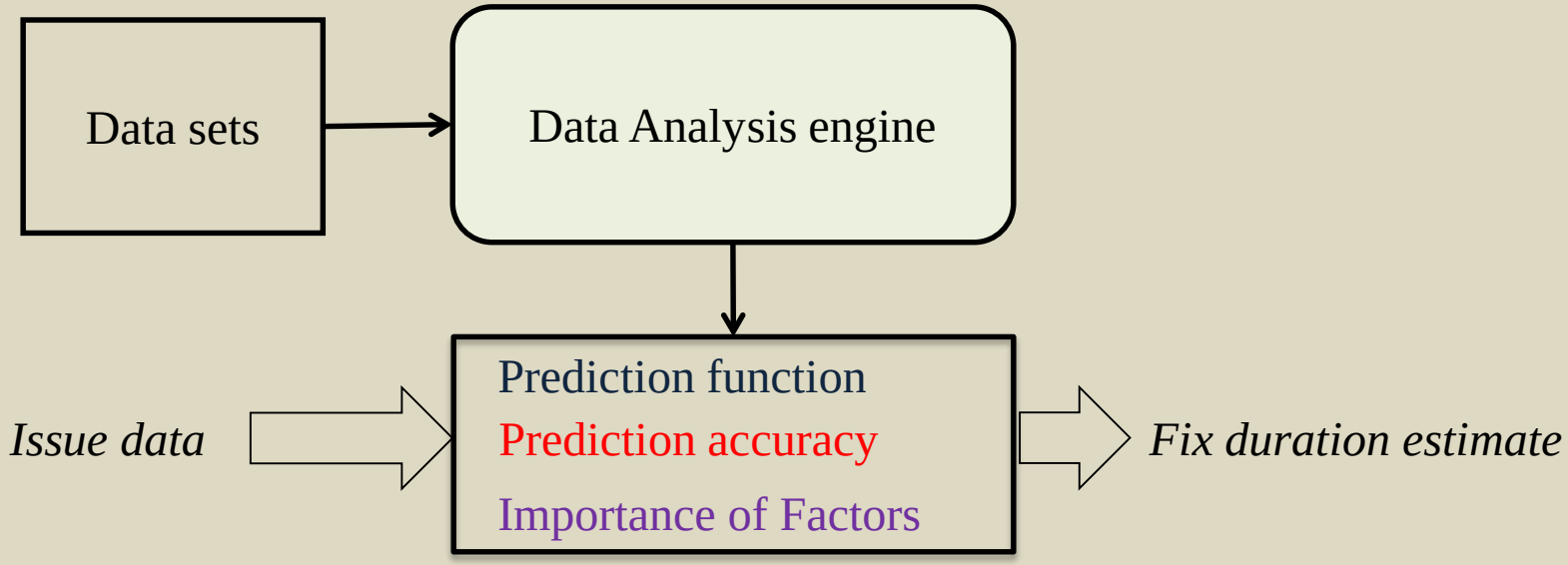
- We have Duration_i = Predict (FIT, INPUT)

=> Provide a set information about a new project and get a cost estimation of fixing security vulnerabilities

$$Total_{Cost}(in\ time) = \sum_j (count_j * cost_j)$$

The Prototype

Provide estimate for fixing given issues



Lessons Learned From the Data Analytics

- Dominant factors for pre-release
  - Project-related characteristics
  - Development-team

- Dominant factors for post-release
  - Components characteristics
  - Human-related factors

Lessons Learned From the Data Analytics

- Difficult to choose among the machine learning methods
- Prediction models depend on the time frame of the data

Further Use of The Results

- Results could be used:
  - as indicator to improve the process
  - to measure the impact of process changes
  - to justify decisions in secure development activities

APPSEC EUROPE

Conclusions

- Vulnerability type is not the most important factor that impacts the vulnerabilities fix time
- The software structure and human factors are dominant factors contributing to the vulnerabilities fix time

Thank you!

ANY QUESTIONS?

lotfi.ben.othmane@sit.fraunhofer.de