DISCOVRE

Efficient Cross-Architecture Identification of Bugs in Binary Code

OUTLINE

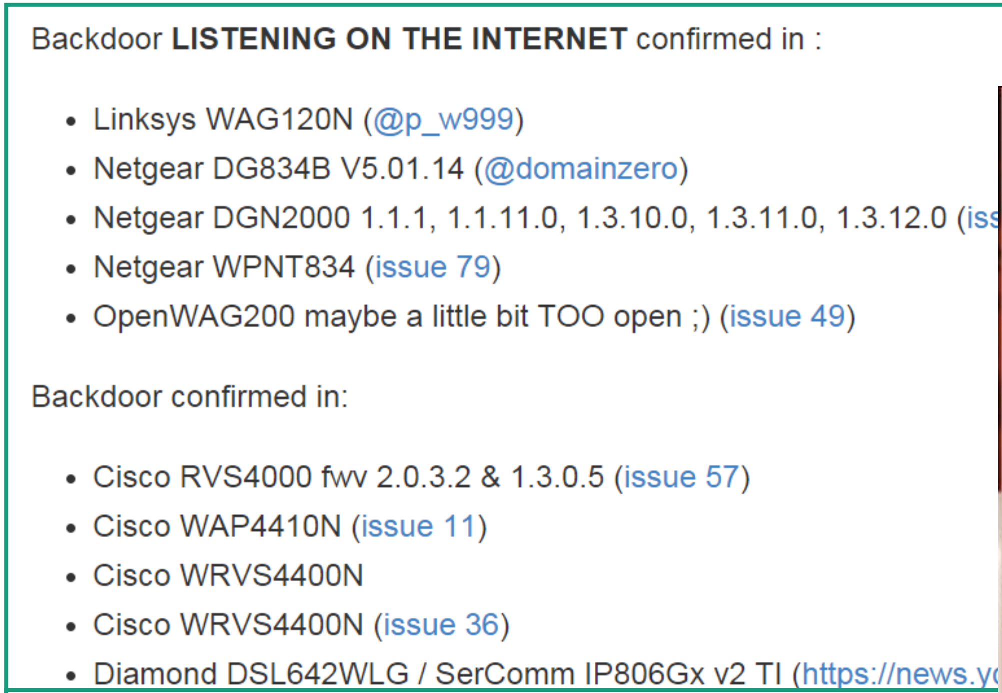
1. Motivation

2. Baseline

3. Derivation of discovRE‘s Key Properties

4. Cross-Architecture Bug Search

Motivation – Finding Firmware Bugs

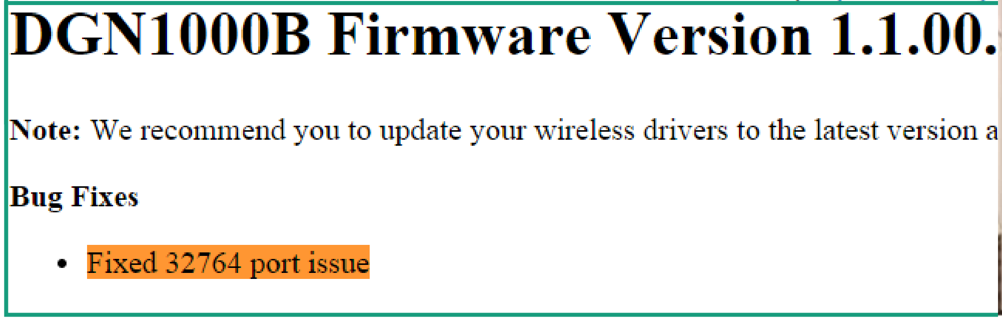


Backdoor **LISTENING ON THE INTERNET** confirmed in :

- Linksys WAG120N (@p_w999)
- Netgear DG834B V5.01.14 (@domainzero)
- Netgear DGN2000 1.1.1, 1.1.11.0, 1.3.10.0, 1.3.11.0, 1.3.12.0 (iss
- Netgear WPNT834 (issue 79)
- OpenWAG200 maybe a little bit TOO open ;) (issue 49)

Backdoor confirmed in:

- Cisco RVS4000 fwv 2.0.3.2 & 1.3.0.5 (issue 57)
- Cisco WAP4410N (issue 11)
- Cisco WRVS4400N
- Cisco WRVS4400N (issue 36)
- Diamond DSL642WLG / SerComm IP806Gx v2 TI (https://news.yc



DGN1000B Firmware Version 1.1.00.

Note: We recommend you to update your wireless drivers to the latest version a

Bug Fixes

- Fixed 32764 port issue

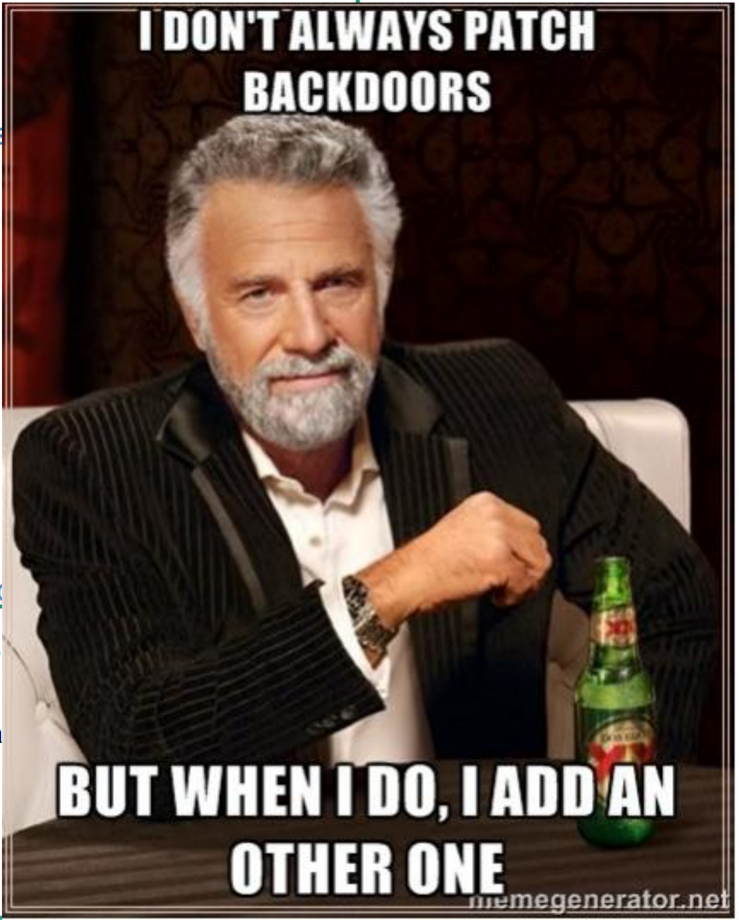

I DON'T ALWAYS PATCH BACKDOORS
BUT WHEN I DO, I ADD AN OTHER ONE
memegenerator.net

Image source: https://github.com/elvanderb/TCP-32764

Baseline

Image source: https://www.vectorstock.com/royalty-free-vector/1068869

Generation of a Ground Truth

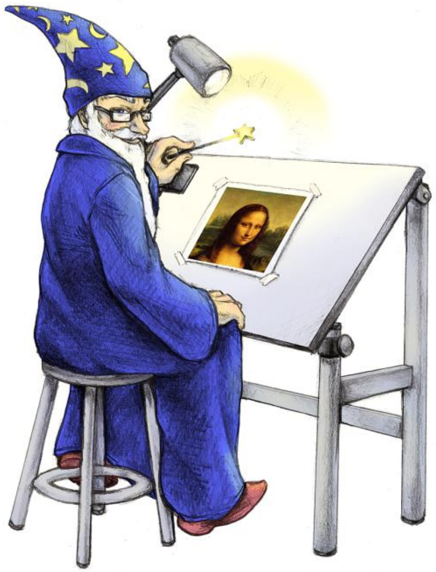
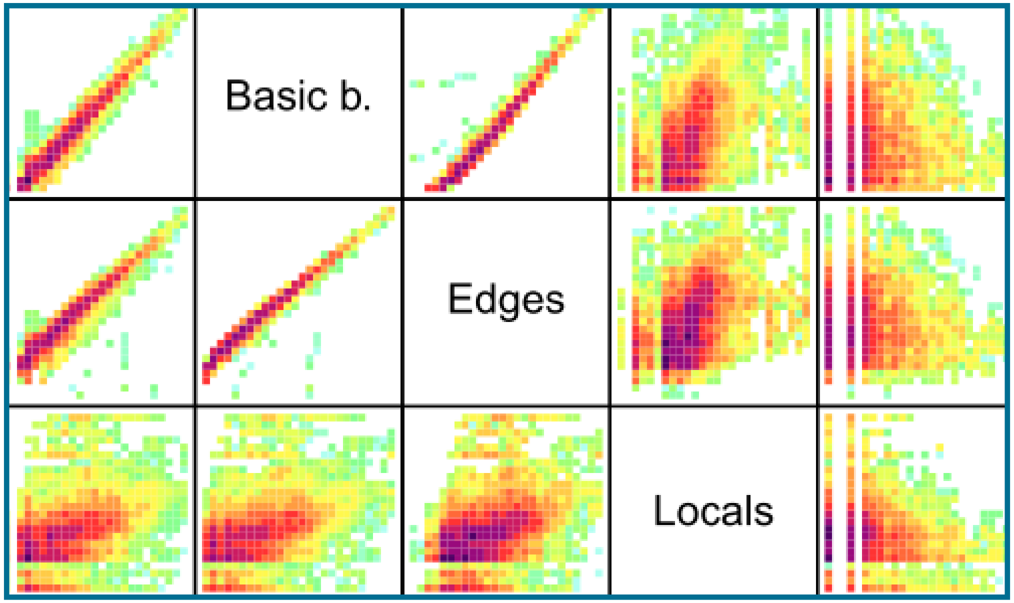


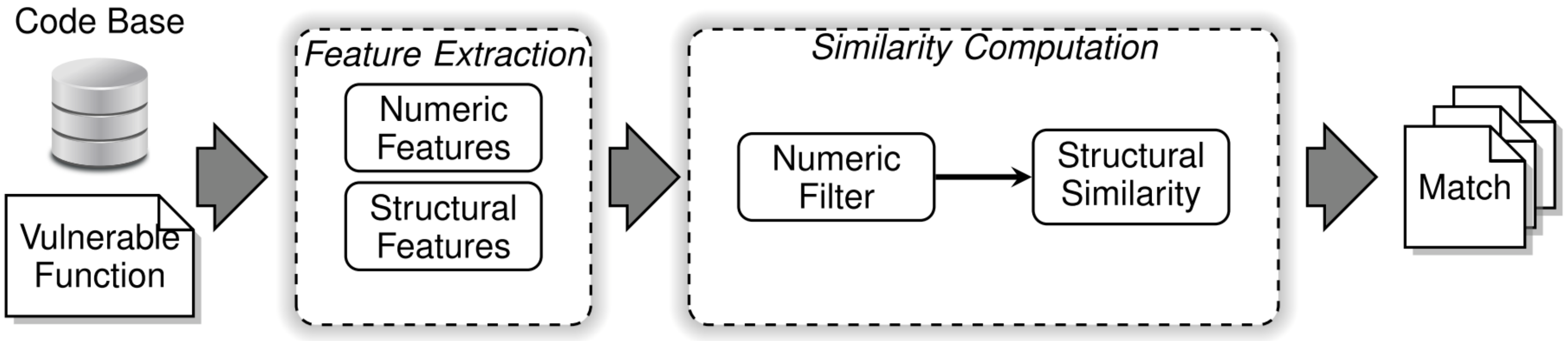
Image source: http://www.imagemagick.org/image/wizard.png

© Sebastian Eschweiler, Cyber Analysis and Defense Department, Fraunhofer FKIE

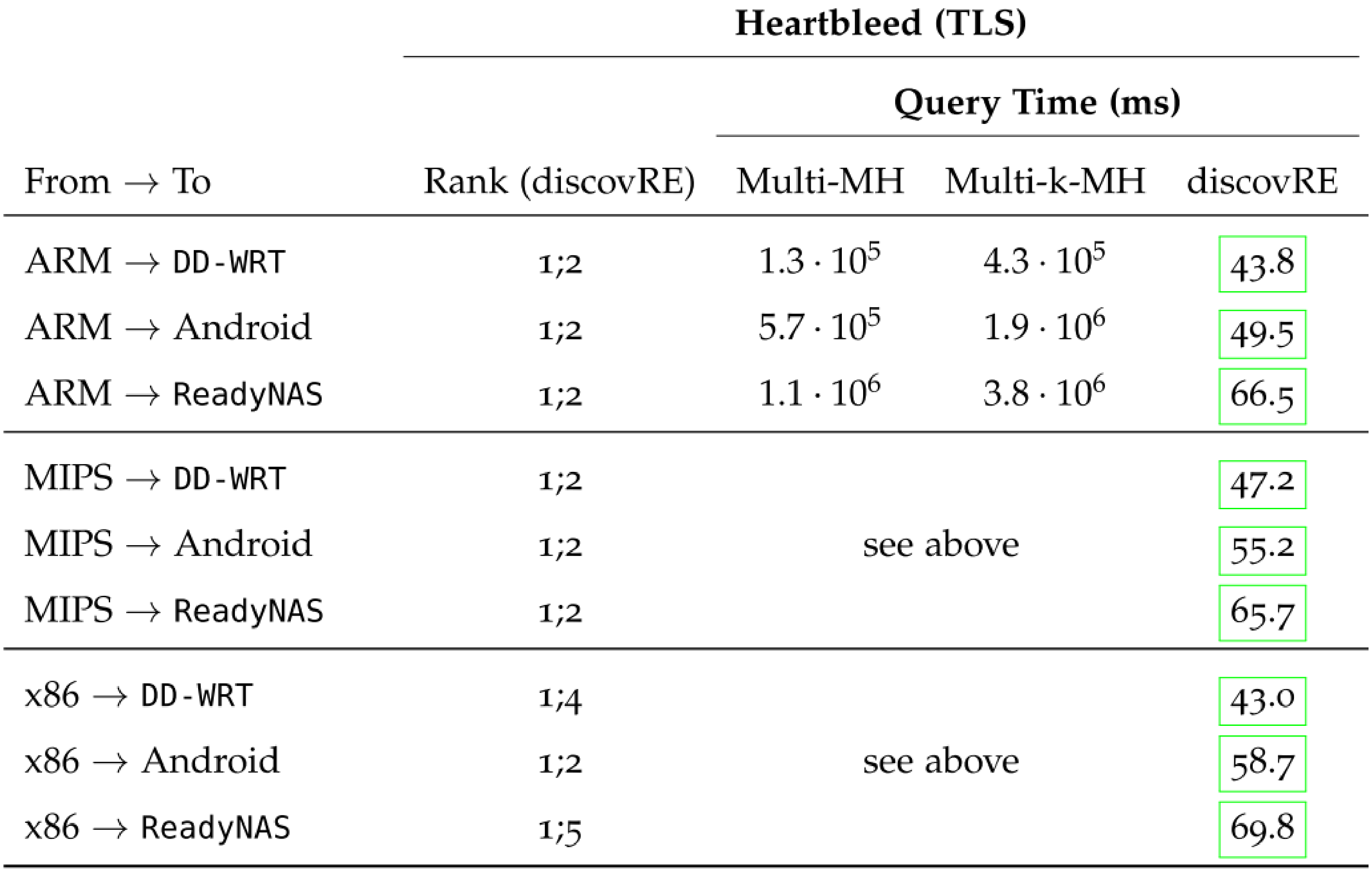
Derivation of discovRE's Key Properties



discovRE


Code Base
Vulnerable Function
Feature Extraction
Numeric Features
Structural Features
Similarity Computation
Numeric Filter
Structural Similarity
Match

Cross-Architecture Bug Search



	Heartbleed (TLS)			
		Query Time (ms)		
From → To	Rank (discovRE)	Multi-MH	Multi-k-MH	discovRE
ARM → DD-WRT	1;2	$1.3 \cdot 10^5$	$4.3 \cdot 10^5$	43.8
ARM → Android	1;2	$5.7 \cdot 10^5$	$1.9 \cdot 10^6$	49.5
ARM → ReadyNAS	1;2	$1.1 \cdot 10^6$	$3.8 \cdot 10^6$	66.5
MIPS → DD-WRT	1;2	see above		47.2
MIPS → Android	1;2			55.2
MIPS → ReadyNAS	1;2			65.7
x86 → DD-WRT	1;4	see above		43.0
x86 → Android	1;2			58.7
x86 → ReadyNAS	1;5			69.8

Conclusion

- Systematic analysis of a wide collection of function-level features

- Multi-staged approach to find similar functions in large code bases

- discovRE is able to discover vulnerable functions in complete firmware images fast:
  < 1 hour preparation time
  < 100 ms query time

THANK YOU FOR YOUR ATTENTION.