# A Large-Scale Analysis of the Security of Embedded Firmwares

Presented by Zhenyu Ning

# Contents

1. Background

2. Motivation & Challenges

3. Architecture

4. Analysis Result & Case study

5. Conclusion

# Contents

1. Background

2. Motivation & Challenges

3. Architecture

4. Analysis Result & Case study

5. Conclusion

# Firmware

- IEEE definition: Combination of a hardware device and computer instructions or computer data that reside as read-only software on the hard ware device.
- Software that is embedded in a hardware device.

# Contents

1. Background

2. Motivation & Challenges

3. Architecture

4. Analysis Result & Case study

5. Conclusion

# Motivation

- Physically analysis
  - Cost
  - Operability
- Online device analysis
  - Difficulty
  - Ethic

# Challenges

- Building a Representative Dataset
- Firmware Identification
- Unpacking and Custom Formats
- Scalability and Computational Limits
- Results Confirmation

# Contents

1. Background

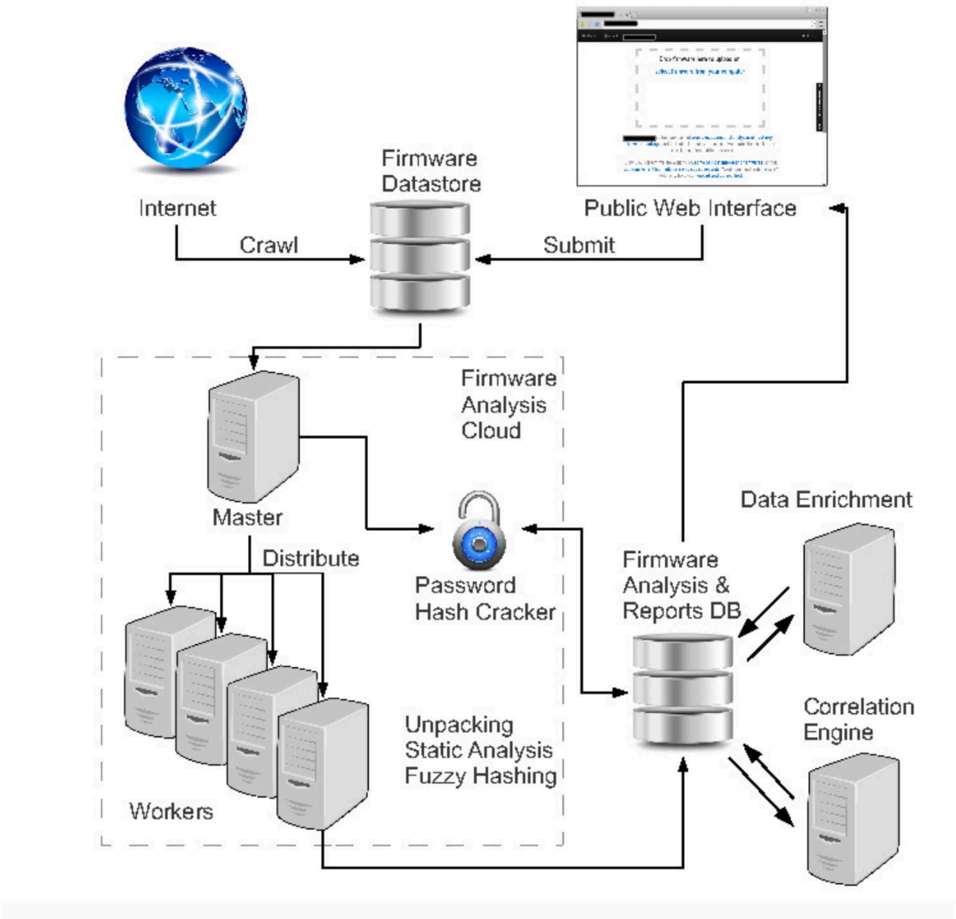
2. Motivation & Challenges

3. Architecture

4. Analysis Result & Case study

5. Conclusion

# Architecture



# Firmware Acquisition and Storage

- Web crawler
  - FTP Index Engine
  - GCSE
- Web submission interface

# Unpacking and Analysis

- Unpacking
  - binwalk, FRAK, BAT

- BAT
  - low false positive
  - recursive unpacking
  - generic interface

# Unpacking and Analysis (Cont.)

- Password Hash Cracking
  - John The Ripper
  - A Dictionary built from common password lists and resources.
- Parallelizing the Unpacking and Analysis

# Correlation Engine

- Comparison
  - Shared Credentials and Self-Signed Certificates
  - Keywords
  - Fuzzy hashes
- Future work
  - Distributed comparison and clustering infrastructure
  - “bins” partitioning approach

# Data Enrichment

- Automated queries
    - <title> tag of web pages
    - authentication realms of web servers
- Passive scans
    - SSL certificates
    - ZMap

# Contents

1. Background

2. Motivation & Challenges

3. Architecture

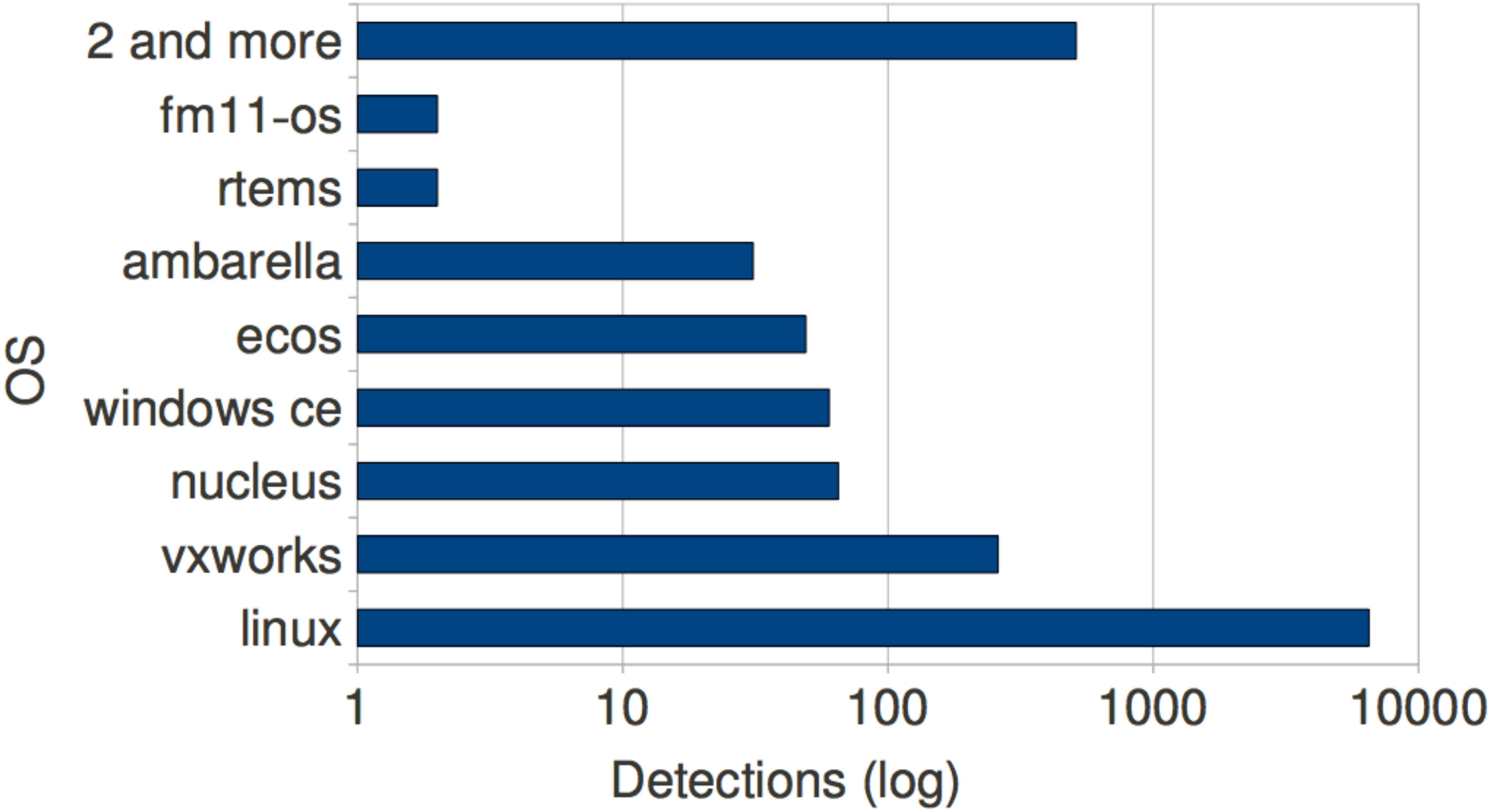
4. Analysis Result & Case study

5. Conclusion

# General Dataset Statistics

- 172,751 files out of 759,273 files collected by crawler.
- 32,356 firmware images out of 172,751 files.
- 26,275 images successfully unpacked

# Files Formats



# Results Overview

- Password Hashes Statistics
- Certificates and Private RSA Keys Statistics
- Packaging Outdated and Vulnerable Software
- Building Images as root
- Web Servers Configuration

# Case study

- Backdoors
  - Plain text search
- Private SSL Key
  - Common vulnerable components
- XSS in WiFi Enabled SD Cards
  - Manually vulnerability confirmation

# Contents

1. Background
2. Motivation & Challenges
3. Architecture
4. Analysis Result & Case study
5. Conclusion

# Conclusion

- Large-scale static analysis
  - Beneficial
  - Desirable
- Future work
  - Continue analysis on current firmware image
  - Improve analysis technique

# Reference

- Costin, Andrei, et al. "A large-scale analysis of the security of embedded firmwares." *USENIX Security Symposium*. 2014.

# Thank you!