On the Malware Detection Problem: Challenges & Novel Approaches

Marcus Botacin[1], Paulo Lício de Geus[2], André Grégio[1]

[1]PhD. Candidate
Federal University of Paraná (UFPR)
mfbotacin@inf.ufpr.br

[2]Co-Advisor
Institute of Computing - UNICAMP
paulo@lasca.ic.unicamp.br

[1]Advisor
Federal University of Paraná (UFPR)
gregio@inf.ufpr.br

Topics

Topics

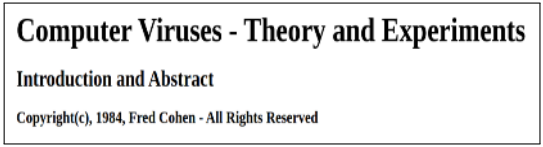
Security remains "unsolved".

Source: `https://thehackernews.com/2021/03/why-do-companies-fail-to-stop-breaches.html`

The Reasons (1/2)

1. Security is Hard!

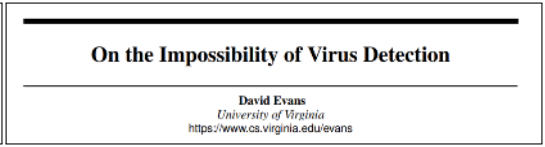
Malware Computation Theory


Computer Viruses - Theory and Experiments

Introduction and Abstract

Copyright(c), 1984, Fred Cohen - All Rights Reserved

Figure: **Source:** https://web.eecs.umich.edu/~aprakash/eecs588/handouts/cohen-viruses.html


On the Impossibility of Virus Detection

David Evans
University of Virginia
https://www.cs.virginia.edu/evans

Figure: **Source:** https://www.cs.virginia.edu/~evans/pubs/virus.pdf

```
1 Application:
2     do_something() // returns?
3     malicious()
```

Code 1: Malware detection and the halting problem.

Don't Give up!

Approximations* of Security

Evaluation Criteria

Effectiveness

- Do AVs really detect the malware samples?

Efficiency

- How much resources do AVs require to operate?

Aren't AVs effective?

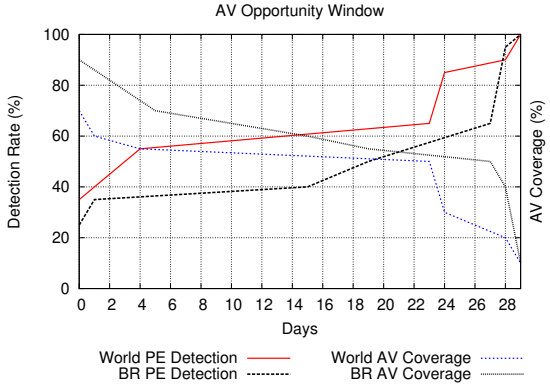


Figure: **Source:** We Need to Talk About AVs (2020).

Attack Opportunity Window. How long does it take for AVs to detect new samples?

Aren't AVs effective?

Figure: **Source:** `https://tinyurl.com/yyphbxjc`

Aren't AVs efficient?

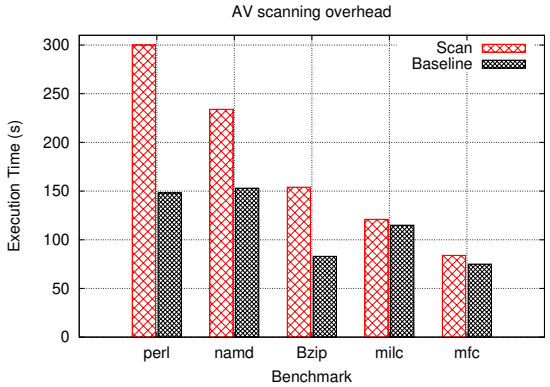


Figure: **Source:** Near-Memory and In-Memory Detection of Fileless Malware (2020).

Memory Scan Overhead.
How much SPEC benchmark applications are affected?

Aren't AVs efficient?

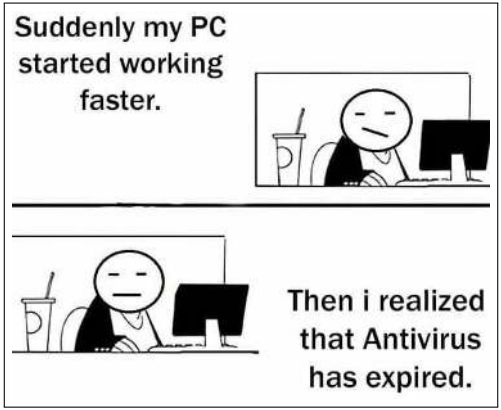


Figure: **Source:** `https://tinyurl.com/y39vquku`

The Reasons (2/2)

2. Security lacks a Method!

The Science of Security

Herley and Oorschot (2017) about the JASON report

"*The science seems under-developed in reporting experimental results, and consequently in the ability to use them. The research community does not seem to have developed a generally accepted way of reporting empirical studies so that people could reproduce the work*"

Shostack and Stewart (2008). The New School of Information Security.

"*We don't want to minimize the difficulties involved in answering such questions. We can't arrange a set of companies in test tubes, add heat, and see what comes out. In that respect, our data sources are more like those of astrophysicists or sociologists than those that a chemist or physicist might create by careful design. But this doesn't mean we can't learn from observation.*"

The importance of methods in science

Auguste Comte and the Positivism

"*On the subject of stars, all investigations which are not ultimately reducible to simple visual observations are...necessarily denied to us...we shall not at all be able to determine their chemical composition or even their density... I regard any notion concerning the true mean temperature of the various stars as forever denied to us.*"

Astronomy Nowadays, Scientific American

Figure: **Source:** `tinyurl.com/nfwwkw4r`

Topics

Research Questions

1. **Why did current malware research work failed on providing greater security to actual systems?**
   1. Which types of research work have been conducted so-far?
   2. How research works have been conducted so-far?
   3. What are the limits and implications of this current scenario?
2. **What could be done to improve future malware research work to be successful in operating on actual scenarios?**
   1. Which type of research could be developed to support real-world needs?
   2. Which methods could be applied to malware research work developments to make them more successful in handling actual malware?
   3. Who are the stakeholder involved in designing research solutions that can be evolved to operate in actual scenarios?

Research Plan

Roadmap

- Systematic review of malware research literature.
- Identify development gaps fields.
- Bridge a sub-problem in each field.

Guideline

- Contributing in broadness in addition to contributing in depth.

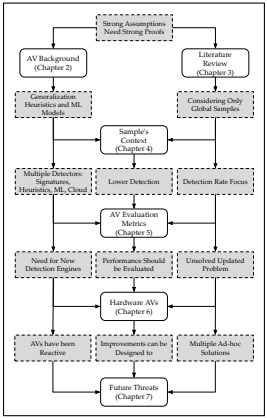


Figure: Thesis Organization

Topics

Why Study AVs?

Knowing AVs

"I was more surprised that...there was very little information about AV software...Although it's comprised of extremely nice people, the AV community tends to be very industry-driven and insular, and isn't in the habit of giving its secrets."

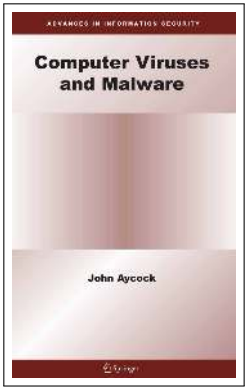


Figure: John Aycock (2006). Computer Viruses and Malware.

Publication

Figure: **Source:**
`https://www.sciencedirect.com/science/article/pii/S0167404821003242`

Which AVs to analyze?

Table: **Analyzed AVs.**

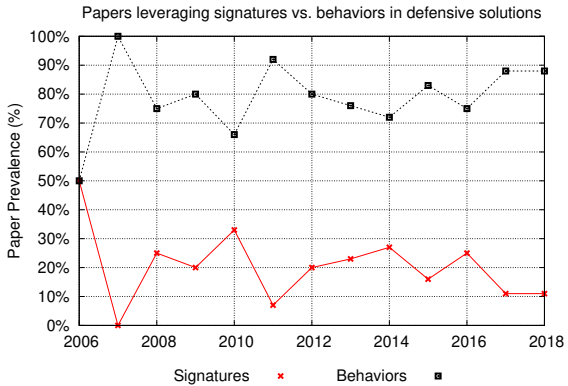
AV	Version	MD5
Avast	19.7.4674.0	172ee63bf3e0fa54abd656193d225013
AVG	19.8.4793.0	0d19e6fc1a4d239e02117f174d00d024
BitDefender	24.0.14.74	0e54eab75c8fd4059f3e97f771c737de
F-Secure	21.05.103.0	2393777281f3a9b11832558f5f3c0bce
Kaspersky	20.0.14.1085	7dc4fb6f026f9713dca49fc1941b22ce
MalwareBytes	3.0.0.199	9c69b2a22080c53521c6e88bd99686a1
Norton	22.17.1.50	2f1f762658dc7e41ecc66abd0270df97
TrendMicro	12.0	f8b8a3701ec53c7e716cf5008fad9aa1
Vipre	11.0.4.2	77a9dbd31ed5ebe490011ffa139afe03
WinDefender	4.18.1902.5	Built-in W10

What to analyze?

- Installation
- Uninstallation
- Updates
- Modularity
- Signatures
- Databases
- Real-Time Checks
- Machine Learning
- Cloud Scans
- Heuristics
- Attack Surface
- Self-Protection

Topics

Academic Production



Malware Detection Methods. Signatures vs. Behavioral (e.g., Machine Learning) approaches.

Figure: **Source:** Challenges and Pitfalls in Malware Research (2021).

Implications (1/2)

1. What About Signatures?

AVs and Common-Sense

Signatures

"It may seem at first that such signatures are not frequently used in today's antivirus products, but the reality is otherwise...Cryptographic hashes are often used by antivirus products."

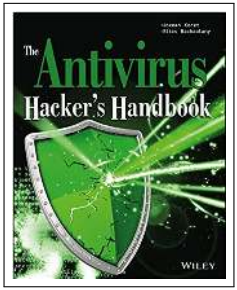


Figure: Joxean Koret and Elias Bachaalany (2015). The Antivirus Hacker's Handbook.

Signature Extraction Algorithm

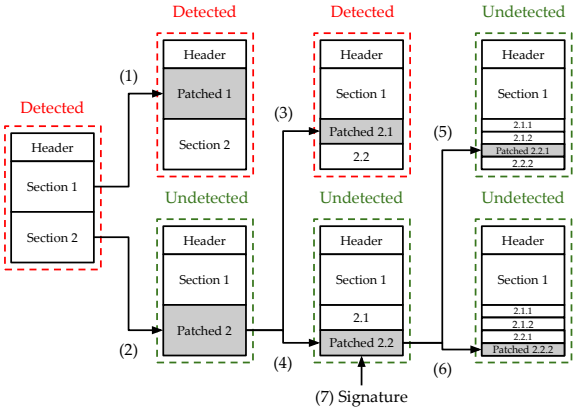


Figure: **Binary Search-Like Signature Identification.**

Signatures in Practice

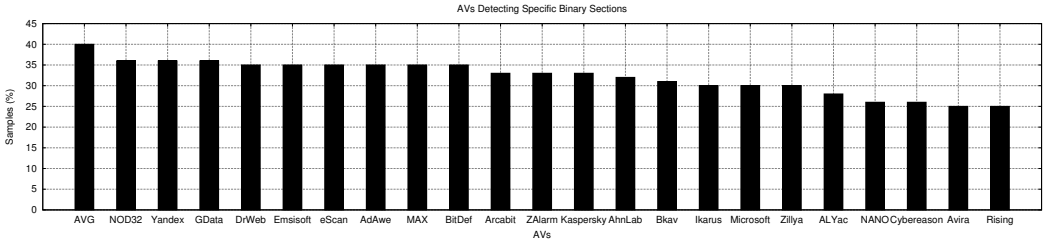


Figure: **Signature Prevalence.** Around a third of the AV's detections are based on specific section's contents.

Implications (2/2)

2. What About Machine Learning?

ML and Academic Models

Table: **DLL Hooking.** Can we assume a unified model?

Antivirus	Functions	Libraries
Avast	17	2
BitDefender	132	11
Fsecure	17	4
VIPRE	45	3

Topics

Reflecting about our own field.

Analyzing the Scientific Production

"*How many anthropologists write books, theses or articles that are read, commented on and criticized by the people they study?*"

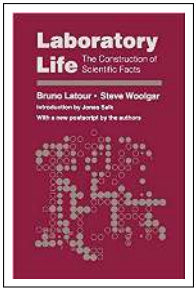


Figure: Latour, Bruno; Woolgar, Steve (1986). Laboratory life: the construction of scientific facts.

Publication

Figure: **Link:**
`https://www.sciencedirect.com/science/article/pii/S0167404821001115`

Malware Literature Venues

Table: **Selected Papers**. Distribution per year (2000 – 2018) and per venue.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	Total
USENIX (Security, LEET & WOOT)	1	0	0	0	0	1	1	6	2	3	7	8	10	12	9	7	9	13	6	95
CCS	0	0	0	0	0	0	0	2	4	6	6	7	11	9	11	14	2	11	6	89
ACSAC	0	0	0	0	2	3	2	4	4	1	3	8	10	7	10	6	3	7	8	78
IEEE S&P	0	1	0	0	0	1	3	2	1	0	0	10	17	12	3	6	4	5	3	68
DIMVA	0	0	0	0	0	4	4	3	8	2	3	0	8	4	8	7	7	5	4	67
NDSS	0	0	0	0	1	0	2	0	3	3	3	3	2	4	5	4	9	7	3	49
RAID	0	0	1	0	0	1	3	0	0	0	0	0	3	5	5	3	4	3	3	31
ESORICS	0	0	0	0	0	1	0	0	2	1	0	0	2	3	3	0	1	1	0	14
Total	1	1	1	0	3	11	15	17	24	16	22	36	63	56	54	47	39	52	33	491

Is Security Art?

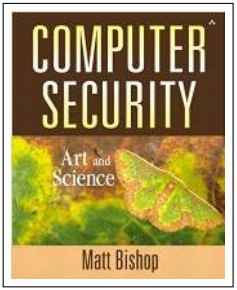


Figure: Matthew Bishop (1974). Computer Security: Art and Science.

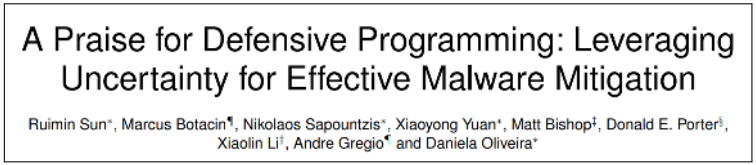


Figure: Our paper. Ruimin Sun et al (2020). IEEE Transactions on Dependable and Secure Computing (TDSC).

A Method for Malware Research

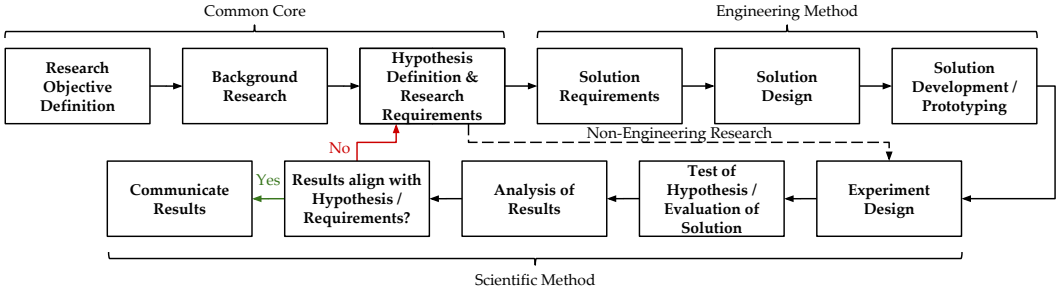


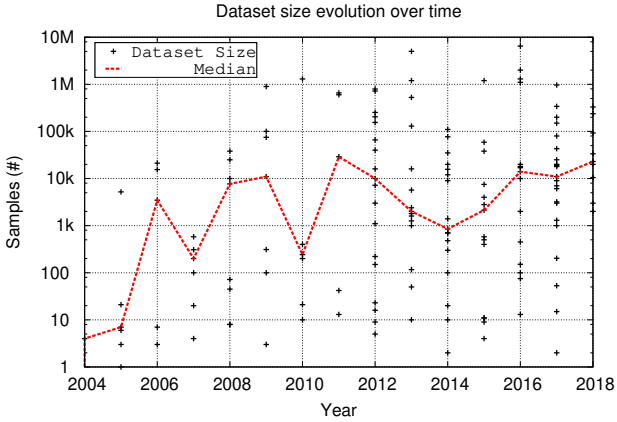
Figure: **Malware Research Method.** Integrating Science and Engineering.

Research Types

Malware Research Types

Is it good to have more engineering solutions than all other types of research?

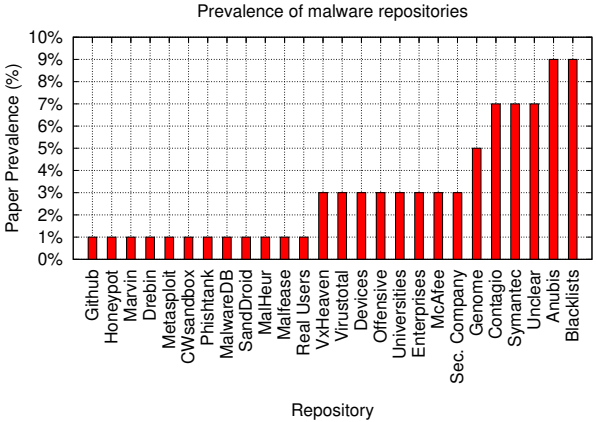
Dataset Sizes



Dataset Size Definition

How to define how many samples are representative? Shouldn't we have some kind of guideline?

Dataset Sources



Research Reproducibility

Are these samples available? Are they described? Were repositories sinkholed?

Summary

1. Inbalance in research work types.
2. Solutions developed not informed by previous study's data.
3. Most work still don't clearly state threat models.
4. Failure in positioning work as prototypes or real-world solutions.
5. Offline and online solutions developed and evaluated using the same criteria.
6. No dataset definition criteria.
7. Few attention to dataset representativity.
8. Most studies are not reproducible.
9. Sandbox execution criteria are not explained.
10. Non-homogeneous AV labels are still a problem.

A final verdict?

About theories

"*We start out confused, and end up confused at a higher level.*"

Figure: A. F. Chalmers (1976). What Is This Thing Called Science?

Topics

Contextual Issues.

Analyzing Security Practices

"*Best practices typically don't take into account differences between companies or, more generally, between industries. The security decisions at an oil firm are made in a very different context than in a clothing wholesaler, and yet we are told that best practices can apply to both*"

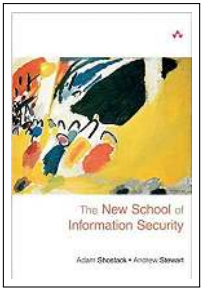


Figure: Adam Shostack and Andrew Stewart (2008). The New School of Information Security.

Publication

RESEARCH-ARTICLE

One Size Does Not Fit All: A Longitudinal Analysis of Brazilian Financial Malware

Authors: Marcus Botacin, Hojjat Aghakhani, Stefano Ortolani, Christopher Kruegel, Giovanni Vigna, Daniela Oliveira, Paulo Lício De Geus, André Grégio Authors Info & Affiliations

Publication: ACM Transactions on Privacy and Security • January 2021 • Article No.: 11 • https://doi.org/10.1145/3429741

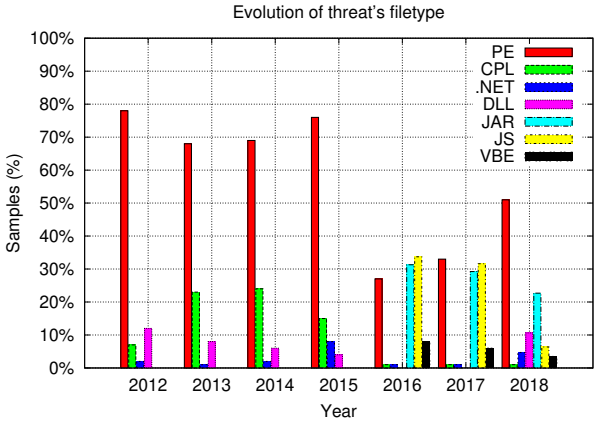
Figure: **Link:** `https://dl.acm.org/doi/10.1145/3429741`

Brazilian Financial Malware

Figure: Passive Banker Malware for Santander bank waiting for user's credential input.

Figure: Passive Banker Malware for Itaú bank waiting for user's credential input.

Brazilian Financial Malware Filetypes.



Brazilian malware filetypes.

Varied file formats are prevalent over the years.

Research Impact

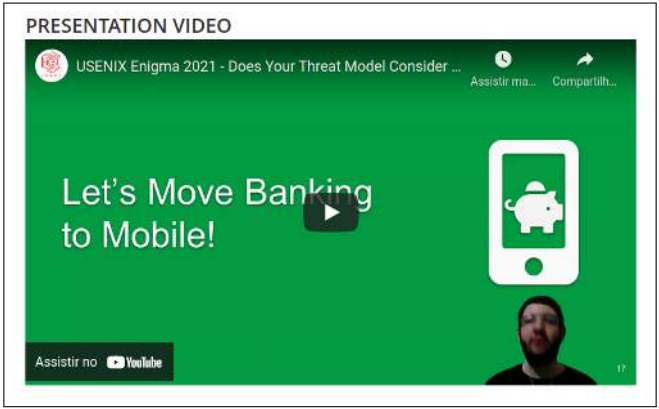


Figure: **Source:** https://www.usenix.org/conference/enigma2021/presentation/botacin

Topics

Why Do We Need Metrics?

Analyzing Security Practices

"If security can't be measured, it continues to be impossible to say whether we have more of it today than we did yesterday."

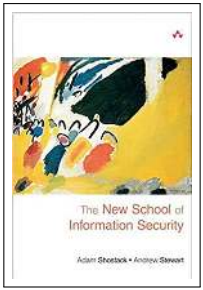
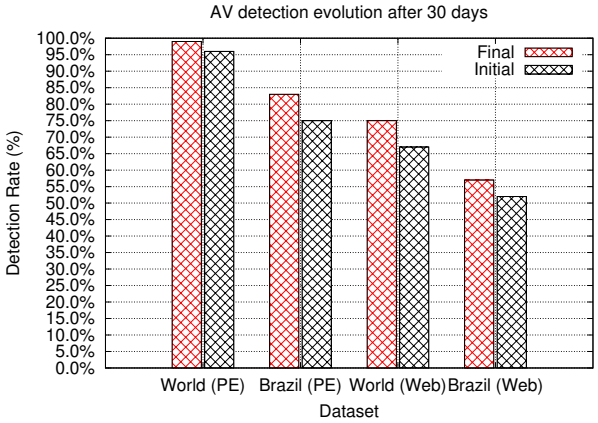


Figure: Adam Shostack and Andrew Stewart (2008). The New School of Information Security.

Publication

Figure: **Source:** `https://www.sciencedirect.com/science/article/pii/S0167404820301310`

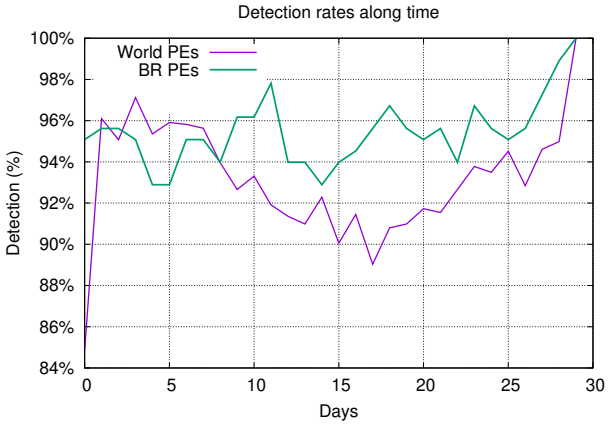
Detection Rates Over Time (1/2)



Initial and Final Detection Rates.

Detection rates increase in a 30-day period.

Detection Rates Over Time (2/2)



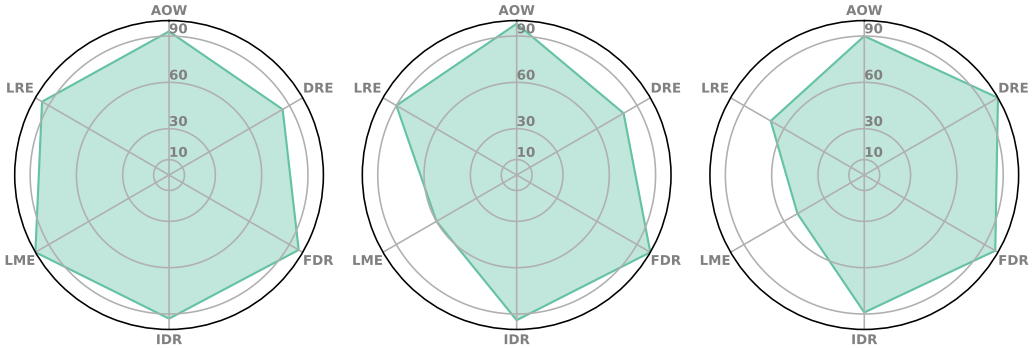
Detection Regression.

Some samples stop being detected after some time.

Summary.

- Initial Detection Rate (IDR)
- Final Detection Rate (FDR)
- Attack Opportunity Window (AOW)
- Detection Regression (DRE)
- Label Regression (LRE)
- Label Meaningfulness (LME)

Multi-Dimensional AV Evaluation.



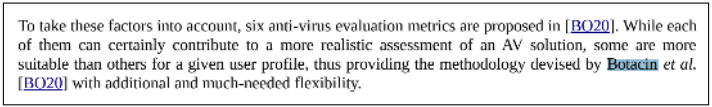
(a) **AV1.** Recommended for incident response teams.

(b) **AV2.** Recommended for corporate users.

(c) **AV3.** Recommended for domestic users.

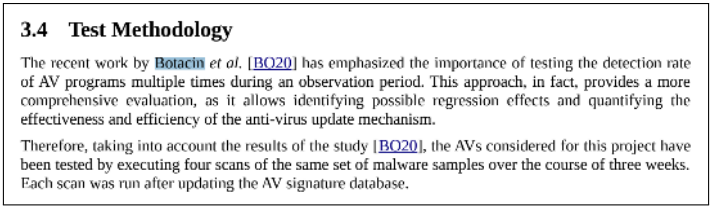
Figure: **AV's operational aspects**, considering the six proposed metrics.

Evaluation Metrics Adoption



To take these factors into account, six anti-virus evaluation metrics are proposed in [BO20]. While each of them can certainly contribute to a more realistic assessment of an AV solution, some are more suitable than others for a given user profile, thus providing the methodology devised by Botacin *et al.* [BO20] with additional and much-needed flexibility.

Figure: **Dissertation Source:**
`https://www.royalholloway.ac.uk/media/16565/techreport-giusepperaffa.pdf`.



3.4 Test Methodology

The recent work by Botacin *et al.* [BO20] has emphasized the importance of testing the detection rate of AV programs multiple times during an observation period. This approach, in fact, provides a more comprehensive evaluation, as it allows identifying possible regression effects and quantifying the effectiveness and efficiency of the anti-virus update mechanism.

Therefore, taking into account the results of the study [BO20], the AVs considered for this project have been tested by executing four scans of the same set of malware samples over the course of three weeks. Each scan was run after updating the AV signature database.

Figure: **Dissertation Source:**
`https://www.royalholloway.ac.uk/media/16565/techreport-giusepperaffa.pdf`.

Topics

Improving AVs Performance

Strategies

- Reduce amount scanned.
- Reduce amount of scans.
- Lower resource requirements.
- Change the algorithm.

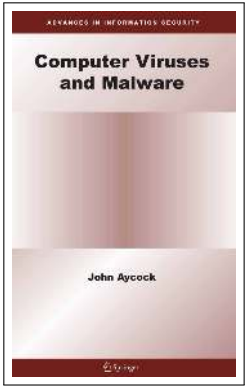


Figure: John Aycock (2006). Computer Viruses and Malware.

Publication

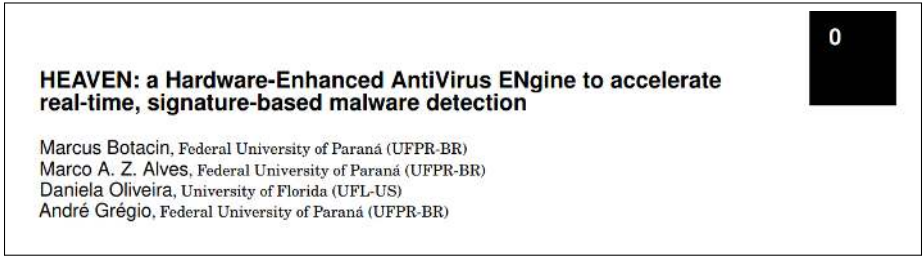


Figure: **Source:** Under Review.

Branch Prediction Background.

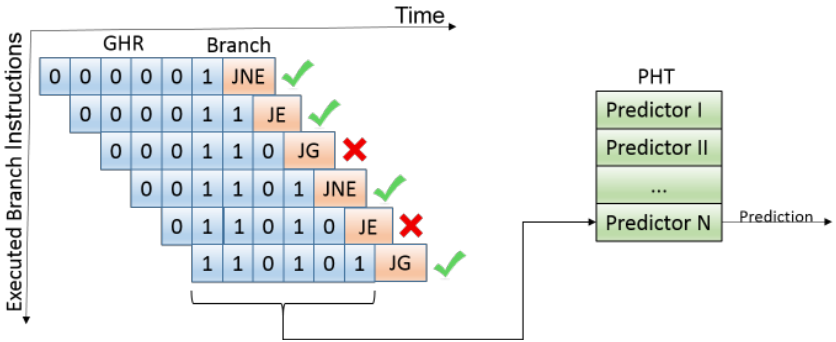
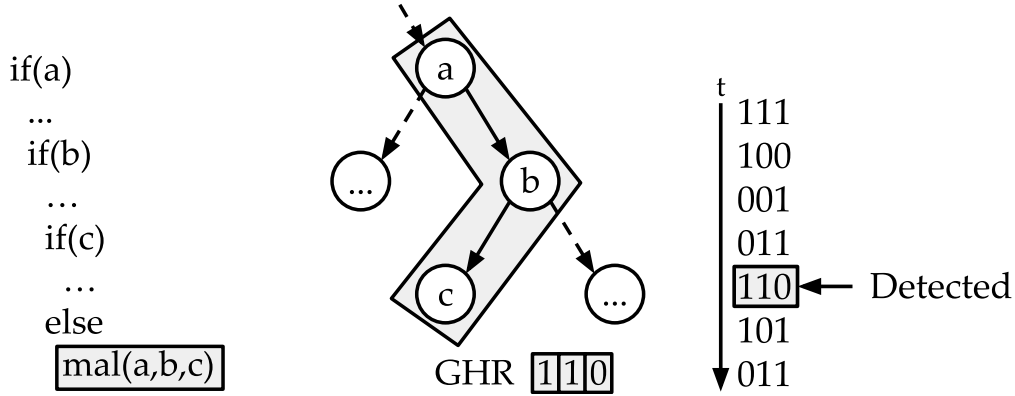


Figure: 2-level branch predictor.

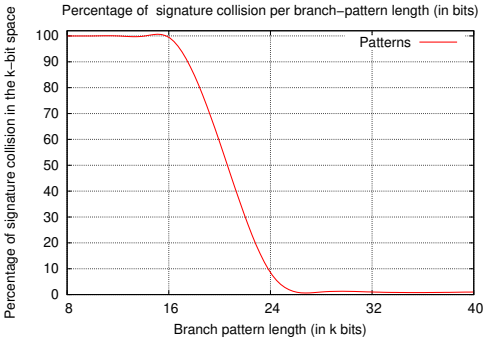
Branch Patterns and Code Patterns



(a) **Code.** (b) **Flow.** (c) **Signature**

Figure: Associating high-level code constructs with their occurrence in the execution flow.

Branch Patterns as Signatures (1/3)



Viability

How long should a branch pattern be to be used as a signature?

Branch Patterns as Signatures (2/3)

Table: Signature distribution along code region in the malware samples evaluated. Percentage of good signatures per code region and percentage of malware samples allowing generation of at least one signature for the given code region. A code region [0%-10%] corresponds to the first 10% of the malware trace.

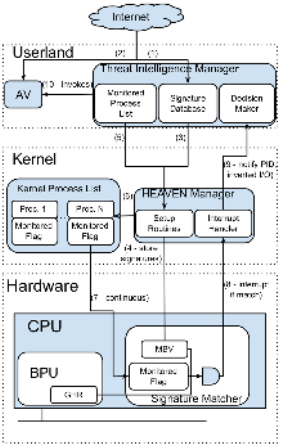
Code region	Signatures	Samples
0%-10%	6%	100%
10%-50%	10%	54%
50%-70%	19%	98%
70%-80%	28%	78%
80%-90%	24%	90%
90%-100%	13%	100%

Branch Patterns as Signatures (3/3)

Table: Malware behaviors associated with HEAVEN produced signatures and the code region in which they are matched (percentage of sample's execution).

Behavior	Signature prevalence	Code region	Samples
Image Load	18%	0%-10%	100%
Image Launch	45%	0%-10%	100%
File Deletion	81%	80%-90%	100%
Connection	100%	0%-10%	100%
Exfiltration	67%	80%-90%	100%

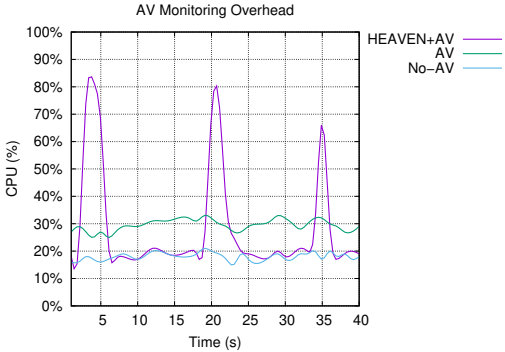
Hardware-Enhanced AntiVirus Engine (HEAVEN)



2-level Architecture

Do not fully replace AVs, but add efficient matching capabilities to them.

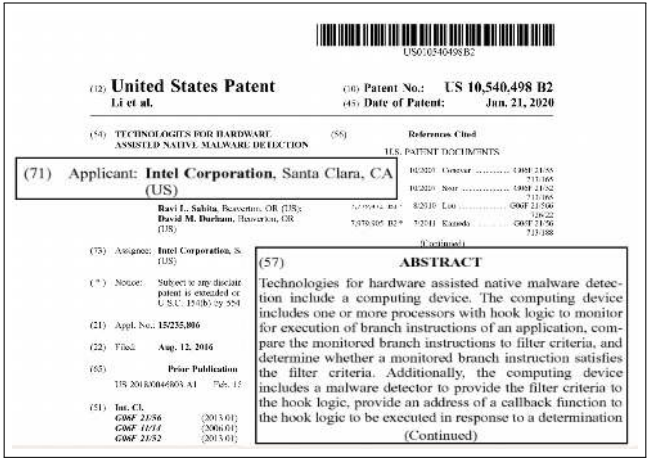
Performance Characterization



2-Phase HEAVEN CPU Performance

The inspection phase causes occasional, and quick bursts of CPU usage. The AV operating alone incurs a continuous 10% performance overhead.

Hardware Solutions Adoption.



US010540498B2

(12) **United States Patent**
Li et al.

(10) Patent No.: US 10,540,498 B2
(45) Date of Patent: Jun. 21, 2020

(54) TECHNOLOGIES FOR HARDWARE ASSISTED NATIVE MALWARE DETECTION

(71) Applicant: **Intel Corporation**, Santa Clara, CA (US)

Ravi L. Sahita, Beaverton, OR (US); David M. Durham, Beaverton, OR (US)

(73) Assignee: Intel Corporation, S (US)

(*) Notice: Subject to any disclaim patent is extended or U.S.C. 154(b) by 551

(21) Appl. No.: 15/235,886

(22) Filed: Aug. 12, 2016

(65) Prior Publication

US 2018/0046803 A1 Feb. 15

(51) Int. Cl.
G06F 21/56 (2013.01)
G06F 11/14 (2006.01)
G06F 21/52 (2013.01)

(56) References Cited

U.S. PATENT DOCUMENTS

(57) **ABSTRACT**

Technologies for hardware assisted native malware detection include a computing device. The computing device includes one or more processors with hook logic to monitor for execution of branch instructions of an application, compare the monitored branch instructions to filter criteria, and determine whether a monitored branch instruction satisfies the filter criteria. Additionally, the computing device includes a malware detector to provide the filter criteria to the hook logic, provide an address of a callback function to the hook logic to be executed in response to a determination

(Continued)

Intel Patent Source:

https://patentimages.storage.googleapis.com/fb/23/ff/9d11b27884f050/US10540498.pdf.

Topics

Memory Scans

About Current AVs

"Some antivirus...claim to support memory analysis, but that is not accurate. Such products do not really perform memory analysis but, rather, query the list of processes being executed and analyze the modules loaded in each one using the files as they are on disk."

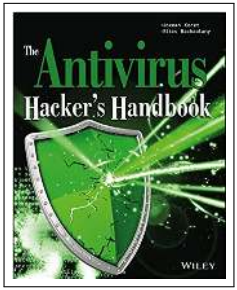
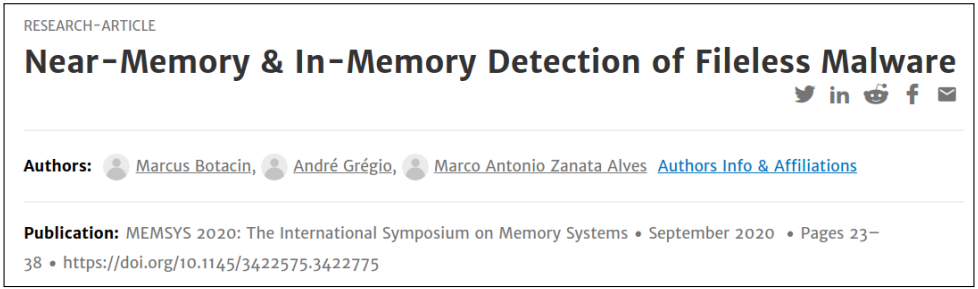


Figure: Joxean Koret and Elias Bachaalany (2015). The Antivirus Hacker's Handbook.

Publication



RESEARCH-ARTICLE

Near-Memory & In-Memory Detection of Fileless Malware

Authors: Marcus Botacin, André Grégio, Marco Antonio Zanata Alves Authors Info & Affiliations

Publication: MEMSYS 2020: The International Symposium on Memory Systems • September 2020 • Pages 23–38 • https://doi.org/10.1145/3422575.3422775

Figure: **Link:** `https://dl.acm.org/doi/10.1145/3422575.3422775`

Memory Controller Background

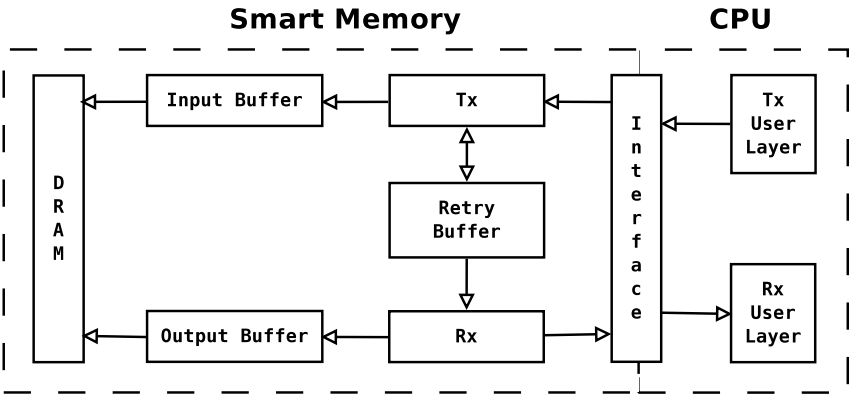


Figure: Memory Controller Queues.

Malware Identification based on Near- and In-Memory Evaluation (MINIME)

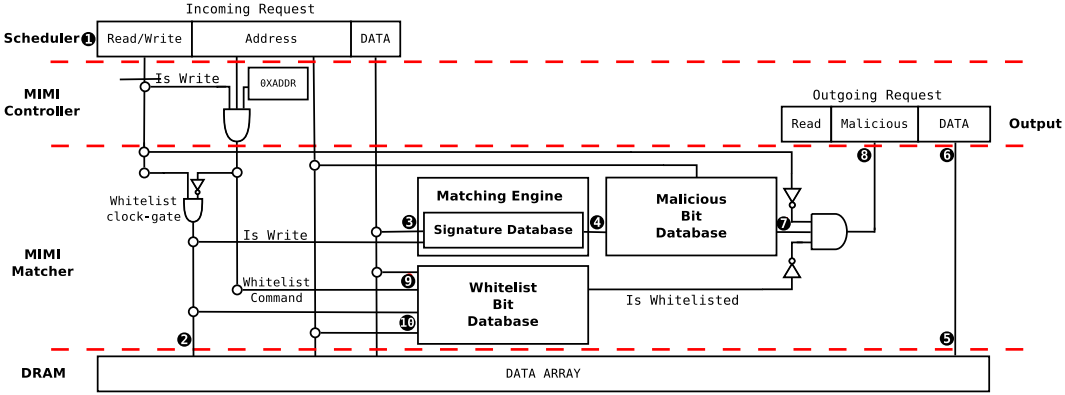
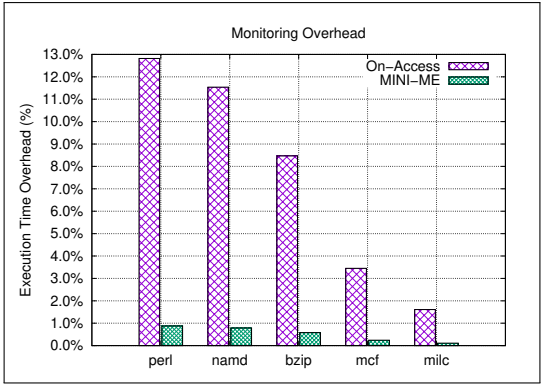


Figure: MINIME Architecture.

Performance Gains

MINIME vs. On-Access AVs

Significant performance gains even in the worst case.



Topics

Contextual Issues: Mobile Banking

RESEARCH-ARTICLE

The Internet Banking [in]Security Spiral: Past, Present, and Future of Online Banking Protection Mechanisms based on a Brazilian case study

Authors: Marcus Botacin, Anatoli Kalysch, André Grégio Authors Info & Affiliations

Publication: ARES '19: Proceedings of the 14th International Conference on Availability, Reliability and Security • August 2019 • Article No.: 49 • Pages 1–10 • https://doi.org/10.1145/3339252.3340103

Figure: **Source:** `https://dl.acm.org/doi/10.1145/3339252.3340103`

Similarity Identification

Figure: **Link:**
`https://www.sciencedirect.com/science/article/abs/pii/S2666281721001281`

Hardware Solutions: FPGA AV

Figure: **Source:** `https://ieeexplore.ieee.org/document/9034972/`

Hardware Solutions: SMC Detector

Original Paper | Published: 13 February 2020

The self modifying code (SMC)-aware processor (SAP): a security look on architectural impact and support

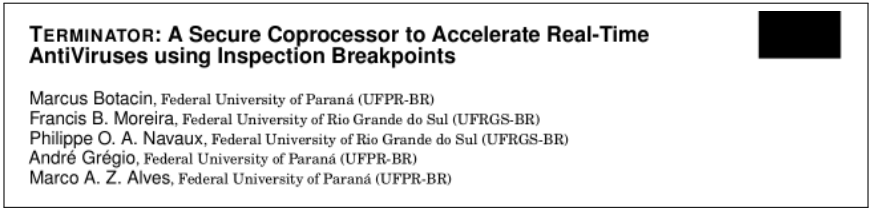
Marcus Botacin, Marco Zanata & André Grégio

Journal of Computer Virology and Hacking Techniques **16**, 185–196(2020) | Cite this article

198 Accesses | **3** Altmetric | Metrics

Figure: **Source:** `https://link.springer.com/article/10.1007/s11416-020-00348-w`

Hardware Solutions: Real-Time Processor

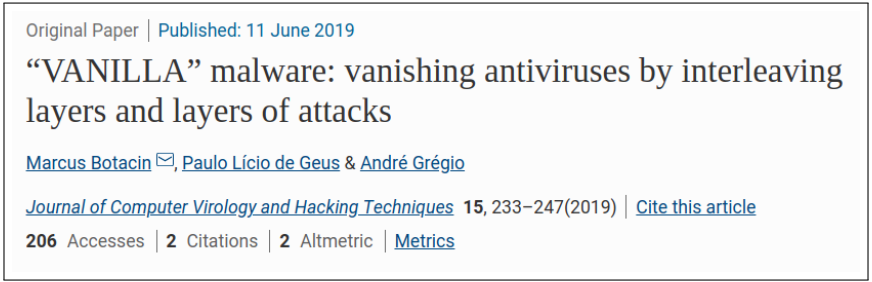


TERMINATOR: A Secure Coprocessor to Accelerate Real-Time AntiViruses using Inspection Breakpoints

Marcus Botacin, Federal University of Paraná (UFPR-BR)
Francis B. Moreira, Federal University of Rio Grande do Sul (UFRGS-BR)
Philippe O. A. Navaux, Federal University of Rio Grande do Sul (UFRGS-BR)
André Grégio, Federal University of Paraná (UFPR-BR)
Marco A. Z. Alves, Federal University of Paraná (UFPR-BR)

Figure: **Source:** To Appear Soon (ACM TOPS).

Attack Prediction: Distributed Malware



Original Paper | Published: 11 June 2019

"VANILLA" malware: vanishing antiviruses by interleaving layers and layers of attacks

Marcus Botacin, Paulo Lício de Geus & André Grégio

Journal of Computer Virology and Hacking Techniques **15**, 233–247(2019) | Cite this article

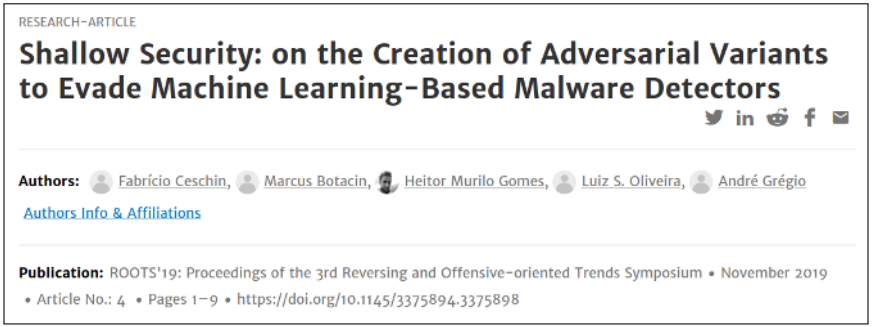
206 Accesses | **2** Citations | **2** Altmetric | Metrics

Figure: **Source:** `https://link.springer.com/article/10.1007/s11416-019-00333-y`

Research Methodology: The Use of Application Installers

Figure: **Source:** `https://link.springer.com/chapter/10.1007/978-3-030-52683-2_10`

Detection Robustness: Adversarial ML



RESEARCH-ARTICLE

Shallow Security: on the Creation of Adversarial Variants to Evade Machine Learning-Based Malware Detectors

Authors: Fabrício Ceschin, Marcus Botacin, Heitor Murilo Gomes, Luiz S. Oliveira, André Grégio

Authors Info & Affiliations

Publication: ROOTS'19: Proceedings of the 3rd Reversing and Offensive-oriented Trends Symposium • November 2019 • Article No.: 4 • Pages 1–9 • https://doi.org/10.1145/3375894.3375898

Figure: **Source:** `https://dl.acm.org/doi/10.1145/3375894.3375898`

Transition to Practice: Corvus Sandbox

Figure: **Source:** `https://corvus.inf.ufpr.br/`

Topics

Summary

1. **Hypothesis:** Malware Research lacks a methodology.
2. **Contribution:** We proposed a possible methodology.
3. **Implications:**
   1. **The Need For Context**
      - Brazilian Financial Malware.
   2. **The Need For Better Evaluations**
      - AV Evaluation Metrics.
   3. **The Viability of Hardware Support**
      - Branch Predictor-Based Signature Matching.
   4. **The Need For Predicting the Future**
      - FIleless Malware Detection.

Acknowledgement time

Thanks!

Questions? Comments?

Really?

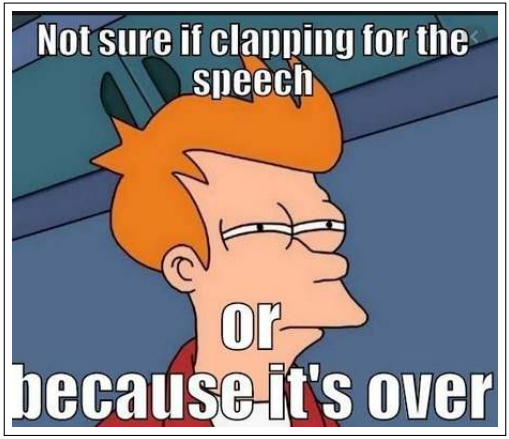


Figure: **Source:** `tinyurl.com/26rsww`

Thanks!

Questions? Comments?