Data and Network Security

(Master Degree in Computer Science and Cybersecurity)

Lecture 1

Sapienza Università di Roma

What is this course about?

This course provides a comprehensive introduction to fundamental concepts, principles, and practices in cybersecurity focusing into emerging trends and future directions in the field.

What is this course about?

This course provides a comprehensive introduction to fundamental concepts, principles, and practices in cybersecurity focusing into emerging trends and future directions in the field.

This course has a research oriented focus, and as such will treat various novel research works in the domain, and will also stimulate the students to carry out independent research and share knowledge with classmates.

Class hours

- **Monday**: 11:00-13:00
  - Start at 11:15
  - End at 12:45

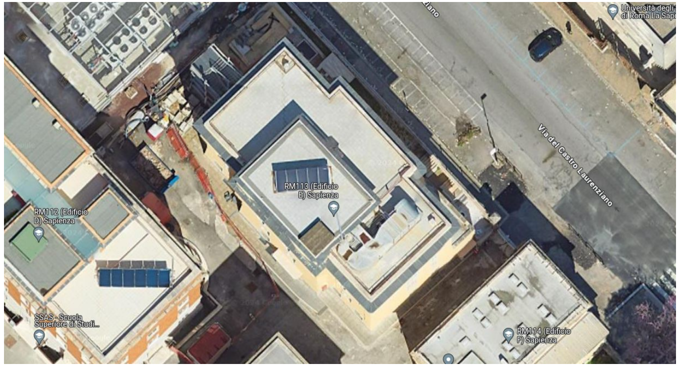
- **Thursday**: 08:00-11:00
  - Start at 08:15
    - Usually 15 min break (09:15-09:30)
  - End at 10:45

Office Hours

Monday: 14:00-16:00

Thursday: 13:00-16:00

***Send an email [hitaj.d@di.uniroma1.it] at least one day before to check availability.**


Università degli
di Roma La Sap
Via del Castro Laurenziano
RM113 (Edificio E) Sapienza
RM112 (Edificio D) Sapienza
SSAS - Scuola Superiore di Studi...
RM114 (Edificio F) Sapienza

Viale Regina Elena 295
E-building
First Floor, Room 101

Evaluation and Examination

The exam consists of an oral presentation, and in submitting a written report.

Evaluation and Examination

Each student (or group of st.) will give a seminar on a topic of their choice from a list of possible topics, and answer questions from the other students in the classroom. Students' participation in the “questions & answers” phase will be considered in the final grade.

Evaluation and Examination

Students also have to deliver a report describing how and in what measure they intend to solve a cybersecurity problem, related to the topic of their seminar.

Evaluation and Examination

The final grade is calculated as follows:

- 45% Literature Analysis and active participation
- 45% Written research report
- 10% Active participation to Question & Answer section.

Evaluation and Examination

The final grade is calculated as follows:

- 45% Literature Analysis and active participation
- 45% Written research report
- 10% Active participation to Question & Answer section.

***If for any reason students do not turn in most of the required above tests, then those students will be required to take an oral exam on the entire course programme (TDB)**

The weight of this final oral exam = 100%.

Announcements and General Information

We will use a google group to share general information.

https://forms.gle/LENFpvx4Nggx42YD7

Course Syllabus

1. Introduction to cybersecurity
2. Concepts and terminology
3. Identification and authentication
4. Access control techniques
5. Virus, trojan and, covert channels
6. Main vulnerabilities of computer systems
7. Analysis of the most widespread attacks: buffer overflow, cross-site scripting, SQL injection.
8. Secure operating systems
9. Security of group communications
10. Security in cloud computing
11. Security in wireless networks
12. Secure protocols for wireless networks
13. Information security management systems

Cybersecurity / Data and Network Security?

Cybersecurity is the practice of protecting digital systems, networks, and data from unauthorized access, alteration, or destruction. It encompasses various technologies, processes, and practices designed to safeguard information assets against a wide range of cyber threats.

Importance of DNS

- Data and Network security

Data

- **Data** and Network security

Data

- **Data** and Network security

- Data is the lifeblood of businesses and organizations.

Data

- **Data** and Network security

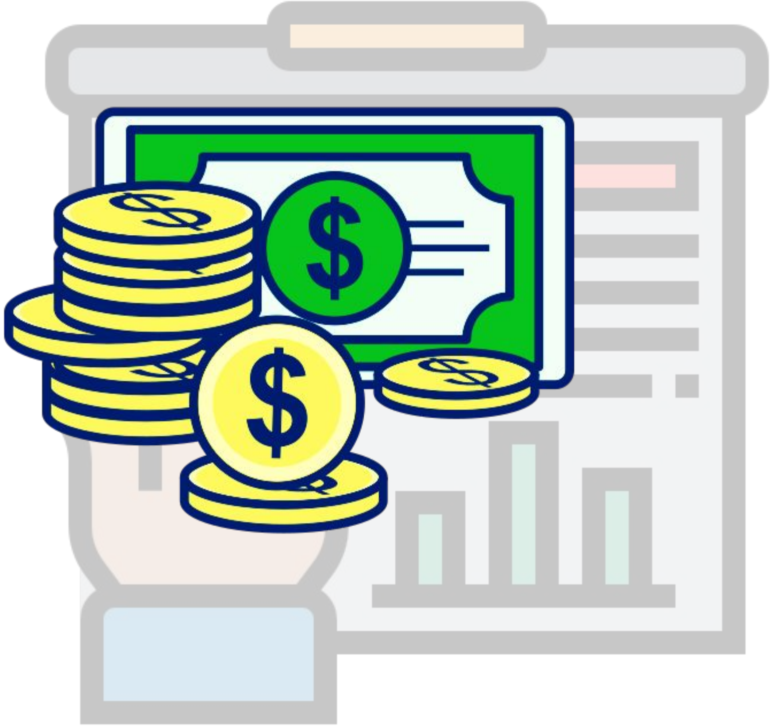
- Data is the lifeblood of businesses and organizations.
  - Inventory management
  - Competitive adv.
  - Market share inc.
  - product /service improvement
  - …

Data

- Data and Network security

- Data is the lifeblood of businesses and organizations.
  - Inventory management
  - Competitive adv.
  - Market share inc.
  - product /service improvement
  - …

Data =



Data loss/damage

- Financial loss
- Reputation damage
- Legal ramifications

Data loss/damage

- **Financial loss**
- Reputation damage
- Legal ramifications

Data loss/damage

- **Financial loss:**
  - theft of sensitive information, disruption of business operations, and remediation costs.

Data loss/damage

- Financial loss
- **Reputation damage**
- Legal ramifications

Data loss/damage

- **Reputation Damage:**
  - entities/organizations failing to protect data, risk damaging their reputation and losing the trust of customers, partners, and stakeholders

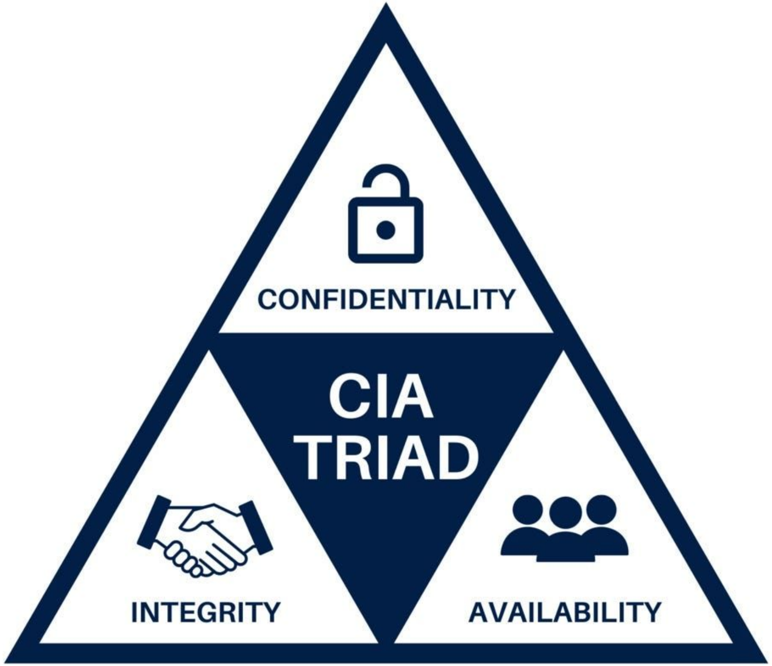
Data loss/damage

- Financial loss
- Reputation damage
- **Legal ramifications**

Data loss/damage

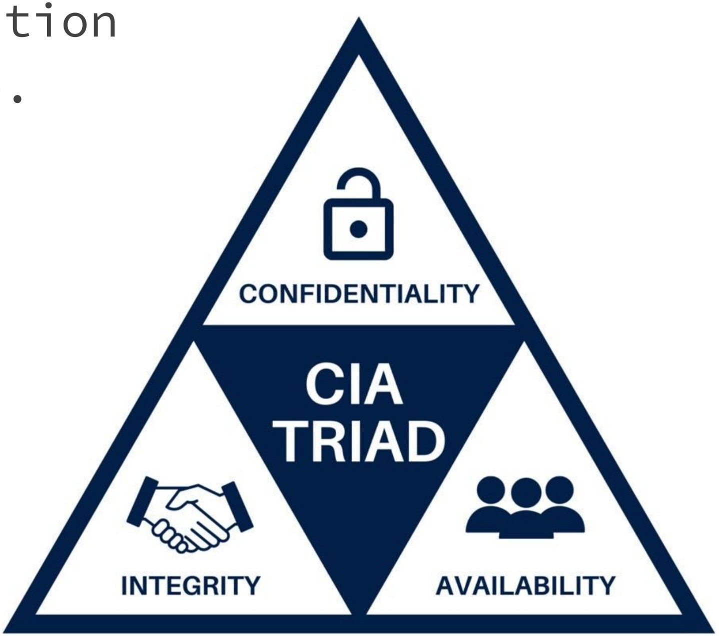
- **Legal ramification:**
  - Regulatory bodies impose strict requirements for data protection and privacy. Failure to comply with these regulations can lead to fines, lawsuits, and other legal consequences.

The goals of DNS



Confidentiality

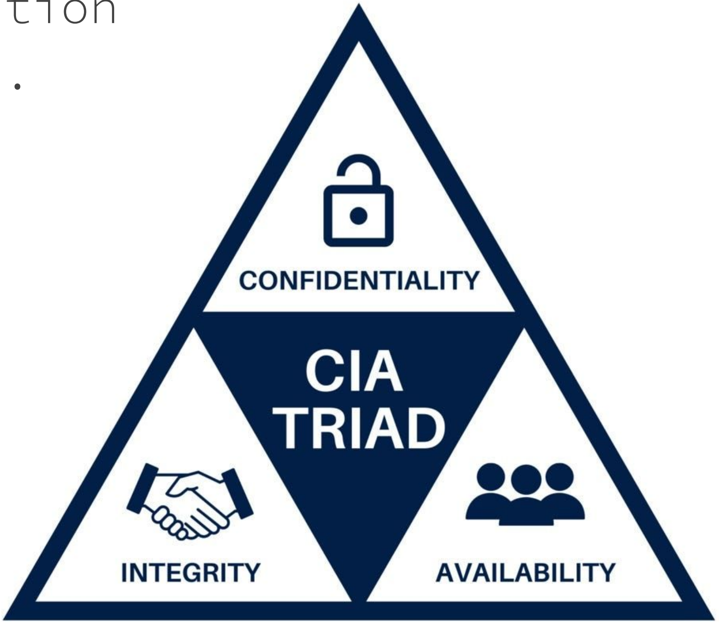
Protecting sensitive information from unauthorized disclosure.



Confidentiality - measures to take

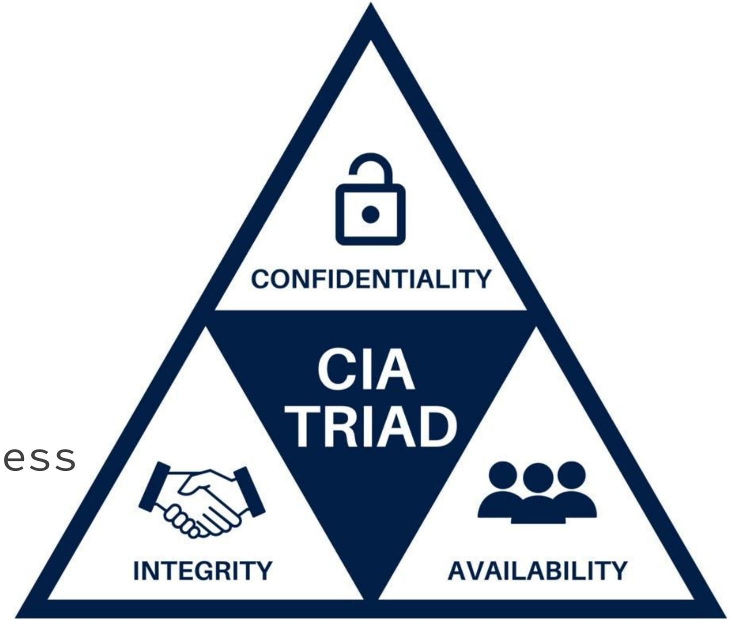
Protecting sensitive information from unauthorized disclosure.

- Encryption
- access controls
- data classification policies



Integrity

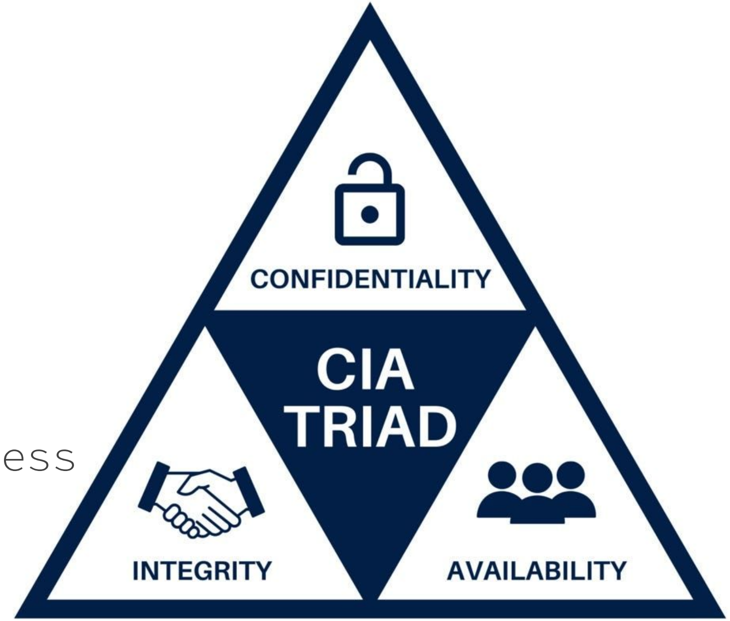
Ensuring the accuracy and trustworthiness of data by preventing unauthorized modifications



Integrity - measures to take

- Data validation
- Checksums
- Digital signatures
- Access controls

Ensuring the accuracy and trustworthiness of data by preventing unauthorized modifications



Availability

CONFIDENTIALITY
CIA
TRIAD
INTEGRITY
AVAILABILITY

Ensuring that data and resources are available and accessible to authorized users when needed.

Availability - measures to take

CONFIDENTIALITY
CIA TRIAD
INTEGRITY
AVAILABILITY

- Redundancy
- Fault tolerance
- Disaster recovery planning
- Denial of service protection

Ensuring that data and resources are available and accessible to authorized users when needed.

Major Threats to DATAs CIA

Malware Threats

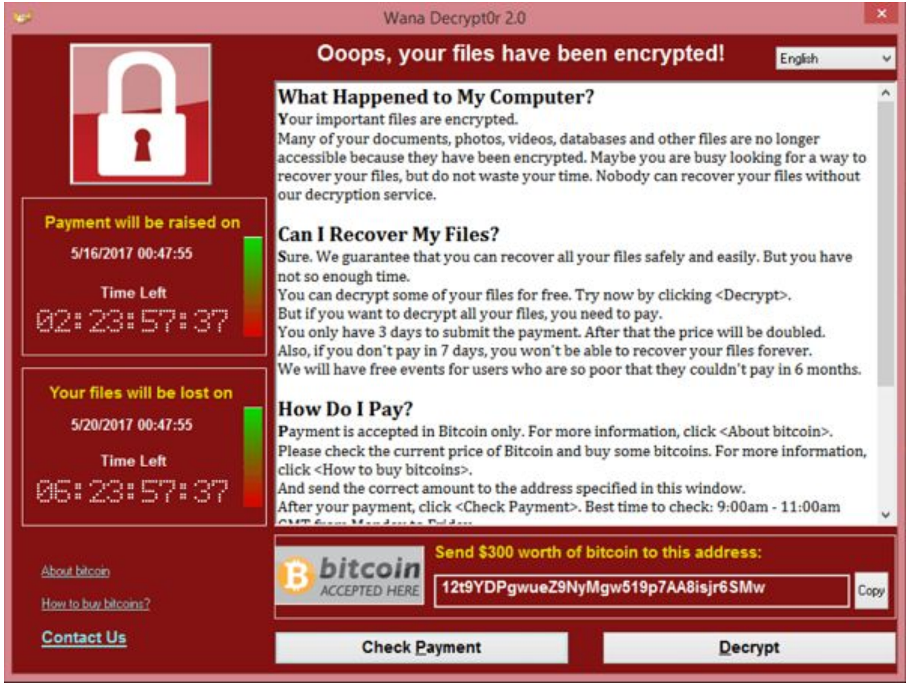
Malware:

Type of software program or code specifically designed to infiltrate, damage, disrupt, or gain unauthorized access to computer systems, networks, or devices, often with malicious intent.

Broad category that encompasses various types of malicious programs, each with its own specific behavior and objectives.

Ransomware

Ransomware



Ooops, your files have been encrypted!

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

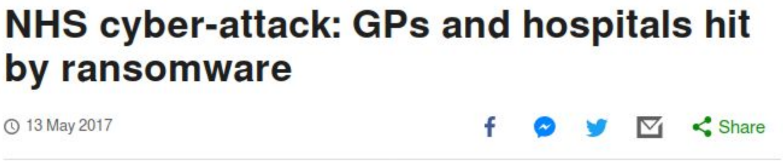
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

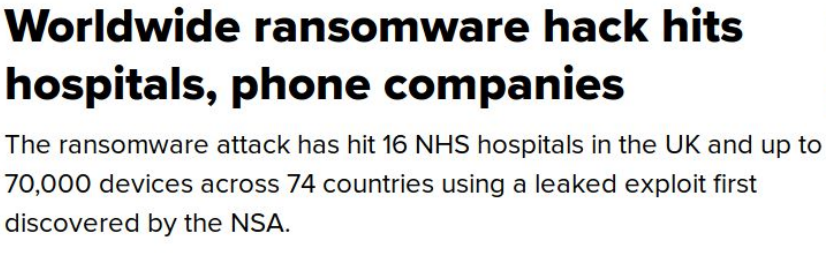
Type of malware from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

The Ransomware Threat



NHS cyber-attack: GPs and hospitals hit by ransomware

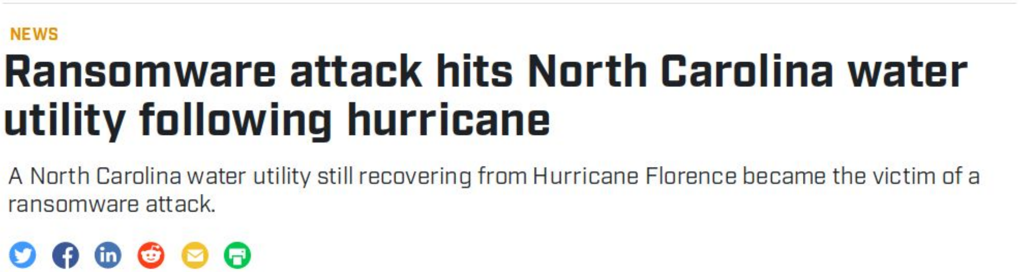
13 May 2017



Worldwide ransomware hack hits hospitals, phone companies

The ransomware attack has hit 16 NHS hospitals in the UK and up to 70,000 devices across 74 countries using a leaked exploit first discovered by the NSA.

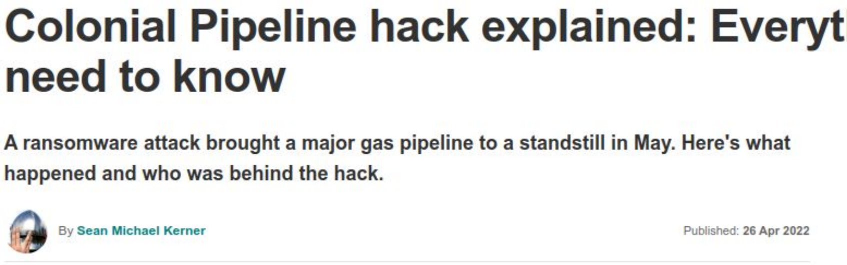
Alfred Ng May 14, 2017 10:20 AM PDT



NEWS

Ransomware attack hits North Carolina water utility following hurricane

A North Carolina water utility still recovering from Hurricane Florence became the victim of a ransomware attack.



Colonial Pipeline hack explained: Everything you need to know

A ransomware attack brought a major gas pipeline to a standstill in May. Here's what happened and who was behind the hack.

By Sean Michael Kerner Published: 26 Apr 2022

Signature based vs. Behaviour based detection

Signature based vs. Behaviour based detection

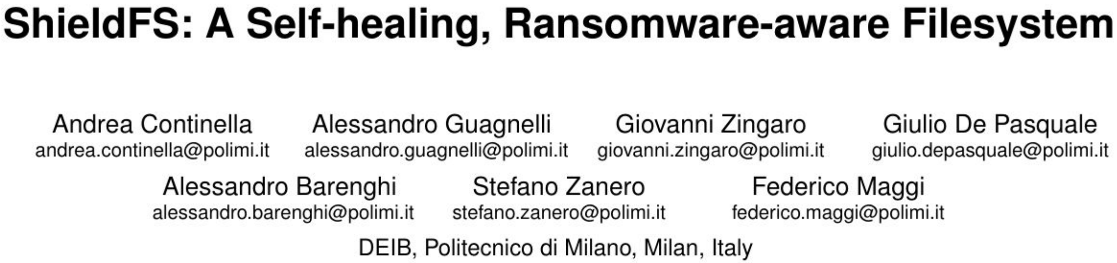
Signature based detection works by searching for a known identity – or signature – for each specific event.

- Very efficient (as long as it is kept up to date)

Signature based vs. Behaviour based detection

Analysing and monitoring how a process behaves in the system, for example how many files it accesses, what locations of the storage affects etc.

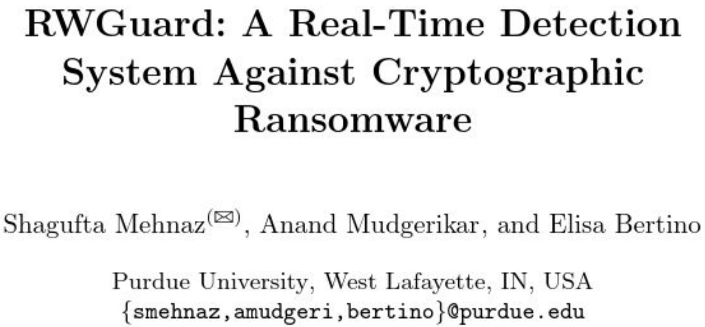
Ransomware detectors



ShieldFS: A Self-healing, Ransomware-aware Filesystem

Andrea Continella andrea.continella@polimi.it
Alessandro Guagnelli alessandro.guagnelli@polimi.it
Giovanni Zingaro giovanni.zingaro@polimi.it
Giulio De Pasquale giulio.depasquale@polimi.it
Alessandro Barenghi alessandro.barenghi@polimi.it
Stefano Zanero stefano.zanero@polimi.it
Federico Maggi federico.maggi@polimi.it
DEIB, Politecnico di Milano, Milan, Italy

Malwarebytes

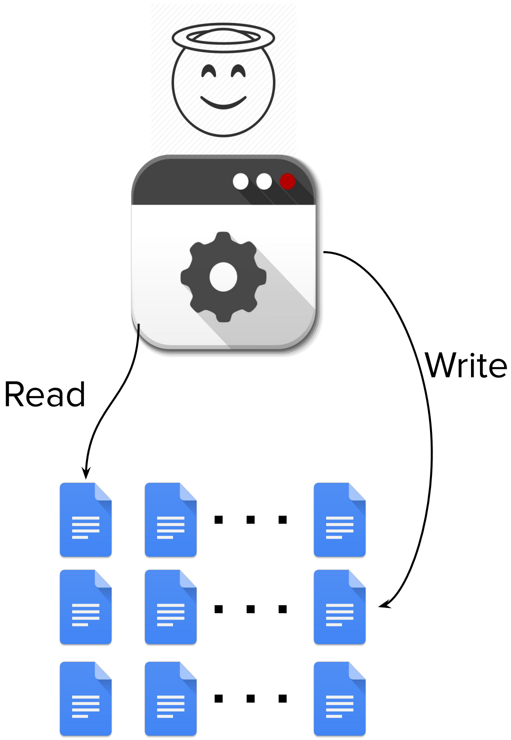


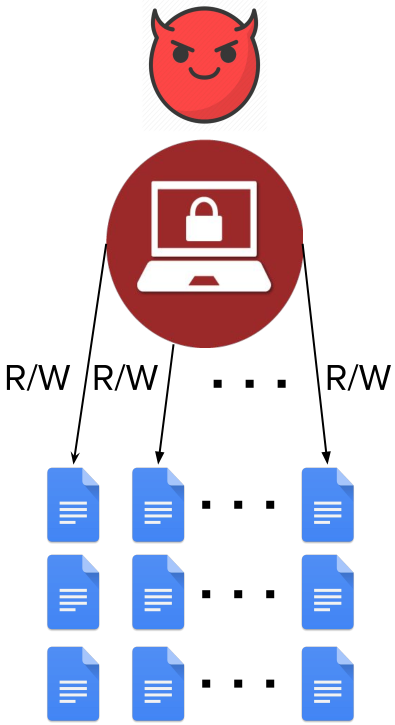
RWGuard: A Real-Time Detection System Against Cryptographic Ransomware

Shagufta Mehnaz(✉), Anand Mudgerikar, and Elisa Bertino

Purdue University, West Lafayette, IN, USA
{smehnaz,amudgeri,bertino}@purdue.edu

Ransomware behaviour





Ransomware features

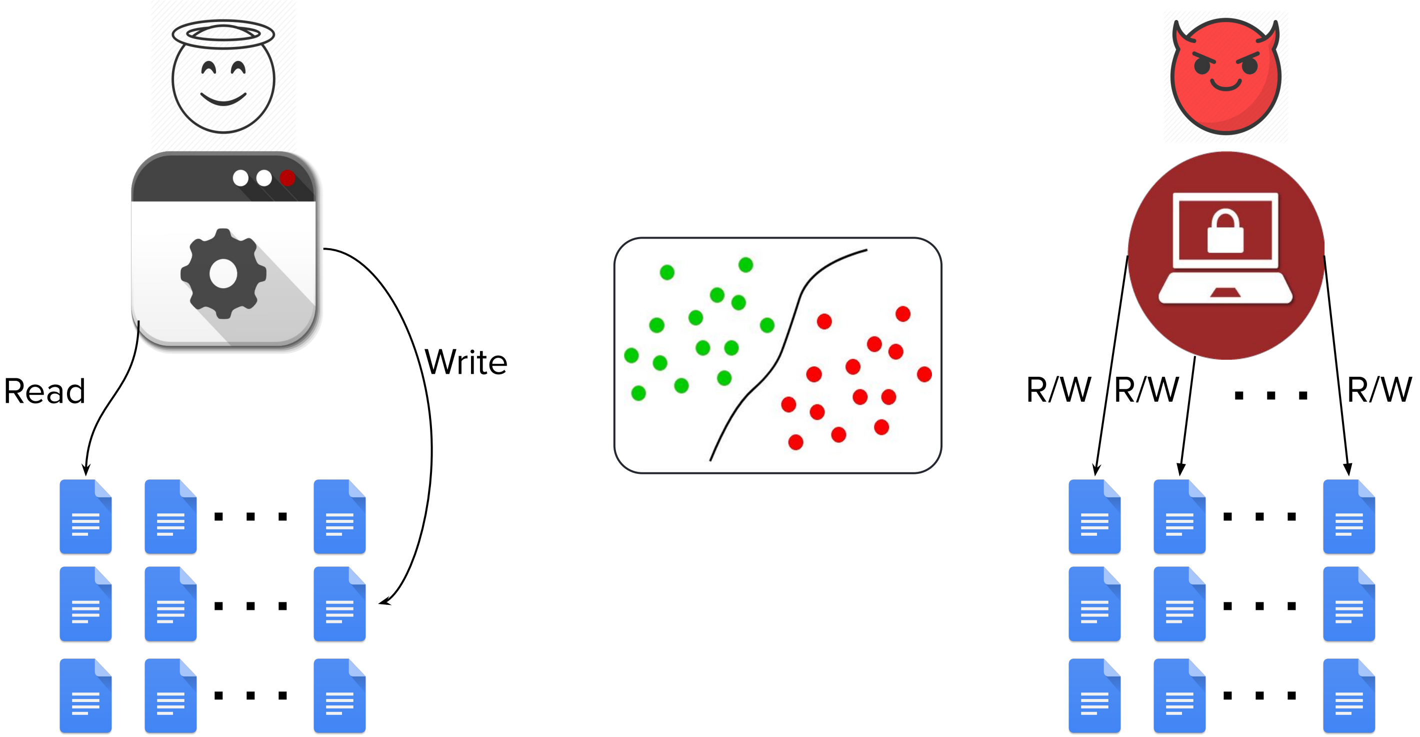
```
- Encrypts files -> - high entropy
                    - overwrites whole file
                    - completely changes file content (no similarity)
                    - changes file type

- Access as many files as possible -> lots of
listing/read/write/open/create/close

- Encrypt all user files -> - access different, unrelated file types
                             - access all files in every directory

- Encrypts as fast as possible -> very high access frequency
```

Ransomware detectors



Behavioural Classification

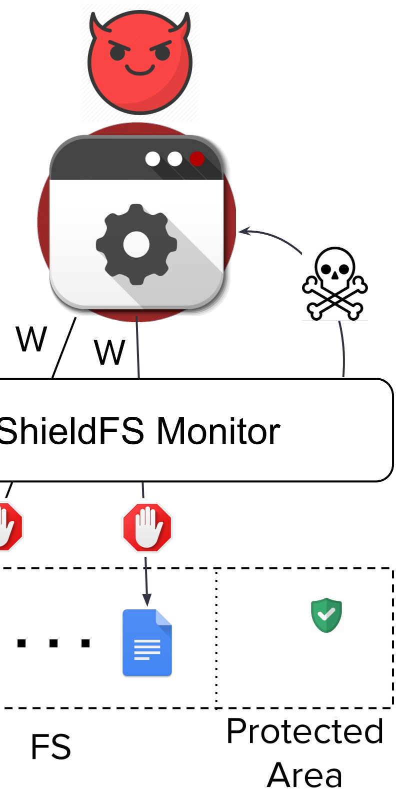
Behavioural classifiers analyse features inextricably linked with ransomware

- e.g., high number of read/write/directory listing, high entropy writes

Model behavior of individual processes

- per-process feature collection

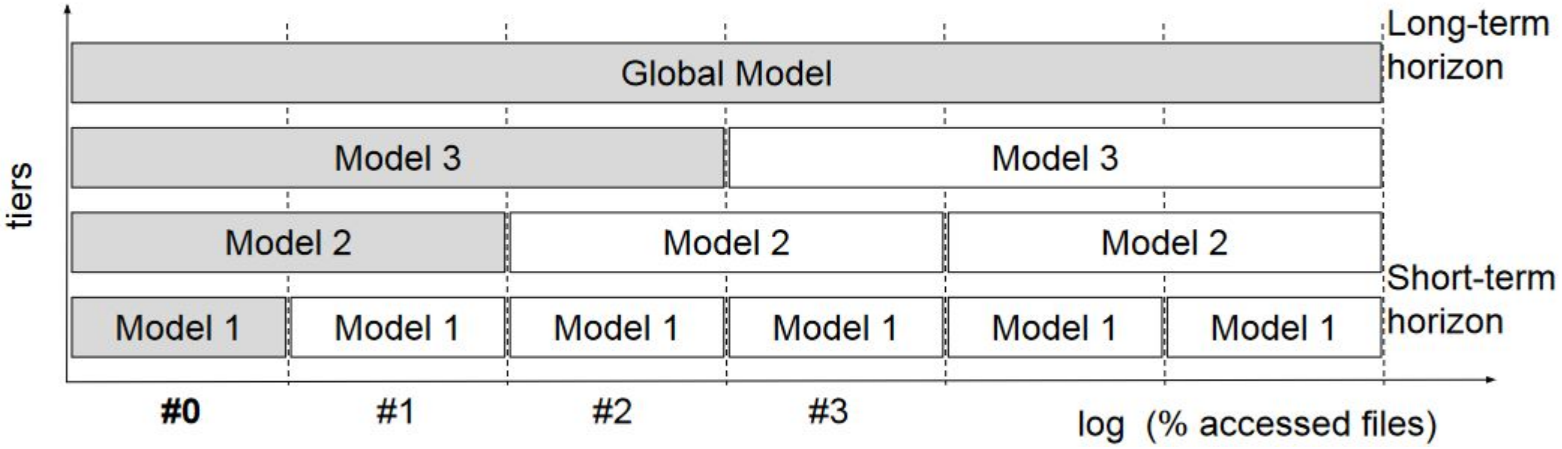
ShieldFS by Continella et al.



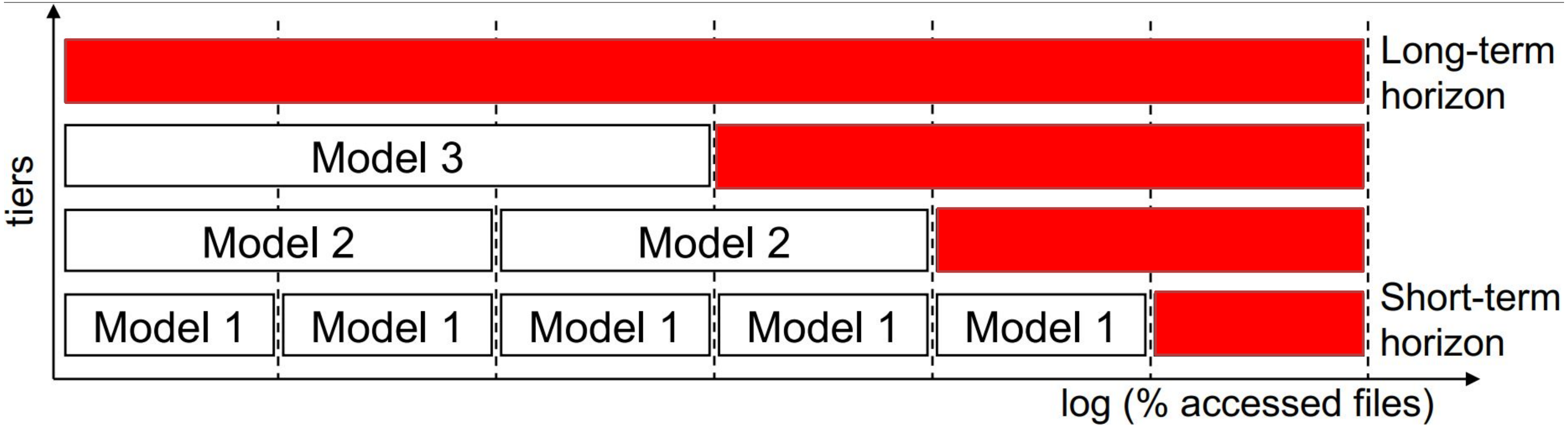
Andrea Continella, Alessandro Guagnelli, Giovanni Zingaro, Giulio De Pasquale, Alessandro Barenghi, Stefano Zanero, Federico Maggi, **ShieldFS: A Self-healing, Ransomware-aware Filesystem**, In Proceedings of the Annual Computer Security Applications Conference (ACSAC), 2016

ShieldFS Detector

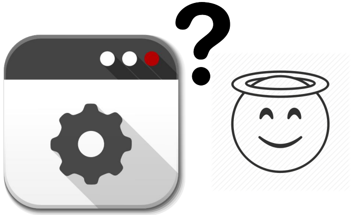
tick #0

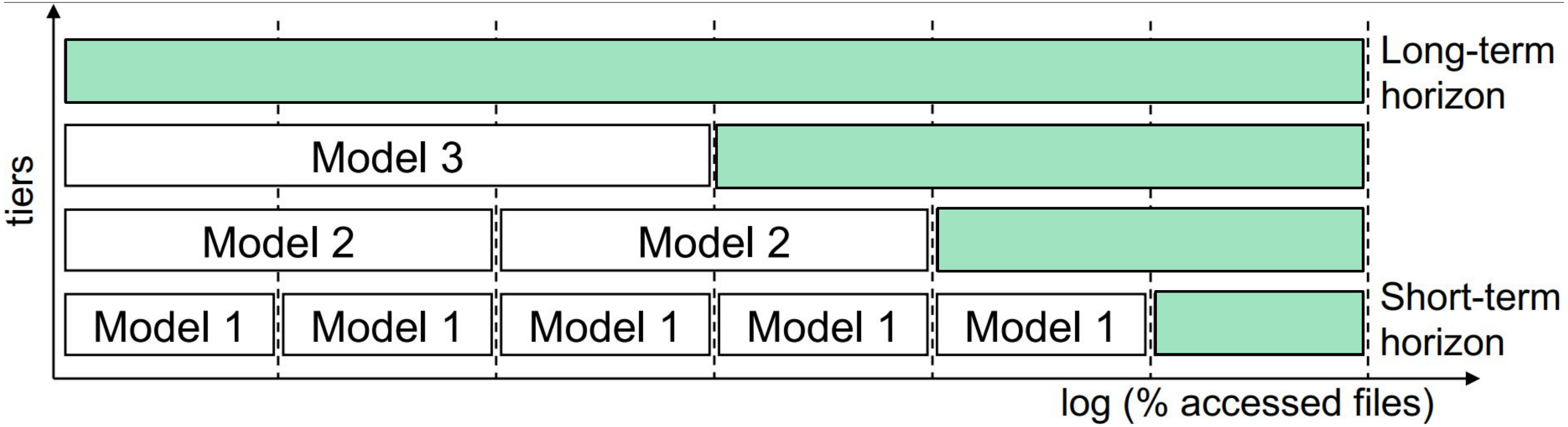


ShieldFS Detection Process

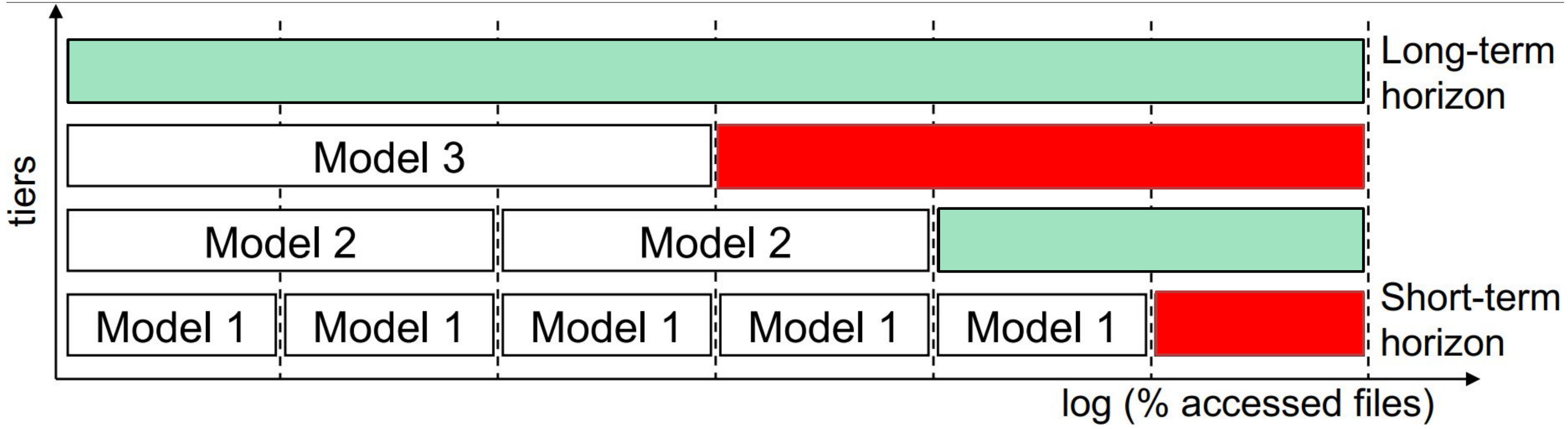


ShieldFS Detection Process

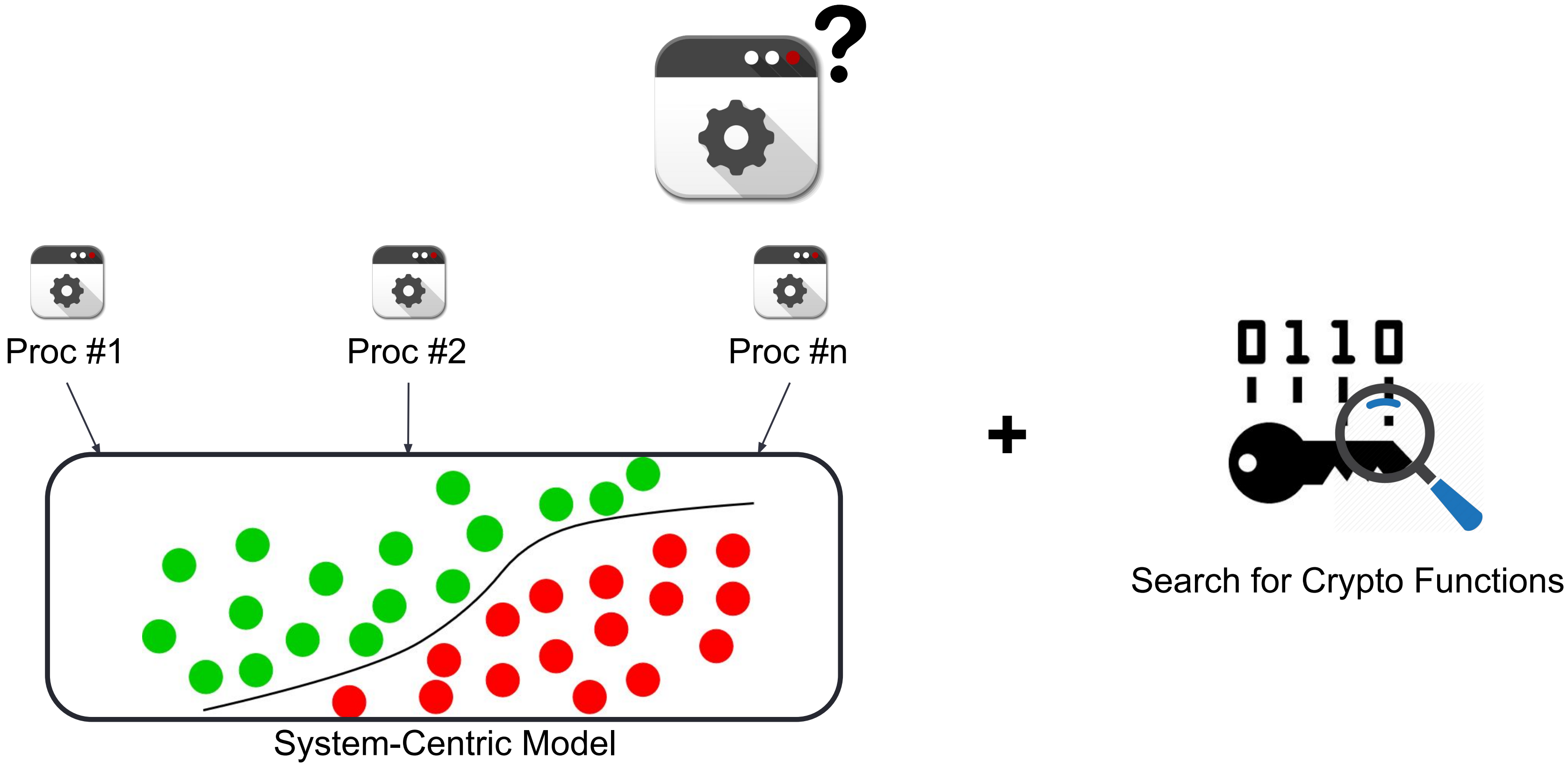




ShieldFS Detection Process



ShieldFS Detection Process



Proc #1

Proc #2

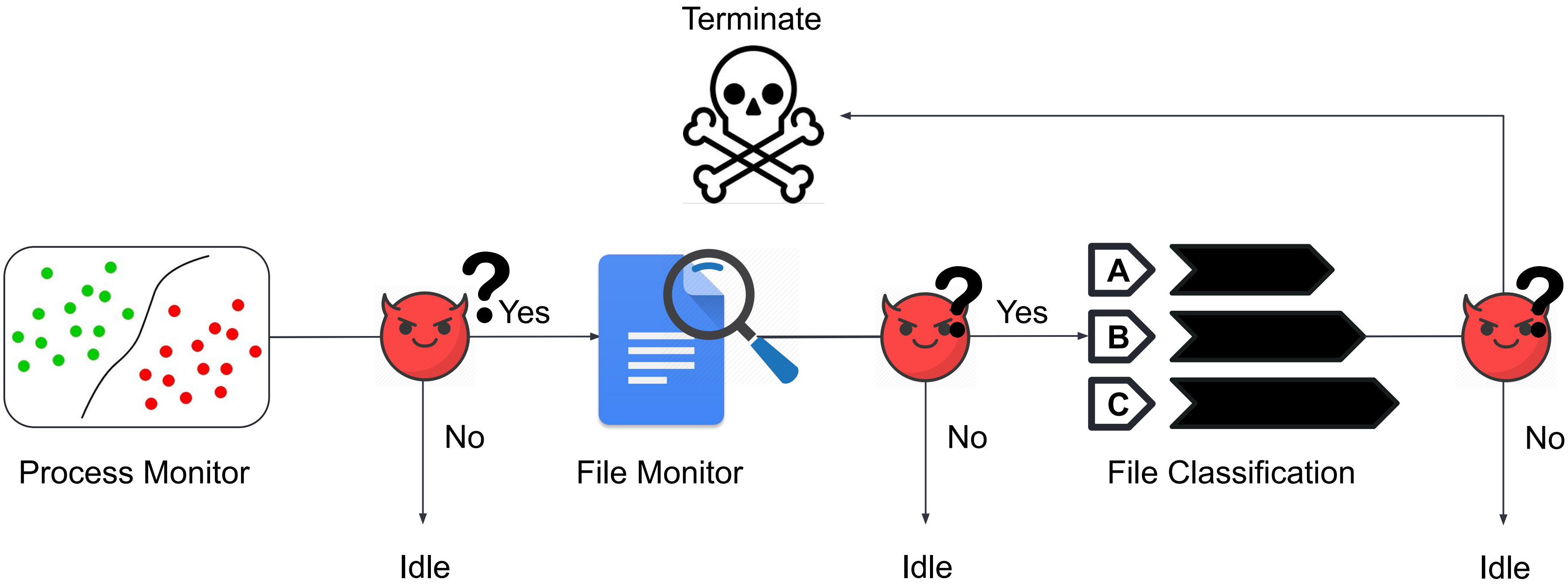
Proc #n

System-Centric Model

+

Search for Crypto Functions

RWGuard by Mehnaz et al.



Mehnaz Shagufta, Mudgerikar Anand, Bertino Elisa. **RWGuard: A Real-Time Detection System Against Cryptographic Ransomware**, RAID, 2018

Are these approaches reliable in adversarial conditions?

Evading Behavioural Classification

How can we lower the expression of all ransomware features at the process level?

- Reduce feature expression by reducing #operations

Evading Behavioural Classification

How can we lower the expression of all ransomware features at the process level?

- Reduce feature expression by reducing #operations

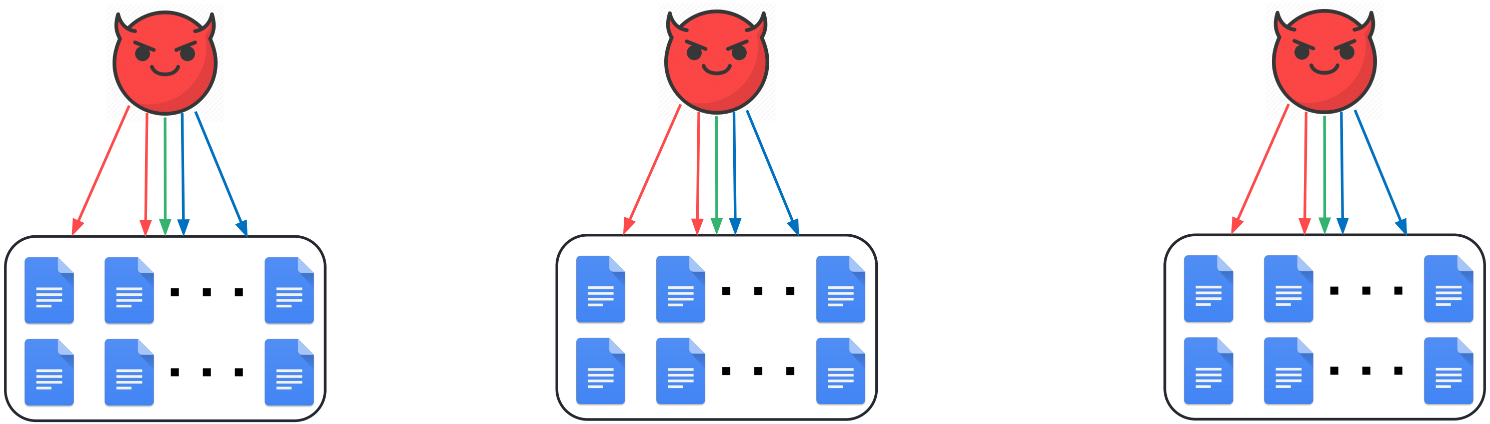
Distribute ransomware operations over independent, cooperating processes

- Process Splitting
- Functional Splitting
- Mimicry

Process splitting

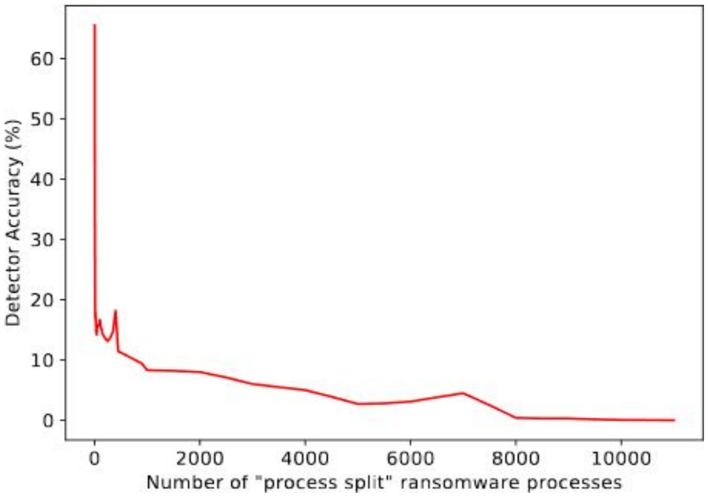
Process Splitting

- 🟥 Ransomware function 1
- 🟩 Ransomware function 2
- 🟦 Ransomware function 3

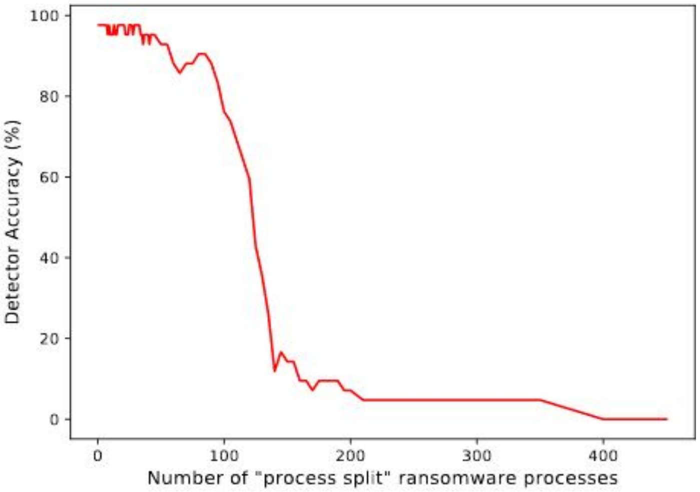


Process Splitting Evaluation

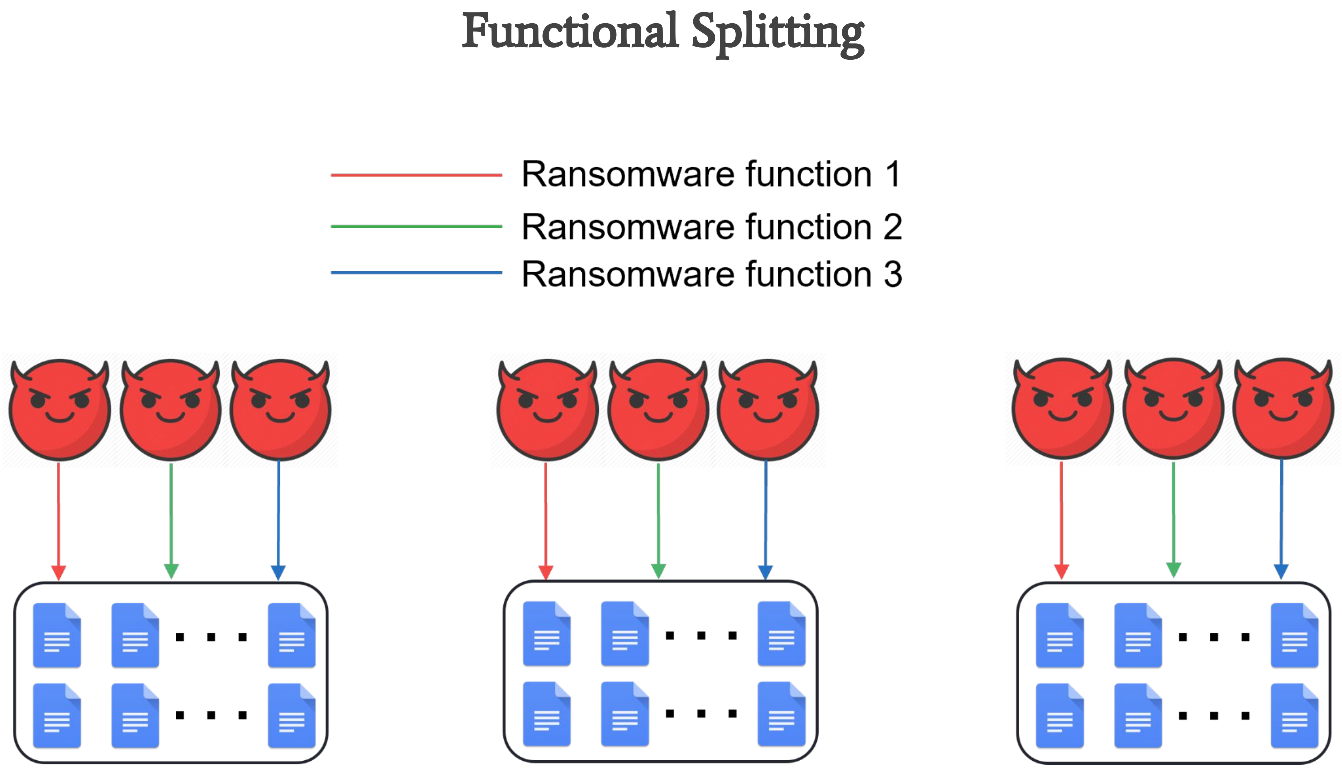
ShieldFS



RWGuard

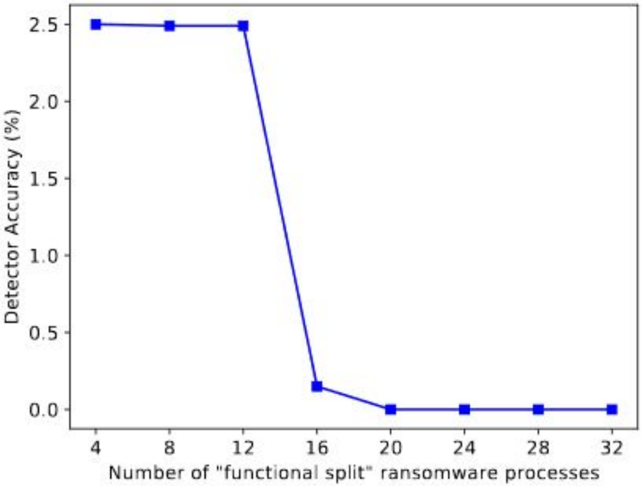


Functional splitting

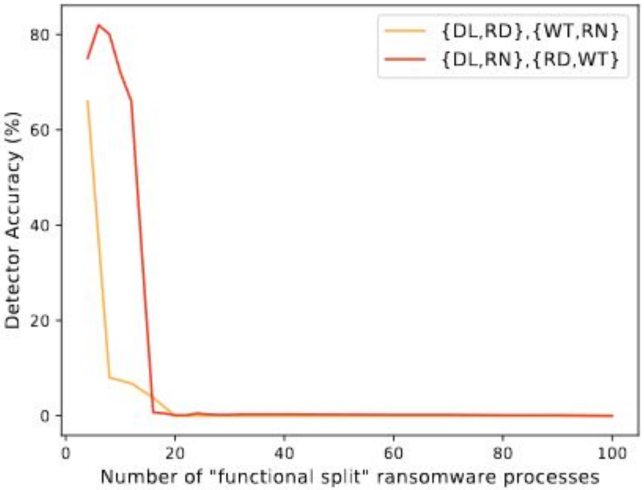


Functional Splitting Evaluation

ShieldFS



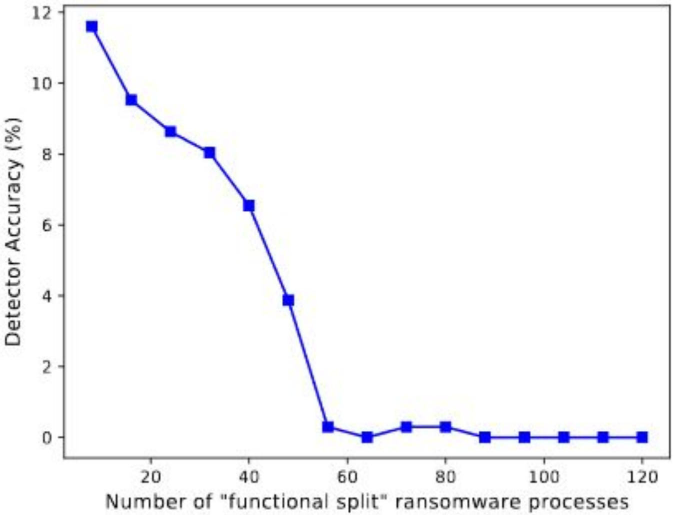
(a) Single functional splitting



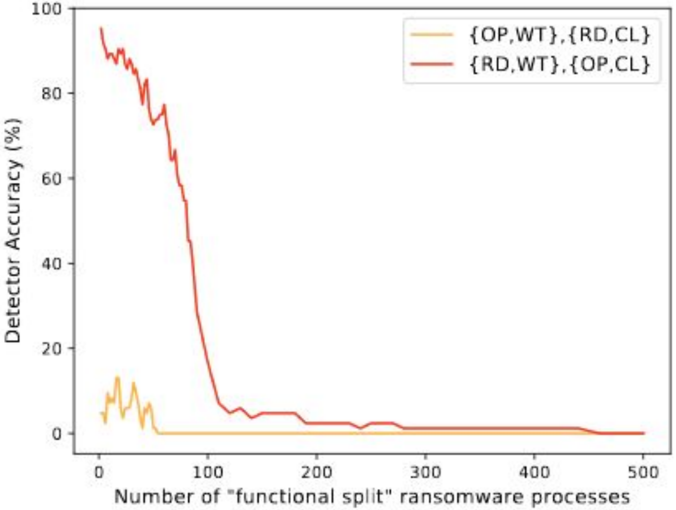
(b) Combined Functional Splitting

Functional Splitting Evaluation

RWGuard



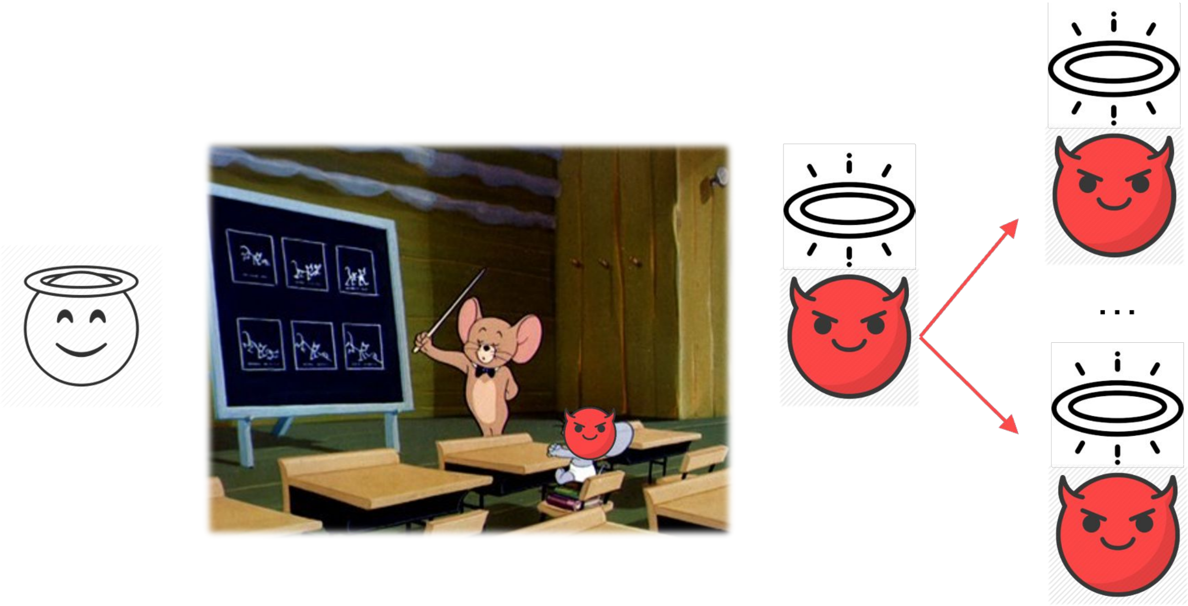
(a) Single Functional Splitting



(b) Combined Functional Splitting.

Mimicry

Mimicry:



Mimicry Evaluation

ShieldFS: full evasion

- 170 mimicry processes

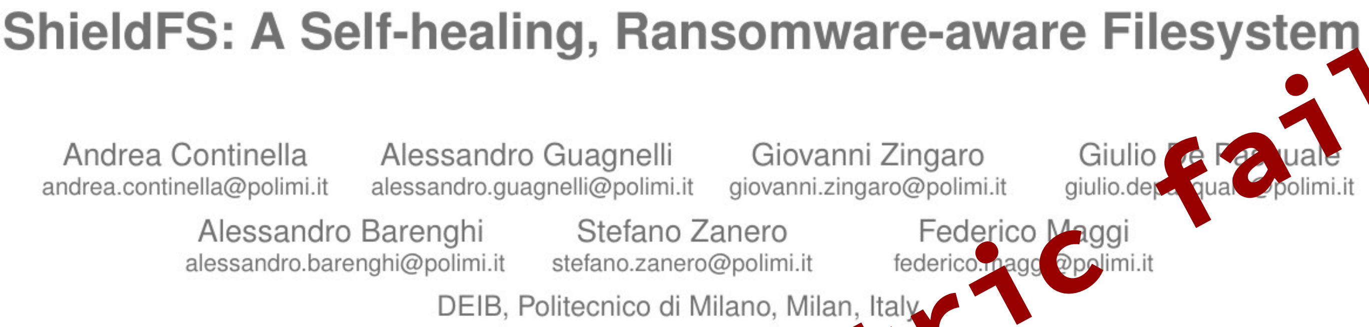
RWGuard: full evasion

- 170 mimicry processes

Malwarebytes: full evasion

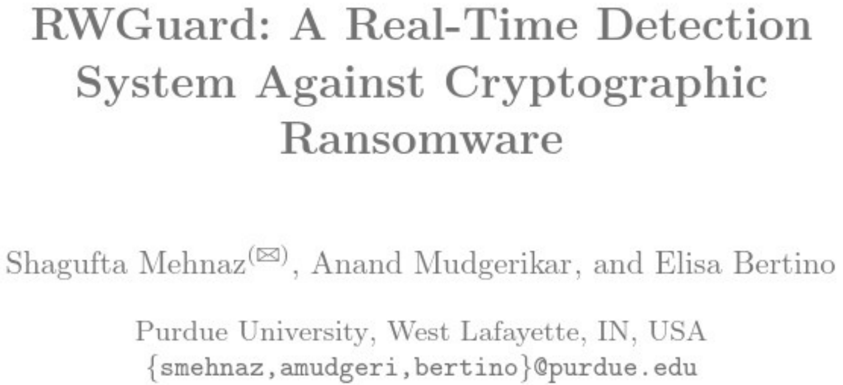
- 470 mimicry processes

Ransomware detectors



ShieldFS: A Self-healing, Ransomware-aware Filesystem

Andrea Continella andrea.continella@polimi.it
Alessandro Guagnelli alessandro.guagnelli@polimi.it
Giovanni Zingaro giovanni.zingaro@polimi.it
Giulio De Pasquale giulio.depasquale@polimi.it
Alessandro Barenghi alessandro.barenghi@polimi.it
Stefano Zanero stefano.zanero@polimi.it
Federico Maggi federico.maggi@polimi.it
DEIB, Politecnico di Milano, Milan, Italy



RWGuard: A Real-Time Detection System Against Cryptographic Ransomware

Shagufta Mehnaz(✉), Anand Mudgerikar, and Elisa Bertino

Purdue University, West Lafayette, IN, USA
{smehnaz,amudgeri,bertino}@purdue.edu

Malwarebytes

Process centric fails

Can we make these approaches more reliable?

A naive approach

- Update the behavioural classifiers on these workload distribution attacks

A naive approach

- Update the behavioural classifiers on these workload distribution attacks
  - works on process splitting and functional splitting

A naive approach

- Update the behavioural classifiers on these workload distribution attacks
  - works on process splitting and functional splitting
  - **But what about Mimicry?**

Will shifting focus help?

Process-Level Features

File-Level Features

Process-Level Features

File-Level Features

Detection Components

- Disk activity monitor
- File based behavioral detector
- File recovery module

Detection Components

- Disk activity monitor
- **File based behavioral detector**
- File recovery module

File-level features

- Read/Write data mismatch
- File write ratio
- File read ratio
- Number of Processes Reading or Writing the File
- Number of Operations on the File

File-level features

- **Read/Write data mismatch**
- File write ratio
- File read ratio
- Number of Processes Reading or Writing the File
- Number of Operations on the File

File-level features

- Read/Write data mismatch
- **File write ratio**
- File read ratio
- Number of Processes Reading or Writing the File
- Number of Operations on the File

File-level features

- Read/Write data mismatch
- File write ratio
- **File read ratio**
- Number of Processes Reading or Writing the File
- Number of Operations on the File

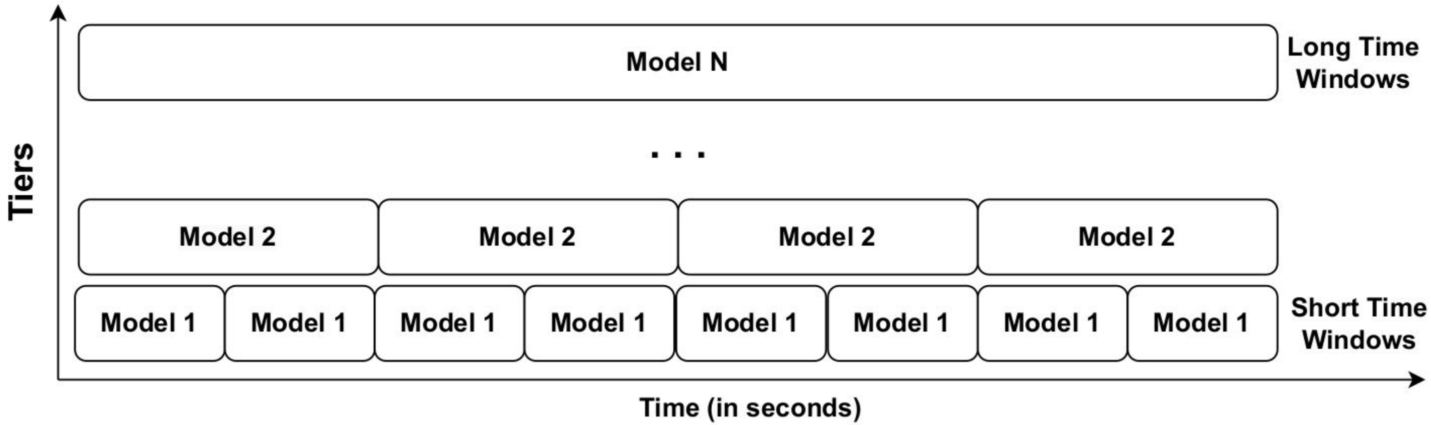
File-level features

- Read/Write data mismatch
- File write ratio
- File read ratio
- **Number of Processes Reading or Writing the File**
- Number of Operations on the File

File-level features

- Read/Write data mismatch
- File write ratio
- File read ratio
- Number of Processes Reading or Writing the File
- **Number of Operations on the File**

Detectors - ShieldFS inspired



Model N — Long Time Windows

. . .

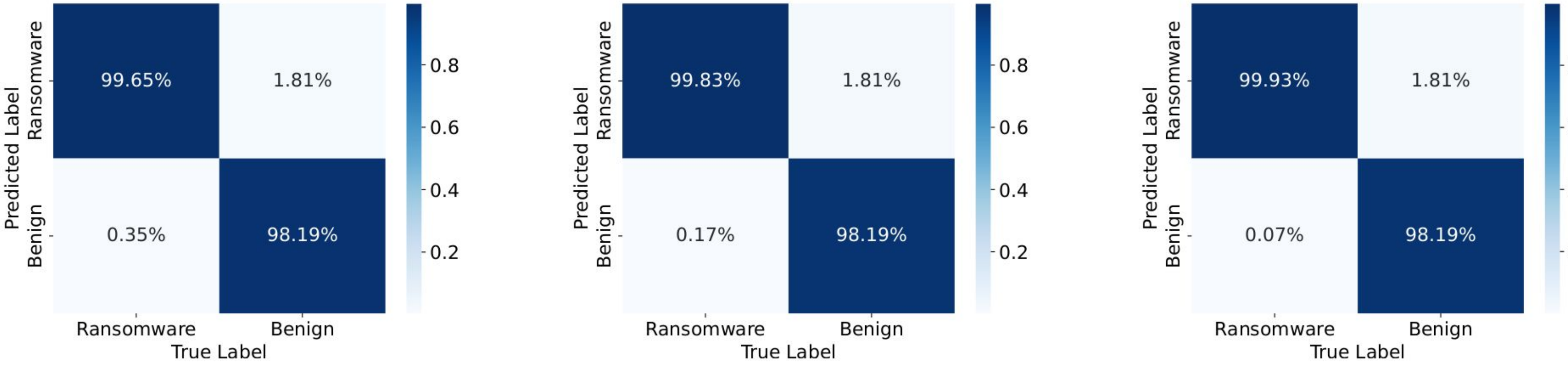
Model 2 | Model 2 | Model 2 | Model 2

Model 1 | Model 1 | Model 1 | Model 1 | Model 1 | Model 1 | Model 1 | Model 1 — Short Time Windows

Tiers

Time (in seconds)

File-centric: How does it perform?



(a) Benign vs. Traditional Ransomware

(b) Benign vs. Evasive Ransomware

(c) Benign vs. Adaptive Ransomware

Reading Material

1. ShieldFS - A self healing, ransomware aware filesystem.
2. RWGuard: A Real-Time Detection System Against Cryptographic Ransomware
3. Evading behavioral classifiers: a comprehensive analysis on evading ransomware detection techniques
4. Reliable detection of compressed and encrypted data