Georgia Tech Research Corporation

Technologies Available for LICENSING

OFFICE OF TECHNOLOGY LICENSING

https://licensing.research.gatech.edu | techlicensing@gtrc.gatech.edu

Streamlined Combination Analysis by FORECAST Accurately Predicts and Identifies Pending Malware Attacks

Overcoming malicious software post-detection is a complex and inefficient process

The detection of malware is only the start of months of chaos for the targeted system(s) and its analysts. Once a system is known to be under attack, analysts are tasked to work against the clock to fully understand the malware's capabilities and identify solutions to prevent future damage. The current practice of having analysts perform complex context switching between static disassembler and memory forensics is arduous and inefficient. The analysts can quickly become overloaded in the repetition and data load, thereby increasing the risk of human error.

The current standalone incidence response procedures are problematic. Without combining the common techniques of symbolic execution and memory forensics, path explosions and high false-negatives will limit accuracy, respectively. As malware becomes increasingly more sophisticated, the solutions to overcome cyberattacks must be swifter and more precise.

FORECAST accurately predicts and triages malware's capabilities and gives analysts a time-advantage

Combining symbolic analysis and memory forensics through a feedback loop, FORECAST automates the path identification of malware and then triages its capabilities with path probability. This streamlined process is significantly faster than the tedious assessment currently required of analysts.

FORECAST utilizes early inputs from memory images to provide an impressive overall accuracy of 94% in path identification. Its probabilistic model alerts analysts of the capability forecast (e.g., 31% code injection, 15% file extraction, 54% command & control URL) for the detected malware. The automated combination analysis removes the need for an analyst to focus on stitching up code or be consumed by the context switching. This frees up cognitive effort to focus on solutions of the probable paths rather than their identification, thereby increasing the analysts strategic time-advantage over the malicious software.

Summary Bullets

- Automating the combined techniques of memory forensics and symbolic analysis accelerates how fast an enterprise or government becomes aware of the true extent of malware's capabilities.
- When countering cyberattacks, FORECAST provides improved accuracy (94%, overall) with its automated analysis, which is crucial to helping cybersecurity efforts to efficiently focus on high-impact solutions.
- FORECAST has the flexibility to be a valuable incidence response tool, even when malware is fileless since it uses the software's memory image to accurately predict the program's capabilities.

Solution Advantages

- **Faster**: Automating the combined analysis through a feedback loop eliminates the tedious context-switching analysis required by analysts.
- **Accurate**: FORECAST's automated identification of probable paths is significantly more accurate (94% accuracy, overall) than the results of data-heavy processing by analysts.
- **Strategic**: Removing the need for analysts to focus on identification of probable paths allows more strategic time to be focused on finding solutions to circumvent the paths.

Potential Commercial Applications

- Cyber security
    - National security
    - Enterprise systems
    - Health care systems

Inventors

- Moses Ike
  Ph.D student - Georgia Tech School of Computing
- Dr. Omar Alrawi
  Former PhD student - Georgia Tech School of Electrical and Computer Engineering
- Dr. Brendan Saltaformaggio
  Assistant Professor - Georgia Tech School of Cybersecurity and Privacy and the School of Electrical and Computer Engineering

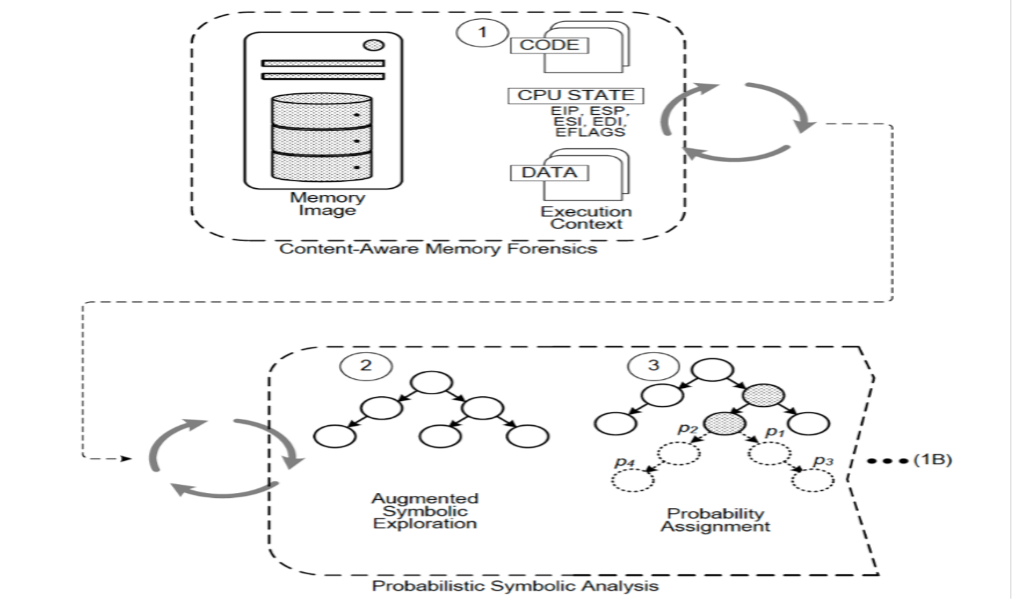
IP Status

<p class="MsoNormal">The following patent application has published<o:p></o:p></p>: US20230044579A1

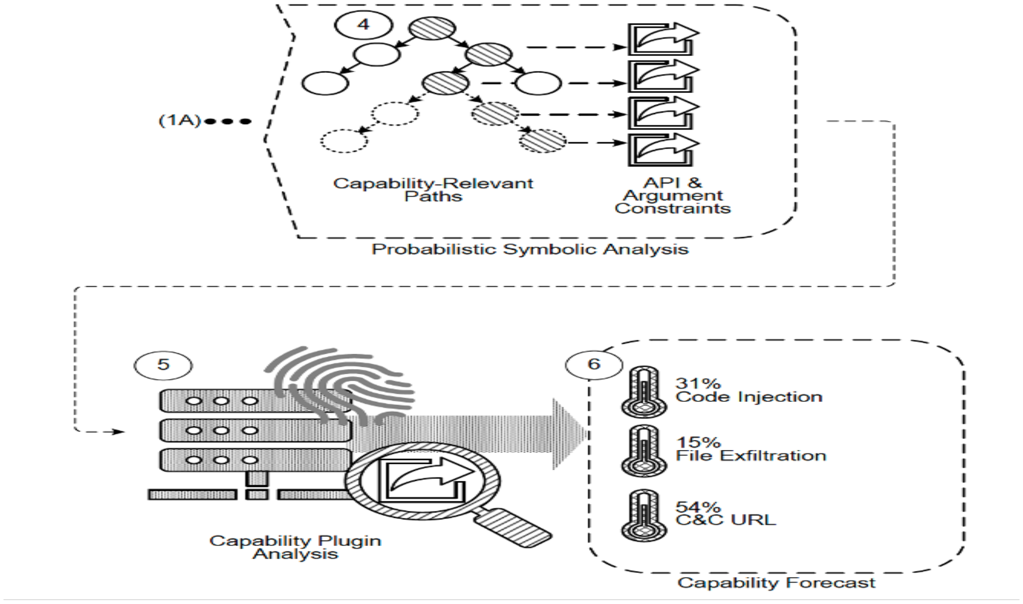
Publications

Forecasting Malware Capabilities From Cyber Attack Memory Images, 30th USENIX Security Symposium - August 11–13, 2021

Images



FORECAST’s automated analysis combines two techniques: memory forensics and symbolic analysis.



FORECAST delivers triaged probable paths

Visit the Technology here:
Streamlined Combination Analysis by FORECAST Accurately Predicts and Identifies Pending Malware Attacks

https://s3.sandbox.research.gatech.edu//print/pdf/node/3184