R&K CYBER SOLUTIONS
Higher Thinking for Higher Stakes

HYPERION

MAKING THE WORLD'S SOFTWARE SAFER

HYPERION: The World's First Behavior Computation System for Application Security

We live in a software-defined world. Software needs to be secure. And we need to know it. It's as simple as that.

But after billions spent, attackers still insert malware into our systems and exploit vulnerabilities. Cybersecurity methods are reaching the limits of their potential. And they are proving insufficient. A new approach is needed.

R&K has created new technology to compute the behavior of software. It's very difficult to hide malware from behavior computation. So R&K finds it. Your risk is reduced. Your cost is reduced. It's as simple as that.

Behavior computation doesn't stop there. It supports software assurance for supply chains, and in the future, will support development and testing as well.

R&K'S HYPERION INNOVATION

R&K's Hyperion system takes in code and automatically computes its behavior, whether legitimate or malicious. The term "behavior" here means what the code does, its net effect on your system. It is an "as-built" specification of the code.

Hyperion is a new class of system. It is not static analysis because it does not look for malware in code. It is not dynamic analysis because it does not look for malware in executions. Hyperion defines a new cybersecurity category called Behavior Computation for Application Security (BCAS). Hyperion is the only commercially available BCAS system.

STATIC ANALYSIS

Scanning for malware in code is a difficult game of signature catch-up, with the advantage on the attacking side.

The syntactic scanning methods of static analysis depend on signatures that are easily thwarted by simple syntactic variations. Signature generation is a permanent arms race with attackers that we are losing. Signatures proliferate, but intrusions continue as malware without signatures slips through.

DYNAMIC ANALYSIS

Executing code to find malware is a frustrating game of finding coverage gaps that attackers can exploit.

Dynamic execution depends on tracing paths in software. But software contains huge numbers of possible paths. Execution can hope to exercise only small fractions of them. And malware on paths not executed slips through.

There are many static and dynamic analysis products developed and fielded by capable organizations. The limits of these methods do not stem from a lack of effort or talent. They arise from fundamental properties of the underlying technologies that are difficult to surmount despite best efforts.

COMPUTING SOFTWARE BEHAVIOR

Hyperion takes a different approach. It does not use or seek to improve static or dynamic analysis. Instead, Hyperion applies the mathematical foundations of denotational semantics to compute the behavior of software. Hyperion reveals the deep meaning of software, literally what it does, and expresses it as individual cases of behavior that the software can produce. The effects of both legitimate functionality and malicious operations are computed.

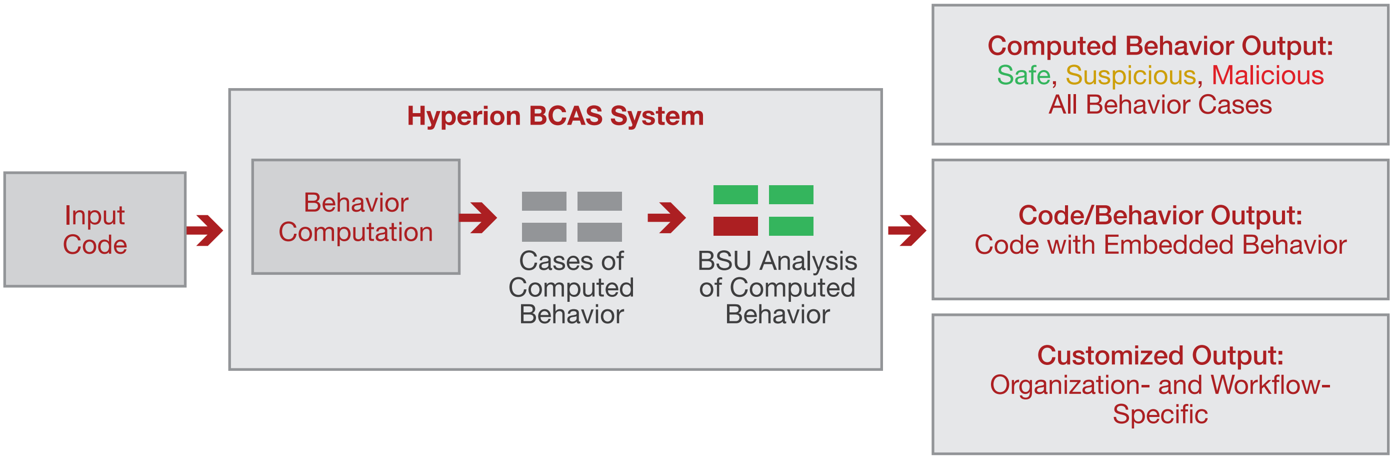
It's not hard to hide malware from static or dynamic analysis, but it's very hard to hide it from behavior computation. This is because malware is code that must run on your machine to achieve its objectives. It's just more code to Hyperion, and it will be aggregated and coalesced into cases of behavior just like everything else, even if it is hidden or distributed in your software. Few or no false positives are generated in this process. The actual behavior of software is revealed, whether good or bad. This capability is baked into the algorithms. The algorithms don't look for malware in the code. They simply compute its behavior, whatever it happens to be.

KNOWING BEHAVIOR

It is important to know behavior, because software with unknown behavior has unknown security.

REVEALING MALWARE IN COMPUTED BEHAVIOR

R&K doesn't stop there. Computed behavior makes malicious content easier to find, and Hyperion capitalizes on this simple fact. The system incorporates R&K's malware expertise and applies it to computed behavior to reveal whatever malware is present.


Input Code
Hyperion BCAS System
Behavior Computation
Cases of Computed Behavior
BSU Analysis of Computed Behavior
Computed Behavior Output:
Safe, Suspicious, Malicious
All Behavior Cases
Code/Behavior Output:
Code with Embedded Behavior
Customized Output:
Organization- and Workflow-Specific

MALWARE BEHAVIOR

Useful generality emerges at the semantic level. For example, there are many ways to code a keylogger, but only one Keylogger BSU is required.

R&K's malware expertise is captured through Hyperion's Behavior Specification Units (BSUs). BSUs are simple definitions of malicious operations.

LEVERAGING EXPERTISE

Malware analyst expertise is incorporated into Hyperion BSUs for permanent reuse to reduce cost and level-of-effort.

Hyperion includes a set of BSUs developed by R&K, and you can add to them. They can be applied over and over to new malware, even by junior analysts. BSUs are very general and broadly applicable. You don't need many of them.

Computed behavior and BSUs automate much of malware detection and analysis. This is one way Hyperion saves time and money. You can do more with existing staff and don't need to add people. Throughput, quality of results, and span-of-control can be improved with no additional expense.

These capabilities are summarized in the following flow of Hyperion operations: behavior computation for compiled binaries, malware detection with Behavior Specification Units, and output generation.

The Computed Behavior output supports CERT use-cases as embodied in Tier 1 and 2 analyses. It identifies code as Safe, Suspicious, or Malicious, and enumerates the computed cases of behavior.

Hyperion's code structuring eliminates spaghetti logic and control flow obfuscation. The Code/Behavior output integrates the input code in structured form with its computed behavior, embedded where it actually occurs in the logic. This output supports Reverse Engineering use-cases at the Tier 3 level.

Hyperion produces a rich variety of previously unavailable information accessible through APIs in a JSON repository. These artifacts include structured code, computed behavior, and BSU analysis. The outputs described above are only examples of what can be easily created for various workflows and user needs within your organization.

Hyperion also produces behavior-based Yara signatures for Automated Indicator Sharing in Computer Network Defense operations.

These outputs support operations carried out by your cybersecurity and IT staff, but the real focus of Hyperion is on providing visibility to executive management. R&K is committed to providing a new level of visibility to achieve intellectual control over enterprise software. The goal is informed decision-making and reduced cybersecurity risk.

WHAT HYPERION CAN DO

In operational use, Hyperion reveals malware in internally and externally developed software. The full power of the system shows up in these examples:

- Revealing zero-day malware: Hyperion routinely identifies malware others can't find. For example, Hyperion detects zero-day malware for which no syntactic signatures or dynamic executions exist. This malware is typically not identified by any of the 50 or so malware tools available on VirusTotal, a popular malware aggregation site.
- Revealing sleeper code: Sleeper code is notoriously difficult to find because of the complex conditions under which it is typically triggered. Hyperion simply aggregates and reveals these conditions in its normal processing.
- Revealing obfuscated malware: Hyperion routinely eliminates control flow obfuscation and randomly inserted no-op code that attackers employ to increase complexity and evade detection.
- Revealing distributed malware: Hyperion detects the functionality of malware that has been intentionally fragmented and distributed throughout your software.
- Rechecking software: Your software can be run through Hyperion any time at virtually no marginal cost to guard against recently inserted malware.

SOFTWARE ASSURANCE AND BEYOND

Validating the security and functionality of vendor, supply chain, and open source software is costly and time-consuming. Hyperion's capability to reveal malware applies in full force to software assurance, and helps to validate legitimate functionality as well.

Computed behavior provides a wealth of solid information previously unavailable to software engineers and executive management. R&K's Hyperion Product Development Plan includes applying this automated technology to reduce cost and effort in software development and testing, and extending behavior computation to additional computer architectures and languages.

R&K'S TRACK RECORD

Initial research on what became the Hyperion system was done at Oak Ridge National Laboratory. R&K holds an exclusive license for this system, and has invested substantially to transform it from a proof-of-concept prototype into a capable and reliable commercial product.

Hyperion was selected by the Department of Homeland Security (DHS) for its Transition to Practice (TTP) program. TTP identifies promising technologies in national laboratories and helps transition them into product-level capabilities for Federal and commercial markets. The system was extensively vetted by Sandia National Laboratories as part of this process.

Hyperion was selected by TTP for pilot projects in the malware laboratories of Federal agencies, including US-CERT in DHS and an agency in the Intelligence Community. These projects revealed the value of Hyperion technology in addressing difficult malware detection and analysis problems while reducing cost and risk. A cost/benefit analysis based on the pilot projects revealed an approximately 20x reduction in cost and level-of-effort, while producing superior results compared to the traditional manual analysis employed by these organizations.

Hyperion effectively automates substantial portions of CERT and Reverse Engineering functions, permitting increased span-of-control for wider and deeper malware analysis, and less risk to an organization. The system also supports software assurance operations, in assessing the security of vendor, supply chain, and open-source software.

R&D 100 AWARD

Hyperion has joined an exclusive club. Previous winners include HDTV and MRI.

R&K's vision for Hyperion is shared by others. The system is a winner of the prestigious R&D 100 Award, selected from thousands of nominations as an advanced technology in cybersecurity.

The system is currently under evaluation by several Fortune 50 companies for use in multiple roles and organizations as a new technology for cyber defense. One Principal Investigator observed that Hyperion is "Setting a new standard in cybersecurity."

R&K employs the inventors of software behavior computation, plus the team of cybersecurity experts from ORNL that developed the Hyperion prototype. This team is uniquely qualified to evolve and support behavior computation technology for our customers.

Hyperion is the "Fourier Transform" of cybersecurity, moving from syntax to semantics where problems are recast in a form that enables effective solutions previously unavailable. This new approach to security is at the beginning, not the end, of its evolution. Hyperion is not more of the past; it is new technology for the future of cybersecurity.

Behavior Computation for Application Security (BCAS) is a new class of analytical system based on computational semantics for software. Hyperion is the first of its kind. The Hyperion BCAS system is available now for evaluation within your organization.