GRAMMATECH

ReSCIND Proposer's Day

System Modeling and Monitoring

Zak Fry

Problem Statement

1. Identify and model human limitations or cognitive biases relevant to cyber attack behavior
2. Understand, measure, and induce changes in cyber attack behavior and success
3. Provide algorithms for automated adaptation of these solutions based on observed cyber attacker behavior.

GrammaTech Capabilities, at a Glance

Modeling > Monitoring > Mitigation

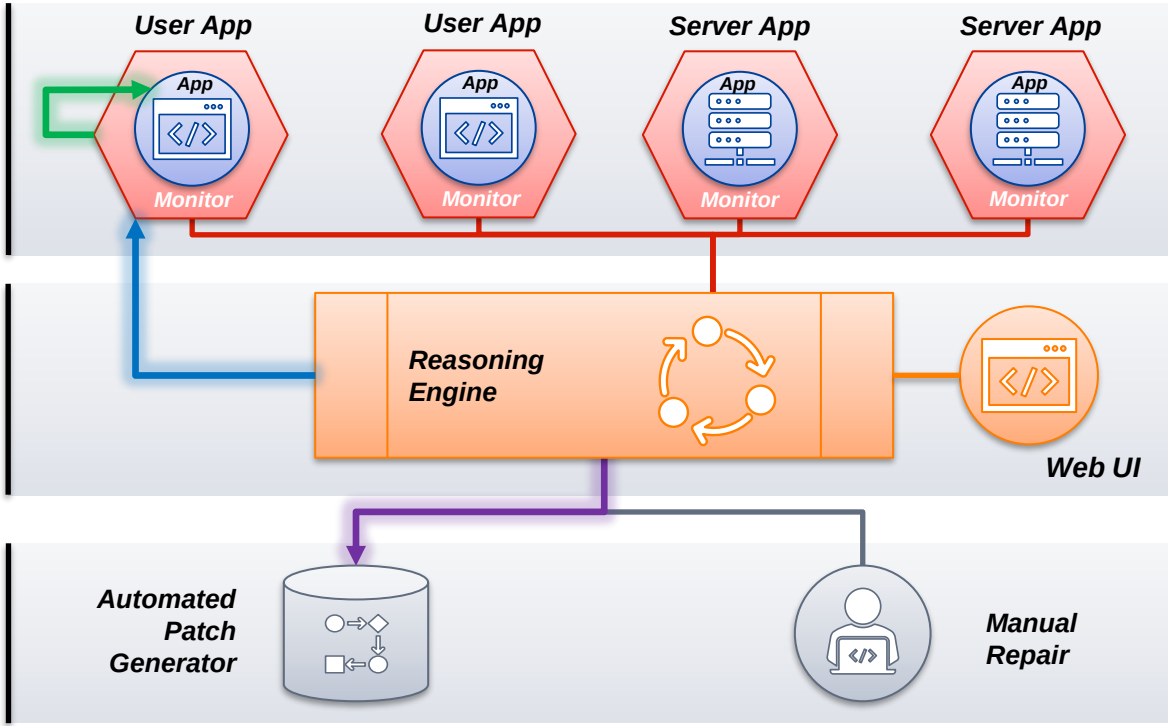
- *Model:* Program Behavior, Configurations, System Properties, Credentials
- *Monitor:* Runtime checkers, note violations as possible attacks, Model checking/querying
- *Mitigation:* Atomic real-time state changes, System-level reconfigurations, Forensics

Deployment: Multi-Layer Security Solution

Deploy ***local monitor policies*** to ***running applications***. Policies watch for malicious behavior and carry out local ***reflex responses***.

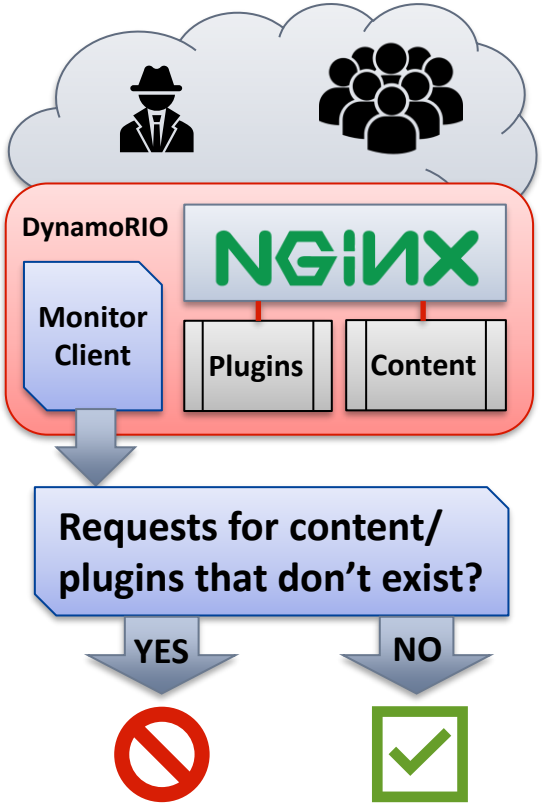
Report monitor events to ***"big picture" reasoning engine*** to track overall system health; detect additional and multi-program attacks. Engine carries ***secondary responses***.

Long-term and recurrent problems result in **longer-term responses**, e.g., ***automated patch generation***, ***manual remediation***.



NGINX Webserver Example

- **Problem**: Bots probe public servers looking for known-vulnerable modules and secure content
- **Autonomic Solution**:
  - Monitor: Use Tiffin-internal variable per-IP to count accesses to non-existent pages/content
  - Mitigation: Block individual or ranges of IPs from initiating requests entirely



ConfINE: System-Level Modeling

- **Formally model complex networked-composed systems**
  - *Network setup:* topology, routing, firewall ACLs, ipsec tunnels, etc.
  - *System setup:* user configuration, file permissions, PKI, X.509, etc.
  - *Service setup:* e.g., ssh, apache, docker configuration
  - *User knowledge:* system-access credentials
  - *Low-level vulnerabilities:* known CVEs, detected 0-days

- **Query system-wide access-control properties:**

Can a user with certain level of physical access and certain knowledge perform a certain operation on certain resource?

System Modeling: Security Applications

- Penetration testing and red teaming:
  - Can an outsider with minimal knowledge gain access to system's sensitive data?
  - If so, how? Can we get a sequence of operations to execute?
- Internal threat minimization:
  - Find system users with privileges that are not required for system functionality
  - Ensure access privileges are properly revoked
- Forensic analysis:
  - The system is breached!
  - What is the breach perimeter? What system data can we still trust?

Problem Statement

Seeking:

1. Identify and model human limitations or cognitive biases relevant to cyber attack behavior
2. Provide algorithms for automated adaptation of these solutions based on observed cyber attacker behavior.