

TARDIS

Trust and Appraisal for Resilience of Distributed Information Systems

Jon Millen
781-271-5172
jmillen@mitre.org

John Ramsdell
781-271-7565
ramsdell@mitre.org

MSR



Problem



- Missions are supported with distributed systems.
- Cyber attacks can be expected to succeed in subverting one or more nodes.
- Resiliency against compromised nodes can be built in, but...
 - Programmers don't have easy access to resiliency capabilities.

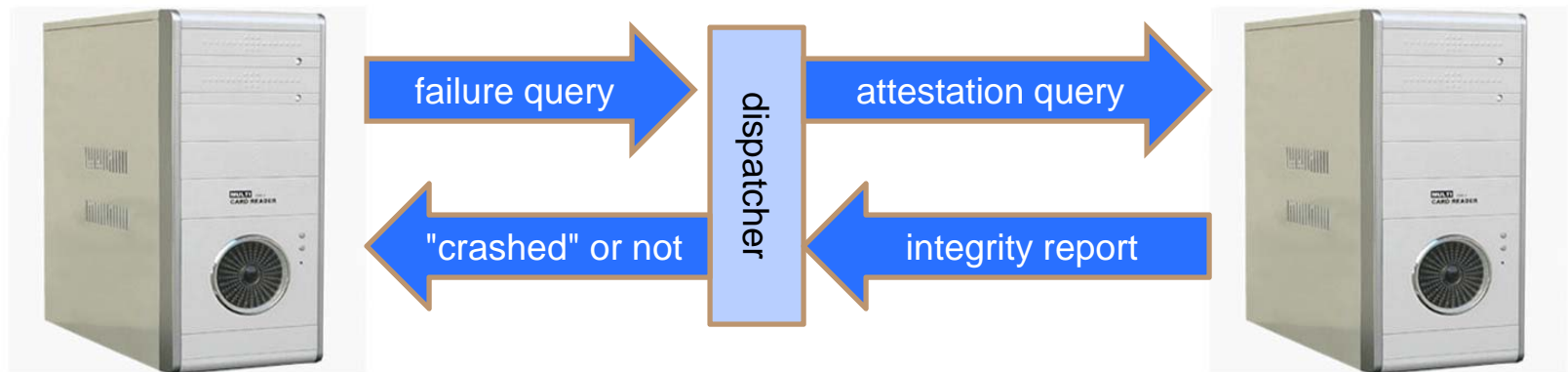
Background



- Many distributed system functions are based on algorithms to establish agreement among cooperating nodes.
- Agreement algorithms use "failure detectors" to distinguish crash failures from normal response delays.
- BUT: cyber attacks can subvert nodes to maliciously provide false responses, rather than simply being nonresponsive.
- Subverted nodes can be detected with a combination of trusted hardware, virtual machine architecture, and cryptographic attestation protocols
 - We have experience with this technology from prior MSR, MOIE, and sponsored projects.

Objective

- Help distributed agreement protocols deal with malicious failures.
- Idea: replace crash failure detection with malicious failure detection, using an attestation protocol.
- A malicious failure can be reported as a crash failure to the agreement protocol!



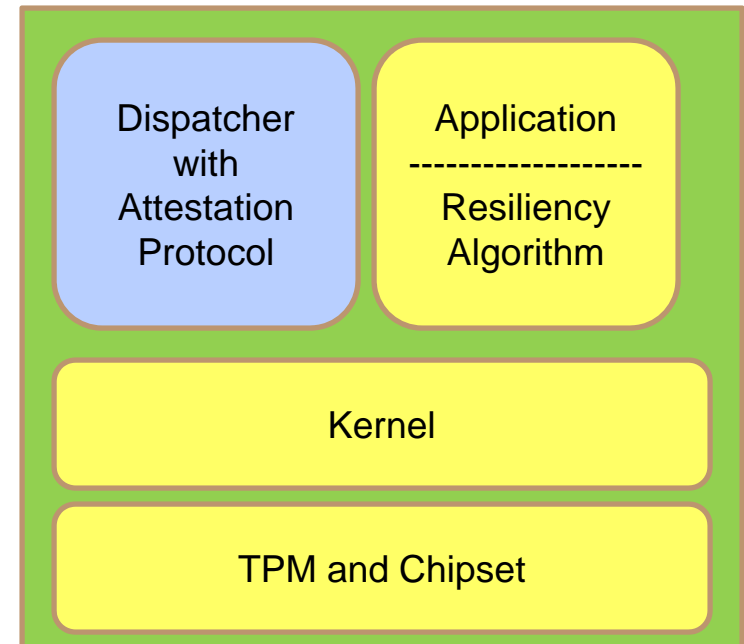
Activities



- **Use Erlang for a prototyping language (easy to write distributed system protocols).**
- **Adapt existing Erlang distributed agreement protocol with failure detection**
 - Erlang version of dispatcher.
- **Implement an Erlang interface to trusted hardware (Trusted Platform Module) for integrity report.**
- **Integrate the resilient distributed agreement capability with potential applications.**

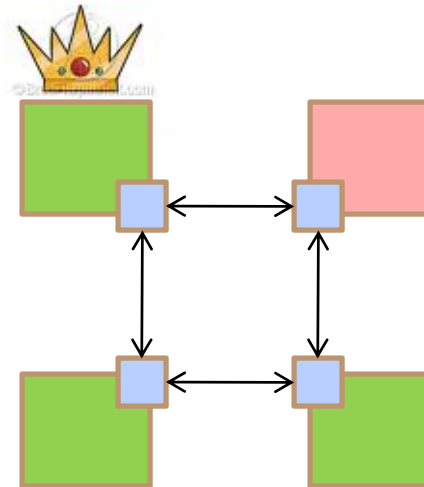
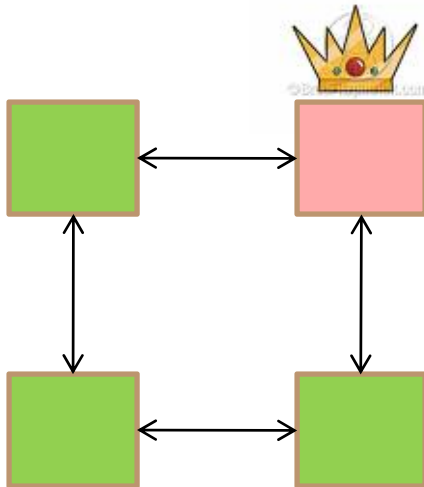
Highlight

- **Resiliency algorithm in application**
 - handles crash failures.
- **Dispatcher with Attestation**
 - handles subversion reports.
- **Trusted Platform Module (TPM)**
 - root of trust for integrity reports.
- **Kernel should be a Virtual Machine Monitor or hypervisor**
 - takes advantage of chipset (CPU+) for greater integrity.



Demonstration

- Distributed system with a few nodes.
- "Leader election" example of distributed application.
- Some nodes may be chosen to be malicious.
- Original application may elect malicious leader.
- Improved system with attestation always elects good leader!



Impacts



- **Application-oriented support for resilient distributed programming.**
- **Widespread, reliable application of cyber attack resiliency techniques.**
- **Continued operation or graceful degradation of mission capabilities supported by distributed systems.**

Future Plans



- **Support for hybrid systems – some legacy nodes.**
- **Resilient attestation infrastructure (measurement authorities).**
- **Attestation with real-time remeasurement.**
- **Measurement and reconstitution of user virtual machines.**
- **Integrity measurement of dynamic and obfuscated software.**
- **Integration with data resiliency mechanisms.**