Designing Mission Survivable Systems Using Proactive Schemes

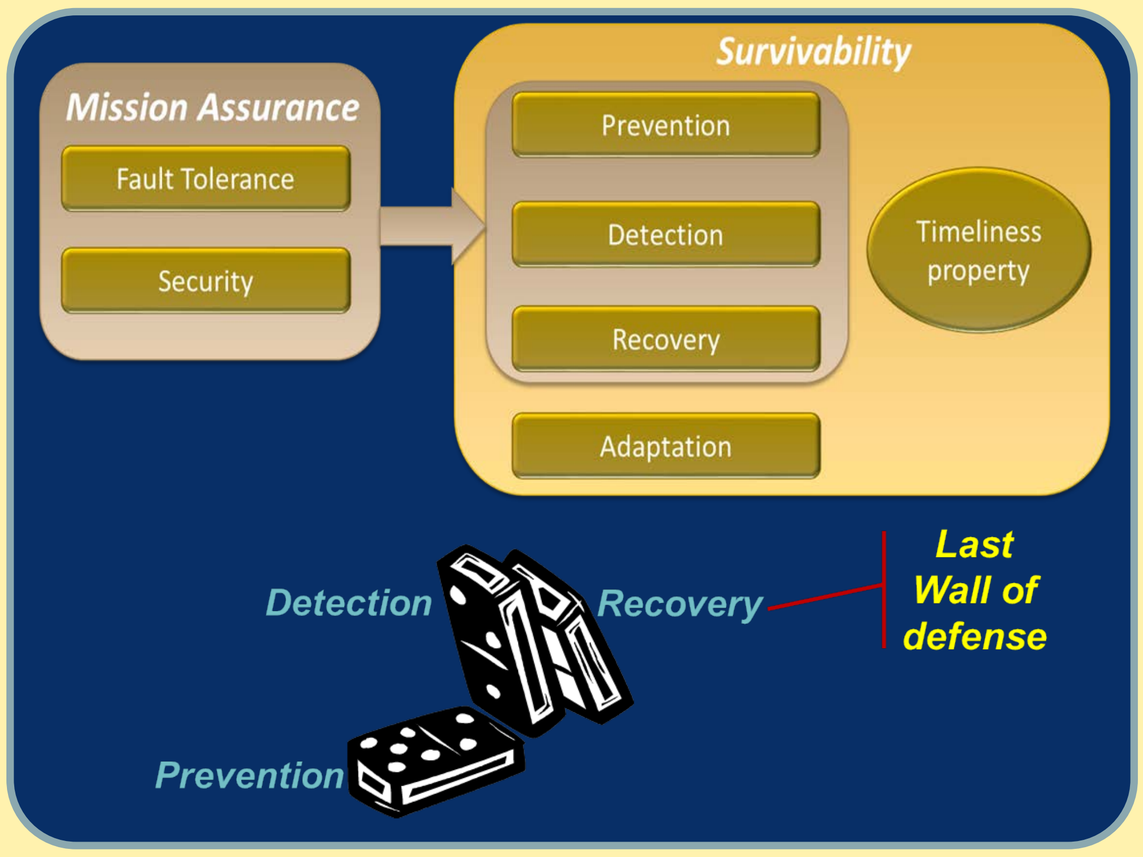
Prof. Shambhu Upadhyaya, University at Buffalo
(http://www.cse.buffalo.edu/~shambhu)

Mission-Critical Systems

- Essential subsystems whose failure disrupts a mission or business operations
- Instances: military, power grid, e-business, etc.

Advanced Attacks

- Smart and adaptive (unpredictable)
- Ample resources (well-sponsored)
- Stealthy and persistent (quiet invader)
- Multiple stages
  - low-risk reconnaissance
  - install spyware
  - design and develop specific exploits, etc.
- Most such attacks have a contingency plan



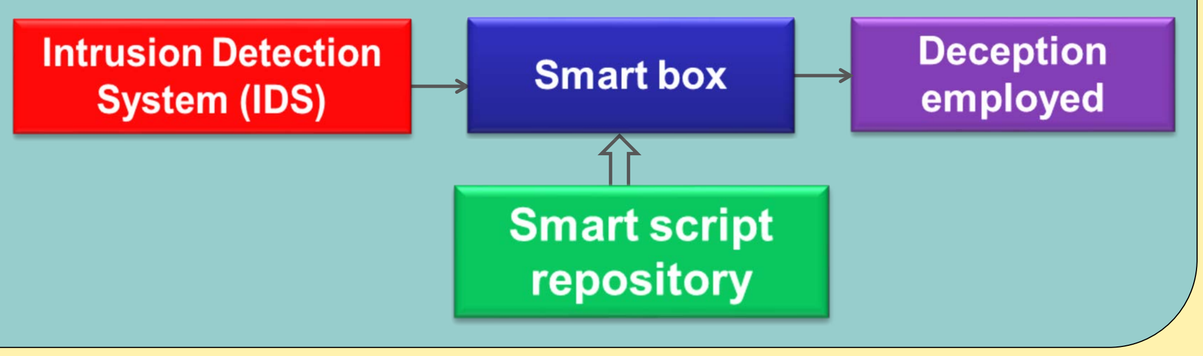
- Recovery is the last wall of defense; but may be attacked, needs to be strengthened
- We aim to provide mission survivability against advanced attacks
- Proposed solution employs a deception-based secure proactive recovery scheme

Approach

Monitoring and Reporting

- Tamper-resistant architecture for reliable host monitoring
- Host based monitor securely and surreptitiously reports intrusions via a hardware-based scheme

Deception-based Recovery



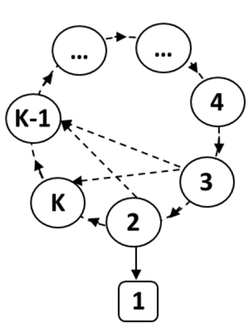
Progress so far

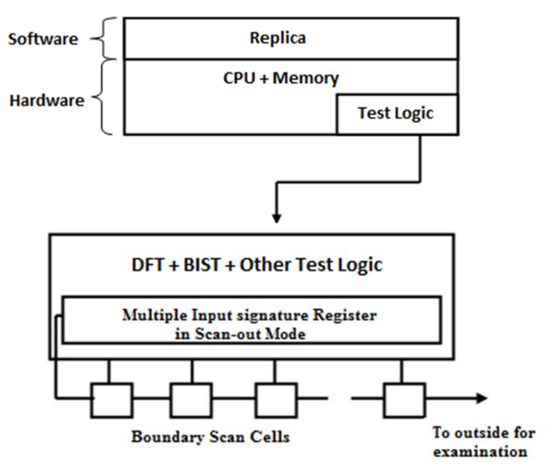
Reliable Host Monitoring

R. Mehresh, J.J. Rao, S. Upadhyaya, S. Natarajan and K. Kwiat "**Tamper-resistant Monitoring for Securing Multi-core Environments**" *Int. Conf. on Security and Management (SAM)*, Las Vegas, NV, July 2011

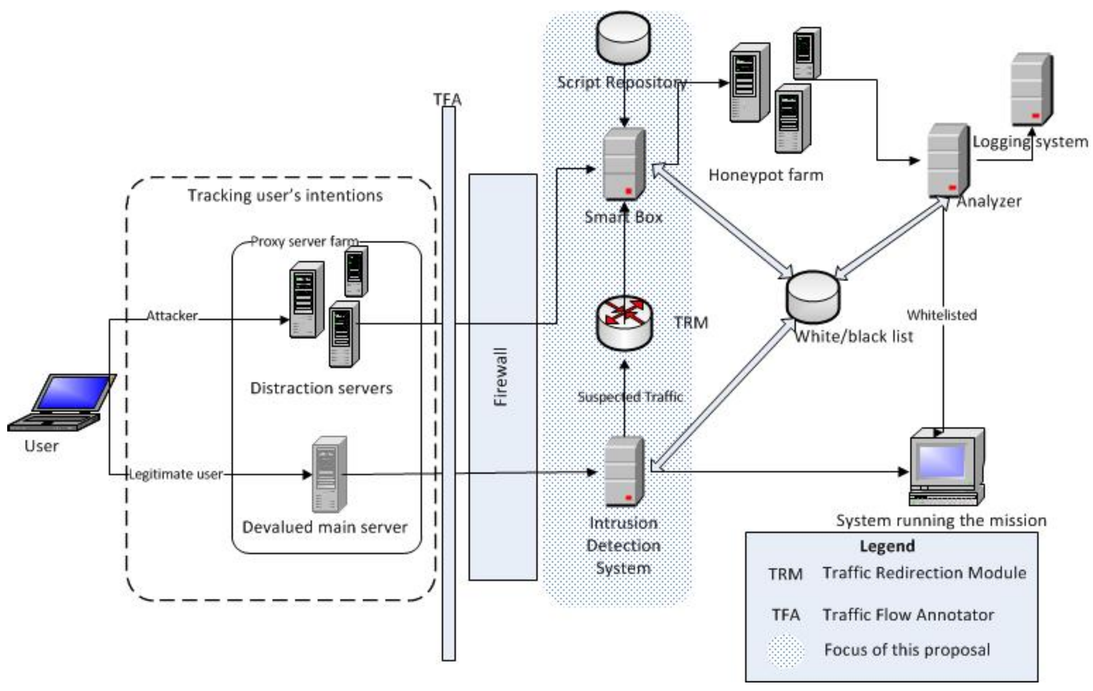
Surreptitious Reporting

R. Mehresh, S. Upadhyaya and K. Kwiat, **"Secure Proactive Recovery – A Hardware Based Mission Assurance Scheme"**, *Journal of Network Forensics*, Vol. 3, Issue 2, 2011





Deception Framework – Prototype



Interested in meeting the PIs? Attach post-it note below!

NSF Secure and Trustworthy Cyberspace Inaugural Principal Investigator Meeting
Nov. 27 -29th 2012
National Harbor, MD

National Science Foundation
WHERE DISCOVERIES BEGIN