A Survey of Self-Protecting Computing Systems

Essien Ayanam
The Volgenau School of Engineering
George Mason University
Fairfax, Virginia, 22030, USA
Email: eayanam@gmu.edu

Outline

- Introduction
- Overview
- Classifications
- Critiques
- Related Work
- Conclusion

Introduction

- Autonomic Computing – implementing technology to install, configure, optimize, and manage technology
- Four key areas to autonomic computing – self-configuration, self-optimization, self-healing and self-protection
- These key areas are the foundation of autonomic computing

Introduction

Area	Summarization
Self-Configuration	An automated configuration of components and systems based on provided high-level policies. The rest of the system adjusts seamlessly and automatically.
Self-Optimization	A system continually seeks opportunities to improve its own performance and efficiency.
Self-Healing	A system automatically detects, diagnoses, and repairs localized software and hardware problems.
Self-Protection	A system automatically defends against malicious attacks or cascading failures. It uses early warning to anticipate and prevent system wide failures.

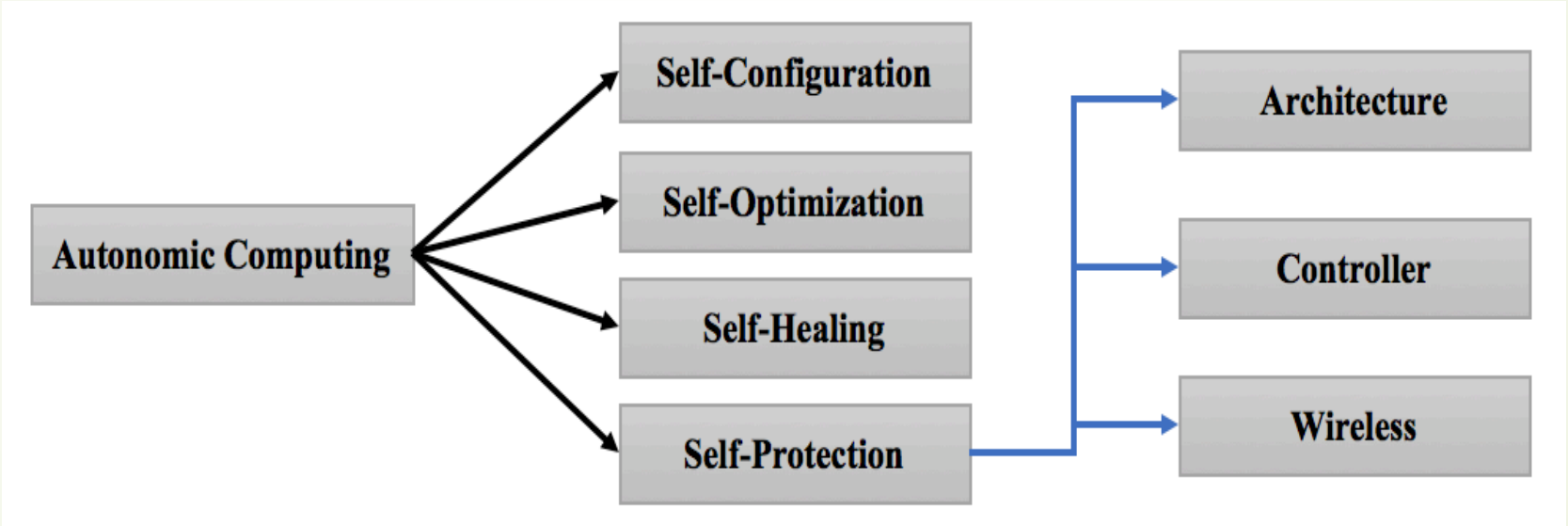
Introduction

- Self Protection/Self Protecting Systems
  - Reactive Security Mechanism: Detects an attack on occurrence and automatically mitigates the attack
  - Proactive Security Mechanism: Anticipate an attack based on current system configuration and learned security occurrences and takes steps to mitigate any potential issues
- Ultimate goal – autonomic security system to operate in a proactive manner

Overview

- Six approaches were surveyed
- Range of topics covering a diverse set of security mechanisms
- Based on their security properties and approach, the mechanisms can be classified as such:
  - Architecture
  - Controller
  - Wireless

Classification



Classification - Architecture

- Employ security mechanisms that protect the system as a whole
- Approach security in terms of a layered approach
- Effective in employing repeatable methods to allow for construction of dynamic software

Classification - Architecture

- E. Yuan, S. Malek, B. Schmerl, D. Garlan, and J. Gennari, "**Architecture-Based Self-Protecting Software Systems**," In Proceedings of the 9th International ACM Sigsoft Conference on Quality of Software Architectures, 2013, pp. 33-42.
- Proposed an architecture-based self protection (ABSP) approach
- Detection and mitigation of security threats are informed by an architectural representation of the software
- Employs architecture-level self protection patterns to solve well-know security threats

Classification - Architecture

- A. Wailly, M. Lacoste, and H. Debar, "**VESPA: Multi-Layered Self-Protection for Cloud Resources**," In Proceedings of the 9th International Conference on Autonomic Computing, 2012, pp. 155-160.
- Virtual Environments Self-Protecting Architecture (VESPA) – self protection for cloud based infrastructures
- Regulates protection of IaaS resources through coordinated security loops
- Enforce granular policies that address multi-layered defense

Classification - Controller

- Ensure optimal system performance while attempting to satisfy conflicting requirements – QoS and Security
- Controller optimizes a global utility function
- Solution employs combinatorial search techniques and queuing network models to dynamically search for a near-optimal security configuration

Classification - Controller

- F. Alomari and D. A. Menascé. "**An Autonomic Framework for Integrating Security and Quality of Service Support in Databases**," IEEE Sixth International Conference on Software Security and Reliability, 2012, pp. 51-60.
- F. B. Alomari, and D. A. Menascé, "**Self-Protecting and Self-Optimizing Database Systems: Implementation and Experimentation Evaluation**," In Proceedings of the 2013 ACM Cloud and Autonomic Computing Conference, no. 18, 2013.

Classification - Controller

- Implement autonomic system capabilities that can integrate both security and QoS requirements in database applications
- Dynamically changes security configurations according to certain workload characteristics
- Implement Intrusion Detection and Prevention System mechanisms to properly secure the system while meeting QoS requirements and maintaining optimal system performance
- Implement a controller in a TPC-W e-commerce – a transactional web commerce benchmark that emulates the operation of an online bookstore

Classification - Wireless

- Implements a general purpose wireless self-protection system that addresses the overall wireless architecture or implement a system that addresses a specific layer of the network
- Accounts for multiple differing technologies (WPAN, WLAN, WRAN, etc.)
- Provide a comprehensive security strategy for a diverse wireless infrastructure

Classification - Wireless

- S. Fayssal, Y. Al-Nashif, B. U. Kim, and S. Hariri, "**A Proactive Wireless Self-Protection System**," In Proceedings of the 5th International Conference on Pervasive Services, 2008, pp. 11-20.
- Self-protect against attacks by online monitoring and analyzing anomalies and misuses in the network features
- Overall WSPS architecture that provides a comprehensive security strategy for a diverse wireless infrastructure

Classification - Wireless

- H. Yang, X. Meng, and S. Lu, "**Self-Organized Network-Layer Security in Mobile Ad Hoc Networks**," In Proceedings of the 1st ACM workshop on Wireless Security, 2002, pp. 11-20. Accounts for multiple differing technologies (WPAN, WLAN, WRAN, etc.)
- Provides a solution to protect the network layer in a mobile ad hoc network
- Protects both routing and packet forwarding functionalities
- Exploits collaboration among local nodes to protect the network layer without completely trust any individual node

Critiques

- Architecture Type Self-Protecting Systems
  - Positives
    - Well written and organized
    - Excellent job in providing the challenges and addressing the challenges via the proposed architecture
  - Negatives
    - Exclusion of pertinent information due to space limitation
    - Expansion on experimental results

Critiques

- Controller Type Self-Protecting Systems
  - Positives
    - Well researched and comprehensive
    - Provided detailed information in identifying the components of the architecture
  - Suggestions
    - Use of actual IDPSs and DB data
    - Implement the controller in a SANs environment

Critiques

- Wireless Type Self-Protecting Systems
  - Positives
    - Innovative solutions
    - Excellent job in providing the challenges and addressing the challenges via the proposed architecture
  - Negatives
    - Poorly completed research study
    - Incomplete research study – missing experimental evaluation

Conclusion

- Comprehensive survey on a number of past and ongoing research efforts on self-protecting computing systems
- Proposal of a new classification for self-protecting systems
- Increased need for additional study in this area through future research
- Limitation – limited number of self-protecting approaches; advantageous to show an effective classification by increasing the scope of the surveys
- Future research – expand scope of self-protecting mechanisms; incorporating the components of from two of the proposed classification to create a new self-protecting mechanism (Architecture and Controller)