GEMOM – Genetic Message Oriented Secure Middleware

Significant and Measureable Progress beyond the State of the Art

Habtamu Abie, Ilesh Dattani, Milan Novkovic, John Bigham, Shaun Topham, and Reijo Savola

ICSNC 2008, October 26-31, 2008 - Sliema, Malta

Habtamu Abie – Norwegian Computing Center - NR
Presentation Outline

Best Existing systems Limitations

GEMOM Advances

GEMOM Architecture

Forward-looking Summary

Benchmarking
Best Existing MOM Systems

• MOMs
  – Increase the interoperability, portability, and flexibility of architectures
  – Typically asynchronous and peer-to-peer, but most implementation also support synchronous messaging
  – Reduce the number of point-to-point connections

• Best state of the art (SoA)
  – Existing commercial products
  – OpenSource products
  – Current research activities
Best SoA Limitations

• Scalable, resilient, and self-healing
  – hot standby brokers with instant switch-over and no data loss
  – no means to compensate for the reliability loss by automatically finding another source of redundancy
  – arbitrary resilience by a brute-force approach
  – self-healing is either rudimentary or non-existent
• Relatively prone to the incidence of feed failures
  – do not take redundant feeds into account
• Clustering topics into groups of one or more
  – but no group replication
• No holistic and systematic adaptive security, privacy and trust
  – No integration of threat and vulnerability management tool set and intelligent techniques to support vulnerability management assurance
GEMOM – Genetic Message Oriented Secure Middleware

- EU FP7 ICT project grant agreement: 215327
- Research and develop a messaging platform that is resilient, evolutionary, self-organizing, self-healing, scalable and secure
- Focus
  - reliability of message sourcing and delivery
  - scalability with respect to message volumes
  - replicating structural and dynamic properties of security metrics, policies, etc.
  - pre-emptive vulnerability testing and updating
GEMOM Advances

- Resilient and self-healing
- Vulnerability management assurance
- Interoperability and Integration of Distributed Systems
- Holistic and systematic adaptive security
  - Monitoring, management and maintenance incrementally
Resilience and Self-healing

- **Resilient**
  - ability to keep going in given scenarios – by learning, evolving, etc., over time

- **Self-healing**
  - ability of the system to preserve its capabilities even in the event of failure of any individual or multiple components

- **Handle redundant message feeds and redundant delivery paths**
  - Instant switch-over to redundant resource with no information loss
  - subsets or messaging segments redundancy
  - new redundant components (nodes, feeds or paths) when redundant components are switched to and used
Resilience and Self-healing...

- Resilience by security adaptation
  - security monitoring and changing the QoS available to applications
  - adaptive security, privacy and trust management
  - proactive detection of vulnerabilities and bugs
- Self-learning capabilities and optimisation approaches
  - using genetic and evolutionary techniques
- Scalability and resilience
  - cooperating brokers, publishers and subscribers with sufficient replication of paths and messages
  - not overload specific brokers
  - be able to sustain random and sudden fallout without interruption of service
Management Vulnerabilities

- Integration of detection
  - security vulnerabilities,
  - input errors,
  - misconfiguration error management
  - bug detection support

- Intelligent techniques
  - search and discovery of vulnerabilities, and other errors
  - detection of violations of QoS and privacy policy

- Threat and vulnerability management tool set
  - threat discovery
  - generic, intelligent, adaptive approaches to robustness and security testing
Management Vulnerabilities...

• Knowledge
  – the different kinds of vulnerabilities
  – the software function and aspects of the semantics of the application domain
  – protocols used

• New techniques to extend models assisted fuzzing by exploiting semantic models

• New approaches to learning for the creation of fuzzing procedures
  – inductive transfer where knowledge learned about some tasks is retained so as to efficiently learn a new task
Interoperability and Integration of Distributed Systems

• Publish/Subscribe variant of MOM (PS MOM)
  – efficient way to integrate distributed systems

• PS MOM’s key properties for efficient system modeling
  – system could be modeled and re-factored during run time
  – system inherently extensible
  – powerful base for implementation of scalability and resilience

• Better interoperability and integration of systems
  – subcontracting various functions to one or more separated, external or federated entities
  – hence the beauty of agent based system, resulting in resilient MOM
Adaptive Security

• Adaptive security
  – learns and adapts to changing environment at run-time in the face of changing threats

• Adaptive security involves
  – gathering contextual information both within the system and the environment
  – analyzing the collected information
  – responding to changes using the adaptation methods

• Adaptation form
  – parametrical via specific variations of the control parameters
  – structural by dynamic changes in the system structure
  – in combination
GEMOM Adaptive Security Architecture

- Client Pub/Sub
- Broker
- Adaptive Authentication / Identity Management
- Adaptive Authorization
- Adaptive QoS
- External identity provider
- Adaptive Analyzer
- Adaptive database
- Adaptive Collectors
  - Security monitoring
  - Security metrics
  - Vulnerability tools
  - Auditing service
GEMOM Adaptive Architecture

Biological and ecosystem metaphors

- A complex adaptive system
  - autonomic systems that mimic biological auto-immune systems
  - behavior of an ecosystem
- Biological and ecological systems maintain integrity
  - reacting to known changes
  - adapting to unknown changes, or
  - dying
- Adaptation
  - macroscopic ecosystem level (e.g. system or species). Managerial level in this case
  - Microscopic biological level (e.g., molecular, cellular). Operational level in this case
Benchmarking

- Perform qualitative and quantitative analysis of various pathways in terms of
  - volumes, resilience and vulnerabilities
- Maintain a variety of usage related information and generate views on that information
  - instruct agents to probe new pathways
  - re-factor the system so it evolves efficiently
  - “satisfy” user needs
- Develop a set of benchmarks
  - monitoring of progress, starting from the SoA and tracking progress as the boundaries are pushed forward
Summary

• Increased
  – resilience, scalability and support for vulnerability assurance

• Adaptive security
  – integrates various tool-sets for monitoring, measuring, pre-emptive vulnerability testing and updating
  – flexible authentication and fine grained authorization

• Reaping the benefits of agent-based message brokers
  – reliability via self-healing
  – performance via self-adaptation
  – security via self-protection (monitoring and vulnerability discovery)
GEMOM – Genetic Message Oriented Secure Middleware

Significant and Measureable Progress beyond the State of the Art

Habtamu Abie, Ilesh Dattani, Milan Novkovic, John Bigham, Shaun Topham, and Reijo Savola

ICSNC 2008,
October 26-31, 2008 - Sliema, Malta

Habtamu Abie – Norwegian Computing Center - NR