

Research Statement

Huiqun Yu

My research interest is focused on rigorous engineering methods for modeling, specification and design of computer systems, especially information security systems and high confidence reactive systems.

1. INFORMATION SECURITY

Security has emerged as a foremost concern for modern information enterprise. How to design highly dependable security systems that protect the systems and resources becomes an increasingly complex and difficult problem. My research goal is to develop a rigorous method for multidimensional security policy modeling and enforcement that supports system evolution, such as changes in security policies, user population, and their roles, and changes in applications.

Recent Research Work

Security Software Architecture Software architecture plays a central role in developing software systems that provide basic functionality and satisfy critical properties such as reliability and security. However, little has been done to integrate system design with security enforcement, which would otherwise benefit both development process and system's quality of service. We proposed a formal approach to integrating architectural functionality design with security administration and enforcement in [YHD04]. Guidelines are proposed to design functionality of software architectures at both element level and composition level. Software security is enforced by stepwise refinement.

Rule-based Security Enforcement Well-established techniques such as operating system protection mechanisms and cryptographic techniques cannot directly enforce security that has no precise definition. We proposed a systematic way to specify security policies, and a rule-based approach to enforcing security policies [YHS03]. A two-tier structure for architectural modeling was proposed. The upper level models the workflow of a distributed system. Each place at the upper level is a super-place that corresponds to a lower level Petri net. An initial distributed architecture can be directly derived from the upper level model. Security of the architecture is checked using the dependence relation of the model. Security policies are enforced by systematically reconstructing the initial architecture.

Future Research Plan

Time and Context-Aware Security Policy Modeling Most security models today deal with policies that are time and context independent. They are not sufficient to capture security requirements in current dynamic, distributed, highly connected and mobile environment. In this research, we will investigate a rigorous method for realization and assurance of time and context-aware access control policies. We aim to provide: (1) a formal model for structuring security policies covering time and context-aware concerns, (2) an aspect-oriented modeling approach for realizing security policy access controls, and (3) a variety of security policy formalization and verification techniques. Our initial vision is to use the role-based access control (RBAC) model as the start point to develop an incremental modeling method [GDY04].

Mediation Security for Heterogeneous Databases Companies and organizations are more and more required to become part of a distributed infrastructure and selectively share their data with other organizations. This trend enlarges the space of possible threats to local data sources. A mediator can provide an extended amalgamation of searching, querying and updating in heterogeneous systems so as to provide interoperation of heterogeneous systems, but may bring new security vulnerabilities. How to encourage data sharing while enforce required protection to local resources is a challenging problem. Traditional access control mechanisms and methods are inadequate to reflect the dynamic heterogeneous environment and the flexible access control requirements. In this research, we will develop: (1) a data security model that is capable of reflecting the flexibility of security requirements of heterogeneous databases, (2) a security enhancing method that is adaptive and scalable for mediation systems. Preliminary investigation in this direction has been presented in [YEY04].

2. HIGH CONFIDENCE REACTIVE SYSTEMS

Reactive systems are playing an increasingly vital role in the normal functioning of our society and are an indispensable part of our daily life. Today's reactive systems are ever increasingly complex, and usually time and safety-critical. My research aims to improve the state of the art of building high confidence reactive systems by developing a formal framework and a methodology for modeling, specifying, analyzing, and implementing such systems.

Recent Research Work

Software Architecture Modeling A software architecture is a high-level abstraction of a software system and is essential for achieving high confidence for system design. In the past five years, we developed a software architecture model called SAM at FIU. SAM is a general software architecture model based on a dual formalism combining Petri nets and temporal logic. We have applied SAM in modeling several systems including an e-commerce system [YHD02a], a multimedia system [YHS02], and a security system [YHS03]. We proposed hierarchically modeling method for components and connectors, as well as their interactions.

System Specification and Verification Typical functional behavioral properties such as safety and liveness properties are specified using temporal logic formulas, which define the constraints associated with individual components and connectors as well as compositions. We have used SAM in specifying a variety of functional behavioral properties such as deadlock and response. Furthermore, we have explored how to specify non-functional behavioral properties such as schedulability [YHD02b] and security [YHS03]. We have successfully applied automatic model checking techniques and tools (SMV from Carnegie Mellon University and STeP from Stanford University) to analyze functional properties of SAM architecture specifications [HYS04].

Future Research Plan

Incremental and Adaptive Design Methodology Today's reactive systems are increasingly complex in many aspects. These systems often need to adapt themselves to respond to changing operational environment and varying performance demands. In this research, we will investigate: (1) an incremental design method for reactive software systems such that they can adapt and reconfigure themselves in response to the changing operational environments and performance demands, (2) a compositional verification technique for ensuring various high-confidence properties such as safety, liveness, security, and fault tolerance in system design, and (3) a middleware-based implementation of software architectural design.

REFERENCES

- [GDY04] Shu Gao, Yi Deng, Huiqun Yu, Xudong He, K. Beznosov, and K. Cooper. Applying aspect-orientation in designing security systems. *Proc. of SEKE'04*, Banff, Canada, 2004. (Accepted)
- [HYT04] Xudong He, Huiqun Yu, Tianjun Shi, Junhua Ding, and Yi Deng. Formally specifying and analyzing software architectural specifications using SAM. *Journal of Systems and Software*, 71(1-2):11-29, 2004.
- [YHEY04] Li Yang, Raimund K. Ege, Huiqun Yu, and Yi Deng. Enhancing mediation security by aspect-oriented approach. *Proc. of SEKE'04*, Banff, Canada, 2004. (Accepted)
- [YHD02a] Huiqun Yu, Xudong He, Yi Deng, and Lian Mo. A formal method for analyzing software architecture models in SAM. *Proceedings of 26th Annual International Computer Software and Applications Conference (COMPSAC'02)*, Oxford, England, pages 645-652, 2002.
- [YHD02b] Huiqun Yu, Xudong He, Yi Deng, and Lian Mo. Formal analysis of real-time systems with SAM. *Proceedings of 4th International Conference on Formal Engineering Methods, LNCS 2495*, Shanghai, China, Springer-Verlag, pages 275-286, 2002.
- [YHD04] Huiqun Yu, Xudong He, Yi Deng, and Lian Mo. A formal approach to designing secure software architectures. *The 8th IEEE International Symposium on High Assurance Systems Engineering (HASE'04)*, Tampa, Florida, USA, 2004 (in press).
- [YHS02] Huiqun Yu, Xudong He, Shu Gao, and Yi Deng. Modeling and Analyzing SMIL Documents in SAM. *Proceedings of 4th IEEE International Symposium on Multimedia Software Engineering*, Newport Beach, California, USA, pages 132-139, 2002.
- [YHS03] Huiqun Yu, Xudong He, Shu Gao, and Yi Deng. Formal software architecture design of secure distributed systems. *Proceedings of 15th International Conference on Software Engineering and Knowledge Engineering (SEKE'03)*, San Francisco, California, USA, pages 450-457, 2003.