Information Security & Privacy in Distributed Systems

In this research avenue, we provide solutions for two types of common security problems in distributed information systems: i) security provisioning for document sharing among legacy and new distributed systems, and ii) tackling the challenging issue of insider attacks caused by trusted and authenticated users who can freely access to the system resources. For the first problem, we consider the system integration and document sharing among the Diagnostic Imaging Repositories (DI-r) and distributed PACS (Picture Archiving and Communication Systems) which is based on a "Trust Model", with key challenges such as: lack of federated capabilities to ensure unique user identity in legacy domains; and preserving consistency of access control rules across all systems. For the second problem we offer data analytics solutions based on data mining, clustering, and pattern matching approaches. A major research obstacle on this kind of problems is the lack of access to real-systems to allow developing effective and fine-tuned solutions. To remove this obstacle we have developed a user-behavior simulation environment, where the system administrators can define complex user-behavior patterns using a behavior pattern language. Then, an event-log engine generates a fully customizable event dataset for the purposes of: developing, testing, and fine-tuning our approaches to pattern-driven user-behavior analysis which serve the final goal of system security policy enhancement.

Abstracts of Selected Publications

User Behavior Pattern Discovery for Security Enhancement

Knowledge-driven User Behavior Pattern Discovery for System Security Enhancement

Weina Ma, Kamran Sartipi, and Duane Bender

(PDF)

Insider threads posed by authorized users have caused significant security and privacy risks to IT systems. The behavior of authorized users in using system services must be monitored and controlled. However, the administrators in large distributed systems are overwhelmed by the number of system users, the complexity and changing nature of user activities. This paper presents a new generation of intelligent decision support system that effectively assists system administrators to get deep insight into the system user's dynamic behavior patterns. With these patterns, the system administrators are capable of constructing dynamic refinement to the existing security policies. We explore the method of interactively and incrementally extracting user's behavior patterns by combining data mining techniques with domain and system knowledge, and applying such knowledge to provide recommendations throughout the whole process. A prototype tool has been developed to analyze the audit logs from distributed medical imaging systems to validate the proposed approach.

Synthesizing Scenario-based Dataset for User Behavior Pattern Mining

International Journal of Computer and Information Technology (ISSN: 2279 – 0764) Volume 04 – Issue 06, November 2015

Weina Ma, Kamran Sartipi, and Duane Bender

(PDF)

User behavior pattern mining has drawn great attention in business and security areas. Realistic and accurate datasets are required for evaluating various user behavior pattern mining approaches, their implementations and optimization results. Synthetic datasets are crucial due to restricted access to production datasets, security and privacy issues, meeting specific needs of consumers, or the high costs of real datasets. This paper presents a synthetic dataset generator that effectively assists data scientists and analysts in designing scenario-driven datasets with embedded user behavior patterns, and visually analyzing the quality of the generated datasets. We developed an interactive data exploration environment to such a design-generate-visualize-analyze-optimize process. An abstract representation of the real-world user behavior pattern is proposed, which allows data analysts to create datasets with both intended and random patterns injected. Dataset generation is controlled by both data statistics (e.g., data size, and attribute distribution) and scenario-based user behavior patterns (e.g., association pattern, sequential pattern and time constraint). A prototype toolkit has been developed to synthesize and analyze the datasets in different application domains.

An Expressive Event-based Language for Representing User Behavior Patterns

Hassan Sharghi Kamran Sartipi

(PDF)

In-depth analysis of user interactions with applications in large systems is widely adopted as a means to understand user's behavior for strategic purposes such as fraud detection, system security, weblog analysis, social networking, and customer relationship management. Overall, the user behavior presents characteristics, relationships, structures, and effects of a sequence of actions in a specific application domain. Formal modelling and representation of complex patterns of user actions using expressive languages are critical aspects of behavior analysis. We present a model to describe the behavior elements and their relationships. The model also provides a systematic mechanism for describing and presenting events, sequence of events, and complex behavior patterns. A behavior pattern can be defined as a sequence of typed events that occur during specific time intervals, An event consists of a tuple of attributes whose values represent an observation of the behavior. In this paper, first we present a semantic model of the user behavior to address the issues around the user behavior representation, and then we define a generic Behavior Pattern Language (BPL), which enables the analysts to define a variety of complex behavior patterns in a declarative manner. We present the feasibility of the approach through several examples of complex behavior patterns expressed using the proposed language

Behavior-Based Access Control for Distributed Healthcare Systems

Journal of Computer Security, Volume 21, No 1, pages 1-39, 2013

Mohammad H. Yarmand, Kamran Sartipi and Douglas G. Down

(PDF)

Sensitivity of clinical data and strict rules regarding data sharing have caused privacy and security to be critical requirements for using patient profiles in distributed healthcare systems. The amalgamation of new information technology with traditional healthcare workflows for sharing patient profiles has made the whole system vulnerable to privacy and security breaches. Standardization organizations are developing specifications to satisfy the required privacy and security requirements. In this paper we present a novel access control model compliant with healthcare standards based on a framework designed for data and service interoperability in the healthcare domain. The proposed model for customizable access control captures the dynamic behavior of the user and determines access rights accordingly. The model is generic and flexible in the sense that an access control engine dynamically receives security effective parameters from the subject user, and identifies the privilege level in accessing data using different specialized components within the engine. Standard data representation formats and ontologies are used to make the model compatible with different health- care systems. The access control engine employs an approach to follow the user's behavior and navigates among engine components to provide the user's privilege to access a resource. A simulation environment is implemented to evaluate and test the proposed model.

=.=

Intelligent Middleware Security Provisioning

Security Middleware Infrastructure for Medical Imaging System Integration and Monitoring

Weina Ma, Kamran Sartipi

(PDF)

With the increasing demand for electronic medical records sharing, it is a challenge for medical imaging service providers to protect the patient privacy and IT infrastructure security in an integrated environment. In this paper, we present a novel security middleware infrastructure for seamlessly and securely linking legacy medical imaging systems, diagnostic imaging web applications as well as mobile applications. In this infrastructure, software agents such as user agent and security agent have been integrated into medical imaging domains that can be trained to perform their tasks. The proposed security middleware utilizes both online security technologies such as authentication, authorization and accounting, as well as post security operations to discover system security vulnerability. By integrating with the proposed security middleware, both legacy system users and Internet users can be uniformly identified and authenticated; access to patient diagnostic images can be controlled based on patient's consent directives and other access control polices defined at a central point; relevant user access activities can be audited at a central repository; user access behavior patterns are studied by utilizing data mining techniques; the explored behavior patterns provide system administrators valuable knowledge to refine existing security policies; behavior-based access control is enforced by capturing user's dynamic behavior and determining their access rights through comparing with the discovered knowledge of common behaviors. A case study is presented based on the proposed infrastructure.

Cloud-based Identity and Access Control for Diagnostic Imaging Systems

Weina Ma, Kamran Sartipi

(PDF)

The evolution of cloud computing is driving the next generation of diagnostic imaging (DI) systems. Migrating DI systems to cloud platform is cost-effective and improves the quality of DI services. However, a major challenge is managing the identity of various participants (users, devices, applications) and ensuring that all service providers offer equivalent access control in cloud ecosystem. In this paper, we propose an access control infrastructure for secure diagnostic image sharing among Diagnostic Imaging Repositories and heterogeneous PACS (Picture Archiving and Communication Systems) in cloud. We utilize an open standard “OpenID Connect” to provide user-centric Single Sign-On solution, and present the extensions for integrating with patient consent directives and system access control policies. Through combining with the dominant access control model XACML in existing DI systems, the extended OpenID Connect authorization server can provide fine-grained access control.

OpenID Connect as a Security Service in Cloud-based Diagnostic Imaging Systems

Weina Ma, Kamran Sartipi, Hassan Sharghi, David Koff, Peter Bak

(PDF)

The evolution of cloud computing is driving the next generation of diagnostic imaging (DI) systems. Cloud-based DI systems are able to deliver better services to patients without constraining to their own physical facilities. However, privacy and security concerns have been consistently regarded as the major obstacle for adoption of cloud computing by healthcare domains. Furthermore, traditional computing models and interfaces employed by DI systems are not ready for accessing diagnostic images through mobile devices. RESTful is an ideal technology for provisioning both mobile services and cloud computing. OpenID Connect, combining OpenID and OAuth together, is an emerging REST-based federated identity solution. It is one of the most perspective open standards to potentially become the de-facto standard for securing cloud computing and mobile applications, which has ever been regarded as “Kerberos of Cloud”. We introduce OpenID Connect as an identity and authentication service in cloud-based DI systems and propose enhancements that allow for incorporating this technology within distributed enterprise environment. The objective of this study is to offer solutions for secure radiology image sharing among DI-r (Diagnostic Imaging Repository) and heterogeneous PACS (Picture Archiving and Communication Systems) as well as mobile clients in the cloud ecosystem. Through using OpenID Connect as an open-source identity and authentication service, deploying DI-r and PACS to private or community clouds should obtain equivalent security level to traditional computing model.

An Agent-based Infrastructure for Secure Medical Imaging System Integration

Weina Ma and Kamran Sartipi

(PDF)

This research paper examines the weaknesses of the trusted models applied on the domain of medical image sharing between the PACS (Picturing Archiving and Communication System) and image-enabled EHR (Electronic Health Record) systems. In this paper, we propose implementing an agent-based infrastructure in the legacy PACS systems along a common infrastructure that we have pro- posed in our earlier work. The proposed architecture allows for capturing PACS communication messages; identifying users; extracting user actions to feed into an action-based access control mechanism; and integrating with modern authentication and authorization technologies (OpenID and OAuth). We also provide a UML model for the patient con- sent directives to allow for systematic enforcement of their impact on the proposed access control technique. Finally, we implemented a prototype of the proposed architecture using open source tools to demonstrate the feasibility and extendibility of our proposed solution.

An Infrastructure for Secure Sharing of Medical Images between PACS and EHR Systems

Kamran Sartipi, Krupa A. Kuriakose, and Weina Ma

(PDF)

New advances in information and communication technologies (ICT) and their incorporation into the medical domain have created opportunities to enhance medical services and provide improvement to workflow at a low cost. However, to implement such services, the current medical system needs to be integrated, secured, and available to health professionals and patients. In this paper, we propose an infrastructure that suggests the use of techniques and standards such as: cooperative multi-agents, standards for user authentication and service authorization, as well as protocols for cross-enterprise document sharing. The proposed infrastructure allows for integration of a PACS (Picture Archiving and Communication system) with a widely accepted HL7 (Health Level Seven) standard infrastructure for provisioning nation-wide electronic health records (EHR). In this approach, the cooperative agents provide: i) an action-based access control mechanism to share medical images that allow safe integration of a PACS and the Diagnostic Image Repository (DI-r) systems within a standard EHR system; and ii) a behavior-pattern based security polity enhancement to assist the system administrator. Such secure and interoperable medical imaging systems are easy to expand and maintain.