SecTag: A Multi-Policy Supported Secure Web Tag Framework
Ruixuan Li, Meng Dong, Bin Liu, Jianfeng Lu, Xiaopu Ma, Kai Li
School of Computer Science and Technology
Huazhong University of Science and Technology
Wuhan, Hubei 430074, China
rxli@hust.edu.cn, {mengdong, bliu9, lujianfeng, xpma}@smail.hust.edu.cn, likai@hust.edu.cn

INTRODUCTION
Web-based enterprise-level applications have gained a tremendous growth in the last decade. Traditional access control module development in web systems often suffers problems, such as lack of fine-grained and multi-policy support, tight coupling of the access control logic with the business logic. It is hard to reconfigure or modify the access control policies after the system has been deployed. Hence, it is ultimately important to provide a development framework considering the features of multi-policy authorization, component reusability, multi-views and high interaction support. As shown in Figure 1, web services are different according to access permissions. The structure of policy configuration is shown in Figure 4. Each policy can set attribute “mode” and “access”, and contains at least one specific rule. “rule” is used to describe the specific access control information, and its attribute “access” specifies the access permission to the rule. We can inject a structured query language (SQL) statement or a method of a class in secconfig.xml when “type” is defined as “SQL” or “Method”. In these cases, Policy Analysis Subsystem (PAS) will automatically load the dynamic data to complete the policy analysis.

DESIGN
FRAMEWORK
Our goal is to design and implement a light-weight basic framework of SecTag, which can be easily satisfied with the traditional model-view-controller (MVC) mode. By using SecTag, fine-grained access control policies can be easily configured through the visual interface without any modification of codes. Most of the general access control logics can be encapsulated in the form of secure tags. Thus, the development and maintenance workload are greatly reduced. Figure 2 shows the architecture of SecTag framework.

POLICY CONFIGURATION
Based on actual secure applications, tag rendering that responds to user’s requests can be divided into three states: normal, view-only and unavailable, taking submit tag as an example shown in Figure 3.
• Tags of user interface (UI) display: mainly includes the visibility and availability of control.
• Tags of data access control: mainly includes the dynamic rendering of the data list.

EXAMPLE
Taking the tag select that receives data as an example, we bind attribute "policy" of select to policy p that is configured in sec-config.xml shown in Figure 6, and describe the user identity in the form of (username, role, level).

CONTRIBUTIONS
We develop a reusable secure development framework SecTag to solve the problem of tight coupling between access control and business logic. It assists developers to achieve fine-grained and multi-policy authorization management for web resource protection.

FOR FURTHER INFORMATION
Please contact rxli@hust.edu.cn or visit http://idc.hust.edu.cn. Source code can be downloaded from http://code.google.com/p/sectag/.