OpenPMF™ Model-Driven Security Policy Automation

Problem
Unmanageable Security Policies
Manually translating security policy & compliance requirements into effective technical implementation is difficult, expensive, and error-prone - esp. for interconnected, agile applications (e.g. SOA & cloud). Where does the policy come from? Who can write the matching technical policy rules? Who can maintain them despite dynamic changes? Who can verify policy correctness & compliance?

Solution
OpenPMF™ Model-Driven Security (MDS)
OpenPMF™ makes application security manageable through MDS automation. MDS automates the process of turning human-understandable security & compliance requirements (e.g. for attribute-based access control, ABAC, and monitoring) into the matching numerous and ever-changing technical security policy rules (whitelists) and configurations. MDS also distributes and proactively enforces those rules at the application layer, and also continuously monitors security. Unlike traditional manual authoring of rules, MDS automates technical policy generation and update from intuitive business security requirements models - including least privilege and workflow policies, which can protect against insider attacks. MDS helps automate policy management even for agile SOAs and cloud platforms. MDS forms a critical part of any authorization management, entitlement management and identity & access management (IAM) strategy. MDS also enables a secure application development lifecycle at development time right from the beginning – dealing with policy abstraction, externalization, authoring, automation, enforcement, audit monitoring/reporting, and verification.

1 Configure
intuitive business security requirements policies
Security professionals can configure or select generic application security requirements in a model-driven security tool, including access and monitoring policies. No need to be an application specialist.

2 Generate
matching technical security policies automatically
Application developers can implement application specific technical application security policy rules at the click of a button. Model-driven security automatically analyzes your software as it is being written or updated, and generates the matching fine-grained access and monitoring policies. No need to be a security specialist.

3 Enforce
technical security policies automatically
At runtime, local authorization management policy decision points and policy enforcement points (PDPs/PEPs) undermine all applications automatically intercept and check all information flows before they are forwarded to the application.

4 Monitor
technical security policies automatically
At runtime, policy monitoring points automatically collect information about security incidents for monitoring and auditing purposes. The collected information can be configured through generic monitoring policy models.

5 Update
technical security policies automatically
Model-driven security uniquely updates technical security policies automatically when systems are reconfigured (e.g. SOA). No need to manually update technical security policies. This unique feature makes policy management and implementation manageable for today’s rapidly evolving interconnected applications (e.g. agile SOA w. BPM and clouds).

6 Verify
compliance/accreditation automatically
This MDS feature automatically produces supporting evidence that the enforced security rules match with accreditation/compliance policy models and security policy models. It helps shorten accreditation/re-accreditation time and reduce cost (esp. for agile IT landscapes such as SOAs).

References objectsecurity.com/publist

“Model-driven security is the tool supported process of modeling security requirements at a high level of abstraction, and using other information sources available about the system (produced by other stakeholders). These inputs, which are expressed in Domain Specific Languages (DSL), are then transformed into enforceable security rules with as little human intervention as possible. It also includes the run-time security management (e.g. entitlements/authorizations), i.e. run-time enforcement of the policy on the protected IT systems, dynamic policy updates and the monitoring of policy violations.”
- Wikipedia