



Model Driven Accreditation of Agile Systems

Rudolf Schreiner, Ulrich Lang

International Common Criteria Conference 2010
Antalya



info@objectsecurity.com
www.objectsecurity.com

Agenda

- New challenges in accreditation: Agile systems
- Proposed approach: Model driven integration of development, protection & accreditation
- Evaluation

ObjectSecurity

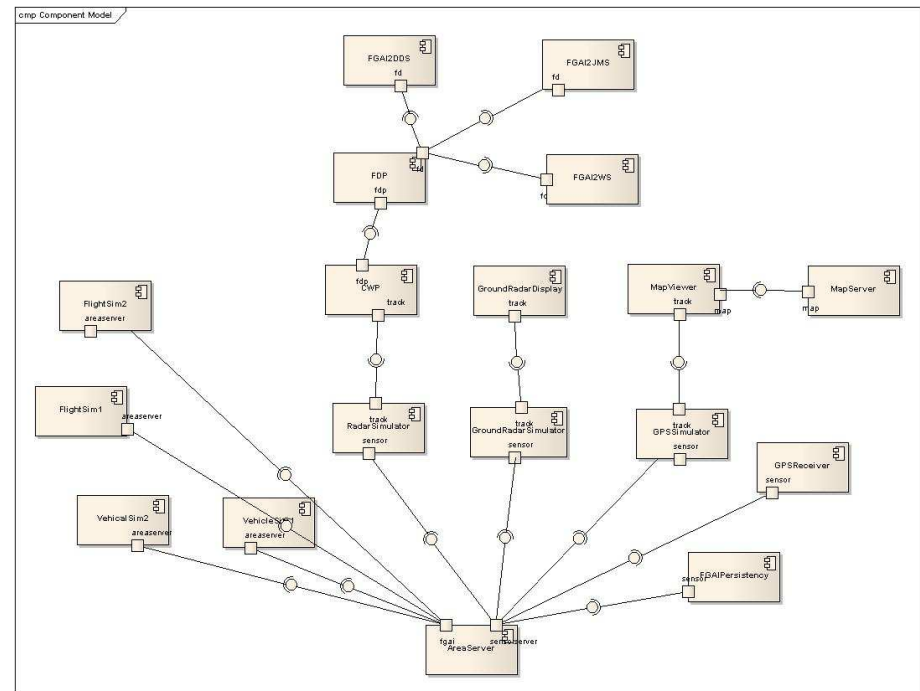
- Founded 2000 as University of Cambridge Computer Lab spinout
- US subsidiary in Palo Alto
- Focus: Development/security/compliance of complex systems
- Customers include US Navy, UK MOD, Intel, Lufthansa Systems,...

Complex Systems: Paradigm Shift

- In the past: Monolithic and static systems from a single vendor
- Development often based on “paper” documentation
- Distinct life cycle phases
 - Requirements
 - Design & Implementation
 - Accreditation
 - Deployment
 - Operation

Agile Systems

- Service oriented, component based, distributed applications meeting specific requirements of users
- Very often Model Driven Development used
- Multiple vendors, multiple stakeholders
- Blurred life cycle phases
 - System under permanent evolution



Our Challenge

Building and running of secure, agile systems over whole systems life cycle

- How do we define *appropriate* security (protection and accreditation) requirements?
- How do we enforce the protection requirements
- How do we ensure that accreditation requirements are met?
- How do we assess residual risks?
- How do we detect policy violations?

Specific Accreditation Issues

- Agility: No fixed life cycle phases
 - No accreditation of a stable, fixed system possible
- No fixed systems
 - Composition of system from components/services
 - Separation of concern
- Multiple stakeholders

Additional CC Issues

- Currently, CC accreditation is
 - mostly done by human evaluators
 - based on documents in human language provided by human developers
 - Results also documents in human language
- Very high effort
 - Costs
 - Time to market
 - Potential of human errors
- Manual accreditation does not work for agile systems

Solution: Automation

Automatic evaluation and documentation generation over whole life cycle

- Automated analysis and testing according to accreditation requirements
 - System and accreditation documentation always consistent
- Assessment of residual risks
- But also: Runtime security monitoring and policy violation detection

Enabler: Integration of Security

- Full Integration of security (protection and accreditation) into system life cycle
 - Processes
 - Information
- Key requirements:
 - Uniform and machine readable representation of information
 - Reuse of information
 - Automated processing of information

Model Driven Development

- Building of models of functional properties of a system
- Then (fully or partially) generating the functional products from the models
- Integration of security: Model Driven Security
 - Model Driven Protection (MDP)
 - Model Driven Security Accreditation (MDSA)
 - Model Driven Risk Assessment (MDRA)
 - Model Driven Security Monitoring (MDSM)

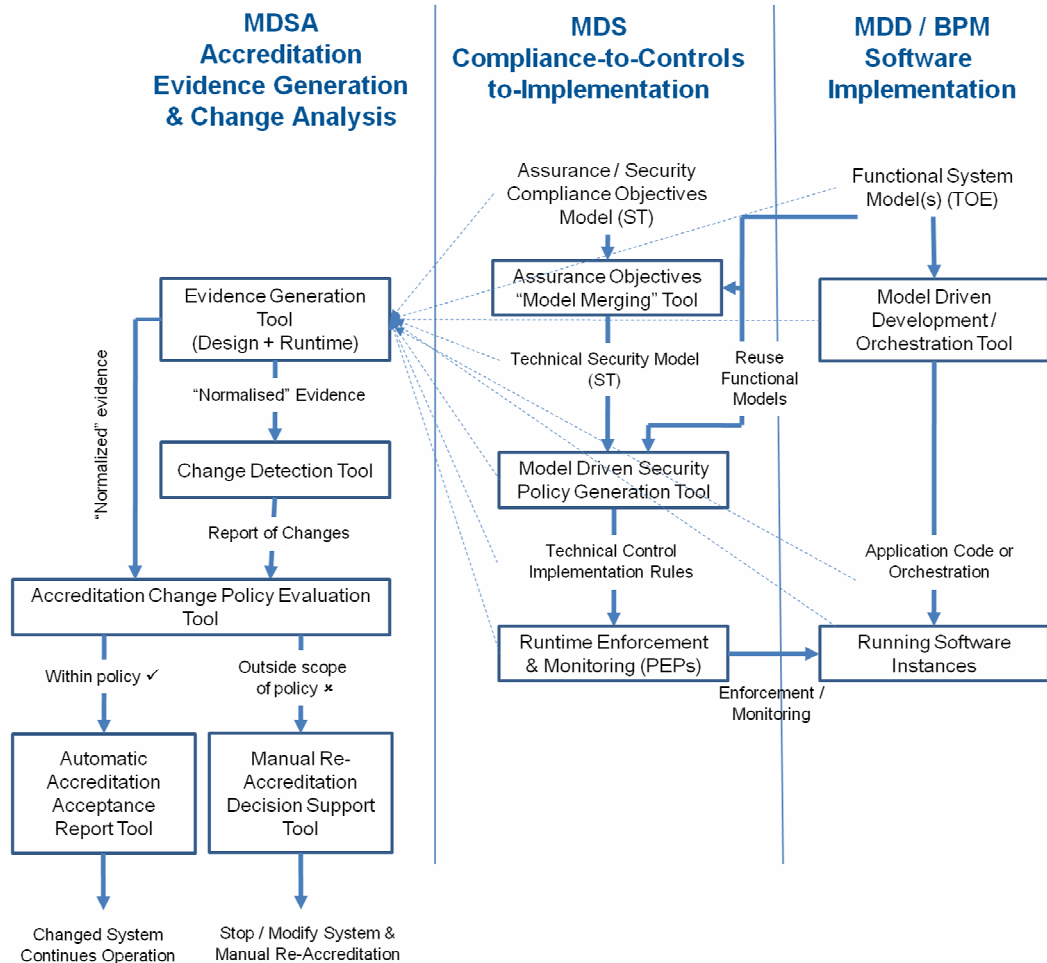
Security Modeling

- Definition of Domain Specific Languages for security aspects, e.g.:
 - Requirements: Security & compliance, accreditation
 - Protection mechanisms, vulnerabilities, risks
- Using the DSLs, security information for concrete system is expressed
- Using model transformations, security products are generated:
 - Protection (access control rules, configuration)
 - Accreditation evidence and documentation
 - Risk assessment
 - Analysis of changes (Human involvement necessary?)

Testing/Human Evaluators

- Model analysis is very powerful, but cannot cover everything
- MDSA is able to integrate information from:
 - Testing
 - Generation of test patterns
 - Automatic execution of tests
 - Import of results
 - Human Evaluators
 - Providing additional information in form of models

MDS Overview



Practical Evaluation

- Test system: System Wide Information Management
 - Heterogeneous distributed application
 - Middleware platform with separation of concern
- Manual enforcement of an appropriate, business driven security policy was impossible
 - Complexity too high

MDS Evaluation Results

- Integrated MDS worked as expected:
 - Correct enforcement of defined security policy and accreditation evidence/documentation generation over all modifications of system **within seconds**
 - Proactive monitoring of system behavior for detection of policy violations
- Quick adaptation to new security requirements
- Initially considerable effort
 - Detailed protection/risk models, esp. for middleware platform and security libraries
 - Mostly independent of application, can be reused
- Great reduction of effort over whole life cycle

Issues

- Conflict with current practice
 - What do organizations need?
 - A clear picture of the state of security at all points in time?
 - Or just a piece of paper that their system met a set of requirements at one point in time?
 - What about independent 3rd parties for accreditation?
 - Human evaluators?
- More focus on security by design than testing/evaluation?

Conclusion

- Model Driven Security greatly improves the integrated and unified protection, risk assessment and accreditation of complex, agile systems
 - Better protection
 - Higher assurance and trust
 - Much reduced effort and costs
- The main issue: Not in line with current accreditation practice



www.objectsecurity.com

info@objectsecurity.com



ObjectSecurity Ltd.
St John's Innovation Centre
Cowley Road
Cambridge CB4 0WS
United Kingdom



ObjectSecurity LLC
Plug & Play Tech Center
530 University Ave (mailbox #202)
Palo Alto, CA 94301
USA



Tel: +44 (0) 1223 420252
Fax: +44 (0) 1223 420844



Tel: 1-650-515-3391
Fax: 1-360-933-9591



www.objectsecurity.com
info@objectsecurity.com



www.objectsecurity.com
info@objectsecurity.com



info@objectsecurity.com
www.objectsecurity.com