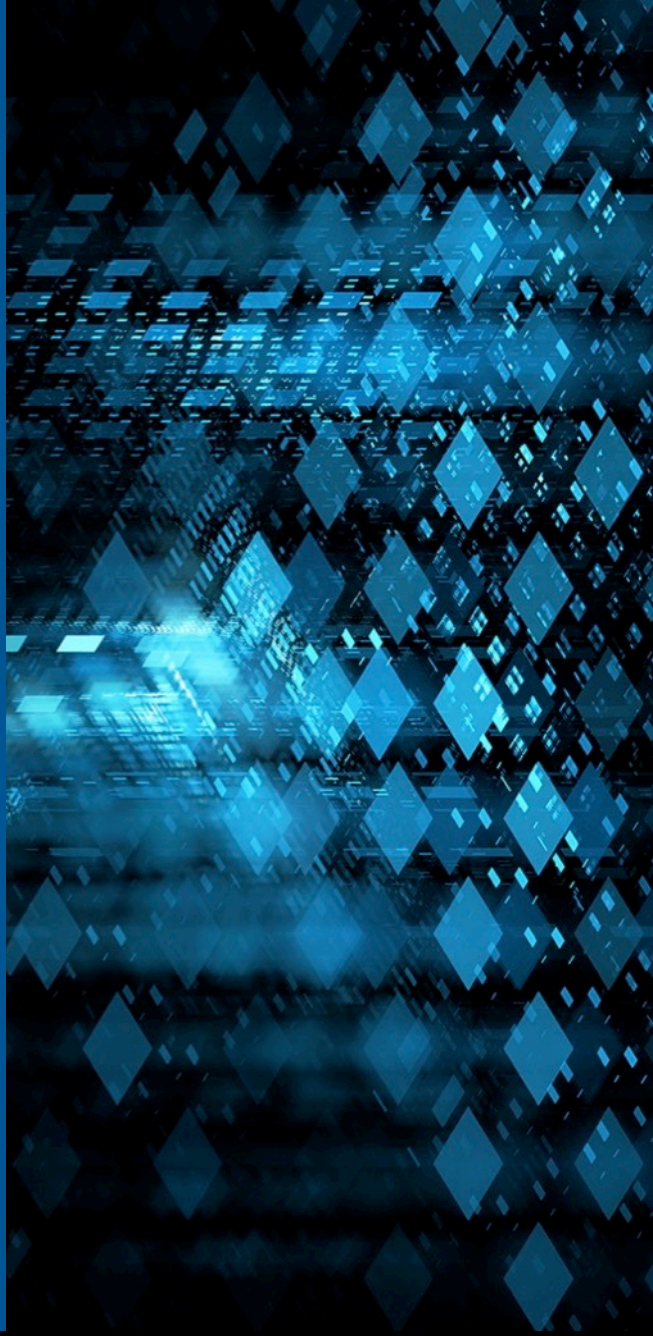
AADL Security Annex Discussion Topics

Dave Gluch

dpg@sei.cmu.edu

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213



This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM17-0305

Security Annex Capabilities - Summary

Security Requirements and Policies - capture security requirements, security policies and verify that security policies satisfy security requirements, and security policies are enforced within the system implementation

Access Control & Protection
model, assess, and assure security access control

Information/Data Protection
model, assess, and assure data protection approaches

Action/Command Protection
model, assess, and assure access control of execution of actions/commands

Threat/Attack Modeling
capture and analyze security threat/attack models

Vulnerability Modeling
identify, model, and analyze security vulnerabilities (may be integrated with threat/attack modeling)

Security Architectures (Modeling)
model and analyze security architectures

Security Requirements and Policies

Capability to capture security requirements, security policies and verify that security policies satisfy security requirements, and ensure there are mechanisms that enforce security policies within a system implementation; does not assure the effectiveness, self-consistency, or validity of those policies

- **verification of security policies** - validate a model against a specific security policy
- **generation of security assurance** - generate security assurance documents from the models
- **implementation of security policies** - generate the system security configuration from AADL models (e.g. code generator of security-related code)

Access Control & Protection

Capability to model, assess, and assure security access control including

- Authentication (single and multiple factor)
- Authorization
- Access permissions
- Access management (who, what permissions)
- Non-repudiation
- Isolation
- Specialized models (e.g. Bell-LaPadula, Biba)
- Intrusion detection and recovery
- Security Classifications – capability to model, assess, and assure security classification management and implementation including
  - personnel
  - information

Information/Data Protection

Capability to model, assess, and assure data protection approaches and levels

- Security Classifications – capability to model, assess, and assure security classification management and implementation including
  - personnel
  - information
- Cryptography & Encryption – capability to model, assess, and assure security encryption and supporting cryptographic methods and implementations, including diverse encryption schemes (e.g. D-H, AES, RSA, etc.), key management, etc.
- Protected Containment – capability to model, assess, and assure protected containment units such as protected address spaces, virtual machines, and partitions

Action/Command Protection

Capability to model, assess, and assure access control of execution of actions/commands including

- Security kernels (e.g. seL4)
- Operating system security controls
- Specialized operating systems

Threat/Attack Modeling

Capability to capture and analyze security threat/attack models including:

- Threat models (e.g. STRIDE)
- Attack/attacker models
- Attack surface models
- Attack trees
- Chain of events models
- FTA/FMEA
- Attack patterns
- Denial of Service

Vulnerability Modeling

Capability to identify, model, and analyze security vulnerabilities - may be closely integrated with Threat/Attack Modeling

- Architecture/code defects
- Malicious code
- Misuse/improper use

Security Architectures (Modeling)

Capability to model, and analyze security architectures such as

- Multiple Independent Levels of Security (MILS, D-MILS)
- Secure kernels (e.g. seL4, MILS separation kernels)

Security Terminology

vulnerability (security hazard)	A vulnerability (security hazard) is a system state or set of conditions (including security procedures, internal controls, design, or implementation) that could be exploited by an attacker.
threat (security)	A threat is a specified vulnerability plus the specification of an attacker, attacker access, and attacker capability to exploit the vulnerability (i.e. a *security hazard* with specified worst-case conditions).
attack	An attack is an unauthorized attempt to access a system, usually with malicious intent, to exploit one or more vulnerabilities.
attacker	An attacker is an entity (or a coordinated set of entities) that engages in or attempts to engage in an attack.

A distinction is made between the system and its environment.

Safety Terminology

loss	A loss is a condition that results from events such as accidents [Leveson 2012] or the realizations of hazards [Feiler 2016] or threats [NIST 2016].
accident	An accident is an undesired or unplanned event that results in a loss, including loss of human life or human injury, property damage, environmental pollution, mission loss, etc. [Leveson 2012].
hazard	A hazard is a system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to an accident (loss)" [Leveson 2012].
hazard contributor	A hazard contributor is a state or set of conditions of a subsystem or component that is part of or adds to a hazard.