A Survey
# of Approaches to
Adaptive Application Security

George Mason University
Department of Computer Science

Ahmed Elkhodary & Jon Whittle

*work supported by FAA

Vision

Develop a methodology for designing security-aware adaptive systems (SECADAs), i.e., systems that adapt in response to an attack

1. Model potential threats to a system
2. Map those threats to features that are targeted by attacks
3. Detect intrusions at run time
4. Swap out features at run time to respond to intrusions

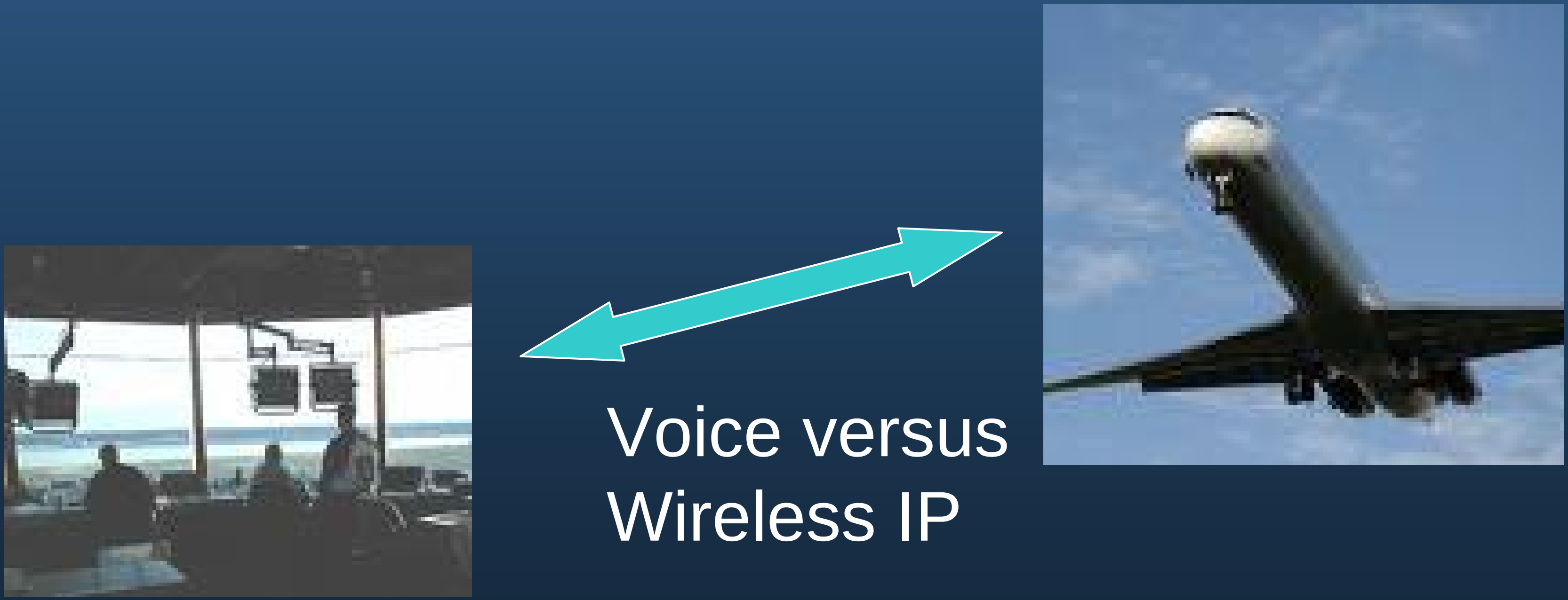
Goal of This Talk

- Survey existing approaches to adaptive (application) security
- Adaptive (application) security = run time modification of security policies and mechanisms
- Four approaches surveyed:
  - Extensible Security Infrastructure
  - Strata Security API
  - Willow Architecture
  - Adaptive Trust Negotiation and Access Control
- Classified each approach along a number of dimensions

  → Not yet any methodology for SECADA design

Motivation

- Why Adaptive Application Security?
  - Increasing rate and complexity of cyber attacks.
  - Security measures need to be strengthened, BUT
    - Additional security measures imply processing overhead
    - AND there may be a trade-off between functionality and security



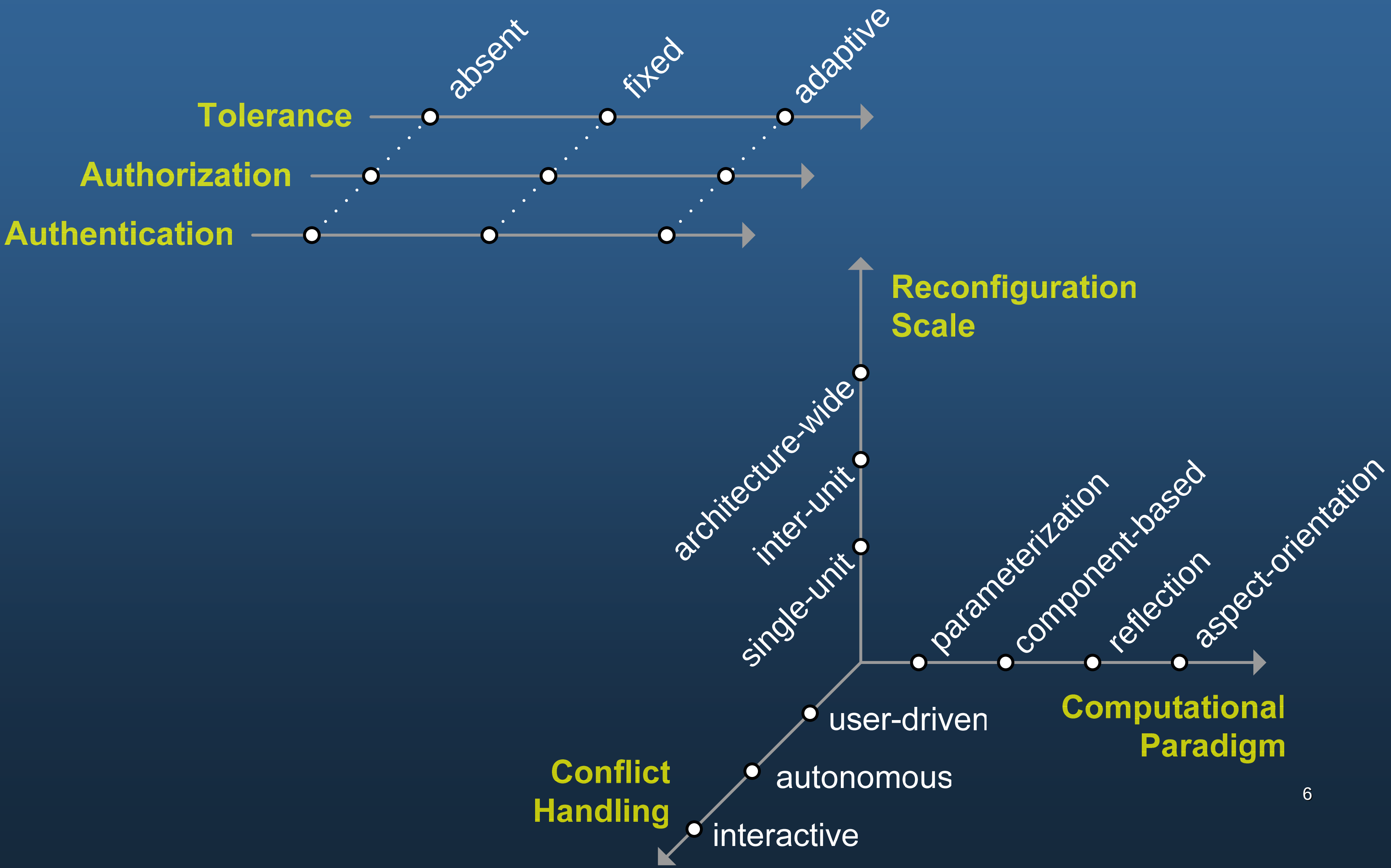
Voice versus Wireless IP

Classification Scheme

- Extend McKinley et al's classification scheme
  - 3 dimensions:
    - **Computation paradigm**
      - How is adaptation designed? (parameterization, component-based, etc.)
    - Adaptation layer
      - Where is adaptation happening? (hardware, network, middleware, application-level, etc.)
    - Adaptation time
      - When is adaptation happening? (configuration time, run time, etc.)
  - This scheme does not focus on security
    - Extend this scheme to include security-relevant dimensions
    - Also extended with other adaptation-relevant dimensions

- Additional dimensions
  - **Conflict handling**
    - If adaptation introduces inconsistent behavior, is it detected, and, if so, how?
  - **Reconfiguration Scale**
    - What level of adaptation granularity (component-level, architecture-wide)?
  - **3 Security Dimensions**
    - Level of adaptive authentication (none, fixed, adaptive)
    - Level of adaptive authorization
    - Level of intrusion tolerance

Classification Scheme



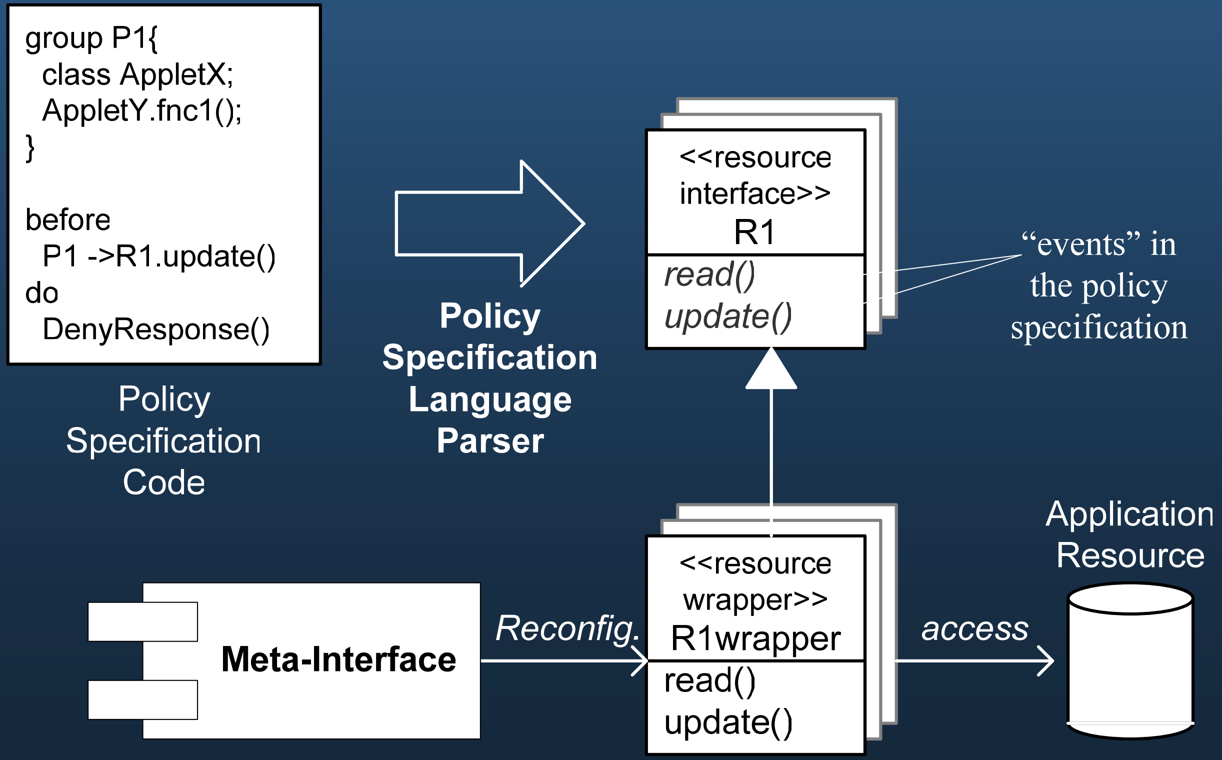
Existing Approaches

- Extensible Security Infrastructure
- Strata Security API
- Willow Architecture
- Adaptive Trust Negotiation and Access Control

Extensible Security Infrastructure

(B. Hashii, S. Malabarba, R. Pandey, M. Bishop)

- Policy Language parser generates policy objects
- Resource wrappers implement policy objects
- Privileged programs use Meta-Interface to change policy objects at runtime



```
group P1{
  class AppletX;
  AppletY.fnc1();
}

before
  P1 ->R1.update()
do
  DenyResponse()
```

Policy Specification Code

Policy Specification Language Parser

<<resource interface>>
R1
read()
update()

"events" in the policy specification

<<resource wrapper>>
R1wrapper
read()
update()

Meta-Interface

Reconfig.

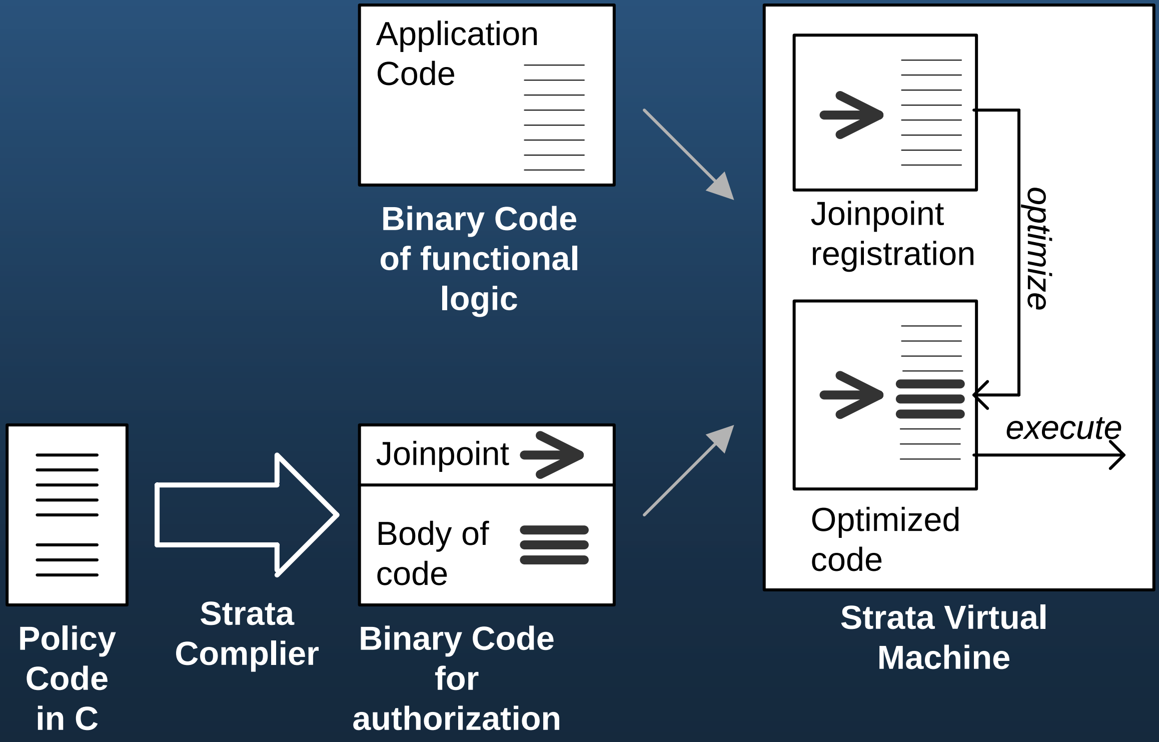
access

Application Resource

Strata Security API

(Kevin Scott, Jack W. Davidson)

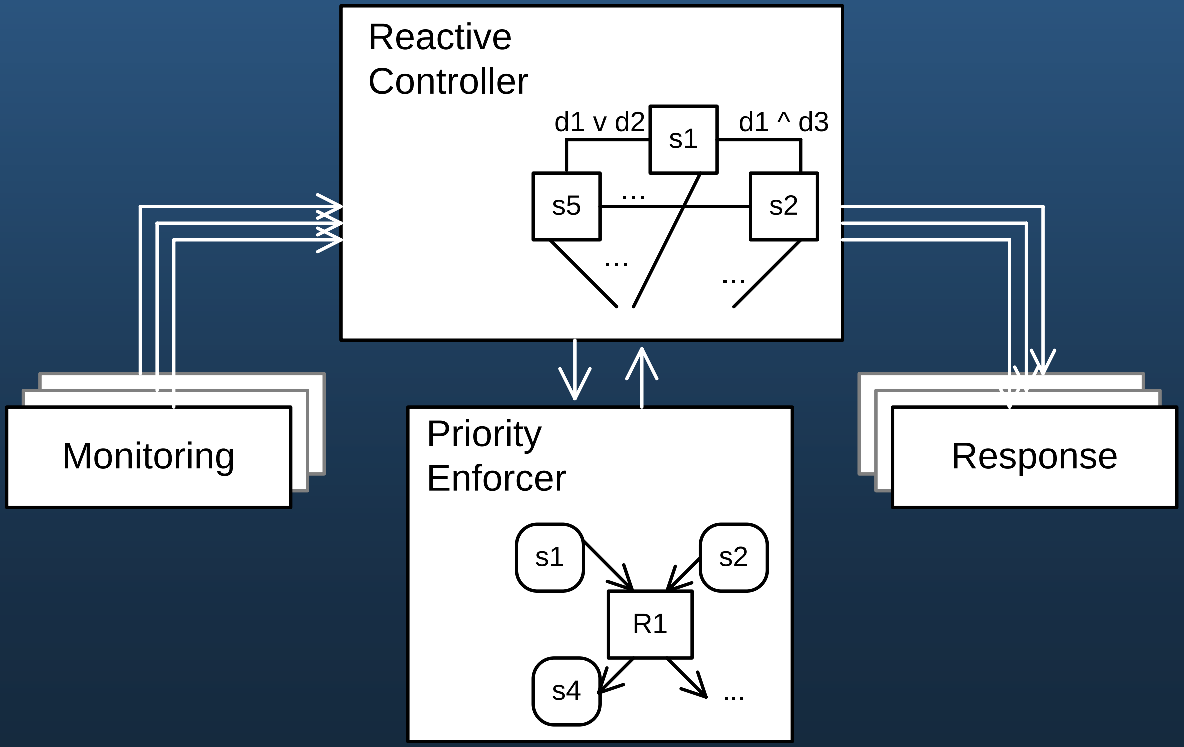
- Policy code specifies method calls to be monitored (*joinpoints*)
- Strata-Compiler generates policy binary
- Strata VM weaves it into application binary



The Willow Architecture

(John C. Knight, D. Heimbigner, A. Wolf, A. Carzaniga, J. Hill, P. Devanbu)

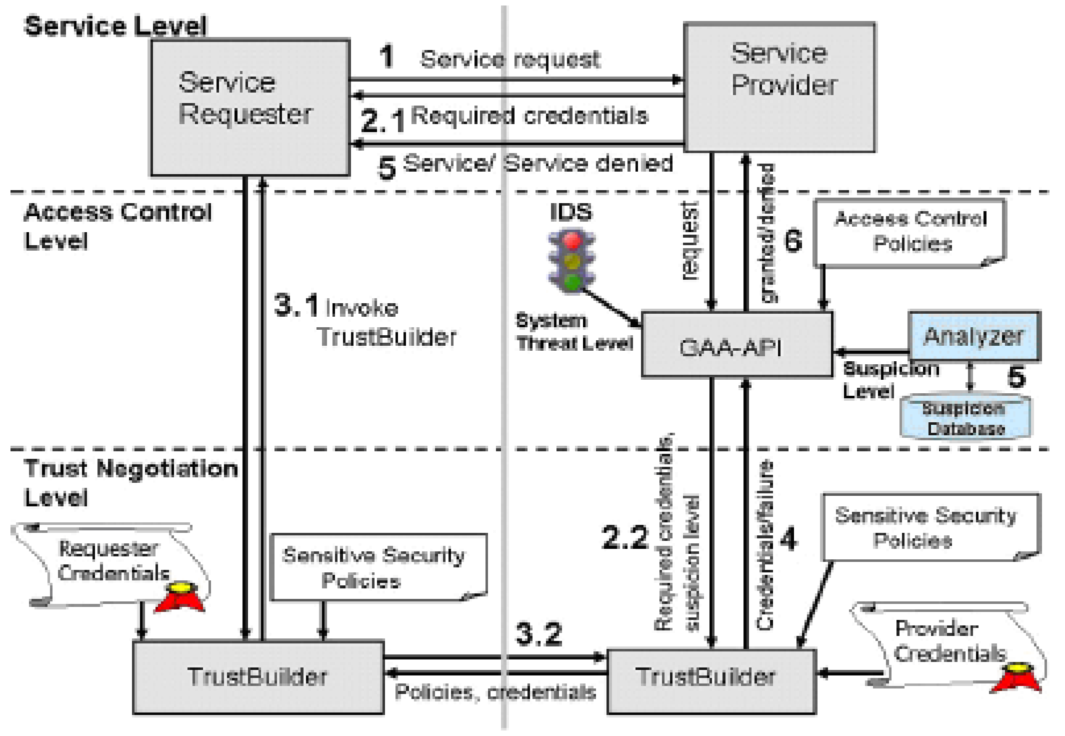
- Control loops interact with monitoring components
- Reactive Controller chooses/accepts a configuration
- Priority Enforcer enforces distributed configuration order



Adaptive Trust Negotiation and Access Control (ATNAC)

(T. Ryutov, Li Zhuo, C. Neuman, T. Leithead, K. Seamons)

- Client issues service request to Server
- Server side GAA-API decides to grant/deny access
- If (grant) {Client side and Server side TrustBuilders negotiate authentication credentials}



Evaluation of the Approaches

Adaptive Application Security Approach	Security Dimensions			Adaptation Dimensions		
	Authentication	*Authorization*	*Tolerance*	*Paradigm*	*Reconfig Scale*	*Conflict Handling*
Extensible Security Infrastructure		Adaptive		Reflection	Inter-unit	Autonomous
Strata Security API		Adaptive		Aspect-Orientation	Inter-unit	None
The Willow Architecture			Adaptive	Component-Based	Arch. Wide	Autonomous
ATNAC	Adaptive	Adaptive	Fixed	Parametarization	Single-unit	None

Conclusion & Future Work

- Adaptive application security requires:
  - All reconfiguration scales
  - Automated detection and resolution of conflicts
  - Consideration of security features collectively

- Future Work:
  - Supporting the full spectrum of reconfiguration scales (single-unit, inter-unit, and architecture-wide)
  - Analyzing productivity/flexibility tradeoffs in autonomous and interactive conflict resolution
  - Investigating the maintainability and reuse potential in current adaptation paradigms

References

- P. McKinley, S. Sadjadi, E. Kasten, and B. Cheng, “Composing Adaptive Software,” *IEEE Computer*, 37(7):56-64, July 2004.
- B. Hashii, S. Malabarba, R. Pandey, M. Bishop, “Supporting reconfigurable security policies for mobile programs.” *Computer Networks*, vol 33(2000), pps. 77-93.
- K. Scott, J. Davidson, Software Security using Software Dynamic Translation. Technical Report CS-2001-29, Department of Computer Science, University of Virginia, 2001.
- J. Knight, D. Heimbigner, A. Wolf, A. Carzaniga, J. Hill, P. Devanbu. “The Willow Survivability Architecture.” *In Fourth Information Survivability Workshop (ISW-2001).*
- T. Ryutov, L. Zhou, C. Neuman, T. Leithead, K. Seamons, “Adaptive Trust Negotiation and Access Control.” *ACM Symposium on Access Control Models and Technologies*, pps. 139-146, 2005.
- J. Lala, “Foundations of Intrusion Tolerance Systems.” IEEE Computer Society Press, Catalog # PR02057, 2003.
- …