Self-Adaptive Security Systems
Self-Adaptive Security System
Aimee Borda
Motivational Example

Security Policy: No visitor should be left alone with Server in $R_3$

Motivational Example\textsuperscript{1}

Security Policy: No visitor should be left alone with Server in $R_3$

Motivational Example

20 Visitors & 20 Employees

\[ e_1 \text{ in } R_1 \Rightarrow v_1 \text{ allowed in } R_1 \]
\[ e_1 \text{ in } R_1 \Rightarrow v_1 \text{ allowed in } R_2 \]
\[ e_1 \text{ in } R_1 \Rightarrow v_1 \text{ not allowed in } R_3 \]
\[ e_1 \text{ in } R_1 \Rightarrow v_1 \text{ allowed in } R_4 \]
\[ e_1 \text{ in } R_2 \Rightarrow v_1 \text{ allowed in } R_1 \]
\[ e_1 \text{ in } R_2 \Rightarrow v_1 \text{ allowed in } R_2 \]
\[ e_1 \text{ in } R_2 \Rightarrow v_1 \text{ not allowed in } R_3 \]
\[ e_1 \text{ in } R_2 \Rightarrow v_1 \text{ allowed in } R_4 \]
\[ e_1 \text{ in } R_3 \Rightarrow v_1 \text{ allowed in } R_1 \]
\[ e_1 \text{ in } R_3 \Rightarrow v_1 \text{ allowed in } R_2 \]
\[ e_1 \text{ in } R_3 \Rightarrow v_1 \text{ allowed in } R_3 \]
\[ e_1 \text{ in } R_3 \Rightarrow v_1 \text{ allowed in } R_4 \]
\[ e_1 \text{ in } R_4 \Rightarrow v_1 \text{ allowed in } R_1 \]

\[ 20 \times 20 \times 4 = 1600 \]

---

MAPE Feedback Loop²

4-Step Adaptive Process:
1. Monitor
2. Analysis
3. Planning
4. Execution

² Tsigkanos, Christos et al. "Engineering topology aware adaptive security: Preventing requirements violations at runtime." *Requirements Engineering Conference (RE), 2014 IEEE*
What exactly do we want to Verify?

We want to show that our system is correct wrt a set of Security Policies.

Because of the increased complexity, we need compositional reasoning:

• Monitoring: all events are detected
• Analysis: all violations are found
• Planning: counter-measures guards against all violations
• Execution: plan implemented faithfully

---

2 Tsigkanos, Christos et al. "Engineering topology aware adaptive security: Preventing requirements violations at runtime." Requirements Engineering Conference (RE), 2014 IEEE
How can we verify such Systems?
Run-time Monitoring$^{3,4}$

3 Schneider, Fred B. "Enforceable security policies." ACM Transactions on Information and System Security (TISSEC) 2000

Our Approach: Adaptive Monitors
Verifying Adaptive Monitors
Conclusion

Research Questions:

• What is the right model for SASS?
• When is a SASS correct?
• What verification techniques can we apply?
• How can we tackle complexity?
Thank You!