Lero THE IRISH SOFTWARE RESEARCH CENTRE

Self-Adaptive Security Systems

University of Limerick
Ollscoil Luimnigh

Trinity College Dublin

DCU

UCD Dublin

OÉ Gaillimh
NUI Galway

Dundalk Institute of Technology

UCC
University College Cork, Ireland
Coláiste na hOllscoile Corcaigh

Maynooth University
National University of Ireland Maynooth

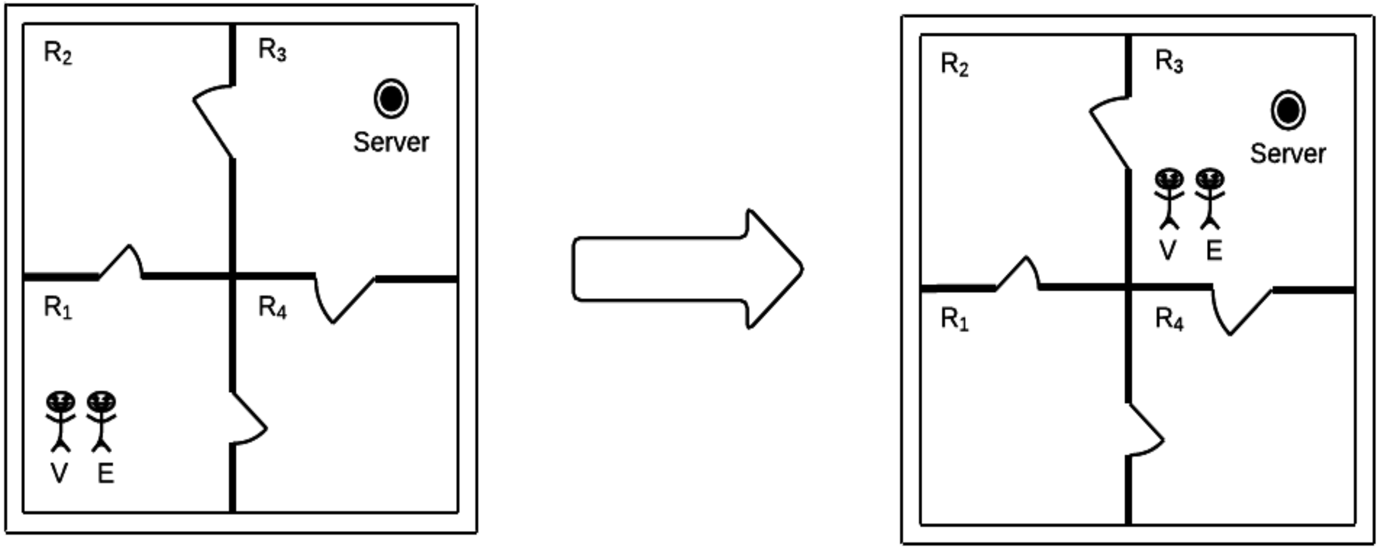
Lero THE IRISH SOFTWARE RESEARCH CENTRE

Self-Adaptive Security System

Aimee Borda

Motivational Example[1]

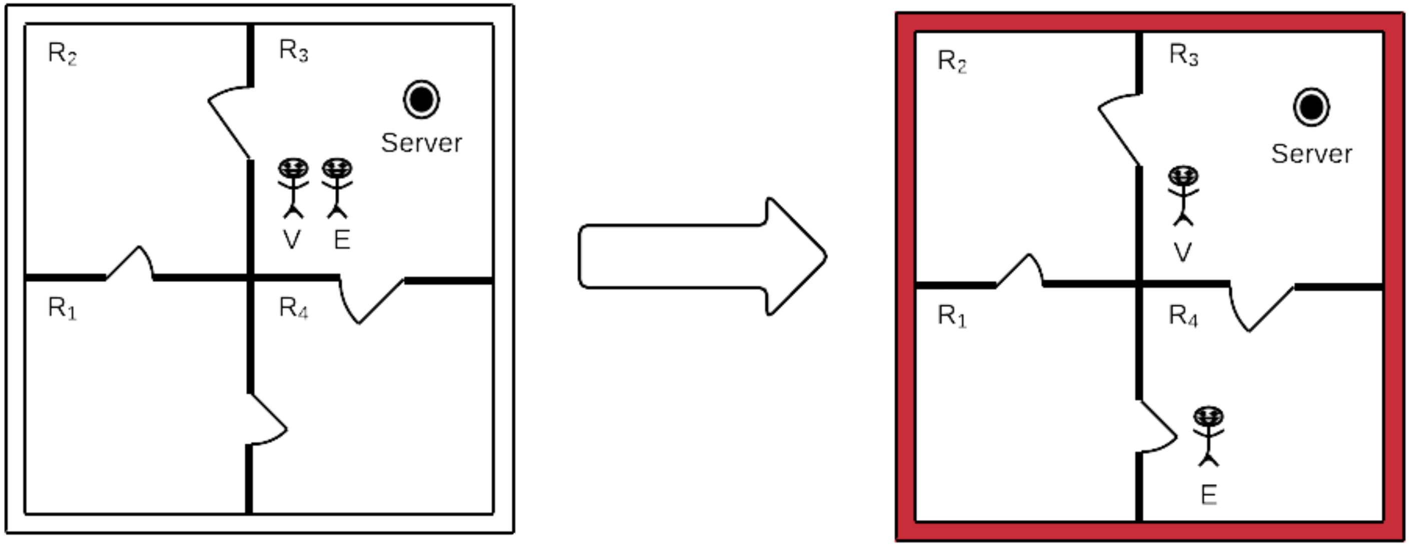
Security Policy: No visitor should be left alone with Server in R_3



[1] Pasquale, Liliana et al. "Topology aware adaptive security." in *Proc of the 9th International Symposium on Software Engineering for Adaptive and Self-Managing Systems* 2014.

Motivational Example[1]

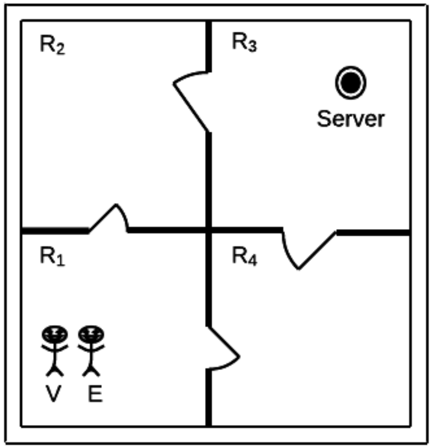
Security Policy: No visitor should be left alone with Server in R_3



[1] Pasquale, Liliana et al. "Topology aware adaptive security." in *Proc of the 9th International Symposium on Software Engineering for Adaptive and Self-Managing Systems* 2014.

Motivational Example[1]

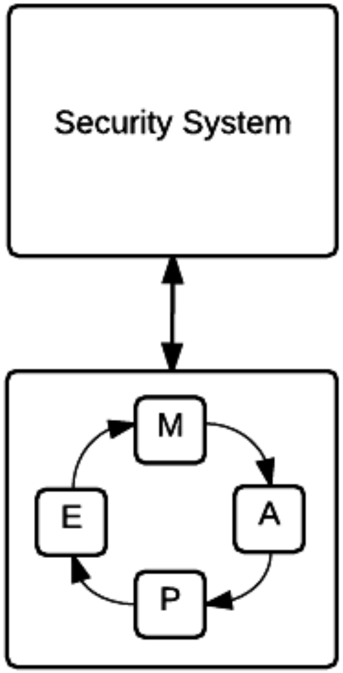
20 Visitors & 20 Employees



$$\left.\begin{array}{l}
e_1 \text{ in } R_1 \Rightarrow v_1 \text{ allowed in } R_1 \\
e_1 \text{ in } R_1 \Rightarrow v_1 \text{ allowed in } R_2 \\
e_1 \text{ in } R_1 \Rightarrow v_1 \textbf{not} \text{ allowed in } R_3 \\
e_1 \text{ in } R_1 \Rightarrow v_1 \text{ allowed in } R_4 \\
e_1 \text{ in } R_2 \Rightarrow v_1 \text{ allowed in } R_1 \\
e_1 \text{ in } R_2 \Rightarrow v_1 \text{ allowed in } R_2 \\
e_1 \text{ in } R_2 \Rightarrow v_1 \textbf{not} \text{ allowed in } R_3 \\
e_1 \text{ in } R_2 \Rightarrow v_1 \text{ allowed in } R_4 \\
e_1 \text{ in } R_3 \Rightarrow v_1 \text{ allowed in } R_1 \\
e_1 \text{ in } R_3 \Rightarrow v_1 \text{ allowed in } R_2 \\
e_1 \text{ in } R_3 \Rightarrow v_1 \textbf{ allowed} \text{ in } R_3 \\
e_1 \text{ in } R_3 \Rightarrow v_1 \text{ allowed in } R_4 \\
e_1 \text{ in } R_4 \Rightarrow v_1 \text{ allowed in } R_1 \\
\qquad\qquad \vdots
\end{array}\right\}
\begin{array}{l} 20 * 20 * 4 \\ = 1600 \end{array}$$

[1] Pasquale, Liliana et al. "Topology aware adaptive security." in *Proc of the 9th International Symposium on Software Engineering for Adaptive and Self-Managing Systems* 2014.

MAPE Feedback Loop[2]



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?

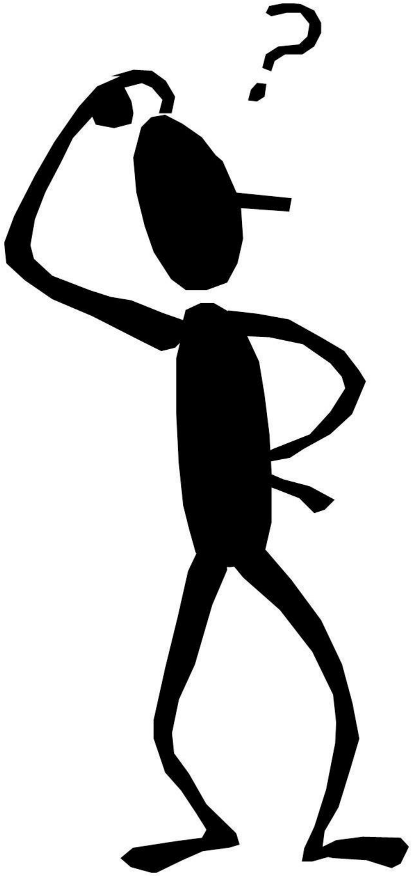
We want to show that our system is **correct** wrt a set of Security Policies

Because of the increased complexity, we need **compositional** reasoning:

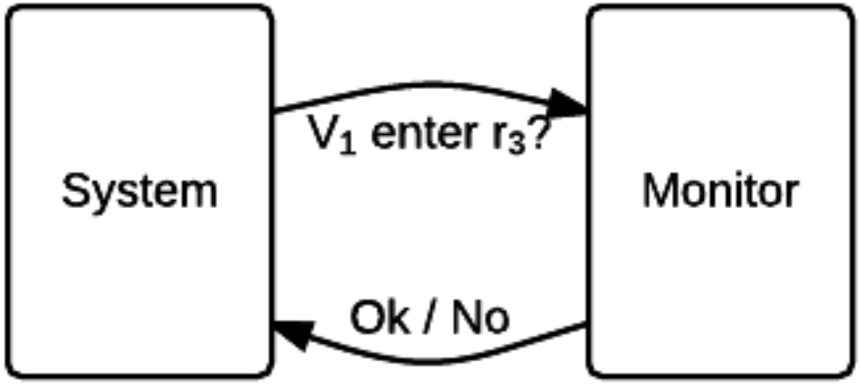
- Monitoring : all events are detected
- Analysis: all violations are found
- Planning: counter-measures guards against all violations
- Execution: plan implemented faithfully

[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?



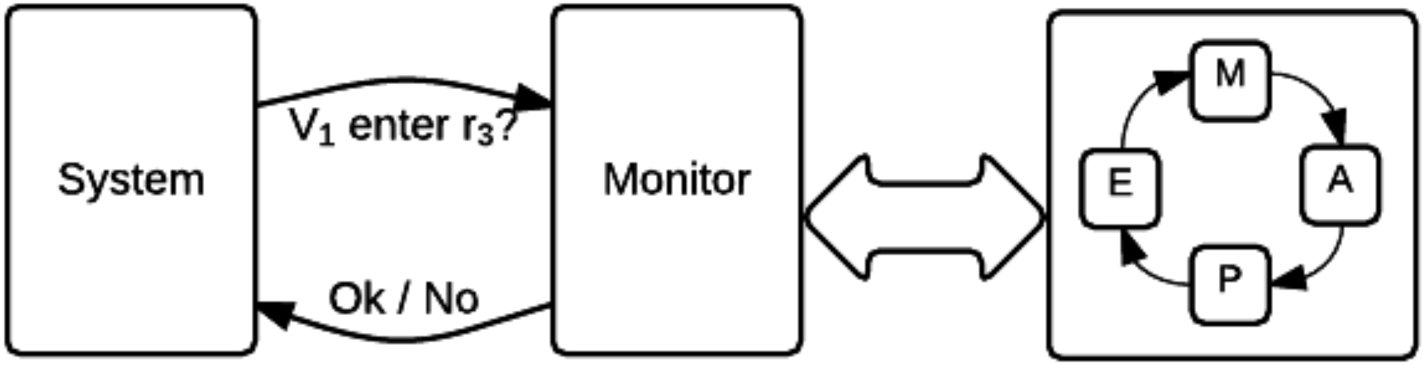
Run-time Monitoring[3,4]



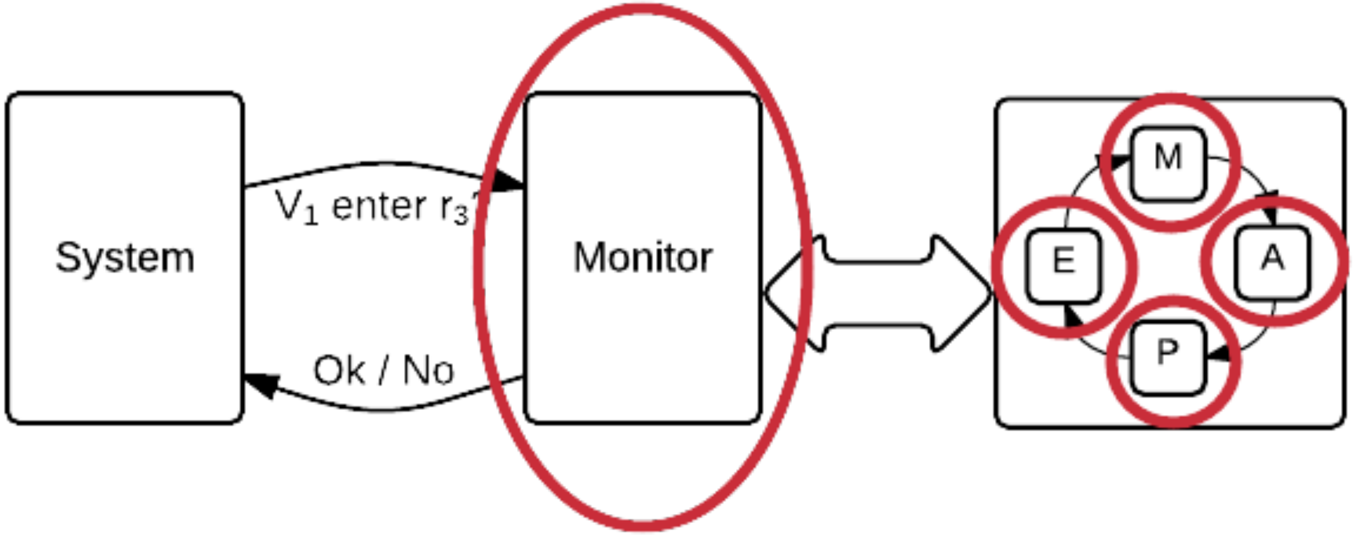
[3] Schneider, Fred B. "Enforceable security policies." ACM Transactions on Information and System Security (TISSEC) 2000

[4] Bauer, Lujo, et al. "More enforceable security policies." in *Proc. of the Workshop on Foundations of Computer Security (FCS'02), Denmark* 2002.

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?

lero THE IRISH SOFTWARE RESEARCH CENTRE

Thank You!

sfi Science Foundation Ireland

Ireland's European Structural and Investment Funds Programmes 2014-2020
Co-funded by the Irish Government and the European Union

European Union
European Regional Development Fund