A Runtime Verification Framework for Access Control

Minh Van Nguyen
ANU Summer Research Scholar 2007/2008
nguyenminh2@gmail.com

30 January 2008

Why runtime verification?

- dynamically monitor systems

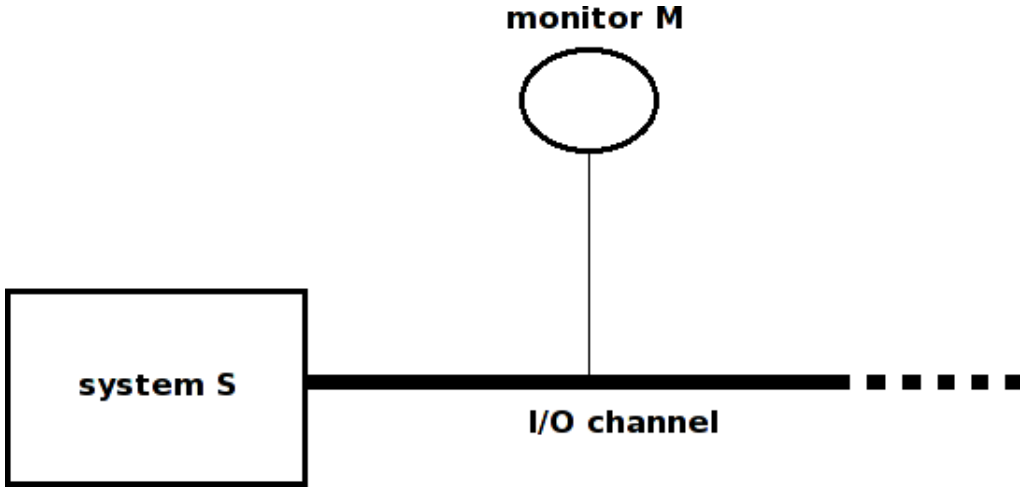

Figure 1: System monitoring during operation.

- advantages:
  - increases confidence on implementation
  - information available at runtime
  - behaviours dependent on operating environment
  - security concerns, critical systems

Specifying system requirements using LTL

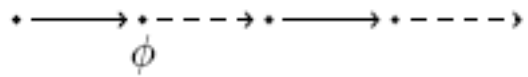

Figure 2: $\mathbf{X}\phi$: ϕ holds at the ne$\mathbf{X}$t state.

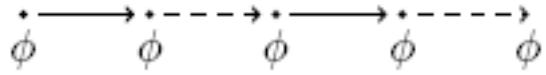

Figure 3: $\mathbf{G}\phi$: ϕ holds $\mathbf{G}$lobally.

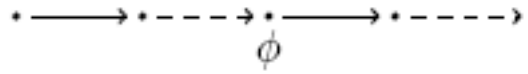

Figure 4: $\mathbf{F}\phi$: $\mathbf{F}$inally ϕ holds.

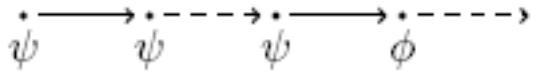

Figure 5: $\psi\mathbf{U}\phi$: ψ holds $\mathbf{U}$ntil ϕ holds.

LTL and Büchi automata

- finite-state automaton: $\mathcal{A} = (Q, \Sigma, \delta, q_0, F)$
- Büchi automaton: $\mathcal{A}$ with infinite inputs

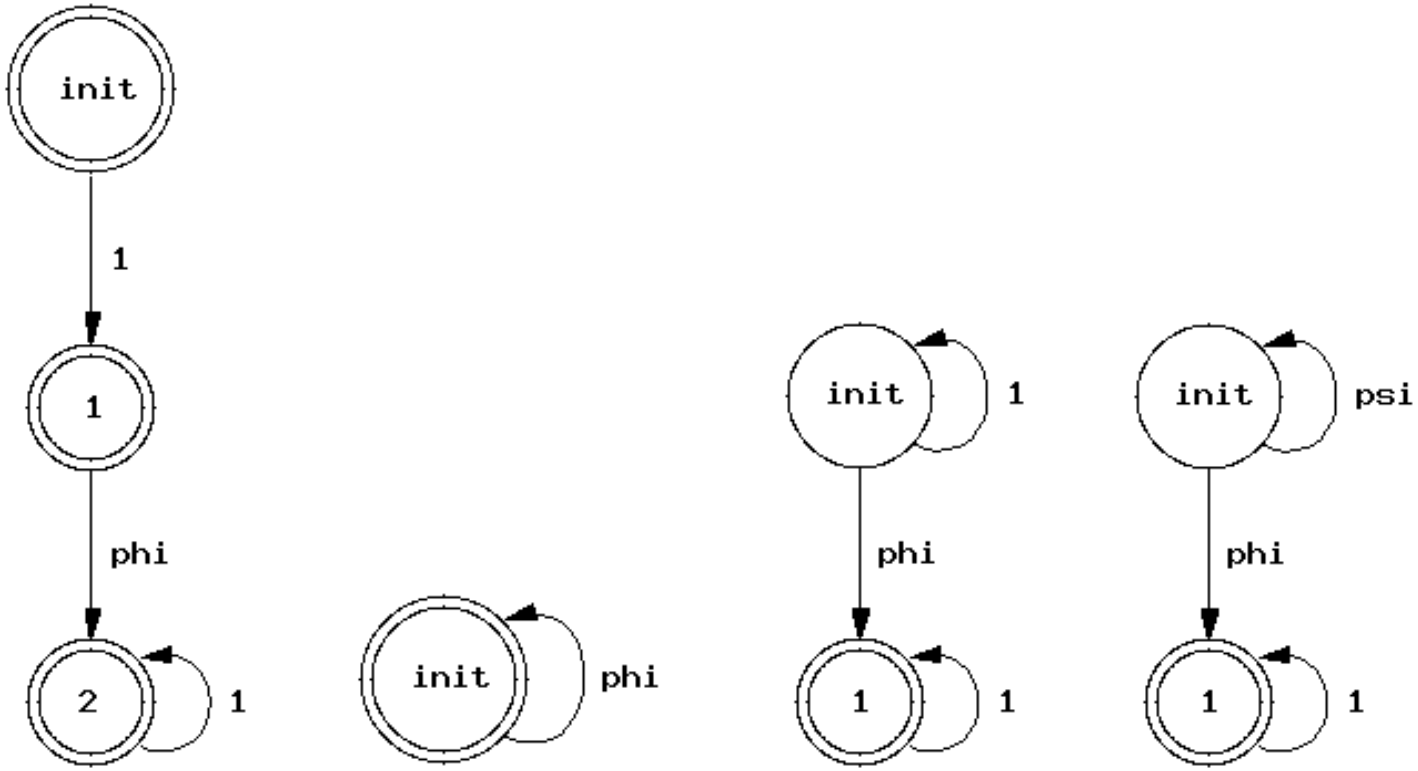

Figure 6: Büchi automata for **X**, **G**, **F**, **U** respectively.

Model checking using Büchi automata

- infinite sequence w, so $w \models \varphi$ or $w \not\models \varphi$ for some φ; finite prefix u of w
- three-valued LTL

$$[u \models \varphi] = \begin{cases} \top & \text{if } uw' \models \varphi \\ \bot & \text{if } uw' \not\models \varphi \\ ? & \text{otherwise} \end{cases}$$

- generate $\mathcal{A}^{\varphi}$ and $\mathcal{A}^{\neg\varphi}$, then input u

φ	$\neg\varphi$	value
SAT	SAT	?
SAT	UNSAT	$\top$
UNSAT	SAT	$\bot$

Table 1: Satisfiability criteria in 3-valued LTL.

References

1. Bauer, Andreas. "Model-Based Runtime Analysis of Distributed Reactive Systems". PhD thesis, Institut für Informatik, Technische Universität München, 2007.

2. Bauer, Andreas, Martin Leucker and Christian Schallhart. "Monitoring of Real-Time Properties" in S Arun-Kumar and N Garg (eds.). *FSTTCS 2006: Foundations of Software Technology and Theoretical Computer Science* (LNCS 4337). Springer-Verlag, 2006, pp.260–272.

3. Hopcroft, John E and Jeffrey D Ullman. *Introduction to Automata Theory, Languages, and Computation*. Addison-Wesley Publishing Company, 1979.

4. JGraphT - Java graph library
   `http://jgrapht.sourceforge.net/`
   Viewed 19 December 2007

5. LTL2BA: fast translation from LTL formulae to Büchi automata
   http://www.lsv.ens-cachan.fr/~gastin/ltl2ba/
   Viewed 20 December 2007

6. LTL2BA4J - Java bridge to ltl2ba
   http://www.sable.mcgill.ca/~ebodde/rv//ltl2ba4j/
   Viewed 29 January 2008

Thank You