Logics in Security **Winter 2014**

Homework for Module 1

Instructor: Deepak Garg
dg@mpi-sws.org

TA: Iulia Boloşteanu
iulia_mb@mpi-sws.org

Release date: November 12, 2014 *Due date: November 19, 2014*

General instructions: Attempt all questions. Submit your homework, in typeset form, via email to both the instructor and the TA before midnight on the due date. The LaTeX source for this homework will be provided to help you typeset. You can also typeset using any other means, including simple ASCII.

Problem 1-1 (5 points)

Consider executions over the alphabet $\{a, b, c\}$. Which of the following are safety properties? For each safety property, construct a corresponding security automata as defined by Schneider on page 36 of the paper "Enforceable Security Policies". You may present your automata in either of the two forms illustrated in Fig. 1 and Fig. 2 of Schneider's paper.

1. c never occurs after a and c never occurs after b.
2. Every a is followed immediately by a b.
3. Every a is followed by a b (not necessarily immediately).
4. Every a is followed by a b within the next 7 steps.
5. In every prefix of the execution, the number of c's is less than the total number of a's and b's.

Problem 1-2 (5 points)

Recall Schneider's quote about Lamport's characterization of safety properties.

> A property Γ is defined in Lamport [1985] to be a safety property if and only if, for any finite or infinite execution σ, $\sigma \notin \Gamma \Rightarrow (\exists i.(\forall \tau \in \Psi : \sigma[..i]\tau \notin \Gamma))$.

Assume that this quote is the definition of a safety property. Prove that the following statement is an alternative characterization of every safety property Γ (that is, the statement above holds if and only if the statement below holds).

> There is a set S of *finite* executions such that for any finite or infinite execution σ, $\sigma \notin \Gamma$ if and only if $\sigma = \tau_1\tau_2$ for some $\tau_1 \in S$ and $\tau_2 \in \Psi$.

Problem 1-3 (5 points)

For each property of Problem 1-1 that is actually a safety property, construct a suitable set S that satisfies the characterization of Problem 1-2.