# Justification: Visual Security Protocol Modeling

J. McDermott

This research paper describes a new visual modeling language for security protocols. Security protocols are sequences of allowable interactions between *principals*. A principal is an entity that participates in a security system. Security protocols are not necessarily about cryptography; one of the two examples in this paper involves no cryptography at all.

The current approach to *model-driven architecture* assumes that no special visual modeling approaches are needed to describe security problems or solutions. Security, including protocol modeling, is treated largely as a service to be mentioned by general visual modeling approaches. This paper disagrees with that stance.

A suitable visual security protocol modeling approach will satisfy the following criteria:

- The visual formalism should be *event-based*. It should focus on interaction patterns between principals and abstract away from details of internal computations. The importance of this is underscored by the fact that existing security protocol modeling tools use event-based visual models, rather than state-based models.

- The visual formalism should support *composition* in a natural way, so that models can be constructed from components that identifiably correspond to the principals of the protocol.

- The visual formalism should be *comprehensive*. It should be capable of defining all traces of a protocol by means of a single diagram.

- The visual formalism should be *concise*. Defining a complex protocol should not require an explosion of modeling details.

- The visual formalism should have a *well-defined* syntax and semantics.

These criteria are based on *suitability* for presentation and human understanding of security protocols rather than computational expressiveness or automated analysis. This paper explains why visual modeling approaches in the OMG's UML 2.0 and possble alternatives outside of UML, including Harel statecharts and labeled transition systems, fail to meet these criteria. A new visual modeling language that satisfies all five criteria is presented, by means of two examples.