***Bounded Memory Protocols and the Unbounded Adversary***

The Dolev-Yao adversary is a non-deterministic adversary which can act as the network, intercept, send, compose and decompose messages, and remember as much information as it needs. That is, its memory is unbounded. We recently proposed a weaker Dolev-Yao like adversary, which can also act as the network, but whose memory is bounded. We showed that this Bounded Memory Dolev-Yao adversary, when given enough memory, can carry out many existing protocol anomalies. In particular, the known anomalies arise for bounded memory protocols, where there is only a bounded number of concurrent sessions and the honest participants of the protocol cannot generate an unbounded number of facts nor an unbounded number of nonces. This led us to the question of whether it is possible to infer a computable upper bound on the memory required by the standard, unbounded Dolev-Yao adversary to carry out a protocol anomaly from the memory restrictions of the bounded protocol. We answer this question negatively. This is joint work with Max Kanovich, Tajana Ban Kirigin, and Vivek Nigam.