Automated Protocol Design and Refinement

Challenge:

- Protocols are designed ad-hoc by engineers
- Formal proofs are difficult to produce and rare
- Security goals should be easier to express and satisfy

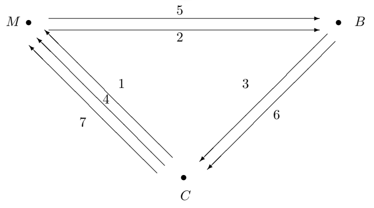
Solution:

- Use the Strand Spaces model
- with Linear Logic theorem proving
- and Disjoint Encryption
- and Attack-based Optimization

1617307 - Jay McCarthy (PI)
University of Massachusetts Lowell
jmccarth@cs.uml.edu

$$\begin{tikzcd}
m_0 \arrow[rr, dashed, "K^{-1} \in \mathsf{S} \qquad a \sqsubset \{\!|h|\!\}_K"] \arrow[d, Rightarrow] & & n_0 \arrow[d, Rightarrow] \\
m_1 & {} \arrow[l, dashed, "a \sqsubset \mathrm{term}(n_1)"'] & n_1 \arrow[l, dashed, "a \sqsubset t'"']
\end{tikzcd}$$

$$\begin{tikzcd}
m_0 \arrow[r, dashed, "a \sqsubset \mathrm{term}(m_0)"] \arrow[d, Rightarrow] & {} \arrow[r, dashed] & n_0 \arrow[d, Rightarrow] \\
m_1 & {} \arrow[l, dashed, "\{\!|h|\!\}_K \sqsubset \mathrm{term}(m_1) \quad K \in \mathsf{Safe}"'] & n_1 \arrow[l, dashed, "a \sqsubset \{\!|h|\!\}_K"']
\end{tikzcd}$$



$$\begin{array}{ccccc}
C & \xrightarrow{1} & M & \xrightarrow{2} & B \\
B & \xrightarrow{3} & M & \xrightarrow{4} & C \\
C & \xrightarrow{5} & M & \xrightarrow{6} & B \\
B & \xrightarrow{7} & M & \xrightarrow{8} & C
\end{array}$$

Scientific Impact:

- Novel theory of protocol goals with specification implementation
- Novel theory of protocol composition with goal-directed compositor
- Novel theory of protocol equivalence with solver

Broader Impact:

- Open source implementation
- Teaching modules for undergraduates
- Use case discussion for AP CSP
- Truth-worthy online services if used