Formalizing Physical Security Procedures

Catherine Meadows[1] and Dusko Pavlovic[2]

[1] Naval Research Laboratory, Washington, DC, USA
Email: meadows@itd.nrl.navy.mil
[2] Royal Holloway, Oxford and Twente
Email: dusko.pavlovic@rhul.ac.uk

Although the problems of physical security emerged more than 10,000 years before the problems of computer security, no formal methods have been developed for them, and the solutions have been evolving slowly, mostly through social procedures. But as the traffic on physical and social networks is now increasingly expedited by computers, the problems of physical and social security are becoming technical problems. From various directions, many security researchers and practitioners have come to a realization that the areas such as transportation security, public and private space protection, or critical infrastructure defense, are in need of formalized engineering methodologies. Following this lead, we extended Protocol Derivation Logic (PDL) to Procedure Derivation Logic (still PDL). In contrast with a protocol, where some principals send and receive some messages, in a procedure they can also exchange and move some objects. in this talk, we use this approach to develop a formal system that can be used to describe and reason about physical movement and containment, and show how it can be applied airport security protocols.

This 5-minute talk will be given by Catherine Meadows.