

Modeli apstraktne kriptografije i protokoli (2)

Neva Slani

3. srpnja 2004.

Izložena su sljedeća dva apstraktna modela, model niti i model struna.

Model niti daje vrlo intuitivnu specifikaciju protokola. Protokoli se predstavljaju grafovima čiji su vrhovi označeni. Oznakama se opisuju akcije slanja, odnosno primanja poruke. Za analizu protokola koristi se relacija "biti podterm" na porukama te relacija kauzalnosti na vrhovima, koja određuje vremenski slijed izvršenih koraka.

Model struna daje specifikaciju u obliku računa procesa, sličnog π -računu. Dana semantika je operativna, a reakcije definirane na strunama su: reakcija apstrakcije (primanje u varijablu) i slanja terma, te interne akcije kreiranja novog objekta i uspoređivanje uzoraka (*pattern matching*). Dekripcija se obavlja uspoređivanjem uzoraka.

Tri modela su na istom nivou apstrakcije, reflektiraju ista svojstva protokola, a ukratko je opisan prijevod modela transformacija multiskupova u model niti i obratno.

Literatura:

N. Durgin, J. Mitchell, and D. Pavlovic. *A compositional logic for protocol correctness*. In *Proceeding of 14th IEEE CSFW*, 2001.

F. J. Thayer Fábrega, J. Herzog, and J. Guttman. *Strand spaces: Proving security protocols correct*. *Journal of Computer Security*, 7(2/3), 1999.

D. Song. *Athena, an automatic checker for security protocol analysis*. In *12th IEEE Computer Security Foundation Workshop*, June 1999.

I. Cervesato, N. Durgin, P. Lincoln, J. Mitchell, and A. Scedrov. *A comparison between strand spaces and multiset rewriting for security protocol analysis*. In *Software Security – Theories and Systems*, Mext-NSF-JSPS International Symposium, ISSS 2002.