Type-Safe Execution of Mobile Agents in Anonymous Networks

Matthew Hennessy[1] and James Riely[2]

[1] Univ. of Sussex.
[2] North Carolina State Univ.

In a previous report we presented a type system for controlling the use of resources in a distributed system. The type system guarantees that resource access is always *safe*, in the sense that, for example, integer channels are always used with integers and boolean channels are always used with booleans. The type system, however, requires that all agents in the system be well-typed. In open systems, such as the internet, such global properties are impossible to verify. In this paper, we present a type system for *partially typed* networks, where only a subset of agents are assumed to be well typed.

This notion of partial typing is presented using the language Dπ. In Dπ mobile agents are modeled as *threads*, using a thread language based on the π-calculus. Threads are located at *sites* and interact using *channels* or *resources*.

In an open system, not all agents are necessarily benign. Some sites may harbor malicious agents that do not respect the typing rules laid down for the use of resources. For example, consider the system

$$\ell[\![(\nu c\!:\mathsf{res}\langle\mathsf{int}\rangle)\ \mathsf{go}\, m.a!\langle \ell, c\rangle]\!] \ \mid\ m[\![a?(z,x)\ \mathsf{go}\, z.x!\langle\mathsf{true}\rangle]\!]$$

consisting of two agents, located at ℓ and m respectively. The first generates a new local channel c for transmitting integers and makes it known to the second site m, by sending it along the channel a local to m. In a benign world ℓ could assume that any mobile agent that subsequently migrates from m to ℓ would only use this new channel to transmit integers. However in an insecure world m may not play according to the rules; in our example it sends an agent to ℓ which misuses the new resource by sending the boolean value true along it.

In this paper we formalize one strategy that sites can use to protect themselves from such attacks. The strategy makes no assumptions about the security of the underlying network. For example, it is not assumed that the source of a message (or agent) can be reliably determined. We refer to such networks as *anonymous networks*.

In the presence of anonymous networks a reasonable strategy for sites is based on *paranoia*. Since the source of messages cannot be determined it is impossible to distinguish messages from potentially "trusted" sites; thus no site can be trusted. To protect itself, a site must bar entry of any mobile agent that cannot be proven to use local resources as intended.

[1] `matthewh@cogs.susx.ac.uk` Research funded by CONFER II and EPSRC project GR/K60701.

[2] `riely@csc.ncsu.edu` Research funded by NSF grant EIA-9805604.