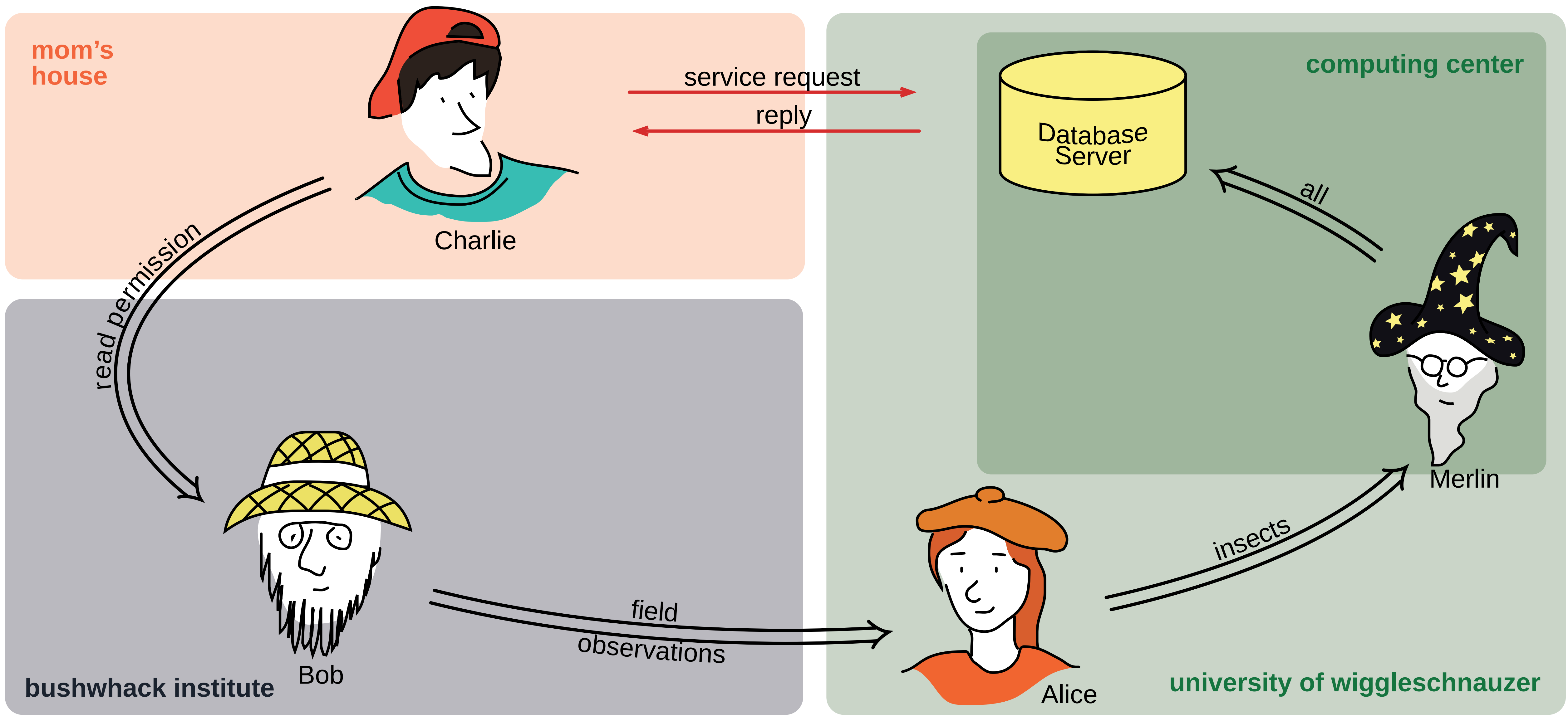
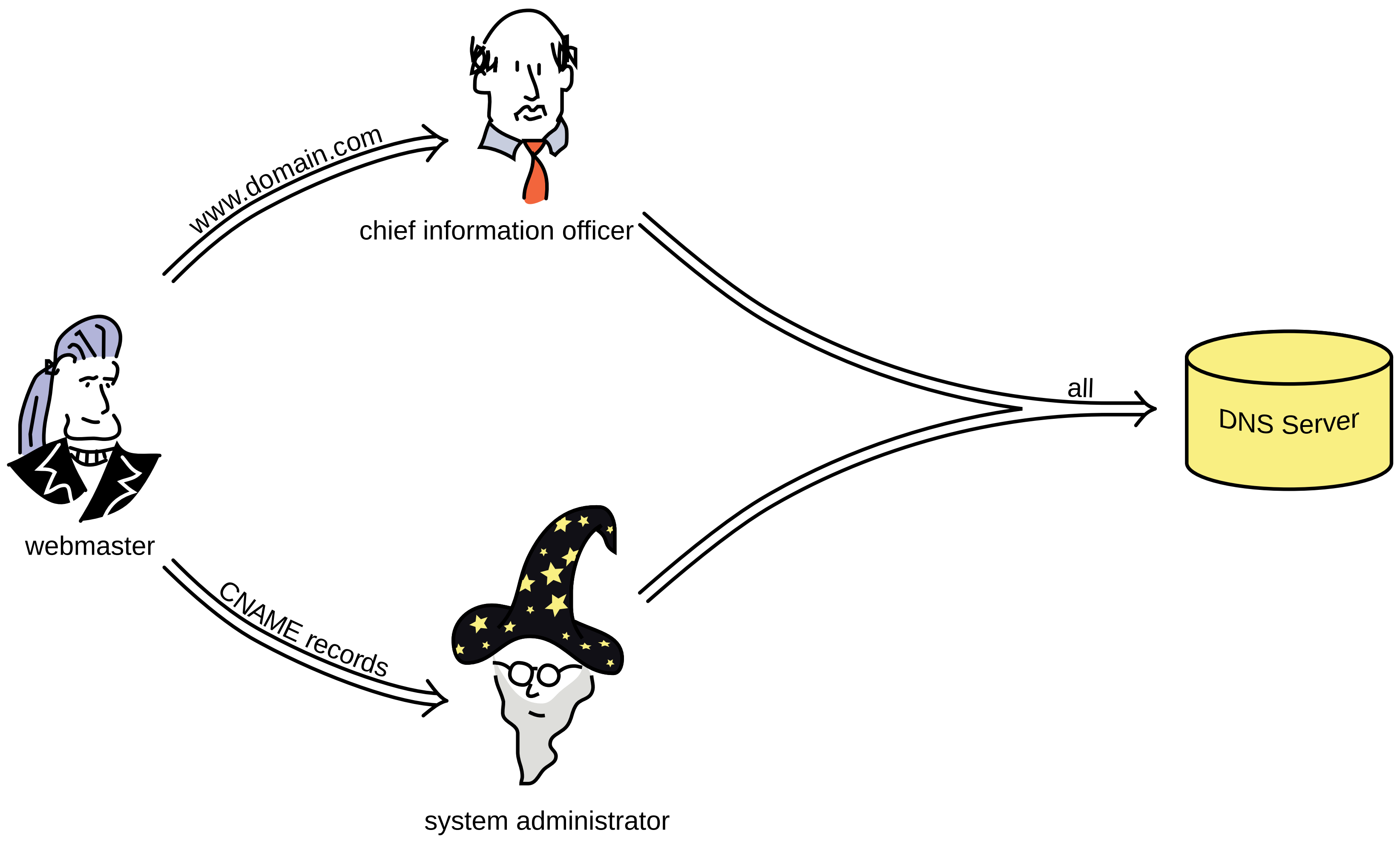
Restricted delegation: seamlessly spanning administrative boundaries

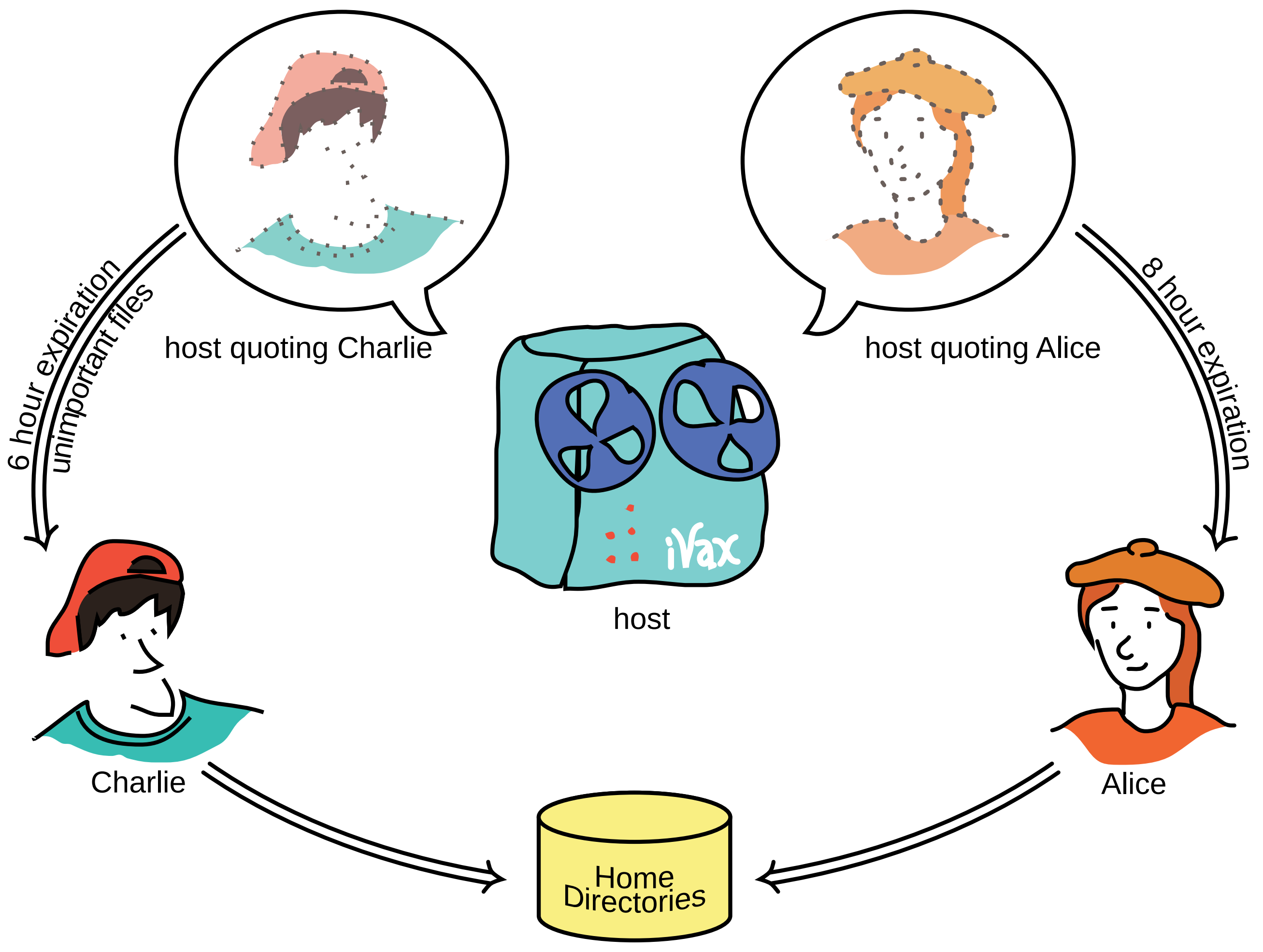
Jon Howell and David Kotz
Dartmouth College
http://www.cs.dartmouth.edu/~jonh/research/delegation/



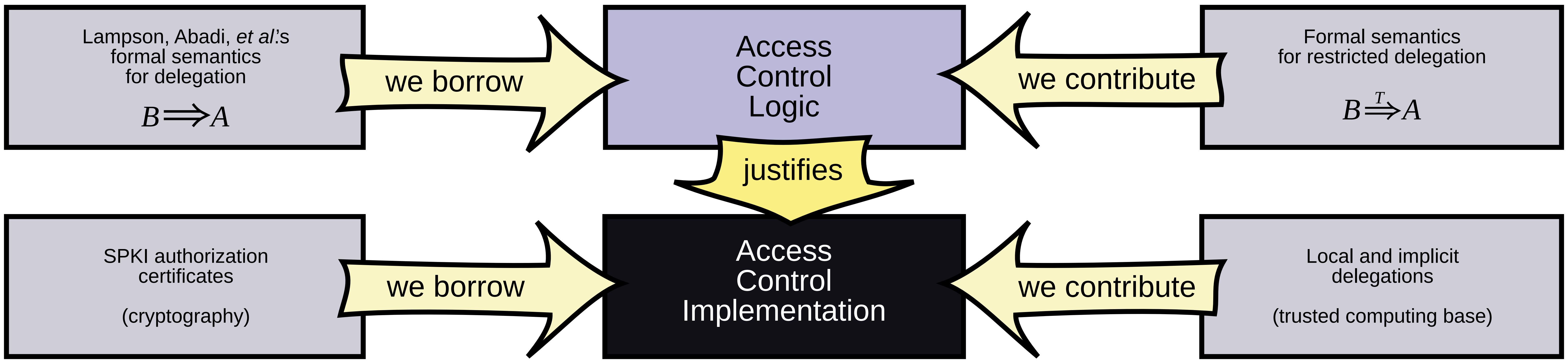
Restricted delegation enables flexible administrative boundaries. Conventional systems assume a hierarchy of administrative control, and thus cannot express non-hierarchical trust relationships. Restricted delegation, on the other hand, models real, social relationships. It can model hierarchy: a manager trusts each of his employees in certain ways. Or it can model arbitrary trust graphs. In the example above, the system administrator trusts Alice to manipulate database records about insects. Alice trusts Bob about field observations, so transitively, Bob may create field observation records about insects. Likewise, Bob may trust Charlie to read any of his data, so Charlie is allowed to read the database records on insect field observations. The red arrows represent Charlie making a request of the database server; for it to be granted, Charlie's software will supply a proof of his permission that references each of the restricted delegations shown.



Conjunct principals let us model redundancy. Here, modifying the DNS server requires the agreement of both the CIO and the sysadmin. The webmaster has obtained restricted permission to speak on behalf of both the CIO and the sysadmin, and is therefore trusted to make certain changes to the DNS server.



Quoting principals defer access control decisions to the ultimate resource server. The host does not make per-file access control decisions, it only needs to take care to quote the right user. Hence quoting makes it easier to build such multiplexed resources securely, and helps reduce the size of the trusted computing base.


Lampson, Abadi, *et al.*'s formal semantics for delegation
$B \Longrightarrow A$
we borrow
Access Control Logic
we contribute
Formal semantics for restricted delegation
$B \overset{T}{\Longrightarrow} A$
justifies
SPKI authorization certificates
(cryptography)
we borrow
Access Control Implementation
we contribute
Local and implicit delegations
(trusted computing base)

We have extended Lampson's calculus for access control to model restricted delegation. Basing a security model on a formal semantics and logic helps us understand its subtle consequences. It also suggests consistent extensions that maintain the integrity of the model.