Mergers and Principals  
(Transcript of Discussion)

Dieter Gollman  
Microsoft Research

When the topic of the workshop was announced I found that for a change I had a paper which was relevant; maybe not broadening the horizon in itself, but pointing out some of the dangers you might encounter in this process. The relation to authentication comes through principals, and the origins of this presentation go back to Autumn last year when Ross Anderson asked me once again to give a talk at the Computer Lab and in despair I decided to find out what this term principal could really mean.

Ten years ago, not twenty as in Roger’s talk, the fashionable statement was, this is the time where computing and communications are merging. What I want to start with in this talk, is to examine the effect of this merger on two case studies. One has to do, as I said, with exploring the meaning of the term principal, the other is name resolution, where I had recently been asked to review a few papers and came across observations I want to share with you. Having a read a few papers on company policies in recent times, it seems that today the management gurus tell companies to concentrate on the core business, so it’s a time of de-mergers.

Case study one: what is a principal, where does this term come from, what purpose does it serve, what is it’s future? Here are some quotes taken from papers around Kerberos, from a community talking about communication:

| Principal: A uniquely named client or server that participates in a network communication.  
A principal is the basic entity which participates in network authentication exchanges. A principal usually represents a user or the instantiation of a network service on a particular host.  
After authentication, two principals (people, computers, services) should be entitled to believe that they are communicating with each other and not with intruders.  
A principal is anything that can sign messages.  
The fundamental purpose of authentication is to enable principals to identify each other in a way that allows them to communicate, with confidence that the communication originates with one principal and is destined for the other. All authentication is on behalf of principals. Principals can act in two capacities, claimant or verifier. SPX recognizes the following two types of principals, users (normally people with accounts) and servers.  
The principals we are considering include people, machines, organizations and network resources such as printers, databases or file systems. |
So a principal is something that participates in a communication. A principal is something that can be authenticated. Interesting at the bottom is “A principal is anything that can sign messages”. Within the same set of papers, again stressing principals are closely related to authentication, what I did not stress on the previous slide was one remark saying a principal can be a programme, a server, a person, we are quite general on this behalf. Stressed here, a principal can be a fair range of things engaging in communication, principals can be authenticated.

From about the same period, late 80s, there is a different set of papers, and they are associated with digital distributed system security architecture. Morrie Gasser happens to be one name popping up again and again as an author for the papers I’m quoting here:

A principal is an entity that can be granted access to objects or can make statements affecting access control decisions.
Subjects operate on behalf of human users we call principals, and access is based on the principal’s name bound to the subject in some unforgeable manner at authentication time.
Because access control structures identify principals, it is important that principal names be globally unique, human-readable and memorable, easily and reliably associated with known people.

So now a principal is something that can be granted access. There is this strong argument: you want to do access control, access control has to be understood by a human being, so the terms you should use, the principals you should use for access control, really very closely reflect human beings. Which is not what principals were on the previous line. This is history really, that is Butler Lampson’s model of authentication and authorisation: the rôle of the principal is to issue access requests, the rôle of the reference monitor is to check where an access request comes from – that’s called authentication – and then look up the rule and decide whether the principal actually should get access – and that step is called authorisation.

I’ve been saying this is history, but it’s still quite important because even today (if I read papers on access control in distributed systems, authentication in distributed systems), that is the reference point I want to go back to, that’s how they want to think about the world. There are simple principals like people, machines, rôles, and there are compound principals, a principal working in some rôle, delegation, conjunction of principals.

Maybe one should start to note that earlier the principal was the source of a request, whilst now principals are becoming rules, and I will elaborate this point later. There are two meanings of principal in this world and they start to deviate.

In the 1992 model of access control, principals are quite definitely the glue between authentication and authorisation: the access control information is stored in access control lists, the entries in an access control list are human readable.