Formalizing Anonymous Blacklisting Systems

This article, as the title suggests, formalizes anonymous blacklisting systems and what they must provide to function properly. The writers say write off the bat that these systems are not new and that they are merely bridging the gap between them to create a generic pattern for solving the problem of blacklisting malicious users. They also discuss some current implementations/solutions along with their merits and drawbacks.

I can say from personal experience that the idea of using online services anonymously can be quite beneficial and makes me feel better. I use several anonymizing systems and tools while online to protect myself and my personal information. I’ve noticed first hands how service providers often do not take into account that some users utilize their resources anonymously and this causes problems. I’ve also seen how other users that operate anonymously can very negatively impact the online community. I have also acted as a service provider and encountered this very problem, how to combat anonymous users who want to cause trouble?

The only methods I have utilized thus far are some of the ones they discuss in the paper. I can require that all users must have proper credentials (username and password) as well as banning users by their IP address (very rarely have I used a MAC address to ban a user). Require a username provides not anonymity (as the authors pointed out) but pseudonymity. For most this is fine but in scenarios where users are in areas where they must be anonymous this is insufficient. IP addresses are, on the other hand, fairly dynamic and can easily be spoofed (through proxies like Tor or just by the nature of DHCP).

To provide true anonymity (as true as you can get online) the authors suggest a system where users are identified by some unique resource. This can be linked to that particular user but does not betray their identity. An example of this is an IP address. This resource can be linked with a lease time so that it can be reassigned to another user if needed. This resource can then be blacklisted if the user misbehaves.

The difficulty then is choosing the proper resource to use to identify users. Most systems use email addresses to identify users. Emails can be registered anonymously to anyone which makes them easy to attain. They do however create something of an identity. Some systems merely ask users to choose a name and that becomes their identity. It’s not backed by anything so is anonymous but it can then be easily created as many times as needed. Other systems require some form of puzzle or computational problem be solved to prove authenticity. This is being utilized more in the form of capchas and graphical images.

The authors also suggested a method of using private/public keys. Users can create SSH style keys that can be used only by them but do not leak any information about them. These must be secured cryptographically which makes it very difficult to reverse identify them.

Defining when a user misbehaves is also a very difficult process. There are many automated systems that can do this to some degree. One example that the authors gave is with forums and their filters. Most forum systems have some system for filtering what members can post and say. If they post inappropriately too many times they can then be banned. Anyone that has spent any amount of time on a forum knows that this filter can be bypassed very easily by just changing the spelling of explicit words so that they are still understandable but missed by the filter.

This is where the idea of Moderators come in. Humans can much more easily define what constitutes a violation of rules. The big problem with using people to detect wrong doers is that it doesn’t scale well. As the scale of the system grows more people are needed to moderate the users.