Problem:
We want to develop trust in the enforcement of security goals across many machines on an Internet scale, but fear of malicious administrators, compromised machines, and unwitting leaks of sensitive data make this difficult. Additionally, the complexity of operating systems makes it difficult to say anything meaningful about the security of another system in a traditional setting.

Our goal is to achieve the guarantees of a reference monitor (tamperproof, completely mediated, simple enough for verification) in a distributed setting. We would like to establish a coalition of virtual machines within which we can make some guarantees about the security of communication and the enforcement of policy. This coalition will be governed by a central authority, called a Shamon to enhance scalability and accommodate dynamic changes to the coalition.

Shamon
A central authority, or Shamon, will be used to manage attestations of the code that runs the VMM.

Current Work
First, we will create usable attestations that can easily be transmitted and checked by principals in the system. To do this, we will be using Bloom filters to reduce the space required for attestations and the complexity required to check them. This helps to make the size and possible values of an attestation manageable.

Then, we will combine these attestations with hooks added to IPsec's dynamic key negotiation to automatically pass attestations over IPsec. By doing so, we create trusted, labeled channels over which coalition members can pass information, hypervisors can negotiate trust, and all members can communicate with the Shamon to receive dynamic updates to the state of the system.

Once this framework is in place, we will use this to create a trusted VNC system in which users can use any untrusted client machine and know that the only way they will be allowed to connect to their VNC session is if the client machine is running "good" software.

Sponsored by IBM Research