Security Profiles

```
   +----------+          SNMP          +----------------+
   | script X |<---------------------->| target systems |
   +----------+        ^               +----------------+
         |             SNMP security profile
         |             (targets and their security parameters)
+----------------+
| runtime system |  <= runtime security profile
+----------------+     (e.g. interpreter restrictions)
         |
+------------------+
| operating system | <= operating system security profile
+------------------+   (e.g. operating system user and access rights)
```

- In order to execute a script securely, you need to know the security profile. A security profile has three components: SNMP + runtime + OS security profile.
- In order to evaluate expressions, you only need to know the SNMP security profile since the expression language does not provide access to things outside of the SNMP domain that need to be secured.
- The SNMP security profile includes the access rules to the local MIB as well as the SNMP security parameters that can be used to access target systems.

Actors and Views in a DISMAN Application

```
                +------------------------------------+
  security      | +------------+ +-----------------+ |
administrator --+>| admin view | |  script owners  |<+-- script owner
                | +------------+ |      view       | |
                |                +-------+---------+ |
                |                        ?           |
                |                +-------+---------+ |
                |  distributed   | script invokers |<+-- script invoker
                |    manager     |      view       | |
                |                +-----------------+ |
                +------------------------------------+
```

- The security administrator establishes and controls the security policy of a DISMAN application.
- The script owner installs scripts and defines the security policy for the script under the rules of the security policy.
- The script invoker starts script execution. He might have its own security restrictions under the rules of the security policy.
- The script owner and script invoker can be the same or different identities.

Design Goals

- Understand the security implications of DISMAN applications. Provide guidelines how to deploy DISMAN applications in a secure way.
- The required security mechanisms should work with the SNMPv3 VACM access control model. Ensure that it is easy to establish "reasonable" VACM access control rules to secure DISMAN applications.
- The model should support three different models of script invocation:
  1. script owner == script invoker
  2. script owner != script invoker, script uses security profile of script owner
  3. script owner != script invoker, script uses security profile of script invoker
- Allow a script owner to install scripts to run under his security profile ("setuid") without having to consult the security administrator.
- Allow a script owner to further restrict the security profile for "setuid" scripts.
- Make the security profile information explicitly available to simplify the security administration instead of relying on security checks inside scripts.
- The security mechanisms should not make any assumptions about the security configuration of target systems.
- However, guidelines should emphasize that a consistent security policy and security configuration in a management domain makes it much easier to avoid security configuration problems.