Safe Base

Safe Base

- Goals of the Safe Base
  - Auto-Loading and Package mechanismns
- When to use the Safe Base
- Problems of the Safe Base
- Extending the Safe Base
- Alternative Ways
- Questions

Goals of the Safe Base

- Execute untrusted scripts safly.
- Provide access to
  - Installed packages
  - [auto_load]ed commands
- No information about the underling paths
- Provides a safe subset of [file], [source], [encoding], [load], [glob] and [exit]

auto_load

- Information is in a file called tclIndex.
- Searched in the $auto_path
- 2 different format exists
  - An old one that have to be parsed
  - A new one that is a valid Tcl file
  - Only the new one can be used with the safe base
- Specifies a script that is executed, usually source or load.
- Stores the scripts in the auto_index array
- See init.tcl

pkgIndex.tcl

- Information is in files called pkgIndex.tcl
- Searched in $auto_path and one descendant
- Valid Tcl file.
- Can be complex logic (see the pkgIndex.tcl for mysqltcl or twapi)
- pkgIndex.tcl usually invokes [package ifneeded]
- See package.tcl

Tcl Modules

- Information is extracted from the filenames
- Searched in [::tcl::tm::list]
- :: is translated to /
- See tm.tcl

When to use the Safe Base

- Plugins
  - Usually not own code
  - Tcllib has a module for it
- Testing untrusted code
- Extra encapsulation (e.g. for the ftpd)

Extending the Safe Base

- A safe interp could have more trust.
- Add a safe subset of
  - [open]
  - [socket]
  - [glob]
- Example: Tcl Plugin

Problems of the Safe Base

- Does not prevent DoS (e.g. big integer calculations)
- Adding paths to the auto_path not possible
  - Breaks tcllib – Workaround: [catch {package require doesnotexist}]
- Documentation out of Date
- Tcl Modules require [glob]
  - [glob] is a hairy monster.
  - Abitiary deep paths have to be added to the access_list
  - Try [package require random] in a safe interp.

Alternative Ways

- Complete VFS
  - Does not break tcllib.
  - [glob] is still a hairy monster
  - Easier to extend the rights of the slave.
  - Example http://johannes13.de/safe.tcl
  - Comm server runs currently on 192.168.2.118 1234 in EuroTcl-1
    - [package require comm]
      [comm::comm send {192.168.2.118 1234} {set foo bar}]
    - Please don't do large integer calculations.

Alternative Ways

- Handle TM in the master
  - No [glob] needed - No hairy monster
  - Probably requires a reimplementation of tm for the safe base.
  - Adding a VFS (with [open] & [glob]) is possible.

Questions