

Security Redesign

Security Redesign
AKA 'SRP'
David Mitchell

Security Redesign Project

- What is it?
- Why are we doing it?
- Where is the project?

What Is It?

- Replacement for our authentication server
- Production server based on FWTK.
- Current design proposal uses FreeRadius
- Minimal user visible changes
 - Challenge will not be displayed
- Significant changes on servers and devices

Why Are We Doing It?

- We can't get the VPN to use the current system.
- Current system requires client to display the challenge.
- FWTK is ancient.
 - No longer updated or patched.
- Current CryptoCard plugin is binary-only and fragile

Where Is The Project?

- Test server up and running.
- Major clients have been tested
- Waiting for security staff to sign off on the implementation.

AuthSrv Details

- Current AuthSrv based on FWTK code
- FWTK has it's own on-wire authentication protocol.
- Not included in any known OS or network device by default.
- Installation on Unix using a PAM module written by Craig Ruff
- Custom TACACS server runs which allows network devices to authenticate to it

FreeRadius Details

- Active and growing project
- Includes (almost) native support for our tokens.
- RADIUS is an RFC-defined standard protocol
- Supported by many network devices and OS's
- RADIUS already mandatory and in use for VPN and dialup. Soon for wireless.

Hangups

- Challenge will not be displayed to users by default. Some method to resync (may) be required
- Password is currently stepped when challenge is displayed
- New system only steps password on a successful authentication
- Reduces or eliminates the need for a resync. May allow an attacker to guess a password