ARPA2 Project

http://arpa2.net
http://internetwide.org

Lightening Talk - Open Source WG @ RIPE 72

Sara Dickinson   sara@sinodun.com

The Problem

- A network of networks
- Partitioned in ≈ 300 million domain names
- Services by ≈ 7,000 service providers
    - Plus fine-grained reseller network (SME's)
- Vast majority running their own instance of roughly the same stack
    - an open source web + databaseserver
      + a PHP driven CMS + sendmail or post x

The Problem

- Market forces lead to generic price war
- ISP/hosting providers offerings frozen by inertia
  => bottleneck to introduction of new services
- Platform wars
  - closed, profitable   vs   open, innovative
- User identity = power (now very political)

The Vision

http://internetwide.org/about/mission.html

“ repopulate a decentralised global internet that offers security and privacy by design”

- Provide a ready-made Future Internet Stack for the professional hosting industry
- Use existing technology (proven, deployed standards)
- All essential internet services run in a fully distributed and fully trust-worthy way respecting internet standards, privacy, cultural and linguistic diversity

The Solution

- Is a **drop-in replacement** for current established internet services
- Tailored to the **real world needs** of actual hosting companies
- Is user-aware (in order to scale) and **user friendly**
- **Small margins** -> no room for large investments or high level expertise
- **Standards-based**, **open internet platform,** implements **best practices** such as DNSSEC, IPv6
- Responsibility for 2.7 billion users; robust, secure, audit-able => **trustworthy**

The Project

- Partners:
  - NLnet, open source fund (Michiel Leenaars)
  - OpenFortress, networking & cryptography (Rick van Rien)
  - InternetWide.org - co-ordination of funding

- Development team of 8

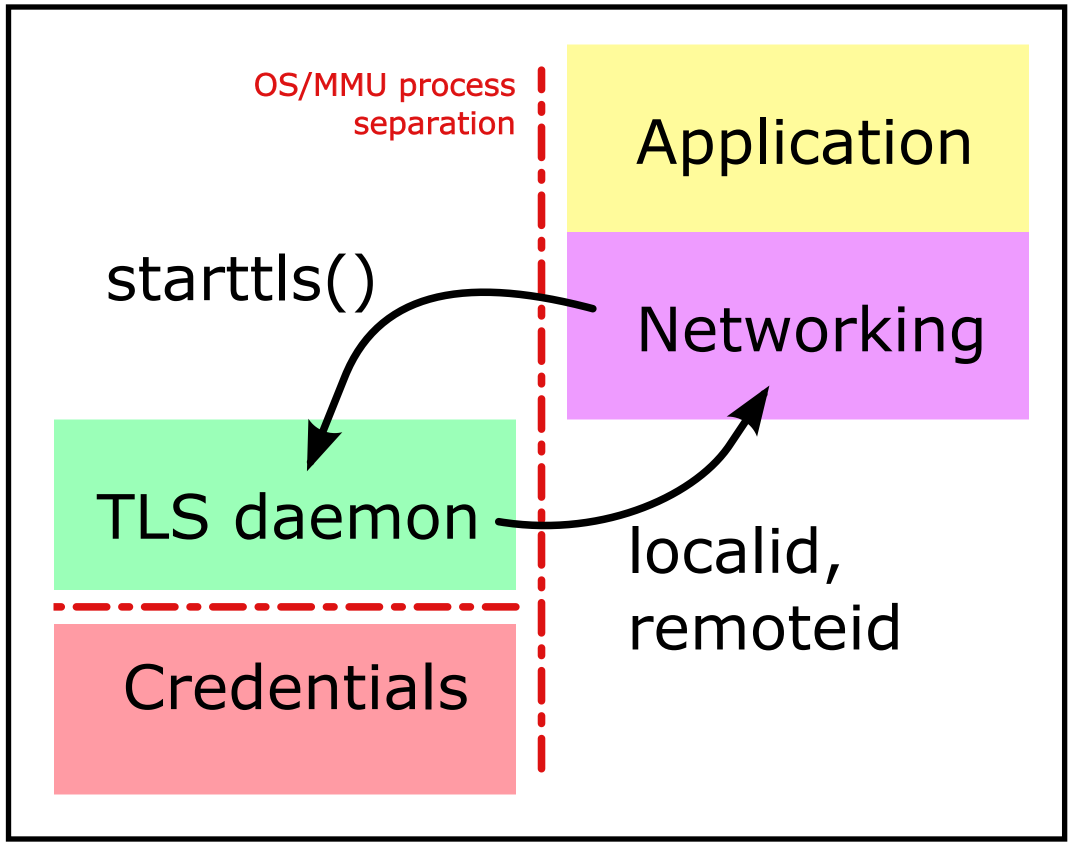
- ARPA2 in 4 phases:
  - SecureHub, ‘usable TLS’
  - IdentityHub, ‘bring your own identity’
  - PluginHub, ‘plugin services for your identity’
  - SocialHub, ‘connect without intermediates’

Phase 1: SecureHub

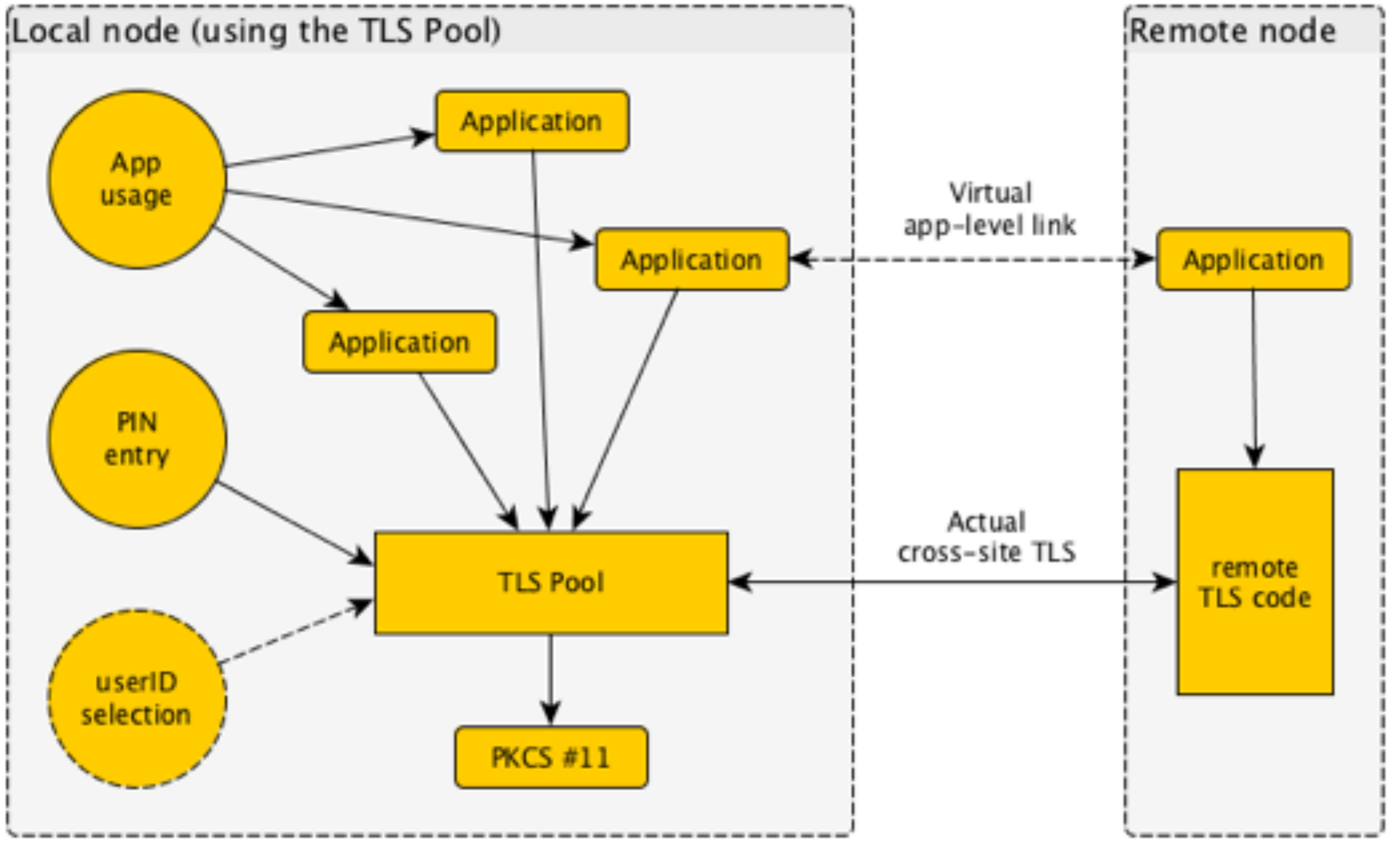
- Cryptographic core protocols
  → TLS, DNSSEC, DANE
  → LDAP for domain-coordinated credentials publication
  → Kerberos security (centrally coordinated)

- Components
  - TLSPool - Manages TLS connections for applications
  - TLS-KDH - Kerberos, Diffe-Hellman and TLS
  - SteamWorks - distribution of configuration information

TLS Pool

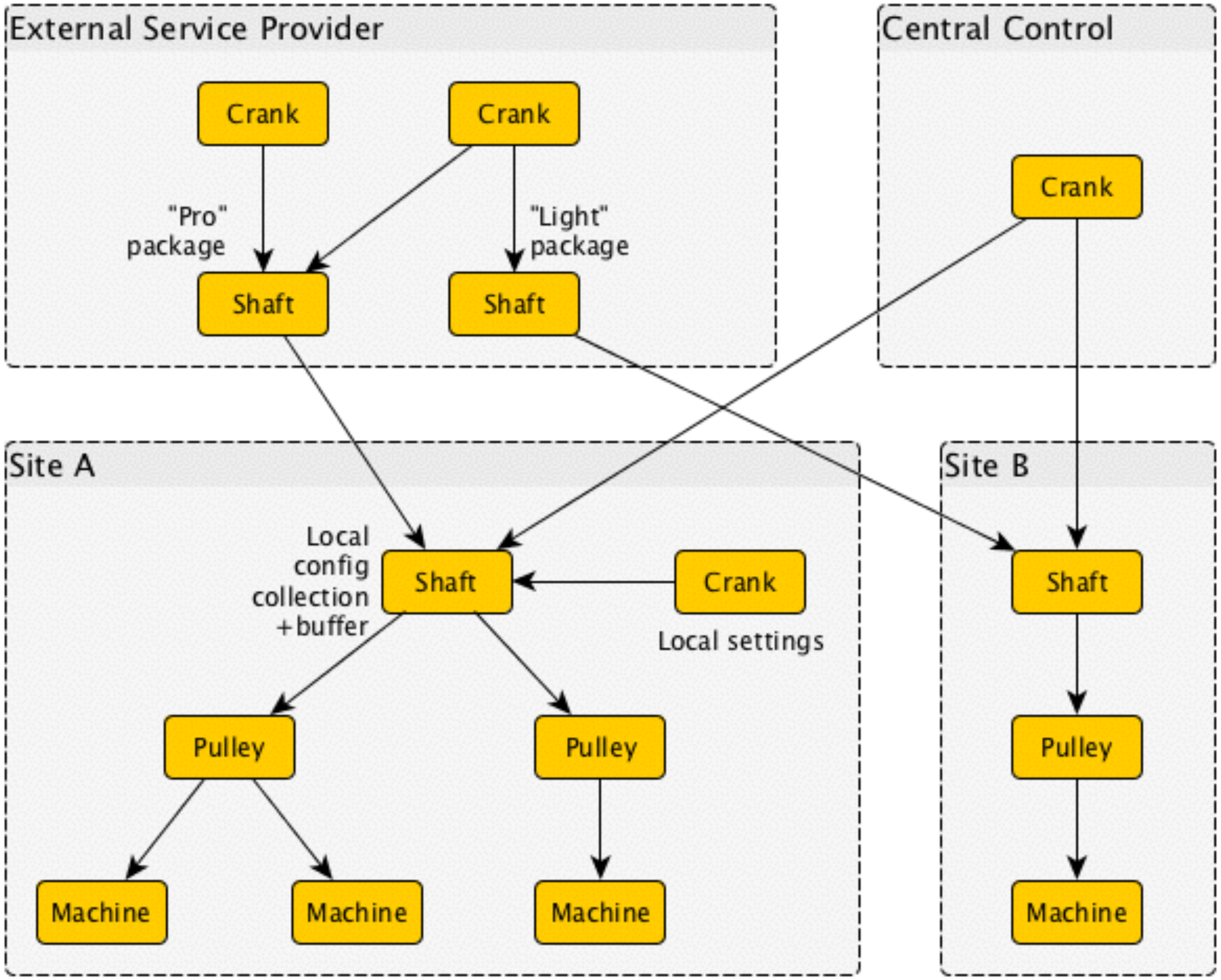


- **TLS daemon** - manages TLS connections and credentials for applications
- TLS policy shared, centralised using LDAP



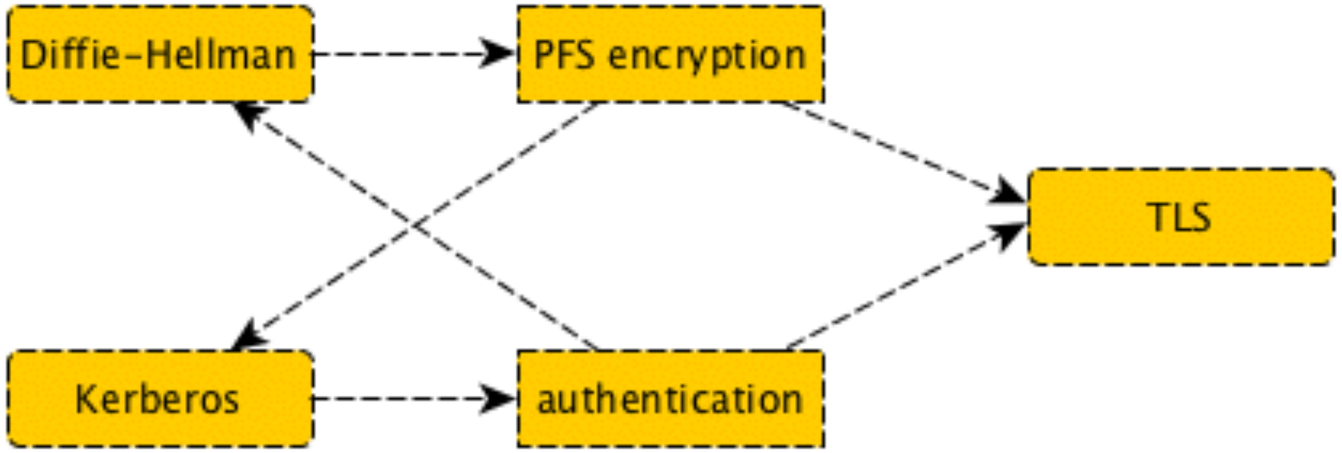
Steamworks

- **Steamworks** - provisioning TLS policy from central site
- CRANK - entry of TLS policy
- SHAFT - combines sources of policy
- PULLEY - delivers policy to TLS Pool



TLS-KDH

- Add support for Kerberos tickets as an authentication mechanism for the TLS protocol, with Diffie-Hellman support for encryption with Perfect Forward Secrecy
- https://tools.ietf.org/html/draft-vanrein-tls-kdh-03
- Currently being implemented in GnuTLS



Future

- Phase 1:
  - Completes July 1st
  - Code in github (Linux/Windows)

- Phase 2:
  - IdentityHub - Identity Management
  - Funding under discussion, interested parties please contact: internetwide@lists.arpa2.org