Kerberos in Embedded Devices

TeamF1’s AuthAgent Kerberos

Mukesh Lulla, TeamF1, Inc.
Who is TeamF1?

Supplier of Embedded Connectivity & Security Software
TeamF1’s Embedded Software Components

Used as building blocks or combined into a complete solution

- **SSHield**
  - SSH1 / SSH2 protocols

- **SSSlimSecure**
  - SSL / TLS protocols

- **V-IPSecure**
  - IPSec and IKE

- **V-IPTF**
  - IP Tunnelling and Filter

- **AuthAgent Kerberos**
  - Kerberos V Agent

- **AuthAgent RADIUS**
  - RADIUS Authentication Agent

- **AuthAgent X.509**
  - Digital Certificate Authentication

- **Switchcraft Merlink**
  - LACP & fail-over

- **NetF1**
  - High Octane TCP/IP, IPV6, VR

- **GrandPPPriv**
  - Multi-Class/Multi-Link PPP

- **FireFly**
  - IP Packet Filtering Firewall

- **GNAT**
  - Network Address Translator
What’s Different About Embedded Kerberos?

- Configuration & Control
- Programmatic Interface
- Cipher Management
- Crypto Lib
- H/W Acceleration
- PRNG
- Universal I/O
- GSS API
- Service & Client Modules
- MIT Kerberos Core
- Custom Subsystems
- CLI Helper Lib
- FIPS Add-on
- Digital Certs
- IDE/Tool Integration
- Reference Apps
- Tasking Model

Open source (MIT & Others)
Open-source with enhancements
TeamF1 proprietary

© Copyright 2009 TeamF1 Inc.
Seamless integration with toolchains and OS + network stack services of various popular embedded platforms

- VxWorks, VxWorks AE, VxWorks ARINC 653
- Mentor Nucleus
- Thread-X with Net-X, US-Net, GHNet
- LynuxWorks LynxOS
- Embedded Linux variants
- Many other Oses (ported or easily Portable to)

Enhanced Memory Management & Partition Support

Drop-in – no special OS or n/w stack source modifications
What Kinds of Devices Use It?

- Devices in enterprise n/w using Kerberos authentication
- Devices using smartcards and industry standards around them (DoD CAC, Packet Cable STB)
- Embedded devices co-existing with networked Windows systems
  - Printers, NAS
  - Corporate routers / VPN terminators, managed switches, Wi-Fi Access Points
- Systems needing high authentication security without the bloat of PKI
  - Building/hospitality network access control, privilege levels etc.
Case Studies

Existing TeamF1 Deployments With Kerberos
Thousands of management modules each managing racks of servers or single server in a datacenter

Need to remotely perform most functions that otherwise require visit to data center, or remote location.

Full "in-front-of-the-server" remote management experience from practically anywhere in the world:
- Includes so-called “Pre-OS” functionality
- Text console and Web (SPNEGO)

Configured to use a directory to authenticate and authorize its users (scalability, security policy enforcement, individual accounts not just roles).

Kerberos used to leverage Windows / AD user credentials
VPN Termination Device

NETGEAR SRXN3205

- SMB-class Unified VPN Firewall Router w/ integrated .11n AP
- Secure Gateway (FW/NAT)
- Unique IPSec + SSL VPN “combo”
- Dual-Band 5.0 / 2.4 GHz .11n
- Business-Class Access Point

Kerberos Used for Windows/Linux Authentication of VPN users
Industrial Process Control

European Industrial Automation Company

- Industrial equipment (sterilization oven)
- Remote authentication of users & services with Kerberos

Kerberos used as common strong authentication between controller and equipment
IPv6 Secure “Gateway”

Cryptek NetGard Family

- IPv6/IPv4 router with CAC (smartcard) authentication
- Straddles network segment between legacy MFDs and LAN
  - Virtual on/off switch for legacy MFDs based on policy
- FIPS certified cryptography and Kerberos/PKINIT authentication

Kerberos + X.509 (smart card) + LDAP authentication
Embedded Kerberos: Looking Ahead

More Proliferation of Kerberos in the connected device world

- Security more on the minds of embedded device makers
  - Partly a result of compliance checks and govt regulations

- Hoping for better integration with network security protocols – IPsec, SSL

- Using Kerberos with WiFi devices
  - Kerberos use in captive portals as alternative to 1x
  - Use Kerberos authentication in preference to native derived key authentication in 11i (especially important for constrained clients)

- Promote the use of Kerberos in industry standards
  - Particularly in constrained environments where PKI is not an option