Kerberos in Embedded Devices

TeamF1's AuthAgent Kerberos

Mukesh Lulla, TeamF1, Inc.

Enabling Embedded Innovations

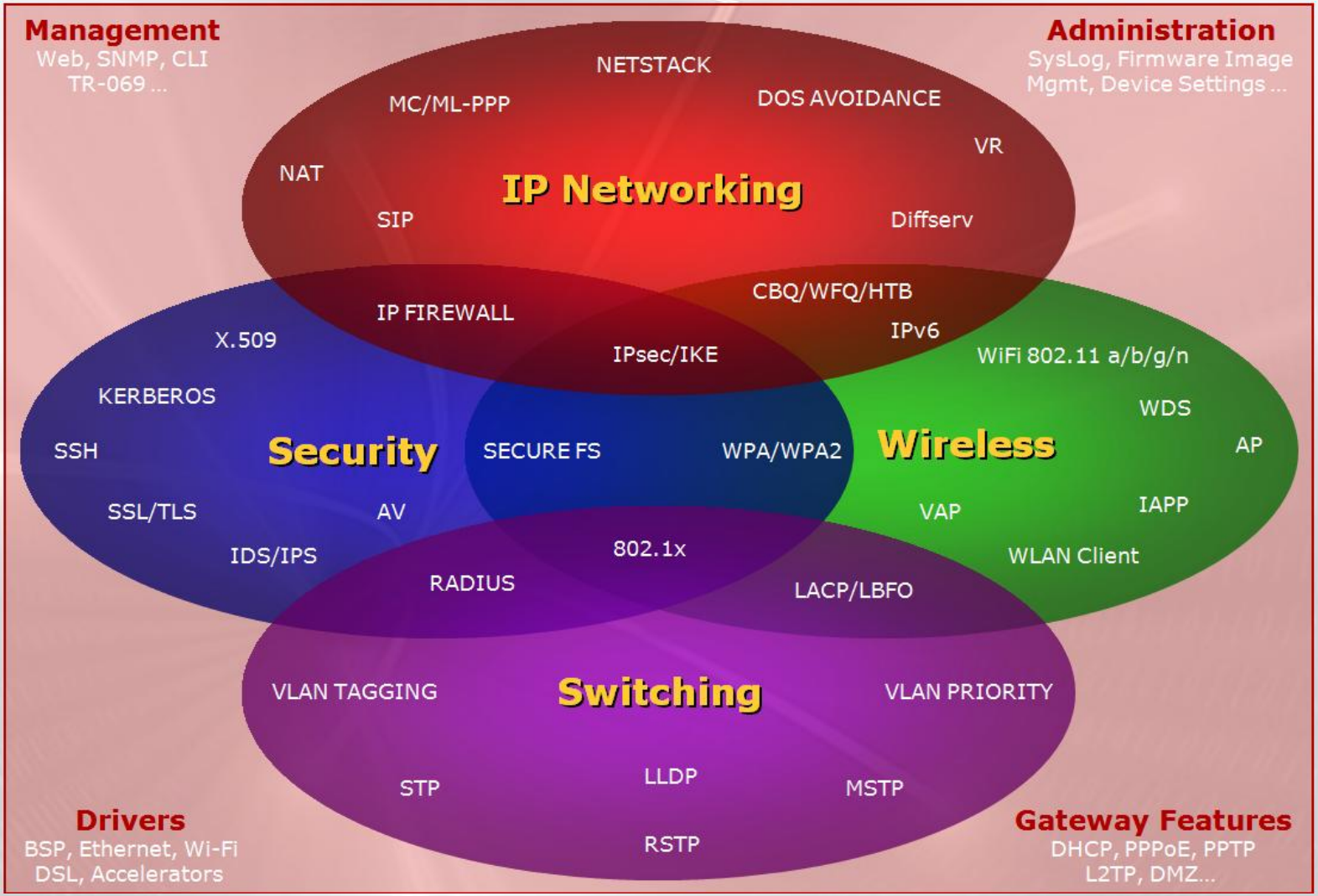
© Copyright 2009 TeamF1 Inc.

Who is TeamF1?

Supplier of Embedded Connectity & Security Software

© Copyright 2009 TeamF1 Inc.

TeamF1's Technology Footprint



© Copyright 2009 TeamF1 Inc.

TeamF1's Embedded Software Components

Used as building blocks or combined into a complete solution

SSHield
SSH1 / SSH2 protocols

AuthAgent Kerberos
Kerberos V Agent

Switchcraft Merlink
LACP & fail-over

NetF1
High Octane TCP/IP, IPV6, VR

SSSLimSecure
SSL / TLS protocols

AuthAgent RADIUS
RADIUS Authentication Agent

Spantasmic
STP, RSTP, MST

GrandPPPrix
Multi-Class/Multi-Link PPP

V-IPSecure
IPSec and IKE

AuthAgent X.509
Digital Certificate Authentication

X-Calibur
IEEE 802.1X

FireFly
IP Packet Filtering Firewall

ASAP / SAS
Air Secure Access Point & Client

AuthAgent TACACS+
Embedded Tacacs+ Clients

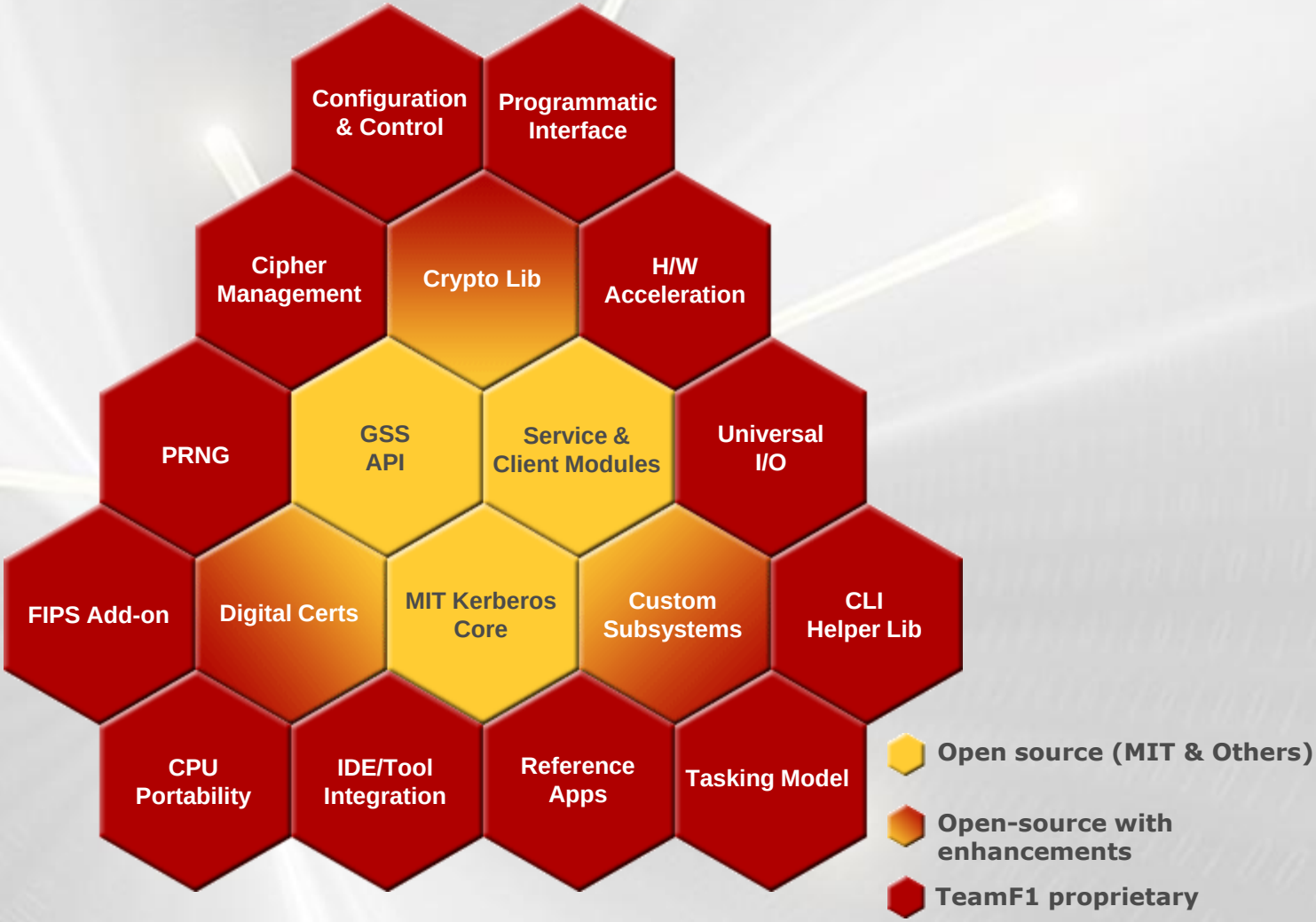
ClassHopper
Alternate Queuing Disc

GNAT
Network Address Translator

TeamF1 INC.
Enabling Embedded Innovations

© Copyright 2009 TeamF1 Inc.

What's Different About Embedded Kerberos?



TeamF1 INC. Enabling Embedded Innovations

© Copyright 2009 TeamF1 Inc.

Tight Integration With Embedded OSes

- 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

© Copyright 2009 TeamF1 Inc.

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.

© Copyright 2009 TeamF1 Inc.

Case Studies

Existing TeamF1 Deployments With Kerberos

Enabling Embedded Innovations

© Copyright 2009 TeamF1 Inc.

Management Module for Datacenter Servers

Large Datacenter Server Manufacturer

- 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

© Copyright 2009 TeamF1 Inc.

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

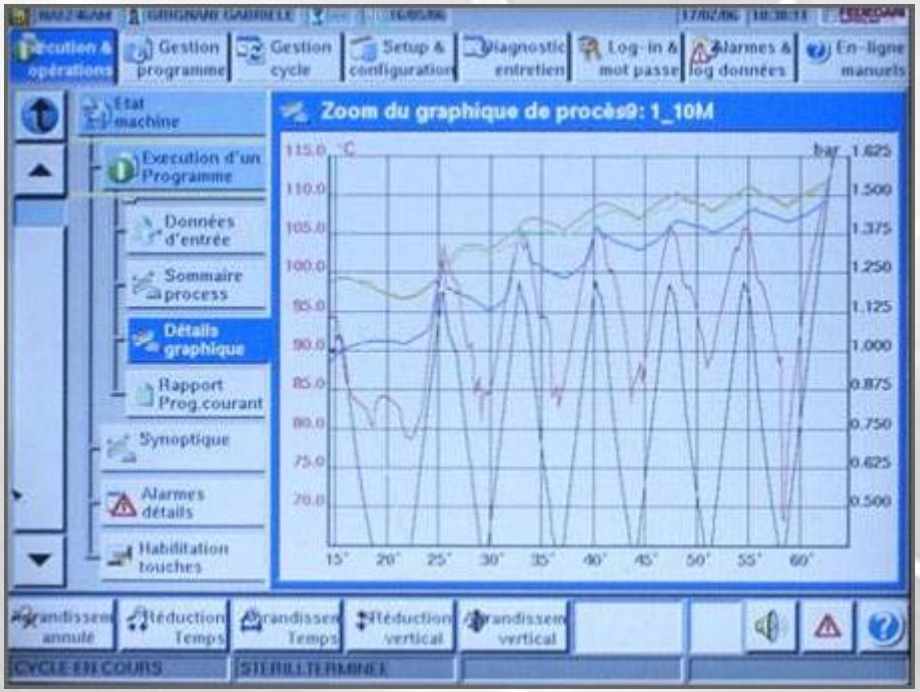
TeamF1 INC.
Enabling Embedded Innovations

© Copyright 2009 TeamF1 Inc.

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

© Copyright 2009 TeamF1 Inc.

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

TeamF1 INC.
Enabling Embedded Innovations

© Copyright 2009 TeamF1 Inc.

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

© Copyright 2009 TeamF1 Inc.

TeamF1 Overview

www.TeamF1.com

info@TeamF1.com

www.TeamF1.com/products.htm

Phone: (510) 505-99F1 (9931)

Enabling Embedded Innovations

© Copyright 2009 TeamF1 Inc.