NMRG 2015 Ottawa

Secure Routing

J. William Atwood
Ronald Brash

Computer Science and Software Engineering
Concordia University

Different approaches to routing

- Intra-AS routing
  - Interior Gateway Protocols (IGPs)
    - OSPF, IS-IS
  - All under one “administration” (more or less)
  - Shortest-path routing
- Inter-AS routing
  - Exterior Gateway Protocols (EGPs)
    - BGP
  - Many policy or contractual issues
  - Preferred routing tends to be defined by lawyers, not network personnel

Security

- Justification
  - IAB Workshop on “Unwanted Internet Traffic”
    - Section 8.1 “A simple risk analysis would suggest that an ideal attack target of minimal cost but maximal disruption is the core routing infrastructure.”
    - Section 8.2 calls for “[t]ightening the security of the core routing infrastructure”.

Main steps

- Increase the security mechanisms and practices for operating routers (OPSEC)
- Clean up the Internet Routing Registry [IRR] repository, and securing both the database and the access, so that it can be used for routing verifications (Liaisons from IETF to others)
- Create specifications for cryptographic validation of routing message content (SIDR)
- Secure the routing protocols' packets on the wire (KARP)

Generic Security Threats: RFC 4593

- Generic Routing Protocol Threat Model
  - Threat sources
  - Threat consequences
- Generally Identifiable Routing Threat Actions
  - Deliberate exposure
  - Sniffing
  - Traffic analysis
  - Spoofing
  - Falsification

Issues with Existing Cryptographic Protection: RFC 6039

    - Weaknesses of MD5 and SHA-1/2 are discussed
    - Technical and management issues are identified

- Protocols reviewed
    - Open Shortest Path First Version 2 (IPv4)
    - Open Shortest Path First Version 3 (IPv6)
    - Intermediate System to Intermediate System Routing Protocol
    - Border Gateway Protocol (BGP-4)
    - Routing Information Protocol (RIP)
    - Bidirectional Forwarding Detection (BFD)

Validating the Contents: SIDR

- BGP is specified by IDR WG
- BGPsec is specified by SIDR WG
- Goal is to permit validation of the ***contents*** of the exchanges
- BGP uses TCP-MD5 or TCP-AO to ensure that the exchanges are authentic and have not been altered

BGPsec

- An extension to BGP that provides improved security for BGP routing
- Motivation
  - BGP does not include mechanisms that allow an AS to verify the legitimacy and authenticity of BGP route advertisements
  - Vulnerability analysis RFC 4272
  - Resource Public Key Infrastructure (RPKI) provides a first step

Validating the Exchanges

- "How to do security" is specified in each protocol specification document
- These specifications typically cover
  - Authenticity of sender
  - Integrity of the packet

Current practice for validating exchanges

- No security
  - The security features of the routing protocol are never activated.
- -OR-
- Install and forget
  - Put a shared key in place
  - Leave it unchanged for 5 years or more, until the router is replaced

Why?

- Operational Issues
  - Changing an active key requires coordinating both ends of the link
- Key rollover is a disaster
  - Usually results in breaking (and re-establishing) an adjacency
  - User data packets are lost during this process
- The (potential) loss of revenue from the lost packets is seen as more of a problem than the (potential) fallout from a security breach

Our goal

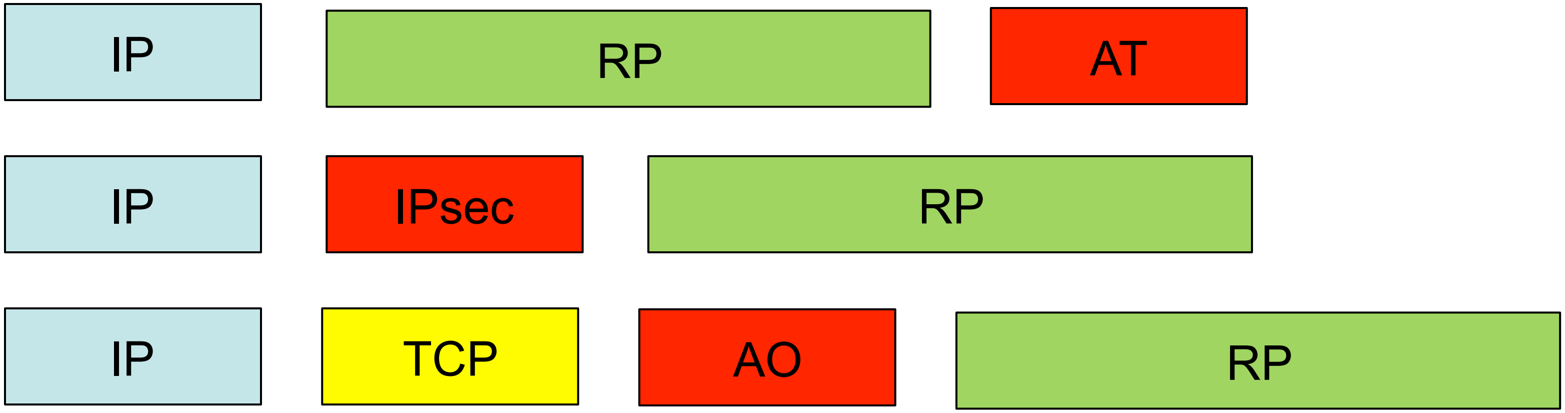
- Changes to this “install and forget” mindset will only come when the new approach is also “install and forget”, but provides improved security
- Incremental deployment is essential. There has to be a benefit when installing these ideas in mixed environments (no change for existing devices plus new approaches for new devices)
- Our goal is to develop a new methodology that provides these security advantages even when incrementally deployed

On-the-wire Security Methods

- Security is achieved at various levels, depending on the Routing Protocol
- Typical Approaches
  - Authentication Trailer
  - IPsec
  - TCP-MD5, TCP-AO

Comparison

- ❑ Authentication Trailer
- ❑ IPsec
- ❑ TCP-AO (or TCP-MD5)



IP RP AT

IP IPsec RP

IP TCP AO RP

Examples

List of Protocols that use specific techniques

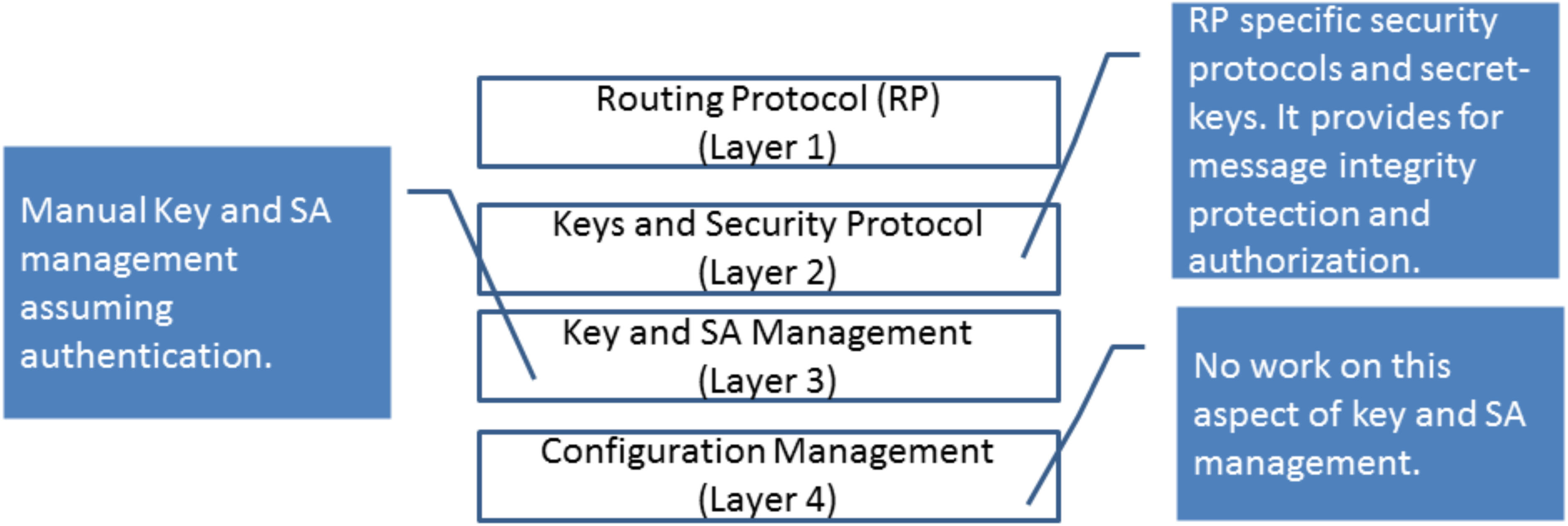
Routing Protocol	Key Scope	Communication Type	Security Feature	Standard
BGP	Peer Keying	Unicast	OoB	TCP-AO
RIPv2	Group keying	Multicast	Built-in	AT
OSPFv2	Group keying	Both	Built-in	AT
OSPFv3	Group keying	Both	Built-in	AT
OSPFv3	Group keying	Both	OoB	IPsec
PIM-SM	Group keying	Multicast	OoB	IPsec

AT: Authentication Trailer
OoB: Out of Band
Both: Unicast and Multicast

Router Configuration (Network Device Config)

- Manual
- Simple Network Management Protocol (SNMP)
- XML forms (XACML)
- NETCONF and YANG

Layers of Configuration Management



Routing Protocol (RP) (Layer 1)

Keys and Security Protocol (Layer 2)

Key and SA Management (Layer 3)

Configuration Management (Layer 4)

Manual Key and SA management assuming authentication.

RP specific security protocols and secret-keys. It provides for message integrity protection and authorization.

No work on this aspect of key and SA management.

Notes

- There have been some proposals for automated key management (as shown later)
- There is lots of work on general configuration management for network devices
- We can find no reported work on configuration management for security in routing protocols

Routing and Security

- ❑ Routing Protocol documents tend to have poor or outdated “Security Considerations”
- ❑ All IETF documents have to be reviewed by the Security Directorate (part of the Security Area)
- ❑ Problem: How to ensure progress on the security side, without “intimidating” the Routing Area personnel
- ❑ Joint agreement between the Security ADs and the Routing ADs: KARP Working Group

KARP Documents

- Overview, Threats, and Requirements
  - RFC 6862
- Design Guide
  - RFC 6518
- Gap Analyses for specific routing protocols
  - RFCs 6863, 6952, 7492
- Proposals for Automated Key Management
  - Case1: unicast exchanges
  - Case 2:multicast exchanges

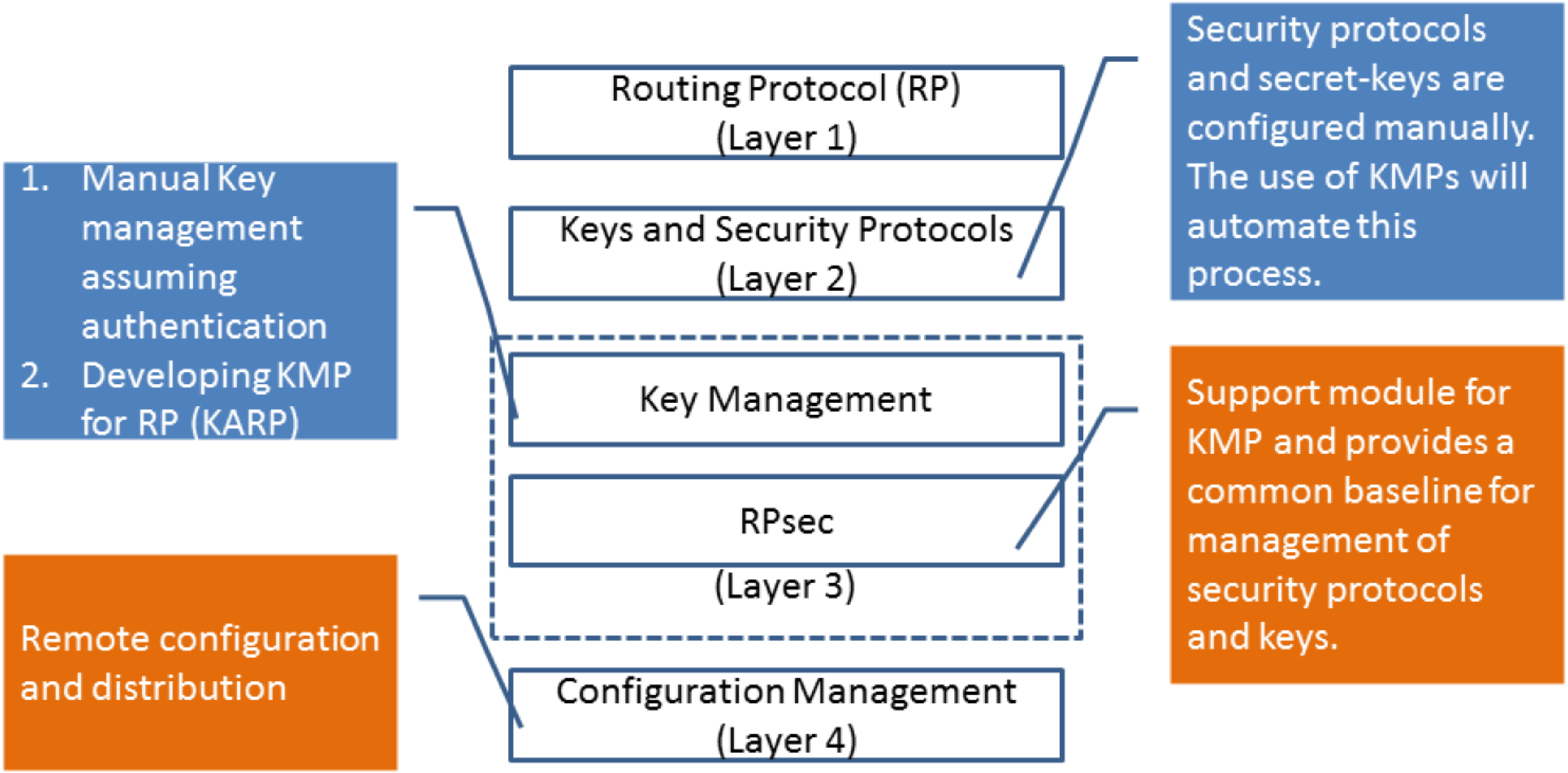
KARP Results

- Goal #1 (Guidelines and gap analyses) was successful
- Goal #2 (Automated keying) failed to attract attention
  - No eyes were found to review the documents
  - No interest in “solutions” that upset the status quo

Requirements

- Has to fit with existing configuration management
- Has to deploy incrementally, i.e., there must be no need to replace any existing box.
- Has to “fall-back” gracefully if a transition/ upgrade fails
- Needs to offer some clear advantage(s) to the operator

Layers of Configuration Management - Revisited



Routing Protocol (RP) (Layer 1)

Keys and Security Protocols (Layer 2)

Key Management

RPsec

(Layer 3)

Configuration Management (Layer 4)

1. Manual Key management assuming authentication
2. Developing KMP for RP (KARP)

Security protocols and secret-keys are configured manually. The use of KMPs will automate this process.

Support module for KMP and provides a common baseline for management of security protocols and keys.

Remote configuration and distribution

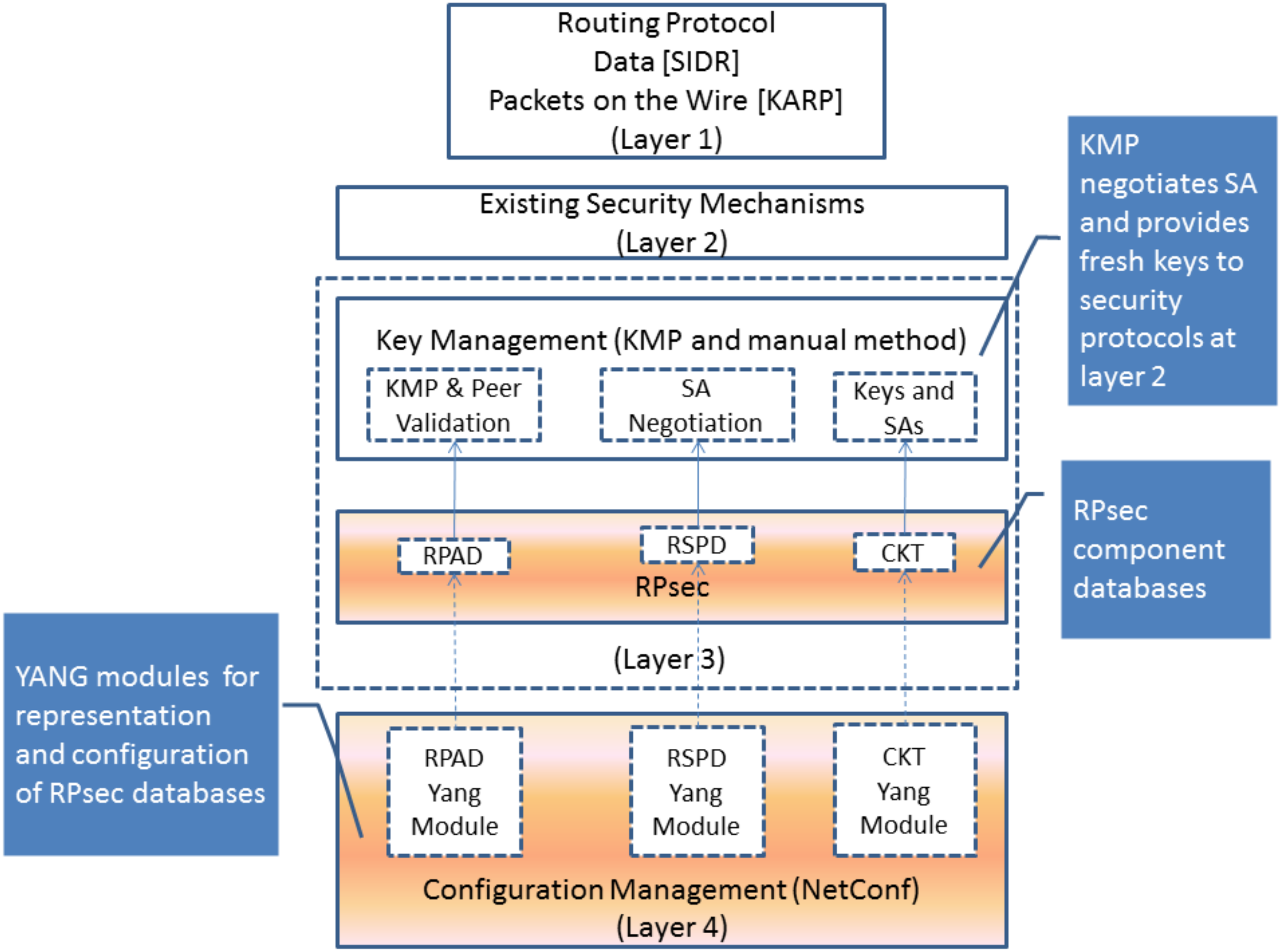
What we have done

- Outlined an overall framework for
  - security management
  - interactions between central controller and individual routers
- Shown the overall framework security
- Used the Crypto Key Table (CKT) (RFC 7210)
- Defined management data structures
  - Router Security Parameter Database (RSPD)
  - Router Peer Authorization Database (RPAD)

..2

- ❑ Defined YANG modules to correspond to:
  - CKT
  - RSPD
  - RPAD
- ❑ Outlined NETCONF procedures to distribute the configuration data (for router security) to devices (i.e., routers)
- ❑ We are beginning to explore deployment issues

Layers of Configuration Management..3



KMP negotiates SA and provides fresh keys to security protocols at layer 2

RPsec component databases

YANG modules for representation and configuration of RPsec databases

Getting the Senior Manager to Understand

- YANG provides a way to model the RPsec databases
- NETCONF provides a way to coherently distribute the configurations (YANG instances) to a set of devices
- Various senior managers have different views of what is important
- How to map from “corporate policies” to individual YANG configurations?

Getting Security Deployed

- Configuration of security is only one aspect of configuration of the overall device
- Any “new” approaches have to fit with existing deployments, and “play nice”.
- It should be easy to leave old equipment in place; it is nice if some of the advantages can be accrued without changing the old devices.
- There has to be a perceived advantage to adding the security, and little or no impact on the existing infrastructure

What we want from NMRG

- Is the 4-layer structure useful?
- Do the two new “databases” provide useful information?
- Is the overall direction of the work useful?
- How can we convince network managers and CTOs that there is a problem here worth solving?

Thank you!

- ❑ Questions?