PktWay Proposed Security Extensions

IETF PktWay (MsgWay) WG

June 24, 1996

Robert T. George

Mississippi State University

Secure PktWay Team

- Work sponsored by the **DARPA** *Secure Heterogeneous Application Runtime Environment (SHARE*HPSC)* project
- **Sanders** (Prime contractor):
  - Jeff Smith, Fred Shirley, Phil Morano
- **Mississippi State University** (Sub-contractor)
  - Anthony Skjellum, Robert George, Thom McMahon
- **MCNC** (Sub-contractor)
  - Greg Byrd
- **Myricom** (Secure PktWay architecture design)
  - Danny Cohen

Secure PktWay Goals

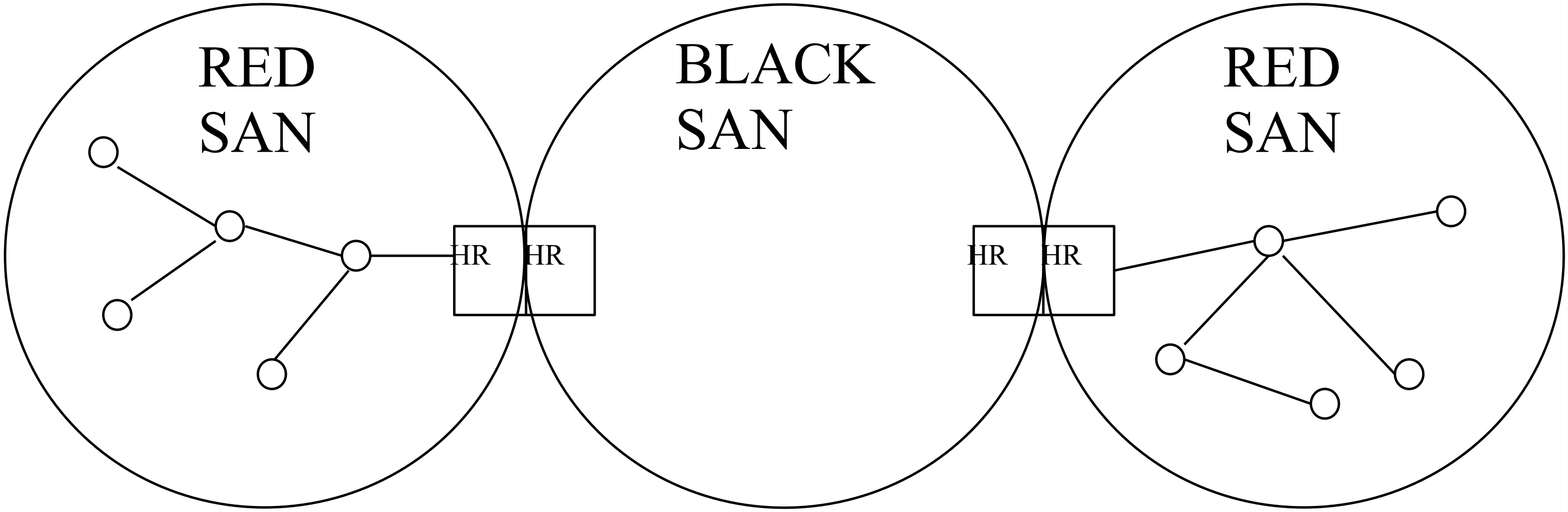
- Provide secure PktWay communication between trusted SAN’s
  - Route data across untrusted SAN’s
- Make minimal, non-intrusive changes to PktWay

Secure PktWay Routing

- Packets from a red (trusted) SAN are encrypted and encapsulated into black PktWay ODB’s
  - Relies on PktWay L3 forwarding
- L2 forwarding is *not* allowed
  - Routing information internal to red SAN’s must not be exposed to black SAN’s

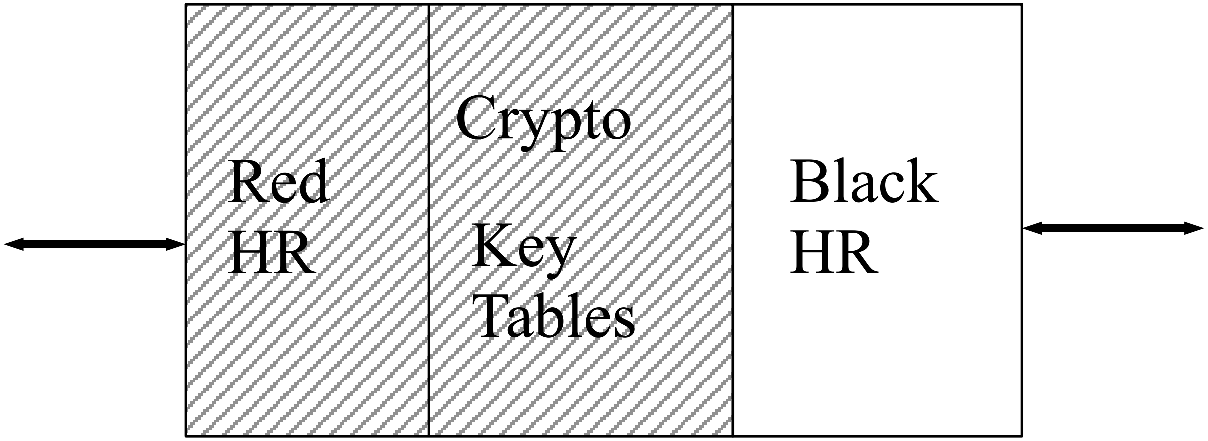
Secure PktWay Architecture

- Red/Black SAN’s:



Secure PktWay Router

- Red/Black HR:



Proposed PktWay Security Extensions (I)

- Additional *Secure* Packet Type
- Additional Optional Headers for each Encryption Method
- Additional *SCID* (Security Context ID) Symbol

Proposed PktWay Security Extensions (II)

- Two additional RRP message types
- Additional RRP record for authentication
- Additional Node Capability for encryption
- Two Additional error messages

Secure PktWay Packet Type

- **Secure** Packet Type:
  - Currently proposed as Code 10
  - Type Extension Field contains key index
- Indicates that PktWay packet contains encrypted ODB
- Requires Optional Header

Secure PktWay Optional Headers

- Optional Header for PT = **Secure**
- Contains parameters necessary for data encryption/decryption
- Encryption parameters are dependent on encryption method

Example: SHARE Optional Header

- SHARE uses DES
  - Optional Header contains long-cycle chaining information
  - Initial Value (IV) is 64-bits

Secure PktWay SCID Symbol

- Symbol address undefined, pending PktWay symbol definitions
  - Used to designate a negotiated *security context* between two SAN’s

Secure PktWay RRP Message Types

- **SCID** RRP Message Type
  - Negotiates Security Context with another router
  - Currently proposed as Code 11
- **MLS?** RRP Message Type
  - Query native security levels from another router
  - Currently proposed as Code 12

Secure PktWay RRP Record

- **AUTH** RRP Record
    - Provides a mechanism for authentication of RRP messages
    - May be useful for ordinary PktWay

Secure PktWay Node Capabilities

- **Secure** Node Capability
  - Node is capable of handling Secure PktWay packets
  - Currently proposed as Code 10

Secure PktWay Error Messages

- **PRIVILEGE** Error Message
    - Indicates insufficient privilege for operation
- **SECURITY** Error Message
    - Indicates incorrect security level
- **KEY** Error Message
    - Indicates unrecognized encryption key

Secure PktWay Status

- Currently being implemented as a variant of MSU’s UDP PktWay implementation
- Implemented as level-C PktWay
  - Requires Node Capabilities

Unresolved Issues

- Relationship with PktWay
    - Additional fields, separate document, RFC?
- Key management
- Dynamic discovery