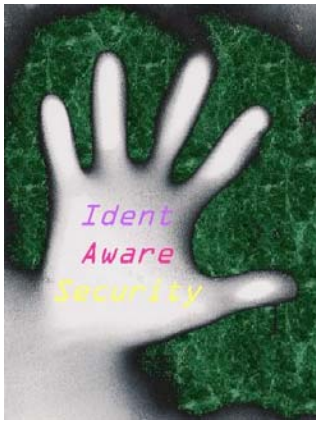
The GSAKMP Application to IP Security



George Gross, IdentAware™ Security
gmgross@IdentAware.com

IETF-60, San Diego, CA

August 2nd 2004

GSAKMP IPsec Documents

- GSAKMP IPsec is specified by two drafts:
  - architecture with application specific payloads
  - GSAKMP IPsec policy token extension
- Both intended for MSEC standards track
- Architecture and GSAKMP IPsec specific payloads are the focus of this presentation
- GSAKMP IPsec policy token draft is still in design/implementation, to be published

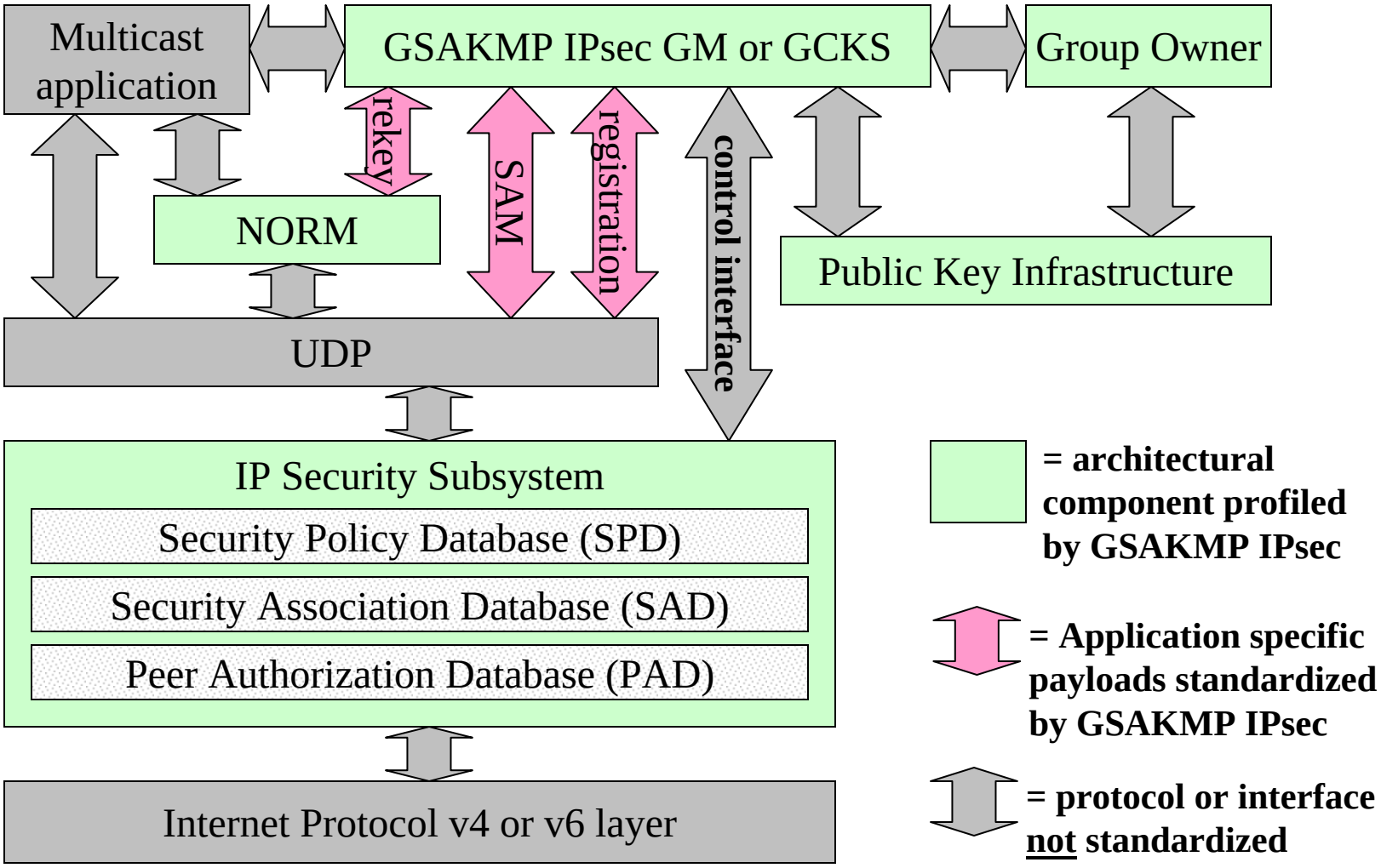
Prerequisite Reading

- draft-gross-msec-gsakmp-ipsec-arch-00.txt
- draft-ietf-msec-gsakmp-sec-06.txt
- draft-ietf-msec-policy-token-sec-00.txt
- draft-ietf-ipsec-rfc2401-bis-02.txt
- RFC3281 - An Internet Attribute Certificate profile for Authorization
- draft-ietf-rmt-pi-norm-10.txt

GSAKMP IPsec Road Map

- GSAKMP IPsec architectural model
- Base GSAKMP profile
- RFC2401-bis IP security profile
- GSAKMP IPsec application specific payloads and IPsec policy token extensions
- Negative-ACK Oriented Reliable Multicast (NORM) for GSAKMP re-key messages
- Public Key Infrastructure profile

GSAKMP IPsec Architectural Model



GSAKMP IPsec Design Goals

- Group Speaker role is a managed privilege
- Do not re-issue the policy token for every change in a Group Speaker's IP address
- Enforce IPsec policy for a permanent "Node Identity" rather than transient IP addresses
  - SSM can handle mobility and NAT gracefully
- Application identity delegates its GSAKMP signature to the Node Identity (e.g. the OS)

Base GSAKMP Profile

- Registration SA uses UDP transport
- Re-key SA uses NORM/UDP/ESP transport
- Cookies exchange proves asserted location
- Verbose mode by default, configurable
- Same Identification types as IKE-v2
- Logical Key Hierarchy re-key required
- Re-key rollover capability required

GSAKMP IPsec Defines Two Application Specific Payloads

- Security Association Configuration (SAC)
  - creates or destroys IPsec Group SA
  - Group SA is constrained by policy token template
  - SAC fills-in the actual parameters to template's formal parameters
- Identity to Transient Address Mapping (ITAM) declares Node Identity => set of IP addresses

GSAKMP IPsec Node Identity

- SPD traffic selectors refer to transient IP addresses, which breaks SSM Group SA
  - This is the well known identity versus locator problem incurred by NAT, mobility, etc.
- GO assigns a permanent IP-v6 globally unique local address for each Node Identity
- Node Identity certificate's SubjectAltName is that identity, encoded as an IP-v6 address

Node Identity (cont'd)

- Node Identity internal structure:
  - Group Owner global identifier prefix, 48 bits as per draft-ietf-ipv6-unique-local-addr-05.txt
  - GSAKMP group sub-net identifier, 16 bits
  - Interface identifier, 64 bits unique across all Nodes managed by the Group Owner
- GSAKMP IPsec policy token's group security association template references Node Identities rather than IP addresses

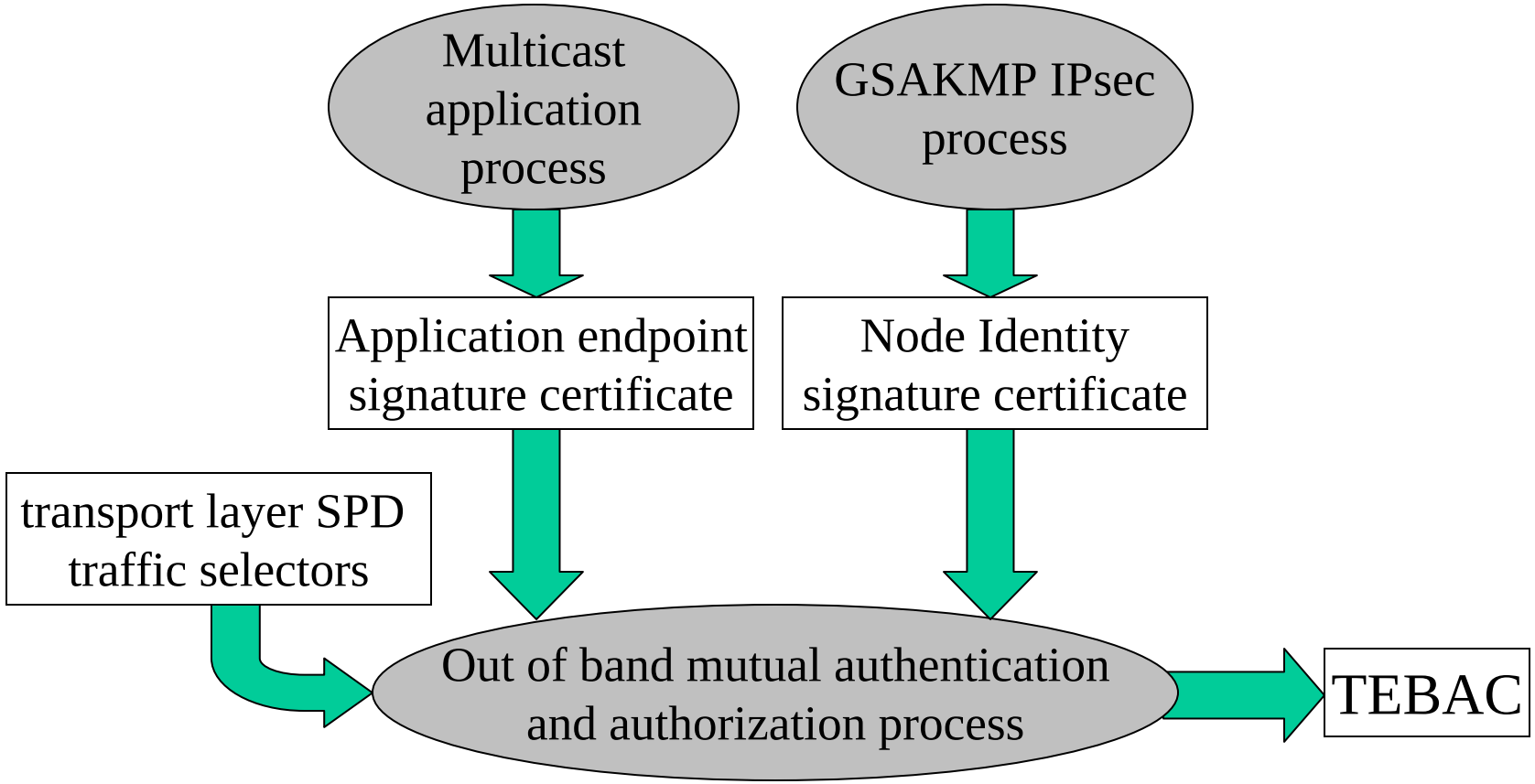
RFC2401-bis IP Security Profile

- RFC2401-bis: ASM and SSM multicast SA, ESP, tunnel mode, IKE-v2 crypto-suite
- Concurrent co-existence with IKE-v2, requires SPD/SAD policy coordination
- SPD/SAD configurable by GO to three dominant multicast service models
- Require multiple speakers with anti-replay
- Multicast Packet Distributor policy action

Security Association Management (SAM) Multicast Message

- Group Speaker creates its Group SA at the Group Receiver endpoints using a SAM multicast
- Group Speaker multicasts SAM after registration:
  - before its first application data transmission
  - after each change in IP address (e.g. mobility)
  - after each re-key event for re-key rollover continuity
- SAM encoded like a GSAKMP message, signed by Group Speaker, and contains Nonce, SAC, ITAM, and TEBAC payloads.

Transport Endpoint Binding Attribute Certificate (TEBAC) Creation



TEBAC Profile on RFC3281

- IssuerName: Application endpoint identity
- Holder: Node Identity
- Use “no revocation” option, timestamp validity period set to expire quickly
- Group attribute type: GSAKMP group id
- accessIdentity attribute type encodes the transport layer protocol and port
  - see GSAKMP IPsec section 9.6 for details

GSAKMP IPsec Registration Protocol

- GM => GCKS messages signed by GM's Node Identity authorized by application endpoint's TEBAC CERT payload
- GCKS Key Download:
  - Group Receiver gets a SAC payload for the Re-Key GSA and each in progress Group SA
  - Group Speaker gets two SAC payloads: speaker's GSA and the Re-Key GSA
- ITAM payload included in RTJ, KDL, RTD

GSAKMP IPsec Policy Token

- Application specific branch under core PT
- Borrows heavily from RFC3585, the IP security policy information model
- Also influenced by the IPsec SPD MIB
  - draft-ietf-ipsp-spd-mib-00.txt
- IPsec PT only defines Group SA templates
  - SAC payload fills-in GSA actual parameters
  - see GSAKMP IPsec section 7.6 for discussion

Examples of IPsec Policy Objects

- Policy filters, a match triggers an action(s)
  - 5-tuple traffic selector filter
  - compound filter: prioritized filters sequence
- Policy actions
  - discard/log packet or allow packet to proceed
  - apply IPsec Group SA processing
  - multicast packet distributor
  - compound action: actions sequenced in a list

GSAKMP IPsec Policy Token Design Issues

- Must coordinate IPsec PT policy with local system's IPsec PAD policy (trust anchors)
- IKE-v2 policy must not collide with GSAKMP, e.g. overlapping traffic selectors
- Multicast packet distributor policy action is a new IPsec subsystem requirement
- Policy token encoding demands one IPsec SPD per system, not one per IP interface

GSAKMP IPsec NORM Profile

- Internet statistics show unacceptable IP packet fragment losses for send and pray
- Reliable multicast transport assures large Re-Key Event message delivery (> 2KB)
- NORM is experimental RFC track, as IESG requires congestion control experience
- GSAKMP IPsec defines a minimal subset of NORM: no file transport, basic FEC

GSAKMP IPsec PKI Profile

- Interprets RFC3280, RFC3281, PKI4IPSEC
- Application end entity signature certificate
  - strive for compatibility with embedded PKI
  - if feasible, align with PKI4IPSEC
- Node Identity certificate is new enrollment
  - GO enrolls Node at GSAKMP installation time
- TEBAC created dynamically as needed for each GSAKMP protocol exchange