Privacy and Security in MPLS Networks

Adrian Farrel
Juniper Networks
afarrel@juniper.net / adrian@olddog.co.uk

www.isocore.com/SDN-MPLS

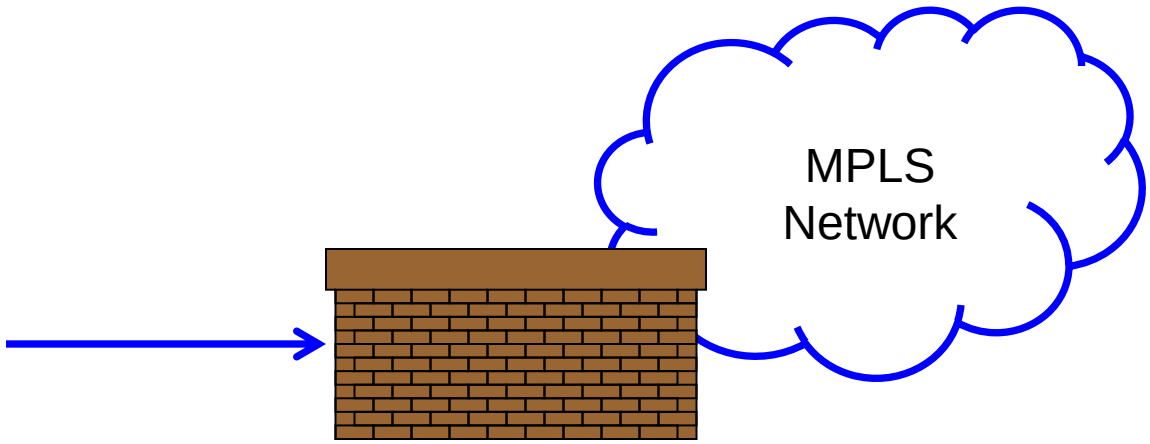
It’s about protecting the network so that it can deliver data and about protecting the data so that it is delivered and not intercepted.

Why Attack an MPLS Network?

- Denial of Service
  - Main vector of attack is the control plane
- Visibility of topology
  - Snoop on the control plane
  - Reveals commercial secrets and openings for DoS attacks
- Diversion of traffic
  - For revenue
  - For easier snooping
  - For replication

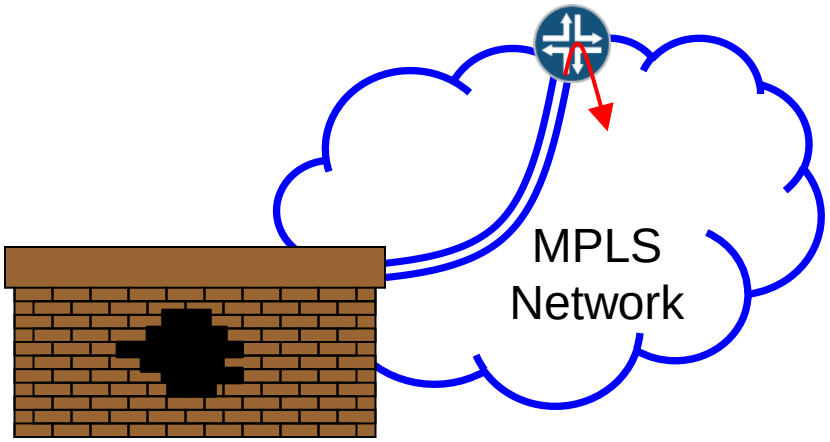
MPLS Control Plane – First Line of Defense

- The MPLS control plane…
  - IGPs, LDP, RSVP-TE, BGP, BFD, *and* management
- Protect the boundaries of the network
- Don't allow packets targeted at any control plane node
  - Only allow management packets by ACL



MPLS Control Plane Vulnerability to Tunnels

- Data plane tunnels punch holes in the walls
- Maybe prevent LSPs (i.e., tunnels) ending at an in-network router
  - But tunnels to PEs are necessary!
- Filter data plane packets as they come out of tunnels



So … Use Control Plane Security

- All of the MPLS protocols include security features
- Some of them are not very robust
  - MD5
  - Cleartext passwords
- There have been some minor holes found
  - For example, no security in LDP Hello messages
- The IETF has been busy fixing things
  - TCP/AO
  - Advice and guidance from the KARP working group
  - Specific fixes and features (MPLS, OSPF, …)
- Security relationships in routing are “hop-by-hop”

Why Don't We Secure the MPLS Data Plane?

- MPLS (and IP) network users take responsibility for securing their own data
  - They do this because the network doesn't offer security
  - And the network doesn't offer security because the user will do it any way
- But there is a serious scaling issue for everyone
  - Internet transactions are "full mesh"
  - That makes for a very large number of security associations to be managed
- Time to put the "P" back into VPN?
  - Unlikely that the customers would trust it

Lawful Intercept

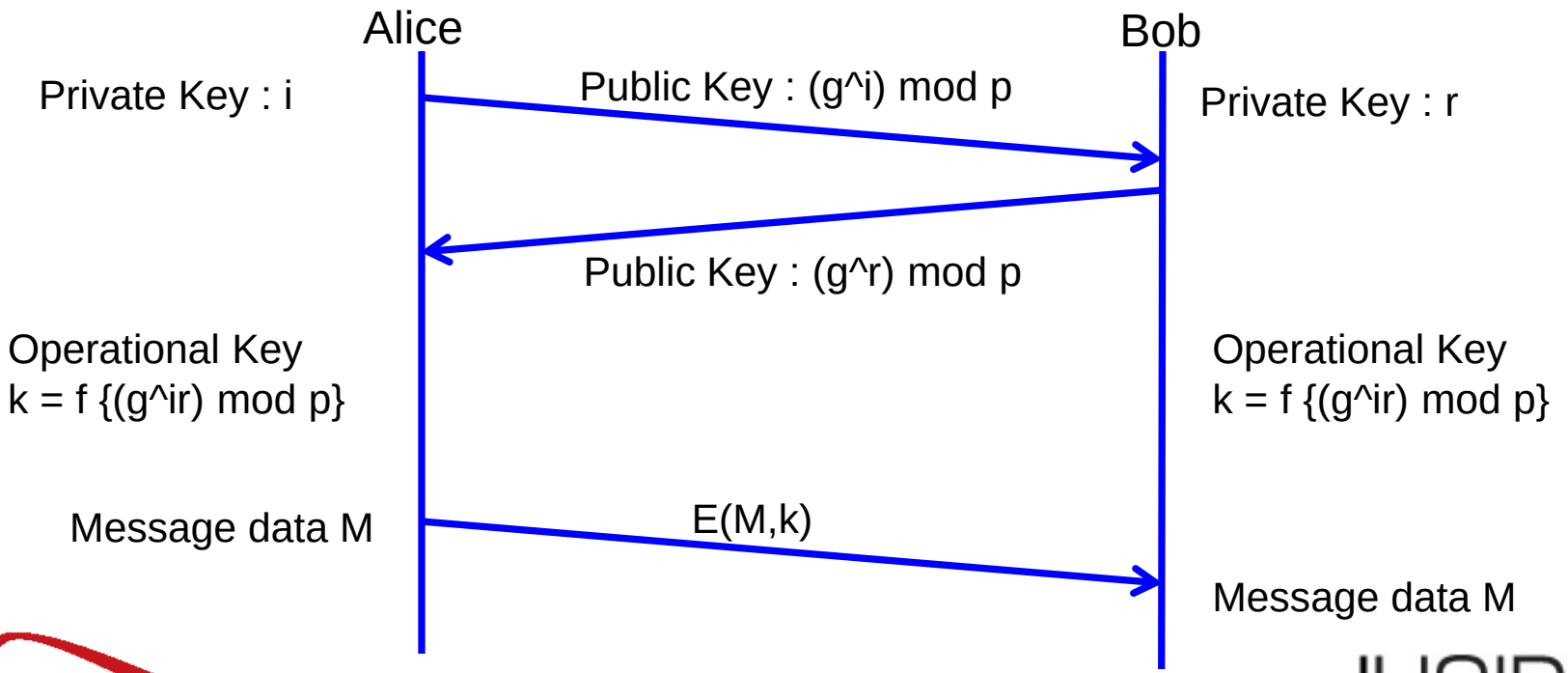
- Lawful intercept is targeted interception of following due process of law
- Traditionally this is applied at the edge of the network
  - Phone tap
  - In Internet speak this is on the CE/PE link
- MPLS encryption doesn't interfere with lawful intercept
  - LSPs don't reach beyond the edge
- Users may still protect their own data using encryption
- Note that this work is ***not*** about Edward Snowden

MPLS Data Vulnerabilities

- We are used to thinking of the network as being “safe” or “trusted”
  - Turns out that data can be extracted from the core
    - Subverted nodes
    - Tapped links
- *Pervasive monitoring is the widespread (often covert) surveillance through intrusive gathering of protocol artefacts* – RFC 7258
- This is an attack that can be performed by
  - Business interests
  - Organised crime
  - Foreign powers
- The end-user might protect their data through encryption
  - Although most do not
- Meta data is usually completely vulnerable
- Most of the data in the core traverses LSPs
  - Leads us to consider MPLS encryption

Diffie-Hellman

- Well known values
  - p : a large prime number
  - g : a number less than p
  - f : a key derivation function
  - E : an encryption function

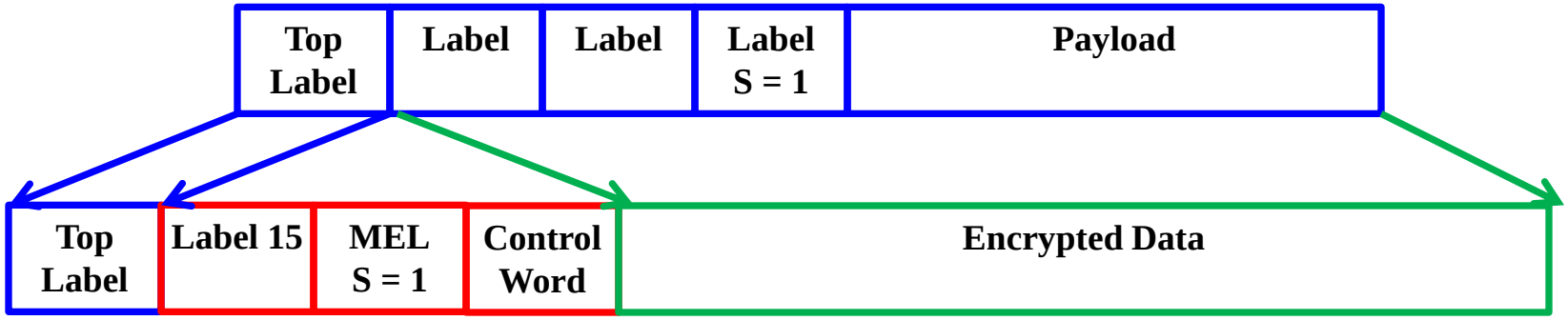


G-ACh Advertisement Protocol (GAP)

- The Generic Associated Channel (G-ACh)
  - "Overhead" associated with an LSP
  - The G-ACh Label (GAL)
    - Identifies special packets on the LSP
    - Packets may be for a number of uses including OAM
    - A "Channel Type" field indicates their use
- The GAP is defined in RFC 7212
  - Exchange capabilities and configuration parameters
  - We can use it for Diffie-Hellman key exchange
    - No control plane signaling (useful if LDP or SDN)
    - Per-LSP control
    - Does not need to be between LSP end-points

Encoding in the Data Plane

- Use an extended special purpose label to indicate encryption
  - Label 15 followed by the MPLS Encryption Label (MEL)
- Use a control word to carry additional info
  - The sequence number to use as the nonce in the encryption algorithm
  - Identifier of key and algorithm to use
- Control word also avoids accidental inspection of encrypted payload



Data Plane Consequences

- The available MTU is reduced by 28 bytes
  - Two labels and a control word = 12 bytes
  - Encrypted data is longer than source data = 16 bytes
- MTU issues can be handled at the LSP ingress
- GAP messages need to be thrown by hardware
  - Can be processed in software
- Encryption and decryption needs to be handled on ingress and egress interface line cards and per LSP
  - Needs to keep up with line rate
  - Needs specialist hardware
  - Transit nodes are not impacted

Continued Vulnerabilities : Key Exchange Failure

- Key exchange failure can be caused by intercepting or corrupting key exchange messages
- Default behaviour must be configurable
  - Ring an alarm bell?
  - Keep trying to exchange keys?
  - Drop back to no encryption?
  - Don’t send any data?
- Similarly, encrypted packets can themselves be attacked

Got to Keep Changing the Key!

- Sequence number is an input to encryption function
- When sequence number wraps key becomes vulnerable
  - This means changing keys at least every 2^64 packets
  - 100Gb is approximately 160 million packets per second
    - 2^44 packets per day
- Change key daily
- But note
  - New key exchanges in the GAP are additionally protected by in-use MPLS encryption

Man In the Middle

Alice

Private Key : i

(g^i) mod p

(g^x) mod p

Bob

Private Key : r

(g^r) mod p

Operational Key
k1 = f {(g^iy) mod p}

(g^y) mod p

Operational Key
k2 = f {(g^xr) mod p}

Message data M

E(M,k1)

Decode
Message data M
Encode

E(M,k2)

Message data M

- Computationally very expensive : must be done in real time
- Can be detected by Alice and Bob sharing public keys out of band

Next Steps?

- MPLS Opportunistic Security is an experiment
  - Does anyone want it?
  - Can it be implemented in the data plane?
  - Is the use of GAP right?
  - Are the Diffie-Hellman and encryption details OK?
  - Is the reduction in MTU OK?
  - How does it interact with OAM?

- draft-farrelll-mpls-opportunistic-encrypt-03.txt
  - Work in progress with Stephen Farrell of Trinitiy College, Dublin

Questions?

afarrel@juniper.net / adrian@olddog.co.uk