Towards a Security-aware Network Virtualization

3rd GI/ITG KuVS Workshop on The Future Internet

Munich 05/2009

Achim Friedland
SONES GmbH / TU Ilmenau
achim.friedland@sones.de
Security Threats in Classical Networks

The diagram illustrates a network consisting of four nodes: Alice, Bob, Carol, and Dave. Dave is marked as an external Mallory attack point. The network is labeled as trusted, with direct connections between Alice, Bob, and Carol. There are arrows indicating attacks from Mallory to Dave.
Security Threats in Virtual Networks

Trusted Network

Alice

Carol

Mallory_{VIRTUAL}

Bob

Mallory_{EXTERNAL}

Dave

Attack!

Attack!
New Security Threats occur...

- Sharing of networking resources with untrusted parties (Mallory_{VIRTUAL})
- Virtualized network equipment might run untrusted or not well understood networking code
- Bitter lessons from practical security: Virtualization boundaries cannot be guaranteed 100%
Basic Idea:

- Reduce the gainable knowledge of an observer
- Lower the impact of an attacker
- Do not disclose end-to-end information
- Do not try to fight an omni-potent attacker
Objectives for a Security-aware NetVirt

- Network Virtualization and Abstraction
- Flow Separation and Aggregation
- Flow Confidentiality and Integrity
- Preventing Traffic Analysis
- Preventing Denial-of-Service
- Scalability
Our Approach…

- Base protocol: Combination of label forwarding and security protocols *(MPLS, IPSec)*

- Allow multiple recursive instances of the base protocol *(ANA Project)*
  (Replace classical network stacks; Enable network abstraction)

- Key management protocol for providing traffic analysis resistance *(Onion Routing)*
Onion Routing uses multiple layers of encryption and authenticity.

Suffers from a high transmission overhead.

Comparable with Strict Source Routing.

Not practicable in large.
Proposed Base Protocol: ELSSA

Extended Label Stream Switching Architecture

Application ICV

Extended Labels (Label Stack)

Transport ICV

Underlay Transport Header
Traffic Analysis Resistance: TASec (1)

- Separate encryption of labels and payload
- Path Encryption: Multiple encryption, but only a single integrity check!
Traffic Analysis Resistance: TASec (2)

- Encryption mode based on *Counter Mode*
- But using an *entangled* encryption scheme
- Constant packet size, less encryption (50%) processes compared with Onion Routing
Conclusion

- ELSSA provides a network virtualization based on a recursive label-switching approach with encryption and authenticity.
- TASec further provides a low-overhead traffic analysis resistance.
- Combination of both meet the proposed requirements.
Future Project Development

• Secure the TASEc against traffic analysis itself
• Release a proof-of-concept implementation (ELSSA-over-UDP/RAWIP)
• Defining more application specific (path management) protocols
Thank you…

- Questions?