

Fig. 2. The ELSSA and TASEC Protocol Stack

protocols like *IPSec* or *IEEE 802.11i* in order to build a powerful framework for further protocol development. We extend these security and privacy concepts of this architecture by defining a key management protocol called *Traffic Analysis Security (TASEC)* which is intended to secure both the confidence and integrity of the transported data and the identity of all members of a communication against external and non-omnipotent internal attackers (fig. 2). We will outline a preliminary protocol design and give a short analytical evaluation of our approach.

## II. OBJECTIVES FOR A SECURITY-AWARE NETWORK VIRTUALIZATION

**Network Virtualization** - The physical links and routers are divided into multiple independent logical links and routers. A secure configuration management must allow on-demand changes by the logical network provider without the need to contact the physical network operator.

**Network Abstraction** - It must be possible to abstract a network path to a single link or multiple routers to a single virtual router. Multiple layers of abstraction and virtualization must be deployable.

**Flow Separation and Aggregation** - It should be possible to differentiate and aggregate the data flows passing a network node in order to forward different kinds of traffic via different virtual networks.

**Flow Confidentiality and Integrity** - A data flow must be secure against unauthorized access and manipulation by external and internal attackers.

**Preventing Traffic Analysis** - A data flow must be reasonable secure against a traffic analysis by non-omnipotent external and internal attackers. To safe from internal attackers the knowledge about the complete logical network and its own importance in this topology should be kept at a minimum.

**Preventing Denial-of-Service** - The network virtualization should not expose targets for denial-of-service attacks. The security of a logical network against attacks within or by other logical networks on the same physical node are of particular importance.

**Scalability** - The system, including means to manage the states and keys, has to scale with the number of network nodes and forwarded data flows.

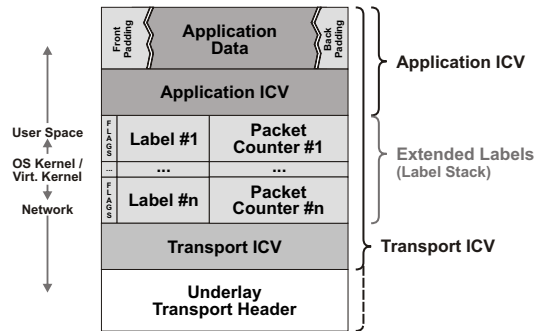


Fig. 3. ELSSA Packet Format

## III. EXTENDED LABEL STREAM SWITCHING ARCHITECTURE

The design of the *Extended Label Stream Switching Architecture (ELSSA)* is based on the well-known idea of packet aggregation, rather than single packet forwarding, and can be compared with the MPLS protocol. Unlike MPLS the intermediate state within the network nodes will not only define forwarding rules, but will also be used to implement security- and privacy-related mechanisms. ELSSA defines *Extended Labels*, which are a combination of a classical *MPLS Label*, an *IPSec Security Parameters Index* and a *packet counter*. The purpose of the *packet counter* is to support the *initialization vector* for encrypting and verifying the packet but also to detect packet lose or reordering which might be of interest for higher layer transport protocols and privacy functions. Two integrity check values can be used to secure the end-to-end application data and the whole packet against unintentional modification during transmission.

Just like the "*Recursive Network Architecture (RNA)*" [3], [4] ELSSA tries to replace the traditional ISO/OSI or TCP/IP layer stack by a very simple base protocol (the extended label) and recursion. If required ELSSA can add multiple layers of abstraction to the actual data flow ("layer stacking") and thus not only replace today's virtual link layers but also network layers, virtual network layers, transport layers and even multiple multiplexing layers within an application.

The packet format of ELSSA is shown in figure 3.

## IV. TRAFFIC ANALYSIS SECURITY

The purpose of the TASEC protocol is to lower the gainable knowledge of an internal attacker analyzing communication patterns by enforcing privacy. Like *MixMasters* or *Onion Routing* this will be deployed by the configuration of forwarding and encryption parameters along the communication path (or paths). While traditional approaches use multiple layers of encryption and thus suffer from a high cryptographic computing effort and an increasing transmission overhead on long paths (fig. 4), TASEC lowers the overall workload by dividing the encryption and integrity

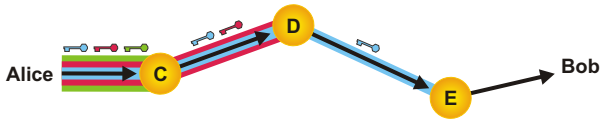


Fig. 4. Multiple layers of encryption lead to a high overhead

check mechanism into multiple separate processes (fig. 5). First the top-most label (without the packet counter) has to be secured, as an attacker must not be able to differentiate or count the number of abstract data flows passing. This "Link Encryption" is done with the help of a security context between the sending and receiving node within the underlay protocol and will not be additionally secured by an integrity check value. The packet counter will not be secured in any way, as its only intention at this point is to detect packet loss. This will not leak more information to an attacker than the attacker could achieve by counting the packets itself.

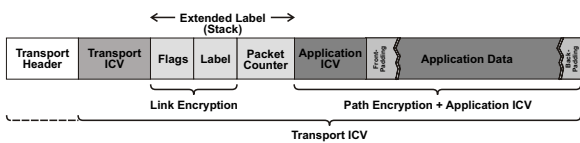


Fig. 5. The ELSSA and TAsEC Protocol Stack

The actual data and maybe upper parts of the label stack, will use a different encryption scheme called "Path Encryption". The base of this scheme is the entangled utilization of *one-time pads* derived from a pseudo random number generator in combination with the packet counter in the top-most extended label (*Counter Mode Encryption* [5]). As figure 6 shows every one-time pad will be used twice along the communication path. This will ensure that the bit pattern will change before it is being forwarded by a network node, which is a requirement for privacy preserving systems [6]. With the help of this encryption scheme the effective size of the transmitted packet is no longer constrained by the length of the communication path which will have a positive effect on the achievable throughput. Additionally the number of crypto operations can be reduced by half compared to the former *Onion Routing* approach which will also foster the transmission throughput and lower its delay.

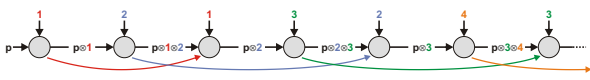


Fig. 6. TAsEC configures an entangled encryption scheme

A remaining problem of this approach is to ensure the privacy of the TAsEC signaling messages. As these messages are sent infrequently and we currently focus on network virtualization there is not much need for very fast signaling of the communication path(s). Therefore the signaling packets may be sent using the traditional *Onion Routing* mechanism without encountering much drawbacks.

## V. RELATED WORK

Network Virtualization and Future Internet is a very agile research area with a lot of very different approaches. Despite this diversity there are although some commons: (1) overcome strict layering (2) experimental cross-layer designs (3) avoiding to reimplement the same functionality at multiple layers (4) experimental overlay designs (5) use of functional protocol entities or protocol heaps. [7], [8], [9], [10] Until now it is still not clearly evident in which direction Future Internet research will evolve.

## VI. CONCLUSION

In difference to common networking approaches the combination of ELSSA and TAsEC is – as far as we known – the only network virtualization approach making use of a light-weight label switching protocol with integrated support of security, privacy, abstraction and recursion. This framework could also be used for the development of new clean-slate Future Internet approaches as it accounts the predefined requirements of *Future Internet* designs given by projects and initiatives like FIND, EIFFEL [7], eMobility [8] and NewArch [9]. However, some issues for this approach remain to be solved. The probably most vital issue is the extension of adoption protocols between ELSSA and routing and transport layer protocols. In order to better understand the effects of network abstraction via recursion the simulation have to be extended to include larger networks with real-life topologies instead of small randomly generated topologies. Last but not least, the delay caused by the need for an explicit path setup signaling has to be reduced. Otherwise ELSSA will not be able to compete with today's transport protocols like TCP or SCTP which solely rely on in-band signaling.

## REFERENCES

- [1] Daniel Mende and Enno Rey, "All your packets are belong to us - attacking backbone technologies," in *Black Hat Europe*, April 2009.
- [2] R. Dingleline, N. Mathewson, and P. Syverson, "Tor: The second-generation onion router," in *13th USENIX Security Symposium*, August 2004.
- [3] J. Touch and V. K. Pingali, "The RNA Metaprotocol," in *IEEE ICCCN (Future Internet Architectures and Protocols track)*, August 2008.
- [4] Wang, Y. Touch, J. and V. Pingali, "A recursive network architecture," Tech. Rep., ISI-TR-2006-626, October 2006.
- [5] Helger Lipmaa, Phillip Rogaway, and David Wagner, "Comments to nist concerning aes modes of operations: Ctr-mode encryption," 2000.
- [6] David Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Commun. ACM*, vol. 24, no. 2, pp. 84–88, 1981.
- [7] Mähönen, Trossen, Papadimitriou, and Polyzos, "The Future Network Society - A White Paper from the EIFFEL Think-Tank," .
- [8] Andersen, Berndt, Ambramowicz, and Tafazolli, "Future Internet - From Mobile and Wireless Requirements Perspective," *eMobility Technology Platform Whitepaper*, 2007.
- [9] David Clark, Karen Sollins, John Wroclawski, Dina Katabi, Joanna Kulik, and Xiyowei Yang, "Newarch: Future Generation Internet Architecture," Tech. Rep., MIT Computer Science & Artificial Intelligence Lab, 2003.
- [10] Marjory S. Blumenthal and David D. Clark, "Rethinking the Design of the Internet: The end-to-end arguments vs. the brave new world," *ACM Transactions of Internet Technology*, vol. 1, 2001.