Secure Overlay-Based Auto-configuration of Complex IPsec VPNs

Michael Rossberg[*,1], Guenter Schaefer[1], and Kai Martius[2]

[1] *Ilmenau University of Technology, PO Box 100565, 98684 Ilmenau, Germany*
[2] *secunet Security Networks AG, Ammonstraße 74, 01067 Dresden, Germany*

Virtual private networks (VPN) offer services for secure data exchange over public networks and are steadily gaining importance for commercial organizations, private individuals as well as governments and military administrations.

However, growing VPN sizes and a dynamic behavior of VPN gateways and clients, e.g., for mobility reasons or perhaps reactions due to denial-of-service (DoS) attacks, make a manual configuration of large, dynamic VPN complicated and expensive. First, the administrative overhead is subject to a quadratic growth with the number of VPN devices, if each VPN device shall be able to communicate with every other VPN device. This will not only lead to higher expenses, but also to more errors introduced by human failure. Second, the robustness of the VPN is not as high as it could be, e.g., in case of partial failures of the transport network some VPN devices could redirect traffic for other devices that cannot reach each other directly anymore. Even though IPsec could support such a resilient behavior by utilizing nested security associations, manual reconfiguration prohibits a timely reaction. Third, manually configured security associations cannot be adopted with sufficient flexibility to support mobile VPNs appropriately. It is impossible to configure security associations between two mobile devices as both regularly change the IP addresses that they are reachable over.

In consequence, a number of diverse VPN auto-configuration approaches have been invented, implemented, and – at least partially – deployed over the last decade. However, many systems are based on hub-to-spoke-like architectures [1,2,3,4], were a central instance represents a potential single-point-of-failure and performance bottleneck. Furthermore, for one system we were able to identify severe security issues [5]. Besides these concerns, it is impossible to dynamically integrate VPN nodes indirectly, i.e., over other nodes of the same VPN, as there must always be a direct connection to the concentrator. However, precisely such architectures are required to realize DoS-resilient as well as mobile topologies.

Additional to the centralized approaches, several specialized, distributed systems exist. However, they either require multicast support in the underlying transport network [6], or use its routing to reactively discover VPN gateways and do not support private address ranges within the VPN [7,8,9]. Some approaches also utilize static VPN topologies in combination with a dynamic routing within the VPN [10,11,12]. Nonetheless, due to the static topology the approaches cannot cope well with DoS attacks, and have a non-negligible configuration effort.

The described deficits of the presented approaches led the development of a novel VPN auto-configuration approach, called Secure OverLay for IPsec Discovery (SOLID). In contrast to the other systems, SOLID [13,14] creates a self-configured VPN overlay with mechanisms for gateway discovery, routing and topology control. Especially the topology control is of large relevance, because the creation of security associations is very time intensive in high security environments due to the use of smart cards. Thus, the number of proactively established associations should be kept at a minimum. In order to still be able to search VPN gateways efficiently, SOLID uses the meanwhile well-understood concept of peer-to-peer overlays [15,16].

*Corresp. author: michael.rossberg@tu-ilmenau.de, Phone: +49-3677-69-4553

First, SOLID's topology control establishes only two security associations proactively to create an ordered ring structure, as illustrated in Fig. 1. Because of the structure, a destination gateway for a data packet can be found by simply sending a search message along the ring. This search requires *O(n)* overlay steps, where *n* denotes to the number of subnets. Thus, a logarithmic number of additional cross-connections are proactively created later on, in order to guarantee a search in a logarithmic number of steps. Besides addtional security properties, this approach only partially differs from Chord or I3 [17].

However, VPN gateways are not ordered by random or hashed identifiers, as this would not allow for a use of variable subnet masks. Instead, the internal IP address ranges are directly used and cross-connections are placed by creating a representative sample of valid address ranges.

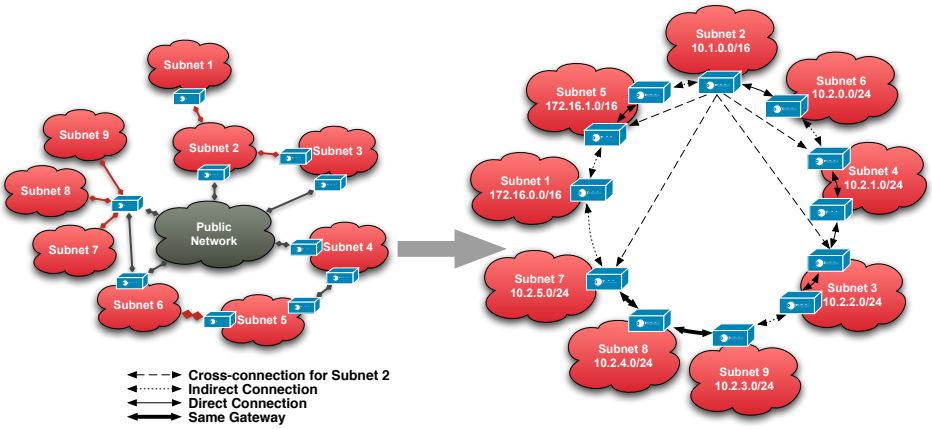

Fig. 1. Mapping of a VPN topology to a SOLID overlay

The Chord principle cannot directly be applied to complex topologies that contain nested VPN gateways, or if gateways are partially disconnected due to network failures, because there is no possibility of direct communication. For this reason, SOLID creates virtual paths through the overlay network itself, in order to connect gateways without possibility of direct communication.

However, in contrast to usual routing mechanisms the construction of the virtual path does not depend on the broadcast of information, but uses the structure of the overlay itself to create optimal paths iteratively. In order to create a virtual path, a search is initiated within the already established overlay. If a destination gateway is found and a direct communication is impossible, the overlay path discovered during the search is used for further indirect communication. As these virtual paths can consist of up to O(log n) overlay hops, a subsequent optimization step shortens each path. For common VPN topologies this shortening even leads to optimal lengths in terms of overlay hops, which is a reasonable metric since the cryptographic operations in each hop dominate delay and bandwidth. By this means it is possible for SOLID to configure even complex topologies (as illustrated in Fig. 2) and map them to a logical ring structure.

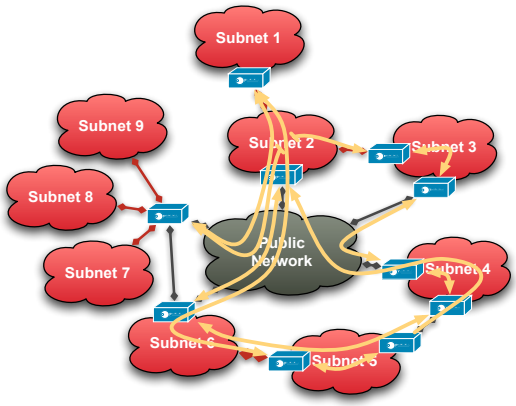

Fig. 2. Embedding of the overlay structure into the transportation net-

The entirely distributed approach allows for a realization of DoS-resistant VPNs as the failure of parts of the overlay can be tolerated; the remaining VPN devices will simply reorganize

and operate independently. Furthermore, unreliable connectivity causes only local message overhead and no broadcast of routing information. Partial failures in the transport network can be circumvented by SOLID, as indirect connections will be established between affected nodes. The indirect connections also allow for a proactive DoS-protection: SOLID is able to use techniques presented in [18] and separate more relevant parts of the VPN from less relevant ones by prohibiting direct connections between them. This allows for an effective infrastructure hiding and less effective attacks, e.g., because the public IP address of a manager's laptop or an important server cannot be determined easily.

However, SOLID's security properties are not limited to availability. As all exchanged data – including all overlay messages – is protected by IPsec associations, data confidentiality, integrity, and authentication can be guaranteed at all times. For indirect connections nested IPsec associations assure an end-to-end protection, which can even tolerate internal attackers. In order to guarantee also access control, SOLID is the first auto-configuration mechanism to make use of certified IP address ranges for VPN gateways. The ranges are embedded into the certificates used during IPsec authentication, and associations can only be established if the negotiated addresses match the ranges in the certificate.

The low number of proactively created security associations and the fact that network fluctuations have only local effects, make SOLID predestinated for the use in mobile scenarios, where some VPN devices have only sporadic connections or periodically changing outer IP addresses. In order to speed up handover procedures, it is also planned to make use of quick reauthentications by exploiting MOBIKE mechanisms.

Quantitative evaluations are performed in both: OMNeT++ simulations and real world scenarios by utilizing a Linux/strongSwan prototype with a common code base. Thus, allowing for an analysis of large-scale factors and complex topologies within simulations and a real world influences in lab environments.

All in all, the present approach SOLID allows for fully automated configuration of complex IPsec VPN, scales well with respect to the number of IPsec gateways, reacts robust to network failures, and supports the configuration of nested networks with private address spaces. The security in terms of data authentication, confidentiality, and integrity as well as access control is guaranteed to be at least as good as in manually configured VPN. The availability of SOLID VPNs is even better as it is possible to react to DoS attacks.

Future research is focusing on four main targets: First, the availability of SOLID VPN shall be further extended by automatically forming VPN topologies that react optimally to DoS-attacks. Second, the mobility properties of SOLID shall be further increased in order to support even highly mobile scenarios, e.g., in ad-hoc disaster communication. A third point is the decentralization of higher layer network services, such as DNS, time synchronization, logging, and certificate updates. This is especially important for mobile scenarios or in the case of DoS attacks, because central services within the VPN might become unavailable. A forth focus lays the extension of SOLID system itself. In order to support a broader range of scenarios, cluster support needs to be developed, IPv6 needs to be integrated, the current multicast implementation needs to be pushed on, and a QoS concept compiled. Thus, the current state of SOLID is only a step towards a more flexible and universal security architecture.

References

[1] V. Bollapragada, M. Khalid, S. Wainner: IPSec VPN Design. Cisco Press, 2005.

[2] L. Deri, R. Andrews: N2N: A Layer Two Peer-to-Peer VPN. Resilient Networks and Services, Springer, 2008, pp. 53–64

[3] Y. Bhaiji: Part III: Data Privacy, Network Security Technologies and Solutions. Cisco Press, 2008

[4] S. Fluhrer: SYSTEM AND METHOD FOR PROTECTED SPOKE TO SPOKE COMMUNICATION USING AN UNPROTECTED COMPUTER NETWORK. United States Patent 2007/0271451 A1, 2007

[5] M. Rossberg, G. Schaefer: Ciscos Group Encrypted Transport VPN – Eine kritische Analyse. D-A-CH security, 2009, pp. 351–360

[6] T. Tran: Proactive Multicast-Based IPSEC Discovery Protocol and Multicast Extension. IEEE Military Communications Conference (MILCOM), 2006

[7] J. Laganier, G. Montenegro, A. Kukec: Using IKE with IPv6 Cryptographically Generated Addresses. Expired Internet-Draft, 2007

[8] S. Fluhrer: DETERMINING SECURE ENDPOINTS OF TUNNELS IN A NETWORK THAT USES INTERNET SECURITY PROTOCOL. United States Patent 2007/7207063 B1, 2007

[9] L. Sanchez, M. Condell: Security Policy Protocol. Expired Internet-Draft. 2002

[10] M. Ek, F. Hultin, J. Lindblom: WASTE Peer-to-Peer Protocol. Luleåtekniska universitet, 2005

[11] M. Kratochvil: CloudVPN how it works. http://e-x-a.org/stuff/cloudvpn-poster.jpg, 2009

[12] G. Sliepens: The difficulties of a peer-to-peer VPN on the hostile Internet. FOSDEM, 2010

[13] M. Rossberg, W. Steudel, G. Schaefer, K. Martius: Eine Software-Architektur zur Konstruktion flexibler IPsec-Infrastrukturen. 11. Deutscher IT-Sicherheitskongress, 2009, pp. 297–308

[14] M. Rossberg, G. Schaefer, T. Strufe: Distributed Automatic Configuration of Complex IPsec-Infrastructures. Journal of Network and Systems Management, 2010, pp. 300-326

[15] I. Stoica, R. Morris, D. Karger, M. Kaashoek, H. Balakrishnan: Chord: A scalable peer-to-peer lookup service for internet applications. ACM SIGCOMM Computer Communication Review 31, 2001, pp. 149–160

[16] B. Ford: Unmanaged Internet Protocol: Taming the Edge Network Management Crisis. Second Workshop on Hot Topics in Networks, 2003

[17] I. Stoica, D. Adkins, S. Zhuang, S. Shenker, S. Surana: Internet indirection infrastructure. IEEE/ACM Transactions on Networking (TON) 12, 2004, pp. 205–218

[18] M. Brinkmeier, M. Rossberg, G. Schaefer: Towards a Denial- of-Service Resilient Design of Complex IPsec Overlays. International Conference on Communications (ICC), 2009