ACHIEVING UNCONDITIONAL SECURITY IN EXISTING NETWORKS USING QUANTUM CRYPTOGRAPHY

Stefan Rass
University of Klagenfurt - Research Group System Security
Universitätsstraße 65-67, 9020 Klagenfurt, Austria

Mohamed Ali Sfaxi, Solange Ghernaouti-Hélie
Inforge - HEC University of Lausanne
1015 Lausanne, Switzerland

Keywords: PPP, Quantum Key Distribution within PPP (Q3P), unconditional security transmission, IPSEC, SeQKEIP, Secure Routing, Network Connectivity.

Abstract: Based on extensions to the protocols PPP and IPSEC, we present a working proposal for building a network over which messages can be sent unconditionally secure. We will show how quantum cryptography can be implemented in classical protocols and how existing networks can be efficiently extended to suit our needs for unconditional security. We show that graph connectivity is crucial for the security of the transmission. For that matter, we provide secure routing services, so an adversary cannot penetrate any message flow successfully. Furthermore, our protocols are extensible to allow up to $t-1$ adversaries (possibly cooperating) while remaining unconditionally secure.

1 INTRODUCTION

Classical cryptographic algorithms are based on mathematical functions. The robustness of a given cryptosystem is based essentially on the secrecy of its (private) key and the difficulty with which the inverse of its one-way function(s) can be calculated. Unfortunately, there is no mathematical proof that will establish whether it is not possible to find the inverse of a given one-way function. On the contrary, quantum cryptography is a method for sharing secret keys, whose security can be formally demonstrated.

Ever since the beginning of quantum cryptography (Bennet and Brassard, 1984), a considerable theoretical framework has been built, providing unconditionally secure establishment of symmetric secrets between two parties. This is often referred to as *quantum key distribution* (QKD). A lot of research effort has been invested in practical results concerning physical devices (single photon sources, etc.) for quantum cryptography or theoretical results concerning privacy amplification, for instance. However, little effort has been put on the problem of distributing secrets between *non-adjacent* partners. Sophisticated protocols have been designed, implementing QKD within existing frameworks. The reader may consult (Ghernaouti-Hélie and Sfaxi, 2005), showing extensions to PPP and (Ghernaouti-Hélie et al., 2005), providing extensions to IPSec [RFC 2401].

A straightforward solution to the problem of distributing secrets among non-adjacent communication partners is relying on the integrity of each station along the path from Alice to Bob. Forwarding the message hop-by-hop without Alice and Bob sharing a secret prior to the transmission will nevertheless make the plaintext show up at every station, thus full secrecy is not guaranteed.

Our solution exploits the underlying network topology in order to have unconditional security across multi-hop connections between Alice and Bob. More precisely, as our intention is the integration of QKD in existing network infrastructure, we provide methods for extending networks, so topological properties can be achieved that allow for information-theoretically secure message relay. Secure routing services exploiting the topological properties are provided.

Unfortunately, practical evaluation of our proposal in terms of performance is not possible, as the QKD technology is still evolving and not fully developed yet.

1.1 Related Work

The contribution of this work is mainly a secure routing service and guidelines for designing networks. Previous articles dealing with secure routing mostly

Rass S., Ali Sfaxi M. and Ghernaouti-Hélie S. (2006).
ACHIEVING UNCONDITIONAL SECURITY IN EXISTING NETWORKS USING QUANTUM CRYPTOGRAPHY.
In *Proceedings of the International Conference on Security and Cryptography*, pages 207-210
DOI: 10.5220/0002094702070210
Copyright © SciTePress

focus on *Byzantine attacks*, where multiple active adversaries are allowed inside a network (Hu et al., 2002). Attacks in these setups include corruption of nodes, packages or entire parts of the network, which our setting can allow up to a particular threshold while preserving information-theoretic security. (Awerbuch et al., 2003) assumes no trusted third party services, mutually authenticated nodes, as well as active adversarial nodes, but basically focuses on how to deliver the package over the network. Our proposal will protect the routing information, such that misrouting is either impossible or will be detected. Computational intractability assumptions for avoiding misrouting packages (like implicitly adopted by using certificates; (Castro et al., 2002; Sanzgiri et al., 2002)) are explicitly avoided by our techniques, at negligible computational cost (in contrast to swarm-intelligence based approaches, like in (Awerbuch et al., 2004)).

2 QKD IN LAYER 2 PROTOCOLS

Securing layer 2 transactions is fundamental because this layer is common to all kinds of nodes' connections. The security processing is done transparently to the users and to the other protocols. Securing this layer is more optimized than securing the above OSI layer since neither additional encapsulation nor header is required. The well known Point to Point Protocol (PPP) [RFC1661] as well as its extensions implementing confidential message relay rests on the conjectured security of symmetric ciphers or on the conjectured hardness of numerical problems. Especially the latter is the basis for key-exchange, and still unproven yet. On the contrary, quantum cryptography does offer provably secure key-establishment, with the limitation of doing it only between adjacent partners. Nevertheless, (Ghernaouti-Hélie and Sfaxi, 2005) and (Ghernaouti-Hélie et al., 2005) elegantly integrate QKD in PPP and IPSec to overcome these difficulties. The resulting protocols are called Q3P (Quantum PPP) and SeQKEIP. The full details of Q3P are beyond the scope of this article, so the reader may consult (Ghernaouti-Hélie and Sfaxi, 2005) for details.

A QKD solution for IPSec is called SeQKEIP (Ghernaouti-Hélie et al., 2005), which is not based on IKE [RFC2409] but on ISAKMP [RFC 2408]. Using this method, we avoid the problem of compatibility between IKE and QKD (Elliott, 2002; Elliott et al., 2003). SeQKEIP runs nearly like the IKE [RFC2409]. As before, for brevity, we spare the details of SeQKEIP and refer the interested reader to the given references, as our focus here is the design of a suitable network topology for running SeQKEIP.

This paper aims at getting rid of the last limitation of a direct connection between communication parties, as required by QKD and implicitly present in Q3P.

3 ESTABLISHING SECRETS

As state-of-the-art quantum cryptography can only create random and secure keys between adjacent (directly connected) nodes, creation of keys between non-adjacent nodes A and B usually requires the trustworthiness of each node on the path between A and B, for otherwise an intermediate node may extract information from the message if the sender and receiver do not possess any pre-distributed secret. We assume such pre-distributed secrets $\sigma_{X,Y}$ only available between adjacent and nodes X, Y (established by BB84 or similar). Multi-links or one-to-many links are not (explicitly) considered.

Our solution combines classical information-theoretically secure schemes like secret sharing (Shamir, 1979) with QKD underlying SeQKEIP and Q3P to provide authentic and secure channels for sending shares of the secret message. To prevent intentional or accidental routing of shares over the same node, we construct networks providing at least t non-intersecting paths between any two nodes, and show how to secure the routing information such that misrouting is either impossible or will be detected. Thus an adversary cannot exceed the number of shares in his possession above the threshold.

Uppercase letters like $X, A, B \ldots$ denote nodes in the network (routers, switches...) as well as sets and graphs, and lowercase letters denote vertices in a graph. Graphs are assumed undirected and connected and are denoted as pair $G = (V, E)$, where V is the set of vertices and $E \subseteq V \times V$ is the set of edges. We assume the reader to be familiar with the basic graph-theoretic terms, otherwise (Chartrand, 2005) provides an excellent introduction. The set of nodes on a path π or in a graph G is denoted as $V(\pi)$ or $V(G)$, respectively. The one-time pad encryption of m using key k is denoted by $m \oplus k$ (i.e. $\oplus$ is the bitwise XOR).

3.1 Network Topology

As we require node-disjoint paths between any two nodes in the network, we shall provide efficient incremental network construction algorithms allowing for extending existing networks as well as joining different networks into one. By node-disjoint, we mean that two paths $\pi'_{X,Y}, \pi''_{X,Y}$, connecting nodes X and Y satisfy $V(\pi'_{X,Y}) \cap V(\pi''_{X,Y}) = \{X, Y\}$. Formally, we will provide methods for incrementally constructing t-connected networks. Informally, a network is t-connected, if up to $t-1$ nodes can be deleted without

the network breaking up into non-connected components (Chartrand, 2005). The following theorem by Hassler Whitney (following from Menger's theorem) is the basis for our considerations:

Theorem 3.1 (Whitney)**.** *A graph is t-connected if and only if at least t node-disjoint paths exist between any two nodes in G.*

See (Chartrand, 2005) for a proof. To create a t-connected graph H having a given graph G as subgraph, we may use the following facts:

Proposition 3.2. *Let G be a t-connected graph and let $v \notin V(G)$. Then the graph H created by joining v to t nodes in G is also t-connected.*

Proposition 3.3. *The complete graph K_{t+1} (with $t+1$ nodes) is the smallest graph being t-connected, i.e. no subgraph of K_{t+1} is t-connected.*

So we may identify a clique of maximum size in G and join nodes and edges until we have enlarged the clique to size $t+1$ (hence being minimal t-connected by prop. 3.3). The remaining nodes are joined by using prop. 3.2 until all nodes have been integrated. The resulting network will be t-connected again by prop. 3.2.

Proposition 3.4. *Let $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ be t-connected graphs. Select two sets $W_1 = \{v_1, \ldots, v_t\} \subseteq V_1, W_2 = \{w_1, \ldots, w_t\} \subseteq V_2$ and create the graph $H = (V_1 \cup V_2, E_1 \cup E_2 \cup \{(v_i, w_i) | v_i \in W_1, w_i \in W_2, i = 1, \ldots, t\})$ Then H is t-connected.*

See, for instance, (Rass, 2005a) for the proofs. The last result implies a straightforward method for joining two t-connected networks G_1 and G_2 into a single t-connected network H, by simply connecting t disjoint pairs of nodes in either network. Prop. 3.4 together with the previous discussion shows an easy method for creating t-connected graphs, without ever having to test this property via complex algorithms like the ones in (Gabow, 2000).

Two more benefits are worth to be mentioned: Safety increases, as failure of at most $t-1$ nodes will not make the network go down. For sufficiently large t, we may concurrently run secure connections.

Routing according to our method requires the network topology known to all nodes in the network. We can achieve this by broadcasting new topology information after having joined a node or another network. Moreover, as pointed out in (Rass, 2005a), at least one node will be able to detect up to $t-1$ active adversaries, as every node will receive t identical updates. If one is different, then some manipulation must have taken place.

3.2 Secure Message Relay

The method presented in this article is mainly based on the constructive approach used in (Rass, 2005a). Let m denote the message Alice wants to send to Bob. She creates t shares for the message, either using a t-out-of-n sharing (cf. (Shamir, 1979)) or an n-out-of-n-sharing (via an XOR with several one-time pads). Each share is passed along its own path, which does not intersect any other path. Each share on his own is forwarded hop-by-hop by decrypting and re-encrypting it using the QKD key established for the incoming and outgoing link. Let the secret sharing be such that t is its threshold, then Eve has to compromise at least t nodes, corresponding to t node-disjoint paths between Alice and Bob. This can either be done by *misrouting packages* or *impersonating other nodes*. Both possibilities can be ruled out, as shown in the following paragraphs.

In the worst case, the adversary is able to have all paths intersect at one node, thus the key and therefore the message appear in plaintext at this node. The first attack can be countered by a special encryption, shown below.

Additionally, if the presence of an adversary has been detected, the packets over such paths are surely lost, so if we raise the threshold of the secret sharing scheme beyond the connectivity number of the network (being also the number of node-disjoint paths, by theorem 3.1), we can tolerate loss of some packages without loosing information or security.

Avoiding Misrouting: For forwarding a message, we assume that each packet has a routing information R attached to it, which contains the path information, i.e. the nodes which have been passed so far. We assume the network topology to be known, so the routing information is a field of fixed length, in order to have one-time pad encryption applicable.

Forwarding of a message by a particular node upon decryption of the routing information proceeds by three rules: (1) If the sender's identity does not appear in R then announce an error. (2) If the next node on the path appears in R then announce an error. (3) Add the own ID to the path information, re-encrypt the new routing information and send the message to the next node.

It is easy to see that this protocol ensures nonselfintersecting paths if carried out successfully and that no passive adversary can extract information from the message flow. See (Rass, 2005a) for a more detailed treatment.

To have the routing information R not accessible, thus not modifiable (s.t. Eve could have her node passed more than once), we encrypt R as follows: Let $\sigma'_{X,Y}, \sigma''_{X,Y}$ be another two (perfectly secure) secrets shared between nodes X and Y, which are dedicated to routing purposes only. We attach $R_E :=$

$E_{\sigma'_{X,Y}}(R) \oplus \sigma''_{X,Y}$ to the package as encrypted routing information. The function E_σ denotes any symmetric cipher with a *strong avalanche effect* (Webster and Tavares, 1986).

It follows that $E_{\sigma'_{X,Y}}(R)$ provides no information for encrypting another (forged) $R' \neq R$ and the one-time pad encryption with $\sigma''_{X,Y}$ prevents exhaustive searching for the key $\sigma'_{X,Y}$ or $\sigma''_{X,Y}$. Since Eve is required to modify R to $R' \neq R$, the avalanche effect will "randomize" the ciphertext, so knowing $E_{\sigma'_{X,Y}}(R)$ is worthless for creating $E_{\sigma'_{X,Y}}(R')$.

Avoiding Impersonation: We can use the QKD established secrets to implement perfectly secure authentication by exchanging portions of the QKD-key with an unconditionally secure MAC (see (Stinson, 1992)) attached to it. This MAC is based on a key, exclusively shared by Alice and Bob. If there is no adversary, then the MAC should correctly be verified. However if there is an adversary in the middle, then with high probability, s/he must have established *two distinct* QKD-keys with Alice and Bob, and thus will be detected upon failure of the verification of the MAC. Moreover, forging the MAC is not effectively possible, as it is unconditionally secure. This idea is elaborated in full detail in (Rass, 2005b).

4 CONCLUSION

Upon the work of (Ghernaouti-Hélie et al., 2005) and (Ghernaouti-Hélie and Sfaxi, 2005) we have built a framework for delivering messages over networks in which adjacent nodes are able to establish secrets by means of quantum cryptography. We fulfil the requirements of classical information-theoretically secure schemes and provide practical solutions for network design and message relay. To the best of our knowledge, this is the first unified approach to implementing QKD in existing protocols and network infrastructure, providing provable security at reasonable effort.

REFERENCES

Awerbuch, B., Holmer, D., and Rubens, H. (2003). Provably secure competitive routing against proactive byzantine adversaries via reinforcement learning. Technical Report 2, Department of Computer Science at Johns Hopkins University, Baltimore, MD.

Awerbuch, B., Holmer, D., and Rubens, H. (2004). Swarm intelligence routing resilient to byzantine adversaries.

Bennet, C. and Brassard, G. (1984). Public key distribution and coin tossing. In *IEEE International Conference on Computers, Systems, and Signal Processing.*, LOS ALAMITOS. IEEE Press.

Castro, M., Druschel, P., Ganesh, A., Rowstron, A., and Wallach, D. S. (2002). Secure routing for structured peer-to-peer overlay networks. *SIGOPS Oper. Syst. Rev.*, 36(SI):299–314.

Chartrand, G. (2005). *Introduction to graph theory*. Higher education. McGraw-Hill, Boston.

Elliott, C. (2002). Building the quantum network. *New Journal of Physics*, (4 (46.1-46.12)).

Elliott, C., Pearson, D., and Troxel, G. (2003). Quantum cryptography in practice.

Gabow, H. N. (2000). Using expander graphs to find vertex connectivity. In FOCS '00: Proc. of the 41st Annual Symposium on Foundations of Computer Science, page 410, Washington, DC, USA. IEEE Computer Society.

Ghernaouti-Hélie, S. and Sfaxi, M. A. (2005). Upgrading PPP security by quantum key distribution. In *NetCon 2005 conference*.

Ghernaouti-Hélie, S., Sfaxi, M. A., Ribordy, G., and Gay, O. (2005). Using quantum key distribution within IPSEC to secure MAN communications. In *MAN 2005 conference*.

Hu, Y.-C., Perrig, A., and Johnson, D. B. (2002). Ariadne: A secure on-demand routing protocol for ad hoc networks. In *Proc. of the 8th Annual International Conference on Mobile Computing and Networking* (MobiCom 2002), pages 12–23.

Rass, S. (2005a). How to send messages over quantum networks in an unconditionally secure manner. Technical Report TR-syssec-05-05, University of Klagenfurt, Computer Science, System Security, Klagenfurt.

Rass, S. (2005b). On information-theoretically secure authentication in quantum networks. Technical Report TR-syssec-05-07, University of Klagenfurt, Computer Science, System Security, Klagenfurt.

Sanzgiri, K., Dahill, B., Levine, B. N., Shields, C., and Belding-Royer, E. M. (2002). A secure routing protocol for ad hoc networks. In *ICNP '02: Proc. of the 10th IEEE International Conference on Network Protocols*, pages 78–89, Washington, DC, USA. IEEE Computer Society.

Shamir, A. (1979). How to share a secret. *Commun. ACM*, 22(11):612–613.

Stinson, D. R. (1992). Universal hashing and authentication codes. In *CRYPTO '91: Proc. of the 11th Annual International Cryptology Conference on Advances in Cryptology*, pages 74–85, London, UK. Springer-Verlag.

Webster, A. and Tavares, S. (1986). On the design of S-boxes. In *Lecture notes in computer sciences; 218 on Advances in cryptology—CRYPTO 85*, pages 523–534, New York, NY, USA. Springer-Verlag New York, Inc.