Chains and Whips - An approach to lighweight MACs

Paul Walther*, Stefan Köpsell*, Frederick Armknecht†, Gene Tsudik‡ and Thorsten Strufe*

* TU Dresden, Germany † Univ. Mannheim, Germany ‡ UC Irvine, USA

In robotic control, it is observable that frequent and small messages are exchanged in a rapid manner. The exchange of this small commands (< 50 bytes) is conducted by connecting controller and actuators with high throughput and low latency (< 1 ms) wireless connections [1]. These commands need to be authenticated in order to prevent malicious interference which could cause structural or human damage. Hence, there need to be communication means which are low latency on one side as well as integrity protected on the other side.

In the following we propose a protocol which protects the integrity of a message streams and reduces the transmitted data used for verification. Its core idea is twofold: on the one hand, the transmitted data will be reduced by using shorter verification tags. On the other hand, the security will be maintained by incorporating all available verification bits into upcoming tags.

Several approaches were proposed for the verification of message chains by connecting multiple messages [2, 3, 4, 5]. Although these schemes are quite effective, they do not aim for efficiency, i.e. they all introduce additional data to be transferred and, hence, increase latency. Our newly proposed schemes particularly aims for reduced latency by minimizing the transmitted data.

To achieve this reduction, while still protecting the overall sequence of messages, the following mechanism is proposed: The underlying scheme for verification are symmetric message authentication codes (MACs). Hence, the start is the calculation of a keyed MAC tag t_i over the current message m_i as $t_i = MAC(m_i)$. Of t_i only the first n bits are concatenated to the messages and transmitted, which effectively reduces the transmitted data. To regain the security of the tag (which is reduce through the reduction of the transmitted tag bits) the whole tag t_i is incorporated in the creation of the tag t_{i+1}. This tag is created by $t_{i+1} = MAC(m_{i+1} \,||\, t_i)$ — thereby, all verification bits of the tag t_i get included into the upcoming tag by building a chain over the tags.

We additionally propose different variations of this idea, which expose different properties regarding recoverability. These variation use different tails of the tag, which are included into upcoming transmitted tags. They are incorporated via XOR and different parts of the tags are used in different upcoming messages — they effectively "whip" forward to those tags.

Finally, we have sketches of security proofs as well as performance evaluations, which suggest, that our schemes reaches the targeted performance gains while still efficiently protecting integrity.

References

[1] A. Frotzscher and others. Requirements and current solutions of wireless communication in industrial automation. In *IEEE International Conference on Communications Workshops, ICC 2014*.

[2] R. Gennaro and P. Rohatgi. How to sign digital streams. In *Advances in Cryptology — CRYPTO '97*, Lecture Notes in Computer Science, pages 180–197. Springer, Berlin, Heidelberg, Aug. 1997.

[3] Y. Challal, A. Bouabdallah, and Y. Hinard. RLH: Receiver driven layered hash chaining for multicast data origin authentification. *Computer Communications*, 28(7):726–740, 2005.

[4] S. Miner. Graph-based authentication of digital streams. In *IEEE Symposium on Security and Privacy*, pages 232–246, 2001.

[5] A. Perrig, R. Canetti, J. D. Tygar, and D. Song. Efficient authentication and signing of multicast streams over lossy channels. In *IEEE Symposium on Security and Privacy*, pages 56–73, 2000.

crypto day matters 28 (2018)
Beiträge vom 28. Kryptotag, 07.-08.06.2018, Kirchheim.
doi:10.18420/cdm-2018-28-25