Don't show your hand: on the security leakages of *BFT systems

Antonio Davoli
Sapienza University of Rome
davoli@di.uniroma1.it

ABSTRACT

After the *Practical Byzantine Fault Tolerance* work [2], the distributed systems literature has improved quality and performance of *BFT systems. Through this definition we address all the solutions, deriving from [2], for State Machine Replication (SMR) that are based on node active replication (usally *3f+1* replicas for *f* faults), and where servers are always synchronized on the set of operations executed.

However, many solutions aim at improving *robustness* and *performance*, providing efficient solutions to *safety* and *liveness* guarantees [3]. These requirements are surely important, but with the growth of clients number other dynamics and issues appear.

The *security* and *resilience* aspect of *BFT environment is indeed an open field where the first results have started to be presented [1]. These results address the clients-replicas interaction in the first part of the protocol (usually attacking the primary or injecting view inconsistency). One of the most important problems is the trust that clients received. *BFT systems usually return to the clients a set of answers (usually a quorum of at least *f+1*) and then clients understand if a correct quorum has been reached. Hiding conveniently what happens inside can relieve the system from DDoS or from targeting the faulty nodes. With the actual solutions the clients can indeed infer from the REPLY messages received the number and the identity of the replicas that are working accurately and the ones that are faulty or unavailable. They can exploit these valuable information to form a coalition and to easily bring an attack against the system.

BODY

*The reply messages of the *BFT distributed systems expose the status of your servers and turn you into a target for malicious attackers.*

REFERENCES

[1] Y. Amir, B. Coan, J. Kirsch, and J. Lane. Prime: Byzantine replication under attack. *IEEE Transactions on Dependable and Secure Computing*, 8(4):564–577, 2011.

[2] M. Castro and B. Liskov. Practical byzantine fault tolerance. In *Proceedings of the third symposium on Operating systems design and implementation*, OSDI '99, pages 173–186, Berkeley, CA, USA, 1999. USENIX Association.

[3] R. Guerraoui, N. Knežević, V. Quéma, and M. Vukolić. The next 700 bft protocols. In *Proceedings of the 5th European conference on Computer systems*, EuroSys '10, pages 363–376, New York, NY, USA, 2010. ACM.

Volume 1 of Tiny Transactions on Computer Science