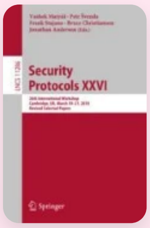
Non-monotonic Security Protocols and Failures in Financial Intermediation

Conference paper | First Online: 24 November 2018

pp 45–54 | Cite this conference paper



Security Protocols XXVI

(Security Protocols 2018)

Fabio Massacci, Chan Nam Ngo, Daniele Venturi & Julian Williams

Part of the book series: Lecture Notes in Computer Science ((LNSC,volume 11286))

Included in the following conference series:
Cambridge International Workshop on Security Protocols

Abstract

Security Protocols as we know them are *monotonic*: valid security evidence (e.g. commitments, signatures, etc.) accrues over protocol steps performed by honest parties. Once's Alice proved she has an authentication token, got some digital cash, or casted a correct vote, the protocol can move on to validate Bob's

evidence. Alice's evidence is never invalidated by honest Bob's actions (as long as she stays honest and is not compromised). Protocol failures only stems from design failures or wrong assumptions (such as Alice's own misbehavior). Security protocol designers can then focus on preventing or detecting misbehavior (e.g. double spending or double voting).

We argue that general financial intermediation (e.g. Market Exchanges) requires us to consider new form of failures where honest Bob's actions can make honest good standing. Security protocols must be able to deal with *non-monotonic security* and *new types of failures* that stems from rational behavior of honest agents finding themselves on the wrong side.

This has deep implications for the efficient design of security protocols for general financial intermediation, in particular if we need to guarantee a *proportional burden* of computation to the various parties.

Chapter

EUR 29.95
Price includes VAT (Poland)

- Available as PDF
- Read on any device
- Instant download
- Own it forever

Buy Chapter

eBook

EUR 42.79
Price includes VAT (Poland)

- Available as EPUB and PDF
- Read on any device
- Instant download
- Own it forever

Buy eBook

Softcover Book

EUR 53.49
Price includes VAT (Poland)

- Compact, lightweight edition
- Dispatched in 3 to 5 business days
- Free shipping worldwide - see info

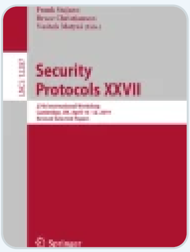
Buy Softcover Book

Tax calculation will be finalised at checkout

Purchases are for personal use only

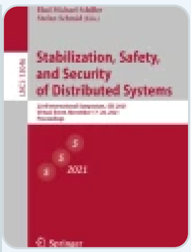
Institutional subscriptions

Similar content being viewed by others



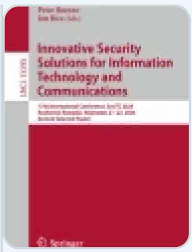
Affordable Security or Big Guy vs Small Guy

Chapter | © 2020



Security in Asynchronous Interactive Systems

Chapter | © 2021



Designing Human-centric security protocols

Chapter | © 2025

Notes

1. Obviously the server would have had more load than a client, but this only happens because the server participates to several authentications with several clients at once.

2. The largest claimed example is the Danish sugar beet auction where 1229 Danish farmers auctioned their production [3]. However, an actual technical reading of the paper reveals that there were only three servers performing MPC over the secret shares generated by the 1200 bidders. As we will illustrate in Sect. 3 it is actually a good example of a monotonic security protocol.

3. See an additional discussion in [15] and a concrete implementation in [14].

4. Security evidence created during a protocol run should not extend beyond the protocol run. Several protocol failures are indeed due to protocol design errors where a credential could be used across sessions [1].

5. A formal definition of a Futures Market is given in [15] (Sect. 4).

6. See additional discussions on non-monotonic security in [14] (Sect. 5, Remark 1).

7. The 1229 parties full MPC variant is still out of reach for the foreseable future as experimental papers typically reported MPC with less than 10 parties [5].

8. See Sect. 7 of [14].

9. This does not violate the proportional burden requirement as each trader has the responsibility to prove the solvency if s/he still wants to be in the game.

10. https://tickhistory.thomsonreuters.com.

11. In some cases this fixed order might interfere with the security goal, if the order of actions may leak some information on who started the process.

References

1. Abadi, M., Needham, R.: Prudent engineering practice for cryptographic protocols. IEEE Trans. Software Eng. **22**(1), 6–15 (1996)

2. Allen, F., Santomero, A.M.: The theory of financial intermediation. J. Bank. Finance **21**(11–12), 1461–1485 (1997)

3. Bogetoft, P., et al.: Secure multiparty computation goes live. In: Dingledine, R., Golle, P. (eds.) FC 2009. LNCS, vol. 5628, pp. 325–343. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-03549-4_20

4. Canetti, R., Lindell, Y., Ostrovsky, R., Sahai, A.: Universally composable two-party and multi-party secure computation. In: ACM Symposium on Theory of Computing, pp. 494–503. ACM (2002)

5. Damgård, I., Keller, M., Larraia, E., Pastro, V., Scholl, P., Smart, N.P.: Practical covertly secure MPC for dishonest majority – or: breaking the SPDZ limits. In: Crampton, J., Jajodia, S., Mayes, K. (eds.) ESORICS 2013. LNCS, vol. 8134, pp. 1–18. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-40203-6_1

6. Dierks, T., Allen, C.: The TLS Protocol Version 1.0 (1999)

7. Gong, L.: Fail-Stop Protocols: An Approach To Designing Secure Protocols (1994)

8. Harkins, D., Carrel, D.: The internet key exchange (IKE), Technical report (1998)

9. Kiayias, A., Zacharias, T., Zhang, B.: An efficient E2E verifiable e-voting system without setup assumptions. IEEE Secur. Priv. (2017)

10. Kosba, A., Miller, A., Shi, E., Wen, Z., Papamanthou, C.: Hawk: the blockchain model of cryptography and privacy-preserving smart contracts. In: IEEE Symposium on Security and Privacy, pp. 839–858. IEEE (2016)

11. Kumaresan, R., Moran, T., Bentov, I.: How to use bitcoin to play decentralized poker. In: ACM SIGSAC Conference on Computer and Communications Security, pp. 195–206. ACM (2015)

12. Kumaresan, R., Vaikuntanathan, V., Vasudevan, P.N.: Improvements to secure computation with penalties. In: ACM SIGSAC Conference on Computer and Communications Security, pp. 406–417, ACM (2016)

13. Malinova, K., Park, A., Riordan, R.: Do retail traders suffer from high frequency traders (2013). SSRN 2183806

14. Massacci, F., Ngo, C.N., Nie, J., Venturi, D., Williams, J.: FuturesMEX: secure, distributed futures market exchange. In: IEEE Symposium on Security and Privacy, pp. 453–471. IEEE (2018)

15. Massacci, F., Ngo, C.N., Nie, J., Venturi, D., Williams, J.: The seconomics (security-economics) vulnerabilities of decentralized autonomous organizations. In: Stajano, F., Anderson, J., Christianson, B., Matyáš, V. (eds.) Security Protocols 2017. LNCS, vol. 10476, pp. 171–179. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-71075-4_19

16. Merkle, R.C.: A digital signature based on a conventional encryption function. In: Pomerance, C. (ed.) CRYPTO 1987. LNCS, vol. 293, pp. 369–378. Springer, Heidelberg (1988). https://doi.org/10.1007/3-540-48184-2_32

17. Miller, S.P., Neuman, B.C., Schiller, J.I., Saltzer, J.H.: Kerberos authentication and authorization system. In: Project Athena Technical Plan (1987)

18. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system (2008)

19. Sasson, E.B., et al.: Zerocash: decentralized anonymous payments from bitcoin. In: IEEE Symposium on Security and Privacy, pp. 459–474. IEEE (2014)

20. Spulber, D.F.: Market microstructure and intermediation. J. Econ. Perspect. **10**(3), 135–152 (1996)

21. Zhai, E., Wolinsky, D.I., Chen, R., Syta, E., Teng, C., Ford, B.: AnonRep: towards tracking-resistant anonymous reputation. In: USENIX Symposium on Networked Systems Design and Implementation, pp. 583–596 (2016)

Author information

Authors and Affiliations

University of Trento, Trento, Italy

Fabio Massacci & Chan Nam Ngo

Sapienza University of Rome, Rome, Italy

Daniele Venturi

Durham University Business School, Durham, UK

Julian Williams

Corresponding author

Correspondence to Fabio Massacci.

Editor information

Editors and Affiliations

Masaryk University, Brno, Czech Republic

Vashek Matyáš

Masaryk University, Brno, Czech Republic

Petr Švenda

University of Cambridge, Cambridge, UK

Frank Stajano

University of Hertfordshire, Hatfield, UK

Bruce Christianson

Memorial University of Newfoundland, St. John's, NL, Canada

Jonathan Anderson

Rights and permissions

Copyright information

About this paper

Cite this paper

Massacci, F., Ngo, C.N., Venturi, D., Williams, J. (2018). Non-monotonic Security Protocols and Failures in Financial Intermediation. In: Matyáš, V., Švenda, P., Stajano, F., Christianson, B., Anderson, J. (eds) Security Protocols XXVI. Security Protocols 2018. Lecture Notes in Computer Science(), vol 11286. Springer, Cham. https://doi.org/10.1007/978-3-030-03251-7_5

.RIS .ENW .BIB

DOI
https://doi.org/10.1007/978-3-030-03251-7_5

Published
24 November 2018

Publisher Name
Springer, Cham

Print ISBN
978-3-030-03250-0

Online ISBN
978-3-030-03251-7

eBook Packages
Computer Science
Computer Science (R0)
Springer Nature Proceedings
Computer Science

Keywords

Security protocol | Non-monotonicity | Honest failure | Proportional burden | Failure-by-omission

Publish with us

Profiles

1. Julian Williams

View author profile