Poster: Byzantine Discrepancy Attacks against Calendar, Set-Intersection and Nations

Yvo Desmedt
Department of Computer Science
The University of Texas at Dallas
Richardson, Texas, USA
y.desmedt@cs.ucl.ac.uk

Alireza Kavousi
Department of Computer Science
University College London
London, UK
a.kavousi@cs.ucl.ac.uk

Aydin Abadi
School of Computing
Newcastle University
Newcastle upon Tyne, UK
Aydin.Abadi@newcastle.ac.uk

Abstract

Nowadays Communication Security usually refers to digital communication and in particular via the Internet. We explain why the topic should be broadened to include any communication, in particular when done in person, e.g., with co-authors, colleagues, reporters, etc.

Thousands of papers have been written on blockchain, and consensus. Despite this, the problem of Byzantine attack has been ignored in some important apps! One of these examples is (Outlook) Calendar. Moreover, the Byzantine attack can also be used in the political world. We explain how using it may undermine the security of nations. Finally, we observe that topics on which a lot of research has been done, such as Private Set Intersection have ignored the problem of Byzantine attacks.

Although the Byzantine general problem is typically described in a peer-to-peer setting, we show that it can also occur in other scenarios.

CCS Concepts

• **Security and privacy** → **Distributed systems security**; **Denial-of-service attacks**; • **Networks** → *Protocol correctness*; • **Human-centered computing** → *Collaborative and social computing theory, concepts and paradigms.*

Keywords

Byzantine General; Calendar; Discrepancy Attack; Teams; National Security; Private Set-Intersection

ACM Reference Format:
Yvo Desmedt, Alireza Kavousi, and Aydin Abadi. 2024. Poster: Byzantine Discrepancy Attacks against Calendar, Set-Intersection and Nations. In *Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security (CCS '24), October 14–18, 2024, Salt Lake City, UT, USA.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3658644.3691379

1 Survey

The poster:

- gives background information on Byzantine attacks and Byzantine agreement,
- briefly surveys the approaches used to achieve consensus,
- explains a concrete Byzantine attack against any app with distributed calendar,
- explains the problems with Outlook Calendar in particular in the context of Microsoft Teams,
- explains how when a governmental "trusted" party leaks information to the press, it may provoke a civil unrest (concrete and potential examples are mentioned),
- explains that research topics, such as Private Set Intersection, need to include consensus to achieve security.

2 The Byzantine Attack

We briefly explain the Byzantine attack [6], which is now a classical part of courses on distributed computing.

Consider three generals, called Byzantine generals. The binary question the three generals have to decide is whether their three armies encircling a city will attack tomorrow at 8 am, or not. Couriers are sent between the generals to make the final decision. A problem now arise if one of the three generals, let say A, sends the message "yes" to general B, *but* sends the message "no" to general C. Even if the generals know that one of them might not be trustworthy, Lamport et. al showed that there is no solution to the problem when there are only three generals!

A classical strategy that could be followed during a Byzantine attack is to abort a protocol.

3 Consensus

We explain what consensus[1] is and briefly survey technical approaches on how to achieve it.

The problem on agreeing on common data is called *consensus*. A classical way to achieve it is the use of Byzantine agreement [6]. The protocol is quite complex and beyond the scope of this poster. When t is the number of dishonest parties, the total number of parties that are needed to achieve consensus is either $3t+1$ or $4t+1$. Consensus will be reached between honest parties. The discrepancy between $3t+1$ and $4t+1$ is due to the question whether synchronized communication is possible or not.

A more modern approach to achieve consensus is by using blockchain[2]. Blocks are linked in a chain by the use of a cryptographic hash function and digital signatures. To prevent too many parties participate, the hash output must satisfy some conditions,

CCS '24, October 14–18, 2024, Salt Lake City, UT, USA.

ACM ISBN 979-8-4007-0636-3/24/10
https://doi.org/10.1145/3658644.3691379

[1] https://en.wikipedia.org/wiki/Consensus_(computer_science)
[2] https://en.wikipedia.org/wiki/Blockchain

which is called a proof of work[3]. Still, it is possible that the chain becomes a fork. In that case the longest subchain wins, i.e., becomes the data parties consent to. Proof of stake has been suggested to reduce waste of energy consumption.

Since bitcoin uses blockchain, the topic has become very popular. Researchers have proposed to put all data into the blockchain, some completely ignoring privacy. Google Scholar lists thousands of papers on the topic of blockchain. One of the many examples is the proposed use of blockchain for train tickets, see e.g. [2].

4 Calendar

Although VOIP tools, such as Skype, exist for more than 20 years, the COVID pandemic has dramatically increased the number of people who work from home and therefore the need for group communication tools, such as Zoom and Teams. Teams gives access to Outlook's Calendar. Since our attack is focused on a distributed calendar, such as Outlook Calendar, we briefly explain how Teams works.

A meeting (called Event) can be planned in Teams by going to the Calendar and then click on the "+" sign. That will allow the host of the event to: give the event a name, invite other parties, decide the date and time. When all this is confirmed, the other parties will receive an e-mail from Microsoft. Note that Teams has many other functions, which are irrelevant in our context.

4.1 The attack

The attack is completely inspired by the Byzantine generals problem. We now give an example of its use for Outlook Calendar in the context of Teams.

Suppose that three people, Aydin[4], Bob and Eve have agreed to have a meeting in exactly 7 days during the morning (they live in the same time zone). The exact time is to be decided by one of them, called Eve. What Aydin and Bob do not know is that Eve is disgruntled. What Eve[5] now can do, is plan *two events*, one for 10am with Aydin and the other one for 11am with Bob. Note however that all three must be present to have a successful meeting! So, the week afterwards, at 10:10am Eve states that Bob has still not shown up, and they stop waiting for Bob, i.e., that event is canceled. At 11:10am Eve states that they waited long enough for Aydin, and that event is canceled too!

Note that in Teams it is even possible to schedule two events at exactly the same time. Giving them similar, but not the same name, allows the party making the invites to distinguish these two events. To check whether this last version of the attack is theoretical or not, one of the three authors made two invitations on Team for *exactly the same timeslot*. This test was done on 31st of July 2024 using the current Teams version. When the second invite was being made, under the name of the host appeared in red: "Busy." However, the two meetings entered the calendar without any problems!

[3]https://en.wikipedia.org/wiki/Proof-of-work_system
[4]The name Alice [1] was not chosen to be inclusive.
[5]Eve could also decide not to participate at the Teams meeting. This is nothing else than an abort, a classical approach to a Byzantine attack.

4.2 Difference with the classical Byzantine generals

Observe the difference between the Byzantine general problem, as it is usually described, and our version. Indeed, the now classical attack is in a peer-to-peer setting, which means that the three generals do not use a trusted party to communicate with each other. In the case of Teams, to set up the event(s), all communications are done via Microsoft. So, strictly speaking it is *not* peer-to-peer. This shows that the Byzantine general attack extends to other settings.

4.3 Possible solutions

When receiving an invite for a meeting, only the host doing the invitations and Microsoft know who all the parties are that have been invited. Currently the "guests" do not receive this information from Microsoft. Teams could easily be updated to include that information when an invite is sent. The attack would then be detected.

Note that in "Classic Teams" (i.e., predating 2024), it was possible to check *during* the meeting who was invited, but did not join it [9]. In the current version of Teams this is no longer possible, making our attack work.

4.4 Breaking up Teams alleged monopoly

Recently, the EU has charged Microsoft for making Teams a monopoly [3]. "Ma Bell" (officially called Bell Telephone), was a monopoly until it was broken up in 1983. In the case of remote meetings, there already exist competing systems, such as Zoom. We now briefly explain what a breakup of Teams would imply from, in particular a security viewpoint.

When Aydin, Bob and Eve are using three different apps to have a meeting, there is no trusted party. So, it is impossible to be certain who has been invited and the attack can not be prevented when only three people are supposed to meet [6].

Note that such a breakup of Teams will also cause *practical problems*. Although these are beyond the scope of this poster, we briefly mention some. When Ma Bell broke down, there were international standards for the phone system, in particular the syntax of the phone number. In our case note that Zoom uses a *number* to connect, which Teams does not! To explain the other problems, let Aydin and Bob use "Google Meet", Bob and Eve use Teams, and finally Aydin and Eve use Zoom. Each user will need to run two apps, it is sharing the camera, the microphone, and the speaker(s), which is far from trivial today!

5 National Security Impact

Before we explain how a Byzantine attack could be used to undermine national security, we give some background information.

5.1 Impact of discrepancies

We start discussing the potential impact of discrepancies and disinformation.

Due to the 1998 Nouméa Accord the electorate for local elections in New Caledonia was restricted to pre-1998 residents of the islands and their descendants who maintained residence for at least 10 years. On April 2, 2024 the French Senate and on May 15, 2024, the French lower house, extended suffrage to those who had been

residing in New Caledonia for an uninterrupted 10 years. Protests and riots followed[6], causing deaths, and the declaration of a state of emergency. So, the unrest can be explained based on a discrepancy between an old agreement and a new law.

Disinformation fed a far-right riot after a deadly stabbing on July 29, 2024, in Southport, England [5]. The UK government stated the danger of disinformation on social media [7].

5.2 Historical background

Since we claim that the Byzantine attack can have national consequences, we give some background information on what role high level governmental employees had, and this for different countries.

The former FBI deputy director William Mark Felt confirmed in 2005 that he was "Deep Throat," the anonymous government source who helped take down President Nixon in the Watergate scandal [8]. A claim has been made that the FBI deputy director was in fact disgruntled and wanted to become director [4].

Some spies succeeded in obtaining high level positions. We just give one example. The secretary of the former West German chancellor Willy Brandt's, Günter Guillaume, was an East German spy[7], a country part of the Warsaw Pact.

Finally note that in certain countries large fractions of the population strongly dislike each other. Lebanon is such an example and had a civil war[8].

5.3 The attack

Imagine now a person in a position similar to deputy director of the FBI, but this time being a foreign spy in a country which is unstable. This person now leaks to the media of one fraction of the population a claim A. However, the person also leaks to the press of the other fraction the opposite claim, i.e., $\bar{A}$.

We now explain what such a strategy may imply. In Section 5.1 we cited examples were discrepancies are the cause of serious revolts. When the Byzantine attack is used in a political context, it might have revolts for consequence, or in a worse case, a civil war.

6 Other Cryptographic Tools and Comments

To any researcher working on Byzantine agreement, it is trivial that any distributed app and many cryptographic protocols are vulnerable to a Byzantine attack. However, not everybody is working on Byzantine agreement. Moreover, the research community working on blockchain has ignored many of these apps and protocols. We now give one example.

In Private Set Intersection a party P_i has a set A_i. The goal is to privately compute the intersection. Imagine we have three parties and one, let say Eve, will run the protocol, but when interacting with Aydin uses A_{Eve}, but when interacting with Bob uses, $\bar{A}_{Eve}$, the complement of A_{Eve}.

It is well known that when the network are asynchronous, solutions become more complex and more parties are needed. Note that some of our examples we provided typically are asynchronous, aggravating the problems.

Acknowledgments

The authors thank the referees for their suggestions. The first author thanks the Jonsson Endowment.

References

[1] Thomas Claburn. 2021. Computer scientists at University of Edinburgh contemplate courses without 'Alice' and 'Bob'. *https://www.theregister.com/2021/10/15/computer_scientist_terminology/* (October 15, 2021).

[2] Cybersecurity [n. d.]. Cybersecurity innovation: Leading companies in blockchain-based ticketing platforms. https://www.hotelmanagement-network.com/data-insights/innovators-blockchain-based-ticketing-platforms-travel-tourism/?cf-view.

[3] European Commission. 2024. Press release: Commission sends Statement of Objections to Microsoft over possibly abusive tying practices regarding Teams. *https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3446* (June 25, 2024).

[4] Max Holland. 2014. *Leak: Why Mark Felt Became Deep Throat.* University Press of Kansas, Kansas.

[5] Ivana Kottasová and Radina Gigova. 2024. A third girl has died in the UK after one of the worst attacks on children in decades. Here's what to know. *CNN World, https://edition.cnn.com/2024/07/30/uk/southport-stabbing-attack-explainer/index.html* (July 30, 2024).

[6] Leslie Lamport, Robert Shostak, and Marshall Pease. 1982. The Byzantine Generals Problem. *ACM Transactions on programming languages and systems* 4, 2 (1982), 382–401.

[7] Martyn Landi and Miriam Burrell. 2024. Keir Starmer warns social media firms over misinformation sparking Southport violent disorder. https://www.standard.co.uk/news/uk/southport-stabbings-keir-starmer-misinformation-social-media-protest-b1174302.html. *The Standard* (August 1, 2024).

[8] Annette McDermott. 2018. How 'Deep Throat' Took Down Nixon From Inside the FBI. *https://www.history.com/news/watergate-deep-throat-fbi-informant-nixon* (July, updated May 10, 2024 2018).

[9] Engine Tyme. 2024. How to see people invited to a meeting but are not in it? *https://answers.microsoft.com/en-us/msteams/forum/all/how-to-see-people-invited-to-a-meeting-but-are-not/d351f0d3-cef5-4162-b4fd-031d8b8f2488* (February 8, 2024).

[6] https://en.wikipedia.org/wiki/2024_New_Caledonia_unrest
[7] https://en.wikipedia.org/wiki/Gunter_Guillaume
[8] https://en.wikipedia.org/wiki/Lebanese_Civil_War