# Provably insecure group authentication: Not all security proofs are what they claim to be

## A cautionary tale

Chris J Mitchell
Royal Holloway, University of London
www.chrismitchell.net
me@chrismitchell.net

6th November 2020

# Background

- A paper presented at the ICICS 2019 conference describes a ‘provably secure group authentication [protocol] in the asynchronous communication model’.
- However the protocol is subject to a serious attack, as shown in this talk.
- Examination of the security theorem provided in the ICICS 19 paper reveals that it is not exactly what it seems to be at first sight.
- Issues raised by this are also briefly discussed.

# The scheme: security goals

- Here a *group authentication protocol* is one where ‘each user acts both roles of the prover and the verifier, and all users in the group are authenticated at once’ (Xia et al., 2020).
- Main goal is to assure all members of a defined group that the specified members are all actively involved in the protocol, and no other parties are involved.
- ICICS paper refers to both insider and outsider attacks, i.e. protocol is intended to be secure against both; also says an outside adversary cannot impersonate a group member without detection, even if it computes a token after seeing all other tokens (communication assumed to be asynchronous).
- However, no reference to trust assumptions for broadcast channel used for communications, apart from being asynchronous — it is standard practice when analysing authentication protocols to assume attacker can manipulate the communications channel, including to intercept, delete, insert and modify messages (see, for example, (Boyd et al., 2020)) — we therefore assume this here.

# The scheme: Overview

- Scheme can be divided into two phases:
  - *initialisation*, when the *Group Manager* (GM) equips each participant with the credentials needed to perform group authentication, and
  - the *group authentication phase* where a subset of the participants simultaneously authenticate each other as a group.
- Suppose that there are $n$ participants $\mathcal{U} = \{U_1, U_2, \ldots, U_n\}$.

# The scheme: Initialisation

The GM chooses/computes:

- parameters $t$ and $\ell$, where at most $t-1$ insiders collaborate, and $\ell$ is the number of sessions with these credentials.
- cyclic group $G$ (expressed multiplicatively) with order a large prime $q$, and randomly selects $g_1, g_2, \ldots, g_\ell$ to be $\ell$ independent generators of $G$ (one per session).
- cryptographic hash function $H$ with domain $G$.
- secret $s \in \mathbb{Z}_q$, and the $\ell$ values $H((g_i)^s)$, $1 \leq i \leq \ell$.
- secret polynomial $f(x) = \sum_{i=0}^{t-1} a_i x^i$ over $\mathbb{Z}_q$ of degree $t-1$, where $a_0 = s$.
- credential $s_i = f(x_i)$ for each participant $U_i$ $(1 \leq i \leq n)$, where $x_i \in \mathbb{Z}_q$ is a unique identifier for $U_i$.

Using an out-of-band secure channel, GM equips participant $U_i$ $(1 \leq i \leq n)$ with $t$, $G$, $q$, $H$, the identifiers $\{x_1, x_2, \ldots, x_n\}$, the generators $\{g_1, g_2, \ldots, g_\ell\}$, the hash codes $\{H((g_1)^s), H((g_2)^s), \ldots, H((g_\ell)^s)\}$, and the participant's secret credential $s_i (= f(x_i))$.

# The scheme: Group authentication: Notation

- Suppose some subset $\mathcal{U}' \subseteq \mathcal{U}$ of the participants (where $|\mathcal{U}'| = m \leq n$) wish to authenticate each other in a group-wise fashion, where $\mathcal{U}' = \{U_{z_1}, U_{z_2}, \ldots, U_{z_m}\}$.
- Suppose every participant in $\mathcal{U}'$ is aware of the membership of $\mathcal{U}'$.
- Also suppose that the set of participants has reached session number $\sigma$ during use of a particular credential set, where $1 \leq \sigma \leq \ell$; each session must be conducted using a new value of $\sigma$, and $\sigma$ determines which generator $g_\sigma$ from the set of generators will be used in this particular protocol instance.

# The scheme: Group authentication: Steps

Each participant $u_{z_i} \in \mathcal{U}'$ proceeds as follows.

- Choose $u_{z_i} \in \mathbb{Z}_q$ uniformly at random, and broadcasts it.
- Once the values $\{u_{z_1}, u_{z_2}, \ldots, u_{z_m}\}$ received, compute:

$$\gamma_i = \prod_{\substack{j\in\{1,2,\ldots,m\}\\ z_j<z_i}} (g_\sigma)^{u_{z_j}} \prod_{\substack{j\in\{1,2,\ldots,m\}\\ z_j>z_i}} (g_\sigma)^{-u_{z_j}},$$

$$L_i = \prod_{\substack{j\in\{1,2,\ldots,m\}\\ z_j\neq z_i}} \frac{x_{z_j}}{x_{z_j} - x_{z_i}},$$

  and

$$c_{z_i} = (g_\sigma)^{s_{z_i} L_i} (\gamma_i)^{u_{z_i}}.$$

- Broadcast $c_{z_i}$ to all members of $\mathcal{U}'$.
- Once values $\{c_{z_1}, c_{z_2}, \ldots, c_{z_m}\}$ received, compute

$$\prod_{r=1}^{m} c_{z_r}.$$

- If $H(\prod_{r=1}^{m} c_{z_r}) = H((g_\sigma)^{s})$ then all users authenticated.

# Analysis: Preliminary observation I

- We consider what can be learnt by observing a single value $c_{z_i}$ in a single instance of the protocol, together with the initial broadcasts of the values $\{u_{z_1}, u_{z_2}, \ldots, u_{z_m}\}$.
- We suppose that the (outside) observer has access to the system parameters, i.e. the values provided by the GM to all participants, namely:
  - $t$, $G$, $q$, $H$,
  - the identifiers $\{x_1, x_2, \ldots, x_n\}$,
  - the generators $\{g_1, g_2, \ldots, g_\ell\}$, and
  - the hash codes $\{H((g_1)^s), H((g_2)^s), \ldots, H((g_\ell)^s)\}$.

# Analysis: Preliminary observation II

- By definition:

$$c_{z_i} = (g_\sigma)^{s_{z_i} L_i} (\gamma_i)^{u_{z_i}}.$$

- Again by definition:

$$\gamma_i = \prod_{\substack{j \in \{1,2,\ldots,m\} \\ z_j < z_i}} (g_\sigma)^{u_{z_j}} \prod_{\substack{j \in \{1,2,\ldots,m\} \\ z_j > z_i}} (g_\sigma)^{-u_{z_j}},$$

- I.e. computing $\gamma_i$ does not involve any secret credential values and hence can be derived by anyone with the system credentials.
- If $u_{z_i}$ is intercepted, the observer can thus compute

$$c_{z_i}.(\gamma_i)^{-u_{z_i}} = (g_\sigma)^{s_{z_i} L_i}.$$

- Yet again by definition

$$L_i = \prod_{\substack{j \in \{1,2,\ldots,m\} \\ z_j \neq z_i}} \frac{x_{z_j}}{x_{z_j} - x_{z_i}},$$

so $L_i$ is also available to anyone with the system credentials.

# Analysis: Preliminary observation III

- Having derived $L_i$, the observer now computes a value $M$ such that $ML_i \equiv 1 \pmod{q}$, a calculation which is simple to perform given that $q$ is known. Note that $M$ is guaranteed to exist since $q$ is prime.
- It follows immediately that

$$[c_{z_i}.(\gamma_i)^{-u_{z_i}}]^M = (g_\sigma)^{s_{z_i} L_i M} = (g_\sigma)^{s_{z_i}}.$$

- That is, an observer of $c_{z_i}$ and the values $\{u_{z_1}, u_{z_2}, \ldots, u_{z_m}\}$ can compute $(g_\sigma)^{s_{z_i}}$, where $s_{z_i}$ is the secret credential for user $u_{z_i}$.
- Moreover, the only occasion $s_{z_i}$ is used in the protocol is to compute $(g_\sigma)^{s_{z_i}}$, i.e. knowing $(g_\sigma)^{s_{z_i}}$ is essentially equivalent to knowing $s_{z_i}$, at least for this session.

# An outsider impersonation attack: Scenario

- The above observation leads to a very simple and powerful attack, enabling impersonation of a participant in any group.
- Suppose an (outsider) adversary controls the broadcast channel with respect to 'victim' participant $U_{z_i}$, i.e. the adversary can:
  - prevent messages sent by other legitimate participants from reaching $U_{z_i}$, and
  - send messages to $U_{z_i}$ on this channel that appear to have come from other legitimate participants.
- Also assume that it is 'time' for a session using the group generator $g_\sigma$.

# An outsider impersonation attack: Gathering data

- Suppose the adversary observes a group of participants $\mathcal{U}'' \subseteq \mathcal{U}$ (where $U_{z_i} \notin \mathcal{U}''$) engaging in the protocol.
- The adversary:
  - intercepts all the $u_{z_j}$ and $c_{z_j}$ values sent by each $U_{z_j} \in \mathcal{U}''$;
  - uses these intercepted values, together with the system parameters, to compute $(g_\sigma)^{s_{z_j}}$ for each $U_{z_j} \in \mathcal{U}''$;
  - prevents any of the messages reaching $U_{z_i}$ (since these messages are not intended for $U_{z_i}$, $U_{z_i}$ should ignore them anyway).

  That is, the adversary now knows information equivalent to the secret credentials for all participants in $\mathcal{U}''$ for session $\sigma$

# An outsider impersonation attack: Completing the attack

- Suppose that the adversary persuades the victim $U_{z_i}$ that it is being invited to join a group of participants $\mathcal{U}' \subseteq \mathcal{U}'' \cup \{U_{z_i}\}$, where $U_{z_i} \in \mathcal{U}'$, e.g. by sending 'fake' messages from members of $\mathcal{U}'$ to $U_{z_i}$.
- Adversary chooses arbitrary values $u_{z_j}$ for every $U_{z_j} \in \mathcal{U}' - \{U_{z_i}\}$, and sends these values to $U_{z_i}$ as if they come from $U_{z_j}$.
- Once $U_{z_i}$ sends its value $u_{z_i}$, the adversary can use the complete set of values $\{u_{z_j}\}$ and the computed values $(g_\sigma)^{s_{z_j}}$ (which it has for every $U_{z_j} \in \mathcal{U}' - \{U_{z_i}\}$) to compute the 'correct' values $c_{z_j}$ for every $U_{z_j} \in \mathcal{U}' - \{U_{z_i}\}$, which it sends to the victim participant $U_{z_i}$.
- Since all the received values are 'correct', the victim will falsely believe that it is part of a group authentication with a set of participants, of whom none believe they are being authenticated to the victim.

# Other attack scenarios

- There are many other scenarios that could be used to launch an attack on the protocol.
- For example, if an attacker could control the broadcast network with respect to two victims, a range of conflicting beliefs about who has been authenticated to whom could be established.
- That is, once an attacker has observed a participant $U_{z_j}$ output a value $c_{z_j}$, this can be used to impersonate $U_{z_j}$ in any group the attacker chooses (assuming control over the broadcast channel).

# But there is a proof of security ... I

- The attack described above clearly breaks the claimed ‘no impersonation’ property.
- Theorem 4 of (Xia et al., 2020) states that ‘The proposed group authentication scheme satisfies the no impersonation property, assuming that $H$ is a preimage resistant hash function and the DDH assumption holds in $G$’.
- The attack does not invalidate the assumptions of the theorem, and hence the theorem must be false.

# But there is a proof of security ... II

- How can this be true?
- Examination of the proof of Theorem 4 suggests why.
- The proof only deals with the ‘honest but curious’ case, where all participants are assumed to follow the protocol correctly.
- The sort of manipulation of messages and beliefs involved in the attack do not appear to be covered by the proof.
- That is, while the mathematics may be correct, the result does not establish that the protocol would actually be secure in a real-world deployment (which, of course, it would not).

# But there is a proof of security ... III

- This issue is admitted in (Xia et al., 2020).
- In the concluding section it is stated that ‘There are two distinct approaches to defining security for cryptographic protocols: simulation proof and reduction proof.
- The former is more intuitive because it models security of the targeted problem via an ideally trusted third party. However, the definitions will become complicated once all details are filled in.
- In contrast, the reduction proof yields definitions that are simpler to describe and easier to work with. However, the adequacy for modelling the problem is less clear. In this paper, we followed the latter approach, and it is still open how to provide formal security treatment for group authentication using the simulation proof.’

# Conclusions

- The fundamental flaw exists despite the fact that theorems are provided asserting its security.
- This is clearly worrying — we know that ‘proofs of security’ are necessary, but clearly they are not of much value if they do not establish what it seems they establish.
- In fact the authors admit that the security model used is not sufficient to establish security other than in a case where the attackers are restricted to behaving in an ‘honest’ fashion.
- This clearly suggests that reviewers need the time to carefully review precise details of claims of security.
- This flies in the face of the modern obsession with speedy publication, both for conferences and many journals (e.g. *IEEE Access* allows referees only a week to complete a review).
- Perhaps we, as the research community, need to think more carefully about finding ways to allow reviewers time and space to write carefully considered and detailed reviews.

# References

- (Boyd et al., 2020): Boyd, C., Mathuria, A., and Stebila, D.: Protocols for Authentication and Key Establishment, 2nd edition. Springer (2020).
- (Xia et al., 2020): Xia, Z., Harn, L., Yang, B., Zhang, M., Mu, Y., Susilo, W., and Meng, W.: Provably secure group authentication in the asynchronous communication model. In: Proc. ICICS 2019, December 15–17, 2019, LNCS 11999, pp. 324–340. Springer (2020).