Can I believe you? Establishing Trust in Computer Mediated Introductions

Borke Obada-Obieh
School of Computer Science
Carleton University
borke@ccsl.carleton.ca

Anil Somayaji
School of Computer Science
Carleton University
soma@ccsl.carleton.ca

ABSTRACT

The problem of trust is one of the more prominent security issue in online communications. This paper critically analyses and discusses the issue of trust in computer mediated introduction (CMI) where individuals are introduced for the purpose of interacting offline. One of the most popular forms of CMI today is online dating. We evaluate and compare the attempts made to solve the problem of trust in various computer mediated communications. We further specifically analyze three online dating platforms, Match.com, Plenty of Fish, and Tinder, and compare how they attempt to establish trust between potential matches. We find that existing mechanisms are not sufficient to establish meaningful trust in online dating. While we propose some potential alternative mechanisms for establishing trust in CMIs, the key contribution of this work is to identify the security challenges that arise in computer mediated introductions as a previously unrecognized class of security problems.

CCS CONCEPTS

• **Security and privacy → Social aspects of security and privacy**;

KEYWORDS

computer security, computer-mediated introductions, online dating

ACM Reference format:
Borke Obada-Obieh and Anil Somayaji. 2018. Can I believe you? Establishing Trust in Computer Mediated Introductions. In *Proceedings of 2017 New Security Paradigms Workshop, Santa Cruz, CA, USA, October 1–4, 2017 (NSPW 2017),* 13 pages.
https://doi.org/10.1145/3171533.3171544

1 INTRODUCTION

Computers are an essential part of interpersonal relationships across the globe. Computer mediated communication (CMC) [3, 7, 30, 36, 39] is essential to how we conduct business and maintain personal relationships. When we go online, however, we must be wary. An attempted e-commerce purchase can lead to fraudulent credit card transactions. Following the wrong link in an email can result in compromised credentials. Accepting the wrong social media connection request can compromise our privacy.

While all online interactions entail some risk, some interactions are clearly riskier than others. Among the riskiest interactions are ones that cross over from the virtual to the physical. When an online interaction goes bad, we may suffer harm to our bank account or our reputation. When an in-person interaction goes bad, it may end in violence or death. It is therefore natural that we want extra guarantees for potential in-person interactions with strangers.

With individuals representing a company, say for services or deliveries, we can contact the company and verify that the representative is indeed there on behalf of the company. If we request a pick-up with Uber or Lyft, we can check the rating for the driver as well as her name, type of car, and license plate. More generally, there exist mechanisms, customs, and social institutions that allow strangers to interact with relative safety for both parties, whether that interaction was initiated via a website, email, or even by postal mail.

What works for business, however, does not necessarily apply to more personal interactions. Where the online interaction is a continuation of an already existing social relationship, such as members of a community organization corresponding via a Facebook page, the risks are low because nobody is a complete stranger. When people meet for the first time online for social purposes, however, the risks are much more significant.

Here we define computer mediated introductions (CMI) as a type of computer mediated communication in which online interaction happens between strangers for the purpose of (eventual) in-person interactions. Two classes of CMI are business CMI and personal CMI. Business CMIs involves introducing people online to meet offline for the sole purpose of exchanging goods and services for monetary value. Examples of business CMIs are Airbnb, Uber, Meetup.com, and Vayable. In personal CMI, monetary value is not attached to the exchange made, whereby people are introduced online and meet offline based on shared interests, hobbies, or to carry out similar activities. Couchsurfing and dating sites are examples of personal CMI. In some cases, some CMI platforms could serve as a means of introducing people for both business and pleasure, thereby serving as a combination of both CMIs. Examples of those include Craigslist and Kijiji. Business CMI is not fundamentally different from other online business interactions. Personal CMI, however, is different and potentially much higher risk because it takes place outside of both an existing social and business context. While personal CMI can be said to take place when one meets a group of strangers after learning about the service online (say, for a fan club), the most common case today for personal CMI is through online dating. The use of online dating sites has increased

NSPW 2017, October 1–4, 2017, Santa Cruz, CA, USA

ACM ISBN 978-1-4503-6384-6/17/10…$15.00
https://doi.org/10.1145/3171533.3171544

significantly over the years, [11, 26, 73, 75, 76] with Plenty of Fish alone having an estimated 100 million users as of 2015 and 3.5 million active members per day [65]. In our past work [59], we found that online daters use a variety of strategies to protect themselves from dangerous situations and individuals. Here we follow up on that work with a simple question: how do online dating sites help establish trust when introducing strangers to each other? What we found was not encouraging, as existing dating sites encourage its users to rely on easily spoofed indicators of trust (such as personal pictures and words) while denying them privacy-preserving tools that would allow them to better establish trust. Individuals have to move their communications off-site, either using other online platforms or by meeting in person, before they can establish that the other party has non-malicious intentions.

Our contributions are 1) defining computer mediated interactions as a threat model, 2) showing how existing solutions in the online dating space do not adequately solve the problem, and 3) proposing strategies for more trustworthy personal CMI. We hope this work will encourage further work by researchers and practitioners in improving personal CMI, particularly to help improve the online dating experience.

The rest of the paper proceeds as follows. We give background on the problem of trust in online and offline interactions in Section 2. We examine the challenge of trust in computer mediated introductions in Section 3 and we define the threat model in Section 4. In Sections 5.1, 5.2, and 5.3, we present case studies on Match.com, Plenty of Fish, and Tinder; we compare them in Section 6. Section 7 outlines our suggestions for alternative trust mechanisms for CMI. Section 8 concludes.

2 BACKGROUND

The challenge with computer mediated introductions is fundamentally one of trust. Here we review the literature related to trust in communities, reputation systems, and how online multimedia (photos, audio, and video) affect trust. We also review work in cryptography related to dating and CMI.

2.1 Trust in Communities

To foster secured and positive relationships in virtual communities, trust must exist, even if no in-person interaction ever takes place. Trust in a social context can be defined as "the extent to which one party is willing to depend on something or somebody in a given situation with a feeling of relative security, even though negative consequences are possible" [14]. The question then arises, how can trust be built or improved between two or more strangers in an online virtual community? Research has gone a long way to show that trust is better built face to face than over virtual communications. Handy insists that ultimate trust can only be formed by touch [31]. However, this cannot be applied in virtual communities, where trust has to be developed in the absence of physical contact.

Trust exists because there is the presence of risk [9, 15, 52]. According to Baier et al.[2], for a trust relationship to occur, there is usually the "Trustor" and the "Trusted". Trust must exist between the "Trustor" and the "Trusted" and in the technology applied to create the sense of trust [56]. The relationship between these parties and the risk involved has been defined thus, "If the level of trust surpasses the threshold of perceived risk, then the trustor will engage in risk-taking in the relationship" [52].

Ring & Van de Ven [71] emphasize that trust increases as the number of successful interactions occur between the trustor and the trusted. We can have some trust in interactions with a stranger if we can have some assurance that they have had successful interactions with others. Third parties can vouch for an individual's trustworthiness by attesting to aspects of their reputation. Reputation is the subjective expectation or collective ideology people have about the behavior of another based on the interaction history. It is the "aggregated opinion that people have based on past behaviors of character" [40]. Both reputation and trust are related, whereby trust births good reputation and good reputation leads to trust.

Research into security and trust in both online and physical communities has been ongoing for over twenty years. Fukuyama et al. (1995) did a study of how trust develops in physical communities. The authors believed "community strongly depends on mutual trust" and that trust happens when "community shares a set of moral values in such a way as to create expectations of regular and honest behavior" [25].

Dasgupta et al. explored the importance of building trust in virtual communities. The authors linked expectation to reputation, explaining that reputation affects users' expectation. They insist that reputation can only be built over time, whereby for reputation to be successfully developed, the trustor must have had previous experiences with the trusted party [13]. There is thus the problem of how users can form trust in online communications without having had prior encounters with the other party.

2.2 Reputation Systems

While reputation in communities is traditionally mediated by humans, work on trust in e-commerce has centered around how computer systems can serve as trusted third parties for the purposes of maintaining and disseminating reputation information. In early 2000, Zacharia et al. proposed two reputation mechanisms that could be used to address trust problems in e-commerce and other online contexts [87]. The authors proposed Sporas and Histros, which the authors explained can be applied to loosely and highly connected communities respectively. Sporas works such that new users have a standard reputation value and as transactions are being carried out, based on the reputation feedback, the user value either increases or decreases. Histros was a web-of-trust based mechanism where users trust other users because someone they know had trusted them in the past.

Cooperation in the community was emphasized by Boyd as a major requirement to build mutual trust in CMC [6]. Boyd focused his evaluation on eBay (in 2002), stating that eBay has successfully been able to build mutual trust on their platform. As a result, this has led to better security in the services offered to the community eBay built. This mutual trust according to author reemphasizes Deutsch's opinion on building trust, which states that "the trustworthy person is aware of being trusted and he is somehow bound by the trust which is invested in him" [14]. The author explains that community trust is the trust that makes eBay stronger. Boyd insists that though safety and security mechanism have been introduced,

such as escrow agents, in the online community, the major thing that safely secures eBay users is community, which Weisul in his paper refers to as "creative self-policing" [6, 81]. Boyd claims that when all transactions and interactions are made openly in the clear sight of other users then there is the high probability of people to act just and fair [6].

Li Xiong et al. also acknowledged the importance of trust to help reduce threats in online e-commerce communities. They introduced PeerTrust, a reputation system to assist in gauging the trustworthiness of those involved in online communication. PeerTrust also employed feedback based reputation model whereby peers are made to rate a transaction and the overall rating is the sum of the ratings aggregated in the past six months [85]. The authors' claim that the unique approach used in the development of their model was based on the use of five factors, which were number of transactions, credibility of feedback, feedback received from peers, transaction context, and community context. To achieve a higher value of reputation one must increase the number of transactions completed [85]. Carrara et al. also did a thorough evaluation of reputation systems and explained that a punishment and reward system is a good way to keep people in check when using CMC. The punishment could range from a drastic reduction of their ratings on the reputation systems or possibly banning them from using the system [8].

Virtually every platform today that allows providers of goods or services to be matched with customers (e.g., eBay, Amazon, Uber, AirBnB) supports some form of online reputation. Buyers rate sellers, and sometimes sellers rate buyers. Low rating can result in loss of business or complete loss of access. Similar mechanisms are even employed in online marketplaces for illicit goods and services [33], with sellers with higher reputation being able to demand higher prices.

2.3 Multimedia-based Trust

While people will factor in a reputation score into their decision as to whether to trust a stranger, people also make use of visual and auditory cues online, just as they do in face-to-face interactions—even though those channels are much easier to falsify online. We review this research below.

Bos et al. evaluated the development of trust in four communication modalities: face-to-face communication, video, audio, and text. The authors recruited sixty-six subjects and tested them with a social dilemma game, Daytrader. They observed that the group with text communication had the most difficulty building trust, and that the audio and video did almost as well as face-to-face communication. The author found it surprising that the audio and video had similar results even though the video was done in very high definition standards and the audio conversations was carried out using a cheap phone [4].

Appearance seems to matter when determining trust. Multiple researchers have observed that the attractiveness of a stranger correlates with how trustworthy they are perceived [17, 72, 83, 84]. A photograph of a person with a smile is enough to improve trust in social dilemma games [74]. Steinbrueck et al. [77] found people showed more trust in ecommerce sites when personal pictures were used. More recently, Ert et al. [20] carried out a user study of Airbnb users to discover if users are likely to trust an apartment owner more when personal photos are uploaded on the Airbnb section of their apartment ad. Their results indicated that personal pictures of the host had a greater influence than the host's reputation. Users in the study picked accommodation with places whose owner uploaded cute personal pictures, even if the reputation of those places were low. The effect was still present even when controlling for the hosts' attractiveness.

Other researchers, however, have found that the effect of pictures on trust online is not so straightforward. With online dating sites, overly attractive pictures seem to reduce trust [53, 59]. Riegelsberger et al. examined the effect of adding pictures of smiling, happy sales assistants to ecommerce sites. Using 115 subjects and twelve sites (half with good, half with poor reputations). The authors observed that the reputation of poor sites were increased by the addition of personal photos while the reputation of good sites decreased. The authors concluded that the presence of photos generally seemed to decrease participants' ability to distinguish between trustworthy and untrustworthy parties online [70].

2.4 Cryptographic approaches

Although cryptography plays a significant role in securing online interactions, it provides remarkably weak trust guarantees in practice in the context of e-commerce and computer mediated communications. TLS protects communication between backend services and mobile and web applications; however, TLS is almost never used to authenticate individuals, despite the standard's support for end-user authentication through client certificates. Cryptographers, however, have developed protocols for some online dating-related tasks.

Mikhail and Dukhovni et al. proposed cryptographic protocols to try to solve the Dating Problem. In the Dating Problem, Alice and Bob have a crush on the other, but they are unaware of their mutual interest. They would love to let the other know of their interest only if the other party is interested [16, 55].

Miers et al. also developed a protocol that could help Alice prove her Sexually Transmitted Infection (STI) status to her past match or her potential match Bob, without Bob knowing that such information came from Alice. If Bob was a past match, Bob can decide to get his STI status tested. If he is a potential match, and Bob has no problem with Alice's status and wants to be matched with her, then Alice can reveal her real identity, else she doesn't and Bob never gets to find out who Alice truly was [54].

Lysyanskaya proposed an ideal dating site that could function using cryptography. In this model, Alice and Bob are matched by a matchmaking service, SophistiCats.com. As a result of using multiparty computation or Secure Function Evaluation (SFE), SophistiCats.com has no idea who Alice and Bob are or that they have even been matched. Alice on the other hand can log on to SophistiCats.com, making use of anonymous authorization that prevents anyone from knowing her identity. After login, Alice uses anonymous channels to contact Bob and vice versa, which makes it impossible for Alice and Bob's ISP to know that they are accessing the services of SophistiCats.com or the content of the messages being sent. Alice's roommate, Eve, however knows about Alice and Bob's budding relationship as well as the content in some of the messages Bob sent. This is because Alice has discussed some

of their messages with Bob and even posted a few on her fridge. However, Eve is incapable of reading the flow of messages between Alice and Bob, however, because they are all encrypted. Also, the digital signatures Alice and Bob uses makes it possible for them to be able to differentiate real messages from fake ones [38].

3 TRUST IN COMPUTER MEDIATED INTRODUCTIONS

Computer mediated introductions (CMI) are a type of computer mediated communication where the purpose of the communication is to find—be introduced—to other individuals in order to interact in the physical world. The key challenge with CMI is the risk of exploitative, fraudulent, criminal, and even violent interactions when one is introduced to the wrong people.

Trust matters in online dating in part because of the high stakes involved in meeting a stranger in person one on one for such an intimate purpose. However, trust is also a vital issue because people generally prefer to be somewhat anonymous when meeting strangers. When interacting in public spaces, strangers will generally not exchange names or contact information until they both feel comfortable with each other. Similarly, users of online dating sites use pseudonyms and conceal contact information until some degree of trust has been established.

Unfortunately, the protection provided by anonymity is also a danger because it allows malicious actors to conceal themselves as well. Dating sites thus must provide alternatives to the subtle interaction of verbal and body language cues that help people detect deception and aggression in face-to-face interactions. All dating sites provide mechanisms to help individuals establish trust with potential matches. From our past work [59], we know that online daters go often into initial meetings with significant amounts of distrust. To compensate, they engage in a variety of risk mitigation strategies such as online searches, staying in contact with friends electronically during a date, and having third parties quietly observe the date from a distance so they can step in if anything goes wrong.

The degree of mistrust we found indicates that online dating sites do a relatively poor job of establishing trust between individuals. To understand why this is the case, we present a threat model of online dating sites and examine the mechanisms for establishing trust on three popular dating sites, Match.com, Plenty of Fish, and Tinder.

4 THREAT MODEL OF ONLINE DATING SITES

Understanding the threats that dating site users face and how they occur can help us better define strategies that will mitigate against these threats. To better understand the security issues in online dating here we present a simple dating site threat model.

4.1 Definitions

Alice and Bob: People seeking matches.

Irene: The party carrying out the introduction of potential matches to Alice and Bob. (Irene could be a person or an online service.)

Before the Match: The time from when Alice and Bob signs up for Irene's services and when they get matched. During this period, Alice and Bob are expected to submit their information directly to Irene, complete Irene's profile template, or link their profiles from existing 3rd party services. Once this is completed, they can actively start searching for potential matches' profile or wait for Irene to suggest possible matches to them.

During the Match: The time during which Alice or Bob interacts online with a potential match found via Irene's services. The decision on whether to proceed to meeting a match offline is usually made within this time period.

After the Match: The time period where Alice and Bob meet offline after their introduction online.

Successful and Unsuccessful Introductions: The aim of dating sites is to introduce people online for the purpose of eventually dating and having a romantic relationship offline. Therefore, an introduction is successful only if Alice and Bob go out on a date and neither is harmed (e.g., assaulted, defrauded) as a result of the meeting. Otherwise the introduction is unsuccessful.

us

4.2 Before The Match

4.2.1 Alice and Bob's Roles.

(1) **Sufficient Background Information:** Alice and Bob's role at this stage is to truthfully provide Irene with current background information she requests. It could range from telling Irene their hobbies, to likes and dislikes, to providing very personal information. The information can be verbally given to Irene or can be collected by filling out required fields in Irene's profile template. Depending on the type of services offered by Irene, Alice and Bob may have already given such information to other 3rd party services, such as Facebook, and are only required to link the information to Irene's services. Alice and Bob should always provide truthful, current and sufficient information to Irene to ensure they are properly matched. Alice and Bob are also required to update the information given to Irene as their requirements or other information change.

(2) **Notification of Genuine Interest:** If Alice or Bob find profiles of other users that they are interested in, they should notify the potential match and/or Irene of their interest.

4.2.2 Irene's Roles.

(1) **Detailed Information Requirements:** Irene should request information from both Alice and Bob that will help her choose appropriate matches for them. This information should also be able to assist Alice and Bob in determining whether a potential match is of interest.

(2) **Verification of Information Collected:** Irene should verify that she has all the requested information or that all the required fields in Alice and Bob's profiles are complete.

(3) **Authenticity of Identity:** Irene should verify the authenticity of Alice and Bob's identity. Irene should also perform a background check to ensure that they are not likely to be malicious or otherwise dangerous towards potential

matches (e.g., have they been convicted of fraud or sexual assault).

(4) **Secured Protection of Information and Identity of Users:** It is Irene's responsibility to employ security mechanisms that will ensure the protection and integrity of Alice and Bob's information as well as protect their identity, such that Alice and Bob's information and identity cannot be compromised in the event of a system's breach.
(5) **Preserve Users' Privacy:** It is Irene's responsibility to ensure that only the information given to Irene by Alice for use in Irene's services is made available to Bob and vice versa. Information provided to Irene that is for Irene's use only (e.g., email and mailing addresses) should not be disclosed to any third party, e.g., Alice's email address should never be disclosed to Bob. At Bob's request, Alice's access to Bob's information should be withdrawn promptly by Irene.
(6) **Authentic Claims:** It is Irene's role to clearly explain the features she offers and to make authentic claims of the viability of her services. The claims made should not in any way misinform Alice or Bob.
(7) **Availability of Potential Matches:** It is the role of Irene to make potential matches available to Alice and Bob. This could be done through search functions, suggestions from Irene, or a combination of both.

4.3 During the Match

4.3.1 Alice and Bob's Roles.

(1) **Honest communication:** It is the role of both Alice and Bob to honestly communicate with each other.
(2) **React to Matches:** It is the role of both parties to react to matches during this time frame. Reaction could involve blocking, reporting, flagging, ignoring, cutting off communication, or continuing communication with matches. Both may also continue to search for other potential matches.

4.3.2 Irene's Roles.

(1) **Effectively React to Users' Requests:** It is Irene's role to effectively act on Alice and Bob's requests made during matches.

If Alice *flags* Bob as acting inappropriately, it is the responsibility of Irene to verify Alice's claim and if true, take proper sanctions.

If Alice requests that Irene *blocks* Bob from contacting her, Irene should carry out this request such that Alice and Bob will be unable to contact each other through the platform. (If Irene preserves Alice's privacy and Alice has not disclosed identifying or contact information to Bob directly, Bob will not be able to contact Alice outside of the platform.)

If Alice requests that her profile be *deleted* from Irene's pool of profiles, it is Irene's responsibility to ensure that Alice's profile is removed and made completely inaccessible to other profile owners.

(2) **Preserve Users' Privacy:** It is Irene's responsibility to ensure that Alice and Bob's privacy is protected and only disclosable information provided to Irene is made available to Bob. At Alice's request, such information should no longer be available to Bob through the platform.

Irene should also keep all past, present and future communications made by Alice to other members strictly private and confidential to Alice. In other words, Bob should have no knowledge of when or if Alice contacts other members using Irene's services.

In addition, during the match, Irene should also ensure she carries out the following roles:

(3) **Secured Protection of Information and Identity of Users**
(4) **Authentic Claims**
(5) **Availability of Potential Matches**

4.4 After The Match

4.4.1 Alice and Bob's Roles.

(1) **Honest communications:** It is the role of both Alice and Bob to continue communicating honestly offline.
(2) **React to Matches:** Reaction should be due to honest communications between both parties. Reaction could include blocking, reporting, flagging, cutting off communication, or dating the match. They may also seek out other potential matches. The reactions at this stage essentially determine if the introduction was successful or unsuccessful.

4.4.2 Irene's Roles. Irene's Role after the match is essentially the same as her role during the match. While Irene is mostly out of the picture after a successful introduction, if an introduction was unsuccessful, Irene may be required to carry out the following roles:

(1) **Effectively React to Users' Requests**
(2) **Preserve Users' Privacy**
(3) **Secured Protection of Information and Identity of Users**
(4) **Authentic Claims**
(5) **Availability of Potential Matches**

4.5 Scenarios

Both malicious and non-malicious factors could lead to an introduction being unsuccessful. While we may not be able to control the roles that Alice and Bob assumes, we can however make efforts to control the roles that Irene carries out so as to ensure users safety. Here we give examples of scenarios that could vary the outcome of an introduction in dating sites and specify the roles Irene failed to carry out that could have changed the negative outcome of an introduction.

The scenarios below all assume the following. Alice is seeking love and companionship. She wants to meet more people beyond her everyday social interactions and improve her relationship life. Alice decides to engage the services of Irene, who specializes in introducing strangers with similar interests, in the hope that they find love. Irene offers both free and paid services, with the promise of offering better services should her users pay. Alice obtains a profile template from Irene and truthfully fills out personal and confidential information about herself, with the belief that the more Irene knows, the better the chances of her introducing someone

Alice will like and vice versa. Alice hands back her profile to Irene, who includes it in her pool of countless profiles. Alice trust that Irene is a credible introducer who only has valid profiles in her pool of profiles.

4.5.1 The Ideal. Bob is also in search of love. He had previously truthfully filled out his profile and submitted it to Irene. Both Bob and Alice believes that, like them, everyone is also sincere in filling out their profiles. Irene introduces many profiles to both Alice and Bob. These profiles were profiles Irene found similar to their submitted profiles. Engaging the services of Irene also meant Alice and Bob could go into the pool of profiles Irene has and look at other submitted profiles to decide for themselves if they would like to date the person with the profiles. Alice and Bob now have many profiles at their disposal. Of all the profiles Alice was introduced to, Bob's profile caught Alice's attention the most. Alice decides to contact Bob through the online space Irene provided and sends Bob a message. Bob sees Alice's message and gets Alice's profile from Irene to find out if he likes her profile. Bob decides he liked Alice's profile too and chats with her online for a while. Both Alice and Bob eventually meet in person and Bob finds out Alice was who she claimed to be in her profile and vice versa. They go on a couple more dates, fall in love and eventually get married. The introduction made by Irene in this case was successful.

4.5.2 The Graceful Ending. In this case, Irene gives Alice, Charlie's truthfully completed profile and vice versa. Charlie, like Alice, is also looking for love. Both Charlie and Alice decide to chat in the online space Irene provided. After few online interactions, they find out they don't have as much in common as they thought they had and didn't really like each other. They decide to end things. Alice and Charlie both disposes of each other's profile and goes back to Irene to get more profiles with similar interests. In this case the introduction was unsuccessful.

4.5.3 One-sided Interest. Cole like Alice is also in search of love. Cole truthfully completes his profile and gives it to Irene. Irene gives Alice Cole's profile and vice versa. They both decide they like the other's profile and resolve to interact in Irene's online space. After chatting online for a while, Alice finds out that she doesn't like Cole as much as she thought and decides to end all interactions with Cole. Cole on the other hand feels he has found his soulmate in Alice.

Cole starts harassing Alice online as a way to get her attention. Alice decides to report the situation to Irene. Irene blocks Cole from accessing Alice's profile and communicating with Alice through her service. Cole, however, has saved Alice's profile details. In that profile Irene had included enough identifying information (such as Alice's real name) such that Cole can find Alice on other online platforms. Cole finds and proceeds to harass Alice on other social media, outside of the control of Irene. This introduction was unsuccessful.

Irene failed in the following roles:

(1) Effectively react to users requests
(2) Preserve users' privacy

4.5.4 An Incomplete Profile. Irene gives Alice Cody's profile and vice versa. However, Cody's profile is incomplete and omits a number of details about himself. Alice decides the little Cody wrote about himself was interesting and resolves to interact with him online. Not long after, Alice found out Cody wasn't someone she wanted to keep talking to and decides to break off all communication with him. She blocks him from accessing her on Irene's service.

Cody has major issues with anger and rejection. Irene's profile template, however, asked no questions about anger issues or mistreatment of past partners. Cody uses information in Alice's profile (saved to his own computer) to find and harass her on other social media. This introduction was unsuccessful.

Irene failed in the following roles:

(1) Detailed Profile Requirements
(2) Verification of Profile Completion
(3) Effectively reacting to users' requests
(4) Preserve users' privacy

4.5.5 A Killer. Alice was introduced to Cam through Irene's "Soul Mate Match" special feature. Getting a match through this feature rarely happened and Irene claimed the feature only showcases people she was strongly confident Alice will date. Alice's understanding of the feature was that, of the possible matches Irene suggested, Cam had to be her soulmate and was therefore the best match for her. As such, Alice was confident she had found the one. Both Alice and Cam were looking for love. However, unknown to Irene and Alice, Cam had a bad criminal record and a violent past. Both Alice and Cam seemed to like each other a lot when they interacted online. They eventually decided to meet in person.

Cam almost instantly became obsessed with Alice on meeting her in person for the first time. Alice, on the other hand, didn't think she liked Cam as much as she thought she would. She decided to end their first date earlier than planned. Cam followed Alice home, broke into her apartment, and raped Alice. When Alice threatened to tell the police, Cam killed Alice. This introduction was unsuccessful.

Irene failed in the following roles:

(1) Detailed Profile Requirements
(2) Authenticity of Identity
(3) Authentic claims

4.5.6 Blackmail. While Alice is seeking love, Dave is not. Dave deceitfully fills up the profile template he got from Irene and hands it back to her. Irene suggests Dave's profile to Alice as a profile that closely matches hers and Alice loved Dave's profile. Irene also gives Dave Alice's profile and Dave sends Alice a message almost instantly. Dave chatted with Alice for a couple of weeks and then requests nude pictures. Alice sends him a few and Dave also sends Alice a couple of pictures without properly showing his face. Dave requests more nudes and Alice sends him some more. Afterward, Dave started demanding for money from Alice and threatened to release the nude pictures to her Facebook contacts if she refused to pay. Alice was scared because she knew Dave could easily find out her Facebook name and access her friends. Alice couldn't report to Irene as that would only make Dave carry out his threat. Alice decides to give Dave the money he requested for. However, Dave could never get enough and he kept demanding for more. Alice kept giving him but she knew she couldn't keep up. Alice reputation was paramount to her and she only sent the nude pictures to Dave

because she thought he truly cared about her. Alice slowly slid into depression and eventually committed suicide. This introduction was unsuccessful.

Irene failed in the following roles:

(1) Authenticity of Identity
(2) Preserve Users' Privacy

4.5.7 Fraud. Alice was introduced by Irene to Dan's profile, and after talking online with Dan, Alice felt like she had found true love. Dan on the other hand had a very deceptive profile linked to a fake Facebook account. Dan insisted they meet in person and Alice obliged. While on their date, Dan sedated Alice and stole all her credit cards, money, and jewelry. After Alice woke up and discovered what had happened, she decided to report the incident to Irene and the police. However, when Alice went to Irene's pool to get more information about Dan from his profile, she discovered that Dan had removed his profile from Irene's service and cancelled his account. Dan's fake Facebook profile had also been deleted. This introduction was unsuccessful.

Irene failed in the following roles:

(1) Authenticity of Identity
(2) Preserve Users' Privacy
(3) Effectively reacting to users' requests

4.5.8 Trafficking. Devon has also deceitfully filled out the profile template he got from Irene. Devon's profile included pictures of places he claimed to have traveled to. He stated on his profile that he loved exploring new cities and he was looking for someone who would be willing to travel the world with him. Alice had listed traveling as one of her hobbies, so she was elated when Irene introduced Devon's profile to her. Devon and Alice chatted in the online space Irene provided and Alice was pleased at how much she seemed to have in common with Devon. After a while, Devon explained to Alice that he was out of the country exploring a new Island. He told Alice he would really love to see her in person but he didn't want to wait to travel back to where Alice was. Devon suggested Alice meets him on the Island where he was currently, so they could explore the place together, after which they could travel back. He offered to bear the cost of transportation and accommodation involved in carrying out the trip. Alice agreed to Devon's suggestion as it seemed like a dream come true for her. However, when Alice got to the Island, she realized it was all a scam and Devon was a sex trafficker. Alice was stripped of all her belongings and was denied access to the Internet. Alice tried to run away and alert the Island authorities, but all efforts proved futile as she was a foreigner in the Island. In the end, not only was Alice held against her will, she also ended up contracting various sexually transmitted diseases. This introduction was unsuccessful.

Irene failed in the following role:

(1) Verification of Information Collected
(2) Authenticity of Identity

4.5.9 Hacking. Henry has been surveying Irene's pool of profiles for a while now and analyzing the mechanism she uses to operate and deliver her services. After a couple of trials, Henry was successfully able to hack into Irene's large pool of profiles and released the personal details of many of Irene's users to the internet. Henry went on to blackmail other users with the threat of releasing their confidential profile details as well as their identity. Henry was also able to get some credit card details of users who paid for Irene's service.

Irene failed in the following roles:

(1) Secured Protection of Profiles and Identity of Users
(2) Preserve Users' Privacy

5 TRUST STRATEGIES BY DATING SITES

We now analyze the mechanisms employed by three popular dating sites to develop trust and ensure safety of their users.

5.1 Case Study: Match.com

When new users signup to Match.com, a welcome message and registration confirmation notification is sent to the email address used to register. Match.com sends another email with an optional verification link, which if left unclicked, does not in any way stop the user from making use of the service. Users are also made to fill up their profiles during sign up where they give information about themselves, both personal and otherwise, that could assist them in being matched. Match first must approve a profile and picture before it can be displayed. Users can also sign up on Match.com using their Facebook account.

Match has both a free and paid version. With the free version, users receive notifications when prospective matches have shown interest in them or sends them messages. However, users are not allowed to see the pictures/profiles of these people or the messages sent until they have fully subscribed to the service. If users fail to subscribe, Match.com will continue to send regular updates of events happening on their account which the user can only see after subscription.

We now describe the various mechanisms Match.com employs to establish trust between potential matches.

- Match.com provides users the ability to be able to block and unblock other users from contacting them. Users can block no more than 2000 members, after which users will have to unblock old users for them to be able to block new ones. Users can also report people they do not feel comfortable interacting with. The options are displayed as "Block from contact," "Block from search," and "Report a concern" [50]. The blocked members are usually unaware that they have been blocked and can still view the user's profile and send messages. However, the user who blocked the member will be unable to receive any messages sent from them [44] . Cobb et al. explains that dating sites users feel "empowered" by the ability to be able to block other users they would rather not communicate with [10]. They tend to feel a sense of safety knowing they can control those they communicate with and vice versa, which in turn helps users better trust the platform [5, 79].
- The site also gives the option of viewing only users with profile pictures. Previous research has shown that users who have more photos are generally more trusted than those who don't, whereby users are more likely to contact those with profile pictures than those without [22, 32, 34, 82]. Also, while profile pictures are being reviewed by

Match.com's customer service team, the pictures are usually not displayed [43]. Therefore profile pictures give users more confidence that the profiles as well as the pictures have been approved by the site.

- Match.com uses the frequency of users' logins as a way of building trust in users. Users generally trust profiles with more recent logins, as this is viewed as an indicator of a person's reliability, seriousness and availability [19].
- Match.com always indicates that a more completed profile gets more attention [42], which in turn suggests to users that complete profiles are more trustworthy.
- Match.com also offers *Mutual Match, Daily Match* and *Singled Out* features. These features present potential matches to users as selected by Match.com. The site explains that the matches have been chosen from their large pool of users based on compatibility [47, 49]. Of their Singled Out feature, Match.com explains that they have high confidence that the selected few singled out will be potential dates for users [49]. This helps users trust that they will most likely be interested in dating members gotten via these features.
- Subscribed members generally have many more benefits than non paying users, such as being able to receive and send messages to other users, even if a profile is yet to be approved by the site [48]. While explaining the benefits of paid subscription, the site states that subscription, "creates a more secure environment and helps ensure that those you're communicating with are as serious in their search as you are." [46] This encourages users to trust paid subscribers more than non paying users.
- Users have the option of filling out their profiles at sign up or at their own convenience. After the profile section has been filled out, Match.com's customer care team takes some minutes to approve the profile before it is displayed. During this period, free users cannot send messages, though paid subscribers are free to communicate even if their profile are yet to be vetted. This process helps users trust that everyone's profile on the site are being vetted by Match.com's team and can be trusted. It also creates a sense of trust in the service provided, with users feeling that someone, somewhere is watching out for them, when in reality this is not necessarily the case [51, 68].
- Match.com advertises upcoming events for singles to participate in. This helps creates a sense of community for those that attend the events and aids in building trust.

5.2 Case Study: Plenty of Fish (POF)

Plenty of Fish (POF) is one of the largest free dating sites available [64]. The site however has an upgraded version which users have to pay for in order to put their pictures in major searches and be seen by more people. However, the basic services offered by dating sites, such as viewing pictures, receiving and sending messages, and finding matches, are offered for free. During sign up, users fill out their profiles which includes personal details and basic interest questions. Like Match.com, POF does not verify your account through your email address. After signing up, new users receive a welcome message from the CEO, after which the users can go on to the site and find people of similar interests.

Like Match.com, POF uses several mechanisms to establish trust between potential matches.

- POF does not allow users to change their birthdays or gender after two weeks of signing up for the service. We believe this is a safety and precautionary measure taken by site, which helps to build trust in the profiles of the users, whereby users are certain their potential match is unable to change their age in order to fit another user's criteria.
- Users who present a variety of pictures on the site are viewed as more trustworthy, with the site encouraging users to upload a minimum of 3 photos, explaining that the more pictures users put up the more people will be able to know how they truly look like [28]. These multiple pictures helps builds confidence in people, making them believe that they are interacting with the same person and not fake individuals. The site further states, "POF users with at least 10 images on their profile receive 8 times more messages!" [18, 62]
- POF claims to delete accounts with sexual language. They explicitly state, "If your profile contains sexual language of any kind your account will be deleted." The site also explains that once a user is deleted, they will be prevented from signing up again. This helps users better trust the services offered on the platform. However users can sign up again simply by using a different email address.
- POF also has a feature called *"Rate Images"* where they display a series of profile pictures that are mostly inappropriate and ask users to make POF better by rating these pictures. They also present instructions on how these pictures should be rated. By enabling users to enforce community guidelines, POF implicitly builds trust in the community of potential matches on the site.
- POF also provide login updates of users, showing users that are consistently logged in. This helps users identify active members and trust that those they are interacting with are actively involved in the platform.
- POF gives users the option of receiving messages only from upgraded users. The sites states that, "The best way to be successful on POF is to become an Upgraded Member." [61] This creates a form of trust in users, making them believe that those "upgraded" profiles are sincere users and not scammers.
- POF also has a section that displays mutual matches for users tagged "My matches" which states, "None of the users who have messaged others for sex/intimate encounters show up in your matches. If you want to prevent people who have messaged others for sex or intimate encounters from contacting you, you can block them entirely here." This filter helps users trust that those they are interacting with have never committed those acts; however, while the account may not have been used to message others for intimate encounters, the individual behind the account may have. [68]

Feature	Match.com	POF	Tinder
Block/Unmatch users	Yes	Yes	Yes
View only users with pictures	Yes	Yes	No
Warning about fraudsters	Yes	No	No
Report users	Yes	Yes	Yes
Frequency of users' login	Yes	Yes	No
Completed profiles	Yes	Yes	No
Subscription to paid versions	Yes	Yes	Yes
Delayed approval of profiles and pictures	Yes	No	No
Events	Yes	Yes	Yes
Special Features	Yes	Yes	Yes
Facebook verification	No	No	Yes
Instagram verification	No	No	Yes

Table 1: Mechanisms used in online dating platforms that helps build trust in other users.

5.3 Case Study: Tinder

Tinder is a dating platform that currently only works on mobile devices. Unlike Match.com and POF, Tinder requires that all users to sign up with a Facebook account. This Facebook profile becomes the primary data source for a user's Tinder profile. After sign up, users can see pictures of other users that are within close range. If two users indicate mutual interest by both "swiping right" on the other's picture, a match is formed and both parties can begin chatting.

Tinder's strategies for establishing trust between potential matches is a bit different from those of Match.com and POF.

- A major way Tinder builds trust is by allowing users to sign up on the platform only through their Facebook account. This is Tinder's method of verifying users are who they claim to be and checking people's identities. While this seems like a better strategy employed than other conventional dating sites, this however does not stop creeps and scammers from creating fake Facebook accounts with the sole purpose of using them on Tinder [57].
- On Tinder, while users can adjust the distance within which a match can be searched for, users cannot change the location from which the search is made from. Tinder applies a user's Facebook location or the current GPS location of the user's phone, depending on the chosen setting. This helps build trust in users that people are actually where they claim to be. To change location to a specific place, get your profile boosted to the top searches once a month, turn off ads, control who sees you, make their distance invisible and other features, users have to pay a fee.
- Tinder has *Tinder social*, where users' friends can invite them to go out on a Tinder social. This brings a form of community feeling to the site for those who choose to engage in the social. Tinder also allows the creation of groups on Tinder social.
- Though not everyone uses Instagram as an additional feature, Tinder allows people to also connect their Instagram account to the site to help build trust.
- Key profile information derived from the linked Facebook account must be changed on Facebook in order to change those values on Tinder. Thus, a user cannot change their name and interests privately on Tinder; those changes will also be visible to their friends on Facebook. Note that age can only be set at profile creation time; it will not be updated even if a person's birthdate is changed on Facebook.
- Tinder also has "verified" badges to confirm the authenticity of profiles; however, it offers this feature only to celebrities, brands, and public figures. For those people to get the verified badge they have to send an email to an authorized email address. The key question though is, why would a public figure want to be verified on a dating application or site?
- Tinder users also have the option of reporting users. When a user is reported, Tinder bans the user for a couple of days, in which they review the account [80]. If reported users want to clarify their stand to Tinder, they have to send an email to Tinder. Users can also block or unmatch with someone if they please. However once you block a user, it is permanent, and they cannot be unblocked. Blocking means you completely disappear from the other person's search, such that you will be unable to message them and vice versa.

6 COMPARISON

Based on experiments and the findings in the case study listed above, we now compare the roles carried out by the introduction services, Match.com, Plenty of Fish (POF) and Tinder, with those carried out by Irene in an ideal situation.

(1) **Detailed Information Requirements:** Although POF and Match.com require users to answer some personal questions in order to be matched, there is currently no profile requirement question that will enable users to know about their matches' personal and social vices or habits. Though such information may not readily be given, the presence or obvious absence of such information can help users better decide on who they would rather be matched with. Tinder on the other hand does not ask for personal user preferences to aid matchmaking, but simply makes use of the users' Facebook profile.

(2) **Verification of Information Collected:** In Match.com and POF, users' profiles do not need to be completed in order for users to interact with potential matches or for the dating service to suggest potential matches to them. This also applies to Tinder whose users' Facebook profiles do not need to be completed for a match to occur.

In the case of Match.com, profiles are checked to ensure the absence of offensive words [51], however users are sent matches almost as soon as they sign up, even before profiles are checked and approved.

When signing up on POF, while all profile fields are marked "required", they do not need to be filled up for users to make use of their services. Users' profile are also not vetted for content. The site also states that they delete pictures which do not meet their requirement [60, 63], however they give the responsibility back to users through their *"Rate images"* feature.

(3) **Authenticity of Identity:** Our definition of authenticity of identity specifies that users are checked to ensure they do not have previous traits or record that could jeopardize the safety of the other. POF and Match.com do not authenticate the identity of their users. Tinder attempts to use Facebook as a means of authenticating its users; however, Facebook does not carry out any background checks or prevent users with past criminal record from signing up for their services [21].

(4) **Secured Protection of information and Identity of Users:** Instances of security breaches, where users' information was leaked has been reported on all three dating services [24, 27, 29, 35, 37, 58].

(5) **Preserve Users' Privacy:** On Tinder, users' Facebook information is used as their profile information. Users can also subscribe to Match.com through Facebook and have the option of uploading their Facebook pictures to the platform. In Match.com, non-active members' profiles can be seen [41, 51]. The site also retains users profiles in their database after deletion [1, 23, 45, 86]. In POF, profiles can be indexed by search engines, making them accessible to anyone via a properly crafted query.

(6) **Authentic Claims:** Dating sites such as Match.com and POF feature testimonials about others that have successfully found matches yet do not show the potential downsides to online dating (beyond straightforward safety tips). Match.com was sued by a woman, Mark Kay Beckman, whose match stalked her and stabbed her multiple times. Beckman argued that dating websites should include safety disclaimers similar to those on cigarettes warning customers about the risks they are facing. [67]

(7) **Effectively React to User Requests:** Blocking of users on Match.com, POF and Tinder does not prevent the user from being contacted through other linked social media platforms.

Table 2 summarizes the comparisons between Irene's ideal roles and the roles currently played by the dating sites surveyed, while Table 1 summarizes the key mechanisms the surveyed dating sites use to establish trust between potential matches. What is remarkable about Table 1 is that *none* of the mechanisms are robust against a malicious adversary. Anyone reading a dating profile asks themselves, "Is this really who they are? Are they leaving out important details? Are they outright lying? Are those pictures even real?" These are basic questions that we constantly ask when we meet someone new. In person we can look a person in the eye in order to assess their intentions. While con artists and actors can imitate sincerity, in-person cues are generally solid mechanisms for establishing trust.

In contrast, every trust signal presented by dating sites can be easily manufactured. Social media accounts can be faked. Time of login can be faked. A complete profile can be faked. A blocked user can create a new account and attempt contact again. None of these signals represent a significant impediment to parties who wish to misrepresent themselves. Today, then, it is unwise for individuals to go into a first in-person meeting with a significant level of trust if their only previous interaction has been through an online dating site. Having a friend sitting at the bar watching the progress of your date may in fact be a good idea.

But can we do better?

7 ALTERNATIVE TRUST MECHANISMS

There are a variety of ways that dating sites, and computer mediated introductions in general, can improve the level of trust potential matches have in each other. We discuss these below in terms of what can be done in three phases: before the match, during the match, and afterwards.

7.1 Before the Match

Dating sites could take steps to not just recommend users, but actually verify the users they recommend. Such verification is common in other contexts, such as obtaining credit, applying for a job, getting a security clearance, and working with a traditional community matchmaker.

The use of general email addresses as a single identifier of a person, should be discouraged. Making use of other forms of verification of the identity of people should be considered. Couchsurfing [12] verifies their users by verification of their payment method, phone number, address and government ID. Similar steps could be taken by dating sites. Further, dating sites could do credit and background checks. At scale such searches of already existing databases need not be expensive or time consuming. While users do not need to know the true identity of who they are matched with initially, ideally the dating site should be able to adequately vouch for the person's identity and general reputation.

Dating sites could also take steps to properly bind the individual using an account to the identity claimed. For example, sites could have users take selfies with a mobile app. These selfies can then be compared with the uploaded pictures on the site. The selfies do not have to be placed as profile pictures; they only need to be seen by dating sites administrators (or their automated proxies) for verification purposes. By requiring the capturing of a live image, it makes it much harder for an adversary to misrepresent their appearance.

Irene's Ideal Roles	Match.com	POF	Tinder
Detailed Information Requirements	No	No	No
Verification of Information Collected	No	No	No
Authenticity of Identity	No	No	No
Secured Protection of Information and Identity of Users	No	No	No
Preserve User's Privacy	No	No	No
Authentic Claims	No	No	Yes
Availability of Potential Matches	Yes	Yes	Yes
Effectively React to User's Requests	No	No	No

Table 2: Comparison of Irene's ideal introduction roles with those offered by Match.com, POF and Tinder

While Tinder employs Facebook as a verification method, it does not absolutely protect users as a Facebook profile can be very easily forged. Dating sites users will most times prefer to remain anonymous, so using Facebook accounts to get a profile picture and profile defeats the whole purpose of anonymity on dating sites. If a user decides to block another on a dating site, the blocked user can find the user on Facebook, which could have the same picture used on Twitter, LinkedIn, and other social media accounts. Therefore, making users sign up with their Facebook name and profile may cause people to create fake Facebook accounts instead for perfectly legitimate reasons. However, having the site verify these accounts would go a long way in solving the problem of fake accounts and reduce the ease at which people can commit crimes and change their identity.

If verification features cannot be applied to the free version of dating sites, then they should be applied to the paid or upgraded versions. At the moment, paid versions of dating sites often put the paid users at the top of searches, thereby increasing their exposure to fraudsters. Paid versions of dating sites could instead ensure users interact with only verified members while also being verified by the means outlined above. Though this may not completely eliminate the creeps or con artists, it will go a long way in reducing their activities on dating sites.

People on dating sites should also be clearly able to differentiate between verified and non-verified members. Match.com writes about a verified badge, but it is unknown what it looks like or which members have been verified. Verified badges should also be for everyone who requests and possibly pays for it, not just for celebrities as is the case with Tinder.

Tinder also tries to build reputation by putting a number next to a Facebook friend. The first number means "you and your match are both friends with this person." The second next number to the Facebook friends' picture means that your friend knows someone who knows your last match [78]. While this is a great idea, it should be applied specifically on dating sites, if possible, and not through Facebook, because as previously discussed, the use of Facebook as a means of verification on dating sites should be discouraged.

A "Rate the Interaction" field could be introduced on dating sites where by early on in a conversation with someone, a user is presented with the option to rate an interaction, based on the speed at which the person replies messages, the tone of conversations, use of words, and the overall quality of the interaction. This rating should be gathered during the early stages of a matched pair's interactions so the rating is of the initial interaction rather than the quality of an ongoing relationship. Such ratings would help users filter out those who are rude or otherwise obviously antisocial.

7.2 During the Match

Dating sites should make use of more user friendly messaging interfaces that encourage users to remain on the platform and continue their conversations on-site. As in the case of Match.com and POF, while their mobile versions do a reasonable job, it is harder to have a conversation with a match using the web interface. Any such difficulties assist con artists when they encourage targets to move their conversations to other messaging platforms.

"Safety" links with tips on dating site guidelines and safety measures should be made more visible to users. If users do not know such links exists they would not be able to read them and better protect themselves.

As text-based chatting has been identified as having major issues in developing trust in humans [4], other methods of communication should therefore be supported. The dating sites could offer 3 communication steps to users as a way to better verify their dates before meet up. Step 1 could involve text based chats, Step 2 could involve voice based communication with the match for a duration of time, and Step 3 could involve a limited-time video conversation.

7.3 After the Match

This step is the core of CMI that differentiates it from other CMC. If proper precautionary measures are taken before and during the period a match is formed, then making use of this step may not be necessary.

One method that could be looked into by dating sites to ensure the security of users on date is to employ the use of something like the panic button mechanism developed for Uber's customers in India. Once this button is pressed on the app, an incident response team is triggered and the police are alerted immediately. Details about the trip is also immediately sent to those being contacted [66]. Similar feature could be applied on dating sites to further protect their users.

7.4 Evaluating Security Mechanisms for Personal CMI

As with other security mechanisms, it will be important to evaluate whether any new mechanism actually improves the security of online dating. The most straightforward evaluation strategy would be to gather feedback from users after they meet with a match

offline. However, as previously stated, getting feedback from dating sites users can be difficult because of the type of interaction that occurs on the platform.

In other CMI interactions, such as Airbnb, guests and hosts give feedback because they have incentives to do so: hosts want to attract more guests, and guests want to be appealing to hosts so they can stay where they want for a reasonable price. These same incentives do not hold on dating sites. Indeed, the goal of most users of dating sites is to stop using them—once they've found someone to date!

Ideally, dating sites would need feedback from users once they meet in person so that patterns of misrepresentation or fraud can be addressed. We are yet to identify effective means through which adequate feedback can be gotten from users as soon as an offline interaction occurs. Periodically, dating sites could engage researchers to carry out user studies in order to find out the effectiveness of the suggested trust mechanisms. The cost, challenge of scale, and invasiveness of any such study, however, make such research extremely challenging. To make more secure platforms for CMI, however, we will need to address these challenges.

8 CONCLUSION

Rheingold rightly stated that, "computer mediated communications provide new ways to fool people" [69]. Computer mediated introductions (CMI) introduce strangers online and bring them together offline. Personal CMIs, specifically dating sites, are not adequately served by standard security practices such as cryptographic authentication and ratings-based reputation systems. In this paper, we evaluated the mechanisms used in three popular dating websites and explain why they are not sufficient to ensure the safety and security of their users. We also suggest alternative mechanisms, such as picture verification and multimedia chat, that could be employed to improve trust with CMIs. The most important contribution of this paper, however, is to identify computer mediated introductions as an understudied area of computer security. We hope this work will encourage others to further study this problem through user studies and the development of technical mechanisms specialized to the CMI problem.

REFERENCES

[1] Erin Anderssen. 2011. You deleted your dating profile. Is it really gone? https://www.theglobeandmail.com/life/the-hot-button/you-deleted-your-dating-profile-is-it-really-gone/article615323/. (2011). Online; Accessed: 2017-07-11.

[2] Annette Baier. 1986. Trust and antitrust. *Ethics, University of Chicago Press* 96, 2 (1986), 231–260.

[3] Prashant Bordia. 1997. Face-to-face versus computer-mediated communication: A synthesis of the experimental literature. *The Journal of Business Communication (1973)* 34, 1 (1997), 99–118.

[4] Nathan Bos, Judy Olson, Darren Gergle, Gary Olson, and Zach Wright. 2002. Effects of Four Computer-mediated Communications Channels on Trust Development. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '02)*. ACM, New York, NY, USA, 135–140. https://doi.org/10.1145/503376.503401

[5] Megan Bostic. 2015. 18 Honest Lessons About Online Dating From Someone Who Has Been There. http://thoughtcatalog.com/megan-bostic/2015/12/18-honest-lessons-about-online-dating-from-someone-who-has-been-there/. (2015). Online; Accessed: 2017-06-30.

[6] Josh Boyd. 2002. In community we trust: Online security communication at eBay. *Journal of Computer-Mediated Communication* 7, 3 (2002), 0–0.

[7] John K Butler Jr. 1991. Toward understanding and measuring conditions of trust: Evolution of a conditions of trust inventory. *Journal of management, Sage Publications Sage CA: Thousand Oaks, CA* 17, 3 (1991), 643–663.

[8] Elisabetta Carrara and Giles Hogben. 2007. Reputation-based systems: A security analysis. *European Union Agency for Network and Information Security (ENISA) Position Paper* 424 (2007).

[9] Cristiano Castelfranchi and Rino Falcone. 2000. Trust and control: A dialectic link. *Applied Artificial Intelligence* 14, 8 (2000), 799–823.

[10] Camille Cobb and Tadayoshi Kohno. 2017. How Public Is My Private Life?: Privacy in Online Dating. In *Proceedings of the 26th International Conference on World Wide Web*. International World Wide Web Conferences Steering Committee, 1231–1240.

[11] Danielle Couch, Pranee Liamputtong, and Marian Pitts. 2012. What are the real and perceived risks and dangers of online dating? Perspectives from online daters: Health risks in the media. *Health, Risk & Society* 14, 7-8 (2012), 697–714.

[12] Couchsurfing. 2017. Verification (Couchsurfing FAQs). https://support.couchsurfing.org/hc/en-us/sections/200670420-Verification. (2017). Accessed: 2017-08-29.

[13] Partha Dasgupta. 2000. Trust as a commodity. *Trust: Making and breaking cooperative relations* 4 (2000), 49–72.

[14] Morton Deutsch. 1958. Trust and suspicion. *Journal of conflict resolution* 2, 4 (1958), 265–279.

[15] Patricia M Doney and Joseph P Cannon. 1997. An examination of the nature of trust in buyer-seller relationships. *The Journal of Marketing* (1997), 35–51.

[16] Samuel Dukhovni, Ja Kob Weisblat, and Istvan Chung. 2016. Solving the Dating Problem with the SENPAI Protocol. http://sigtbd.csail.mit.edu/pubs/veryconference-paper10.pdf/?utm_term=.dc0917fe6ff7/. (2016). Online; Accessed: 2017-04-14.

[17] Catherine C Eckel and Ragan Petrie. 2011. Face value. *The American Economic Review* 101, 4 (2011), 1497–1513.

[18] eHarmony. 2013. The Most Successful Online Dating Profile Photos Revealed. http://www.eharmony.com/dating-advice/using-eharmony/the-most-popular-online-dating-profile-photos-revealed/#.WW0c88YZNbU/. (2013). Online; Accessed: 2017-06-30.

[19] Nicole Ellison, Rebecca Heino, and Jennifer Gibbs. 2006. Managing impressions online: Self-presentation processes in the online dating environment. *Journal of Computer-Mediated Communication* 11, 2 (2006), 415–441.

[20] Eyal Ert, Aliza Fleischer, and Nathan Magen. 2016. Trust and reputation in the sharing economy: The role of personal photos in Airbnb. *Tourism Management* 55 (2016), 62–73.

[21] Facebook. 2017. Facebook Terms of Use. https://www.facebook.com/terms/. (2017). Online; Accessed: 2017-07-11.

[22] Andrew T Fiore, Lindsay Shaw Taylor, Gerald A Mendelsohn, and Marti Hearst. 2008. Assessing attractiveness in online dating profiles. In *Proceedings of the SIGCHI conference on human factors in computing systems*. ACM, 797–806.

[23] Atlantic Data Forensics. 2016. Why You Shouldn't Use Your Facebook Picture on a Dating Website. https://www.atlanticdf.com/news/2016/03/shouldnt-use-facebook-picture-dating-website/. (2016). Online; Accessed: 2017-07-11.

[24] Emily Fox. 2016. Here's How To Check If Your Partner Is Cheating On Tinder. http://www.vanityfair.com/news/2016/04/check-tinder-cheater-swipe-buster/. (2016). Online; Accessed: 2017-07-11.

[25] Francis Fukuyama. 1995. Trust: The social virtues and the creation of prosperity. *Free Press Paperbacks* D10 301 c. 1/c. 2 (1995).

[26] Karoline Gatter and Kathleen Hodkinson. 2016. On the differences between Tinder™ versus online dating agencies: Questioning a myth. An exploratory study. *Cogent Psychology* 3, 1 (2016), 1162414.

[27] Mof Gimmers. 2017. Match.com is Latest Dating Site to be Hacked. https://www.bitterwallet.com/privacy/match-com-is-latest-dating-site-to-be-hacked-87645/. (2017). Online; Accessed: 2017-07-11.

[28] Sarah Gooding. 2013. The Most Important Tips To Online Dating Success. http://blog.pof.com/2013/06/the-10-most-important-tips-to-online-dating-success/. (2013). Online; Accessed: 2017-06-30.

[29] The Guardian. 2016. New Website Lets Anyone Spy on Tinder users. https://www.theguardian.com/technology/2016/apr/05/tinder-swipebuster-spy-on-users-privacy-dating-app/. (2016). Online; Accessed: 2017-07-11.

[30] Keith Hampton, Lauren Sessions Goulet, Lee Rainie, and Kristen Purcell. 2011. Social networking sites and our lives. *Pew Internet & American Life Project* 16 (2011).

[31] Charles Handy. 1995. Trust and the virtual organization. *Harvard business review* 73, 3 (1995), 40–51.

[32] Rebecca D Heino, Nicole B Ellison, and Jennifer L Gibbs. 2010. Relationshopping: Investigating the market metaphor in online dating. *Journal of Social and Personal Relationships, Sage Publications Sage UK: London, England* 27, 4 (2010), 427–447.

[33] Nick Janetos and Jan Tilly. 2017. Reputation Dynamics in a Market for Illicit Drugs. *arXiv preprint arXiv:1703.01937* (2017).

[34] Annukka Jänkälä and others. 2017. *Dating expectations in social media: From profile pictures to a date and beyond.* Master's thesis. Aalto University.

[35] KrebsOnSecurity. 2011. PlentyofFish.com Hacked, Blames Messenger. https://krebsonsecurity.com/2011/01/plentyoffish-com-hacked-blames-messenger/.

(2011). Online; Accessed: 2017-07-11.
[36] Amanda Lenhart, Rich Ling, Scott Campbell, and Kristen Purcell. 2010. Teens and mobile phones: Text messaging explodes as teens embrace it as the centerpiece of their communication strategies with friends. *Pew Internet & American Life Project* (2010).
[37] Natasha Lomas. 2017. Someone Scraped 40,000 Tinder Selfies to Make a Facial Dataset for AI Experiments. https://techcrunch.com/2017/04/28/someone-scraped-40000-tinder-selfies-to-make-a-facial-dataset-for-ai-experiments/. (2017). Online; Accessed: 2017-07-11.
[38] Anna Lysyanskaya. 2008. Cryptography: How to keep your secrets safe. *Scientific American* (2008), 89–94.
[39] Adriana M Manago, Michael B Graham, Patricia M Greenfield, and Goldie Salimkhan. 2008. Self-presentation and gender on MySpace. *Journal of Applied Developmental Psychology* 29, 6 (2008), 446–458.
[40] Stephen Paul Marsh. 1994. *Formalising trust as a computational concept.* Ph.D. Dissertation. University of Stirling.
[41] Match.com. 2016. Match.com, L.L.C. Privacy Policy. http://www.match.com/registration/privacystatement.aspx/. (2016). Online; Accessed: 2017-07-11.
[42] Match.com. 2017. Match Help Page. http://www.match.com/help/faq/7/145/. (2017). Online; Accessed: 2017-04-14.
[43] Match.com. 2017. Match.com FAQ Adding photos. http://www.match.com/help/faq/7/128/#holder/. (2017). Online; Accessed: 2017-06-30.
[44] Match.com. 2017. Match.com FAQ Blocking and Unblocking. http://www.match.com/help/faq/3/50/#holder/. (2017). Online; Accessed: 2017-04-14.
[45] Match.com. 2017. Match.com FAQ Canceling A Membership. http://www.match.com/help/faq/1/2/#holder/. (2017). Online; Accessed: 2017-07-11.
[46] Match.com. 2017. Match.com FAQ Messaging Free Members. http://www.match.com/help/faq/3/63/#holder/. (2017). Online; Accessed: 2017-06-30.
[47] Match.com. 2017. Match.com FAQ Mutual Matches-Explained. http://www.match.com/help/faq/8/164/#holder/. (2017). Online; Accessed: 2017-06-30.
[48] Match.com. 2017. Match.com FAQ Profile Completion Requirements. http://www.match.com/help/faq/7/143/#holder/. (2017). Online; Accessed: 2017-06-30.
[49] Match.com. 2017. Match.com FAQ Singled Out - Explained. http://www.match.com/help/faq/8/178/#holder/. (2017). Online; Accessed: 2017-06-30.
[50] Match.com. 2017. Match.com Homepage. https://www.match.ca/. (2017). Online; Accessed: 2017-04-14.
[51] Match.com. 2017. Match.com Terms of Use Agreement. http://www.match.com/registration/membagr.aspx/. (2017). Online; Accessed: 2017-06-30.
[52] Roger C Mayer, James H Davis, and F David Schoorman. 1995. An integrative model of organizational trust. *Academy of management review* 20, 3 (1995), 709–734.
[53] Rory McGloin and Amanda Denes. 2016. Too hot to trust: Examining the relationship between attractiveness, trustworthiness, and desire to date in online dating. (2016), 1461-4448 pages.
[54] Ian Miers, Matthew Green, Christoph U Lehmann, and Aviel D Rubin. 2012. Vis-à-vis Cryptography: Private and Trustworthy In-Person Certifications. In *Presented as part of the 3rd USENIX Workshop on Health Security and Privacy*. USENIX, Bellevue, WA.
[55] John Mikhail, Emad Farag, and Minasyan. 2016. Cryptographic Dating. https://courses.csail.mit.edu/6.857/2016/files/35.pdf/. (2016). Online; Accessed: 2017-06-30.
[56] Ananda Mitra. 2002. Trust, authenticity, and discursive power in cyberspace. *Commun. ACM* 45, 3 (2002), 27–29.
[57] V Narendhiran. 2016. Tinder Without Facebook. https://www.allinfopark.net/tinder-without-facebook-working-methods. (2016). Online; Accessed: 2017-06-30.
[58] Dave Neal. 2015. Match.com claims that members have been untouched by malvertising attack. https://www.theinquirer.net/inquirer/news/2424475/matchcom-malvertising-hack-suggests-that-digital-daters-are-doomed/. (2015). Online; Accessed: 2017-07-11.
[59] Borke Obada-Obieh, Sonia Chiasson, and Anil Somayaji. 2017. "Don't Break My Heart!": User Security Strategies for Online Dating. (2017).
[60] Plenty of Fish. 2017. Plenty of Fish Help Center: POF FAQ. http://www.pof.com/helpcenter/helpcenter_faq.aspx/. (2017). Online; Accessed: 2017-07-11.
[61] Plenty of Fish. 2017. Plenty of Fish Help Center: Upgraded Memberships. http://www.pof.com/HelpCenter/helpcenter_upgradedMemberships.aspx/. (2017). Online; Accessed: 2017-06-30.
[62] Plenty of Fish. 2017. Plenty of Fish Help Center: Upload image. http://www.pof.com/HelpCenter/helpCenter_uploadImage.aspx/. (2017). Online; Accessed: 2017-06-30.
[63] Plenty of Fish. 2017. Plenty Of Fish Image Upload. http://www.pof.com/userimages.aspx/. (2017). Online; Accessed: 2017-07-11.
[64] Plenty of Fish. 2017. POF Homepage. http://www.pof.com/. (2017). Online; Accessed: 2017-04-14.
[65] Plenty of Fish. 2017. POF Statistics. http://www.datingsitesreviews.com/staticpages/index.php?page=Plenty-of-Fish-Statistics-Facts-History/. (2017). Online; Accessed: 2017-04-14.
[66] Andrea Peterson and William Wan. 2017. Uber Panic Button. https://www.washingtonpost.com/news/the-switch/wp/2016/02/22/uber-has-a-panic-button-in-india-but-dont-expect-it-to-come-to-the-u-s/?utm_term=.dc0917fe6ff7/. (2017). Online; Accessed: 2017-04-14.
[67] Huffington Post. 2016. Mary Kay Beckman Sues Match.com After Wade Ridley Tried To Murder Her. http://www.huffingtonpost.com/2013/01/24/mary-kay-beckman_n_2544390.html/. (2016). Online; Accessed: 2017-07-11.
[68] Anita Ramasastry. 2012. Does Match.com Have To Make Sure Its Member Profiles are Real and Accurate? Why A Federal Judge Correctly Ruled No. https://verdict.justia.com/2012/09/11/does-match-com-have-to-make-sure-its-member-profiles-are-real-and-accurate/. (2012). Online; Accessed: 2017-06-30.
[69] Howard Rheingold. 1996. A slice of my life in my virtual community. *High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace, MIT Press* (1996), 413–36.
[70] Jens Riegelsberger, M Angela Sasse, and John D McCarthy. 2003. Shiny happy people building trust?: Photos on e-commerce websites and consumer trust. In *Proceedings of the SIGCHI conference on Human factors in computing systems*. ACM, 121–128.
[71] Peter Smith Ring and Andrew H Van de Ven. 1992. Structuring cooperative relationships between organizations. *Strategic Management Journal, Wiley Online Library* 13, 7 (1992), 483–498.
[72] Elena Rocco. 1998. Trust breaks down in electronic contexts but can be repaired by some initial face-to-face contact. In *Proceedings of the SIGCHI conference on Human factors in computing systems*. ACM Press/Addison-Wesley Publishing Co., 496–502.
[73] Michael J Rosenfeld and Reuben J Thomas. 2012. Searching for a mate the rise of the internet as a social intermediary. *American Sociological Review* 77, 4 (2012), 523–547.
[74] Jörn PW Scharlemann, Catherine C Eckel, Alex Kacelnik, and Rick K Wilson. 2001. The value of a smile: Game theory with a human face. *Journal of Economic Psychology* 22, 5 (2001), 617–640.
[75] Aaron Smith and Monica Anderson. 2016. 5 facts about online dating. http://www.pewresearch.org/fact-tank/2016/02/29/5-facts-about-online-dating/. (2016). Online; Accessed: 2017-07-25.
[76] Aaron Whitman Smith and Maeve Duggan. 2013. Online Dating & Relationship. http://www.pewinternet.org/2013/10/21/online-dating-relationships/. (2013). Online; Accessed: 2017-07-25.
[77] Ulrike Steinbrück, Heike Schaumburg, Sabrina Duda, and Thomas Krüger. 2002. A picture says more than a thousand words: Photographs as trust builders in e-commerce websites. In *CHI'02 extended abstracts on Human factors in computing systems*. ACM, 748–749.
[78] Tinder. 2017. Tinder Homepage. https://www.tinder.com/. (2017). Online; Accessed: 2017-04-14.
[79] Angela Upex. 2017. How to protect yourself when using online dating services. http://www.chroniclelive.co.uk/special-features/how-protect-yourself-using-online-13047420/. (2017). Online; Accessed: 2017-06-30.
[80] Reddit User. 2016. Reddit Tinder Comment. https://www.reddit.com/r/Tinder/comments/3lymz1/reported_too_many_times_cant_even_delete_my. (2016). Online; Accessed: 2017-06-30.
[81] K Weisul. 1999. eBay launches anti-fraud measures. *Inter@ ctive Week* 6, 3 (1999), 12.
[82] Monica Whitty and Adrian Carr. 2006. Cyberspace romance: The psychology of online relationships. *Palgrave Macmillan New York* (2006), xvi, 218 p. ;.
[83] Jeanne Wilson, Susan Straus, and Bill McEvily. 2000. All in due time: The development of trust in electronic and face-to-face groups. *Organizational Behavior and Human Decision Processes, Elsevier* 99 (2000), 16–33. Issue 1.
[84] Rick K Wilson and Catherine C Eckel. 2006. Judging a book by its cover: Beauty and expectations in the trust game. *Political Research Quarterly* 59, 2 (2006), 189–202.
[85] Li Xiong and Ling Liu. 2004. Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities. *IEEE transactions on Knowledge and Data Engineering* 16, 7 (2004), 843–857.
[86] Artem Yankov. 2015. How to Find Facebook Users on Match.com by Using Face Recognition Tools. http://artemyankov.com/how-to-find-facebook-users-on-match-dot-com-by-using-face-recognition-tools/. (2015). Online; Accessed: 2017-07-11.
[87] Giorgos Zacharia and Pattie Maes. 2000. Trust management through reputation mechanisms. *Applied Artificial Intelligence* 14, 9 (2000), 881–907.