HAL
open science

Contrasting False Identities in Social Networks by Trust Chains and Biometric Reinforcement

Francesco Buccafurri, Gianluca Lax, Denis Migdal, Serena Nicolazzo, Antonino Nocera, Christophe Rosenberger

To cite this version:

Francesco Buccafurri, Gianluca Lax, Denis Migdal, Serena Nicolazzo, Antonino Nocera, et al.. Contrasting False Identities in Social Networks by Trust Chains and Biometric Reinforcement. CyberWorlds, Sep 2017, Chester, United Kingdom. hal-01589753

HAL Id: hal-01589753

https://hal.science/hal-01589753v1

Submitted on 19 Sep 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Contrasting False Identities in Social Networks by Trust Chains and Biometric Reinforcement

Francesco Buccafurri[1], Gianluca Lax[1],
Denis Migdal[2], Serena Nicolazzo[1], Antonino Nocera[1], Christophe Rosenberger[2]
[1]DIIES Dept., University of Reggio Calabria, Italy
Email: {bucca,lax,s.nicolazzo,a.nocera}@unirc.it
[2]ENSICAEN - UNICAEN - CNRS
GREYC UMR 6072, F-14050 Caen, France
Email: {denis.migdal,christophe.rosenberger}@ensicaen.fr

***Abstract*—Fake identities and identity theft are issues whose relevance is increasing in the social network domain. This paper deals with this problem by proposing an innovative approach which combines a collaborative mechanism implementing a trust graph with keystroke-dynamic-recognition techniques to trust identities. The trust of each node is computed on the basis of neighborhood recognition and behavioral biometric support. The model leverages the *word of mouth* propagation and a settable degree of redundancy to obtain robustness. Experimental results show the benefit of the proposed solution even if attack nodes are present in the social network.**

***Index Terms*—Social networks; trust; keystroke dynamics;**

I. Introduction

Social network profiles whose claimed identity does not match with the real user are certainly potential security threats in the Web [1]. This happens in two cases. The first case is that of fake profiles, in which the owner of a profile intentionally claims the real-life identity of another individual.

The second case is that of violated profiles, in which an intruder, permanently or temporarily, uses the profile of a victim in a fraudulent way.

In both cases, the risk of anomalous behavior with potential damage of the victim reputation, espionage, or social engineering attacks towards people connected to the victim is very high. To give an example, according to security firm Symantec [2], a growing number of hackers are targeting professionals on LinkedIn. Through these connections, attackers can entice users to give up personal data, hijack them towards infected websites and, once their email addresses is known, launch spear-phishing campaigns.

The problem has thus a high practical relevance. A number of studies have been proposed in the recent literature [3], [4] to contrast this problem. However, all the existing proposals require a strong effort of analysis done centrally by the social network provider, which takes into account all the behavioral and topological information of the profiles.

In this paper, we offer a different approach based on a collaborative trust mechanism that may operate in principle in a truly distributed fashion, combined with behavioral biometric methods to contrast profile compromising. The originality of our proposal is that it only leverages user-to-user interactions, and no information that only the social network provider can have. Moreover, we adopt a conservative approach, because our goal is to provide assurance that a profile is genuine instead of detecting fake profiles. The underlying idea exploits the social structure of our domain: Indeed, the trust model is based on a robust implementation of a *worth of mouth* approach and robustness is obtained by redundancy. In words, we follow the principle that if a sufficient number of people trust the identity of a social network profile, we can trust it too. This way, we obtain a graph of trust, because we propagate trust under the basic assumption that a fake user (and then fake behavior) is transitively excluded. We base our assumption on the consideration that, when the real-life identity is known, sanctions are facilitated in case of misbehavior (e.g., victims might sue users who certified the offender), thus misbehavior is prevented.

Trust is obtained through redundant trust chains in which any node plays a role similar to an intermediate certifier in a certificate chain, until a certified profile is reached. In our model, indeed, the presence of some profiles certified by a Trusted Third Party is also required. In order to identify possible intrusions in a legitimate profile, the trust model takes also into account the behavioral biometric traits of users that they record and verify in a peer-to-peer fashion (i.e., no storing of biometric data is required to the social network provider). In other words, the word of mouth mechanism propagates the information that the current behavior of a given node is not compliant with that of the initial safe state, thus reducing the trust of the community towards that node. We use in this paper keystroke dynamics as behavioral biometric modality. This information is very easy to collect on web pages (e.g., by using a JavaScript code) and allows a simple and low cost solution to verify the identity of one user [5], [6], [7].

The structure of the paper is the following. In the next section, we contextualize our proposal in the state of the art. In Section III, we describe our model and the related methodology, by giving general principles, the behavioral biometric modality used in our approach, and the theoretical

support of the trust mechanism. In Section IV, we test our methodology. Finally, in Section V, we draw our conclusions and discuss the future work.

II. Related Works

Identity theft in Online Social Networks (OSNs) is becoming a significantly growing concern [1]. Threats vary from terrorism to scamming, spear phishing, trolling, and so on.

Typical solutions for identity deception attacks rely on legitimate community members and administrators who are called to manually identify malicious accounts [8]. Whereas, automatic solutions focusing on verbal and non-verbal approaches for identity deception detection have been proposed in [9], [10]. In particular, in [9] the authors present a computational solution of deception prevention that uses social network data and a common contribution network. This machine learning based solution can not be applied to our scenario because it focuses on proactively disabling the ability of a deceiver to cause disruption in a social media platform preventing the access only to a sub-community of an OSN. Hence, it protects only the identity of a user belonging to a given group of an OSN. In [11], the authors propose two detection schemes to discover potential faked identities in OSNs. These schemes help to resist Identity Clone Attacks (ICA), where the adversary forges the victim's identity and creates a profile with the same information and circles as friends of the victim.

The approach described in [12] shows that enhanced forms of ICA can be carry out, for instance the adversary can also implement an automated, cross-site profile cloning attack, if the attacker can forge the identity of the victim on another OSN site in which the victim is not registered yet. In [13] the authors propose *Safebook*, a decentralized and privacy-preserving OSN. This system provides registered users with data storage and data management functions relying on trust relationships that are part of social networks in real life. A similar system is presented in [14]. In this platform, users are associated with public keys they exchange out of band while creating OSN links, and data confidentiality and privacy are ensured through encryption. These systems do not protect from identity theft on the original OSN, but their aim is to provide a tool to anonymously communicate through hop-by-hop encryption among trusted users.

Our approach is also related to the concept of information diffusion in OSNs, in the sense that the roots influence the trust values of other nodes in the network following the rules of OSN information flow [15], [16]. Most of these works study how information flows in OSNs and propose strategies to maximize this diffusion by identifying strategical nodes for the information propagation. The aim of our paper is somehow orthogonal to these studies and may exploit these solutions to improve trust propagation through the OSN.

Moreover, our approach leverages biometric data, which is a practice not new for social networks applications [17]. Most of the papers focus on user authentication using biometric data in order to enhance its security. Some papers in the literature considered soft biometrics with possible applications to social networks. Most of the works consider gender recognition by analyzing the type of images posted or the keystroke dynamics [18], [19]. To our knowledge, no work considered keystroke dynamics as solution for continuous authentication for enhancing trust in social networks.

Several works exploit biometrics to implement continuous authentication schemes [20], [21], [22], [23]. Indeed, in high-security environments the typical session level authentication can be exposed to session hijacking in which an attacker targets a post-authenticated session. In those scenarios, continuous and real-time verification of user identity may become mandatory and a lot of research effort has been devoted to use biometrics as a mean to achieve this objective. However, the goal of these strategies is very far away from ours. Indeed, our approach does not aim at proposing a strategy to continuously verify that an active login session is controlled by the right user; instead, our approach exploits biometric data as a feedback to our trust model to measure the trustworthiness of an online profile.

III. Proposed method

A. General principle

The reference scenario is that of a social network. The approach works by considering trust chains among users. Each chain starts from a root profile, which is a profile certified by a Trusted Third Party (TTP). To build a certified profile (root profile), a user has to register to the social network via TTP (also by exchanging identification documents or using a public digital identity system). In this phase, TTP gathers the biometric (behavioral) parameters of the user to create a model that will be exploited, in the future interaction with the user, to verify whether the account is still under this user control. In the negative case, the profile will be no longer certified.

We represent a social network as a directed graph $G = \langle N, E \rangle$, where N is the set of profiles, and E models friendship among social network profiles. To be general, we use the notion of directed graphs, so that the case of symmetric friendship (as Facebook) is simply handled by including two edges in both directions.

N is thus partitioned into two subsets: the set of certified nodes (denoted by N_c), and the set of non-certified nodes. Any node of the social network (both certified and non-certified) may directly recognize some of its direct contacts. The underlying idea is that a node recognizes only those adjacent nodes for which past real-life interactions occurred, allowing to conclude, also by using external knowledge, that the claimed identity is not fake (this typically happens for a significant portion of social network contacts). When a safe interaction occurs (for example, at the first message exchange allowing to recognizes the interlocutor) the profile playing the role of recognizer builds a biometric model of the recognizing node, in order to detect, in the future, the possible presence

of an intruder. Importantly, only a node already recognized can play the role of recognizer. The underlying rationale is that the misbehavior of a user is directly connected to his/her anonymity in the social network. In other words, making the recognizing process fully accounted and traced (and related to a real-life identity), we can increase the trust about recognized identities, provided that transitively, the process leads to root nodes. As we cannot give an absolute value to the principle above, we have to increase the level of trust by requiring redundancy in the recognizing process, thus making more improbable the conjunct misbehavior of identified recognizers. The level of redundancy sets the level of trust. The biometric model built by any participant, allows us to detect possible profile compromising, thus including in the trust also the expectation that an initially identified profile is still under the exclusive control of the legitimate owner. It is worth noting that, in principle, the biometric model could be learned by means of multiple channels (social network interactions, chats, shared editing, and so on) by associating the model to the asserted identity.

Before giving into detail, we remark that the proposed approach is not aimed to define a digital identity system, since, as already observed, only a level of trust is obtained and, further, it regards not all identifying data. Indeed, when a user a recognizes a user b, she/he is stating just that b is not claiming an identity not belonging to him, not the veracity of all published information. The number and quality of information needed to a to reach this conclusion depend on the social context. Besides name and surname, they may regard the job, the age, the friends, etc. A detailed study of these aspects is out of the scope of this paper whose aim is just to define the basic approach, leaving the detail (also for example the case of multiple profiles of the same user, that of social network profiles managed by more people, etc.) to future work.

B. Keystroke dynamics

Keystroke dynamics is a behavioral biometric modality consisting in analyzing user's way of typing on a keyboard. This biometric information can be computed easily on Internet using a simple JavaScript code. Keystroke dynamics has been experimented for the first time in 1980 in a study where seven secretaries were asked to type three different texts [24]. The results were promising, but lacked a sufficient number of users involved in the database. The first patent on keystroke dynamics was registered in 1986 [25]. Other methods have been defined during the last twenty years [26]. In previous references such as [27], it has been shown that keystroke dynamics is invariant to the keyboard type (laptop or terminal). The use of mobile devices is not considered in this paper but many methods exist to deal with this type of capture [28].

The capture process of keystroke dynamics is presented in Figure 1. It consists in computing several features when the

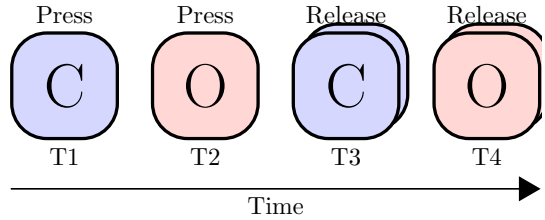

Figure 1: Information captured in a keystroke dynamics system when pressing C and O keys [29].

keys are pressed and released (timestamp of the event, code of the key, ...) provided by any Operating System (OS). The feature extraction consists mainly in computing different latencies and duration times between each key. Figure 1 shows an example where the user presses two keys of the keyboard. The user presses "C" at T1, "O" at T2 and releases "C" at T3 and "O" at T4. Note that the following relation is always respected: $T3 > T1$ and $T4 > T2$ (we always release a key after pressing it), while the following condition may not always be respected: $T2 > T3$ (because, as in our example, a user may press another key before releasing the previous one). We can extract three different types of latencies (T2-T1, T4-T3,T2-T3) which we call PP (latency between two pressures), RR (latency between two releases), RP (latency between one release and one pressure) respectively and one type of duration (T3-T1 or T4-T2) which we call PR (duration of a key press). The described process is repeated for all the keys.

Keystroke dynamics can be used either with passwords to enhance the security of user authentication or on free text. In this paper, we intend to use it on free text. Subsequently, we consider the different timing information between two-character sequences known as *digraphs*. Digraphs are the latency times between two successive keystrokes. The biometric template associated to user z is composed of n digraphs $B_z = \{b_z^1, .., b_z^n\}$. The considered digraphs could be associated to one language. We have to build the user reference biometric template by analyzing keystroke dynamics during a period of time where we assume only the legitimate user interacts with the social network. The reference template of user z is defined by $\vec{B}_z = \{E[B_z], \sigma[B_z]\}$ where $E[.]$ corresponds to the average value of biometric templates of user z and $\sigma[.]$ the associated standard deviation. To decide if a biometric template B_x belongs to user z, we need to compare it with the reference template of user z denoted $\vec{B}_z$ as follows [30]:

$$Score = 1 - \frac{1}{n}\sum_{i=1}^{n} e^{-\frac{|B_x - E[B_z]|}{\sigma[B_z]}}$$

This score gives a confidence measure the user z is legitimate and will be used in the trust model we propose in the next section.

C. Trust Model

In this section, we describe how our trust model works. Throughout this section consider given a directed graph $G = \langle N, E \rangle$ representing a social network and a *redundancy* parameter t, i.e., a positive integer representing a level of trust. Let TTP be a Trusted Third Party. Let denote by N_c the set of *certified nodes*, that is the nodes whose identity is assured and monitored by TTP. Given a node $u \in N$ we denote by $\Gamma(u)$ the set of neighbors of u (i.e., adjacent nodes). Moreover, we denote by $R(u) \subseteq \Gamma(u)$ the set of nodes recognized by u.

Definition III.1. *We say that a node $u \in N$ is t-*recognized *(*in $A \subseteq N$*) if either: (i) $u \in N_c$ (i.e., is a certified node), or (ii) there exist t other t-recognized nodes in A that recognize u.*

When the set A of the definition above is not specified, we intend that a node is t-recognized in N. From the above definition it immediately follows that nodes in N_c are t-recognized for any t and in any set A. We define now the notion of *t-closed* set.

Definition III.2. *A set $A \subseteq N$ of t-recognized nodes in A is said t-*closed*, if there is no $u \in N \setminus A$ that is t-recognized in A too.*

From the above definition it immediately follows that all certified nodes must belong to any t-closed set.

Theorem III.1. *For any t-closed set A, it holds that $N_c \subseteq A$.*

With the next theorem we state that the operator $\subseteq$ induces a partial order over the set of t-closed sets, which is a lower semi-lattice. First, we define this set.

Definition III.3. *We denote by $N^t \subseteq 2^N$ the set of non-empty t-closed subsets of N.*

Now, we are ready to state the following theorem.

Theorem III.2. *N^t is a lower semi-lattice.*

Let denote by N_b^t the bottom of the semi-lattice N^t. In our model, the role of N_b^t is central, because it includes exactly all nodes that are t-recognized, but, due to subset minimality, they do not form clusters whose recognizing is only mutual. In other words, N_b^t is the set of nodes for which trust paths start from certified nodes. For this reason, we use N_b^t to trust nodes.

Definition III.4. *Given a node $u \in N$ we say that u is t-*trusted (in N) *if $u \in N_b^t$. N_b^t is also said the* set of t-trusted nodes (in N).

To formalize the relationship of t-trustworthiness of a node with the presence of certified nodes supporting the trust, we introduce the notion of *support* and *kernel* of a t-trusted node in N_b^t.

Definition III.5. *A* support *for a node $u \in N_b^t \setminus N_c$ is any subset $S_u^t \subseteq N_c$ such that u is t-trusted also in the transformation of G obtained by restricting the set of certified nodes to S_u^t. A* kernel *K_u^t for u is any subset minimal support for u.*

The next theorem states in which terms we intend the level of trust represented by t-trustworthiness. Informally, being t-trusted for a node means that there are at least t trust chains starting from certified nodes.

Theorem III.3. *Given a node $u \in N_b^t \setminus N_c$, any kernel K_u^t for u is such that $|K_u^t| \geq t$.*

The above definition of N_b^t and, consequently, of t-trustworthiness of a node, is declarative, so it does not give us any information about how to compute if a node is t-trusted or not. Thus, we provide an operational definition of N_b^t, based on the fixpoint of a monotone operator Λ_t, called *t-recognizing operator*. This definition also gives us a more intuitive support about the property stated earlier, for which the trust of nodes in N_b^t can be directly or indirectly linked to (at least) t certified nodes.

Definition III.6. *We define the* t-recognizing operator *$\Lambda_t : 2^N \rightarrow 2^N$ as follows: (i) $\Lambda_t(\emptyset) = N_c$ (ii) $\Lambda_t(A) = \{u \in N \mid \exists B \subseteq A \text{ s. t. } |B| \geq t \wedge u \in \bigcap_{v \in B} R(v)\}$.*

Now, we define the following sequence of sets: $\Lambda_t^0 = \Lambda_t(\emptyset)$; $\Lambda_t^k = \Lambda_t(\Lambda_t^{k-1})$, for any $k > 0$.

By proving first that the operator is monotone, we can obtain the following results:

Theorem III.4. *The operator Λ_t has a fixpoint, i.e., there exists $k > 0$ such that $\Lambda_t^k = \Lambda_t^{k-1}$. We denote this fixpoint as Λ_t^∞.*

The next theorem states the equivalence between the declarative definition above and the operational one.

Theorem III.5. *The set of t-trusted nodes N_b^t coincides with the fixpoint of the t-consequence operator Λ_t^∞.*

The above theorem provides a direct way to compute the set of t-trusted nodes N_b^t, and thus to establish if a node is t-trusted or not. Algorithm 1 summarizes this computation strategy.

The above notion of t-trustworthiness embeds a lossless propagation of trust, in which the level of assurance of identity based on recognition of users, does not degrade if the t redundancy property holds at every step of propagation. In other words, the t-redundancy property is considered as a threshold to propagate the trust. The t-redundancy parameter implicitly represents the assumption that the multiple identification of a node u done by nodes in turn identified with the same trust level, and so on, until t certified nodes are reached, can be considered sufficient to trust the identity of u. The approach applies the concept of trust chain used in the context of digital certification to the domain of identity management in social networks, with the aim of contrasting the problem of fake identities. It is worth remarking that the model cannot provide absolute guarantees,

Algorithm 1 Implementation of Operator Λ_t (Definition III.6)

```
procedure COMPUTE N_b^t
    Variable: n_1, ..., n_|N|, array of nodes;                          ▷ The set of all graph nodes
    Variable: v_1, ..., v_|N|, array of boolean;                        ▷ The set of already visited nodes
    Variable: t_1, ..., t_|N|, array of integer;   ▷ The set of integers representing the computed level of trust of each node
    Variable: found, boolean;                      ▷ Used to terminate the algorithm when no change in trust values is found
    for all nodes n_i ∈ N do                       ▷ Initialization: trust level is 1 for certified nodes, 0 otherwise
        if (n_i ∈ N_c) then
            v_i=true;   t_i=t;
        else
            v_i=false;   t_i=0;
    found=true;
    while (not found) do                           ▷ Iterative computation of node trust level
        found=false;
        for all nodes n_i ∈ N do
            if (not v_i) and (t_i ≥ t) then
                found=true;
                v_i=true;
                for all nodes n_j ∈ R(n_i) do
                    t_j = t_j + 1;
    for all nodes n_i ∈ N do                       ▷ Building N_b^t to be returned
        if (t_i ≥ t) then
            add n_i to N_b^t;
```

but only a trust level directly connected with the value t. The higher t, the higher the trust about identities.

So far, the trust model assumes that, once a user has recognized another user, no revision of this information must be done. This assumption would be valid only in absence of attacks able to give the attacker the access to the user profile (even temporarily). So we assume a sort of *safe state* with regards to fraudulent accesses. In other words, the trust model above prevents from the risk of fake profiles and fake identities but not from fraudulent access to legitimate profiles.

To contrast this further case, we introduce a biometric-based reinforcement to combine with the above trust-chain mechanism, in order to decrease the trust on a given subject if the biometric trait is not recognizable and thus managing also non-safe states. Indeed, the full trust in our mechanism is obtained by relying on the assumption that the disclosure of trusted real-life identities prevents from misbehavior of users in the trust mechanism itself, under the t-redundancy assumption.

But, if the operating user is not the legitimate one, the above assumption fails, so the identity of those users whose trust is based on paths involving the potentially attacked profile should be not fully trusted. In other words, to take into account this aspect, we have to enable a gradual level of trust, from 0 to 1 (while before the trust was basically either 0 or 1), and use an ϵ-approximation approach to trust identities. The first step is to modify the notion of t-recognized. Obviously, we keep the redundancy parameter t in the new definition, but we introduce the possibility that a user is not fully identified in a given moment, due to the fact that the biometric support is giving a warning rate. We require that nodes in N_c (i.e., certified nodes) loose their state if the biometric support gives a warning rate. Thus, we can assume that certified nodes are not attacked. Given a node u, we define the set $R^\epsilon(u)$ (where $0 \leq \epsilon \leq 1$) as the set of pairs $\langle v, b_r(v)\rangle$ such that $v \in R(u)$ (i.e., v is a node recognized by u in the safe state) and $1-\epsilon \leq b_r(v) \leq 1$ is the current biometric rate (i.e., the score computed as in Section III-B normalized from 0 to 1), provided that it is higher than a given threshold $0 < 1-\epsilon \leq 1$ under which v must be currently considered not recognized. Obviously, for $\epsilon = 0$ we fall in the safe state. We say that nodes in $R^\epsilon(u)$ are *ϵ-recognized* by u. At this point, we are ready to extend the notion of t-recognized to a non-safe state.

Definition III.7. *We say that a node $u \in N$ is $\langle t, \epsilon, r\rangle$-*recognized *(in N) if either: (1) $u \in N_c$ (i.e., is a certified node), or (2) there exists a set B of $\langle t, \epsilon, r\rangle$-recognized nodes such that both (i) $u \notin B$, (ii) $|B| \geq t$, (iii) $u \in R^\epsilon(v)$, for each $v \in B$, (iv) $1-\epsilon \leq r \leq 1$, and (iv) $\frac{\sum_{v\in R} b_r(v)}{|B|} \geq r$.*

It is easy to see that a node is t-recognized, according to Definition III.1, if and only if it is $\langle t, 0, 1\rangle$-recognized, according to the above definition. The intended meaning of Definition III.7 is to take into account warnings triggered by the biometric support (through the parameter ϵ), and, at the same time, to require by means of the parameter r that a possible fault of trust introduced by ϵ can be partially recovered by fortifying redundancy in order to reduce approximation. In words, if we

can trust less nodes because we are not sure they are not attacked we need a larger set of witnesses to reach a safe conclusion anyway. This means that r modulates the level of assurance of trust, so that the higher r, the higher the trust on the identity of $\langle t, \epsilon, r\rangle$-recognized nodes. Actually, to talk about trust we have to avoid mutual self-sustained cluster of $\langle t, \epsilon, r\rangle$-recognized nodes, so we have to proceed as in the safe state above by requiring the minimality condition. For brevity we do not give all detail, but it is rather clear that definitions of N_b^t and, consequently, of t-trustworthiness of a node, can be easily extended to the non-safe case, on the basis of Definition III.7. We reach thus the definition of $N_b^{\langle t,\epsilon,r\rangle}$ as the bottom of the semi-lattice of subsets of $\langle t, \epsilon, r\rangle$-closed nodes of N. Therefore, a node is $\langle t, \epsilon, r\rangle$-trusted if belongs to the set $N_b^{\langle t,\epsilon,r\rangle}$. Also the definition of *recognizing operator* can be trivially extended so obtaining the operator $\Lambda_{\langle t,\epsilon,r\rangle}$ in such a way that $N_b^{\langle t,\epsilon,r\rangle}$ coincides with the fixpoint $\Lambda^{\infty}_{\langle t,\epsilon,r\rangle}$ of such operator.

IV. Experimental results

In this section, we conduct a preliminary experimental analysis of our approach aimed to obtain a first validation. Even though as future work we plan to contextualize our method in the related literature also experimentally, we argue this is not a crucial task in this first assessment because of the novelty (shown in the introduction and in Section II) of our approach, which, differently from the existing ones, is only based on information related to user-to-user interactions to trust the the identity of the interlocutor.

In our experiments, the parameters and their default value are: $t = 15$ is the level of trust, $\epsilon = 0.2$ is the level of approximation (system parameter), $r = 0.9$ is the level of assurance (system parameter), $N = 2.500$ is the number of nodes, $C = 250$ is the number of certified nodes, and $M = 0$ is the number of attacked nodes.

Test Bed. The dataset used in this experimental campaign is a synthetic graph combined with real-life biometric data. It is well known that the degree of social-network graphs follows a power-law distribution [31], [32], [33]. This can be obtained by using the Barabási–Albert model [34], one of the most famous algorithms for generating random scale-free networks using *preferential attachment*. Starting from a single-node graph, each new node is connected to the existing nodes by following the law: the more the node degree, the more the probability to receive new links is. The parameters of the Barabási–Albert model used in our experiments are the most commonly adopted in this context.

We started by randomly elect certified nodes (whose number is denoted by C) among nodes with degree higher than 0, assuming that isolated nodes do not ask to be certified. We simulate the interaction among connected nodes and used biometry to decide if an interacting node is attacked. As for the biometric component of the experiments, we used a biometric benchmark database composed of keystroke dynamics [35]. It is composed of biometric template from 110 individuals typing on two desktop keyboards (French keyboard for users in France and Norwegian keyboard for users in Norway) *i.e.* AZERTY and QWERTY (this is not a classical QWERTY keyboard, however, we do not use specific Norwegian keys), respectively.

Giot *et al.* tested the influence of keyboards on the performances, and noticed no significant differences between a laptop and a USB keyboard [29].

For this dataset, we considered 14 digraphs: latency of 'ca', 'ic', 'ed', 'he', 'pe', 'te', 'ch', 'li', 'ri', 'll', 'on', 'er', 'es' and 'st'. The size of the biometric template is 14. We generated legitimate scores by comparing the reference template with templates from the same user. In our attack model, we simulated impostors by replacing the reference template of the victim user with templates coming from other users.

Results. The first experiment is devoted to the study of the performance of our approach when no attack is performed. Starting from our dataset, we varied the number of certified nodes C from 0 to 15% nodes (i.e., 375 of 2.500 nodes) and we measured the overall number of non-certified nodes that are considered trusted, say T_n. We used as metric $CV = \frac{T_n}{C}$, measuring the gain in the number of trusted nodes with respect to the number of certified nodes. In Figure 2, we show the values of CV for three levels of trust, $t = 10, 15$, and 20. From the analysis of these results, we observe that there is a threshold value of certified users, under which the low number of certified nodes makes ineffective our solution. This threshold can be quantified in about 6-7 times the level of trust t: for example, when $t = 10$, with about 2.5% certified nodes (i.e., about 62 certified nodes) we are able to classify about $8{\cdot}62$ nodes as trusted. After this threshold, trusted relationships are established and further increasing in the number of certified nodes do not any advantages. Observe that the decreasing trend of all the three curves is due to the fact that C is in the denominator of CV.

Now, we study the performance of our model when attacks occur: specifically, we study the strength of trust relationships when some nodes are compromised. Starting from a trusted scenario, we computed the fraction TV of trusted nodes which are yet recognized after M nodes are attacked, with M varying from 0 to 15% nodes. The result of this experiment is shown in Figure 3. We consider two cases: in the first one (with label "random" in the figure legend), compromised nodes are selected randomly; in the second case (label "level"), compromised nodes are first selected among those distant one hop from certified nodes, then among those distant two hops from certified nodes, and so on. This case is representative of a collusion attack in which attacker close to a victim collaborate to compromise its reputation. The fact that attacked nodes are not trusted anymore is directly entailed by our mechanism, so we do not report this trivial result. Instead, we studied the resilience of the global trust graph to analyze the global impact

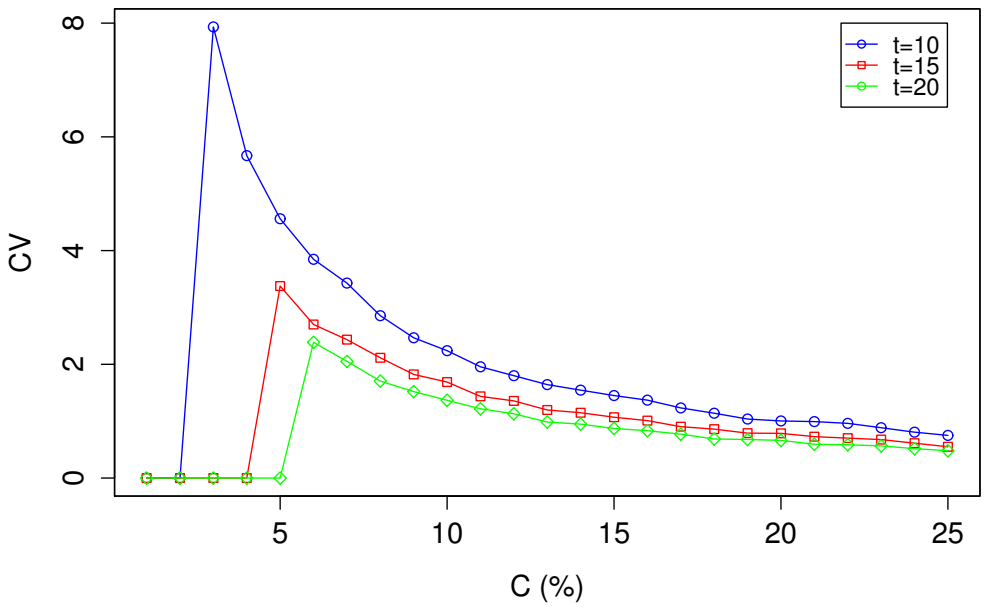

Figure 2: The gain in the number of trusted nodes with regards to the number of certified nodes for a trusted scenario

of attacks.

From the analysis of this result, we observe that the system is robust, even in presence of a not negligible number of attacked nodes, as the most of the remaining trusted nodes continue to be classified as trusted. In contrast, the model performance degrades quickly if attacked nodes can be suitable selected: however, it is quite unrealistic to identify and compromise specific accounts in a large social network.

V. Conclusion and perspectives

In this paper, we proposed a collaborative approach based on user-to-user interaction and keystroke-dynamics to trust identities in a social network. The peculiarity of our method is that it only relies on the view a user has of the neighborhood combined with real-life background information and trust propagation. We tested our method on a combination of real-life and synthetic data, by obtaining promising results (a good coverage with few certified nodes and a good resilience in case of attacks). The next step of our research will be to complete the theoretical characterization of the model, to deal with some detail about user recognition, to deepen the experimental analysis, and to deal with implementation issues.

References

[1] A. Nosko, E. Wood, and S. Molema, "All about me: Disclosure in online social networking profiles: The case of facebook," *Computers in Human Behavior*, vol. 26, no. 3, pp. 406–418, 2010.

[2] "BBC News [Online Version]," `http://www.bbc.com/news/technology-34994858`, 2017.

[3] J. R. Graham, D. Watts, and R. E. Timbrook, "Detecting fake-good and fake-bad mmpi-2 profiles," *Journal of personality Assessment*, vol. 57, no. 2, pp. 264–277, 1991.

[4] M. Conti, R. Poovendran, and M. Secchiero, "Fakebook: Detecting fake profiles in on-line social networks," in *Advances in Social Networks Analysis and Mining (ASONAM), 2012 IEEE/ACM International Conference on*. IEEE, 2012, pp. 1071–1078.

[5] A. Messerman, T. Mustafić, S. A. Camtepe, and S. Albayrak, "Continuous and non-intrusive identity verification in real-time environments based on free-text keystroke dynamics," in *Biometrics (IJCB), 2011 International Joint Conference on*. IEEE, 2011, pp. 1–8.

[6] X. Song, P. Zhao, M. Wang, and C. Yan, "A continuous identity verification method based on free-text keystroke dynamics," in *Systems, Man, and Cybernetics (SMC), 2016 IEEE International Conference on*. IEEE, 2016, pp. 000 206–000 210.

[7] S. Mondal and P. Bours, "Person identification by keystroke dynamics using pairwise user coupling," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 6, pp. 1319–1329, 2017.

[8] M. Tsikerdekis and S. Zeadally, "Detecting and preventing online identity deception in social networking services," *IEEE Internet Computing*, vol. 19, no. 3, pp. 41–49, 2015.

[9] M. Tsikerdekis, "Identity deception prevention using common contribution network data," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 1, pp. 188–199, 2017.

[10] G. A. Wang, H. Chen, J. J. Xu, and H. Atabakhsh, "Automatically detecting criminal identity deception: an adaptive detection algorithm," *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, vol. 36, no. 5, pp. 988–999, 2006.

[11] L. Jin, H. Takabi, and J. B. Joshi, "Towards active detection of identity clone attacks on online social networks," in *Proceedings of the first ACM conference on Data and application security and privacy*. ACM, 2011, pp. 27–38.

[12] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda, "All your contacts are belong to us: automated identity theft attacks on social networks," in *Proceedings of the 18th international conference on World wide web*. ACM, 2009, pp. 551–560.

[13] L. A. Cutillo, R. Molva, and T. Strufe, "Safebook: A privacy-preserving online social network leveraging on real-life trust," *IEEE Communications Magazine*, vol. 47, no. 12, 2009.

[14] R. Baden, A. Bender, N. Spring, B. Bhattacharjee, and D. Starin, "Persona: an online social network with user-defined privacy," in *ACM*

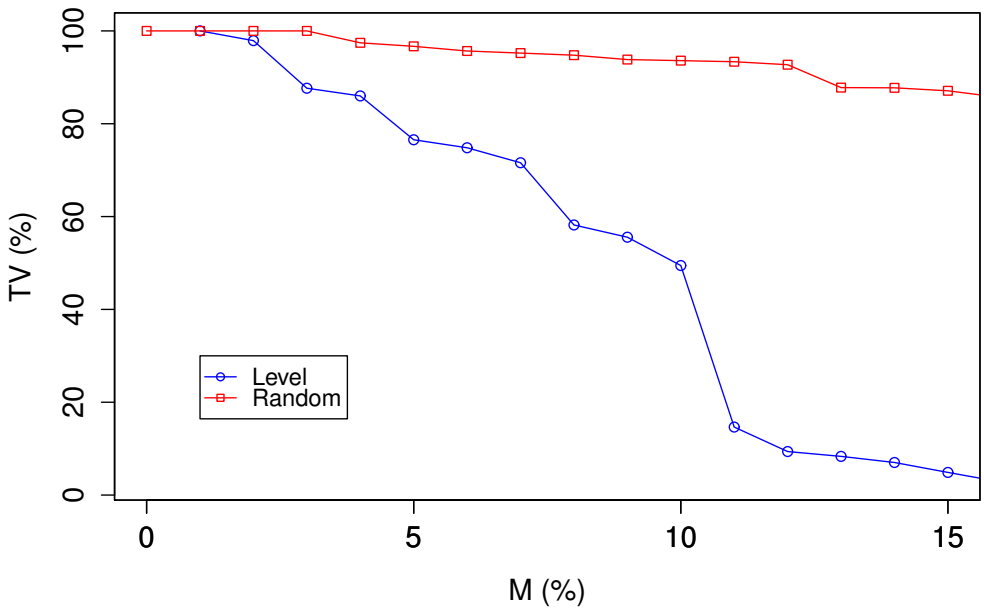

Figure 3: The variation of the fraction of trusted nodes against the number of attacked nodes in an untrusted scenario

SIGCOMM Computer Communication Review, vol. 39, no. 4. ACM, 2009, pp. 135–146.

[15] E. Bakshy, I. Rosenn, C. Marlow, and L. Adamic, "The role of social networks in information diffusion," in *Proceedings of the 21st international conference on World Wide Web*. ACM, 2012, pp. 519–528.

[16] S. Peng, A. Yang, L. Cao, S. Yu, and D. Xie, "Social influence modeling using information theory in mobile social networks," *Information Sciences*, vol. 379, pp. 146–159, 2017.

[17] C. Li, "Chapter 5 biometrics in social media applications," in *Biometrics in a Data Driven World: Trends, Technologies, and Challenges*. CRC Press, 2016, pp. 147–190.

[18] M. Gadiya and S. Jain, "Gender prediction using images posted on online social networks," 2016.

[19] G. Tsimperidis, V. Katos, and S. Rostami, "Age detection through keystroke dynamics from user authentication failures," *International Journal of Digital Crime and Forensics (IJDCF)*, vol. 9, no. 1, pp. 1–16, 2017.

[20] I. Deutschmann, P. Nordström, and L. Nilsson, "Continuous authentication using behavioral biometrics," *IT Professional*, vol. 15, no. 4, pp. 12–15, 2013.

[21] S. J. Upadhyaya, "Continuous authentication using behavioral biometrics," in *Proceedings of the 3rd ACM on International Workshop on Security And Privacy Analytics*. ACM, 2017, pp. 29–29.

[22] E. Schiavone, A. Ceccarelli, and A. Bondavalli, "Continuous user identity verification for trusted operators in control rooms," in *International Conference on Algorithms and Architectures for Parallel Processing*. Springer, 2015, pp. 187–200.

[23] S. Mondal and P. Bours, "Continuous authentication using behavioural biometrics," in *Collaborative European Research Conference (CERC'13)*, 2013, pp. 130–140.

[24] R. Gaines, W. Lisowski, S. Press, and N. Shapiro, "Authentication by keystroke timing: some preliminary results," Rand Corporation, Tech. Rep., 1980.

[25] J. D. Garcia, "Personal identification apparatus," Nov. 1986, uS Patent 4,621,334.

[26] V. V. Phoaha, S. Phoha, A. Ray, S. S. Joshi, and S. K. Vuyyuru, "Hidden markov model (hmm)-based user authentication using keystroke dynamics," patent, fev 2009.

[27] R. Giot, M. El-Abed, and C. Rosenberger, "Greyc keystroke: a benchmark for keystroke dynamics biometric systems," in *Biometrics: Theory, Applications, and Systems, 2009. BTAS'09. IEEE 3rd International Conference on*. IEEE, 2009, pp. 1–6.

[28] M. Dafer and M. El-Abed, "Evaluation of keystroke dynamics authentication systems: Analysis of physical and touch screen keyboards," in *Developing Next-Generation Countermeasures for Homeland Security Threat Prevention*. IGI Global, 2017, pp. 306–329.

[29] R. Giot, M. El-Abed, B. Hemery, and C. Rosenberger, "Unconstrained keystroke dynamics authentication with shared secret," *Computers & Security*, vol. 30, no. 6, pp. 427–445, 2011.

[30] S. Hocquet, J.-Y. Ramel, and H. Cardot, "User classification for keystroke dynamics authentication," in *The Sixth International Conference on Biometrics (ICB2007)*, 2007, pp. 531–539.

[31] R. Kumar, J. Novak, and A. Tomkins, "Structure and evolution of online social networks," in *Link mining: models, algorithms, and applications*. Springer, 2010, pp. 337–357.

[32] M. Cha, H. Haddadi, F. Benevenuto, and K. P. Gummadi, "Measuring user influence in twitter: the million follower fallacy," in *Fourth International AAAI Conference on Weblogs and Social Media (ICWSM 2010)*. AAAI Press, 2010, pp. 10–17.

[33] F. Buccafurri, V. D. Foti, G. Lax, A. Nocera, and D. Ursino, "Bridge analysis in a social internetworking scenario," *Information Sciences*, vol. 224, pp. 1–18, 2013.

[34] A.-L. Barabási and R. Albert, "Emergence of scaling in random networks," *science*, vol. 286, no. 5439, pp. 509–512, 1999.

[35] S. Z. S. Idrus, E. Cherrier, C. Rosenberger, and P. Bours, "Soft biometrics database: A benchmark for keystroke dynamics biometric systems," in *Biometrics Special Interest Group (BIOSIG), 2013 international conference of the*. IEEE, 2013, pp. 1–8.