Attacks on Confidentiality of Communications Between Stranger Organizations

Mikaël Ates, Entr’ouvert, Paris, France
Gianluca Lax, Department of Computer Science, Electronics, Mathematics and Transportation (DIMET), University Mediterranea of Reggio Calabria, Reggio Calabria, Italy

ABSTRACT
Knowledge has become the main intangible asset of many organizations. Two organizations that have had no previous contact or relationship are defined strangers. When two stranger organizations enter into a relationship, knowledge plays a very critical role since each party has to disclose its own knowledge to achieve knowledge from the other party. In this paper, the authors study the confidentiality of communications between stranger organizations, showing that even when strong authentication algorithms, like RSA, are exploited, no guarantee that the communication is confidential can be given. This study is surely useful to keep in mind the limitations concerning the confidentiality whenever stranger organizations are involved.

Keywords: Communication Between Strangers, Confidentiality, Privacy, Stranger Organizations, Trust

INTRODUCTION
In the industrial era, organizations were based on the physical work done by individuals in factories and, for this reason, they are referred as job-based organizations. Nowadays, the idea of workers holding a job is replaced by that of workers bringing knowledge to the organization, knowledge understood as capability of solving a problem, identifying a threat, analyzing a scenario, and so on. In this case, we refer to knowledge-based organizations (KBOs) (Lindgren Stenmark, & Ljungberg, 2003). Knowledge has become the main intangible asset of KBOs and plays a very critical role when two organizations enter into a relationship, since each interlocutor has to disclose its own knowledge in order to achieve knowledge from the other party (Allison & Strangwick, 2008). The above issue is also more critical whenever the two organizations are strangers, that is, they have no a priori information about their interlocutor and they have to take decisions (Heikkinen, Matuszewski, & Hammainen, 2008). This typically happens when organizations are in open environments, such as the Internet or ubiquitous and pervasive environments, where the perceived risk is high.

DOI: 10.4018/ijkbo.2013040101
(Cunningham, Gerlach, Harper, & Kellogg, 2008). In this case, the environment is marked by the following three characteristics:

- **Absence of Identifiers (C1):** Claiming an identity to the interlocutor is useless;
- **Insecure Channel (C2):** The communication takes place over an insecure channel;
- **Absence of a Single Trusted Party (C3):** There is no single authority able to ensure security services (e.g., confidentiality).

C1 derives directly from the definition of strangers: indeed, since organizations are strangers, any identifier name is unknown to the interlocutor. C2 is due to the fact that we are in open environments so that an attacker can sniff, modify, intercept, kill, re-route, delay, and reorder messages (Srinivasulu, Nagaraju, Kumar, & Rao, 2009). C3 models the fact that it is possible to have an external party trusted by two or more organizations but it is unrealistic to assume the presence of a third party trusted by all organizations.

It is expected that in the future there will be a lot of stranger organizations that will have the necessity of entering into a relationship for business reasons. In this paper, we analyze the relationship between stranger organizations and, in particular, the concepts of trust and confidentiality. Indeed, relationships between strangers in an open environment rely on trust, considered as a state in which an entity accepts to enter into a relationship with another entity, expecting to reach a goal (McKnight & Cher- vany, 2001). Confidentiality, usually defined as a service used to keep secret the content of a communication from all but those authorized to have access (Menezes, Vanstone, & Oorschot, 1996), may be requested for relationships. In this study, we formalize the task in which two entities enter into a relationship. Then, we analyze the confidentiality of their communication and we show possible threats.

We observe that the topic of communication between strangers is very relevant also in many other application contexts, like P2P systems, C2C e-commerce, ad-hoc networks, privacy preserving, authentication, trust negotiation, unlinkability, only to cite some examples (some of them will be discussed in the related work section). It is worth noting that we do not introduce here a new technology or a solution to the problem of confidentiality since, as we explain in the paper, no solution exists. Conversely, the contributions of our study can be summarized as follows:

- We define relationships between strangers in an open environment. Even though many works of the literature deal with this topic, they always assume less restrictive hypotheses (see the related work section). To the best of our knowledge, our paper is the first one that formalizes and analyzes such relationships over an environment constrained by the characteristics previously introduced.
- We highlight possible threats and attacks on confidentiality in this scenario. In particular, we explain why, also the use of strong cryptographic algorithms, like RSA, cannot guarantee confidentiality. New technologies often bring some illegitimate expectations and this study is useful to keep in mind their limitations concerning the confidentiality paradigm.
- We prove by model checking that the attacks presented in this paper succeed. The model here built could be used to validate future protocols assuming less restrictive hypotheses or to highlight their possible flaws.

The rest of the paper is organized as follows. We start with the description of the reference scenario by a running example. Then, we give a formal definition of the scenario and we introduce the definitions of trusted and authorized (for confidentiality) entities. We follow this with an analysis about possible attacks on the confidentiality of the communication between
Related Content

Opportunities for Data Mining and Customer Knowledge Management for Shopping Centres
www.igi-global.com/chapter/opportunities-data-mining-customer-knowledge/25235?camid=4v1a

Effective Knowledge Management through Measurement
www.igi-global.com/chapter/effective-knowledge-management-through-measurement/68325?camid=4v1a
Networks of Objects: Practical Preconditions for Electronic Communication
www.igi-global.com/chapter/networks-objects-practical-preconditions-electronic/27289?camid=4v1a

The Amplification-Reduction Structure of Technology: The Example of the Intranet
www.igi-global.com/article/the-amplification-reduction-structure-of-technology/90452?camid=4v1a