Computers and Electrical Engineering 58 (2017) 67–75

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Conceptualizing the silent risk of inadvertent information leakages[☆]

Thomas Lechler, Susanne Wetzel[*]

Stevens Institute of Technology, Castle Point on Hudson, Hoboken, NJ 07030, USA

ARTICLE INFO

Article history:
Received 1 May 2016
Revised 15 December 2016
Accepted 21 December 2016

Keywords:
Inadvertent information leakage
Semi-honest behavior
Risk framework
Case study

ABSTRACT

Cybersecurity researchers and professionals alike strive to develop and implement effective countermeasures to address the problem of data breaches. However, even if all breaches due to misbehavior were preventable, this would not imply that all challenges in the context of data breaches and privacy were addressed. In fact, even intentional sharing of data to enable collaboration bears risks. We argue that the risk of potential information leakages in complex networks by and large is still underestimated to date. This paper introduces the notion of inadvertent information leakages, develops a framework to categorize generic network structures, and analyzes the different categories with regards to their potential for inadvertent information leakages. Furthermore, this paper reviews a case study in the healthcare sector and analyzes the respective network structure based on the risk framework introduced in this paper.

1. Introduction

Today, hardly a month goes by without an announcement on yet another major data breach. Some of the most prominent examples in the recent past include Qatar National Bank, SWIFT, Verizon, and Neiman Marcus [1]. Irrespective of the exact details that have led to data breaches in the past and will continue to lead to such in the future, it is generally recognized that these data breaches typically involve some kind of adversarial behavior or action [2–4]. Cybersecurity researchers and professionals alike strive to develop and implement effective countermeasures to address this problem—with solutions ranging from hardening systems (including data protection techniques, access control mechanisms, firewalls, intrusion detection systems) to user awareness and training (e.g., [5–11]). However, it is important to recognize that even if all breaches due to misbehavior were preventable, this would not imply that all challenges in the context of data breaches and privacy were addressed. In fact, even intentional sharing of data (e.g., with a service provider to enable the completing of a specific task) bears risks for data breaches (e.g., [12,13]). While approaches including information flow control or privacy-preserving techniques strive to address some of these aspects (e.g., [14–16]), we argue that the risk of potential information leakages in complex networks by and large is still underestimated to date. While information leakages are discussed generally (e.g., [12,13]), to the best of our knowledge, there is no formal framework yet which categorizes this problem for specific network structures to facilitate legitimate data exchanges on one hand and analyzes their implications with regards to possibly enabling *inadvertent* information leakages on the other. It is in this context that this paper introduces the notion of inadvertent

[☆] Reviews processed and recommended for publication to the Editor-in-Chief by Area Editor Dr. G. Martinez.

[*] Corresponding author.
E-mail addresses: tlechler@stevens.edu (T. Lechler), swetzel@stevens.edu (S. Wetzel).

http://dx.doi.org/10.1016/j.compeleceng.2016.12.020
0045-7906/© 2017 Elsevier Ltd. All rights reserved.

information leakages, develops a framework to categorize generic network structures, and analyzes the different categories with regards to their potential for inadvertent information leakages. Furthermore, this paper reviews a case study in the healthcare sector. As part of this paper, the overarching network structure from the perspective of a specific hospital is analyzed based on the risk framework presented earlier in this paper.

Outline: The remainder of the paper is structured as follows: In Section 2, we introduce the terminology used in this paper, followed by deriving the risk framework and the respective characteristics in Section 3. In Section 4, we review a case study which was previously presented in [17] and then apply the risk framework as introduced in this paper (Section 5). We close the paper with some conclusions.

2. Context and Terminology

In the following, we further detail some of the basic terminology introduced informally above and then derive our framework to classify the inadvertent information leakage in the context of complex network structures.

2.1. Malicious and Semi-Honest Behavior

Malicious behavior of an adversary (whether inside or outside of a specific entity or network) has been extensively studied in the security literature. Generally speaking, malicious behavior describes the fact that such an adversary may actively carry out arbitrary actions in order to breach a system.[1] Over the years, the security community has developed and implemented a wealth of tools and approaches to mitigate such malicious attacks—including encryption and integrity mechanisms, firewalls, intrusion detection systems, spam filters, to just name a few.

In turn, there is passive behavior of an adversary, also referred to as *semi-honest* or honest-but-curious behavior [18]. In general, this describes a much more subtle type of an adversarial behavior where an adversary behaves honestly in that he carries out all actions as prescribed but takes the liberty to observe and learn and then subsequently use this information to his advantage to the largest extent possible. In fact, one may even argue that this type of behavior is naturally found much more prevalently in any entity or setting, describing an attack pattern that one should assume to be inherently present in practice at all times. There are various approaches known from the literature to thwart semi-honest behavior in certain contexts. Prominent examples include encryption, the use of a trusted third party, or privacy-preserving techniques.

2.2. Inadvertent Information Leakage

In focussing on entities sharing data with each other, we assume that each entity deliberately and very carefully assesses and then decides which data is shared with whom. We furthermore assume that both the sending and the receiving entity take the necessary precautions to thwart malicious behavior. Or put differently, we assume that any entity receiving the data is legitimately entitled to do so; the sending entity provides the data with the *intention* to share the respective data in order to enable the receiver to carry out some specific task; and the expectation of the sender is that the receiver does not have any knowledge of any of the sender's data except for what it deliberately received from the sender itself. Based on these assumptions, we can now introduce the notions of *first-order and second-order inadvertent information leakage*:

Definition 1. Let sender S holding data D_S send exactly $D_{S\rightarrow R} \subseteq D_S$ to receiver R. Then, *First-Order Inadvertent Information Leakage*(IIL_{FO}) at receiver R from the perspective of sender S in regards to $D_{S\rightarrow R}$ which was intentionally provided to receiver R is defined as

$$IIL_{FO}(S, D_{S\to R}, R) := [I(D_{S\to R} \cup \underline{D}_{A_R[S]}) - (I(D_{S\to R}) + I(\underline{D}_{A_R[S]}))] \tag{1}$$

where $I(D_{S\rightarrow R})$ denotes the information associated with data $D_{S\rightarrow R}$.[2] Furthermore, $D_{A_R[S]}$ is some arbitrary data which R might have acquired in some fashion unbeknownst to or unexpected by sender S such that there is a subset $\underline{D}_{A_R[S]}$ of $D_{A_R[S]}$ with $\underline{D}_{A_R[S]} := D_{A_R[S]} \cap D_S$ (with respective information $I(\underline{D}_{A_R[S]})$).

Obviously, $0 \leq IIL_{FO} \leq I(D_S)$. Also, $IIL_{FO} > 0$ if and only if the receiver R holds some $\underline{D}_{A_R[S]} \neq \emptyset$ such that $D_{S\to R} \subset (D_{S\to R} \cup \underline{D}_{A_R[S]})$. Generally speaking, the notion of first-order inadvertent information leakage captures the fact that the receiver may hold more information on the data of the sender than the sender intended when intentionally providing the receiver with $D_{S\rightarrow R}$. It is important to note that the definition does not capture whether or not the IIL_{FO} does actually occur. In fact, for the IIL_{FO} to occur it will be necessary for the receiver R to combine $D_{S\rightarrow R}$ with $\underline{D}_{A_R[S]}$ in order to realize the IIL_{FO}. In particular, this would occur in case of a receiver who exhibits semi-honest behavior.

Furthermore, we observe that a receiver may be able to realize an information gain over $I(D_{S\rightarrow R})$ even in case $D_{A_{R[S]}} \cap D_S = \emptyset$. For example, a cloud provider may be able to derive patterns that cannot be seen by having access to (some) data of individual users only. In the following, we refer to this as second-order inadvertent information leakage which formally is defined as follows:

[1] For a formal definition, see [18].

[2] It is outside the scope of this paper to detail the function that might be used to derive the information from data.