Usable Authentication for Electronic Healthcare Systems

[Poster Abstract]

Qihua Wang
IBM Almaden Research Center
qihua@us.ibm.com

Hongxia Jin
IBM Almaden Research Center
jin@us.ibm.com

1. INTRODUCTION

Access control in electronic healthcare systems has gained popularity in the research community. User authentication is a prerequisite of access control. However, little work has been done on designing authentication schemes in healthcare systems. Most existing healthcare systems require users to login by typing passwords. Even though password authentication has been widely adopted by many practical applications including online banking systems, in our interviews, healthcare practitioners reported poor usability of password authentication in hospitals due to the following fact.

Issue 1: *Doctors wear gloves most of the time during their work.*

Currently, when a doctor wants to access patient records on a computer, she has to take off her gloves to type in password. After she finishes browsing the information, in order to prevent the spread of germs, the doctor has to wash her hands and put on her gloves before continue to work. This is considered very inconvenient by many doctors.

Another concern administrators in hospitals have relates to logout.

Issue 2: *Doctors rarely remember to logout after using a computer.*

Doctors are very busy persons, and oftentimes, they have to rush from one room to another. Having to logout from a computer before leaving is a burden for them, and when they forget to do so, the unattended computer opens a window of security breach.

The above issues, which have been overlooked by researchers, motivated us to propose a usable authentication scheme for healthcare systems.

2. BACKGROUNDS

In an electronic healthcare system, medical records of patients' are maintained in a centralized manner. A doctor is authorized to access the records of her own patients'. There are computer terminals all around the hospital that are connected to the central server. Doctors access medical records through those terminals. Terminals locate in labs, offices, patients' rooms, etc. There are two kinds of rooms where most doctors work daily.

- *Exam rooms for outpatients*: Outpatients are people who come to see the doctors and leave the hospital after a visit. A doctor meet with only one patient in a room at a time. And a doctor may be assigned several exam rooms a day. A doctor may browse patients' records using the computer terminal in an exam room or a computer terminal in an office close to the rooms assigned to her.
- *Resident rooms for inpatients*: Inpatients stay overnight in hospital. Doctors go to these resident rooms to visit their patients from time to time. There is a computer terminal in every room so that doctors may access patients' records whenever necessary.

To allow doctors to authenticate themselves without having to take off gloves, an authentication process should not require users to physically touch anything. RFID authentication is a low-cost authentication approach that provides the "touch-free" property. To authenticate, a user places her badge that contains an RFID tag close to an RFID reader. Many corporations and government agencies use RFID tags as an authentication method for their employees to control the entrance of restricted areas in their buildings. However, RFID authentication is subject to a number of attacks, such as badge-stealing, badge-cloning, and relay attack.

3. DESCRIPTION OF THE AUTHENTICATION SCHEME

Our authentication scheme is based on RFID tags so as to allow doctors to login without taking off their gloves. The scheme employs a novel two-level timeout approach to address the problem that doctors often forget to logout. A number of design decisions are made to enhance the security of the authentication scheme. Furthermore, we adopt a defense-in-depth strategy by specifying a couple of context-aware access control rules to further restrict accesses without compromising the system's usability for honest users.

Equipments Our authentication scheme uses the following equipments.

- *Badges*: Every healthcare practitioner in the hospital is given a badge that contains an RFID tag. The RFID tag is rewritable and has maximum reading range of about $50cm$.
- *RFID readers*: Every computer terminal in the exam rooms and resident rooms is equipped with an RFID reader.
- *RFID writers*: A number of computer terminals (say, five per floor) are equipped with an RFID writer. These writers are used for doctors to refresh a secret stored in their RFID tags.
- *Cameras*: Every computer terminal in the exam rooms and resident rooms for patients is equipped with a camera. The camera is mainly used as an input device that allows doctors to control the terminal in a touch-free manner.

Note that RFID readers and cameras are equipped only to the computer terminals in the working areas where doctors meet with patients and where they have to wear gloves.

Login A doctor may authenticate herself to the system either by using her badge or by typing password. To authenticate with a badge, the doctor stands close to a terminal equipped with an RFID reader and wave her hand in front of the camera to indicate the intension to login (so as to avoid unintentional login). The RFID reader, with a reading range of $50cm$, can detect the doctor's badge when she stands close enough.

A badge stores an identity information and a secret that is shared between the badge and the central server. Upon authentication, both the identity information and the secret are sent to the reader. The secret expires after 24 hours, so every doctor has to refresh the secret on her badge every day before working by putting her badge in an RFID writer and authenticate to the system through password. This is to limit the validity time-span of a stolen or cloned badge. To further raise the bar of common attacks against RFID authentication, if one logs in using a badge, she is subject to context-aware access control rules, which will be discussed later.

Alternatively, a doctor may login by typing password, which requires her to take off her gloves. In our authentication scheme, password is considered to be a stronger authentication method than badge, as stealing a password is normally more difficult than stealing a badge (or luckily find a lost badge on the floor of a corridor). If a doctor logs in using password, she is not subject to context-aware access control rules. This provides flexibility in emergent situations. But we expect doctors to use badges most of time for the sake of convenience.

Logout One may use a traditional timeout approach for the terminal to logout automatically. However, it is not easy to determine an appropriate length for the timeout period. A long timeout period opens up a window of vulnerability as the terminal may remain logged on long after the doctor leaves. In contrast, a short timeout period may force the doctor to login multiple times during a visit, which could be frustrating (as each login procedure takes time).

A key observation is that, when a doctor needs to use a terminal, she must get close to it. A terminal can tell whether the doctor is getting close enough by checking whether the corresponding badge is within the reading range of its RFID reader (which is $50cm$ in this case). This enables us to design a *two-level timeout approach* to address the logout problem. After a doctor logs in using a badge, the computer terminal periodically checks whether the corresponding badge is within the reading range of its RFID reader. If the badge is outside of the reading range (i.e. cannot be detected) for more than 1 minute, the terminal locks itself. A terminal that is locked is unlocked immediately when the corresponding badge is found to be within reading range again. A terminal automatically logs out after being locked for more than 30 minutes. By simulating a very short timeout period while actually having a long one, our two-level timeout approach offers excellent usability and security.

Comparing to an alternative approach in which a computer periodically checks whether the logged-in badge is still in the room, our timeout approach allows the usage of RFID tags with short reading range, which makes cloning and relay attacks more difficult.

Touch-free control of terminals A doctor needs to control a terminal to browse information after login. A touch-free login approach does no good, if the doctor has to touch a keyboard and/or a mouse to control the terminal. Here, we use a camera to allow a doctor to browse information without physically touching an input device. The doctor may move the mouse cursor on the screen by moving her hand or finger in front of the camera accordingly. The motion of her movement is captured by the camera and processed by a motion-tracking application in the terminal. Motion-tracking techniques have been widely used in areas such as video games, e.g. EyeToy for PlayStation. And the functionalities provided by existing products such as EyeToy are more than enough to control a computer terminal to browse documents. Preferably, the browser user-interface of the healthcare system should be designed in a way that facilitates users' browsing control with a camera.

3.1 Context-Aware Access Control

We specify context-aware access control rules to further enhance the security of the authentication scheme. Location and time are the major context information that affects access decisions in healthcare systems. The following context-aware access control rules apply only when a doctor authenticates using her badge.

Rule for inpatients: *A doctor can access her patient X's records only if she is using the terminal in X's room.*

On the one hand, a doctor usually checks her patient's records when she is visiting the patient. So it is natural that the terminal in a patient's room can be used to access the patient's records. However, it is very unusual that a doctor will access patient X's records when she is in patient Y's room. Hence, the above rule does not prevent doctors from doing their jobs as usual.

On the other hand, the rule makes it more difficult for adversaries to steal sensitive information. Without the above rule, an adversary who stole a badge (or possesses a cloned badge) can simply go to an empty room in the hospital and use the computer there to access *any* record that is authorized to the real owner of the badge. In contrast, with our rule, the adversary has to go to a patient's room to access the information of that particular patient. Since the patient is living in the room, the adversary will have to catch a time when the patient is absent so as to use the computer in the room. It is clear that doing so is more difficult than finding an empty room in the hospital.

Our rule also slows down the process of information leakage. To access multiple patients' records, the adversary now has to physically enter multiple rooms, rather than being able to steal all records authorized to the badge using one computer. Furthermore, if the adversary visits several rooms in a short period of time to access several patients' records, his activity can be easily classified as abnormal behavior by the system, because doctors would not visit patients in such a hasty manner. An abnormal behavior will be reported to administrators and future authentication from the suspected badge will be denied.

Rule for outpatients: *A doctor can access her patient X's records only if she is using the terminal in the examine room assigned to X during X's appointment time.*

Most patients make appointments when they would like to see a doctor. For patients who walk in without an appointment, we assume that an appointment is made over the counter. The start time of the meeting is stated in the appointment, and a room is assigned to the patient when he checks-in.

On the one hand, a doctor is unlikely to look at a patient's records unless the patient is meeting with her. And the doctor must be in the room assigned to the patient when they meet. Hence, our rule does not affect the job of the doctor. On the other hand, an adversary who stole the badge from a doctor cannot enter an examine room during appointment time, as the doctor and a patient are in the room. When there is no on-going appointment in an examine room, the computer in the room is not allowed to access the records of any patient due to the above rule.

From the above arguments, we can see that our context-aware access control rules provide an effective second-line defense against attacks on authentication without sacrificing the usability of the system.

4. CONCLUSION

In this paper, we have proposed a usable authentication scheme for electronic healthcare systems. We hope that our work can raise interests on the design of user-focused secure systems, in particular, for those areas with special needs.