Chapter 2
Threshold-Based Location-Aware Access Control

Roel Peeters
Katholieke Universiteit Leuven, Belgium

Dave Singelée
Katholieke Universiteit Leuven, Belgium

Bart Preneel
Katholieke Universiteit Leuven, Belgium

ABSTRACT
Designing a secure, resilient and user-friendly access control system is a challenging task. In this article, a threshold-based location-aware access control mechanism is proposed. This design uniquely combines the concepts of secret sharing and distance bounding protocols to tackle various security vulnerabilities. The proposed solution makes use of the fact that the user carries around various personal devices. This solution offers protection against any set of (t-1) or fewer compromised user’s devices, with t being an adjustable threshold number. It removes the single point of failure in the system, as access is granted when one carries any set of t user’s devices. Additionally it supports user-centered management, since users can alter the set of personal devices and can adjust the security parameters of the access control scheme towards their required level of security and reliability.

INTRODUCTION
Contactless smartcards are often used to enforce access control for secure facilities and buildings. These security tokens contain identifying information and a secret key, used to identify the user carrying the smartcard. When the user approaches the building, he puts his contactless smartcard close to a reader installed in the proximity of the door. Both devices will then carry out a challenge-response protocol, in which the user’s smartcard authenticates itself to the reader (in some scenarios, mutual authentication is required). If the protocol finishes successfully, the user is granted access. Besides access to buildings, similar mechanisms are employed to enter a car

DOI: 10.4018/978-1-4666-2785-7.ch002
Threshold-Based Location-Aware Access Control (Microchip KeeLoq), to use public transport (Octopus Cards, OV-chipkaart, Oyster Online), and even for payments with contactless credit cards (Mastercard PayPass, Visa Paywave).

Although widely used, this conventional access control solution has some important drawbacks, such as several security vulnerabilities. First, the use of a single security token introduces a single point of failure in the system. If this token gets stolen, an unauthorized adversary could get access to a secure building or resource. Security tokens and smartcards could also be compromised or cloned. A recent example of the latter was the MIFARE attack discovered by Gans et al. (2008).

A second security vulnerability is relay attacks, which are also known as mafia fraud attacks. These are man-in-the-middle attacks where a verifier (e.g., the reader next to the door of a building) is tricked in believing that a prover (e.g., the smartcard) is in its close vicinity by an adversary surreptitiously forwarding the signal between the verifier and an out-of-range prover (Kim et al., 2009). Such an attack is important in the setting of access control systems, particularly when challenge-response protocols are employed, and should definitely be avoided.

In addition, both reliability and user-friendliness could be improved in conventional access control systems. For each system the user is enrolled to, and this can be a relatively high number, he has to carry around a separate smartcard or security token. The legitimate user that does not carry around the security token automatically cannot get access. Furthermore, revocation of a particular token is often a cumbersome and relatively slow process. This is illustrated by the following plausible scenario. When initiating the revocation process, the user first informs the facility manager. Second, revocation lists are updated and distributed. Third, the user gets a new token or smartcard. Since such a revocation process is slow, it also poses a security risk: there is a grace period in which the adversary can still use the token before the revocation lists are updated.

Fortunately, both security vulnerabilities can be tackled by introducing several countermeasures. The single point of failure can be removed by sharing the secret over a set of user’s personal devices. The vulnerability against relay attacks can be solved by using distance bounding protocols. In addition, secret sharing also provides reliability to the user and allows for, through the mechanism of resharing, user-centered access control. It hence automatically improves the user-friendliness of the system.

Secret Sharing

The concept of secret sharing was first introduced by Shamir (1979). Instead of storing a secret on one device, the secret is divided into \( k \) pieces, each stored on different devices. Let \( t \) be a threshold number chosen by the user. This parameter directly relates to the security level of the scheme. The main characteristic of secret sharing is that the key can easily be reconstructed from any \( t \) pieces, but even complete knowledge of \( (t-1) \) pieces reveals absolutely no information about the secret. These shares are evaluations of a unique polynomial of degree \( (t-1) \). For \( (t-1) \) or fewer shares, one does not obtain any information at all about the secret, as one cannot reconstruct the unique underlying polynomial. For \( t \) or less stolen devices, there is hence no need for revocation as the adversary obtains no information about the secret. Secret sharing also allows for user-centered access control, since the user can decide which devices get a piece of the key, how large the threshold value \( t \) should be, and when the secret shares should be updated (i.e. when the resharing process should take place).

Outline

In the introduction, we showed that conventional access control mechanisms suffer from several security, reliability and usability issues. We put forward the idea of employing distance