A Context-Aware System to Secure Enterprise Content: Incorporating Reliability Specifiers

Oyindamola Oluwatimi, Maria Damiani, Elisa Bertino

PII: S0167-4048(18)30301-8
DOI: 10.1016/j.cose.2018.04.001
Reference: COSE 1321

To appear in: *Computers & Security*

Received date: 17 November 2017
Revised date: 31 March 2018
Accepted date: 2 April 2018

Please cite this article as: Oyindamola Oluwatimi, Maria Damiani, Elisa Bertino, A Context-Aware System to Secure Enterprise Content: Incorporating Reliability Specifiers, *Computers & Security* (2018), doi: 10.1016/j.cose.2018.04.001

A Context-Aware System to Secure Enterprise Content: Incorporating Reliability Specifiers

Oyindamola Oluwatimi
Department of Computer Science
Purdue University
West Lafayette, IN, USA
ooluwati@purdue.edu

Maria Damiani
Department of Computer Science
University of Milan
Milan, Italy
mdamiani@di.unimi.it

Elisa Bertino
Department of Computer Science
Purdue University
West Lafayette, IN, USA
bertino@purdue.edu

ABSTRACT

The sensors of a context-aware system extract contextual information from the environment and relay that information to higher-level processes of the system so to influence the system's control decisions. However, an adversary can maliciously influence such controls indirectly by manipulating the environment in which the sensors are monitoring, thereby granting privileges the adversary would otherwise not normally have. To address such context monitoring issues, we extend CASSEC by incorporating sentience-like constructs, which enable the emulation of "confidence", into our proximity-based access control model to grant the system the ability to make more inferable decisions based on the *degree of reliability* of extracted contextual information. In CASSEC 2.0, we evaluate our confidence constructs by implementing two new authentication mechanisms. Co-proximity authentication employs our time-based challenge-response protocol, which leverages Bluetooth Low Energy beacons as its underlying occupancy detection technology. Biometric authentication relies on the accelerometer and fingerprint sensors to measure behavioral and physiological user features to prevent unauthorized users from using an authorized user's device. We provide a feasibility study demonstrating how confidence constructs can improve the decision engine of context-aware access control systems.

Keywords

Access Control; Context Awareness; BYOD; Security; Mobility; Biometric; Authentication; Reliability; Proximity

1. INTRODUCTION

Context-aware access control systems aim to secure access to sensitive resources by adapting their access authorizations to the current context *without* explicit user intervention. In fact, enterprise organizations have adopted context-aware systems that leverage proximity-based access control (PrBAC) to mitigate threats of information leakage. That is, access control decisions are not solely based on the requesting user's location, but also on the location of other users in the physical space. In our previous paper [30], we introduced a secure, automated PrBAC architecture and prototype system that we referred to as the Context-Aware System to Secure Enterprise Content (CASSEC). CASSEC addressed two proximity-based scenarios often encountered in enterprise environments (c.f. Section 2): Separation of Duty (SoD) and Absence of Other Users (AOU).

To address such access control scenarios, CASSEC took a wireless, infrastructure-based approach to achieve the localization of occupants within a monitored space which enables geo-spatial RBAC [9, 22]. A wireless, infrastructure-based approach makes the system more resilient to malicious attacks; we assumed, for example, the least amount of trust in users since users may attempt to circumvent the access control process by not manually reporting their location or providing false location data. In addition, the architectural model allowed a fluid context-sensitive authorization process, thereby enabling zero interaction authorization (i.e., it did not require user intervention). While our system was agnostic with respect to the technological choices for detecting physical proximity, we had provided a simple implementation of the complete CASSEC architecture. We utilized Bluetooth and WiFi devices, which are widely used in enterprise environments, to address the occupancy detection problem [17], and therefore, no additional hardware was needed to deploy our system. We first showed how to enforce SoD by using Bluetooth MAC addresses of Client devices of nearby occupants as proof-of-location. That is, we extracted the MAC address from these devices to determine *who* was in a given space. We then showed how to enforce AOU by exploiting the degradation of WiFi received signal strength as a result of human-induced interference when people are near access points. That is, we utilized WiFi-capable devices to determine *how many* people were in a given space. With such information obtained passively by a Proximity Module (PM), the Authorization Server (AS) component was able to enforce PrBAC policies whenever an authenticated Client requested from the Enterprise Content Server (ECS) component access to resources depending on the presence, or lack thereof, of users. Our approach was the first to incorporate WiFi signal interference caused by occupants as part of a PrBAC system. Figure 1 displays CASSEC's architectural components.

The previous approach, however, has several drawbacks. First, it does not take into account the phenomena of radio signals permeating through walls. Multiple proximity modules residing in adjacent proximity zones would simultaneously detect the same Bluetooth-enabled Client, when in fact, the Client only existed in one of said proximity zones. As a result, such a benign occurrence is automatically inferred as malicious activity. Given that Bluetooth's omni-directional transmission range is 10m (~33 ft), the number of false attack detections may increase in standard enterprise settings, such as small offices or conference rooms.