Implementing Graceful RFID Privilege Reduction

M. Butler, S. Reed, P. Hawrylak, J. Hale

Institute for Information Security
University of Tulsa, 800 Tucker Drive, Tulsa, Oklahoma, 74104

Abstract

Radio frequency identification (RFID) technology is used for access control systems, public transit fares, credit and debit cards, and for anti-counterfeiting purposes. In all three cases malicious duplication of RFID tags or their theft can have significant consequences for the owner or product user. This paper presents an implementation of a risk-based access control system, Dynamic Risk Assessment Access Control (DRAAC) for the Microsoft Windows operating system. This implementation of DRAAC can be connected to a wide range of devices including RFID systems, smartphones, and PCs.

Likelihood, Impact, Risk

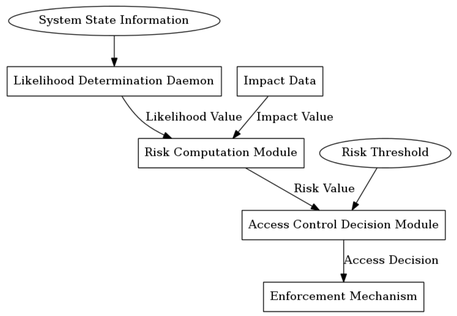

Figure 1: *"DRAAC is broken into independent sections"*

To apply the DRAAC system to RFID related scenarios, card IDs have a "Likelihood" value associated with them stored in a database. Rooms have an "Impact" value denoting importance or how vital it is that an intruder be diverted from the room. Lastly, a "Risk" value can be computed as a function of the Likelihood value of a card and the Impact value of the area it is trying to access, and compared to a "Risk Threshold" which will determine access control (i.e. whether a given door grants access).

Identifying Suspicious Behavior

In Figure 2, circled numbers are doors controlled by RFID scanners, while boxed numbers are Impact scores associated with rooms. The graph on the right shows how a floor plan is understood in DRAAC. Doors that have direct paths between them are connected by an edge. Additionally, doors which lead outside the building are connected to a common zero-node.

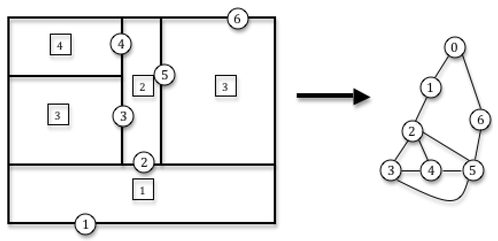

Figure 2: *"Example floor layout and corresponding representation in DRAAC"*

In Figure 3 we will look at an example scenario where two users, one legitimate the other malicious, traverse a building who's doors are monitored using DRAAC. The legitimate user is marked using a green path, while the malicious user is denoted by a red path.

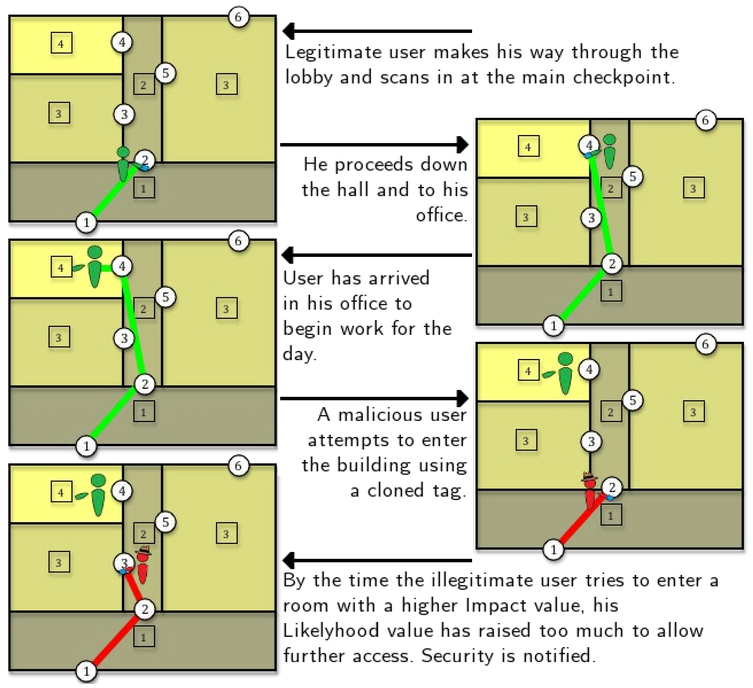

Figure 3: *"Sample DRAAC Scenario"*

By recording all scans and access attempts and putting them into context relative to one another, DRAAC is able to make assertions about how suspicious the behavior of a certain user is. If a card has been cloned, its abnormal use will stand out and cause DRAAC to respond accordingly.

The potential does not stop at basic access control. There are many uses for RFID technology in electronic commerce as well as product shipment. Binary decision processes such as access or no access introduce problems for legitimate users. Graceful degradation of privilege in response to potential security violations is a better option. In the commerce example, the purchasing limit can be restricted gradually to prevent large-scale fraud, but allow the legitimate user the ability to perform critical tasks, such as paying their bus fare home.

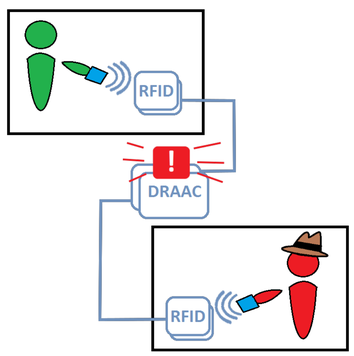

Figure 4: *"Suspicious behavior is recognized"*

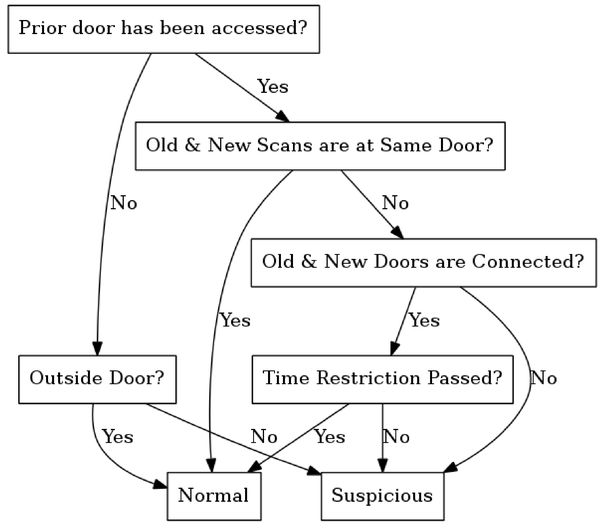

Figure 5: *"Rules are formed to identify suspicious behavior"*

In this implementation, two types of suspicious activity are detected: adjacency violations and temporal violations. Adjacency violations are situations in which a badge is used to open two doors separated by a third which the badge was not used to open between the two access attempts. Temporal violations are situations in which a badge is used to open two doors separated by a distance that would not be physically possible to travel within the time between accesses.

Other suspicious activities could be detected by creating more rules which quantify the activities appropriately using the facts presented to DRAAC. The expert system used for decision making makes adding additional rules on top of existing rules trivial. Furthermore, facts generated by one decision tree can easily be used by another.

Future Work

- Distribution of state information efficiently across multiple systems
- Giving multi-building/multi-site organizations a more accurate picture of RFID tag activity
- Interactions between the environment and the access control system
- Handling emergency situations in combination with risk analysis
- Integrating a more advanced AI system for decision making
- Accessing knowledge beyond just RFID scans to help with decision making
- Help identify unsafe behavior such as tail-gating or letting a co-worker through a door with your ID
- Using spatial access control systems to gather more data about users

This material is based on research sponsored by DARPA under agreement number FA8750-09-1-0208. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon.
The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of DARPA or the U.S. Government.