17-10-2007

Location-based DRM using WiFi Access Points

Martin Jan Surminen
University of Wollongong, surminen@uow.edu.au

Nicholas Paul Sheppard
University of Wollongong, nps@uow.edu.au

Reihaneh Safavi-Naini
University of Calgary, Canada, rei@uow.edu.au

Recommended Citation

Surminen, Martin Jan; Sheppard, Nicholas Paul; and Safavi-Naini, Reihaneh: Location-based DRM using WiFi Access Points 2007.
https://ro.uow.edu.au/infopapers/656

Location-based DRM using WiFi Access Points

Abstract

Location-based Digital Rights Management (DRM) refers to a system allowing the owner of an electronic file to specify not only the actions a user is allowed to perform regarding the content, but also restrict the actions to a specified geographical area. A method for retrieving location information is required. One such method is to place wireless accesspoints in areas of interest, requiring a device to be in the vicinity of the correct accesspoint(s) in order to access a file.

Disciplines

Physical Sciences and Mathematics

Publication Details

This conference paper was originally published as Surminen, MJ, Sheppard, NP, Safavi-Naini, R, Location-based DRM using WiFi Access Points, International Symposium on Communications and Information Technologies ISCIT 2007, 17-19 Oct, 882-886.

Location-based DRM using WiFi Access Points

Martin Jan Surminen[*], Nicholas Paul Sheppard[†], Reihaneh Safavi-Naini[‡]
[*]School of Computer Science and Software Engineering, University of Wollongong, NSW, 2522, Australia
Email: surminen@gmail.com
[†]School of Computer Science and Software Engineering, University of Wollongong, NSW, 2522, Australia
Email: nps@uow.edu.au
[‡]Department of Computer Science, University of Calgary, 2500 University Dr. NW, Calgary AB T2N 1N4, Canada
Email: rei@cpsc.ucalgary.ca

***Abstract*—Location-based Digital Rights Management (DRM) refers to a system allowing the owner of an electronic file to specify not only the actions a user is allowed to perform regarding the content, but also restrict the actions to a specified geographical area. A method for retrieving location information is required. One such method is to place wireless accesspoints in areas of interest, requiring a device to be in the vicinity of the correct accesspoint(s) in order to access a file.**

I. Introduction

Digital rights management (DRM) technology allows the owners of electronic information to control the use and distribution of that information. DRM restricts access to an encrypted file according to a policy set out in a machine-readable *license*.

Traditional DRM was used to protect multimedia such as music, video or artwork. With the increased use of electronic document storage the need for protection of digital objects during their lifecycle increases. In the case of corporate Intellectual Property (IP) there is the additional need of restricting access to limited times and locations. E.g.

- University library, lending material to students
- Club, licensing music for playing in a club area
- Employee accessing IP at office but not at home

In addition, the increased use of wireless connections and networks bypasses the need for a malicious user to gain physical access to a terminal or network in order to access content. The use of portable PDAs and wireless enabled laptops may enable an attacker to access corporate data from outside a company's physical security measures. Location constraints are meant to address this issue by ensuring that a device is present on-site, allowing an employee access to content when at work but not from home or outside the company.

Since most corporate and academic environments already have a network of WiFi accesspoints in place, and since these devices rarely move, it might be possible and convenient to use these to verify the location of a device and enforce the constraints. In the case of a WiFi location system like this, the DRM client does not need to know where it is, only whether or not it is in the vicinity of the WiFi accesspoint(s) specified in the license, and the DRM provider does not need to know where the device is at all. This has the added benefit of providing privacy to the user since only the user's device holds the location information.

Abbr.	Description
RO	**R**ights **O**bject, license
AP	Wireless **A**ccess**P**oint
BSSID	**B**asic **S**ervice **S**et **I**dentifier, unique AP identifier
DRM	**D**igital **R**ights **M**anagement
Hotspot	Area covered by one or more AP(s)
wifi	**Wi**reless **fi**delity, 802.11 type networks
ODRL	**O**pen **D**igital **R**ights **L**anguage
REL	**R**ights **E**xpression **L**anguage
dBm	dB milliWatts. dBm = log(mW) * 10
RSSI	**R**eceived **S**ignal **S**trength **I**ndication, measures received signal strength in a WiFi adapter

TABLE I
Notation and Definitions

In this paper we propose a simple addition to the existing OMA DRM system. By allowing a DRM system to enforce a location constraint using an already present infrastructure the system can be used in a wider range of situations. One such example is within Enterprise DRM (EDRM) where the prevention of intellectual property leaking outside a company is crucial.

In Section III we present a short description of the 802.11 wireless structure and how the signalstrength and range of standard hardware WiFi accesspoints can be used to determine or verify location. Our implementation is described in Section IV. We give an overview of the OMA DRM system followed by a description of how to define a spatial constraint in a license. Some data from our experiments follows. Attacks on the system are outlined in Section V and a conclusion follows in Section VI.

II. Related Work

Numerous systems have been proposed for determining or verifying the location of a mobile device. In the application considered in the present paper, we require the location of a mobile device to be verified such that a dishonest user cannot fake his or her location. Many such systems have been proposed, based on WiFi networks, GPS, cellular telephone networks, RFID and other sensor networks. A variety of commercial systems are available from Newbury Networks [8], Ericsson [3] and Ekahau [2].

The approach described in this paper differs from most of the foregoing work in that we do not attempt to determine the

1-4244-0977-2/07/$25.00 © 2007 IEEE

location of the device, or require a third party to track the location of a mobile device. Our approach is most similar to that of Kindberg, et al. [6] in that we use the presence or absence of a signal with a known geographical distribution to bound the location of a device. Their system, however, requires mobile devices to engage in a challenge-response protocol with a third party location verifier while our system enables the device to perform an entirely self-contained location verification.

In this way, location-based access control rules can be enforced without any implications for the privacy of the user, and without the need for devices to contain large databases of reference points from which they can compute their position as in the Placelab [9] and Herecast [4] systems. While GPS-based systems such as Mundt's [7] have similar properties, GPS signals cannot penetrate buildings and WiFi-based systems are more effective in this context.

III. Bounding Location using WiFi

A. WiFi

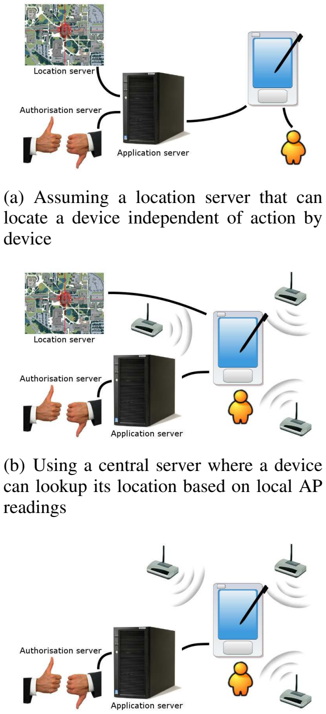
WiFi is short form for "wireless fidelity" and refers to any type of 802.11 network, whether 802.11b, 802.11a etc. The term is promulgated by the Wi-Fi Alliance. WiFi was originally intended for use with mobile devices and LANs, but is now used extensively for Internet access as well. A region covered by one or more AP(s) is called a hotspot and allows a device to access the network(s) serviced by the AP(s).

Each AP has a unique identifier, the BSSID. This identifier is broadcast by most public APs and allows a client to identify which APs it is connected to or has access to.

The BSSID of (an) AP(s) can be used by a device to determine its location. This can be done in at least two ways. One way is having the device read AP BSSIDs and signalstrengths of the APs surrounding it and sending the information to a server capable of interpreting the information and return an absolute geographical position as in 1(b). Another way is to let the device read the AP information and determine its location relative to the APs as in 1(c).

RSSI is an acronym for Received Signal Strength Indication and is a numerical representation of the strength of the received signal in a WiFi adapter. RSSI measurements may vary from 0 to 255 depending on the vendor. 0 indicates no signal and RSSI_Max indicates full signal strength. For example, Cisco Systems cards will return an RSSI of 0 to 101. In this case, the RSSI_Max is 101. RSSI is however an arbitrary numeric interpretation of the basic signal strength. It is not specified what dBm should be mapped to what RSSI value, so this is largely up to the vendors to decide, allowing for variations between devices of different brands. The RSSI was originally only meant to be used internally in the device to among other things decide when a device is clear to send.

As demonstrated in the Placelab and Herecast systems [4], [9], an absolute location can easily be determined. This requires the existence of a globally accessible database. It also requires the device to obtain its location from said server, diminishing the privacy of the devices using the system. In this case, the license needs to specify the geographical coordinates that limit the area within which the content can be used. This requires detailed knowledge on the part of the license creator that needs to know the absolute geographical positions, BSSIDs, and signalstrengths of every AP to be included in the license.



(a) Assuming a location server that can locate a device independent of action by device

(b) Using a central server where a device can lookup its location based on local AP readings

(c) The device determines whether it is within specified range of a set of APs specified in the license

Fig. 1. Different methods with which the location information can be obtained

In a DRM scheme, a device need not know its real world location. It needs only know where it is in relation to a specified set of APs. By specifying a set of APs, using their BSSIDs, and require a device to identify and be within range of one or more of them, an area can be defined. A device that can access the required number of the specified APs can therefore verify that it is in a specified location and allowed to access a file. This only requires the license creator to know the BSSIDs and signalstrengths of the APs to be used. These can all be easily measured as needed.

B. RSSI value normalization

It is possible to further refine the area in which a file can be accessed by observing the RSSI value of each AP. Specifying accepted signal strength range(s) along with the BSSID(s) can help specifying the accepted area with even smaller granularity.

Since the RSSI values vary between vendors and even between different cards by the same vendor in some cases, it may be necessary to normalise the RSSI values.

Name	MinRSSI (a)	MaxRSSI (b)
D-LinkAirPlusDWL-650+	50	100
D-LinkAirDWL-610	-50	-100
TopComSkyr@cerPCCard3044	50	100
Atheros based cards	0	60
Cisco cards	0	100

TABLE II
DIFFERENT VENDOR CARD'S RSSI RANGES

RSSI values can be normalized into a percentage scale using Equation 1. The equation consists of the variables RSSI, a, and b. RSSI is the actual value from the access point, a is the lowest possible signal strength, and b is the highest signal strength possible.

$$normalizedRSSI = abs\left(\frac{(RSSI - a) \times 100}{a - b}\right) \quad (1)$$

Table II shows a few cards and their RSSI value ranges. The range depends on the manufacturer of the chipset the card is based on. Cisco cards range between 0 and 100 while Atheros based cards range between 0 and 60.

Different RSSI values between diffent vendors is not a major issue in an enterprise environment where this type of system is likely to be implemented. Within a company or similarly controlled environment, uniform hardware is commonly deployed and the system can be attuned accordingly.

IV. IMPLEMENTATION

A. OMA DRM

The Open Mobile Alliance (OMA) is the organization that specifies mobile service enablers that ensure service interoperability across devices, geographies, service providers, operators, and networks. OMA DRM Version 2.0 is a standard to specify methods of secure delivery of and protection of multimedia content. The OMA DRM system consists of rights issuers (RIs) who are responsible for providing rights objects (ROs), or licenses, that permit access to protected content and managing authorized domains, and DRM agents that permit users to to use protected content according to the rights specified in ROs.

All DRM agents must meet tamper-resistance requirements specified by OMA, and be certified by the Content Management License Administrator (CMLA) before being permitted to access ROs and protected content. This guarantees that dishonest users will not be able to extract unprotected content or decryption keys from devices.

Protected content is distributed in an encrypted format called the DRM Content Format (DCF). Each DCF file is encrypted using a random content encryption key (CEK) and can be freely distributed using any convenient method. The content encryption key is included in any RO that awards rights to use the associated content, and the sensitive parts of the RO (including the CEK) are encrypted using a rights encryption key (REK). Finally, the rights encryption key for an RO is encrypted using the public key of the DRM agent for which the RO is intended. This DRM agent can then access the content by reversing the chain of encryption.

Typical constraints supported by OMA include count and time constraints, allowing a user to access a content a certain number of times or for/during a certain period of time. The OMA specification does not explicitly define a location or spatial constraint.

B. Our spatial constraint

We have developed a system using WiFi devices for location verification, adding location as an additional control parameter in our extended OMA DRM system. The Placelab API [9] was used to access WiFi APs and read signalstrengths. This system can be used with Bluetooth beacons, WiFi APs, or a combination thereof.

In our DRM system, the extended rights object contains information specifying the geographical area in which the content associated with the rights object can be used. In order to specify a location the rights object needs to contain information about AP(s) and signalstrength(s). To accomplish this, a rights object using an extended version of the ODRL was created. This rights object specifies the BSSID(s) of one or more APs located in the area where the content is allowed to be used. It may also contain an upper and/or lower bound on the signalstrength for each AP *(See table III)*.

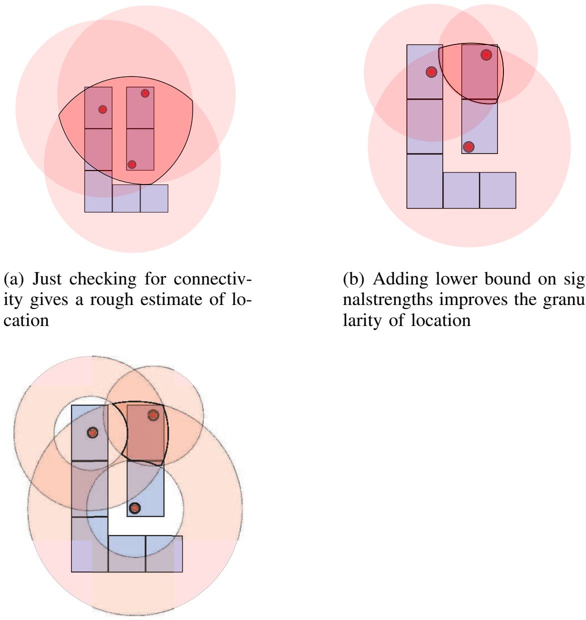
```
<o-dd:play>
  <o-ex:constraint>
    <o-dd:count>7</o-dd:count>
  </o-ex:constraint>

  <o-ex:constraint>
    <o-dd:location>
      <o-dd:accesspoint>
        <o-dd:bssid>
          00:0e:38:a3:cf:cb
        </o-dd:bssid>
        <o-dd:rssi>43,55</o-dd:rssi>
      </o-dd:accesspoint>
      <o-dd:accesspoint>
        <o-dd:bssid>
          00:0e:83:5c:cf:cb
        </o-dd:bssid>
        <o-dd:rssi>26,61</o-dd:rssi>
      </o-dd:accesspoint>
    </o-dd:location>
  </o-ex:constraint>
</o-dd:play>
```

TABLE III
EXTRACT FROM RIGHTS PART OF RO WITH LOCATION INFORMATION

The device can enforce the location constraint by refusing to use content if the correct APs, as specified in the rights object, cannot be accessed. The rights object could specify a number of APs and require the device to be within range of any them. The rights object could also specify several APs and require the device to be within range of all or some APs listed, thus limiting the area. Since the BSSID of the AP(s) can be read directly by the device, no server lookup is needed.

As can be seen in Figure 2, different levels of granularity can be achieved depending on the amount of information specified in the rights object. More APs and tightly specified allowed ranges for the signalstrengths to each allows for finer granularity. As can be seen in Figure 3, an issue with using APs indoors is that a hotspot extends in a sphere. This may allow an attacker sitting on a higher or lower floor to access content meant for a room on this floor. The signal will however be attenuated when passing through the ceiling of this floor, making it possible to exclude other floors with carefully selected signal ranges.


(a) Just checking for connectivity gives a rough estimate of location

(b) Adding lower bound on signalstrengths improves the granularity of location

(c) Adding range for signalstrengths improves the granularity even more

Fig. 2. Levels of granularity depending on specified signalstrengths

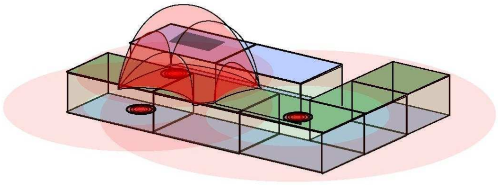


Fig. 3. The range from each AP is extended as a sphere, allowing for access from an elevated point

The ranges as described and as shown in Figures 2 and 3 are idealized. In a real environment objects and walls will interfere with the signals and distort the ideal spherical hotspot as in Figure 4. This is a problem that affects all technologies relying on connection between objects, like WiFi, GPS and GSM.

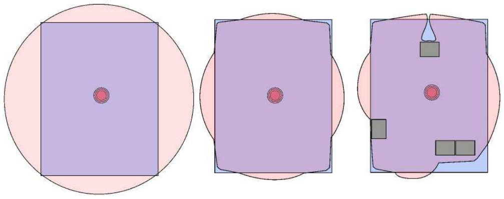


Fig. 4. The ideal spherical hotspot around an AP can be distorted by walls and objects like heavy cabinets

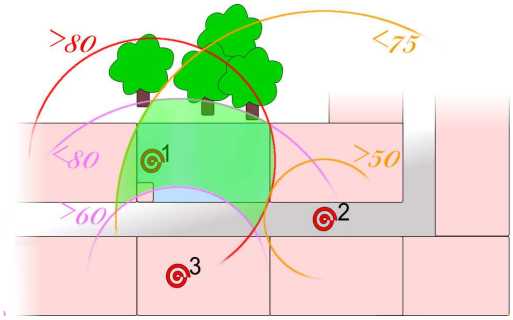


Fig. 5. Positions and layout of the testing area

C. Experiments

We performed a series of tests with the aim of determining whether a limited area could be bounded by measuring signalstrengths of surrounding WiFi accesspoints. The general layout of the testing area can be seen in Figure 5 where the numbered twirls represent accesspoints. The strength of the signal is given by a number between 0 (no connection) and 100 (perfect connection).

We noted the strengths of a series of readings at different times in each corner of the room in which accesspoint 1 is located. Several readings were made to eliminate the chance of getting a misread due to temporary atmospheric distortions, moving people and similar disturbances. The average values of the readings for each corner can be found in Table IV

As can be seen, by requiring that a device can get a signalstrength above 80 connecting to accesspoint 1, the area where a device can access a content can be limited to within a certain distance of that accesspoint. By requiring a signalstrength between 50 and 75 to the second AP, the area can be further limited. Combining this with a required signalstrength between 60 and 80 to AP number 3, the bounded area is limited to within the room.

The areas overshooting the desired area, allowing an attacker to access a content by standing just outside a wall, e.g. at the top, left and bottom right parts of the room, will be almost non-existent due to signal attenuation through the walls *(see Figure 4 for an example)*.

By incorporating a WiFi reader into our implementation we found that content could not be accessed anywhere outside the bounded room but could be accessed from anywhere within the room most of the time. Trying to access content within

Accesspoint	NW	NE	SE	SW
1	89	91	80	83
2	51	61	71	64
3	69	63	78	74

TABLE IV
Average signalstrength readings from test location

the area but standing close to a boundary would occasionally cause access to be rejected.

V. Attacks

This technology used in this way is vulnerable to a number of attacks due to the fact that WiFi APs are not intended for the purpose of locating themselves or devices connecting to them. The purpose of an attack in this context would be either to trick a device into verifying that it is in a specific location when it is not, or to prevent a device from verifying that it is in a location when it actually is.

A. Authentication

One issue is **authentication** of the AP itself. An AP broadcasts its BSSID to every device in range, but a rogue accesspoint with the same BSSID can relatively easily be created using tools like airsnarf [1]. This would allow an attacker to make a device believe it is in the vicinity of a specific AP even though it is not. Unless the AP have the means of encrypting the broadcasted data with for example a private-public key-pair, there is little that can be done to prevent this. An approach would be to have the AP broadcast its BSSID and a timestamp, all encrypted with a private key. A device can then verify that the broadcasted BSSID comes from the real AP and that it has not been tunnelled from another location using a wormhole attack.

B. Wormhole attacks

Wormhole attacks are attacks where an attacker receives packets at one point in a network and tunnels these packets (possibly selectively) to another point. This allows a rogue AP to pose as a real AP even if a device authenticates an AP using a protocol. The attacker can simply pose as the real AP, tunnel the device's authentication code to the real AP and tunnel the responses back to the device, making the device assume it is in an accepted location to access content. These attacks are difficult to detect and protect against. One proposed method is to use packet leashes as described by Hu, Perrig and Johnson [5]. This requires the devices and AP(s) to have tightly synchronized clocks allowing for detection of large tunnelling times of packages (temporal leash). Mundt defines a system that can be used with WLAN mesh networks to authenticate APs and prevent tunnelling or wormhole attacks in his paper [7]. In this system each AP is assumed capable of two-way communication and in possession of a public/private key-pair. Each AP is also paired with a secure hardware module with a precise clock. In order to prevent spoofing of the node, messages are signed using the private keys. The secure clock is used to measure network latency. A tunnelling or wormhole attack introduces latency in the signal since all data must be retransmitted to a remote location. By measuring this latency and by making multiple measurements and use the minimum as the correct latency, normal temporary delays due to busy channels can be distinguished from tunnelling which introduces a constant delay.

C. Denial of Service attacks

Another easily mounted attack on an AP is a **Denial of Service** (DOS) attack. A DOS attack is commonly executed by flooding a device, in this case an AP with a large amount of fake messages or requests. A DOS attack will in this case never result in a successful retrieval of protected content. If the communication is interrupted by an attacker, the location will in worst case not be established and the DRM system will reject the request.

VI. Conclusion

We proposed a method that uses location as an additional decision parameter in a Digital Rights Management system by using WiFi accesspoints to verify the location of a device. In order for this method to be used in a real-world system, a few things are required from the WiFi acesspoints. The existence of public/private key-pairs and the addition of a precise, tamper-proof internal clock are needed to ensure that the location obtained by a device is correct. Using more advanced, later generation accesspoints with on-board processing capability will allow for two-way protocols for authentication and timestamping.

VII. Acknowledgements

This work was partly funded by the Co-operative Research Centre for Smart Internet Technology, Australia. We would like to thank Harikrishna Vasanta for stimulating discussion on this subject.

References

[1] Airsnarf. airsnarf. http://airsnarf.schmoo..com., January 2007.

[2] Ekahau. Ekahau. http://www.ekahau.com, 2007.

[3] Ericsson. Mobile positioning system. http://www.ericsson.com/mobilityworld/sub/open/technologies/mobile_positioning/index.html, 17 February 2007.

[4] Herecast. herecast. http://www.herecast.com., April 2006.

[5] Hu, Y., Perrig, A., and Johnson, D. Packet leashes: A defense against wormhole attacks in wireless ad hoc networks. *In Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003)* (April 2003).

[6] Kindberg, T., Zhang, K., and Shankar, N. Context authentication using constrainted channels. In *Fourth IEEE Workshop on Mobile Computing Systems and Applications* (2002), pp. 14–21.

[7] Mundt, T. Two methods of authenticated positioning. In *Q2SWinet '06: Proceedings of the 2nd ACM international workshop on Quality of service & security for wireless and mobile networks* (New York, NY, USA, 2006), ACM Press, pp. 25–32.

[8] Newbury Networks. WiFi Watchdog. http://www.newburynetworks.com/products-watchdog.htm, 2006.

[9] Placelab. placelab. http://www.placelab.org., April 2006.