Location Aware Mobile Device Management

Jaco du Toit
Academy of Computer Science and Software Engineering
University of Johannesburg
Johannesburg, South Africa

Ian Ellefsen
Academy of Computer Science and Software Engineering
University of Johannesburg
Johannesburg, South Africa

Abstract—**Mobile devices have created a situation where system-focused security may not be sufficient in an environment where security requirements can change depending on the location of a mobile device. The security on a network at a corporate company may be different in a boardroom, where sensitive information is discussed and acted upon, than at an employee's desk, where the employee works with his normal line of business application. The Neo Model is a conceptual model that describes a hypothetical black box, called the Neo device, which uses secure containers and mutual authentication to connect to specialised gateway controllers. The gateway controllers have the ability to control and manage the Neo devices to ensure that specialised secure containers can be provisioned to Neo devices and activated or deactivated, depending on where the Neo device is physically located on the network. The Neo Model allows companies to define security controls that is applicable depending on where the mobile device is located on the network.**

Keywords—security, mobile, network

I. Introduction

In a company, the typical "Bring Your Own Device" (BYOD) policy concerns itself with the security of company assets, the confidentiality of corporate data and the privacy of its users [1].

Mobile devices are here to stay and has had a significant impact on corporations [2]. Mobile devices create an environment where system-focused security requirements may not be capable of addressing the risks exposed by these devices. Examples of risks can include the following: A user can record a potentially sensitive meeting and then access it from her desktop computer, using an integrated cloud based storage solution. While the sensitive information is stored in the cloud based storage solution, the information is susceptible to unauthorized access by anyone that has access to the user's cloud login credentials.

In some companies the use of the camera in a mobile device is strictly controlled to ensure compliance with regulations, specifically where minors are involved. The use of a camera by childminders in the United Kingdom is allowed, but for only specific reasons and the photos must be controlled after a picture is taken [3] [4].

BYOD implementations imply that the device used by the employee is private property. Employees are hesitant to allow a company control over their devices, potentially exposing private data to the company [5] .

The problem addressed in this paper can be formulated as follow: Some corporations need to control mobile devices depending on the location of the devices on their networks, as well as assuring employees that their privacy will not be breached.

This paper describes the Neo Model [6], with specific emphasis on how the Neo Model approaches location aware device management so that personal data and information is kept secure.

The Neo Model has two important properties. These two properties allow corporations to control access to specific applications and data, depending on where the device is located, while assuring privacy of personal information. The two properties of the Neo Model are:

- The secure container property (SCP). The Neo Model isolates user data and applications using virtualisation. Any user must first be authorised access to the Neo device before they can use a container on the device.
- The mutual authentication property (MAP). Any user, peripheral or network must first be authorised before they can connect to a container on the Neo device. Authorisation is granted to a specific container and not the device in general.

This paper is organised as follows.

Section II gives an overview of the Neo Model, providing background information on how information is stored and controlled. Section III describes how the Neo Model allows data and applications to be isolated between company and personal data and applications. Section IV describes how a company can control access to its network and control access to company specific applications and data. Section V concludes with a summary of the problem and how the Neo Model can be used to control access to company applications and data depending on physical location.

II. Overview of the Neo Model

The Neo Model was first described in 2015 by [6] to address the problem of private devices being used to capture company data and then using potentially insecure methods to share, backup and gain access to the data that was captured.

At its core, the Neo Model describes a hypothetical black box, called the Neo device. The Neo device consists of a number of secure containers and controls access to the secure containers through an identification and authorisation layer.

Other characteristics of the Neo device is that it has no built in screen or does not have any other Input\Output (I\O) peripherals connected to it. The device primarily uses wireless

978-1-4799-7755-0/15/$31.00 ©2015 IEEE

peripherals to communicate with the device. This gives the user the flexibility to select different form factor peripherals that he prefers.

The Neo device, displayed in Figure 1 consists of a number of containers that hosts a fully functional operating environment, including virtualised network interface cards. Each container is separated from each other. Any user and I\O peripheral must first be authenticated and authorised before it can gain access to a specific container. This is known as the secure container property (SCP) of the device.

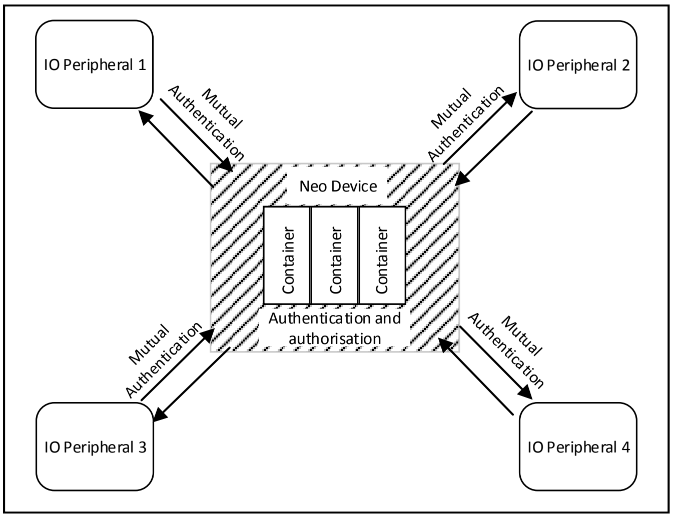

Figure. 1. Overview of the Neo Model [6].

The Neo device has an authentication and authorisation layer that controls the access between the Neo device and the I\O peripherals that connects to it. Each I\O peripheral also consists of an authentication and authorisation layer which in turn also authenticates and authorise the Neo device to connect to it. This means that there are mutual authentication between the I\O peripheral and the Neo device and is known as the mutual authentication property (MAP).

The Neo Device can be used in a number of scenarios. They are:

- **Connecting different I\O peripherals**. The Neo Device is not limited to a specific size or type of I\O peripheral. This means the user of the Neo device can have a mobile phone sized touch screen with microphone and speaker while commuting to and from work, while it can use a specialised docking station when at work to interact using a physical screen, keyboard and mouse.

- **Corporate connectivity**. While at the office the Neo device is granted access to a specific docking station or wireless network. This allows the user to use the Neo device not only for personal use, but also for company use. Wireless connectivity at a company is managed through a specialised Gateway Controller. The Gateway Controller authorises and authenticates different users and Neo devices. This aspect of the Neo Model is described in more detail in section IV of this paper.

- **Device interconnectivity**. The mutual authentication model that exists between the Neo device and its I\O peripherals also exists when one Neo device connects to one or more other Neo devices. This allows the Neo device to share and interchange information between Neo devices for specific secure containers that exists on the Neo devices.

This section gave a high-level overview of the Neo Model. The Neo Model makes use of a hypothetical device called the Neo device. The Neo Model has a secure container property and a mutual authentication property. The next section goes into more detail about the SCP and how it ensures isolation of corporate data and personal data.

III. Business access using secure containers

The two components in the Neo model that allows the system to be used for both personal and company use are:

- **Secure containers**. The Neo device stores personal data and applications in a personal container and any company related applications and data in corporate containers.

- **Identification and authorisation service**. The identification and authorisation service controls access to the personal and corporate containers ensuring privacy of user information, but also allowing corporate control over company data and applications.

These two aspects are now described. The first aspect described is the secure containers

A. Secure containers

Strategies to isolate personal and company applications and data can be categorised into three categories [7].

- **Secure Containers** are achieved by using application level activity to separate and manage user and company applications and data. This is usually managed by using some type of management framework and policies in the mobile operating system or third-party applications [8]

- **Mobile Virtualisation** creates operating system environments with their own set of virtualised hardware separate from the physical hardware on the device. The virtualised systems are managed through a hypervisor and has been widely used on traditional computers [9].

- **Operating System Extensions** are built into mobile operating systems to categories data and applications as either personal or company. The operating system then ensures that any mobile device management (MDM) system can only access content categorised as company [10] [11]

Secure containers have the advantage of running as an application inside the mobile operating system. It does not require any changes to the mobile operating system image [7].

Mobile virtualisation ensures isolation of not just data and applications, but also hardware. Mobile virtualisation can produce a more isolated environment for data and application isolation. The disadvantage of mobile virtualisation is that the ARM processor has limited hardware virtualisation capacity, which makes full virtualisation on today's hardware slower than native applications [12].

Both Apple with iOS 8.x and Google Android 5.x support categorisation of company and personal data and applications. In the case of MDM systems, the operating system ensures that only applications and data marked for company use can be accessed [10] [11]. The functionality of these mobile operating system extensions fall short of some of the requirements where a company may have different levels of access and thus require different levels of categories of company data and applications.

The Neo Model describes the Neo device with multiple secure containers by using virtualisation as a method to achieve the secure container property. The virtualisation techniques and how they apply to the Neo Model is described in more detail in [6].

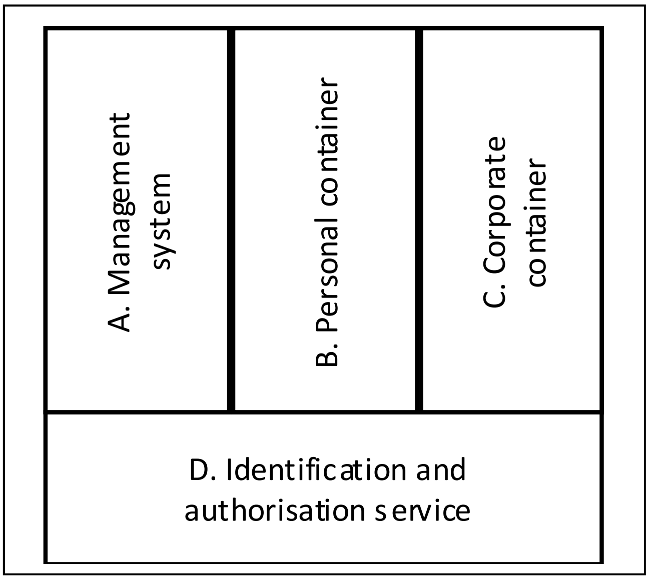

Figure. 2. Software architecture on the Neo device [6].

Figure 2 shows the Neo device with three distinct containers (A, B and C) and the ever present identification and authorisation service (D).

The first container that always starts up in the Neo device is the management system (A in Figure 2). The management system controls the identification and authorisation service and starts up and shuts down other containers. Users cannot store personal information in the management system, instead they interface with the management system when they select a specific personal or corporate container.

The first user that makes use of the Neo device is known as the owner of the system. This user has the ability to give other users or corporates access to the Neo device. Every user on the Neo device has its own personal container (B in Figure 2).

The Neo device creates one or more corporate containers (C in Figure 2) to store and access corporate data and applications. These corporate containers can be linked to different companies, or even different areas inside a specific company.

The corporate containers have no access to the personal containers on the Neo device. In fact the corporate containers have access to nothing outside their own containers. This means that the Neo device can be used not just at one company, but other companies as well, and each company can be assured that their data and applications are isolated from each other.

Each container is encrypted while at rest and can only be decrypted by either the correct user account, in the case of personal containers, or through the connection to an authorised gateway controller, in the case of corporate containers. More information regarding the encryption properties of the containers can be found in [6]. More information regarding the gateway controller can be found in section IV.

Corporate containers are created when a user enrols their device on a corporate network. The company authorises the Neo device access to the network and then the device creates the corporate container according to policies defined by the MDM system. The policies and how the MDM accesses the Neo devices is described in more detail in section IV.

The SCP of the Neo model ensures data and applications are isolated in the Neo device. Then next component in the Neo Model that ensures isolation and controlled access of personal and company data and applications, is the identification and authorisation service.

B. Identification and authorisation services

The identification and authorisation service (D in Figure 2) controls access to the different containers for users and other I\O peripherals and devices.

The identification and authorisation service uniquely distinguishes between users, I\O peripherals and gateway controllers. Access to the different containers are controlled using rules. These rules are stored by the management system and used by the identification and authorisation service.

Figure 3 shows two rules that the identification and authorisation service uses to control access to a specific container in the Neo device. It shows that at a specific time various security objects and subjects can interact with each other. The two access rules ensure that a user account using a specific I\O peripheral will firstly have access to the Neo device (Access Rule 1) and secondly that it can access Container A on the Neo device (Access Rule 2). The interaction between gateway controllers and the Neo device is explained in more detail in section IV of this paper.

When a user enrols the Neo device on a corporate network, the Neo device creates a corporate container on the Neo device. The owner of the Neo device does not have default permissions to the corporate container, except to delete the container.

The company makes use of a MDM system that ensures that only a specific user on the Neo device, using a pre-defined combination of I\O peripherals have access to the corporate container.

This means the company can control which user on a Neo device, if there are more than one user, has access to the corporate data. The company can further control which I\O peripherals the user can use to access the company data. That means that the company may choose to lock down corporate data to only be accessible when using the corporate owned docking station at the office, or only the tablet-sized touch screen device that the user owns.

The identification and access control service handles the encryption and decryption of containers in the system. Each container handles its own network encryption established between the corporate container and the gateway controller. This ensures that data in transit is protected not just on the network, but also from other containers on the Neo device.

The user cannot change the rules used by the identification and access control service. The rules are created and controlled by the company in the case of company access, or created and controlled in the case of personal data.

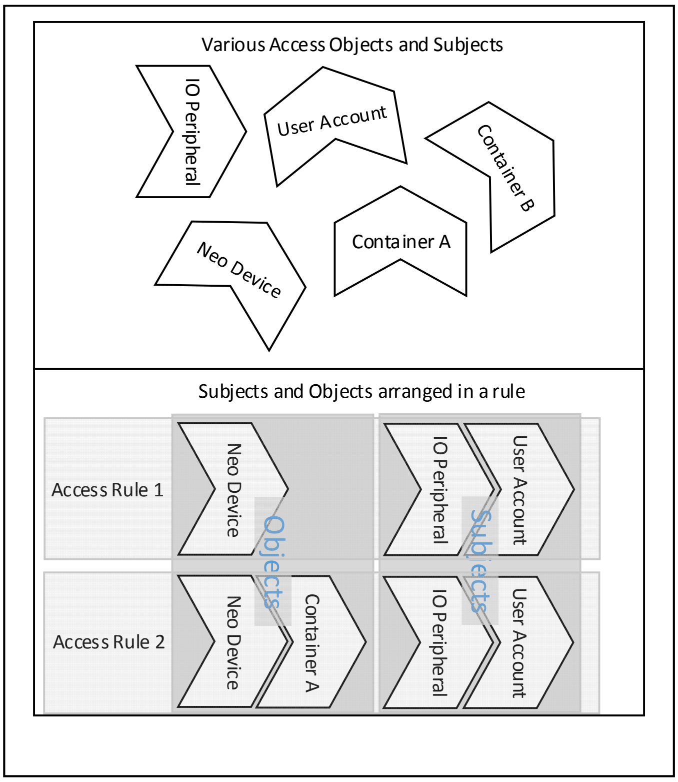

Figure. 3. Access control rules [6].

The SCP of the Neo Model ensures data and applications runs in isolated secure containers. The MAP ensures that whenever data gets accessed by I\O peripherals or company networks, that both the Neo device and the connecting I\O peripheral or network device are mutually authenticated and authorised.

The next section describes how the Neo Model ensures company control over company data and applications being accessed in a company network.

IV. Network Authorisation and Access Control

Computer devices normally access a company network either through a wired network or a wireless network. This section will first look at some of the more commonly used technologies that controls access to network infrastructure. The section will also look at the components described by the Neo Model that controls access to network resources for use by the Neo device

A. Existing technologies

This paper describes two sets of networking technologies, because many of the concepts that exists in these technologies are described in the Neo Model.

The Neo Model does not prescribe to use these technologies. Instead it makes use of the concepts describe in these technologies. The two network access technologies that are being described are:

- Remote Authentication Dial In User Service (RADIUS)
- Virtual Private Networks (VPN).

These two technologies are described in sections IV.A.1 and IV.A.2.

1) RADIUS Authentication

Authentication and authorization technologies such as RADIUS allow companies to control access to networked resources. RADIUS supports multiple authentication standards to authenticate users and it allows authorisation rules based on physical access points on the network [13]

RADIUS can be implemented by various vendors. In Linux, RADIUS is implemented as FreeRADIUS [14]. Microsoft implement RADIUS and called it Network Policy Server in Windows Server 2008 [15]. Microsoft implemented RADIUS with the following concepts [16]:

- Access client: This is the device that wants to gain access to the network.
- Access servers: This can be a wireless access point, network switch or VPN server. It is a device that an access client connects to in order for it to gain access to the network infrastructure. RADIUS clients register with a radius server to transfer access and authorisation requests.
- RADIUS server: The RADIUS server receives access and authorisation requests from radius clients and determine access using different access policies.
- Access policy: The access policy determines if the user can gain access using some type of rule checking and can also define certain requirements for the connection, if the connection is approved. The requirements can include whether encryption will be used or which IP addresses the clients can connect to.

It is important to note that RADIUS does not route network traffic through the RADIUS server. RADIUS only authenticate and authorise access.

With RADIUS, a wireless client does not only have to authenticate itself, but it can also provide information about the type of connection, the date and time, and many other attributes that is first evaluated on the RADIUS server before the client is allowed access to the network. This concept of evaluating and interrogating a client before a connection is allowed is also used in the Neo Model.

In Section. IV.B.1 the Neo Model describes the gateway controller that uses identification and authorisation techniques similar to RADIUS.

2) VPN Technologies

Another set of technologies that includes the access control and authorisation of clients to networks is in virtual private network (VPN) technologies. A VPN network can generally be defined as a private network that gets constructed over a public network infrastructure [17]

There are many different VPN implementations. Virtual private networks can be constructed using tunnelling and\or encryption [17].

Within a VPN implementation network traffic has to flow between at least two VPN nodes. These VPN nodes can be a VPN client and a VPN server. Before two nodes starts encrypting data, the VPN nodes must go through some type of identification and authorisation process, after which it allows network traffic between the two points [18].

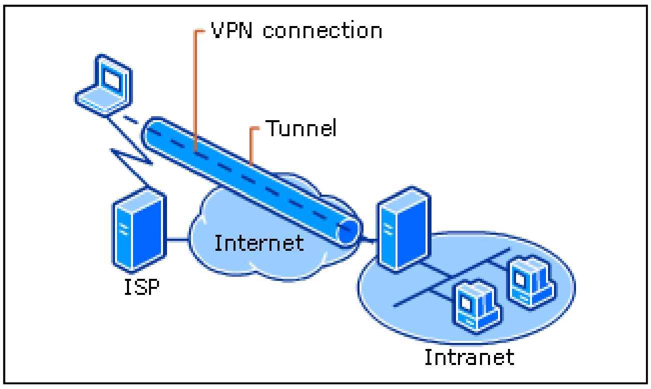

Figure. 4. The VPN connection to a corporate network [19]

Figure 4 describes a client that connects to the Internet through his Internet Service Provider (ISP). The client acts as a VPN node in a VPN and establishes a connection with a VPN server. The connection between the client and the VPN server is encrypted, ensuring confidentiality. The VPN connection that gets created connects the client to the company intranet.

VPN technologies rely on traffic that gets routed through the VPN nodes. This is different from RADIUS where the RADIUS server only authenticate and authorise. VPN technologies creates a connection between two nodes and it usually authenticate and authorise clients.

The routing principle and encryption principle in VPN technologies is used in the Neo Model.

Section IV.B.1. describes the gateway controller that acts like a VPN node into the corporate network for the Neo device.

RADIUS allows fine grain control over authentication and authorisation. VPN technologies ensure confidentiality of data in transit between two points. In the next sub section, the ability of the Neo Model to authenticate and authorise network access is described.

B. Network Access and Device Management in the Neo Model

It has already been explained that the Neo Model uses a black box device, called the Neo device. When connecting to a corporate network, Neo Model makes specific provisions for authorisation and authentication, as well as device management.

This section describes how the Neo Model authenticates and authorise access on a corporate network and then continues to describe the capabilities in managing device features while maintaining private data and applications.

1) Network access and authorisation

The Neo device uses secure containers to isolate personal and company data and applications. Access to the different secure containers are managed using the identification and authorisation service. It has also been described that any I\O peripheral and Neo device must be mutually identified and authorised.

In a corporate network, the Neo Model requires a component called a **gateway controller**. The gateway controller is part of the Neo Model and assumes the responsibility of managing access to the corporate network for Neo devices.

Figure 5 shows a Neo device that may or may not be using a docking station. Access to the corporate network is controlled through a gateway controller. The gateway controller has a list of access rules that defines access to specific resources on the corporate network. The gateway controller also establishes an encrypted session between the gateway controller and the corporate container. This ensures that data is confidential while in transit.

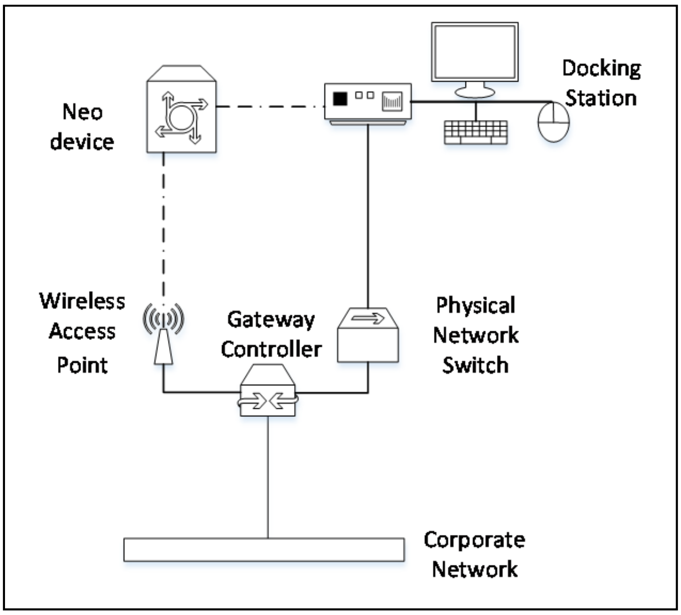

Figure. 5. The possible location of the gateway controller on a network.

The gateway controller has three classes of objects. They are:

- **Zones**: Zones are identified as a collection of resources. The resources are grouped together and managed as a zone. There can be many zones on a network depending on the company requirements. Network level access is controlled at a zone level. Application level access is controlled from within the application and the Neo model does not define any requirements or specifications for application level access control. The network administrator can decide what authorisation needs to happen before a user and device can gain access to a zone. There is one default zone that is always defined. This zone is the untrusted zone and is a catch all zone for any unauthenticated and unauthorised devices and users.
- **Resources**: Resources are different network resources made available to the Neo devices. Network resources can include a number of different classes of network resources. Defined resources only become available once they are defined as being available or blocked in a specific zone. Network resources can include, but is not limited to: IP address ranges, individual IP addresses, network protocols, TCP or UDP services, or general network services, which can be a combination of IP address, TCP or UDP services. It can also include network locations, which can be a combination of IP address ranges or special network locations like the Internet.
- **Policies**: Policies disable or enable specific features on the Neo device and allows fine grained control in a specific secure container. Policies are described in more detail in the Section IV.B.2.

Figure 6 shows a number of network resources. They include specific network areas, like the corporate LAN, specific servers, like the database, email and line of business server. It also contains the Internet object, which is a special network object that defines anything on the Internet. It can also include specific TCP protocol ports like TCP port 445 network traffic. These resources can now be grouped into specific zones, which is effectively just a group of network resources.

When a Neo device connects to a gateway controller, the Neo device and gateway controller goes through an initial identification and authorisation process. During this process a specific secure container for the zone gets created on the Neo device and the zone becomes the owner of the container.

Once the container is created the container gets encrypted on the Neo device so that it can only be decrypted when the Neo device connects to the gateway controller and requests access to the applicable zone. It also creates an encrypted channel between the secure container and the gateway controller. Because encryption happens on the secure container level even other containers in the Neo device cannot gain access to the network traffic between the container and the gateway controller. This feature has an added advantage that given the location of the gateway controller a Neo device can gain access to corporate resources from anywhere on the Internet.

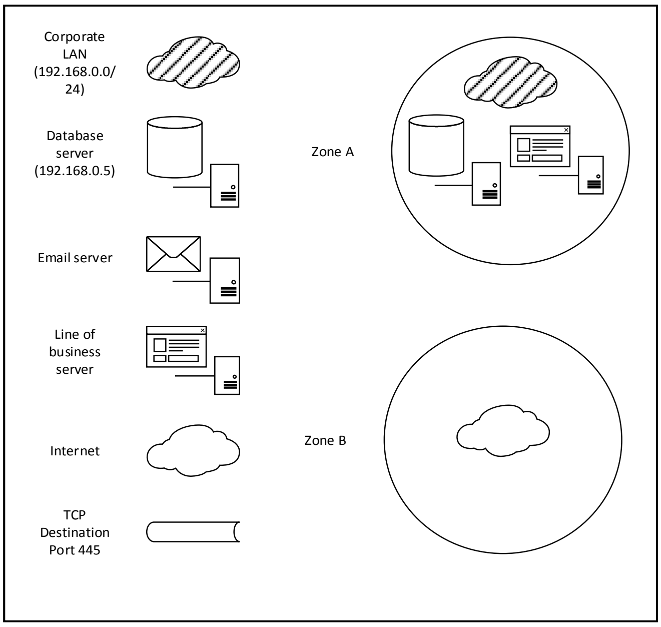

Figure. 6. Zones and zone resource allocation.

Before a Neo device can gain access to any corporate resources the Neo device must be enrolled as a resource on the gateway controller. This is explained in more detail in the next section.

2) Neo device management

The first time a Neo device is switched on in a corporate network, the Neo device identifies itself to the gateway controller.

If this is the first time the Neo device connects to the gateway controller, the controller creates the Neo device as a resource available to the gateway controller. The gateway controller automatically adds the Neo device to the untrusted zone. The untrusted zone is a special zone on the gateway controller which is a default setting that allows unauthenticated access. The network administrator can decide which resources are made available to the untrusted zone.

The network administrator also defines authorisation rules for a specific zone. This can include only username and password, or specifically defined username, Neo device and I\O peripheral combination.

Figure 7 explains the process where a Neo device connects to the corporate network the first time.

The first time a Neo device connects to the corporate network the Neo device locates the gateway controller. The Neo device registers as a resource in the gateway controller and is granted access to resources in the untrusted zone.

The user on the Neo device uses a touch screen I\O peripheral and initiates a request for access to network resources. The gateway controller responds to the Neo device with a list of zones available on the network.

The user on the Neo device requests access to a zone configured to only require a username and password. As soon as the user sends the requests to the gateway controller the gateway controller authenticates the request and receives information from the Neo device. The information provided by the Neo device is the identity information of the Neo device, the logged in user of the Neo device and the identity information of the I\O peripherals from where the request came from.

The gateway controller responds to the request from the Neo device with information of its own. It sends identity information about the gateway controller and the zone.

The Neo device determines whether a secure container for the zone already exists. If no secure container exists, a default container gets created for the zone. The Neo device and the gateway controller finalise the request by ensuring the access rules required gets created on both the Neo device and gateway controller.

After the access rules are created on both the Neo device and the gateway controller a policy for the zone gets applied to the Neo device.

The last step in the process is where the Neo device and the gateway controller establishes a secure channel and the Neo device encrypts the secure container.

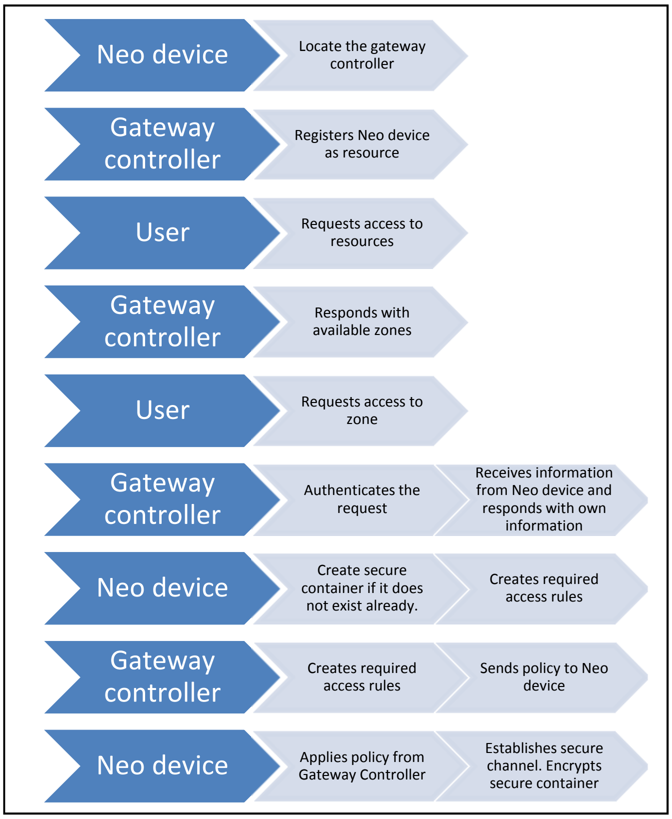
Neo device
Locate the gateway controller
Gateway controller
Registers Neo device as resource
User
Requests access to resources
Gateway controller
Responds with available zones
User
Requests access to zone
Gateway controller
Authenticates the request
Receives information from Neo device and responds with own information
Neo device
Create secure container if it does not exist already.
Creates required access rules
Gateway controller
Creates required access rules
Sends policy to Neo device
Neo device
Applies policy from Gateway Controller
Establishes secure channel. Encrypts secure container

Figure. 7. Establish a connection to a corporate network.

The policy can include multiple settings. Some of the settings that the policy can define are:

- **Exclusive use**: When exclusive use is enabled the container has exclusive use over the Neo device. This means that when the container is active, all the other containers suspends.
- **Device features**: The device features policy define which features of the Neo device is enabled when the container is active. By default only the basic input and output is allowed in a container. Other device features must be specifically allowed. This means that the camera must first be enabled access to the container before the camera can take pictures and store the photographs in the container.
- **Application policies**: The application policy can define which applications are available in the container and it can also control configuration of an application. This means that the policy can specify the email application to be available and can control which email server it can connect to and how often it synchronises. It is important to note that if one application is available in multiple containers, the data generated by the application is separate from the containers. This means that the emails received and created is only available in the secure container associated with the specific zone.
- **Offline use**: The offline use policy specifies if a container can be accessed even when a specific gateway controller is not available.

3) *Location aware management*

Gateway controllers can be made available to only specific areas of the network. That means that a company can have a wireless access point connected to a specific gateway controller servicing an area of the corporate network. Wireless signals can be isolated using specific building techniques, special paints or wallpapers or more complex triangulation systems [20] [21]

Consider the case of a boardroom where executives needs to discuss confidential and sensitive company information. The wireless access point servicing the boardroom is connected to a specific gateway controller.

The untrusted zone on the gateway controller gives access to nothing on the network. The network administrator defines a boardroom zone on the gateway controller. The network administrator creates a zone resource for a voting system as well as a storage area where recordings for meetings can be stored.

Access to the boardroom zone is controlled using authorisation rules, which includes predefined Neo device identities. This means that only pre-defined Neo devices can gain access to the boardroom zone.

As soon as the user enters the boardroom the Neo device connects to the gateway controller. The user initiates an access request if this is the first time the user uses the boardroom zone. The Neo device and gateway controller authenticates and the secure container for the boardroom zone gets created.

The network administrator defined the zone policy for exclusive use, with the microphone as a valid device feature, and does not enable offline use. Furthermore the sound recording app is made available to the boardroom container, as well as a specific voting application.

The boardroom container is only available while connected to the gateway controller because the policy disabling offline use is enabled. Furthermore, all other containers on the Neo device is suspended while the device is connected to the gateway controller for the boardroom. This ensures that the Neo device can only be used for sound recordings during the meeting and voting.

As soon as the user steps out of the boardroom the Neo device disconnects from the gateway controller and reconnects to the normal corporate gateway controller. The secure container for the boardroom suspends and stays suspended until the Neo device is reconnected to the boardroom gateway controller.

Location aware mobile management becomes a reality with the Neo model by using gateway controllers for specific wireless or wired locations on a corporate network.

V. Conclusion

Some corporations need to change the control over mobile devices depending on where they are located on the corporate network. The Neo Model allows the development of mobile device whose configuration can adapt depending on where the mobile device is located.

Special gateway controllers control access to network resources and control special features in the Neo device. This allows an administrator to lock down a mobile device in cases of high control and ensure only specific applications rights while the device is connected to different areas of the network.

The Neo model assures device owners and corporate entities separation of data and applications by using isolated secure containers.

The Neo model forms part of ongoing research for a PhD. and a prototype implementation will be an aspect of future research.

References

[1] B. M. Gaff, “BYOD? OMG!,” *Computer,* vol. 48, no. 2, pp. 10-11, February 2015.

[2] E. Demerouti, D. Derks, L. L. Brummelhuis and A. B. Bakker, “New Ways of Working: Impact on Working Conditions, Work–Family Balance, and Well-Being,” in *The Impact of ICT on Quality of Working Life*, C. Korunka and P. Hoonakker, Eds., Springer Netherlands, 2014, pp. 123-141.

[3] Northamptonshire Childminding Association, “Legal requirements for childminders,” 2015. [Online]. Available: http://www.childmindinguk.com/legal-requirements/. [Accessed 2 March 2015].

[4] United Kingdom, *Data Protection Act,* The National Archives, 1998.

[5] K. W. Miller, J. Voas and G. F. Hurlburt, “BYOD: Security and privacy considerations,” *IT Professional,* vol. 14, no. 5, pp. 53-55, 2012.

[6] J. du Toit and I. Ellefsen, “A Model for Secure Mobile Computing,” London, 2015.

[7] Y. Zhauniarovich, M. Conti, B. Crispo and E. Fernandes, “MOSES: Supporting and Enforcing Security Profiles on Smartphones,” *Dependable and Secure Computing, IEEE Transactions on,* vol. 11, no. 3, pp. 211-223, 11 May 2014.

[8] Enterproid, Inc., “Divide Web Site,” 2015. [Online]. Available: http://www.divide.com. [Accessed 24 March 2015].

[9] K. Barr, P. Bungale, S. Deasy, V. Gyuris, P. Hung, C. Newell, H. Tuch and B. Zoppis, “The VMware Mobile Virtualization Platform: Is That a Hypervisor in Your Pocket?,” *SIGOPS Oper. Syst. Rev.,* vol. 44, no. 4, pp. 124-135, 2010.

[10] Google, Inc., “Google for Work | Android,” 2015. [Online]. Available: https://www.google.com/work/android/. [Accessed 24 March 2015].

[11] Apple, Inc., “iOS Security Guide,” 2014. [Online]. Available: https://www.apple.com/business/docs/iOS_Security_Guide.pdf. [Accessed 24 March 2015].

[12] P. Garcia, T. Gomes, F. Salgado, J. Monteiro and A. Tavares, “Towards Hardware Embedded Virtualization Technology: Architectural Enhancements to an ARM SoC,” *SIGBED Rev.,* vol. 11, no. 2, pp. 45-47, September 2014.

[13] C. Rigney, S. Willens, Livinston, A. Rubens, Merit, W. Wimpson and Daydreamer, *Request for Comments: 2865,* Network Working Group, 2000.

[14] The FreeRADIUS Server Project and Contributors, “FreeRADIUS,” 2015. [Online]. Available: http://freeradius.org. [Accessed 9 July 2015].

[15] Microsoft, “Windows Server 2008 R2 and Windows Server 2008,” Microsoft, 2015. [Online]. Available: https://technet.microsoft.com/en-us/library/dd349801%28v=ws.10%29.aspx. [Accessed 25 March 2015].

[16] Microsoft , “RADIUS Servers,” Microsoft, 2015. [Online]. Available: https://technet.microsoft.com/en-us/library/cc755248(v=ws.10).aspx. [Accessed 25 March 2015].

[17] P. Ferguson and G. Huston, “What is a VPN? - Part I,” *The Internet Protocol Journal,* vol. 1, no. 1, pp. 2-19, June 1998.

[18] J. T. Harmening, “Virtual Private Networks,” in *Computer and Information Security,* 2nd ed., J. R. Vacca, Ed., Waltham, Elsevier Inc., 2013, pp. 855-867.

[19] Microsoft, “How VPN Works,” Microsoft, 28 March 2003. [Online]. Available: https://technet.microsoft.com/en-us/library/cc779919(v=ws.10).aspx. [Accessed 25 March 2015].

[20] G. Deak, K. Curran and J. Condell, “A survey of active and passive indoor localisation systems,” *Computer Communications,* vol. 35, no. 16, pp. 1939-1954, 2012.

[21] O. Smith, “Signal-blocking wallpaper stops Wi-Fi stealing (and comes in a snowflake pattern!),” CNN, 18 July 2012. [Online]. Available: http://edition.cnn.com/2012/07/18/tech/signal-blocking-wallpaper-stops-wi-fi-stealing-and-comes-in-a-snowflake-pattern/index.html. [Accessed 2015 March 2015].