International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Risk Scoring Algorithm for Endpoint Devices using Zero Trust

Fagbohunmi, Griffin Siji

Department of Computer Engineering Abia State University, Uturu, Abia State, Nigeria

ABSTRACT:

In recent times. There has been a tremendous increase in the use of computes outside the office premises due to COVID-19 outbreak. This scenario has led to the need for a design of a more secure endpoint protocol for the protection of a company's network. Some establishments now use the zero trust endpoint security options as opposed to the traditional network boundary solution. The design criteria of zero trust assumes every endpoint device connected to a company's backend to be untrustworthy. It is then required to run the zero trust heuristics on every endpoint device that intends to access a company's network to prove both its integrity and authenticity. The drawback of the zero trust security is its tough security measures which can erroneously label a risk-free device as error prone. This leads to the low availability of many endpoint devices in getting access to resources on the company's database when used with the zero trust protocol. In order to find a solution to this drawback, an error-scoring algorithm is proposed which aims at balancing the integrity and availability of endpoint devices by analysing the importance of the endpoint device query on the network resources sought in relation to the debilitating effect of it being denied. The following are the contributions made by this paper, (i) Give detailed breakdown of shortcomings in current risk scoring systems that employs zero trust, (ii) design an Improved relative importance metric that compares the risk in denying an endpoint device access to the sought after resources to the gain in denying it using the zero trust heuristics and (iii) proposing an algorithm for risk versus gain measurement using the relative importance metric embedded in zero trust to enhance the availability status of resources sought by the endpoint devices. In the results and analysis section it was shown that the relative importance metric proposed in this paper presents an improved analysis of risk, making it possible to make a more informed security decisions which ultimately led to improved availability of resources for authentic users. The overall aim of this paper is to help establishment make a more informed decision to endpoint device security especially in the face of increased use of endpoint devices at locations remote to the establishments.

Keywords: Zero trust; relative importance metric, scoring; risk score; security

Introduction

The need for working outside the premises of our working place has increased tremendously in recent times due to the COVID-19 outbreak all over the world. In the past, the network boundary security options was used to protect endpoint devices used at remote locations to industries from network threats. The concept of network boundary is based on the separation of endpoint devices used locally in the concerned industries from those used at the remote locations. The aim is normally to prevent access of remote endpoint devices suspected to having threats from crossing the boundary of the network to the devices within a company's premises. Here only remote endpoint devices that are trusted are allowed to have access to the internal network of the company. In this case the network administrator keeps track of all remote devices that can access the internal network. In recent times the number of endpoint devices used at remote location has drastically increased due to unforeseen circumstances as the spread of COVID-19 continues unabated, and especially with the various variants of the disease now common worldwide. This increase has exposed the weakness of remote software solutions in addressing the challenges posed by threats to the internal network of establishments. This coupled with the increase in the number of endpoint devices that can access the internet has made the problem even more challenging (Waizenegger et al 2022), (Green et al 2022), (Mandal and Jain 2023). In recent past, only a limited number of endpoint devices can access a local network, and this are normally monitored by the network administrators. However with the increase in the number of endpoint devices that can access a the network, it becomes increasingly impossible for network administrator to keep track of all remote access especially when such connection is ad-hoc.

The traditional network boundary protocol is limited in that it cannot prevent access of infected endpoint devices from accessing a company's network because only limited number of endpoint devices can be monitored by it. When this number is exceeded, the network security mechanism becomes powerless to adversarial systems intending to access the network. The shortcoming of the boundary network protocol led to the search of a more holistic secured protocol which can address this limitation. This brought about the introduction of the zero trust software to address the limitation of the network boundary security software. The idea behind the zero trust security solution is based on the fact that no endpoint devices is trusted until it passes the risk assessment checklist requirements embedded in the zero trust algorithm (Kindervag and Balaouras 2012), (Rose et al 2022), (Mehraj and Banday 2022). It must be emphasized here that these checks are performed regularly on every endpoint devices that intends to access the internal network. In other words risk assessment is carried out on all endpoint devices before they can access the local network. Access to the network is then based on the outcome of the risk assessment (Rose et al 2022), (Patil et al 2022).

The secured nature of zero trust is due to its certification of each and every endpoint devices that intends to access a company's network on a regular basis (Uehara 2023). The essence here is that since the same risk assessment criteria is performed on all the endpoint devices the local network is secured from adversarial endpoint devices, however the drawback here is that the stringent assessment criteria may lead to the unavailability of the network to some authentic endpoint devices. It should be stressed here that availability refers to the promptness to which an endpoint device has access to the resources on the network. The reduction in response time for a given endpoint devices in accessing a network's resources can lead to a downtime in the overall efficiency of the network. This situation can become precarious for real time systems which demands immediate response from a network. Also it is understandable that different categories of workers in an establishment are given different level of access rights to a company's network, so using the same scoring assessment criteria for all endpoint devices will be wasteful especially for those with limited access rights to the company's network resources. It therefore becomes pertinent that different scoring assessment criteria be used for different categories of workers so as to maximize the network resource utilization and the overall network throughput.

In order to increase both the confidentiality and availability of endpoint devices that access a company's network using the zero trust paradigm, the following approaches were used in this paper, (i) a relative importance metric is used for assessing the level of access right accorded different categories of workers in an establishment. Access right to a company's network resources are sometimes based on the category of staff, for example in a university, the staff attached to the vice-chancellor has a higher access right than those under the Deputy Vice-chancellor and progressively down to the staff under the Head of Departments (ii) a threat-scoring algorithm is proposed based on the User Experience Score System (UXSS) base metric. In this performance metric, the level of security for a given user is based on access rights of such individual, i.e. an individual with high access right will have a higher relative importance metric as compared to an individual with a lower access right. The essence here is to prevent individuals with lower access right from having unusual delay in accessing the required network resources. The User Experience Score System (UXSS) is a technique where values are assigned to endpoint devices based on a relative importance metric to the network resource being sought. User experience here refers to the satisfaction a user has when using a particular software, of course every user will want prompt response from the network, this is the overall aim of user experience. The relative importance metric is closely related to how vulnerable a device is to network threats.

The following are the contributions of this paper, (i) Analyse the shortcoming of the risk scoring system that employs the zero trust algorithm in companies. (ii) To formulate a relative importance metric for the various resources accessible to users in the company's local network that use the zero trust algorithm. (iii) To formulate a threat-scoring algorithm using the relative importance metric with the aim of increasing the availability of network's resources to endpoint devices with high access rights.

The rest of the paper is as described below, in section 2 the need for risk scoring for network systems that use zero trust algorithm is described together with current development in risk scoring. The section also discusses the UXSS, a platform that analyses how vulnerable an endpoint device is to network threats. In section 3, the relative importance metric which progressively measures the level of access right a user has in comparison to others is analysed. This is matched with the zero trust risk based design which uses the relative importance metric. Section 4 concludes the paper and offer future paths for research.

2. Review of Related Work

2.1 Zero Trust Algorithm Design

The concept of the zero trust security is based on the notion that no endpoint device is trusted in accessing the network resources, this is depicted in Figure 1. In this paradigm, all endpoint devices that request access to the network resources must be continuously verified. The zero trust algorithm consists of the following, (i) Policy Decision Point (PDP) and (ii) Policy reinforcement point (PRP). The PDP is responsible for determining the policy adopted by the company in accessing its network resources, while the PRP either permit or deny resource access based on the policy set by PDP. The implication here is that users request to the network resources that uses the zero trust policy are only permitted after being verified by the PDP and PRP (Rose et al 2022), (Uehara 2023).

From the aforementioned, it can be seen that the PDP can be likened to the central processor of the zero trust. The trust algorithm is responsible for either granting or denying a user's access to the network resources based on the company's policy. The trust algorithm describes a step by step procedure that determines whether or not access to the network resources will be granted. This procedure is shown in figure 2. Figure 2 comprises the following, (i) access request status which describes whether endpoint devices request access for network resources is granted or denied. This step is important in order assign threat score value to such request. If the threat score value is below a threshold value, the request is granted, otherwise the request is denied. (ii) history of database which describes the login of different endpoint devices to the network. (iii) asset database which describes the types of request that the network is bombarded with. (iv) policy requirement of the resources which describes the requirements set by the company before any network resource is accessed.

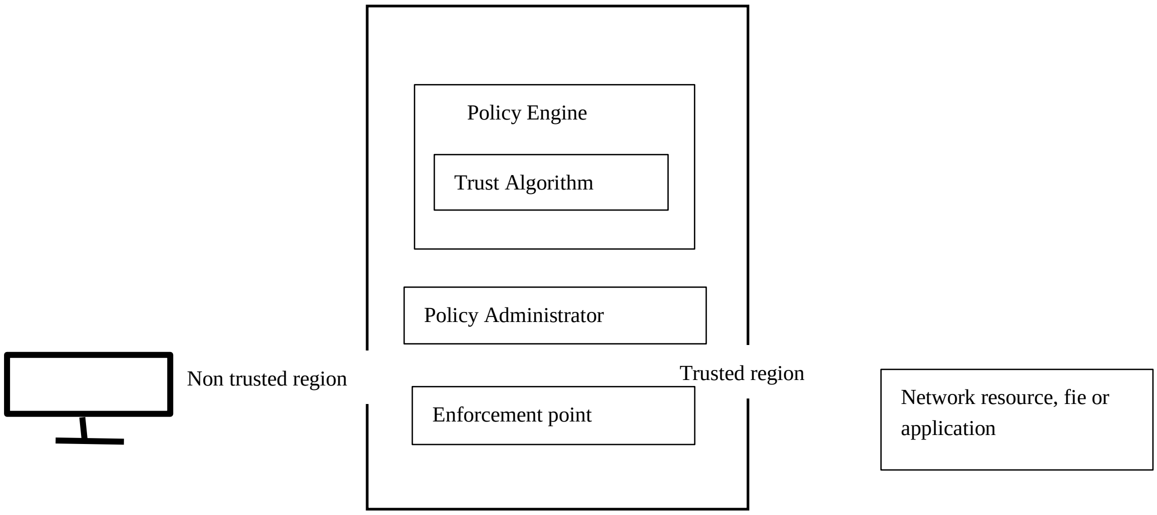

Figure 1. User access in Zero Trust

This also describes the requirement set for different categories of users to access a given network resource. (v) threat intelligence and logs which stores the source code of various network threats together with the login of endpoint devices captured for a given network threat. The connection between trust algorithm and threat scoring in zero trust is shown in figure 3.

Threat score is based on the security level of the device which also determines its access right. Whenever a user requires access to a network resource, the threat score analysis is performed on the device (Rose et□al 2022), (Kerman,2022), (Dimitrakos et al 2022). Zero trust threat score is based on the algorithm describing its implementation. A device is granted access to the network resource if its threat score is below a threshold value referred to as the limiting value. As said earlier, the same threat score analysis is performed on every endpoint device that request access to the network resources.

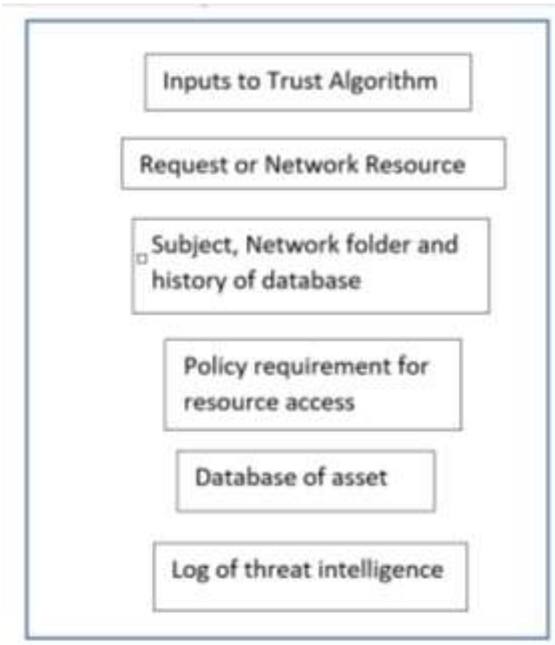
Inputs to Trust Algorithm
Request or Network Resource
Subject, Network folder and history of database
Policy requirement for resource access
Database of asset
Log of threat intelligence

Figure 2 Block diagram for Zero trust Algorithm

For example if an employee of a manufacturing company named Stephen request access to the company's network resources from a remote location, he will have to undergo threat score analysis designed for all users of the company. It is however important to note that, in the design of threat score analysis, adequate care must be taken to give a proper balance between security and availability (Rose et al 2022). To buttress this point, assuming the same high threat score analysis is performed on all users in a company, it will be observed that such analysis will only favour users whose devices are equipped with high level security functions, and it will increase security of network resources but it is at the expense of availability especially for those endpoint devices with a lower level security i.e. those devices with limited access to the network resources. On the other hand if a low threat score analysis is done, then all users will be granted access to the network resources. While this increases availability, it is highly detrimental to the network security.

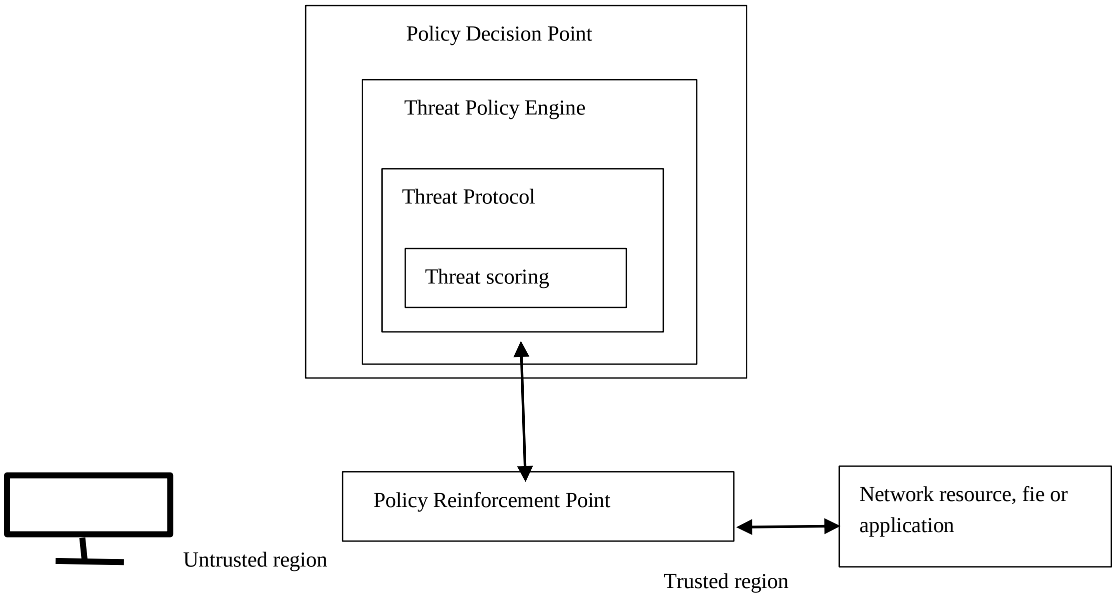

Figure 3 Zero trust risk scoring block diagram

3.1 Trends in Device Risk Scoring and User Experience Scoring System

Access to a network's resources is based on the trust algorithm which is done by comparing each device's access request with the asset database information that is set to its security level, this is referred to as the relative importance metric system. This means that the threat score analysis is performed relative to each endpoint device's security level, and is not uniform for all devices connected to the network. This is an advantage over the zero trust scoring procedure where the same threat score analysis is performed on all devices connected to the network.

The importance of the relative importance metric proposed in this paper is that each endpoint security configurations are analysed in order to design an appropriate evaluation standard for each device. In order to design an appropriate evaluation standard, the User Experience Security Standard (UXSS) is adopted. UXSS is designed to analyse the inherent security weakness in each endpoint device system settings. In this section, attempts will be made to describe the trends of threat-scoring in different establishments that have adopted zero trust system. Then the user experience security standard will then be explained.

3.2 Current Trends

The zero trust protocol was designed by Microsoft to be used within establishments. In its design, client's devices and its IDs will be managed and registered in Microsoft Intune (Conway 2022). Microsoft Intune is a management tool designed by Microsoft to give all in one solution and bring your own device (BYOD) embedded endpoint device management.

In this management system, Microsoft Secure Score does a threat scoring on endpoint devices that requires access to resources on the network. This it does by linking each device's request with Intune's policies and Microsoft Defender. These two functionalities combine to manage endpoint device security checks. The endpoint device's security state is denoted by the Microsoft Secure Score. This secure score is a function of the endpoint device configuration, user action and behaviour and other online actions which are measurable. The outcome of the Microsoft Secure score (which represents the endpoint device network resource access quotient) is determined using risk level classification (Brenduns 2022).

The Microsoft's Secure Score is an evaluation of several characteristics of the endpoint device's level of security that employs the zero trust protocol. The score also indicate the necessary security checks to be performed on a device before network resource access can be granted (Siosulli 2022), (Katzer 2020). It must be highlighted here that Microsoft Secure Score does not take user experience into cognizance. User experience can be defined as the overarching satisfaction a user derives from the use of a given software . A user whose endpoint device has a high security function must not be made to undergo the same stringent security criteria checks as those with low security functions.

In systems that use Microsoft zero trust system, a score of 9 is a perfect score which means that any endpoint device with such score will be granted multi-factor authentication check for network resource access. This of course imply that all systems underwent the same dynamic inspection check. In other words, the Microsoft zero trust system uses the same criteria checks for all systems connected to it.

Now for companies that employs Cisco zero trust system, it determines the value for the weaknesses in its systems. The scoring system in Cisco zero trust system is embedded in its software implementation. This makes it different from the Microsoft's zero trust system that analyses weakness in endpoint devices to determine its secure score. However in both Cisco and Microsoft version of zero trust system, their scoring is uniform for all system connected to it and do not factor in user experience (Samaniego and Deters 2020).

The shortcoming for companies that employs the zero trust system is that each company relies on the criteria set in zero trust system to allow access to the network resources and so, the companies has no control on how access is granted. In recent times, there has been renewed search for an optimum solution on how risk scoring can be performed on endpoint devices. These companies determine the secure score for its endpoint devices and are therefore best suited or their service delivery. However the shortcoming still remains that the same criteria is used is checking all systems connected to the network. The shortfall here is that such scoring criteria does not take into cognizance the different security configurations in each endpoint devices such as resource access permission and user experience.

3.3 System Scoring based on User Experience

In order to employ the use of endpoint threat scoring for network security, different companies can either define their individual protocol or use any of the standard threat scoring platforms. An example is the User Experience Scoring System (UXSS). In the UXSS threat scoring system, there are three classifications of metrics used in classifying weaknesses in endpoint devices. This includes (i) individual experience (ii) temporal and (iii) environmental (Scarfone and Mell 2015). The individual experience metrics is a measure of the endpoint system configuration and weaknesses in its default configuration. The weakness here refers to the limitations over the range of operations or network resources that can be accessed by each endpoint device. The temporal metrics is a measure of the projected level of decrease in threat resilience resulting from previous cycle of attack and other network conditions on the endpoint device. The environmental metrics is a measure of the endpoints interaction with the network configurations, this interaction in turn influences both the user experience and temporal metrics. The term environmental here refers to network system and its configuration settings.

It is compulsory to use the user experience metrics in the UXSS platform, while the remaining two metrics may be used if the need arises. However there exists limitations in the use of these two metrics in complex multi-user system architecture. In line with this action only describes the base metric (Scarfone and Mell 2015) , (Kasprzy and Stachurski 2019), (Torkura et al 2020).

4. Methodology

4.1 User Experience Metrics and Score in UXSS

This section describes the evaluation metrics (User Experience metrics) used in this paper. User Experience metrics analyses the weaknesses in endpoint devices based on their basic configuration security settings, while the user experience score use the analysis to determine the level of compromise such weakness can have on the device. UXSS base metric system is shown in figure 4. It should be noted here that the satisfaction enjoyed by a user is based on the security configuration settings of his endpoint device and the other two factors namely, temporal and environmental factors as explained in section 3.3. The level of compromise as determined by the user experience metrics shows how the security configuration of an endpoint device can be exploited and its consequences on the overall performance of the device. The metrics that show how the endpoint device can be compromised are (i) entry vector (EV), (ii) entry authentication (EA) and (iii) entry complexity (EC), while the influence metrics are (i) confidentiality influence (CI) (ii) integrity influence (II) and availability influence (AI). The Exploitation method (EM) is used in determining if the type of compromise on the device is active or passive. EM is used to decrease or lower the level of compromise a threat can have on a device and is not directly involved in threat scoring (Scarfone and Mell 2015). The value of the access vector metric is dependent on the location of the threat. AV can either be the current network, adjacent network or a neighbour device. Authentication refers to security checks carried out on an endpoint device before having access to the network resources and its value is an integer between 0 ---- n. Access complexity (AC) refers to the number of attempts an attacker will execute before it can compromise the network. It should be noted here that the number or value representing AC will be based on the level of compromise a threat will cause the network. AC can be high in which case the compromise will result in catastrophic damage to the network, medium in which case the compromise will damage devices in the same cluster or group of clusters or low in which case the compromise will only affect few endpoint devices in close proximity in the network. AC is normally set high for administrative privileges to the network, it is set to medium for user access permission to the network and set to low in every other cases.

In the case of the following (i) confidentiality influence (ii) integrity influence and (iii) availability influence their values can either be set to complete, partial or none depending on the level of a threat's impact on the network integrity, availability and confidentiality. The results gotten from all this performance metrics are combined to form a vector. The pseudocode in Figure 5 gives the equation used in computing UXSS base score (Scarfone and Mell 2015). This equation (figure 5), depicts the network security configuration and its level of vulnerability when all the performance metrics stated earlier are computed. The exact values of each performance metric is used to replace the constant values in the vector represented by in equation in figure 5. The values of the parameter vector in the equation are used to compute the impact, exploitability and h(impact) components. Finally the value of the base score will be between 0 and 10 (Scarfone and Mell 2015), (Wicaksana and Wira 2023), Yu et al 2023).

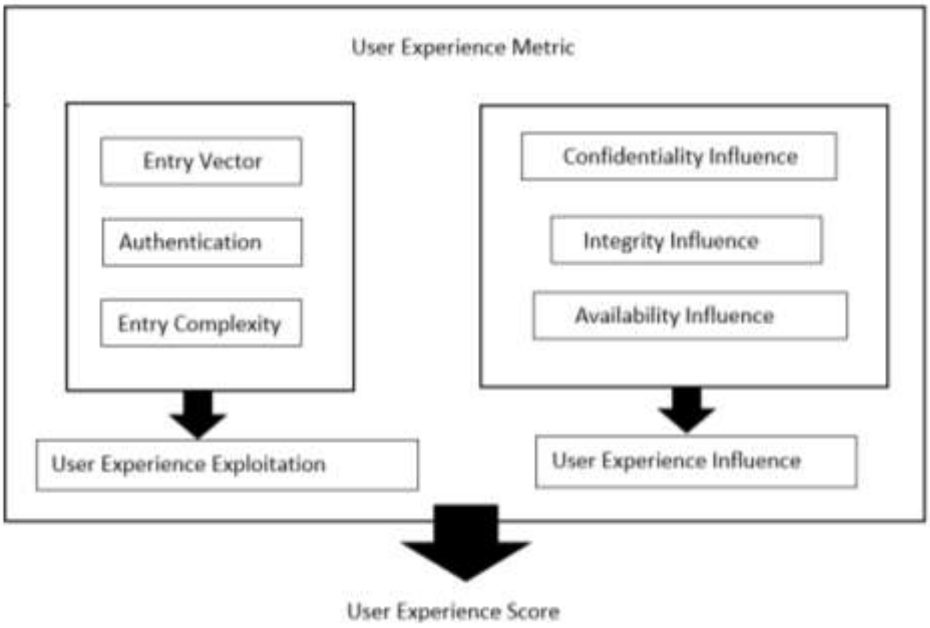

Figure 4 Components of User Experience (UXSS) Metrics

BaseScore = iter_to_1 _real(((0.65 × Impact) + (0.35 × Exploitability) − 1.7) ×

h (Impact))

Impact = 10.351 × (1 − (1 − Pro h Impact) × (1 – sum Impact) × (1 − pres Impact))

Exploit = 25 × Access Vector × Authentication × Access Complexity

h (Impact) = 0 if Impact = 0, 1.2 otherwise

AccessVector = case Access Vector of:

needs local access: 0.4

neighbour network accessible: 0.6

network avail: 1.0

Authentication = case Authentication of:

needs many occurrences of authentication: 0.4

needs one occurrence of authentication: 0.6

needs no authentication: 0.7

Access Complex = case Access Complex of

high: 0.3

medium: 0.7

low: 0.81

Con h Impact = case Confidentiality Impact of

none: 0.0

part: 0.3

full: 0.7

sum Impact = case Integrity Impact of

none: 0.0

part: 0.3

full: 0.7

Access Complexity = case Access Complexity of

none: 0.0

part: 0.3

full: 0.7

Figure 5 User Experience Score Equation

Figure 5 shows how to compute the UXSS base score in order to login automatically on a personal computer. From figure 5, AV is set to local as it can be accessed physically. AU has been set to none as additional authentication will not be required. The AC value was set to low as additional effort will not be needed to obtain the password since login was set .to automatic. Using these assumptions, the values for integrity impact, confidentiality impact, and availability impact can be obtained as partial. Now, expression for the vector components and the UXSS base value can be shown as “UX:L/DC:L/Bu:M/C:T/L:T/U:T”, Base Score: 4.5.

4.2 Relative Importance Scoring Metric

The risk scoring algorithm (for user experience metrics) uses the relative importance score metric uses the criteria described next for endpoint devices connected to a company’s network. The criteria involves the ratio of the relative importance to the risk involved in accessing a given network resource. For example, a user with a high level access permission to the network will pose higher threat than a user with a low access permission if wrongly granted access to the network’s resources. This is because a user with high access permission will have access to all the functionalities provided for in the network, while a user with a low access permission will have limited access to the functionalities of the network. In fact users with low access permission will only be granted access to basic requirements of the network (with low relative resource component index), and as such its relative importance to the risk involved will be high, whereas for the user with high access permission his relative importance to risk value will be low. The bottom line here is that more stringent tests will be done on users with high access permission before access can be granted. The relative importance score will be progressively made higher as it passes the security checks embedded in the relative importance score algorithm. On the other hand less stringent checks will be performed on users with low access permission such that the resource availability and confidentiality will be higher for them for less stringent conditions as compared to devices with high access permission.

The idea behind the relative importance metric scoring system is hinged on the fact that every company are expected to design its scoring algorithm to involve the functionalities of the endpoint devices used by them. This can be done by using the User Experience Score System (UXSS). In order to design the UXSS, two components are necessary, (i) the relative importance score metric which provides a measure of the ratio of the relative importance to the risk involved in accessing a given network resource, and (ii) an algorithm for risk scoring that is based on the relative importance metric.

The relative importance metric is made up of three components, (i) resources accessible to device, (ii) Access permission value and (iii) level of importance of resource. Weights are attached to each of this three components to determine the relative importance score metric for each endpoint device..

The next subsection will now deal with the procedure for the risk scoring using the relative importance metric. The risk scoring protocol is based on the User Experience Score System (UXSS). UXSS is a threat scoring paradigm that comprises of three types of metric (individual attributes, inherited features and external influence). The individual attributes refers to the individual weaknesses or vulnerabilities in each endpoint device, this is reflected in the access permission value for an endpoint device. The inherited features refers to those vulnerabilities resulting from the interaction of the endpoint devices with other devices on the network, this is shown by the inherited induced access permission (IIAP). The external influence measures the degradation resulting from the continuous use of an endpoint device in any given network setting, this is depicted with the device half-life value (DHV) It should be realized here that a device system capabilities is bound to reduce with time due to wear and tear of the system. This will invariably affect the systems overall performance and security levels with time.

As stated earlier, zero trust systems impose strict authentication checks on all endpoint devices before they are granted access to the network resources. The shortcoming is the same very strict authentication checks performed on all endpoint devices irrespective of their access permission value network. It is therefore the aim of this paper to propose different authentication checks based on device access permission value for companies interested in employing zero trust.

4.3 The Relative Importance Metric

In this section, the relative importance metric will be described. It is based on three parameters, (i) resources accessible to device, (ii) Access permission value and (iii) level of importance of resource. Weights are attached to each of this three components to determine the relative importance score metric for each endpoint device. The block diagram of the relative importance metric is shown in figure 6. As can be seen from the figure, it comprises of (i) resources accessible to device, which is a measure of the access permission granted an endpoint device to the network resources. This defines the class of network resources accessible to various categories of endpoint devices connected to the company’s network. (ii) Resource Access permission value

(RAP) which is a measures of a network resource access value. The higher this value, then the less the categories of endpoint devices that can access it. The value can be (i) high, for network resources with very high access value, i.e. network resource that is accessible to only staff in the VC's office in a university, (ii) Medium I i.e. network resources that are accessible to only staff in the DVC's and VC's office (iii) Medium II i.e. network resources that are accessible to only staff in the Dean, Directors, DVC's and VC's office. (iv) Medium III .i.e. network resources that are accessible to only staff in the HOD's Deans, Directors, DVC's and VC's office staff in HOD.s office and (V) low for other members of academic staff. A similar division is also made for those in the non-academic cadres. Therefore in a university two parallel systems for zero trust design with the relative importance metric will be implemented, one or academic staff and the other for non-academic staff. This template can also be extended to other companies. (iii) level of importance of resource, this describes the level of importance of a given network resource. For example some resources can only be accessible to users with high access permission. The relative importance metric is used together with the UXSS system to propose a robust endpoint security system.

It should also be stressed here that some aspects of network resources should only be made available to certain categories of staff, for example an employee in human resource department should not access network resources meant for those in the security department. This automatically shuts out certain adversarial threats possible with the zero trust system. This is because, it performs evaluation of classes of resources available to different categories of workers in the company. Secondly this component in the relative importance metric underscores the effect being able to attack a network resource. In summary the relative importance metric comprising of the three components stated earlier assigns weight to the confidentiality impact (CI), integrity impact (II) and the availability impact (AI) based on both the access permission values for every endpoint devices as well as the permission rights given to the network resource.

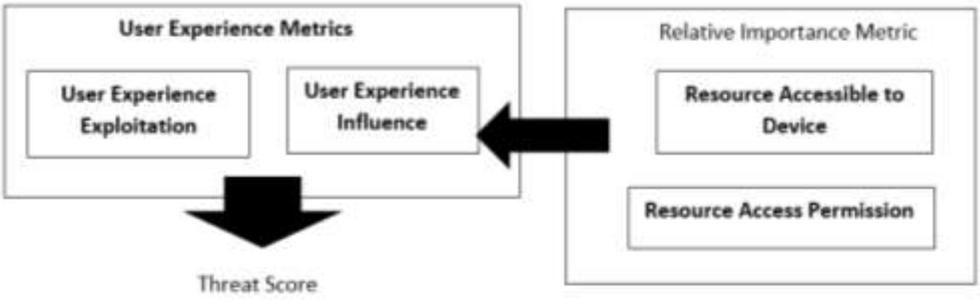
User Experience Metrics
User Experience Exploitation
User Experience Influence
Threat Score
Relative Importance Metric
Resource Accessible to Device
Resource Access Permission

Figure 6 Overview of Relative Importance Metric with User Experience Metrics

4.4 *Vector Diagram for Relative Importance Metric*

In this section, the flowchart for the generation of values for the relative importance metric is described. The flowchart for endpoint device request access for network resources is shown in figure 7, while the flowchart for Resource Importance is shown in figure 8. The relative importance metric vectors are added to the UXSS scores for the generation of the risk scoring algorithm. The components of the relative importance metric which are, (i) resources accessible to device, (ii) Access permission value and (iii) level of importance of resource are computed with respect to the access permission each endpoint device has on the confidentiality, integrity and availability of network resources. In the case of resources accessible to a device, the value of the metric is set to none, part or full by taking into cognizance the categories of network resources availability to different categories of company staff as well as if such staff have right to modify contents or information on the network. The flowchart for endpoint device request access for network resources is shown in figure

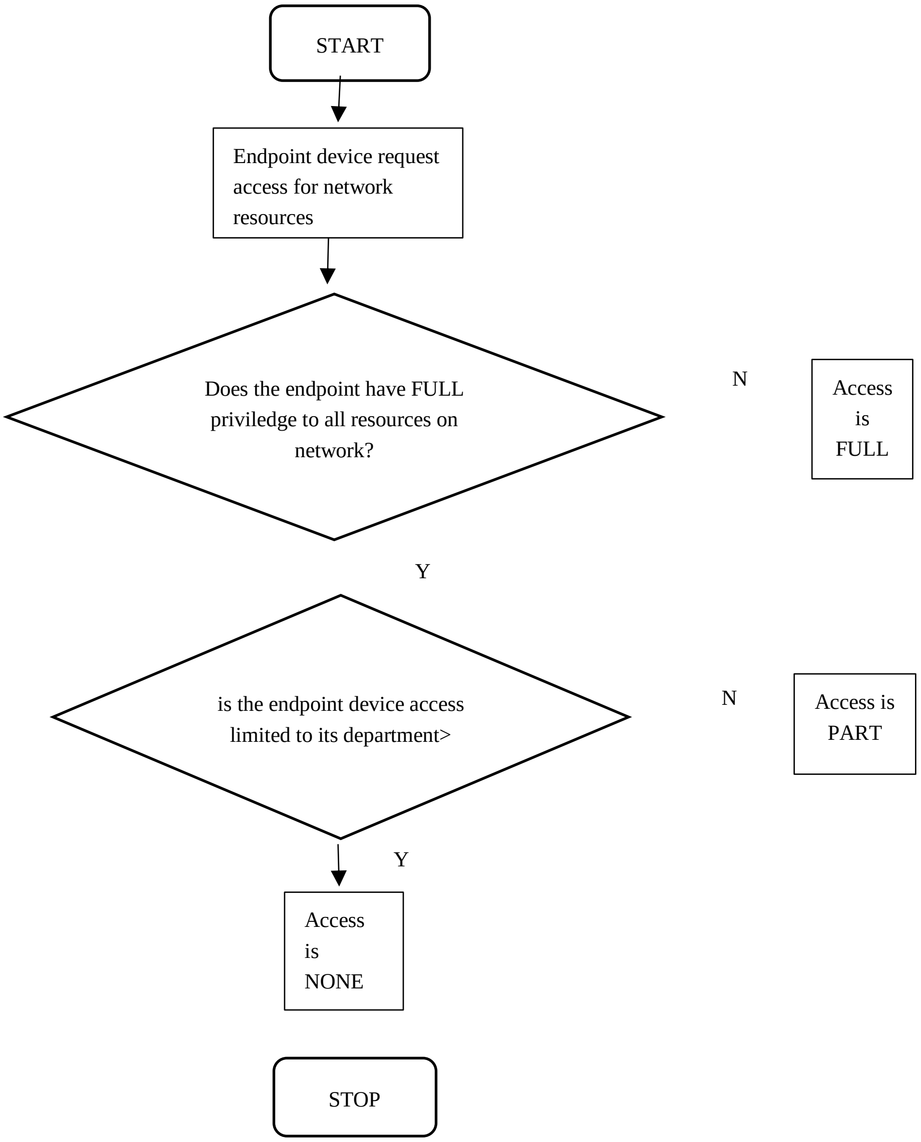
START
Endpoint device request access for network resources
Does the endpoint have FULL priviledge to all resources on network?
N
Access is FULL
Y
is the endpoint device access limited to its department>
N
Access is PART
Y
Access is NONE
STOP

Figure 7 Flowchart for endpoint device request access for network resources

One of the methods used in the deployment of relative importance vectors on endpoint devices used in a company's network is to separately define each user's access rights which is closely linked to their positions in the company. As said earlier the access right priority of a Vice Chancellor's staff in the university will be higher than those of Heads of Department. It is also important to note here that security weakness in a department network infrastructure within an institution will expose confidential information of the company's network. In the same vein security checks are embedded in the relative importance protocol to address cross-linking information across departments in an establishment.

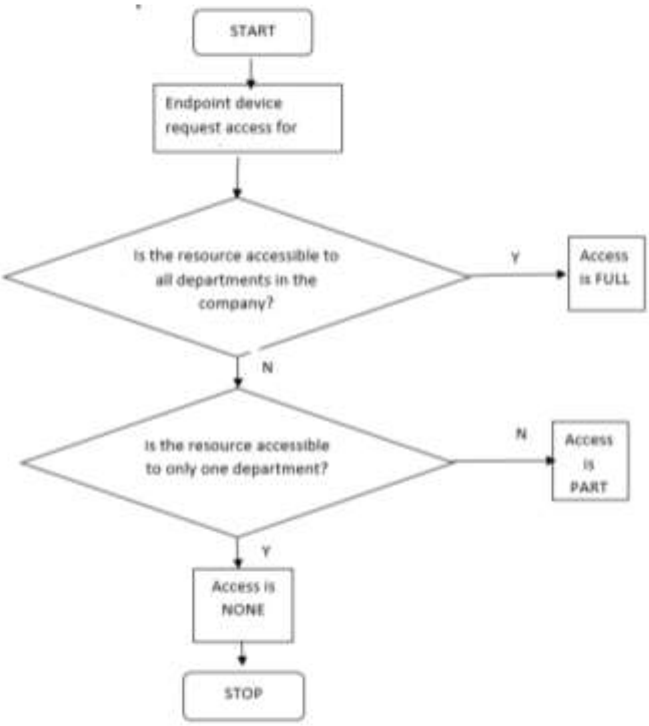
START
Endpoint device request access for
Is the resource accessible to all departments in the company?
Y
Access is FULL
N
Is the resource accessible to only one department?
N
Access is PART
Y
Access is NONE
STOP

Figure 8 Flowchart for Resource Importance

4.5 Algorithm for Device Risk Scoring in Zero Trust

The UXSS base scores will be combined with the zero trust threat scoring algorithm in this section. This will be achieved by applying the algorithm defined in figure 9 to the different security checks. The result of this comparison is shown in table 1. From figure 9, constants defining the relative importance metric are inserted as values of weight to base vectors in zero trust.

ThreatScore = roundoff_to 1_dec(((0.65 X Impact) + (0.35 X Exploit) – 1.6 X h(Impact))

Impact = 5.65 + RelativeImportance) X (- (- ConhImpact) X (1 – SummImpact) X (1 – PossImpact)

RelativeImportance = ReachableResource + ResourceRelevance

ReachableResource = case ReachableResource of

none: 0.0

part: 1.5

full: 3.0

ResourceRelevance = case ResourceRelevance of

none: 0.0

part: 1.5

full: 3.0

Figure 9 Threat scoring Algorithm

The technique for computing values using the threat scoring algorithm can be described as follows. For instance if a staff in the personnel department decides to access the network resources from his department, threat scoring in this scenario will be set to automatic. For this purpose an automatic login is enabled because the network resource is within the same department. When the threat scoring algorithm is applied, the UXSS vector will be defined as follows: UX: L / DC: L/Bu:M/C: T/L:T/U:T while the base score will be 4.8. The following values will be computed for two positions in an establishment using the relative importance threat scoring algorithm. For example a staff under the Head of Department in a university will have a score of none for reachable resource (RR), this is due to the fact that the staff has very limited access permission to the institution’s resource network. However the value for resource relevance (RE) is full as information within the same department is sought.

In the case of staff under a Vice Chancellor of a university, the value for reachable resource (RR) under the relative importance metric will be full. This is because the staff has a high access permission due to his full accessibility status. Such staff can access and modify contents of files on the network's resources. Also the value for the resource relevance (RE) will be full because the information sought is within his department.

Table 1. Sample table of threat scoring algorithm

Item	UXSS Vector	UXSS Base Score	Risk Score (RR:F/RE:R	Threat Score (RR:N/RE:N)
Auto login settings	UX:L/DC:L/Bu:M/C:T/L/T/U:T	4.8	4.8	2.3
USB AutoRum	UX:L/DC:L/Bu:M/C:S/L/S/U:S	7.5	7.5	3.5
Weak Password Setting	UX:L/DC:L/Bu:M/C:P/L/P/U:P	6.4	6.4	4.2
Installation of Antivirus	UX:L/DC:L/Bu:M/C:A/L/A/U:A	11	11	7.6

From the two examples illustrated above, the value or 'RR:N/RE:F/' was computed for the staff under the Head of Department in a university, while the value for a staff under the Vice Chancellor of the university was 'RR:F/RE:F/'. From the threat scoring equation shown in section 3.2 the value of the relative importance metric for the staff under the Head of Department was 3.5 points and the value for the staff under the Vice Chancellor was 4.8 points. In the second instance, the base score for UXSS when using the AutoRun device driver for USB can be computed as described below. The value for UX is local since the USB must be inserted physically. Bu was none and the DC was of minimal value since the USB will be detected automatically by the network operating system. This implies that a complete threat check will be performed on the USB to ascertain its confidentiality, integrity and Availability. The UXSS vector for the AutoRun check on the USB is 'UX:L/DC:L/Bu:M/C:S/L/S/U:S', the base score of 7.6 points was computed for this because the full complement of the threat analysis must be performed on the USB as a device rom external source is usually untrusted. It can be realized here that the relative importance metric was explained in two parts, the first RR:F/RE:F while the second was RR:F/RE:F. RR evaluates the reachable resource on the confidentiality, integrity and availability of network resources based on the access granted to the class of user in the establishment. The access rights are broken down into none, part and full. Resource relevance (RE) computes the confidentiality, integrity and availability based on the type of network resource being requested by the user and whether the department where the resource is being requested is within or outside to the user's department. The threat score given to this was none, part or full. For example, a resource requested by a user could be data that is in public domain. Public here refers to the act that such data can be accessed by all users in the company however different threat checks will be applied to the user's endpoint device depending on the access rights of such user. A resource being requested can also be a confidential data that is only open to only a section of users in the company. In his case users will low priority access permission to the network resource will have a score of none for such resource request. This means that different vectors from RR:F/RE:F to RR:N/RE:N could be used to represent the UXSS vector for USB AutoRun. The next paragraph explains the different vector used to describe the treat score using the relative importance score metric.

In the first instance, RR:F/RE:F represents confidential information that can only be accessed by users with high access right permission. In the second instance, RR:N/RE:N is used to represent public information or data that is open to access by all users of the establishment irrespective of their access right priority.

In the first instance described above, the threat score of 7.6 points was computed using the relative importance metric algorithm. This is because the vector represents users with high access right priority to the company's network resources and therefore the criteria for risk scoring needn't be relaxed. In the second instance, the value for the threat score was 4.2 points when the same algorithm was applied. The reason for the low threat score is because information (resources) that is open to all users in the company is being sought. Therefore the criteria for risk scoring was lowered so as to increase availability for users whose endpoint devices has low priority access score.

Table 1 shows the threat scores using the relative importance metric algorithm for selected secured configurations. From the table, it will be realized that installation of Antivirus on a network operating system will increase its resilience to adversarial attacks. This was evident in the comparably higher threat score of this configuration compared to other security configurations. It can also be noticed that the Auto login configuration has the weakest resilience to adversarial threats because it is assumed that such configuration is open to all class of users in the company. Therefore according to the relative importance metric algorithm, the criteria for the score was lowered to enable high availability to users with low priority access right.

5. Conclusion

Due to the increase in remote work necessitated by the surge in COVID 19, the use of endpoint devices by employees in accessing many company's network resources have increased. As a result of this, new security techniques must be used to reduce the shortcomings in the present security systems so as to safeguard the network resources as well as increase the availability to users in the network. The zero trust algorithm is used to better the current boundary security paradigm. A lot of companies make use of this zero trust algorithm for their company's network. The zero trust algorithm has proved in recent times to enhance the security status of a network and therefore resisting attempts by endpoint devices with adversarial threats compromising the company's network resources. In the zero trust algorithm, certain criteria were used to check the security status of every endpoint devices, (i.e. confidentiality, integrity and availability), that request access a company's network resources. In this paper, the relative importance metric algorithm was proposed. It has the ability of enhancing the availability status for users with low priority access score to the company's network resources, especially when such resource are open to all categories of users. In order words the same stringent access criteria used in checking the security of endpoint devices with high priority access score are not applied to those with low priority access score. This means that the same criteria are not applied to all endpoint devices accessing the network as is the case with the zero trust algorithm.

An analysis was carried out to compare the relative importance metric with the zero trust and the results show the shortcoming in the zero trust algorithm. Secondly, a relative importance metric was designed with different weights for different categories of network resources sought by users in the company. The algorithm uses threat scoring that is relative to the class of resource being sought as well as the access right priority of every endpoint devices to the company's network resources. Thirdly, different class of security configurations were also tested using the relative importance metric and the results show the advantages inherent in the relative importance metric. It is therefore recommended that the relative importance metric based threat scoring algorithm be used with the zero trust algorithm so as to increase availability to users with low priority access score. Overall this will help improve the security and availability of different categories of endpoint devices to the network resources as access will not be based solely on a device security configuration or access right to resources on the network. In the future, research will be carried out on a combination of user experience and user's expectation in a network setting. This will be used as a yard stick in computing individual endpoint device threat score using the relative importance metric.

Funding: Done by author

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The author declare no conflict of interest.

References

Albuali, A., Mengistu, T. and Che, D. (2022) ZTIMM: A zero-trust-based identity management model for volunteer cloud computing. In Proceedings of the Cloud Computing–CLOUD 2022: 15th International Conference, Held as Part of the Services Conference Federation, SCF 2022, Honolulu, HI, USA, Springer: Cham, Switzerland, pp. 287–294.

Conway, A. (2022) New Data from Microsoft Shows How the Pandemic Is Accelerating the Digital Transformation of Cyber-Security, Microsoft Security Blog—microsoft.com. Available online: https://www.microsoft.com/en-us/security/blog/microsoft-shows-pandemic-accelerating-transformation-cyber-security/ (accessed on 6 December 2022).

Dimitrakos, T., Dilshener, T., Kravtsov, A., La Marra, A., Martinelli, F.;,Rizos, A.; Rosetti, A. and Saracino, A. (2022) Trust aware continuous authorization for zero trust in consumer internet of things. In Proceedings of the 2022 IEEE 21st International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China, pp. 1801–1812.

Green, N, Tappin, D and Bentley, T. (2022) Working from home before, during and after the Covid-19 pandemic: Implications for workers and organisations. N. Z. J. Employ. Relations, Vol 45, pp 5–16.

Kasprzyk, R. and Stachurski, A. (2019) A concept of standard-based vulnerability management automation for IT systems. Comput. Sci. Math. Model, Vol 3, pp 33–38.

Katzer, M. (2020) Microsoft Secure Score. In Securing Office 365: Masterminding MDM and Compliance in the Cloud; Apress: California, MA, USA, Vol 2 pp. 97–156.

Kerman, A. (2022) Zero Trust Cybersecurity: 'Never Trust, Always Verify'. Available online: https://www.nist.gov/ blogs/taking-measure/zero-trust-cybersecurity-never-trust-always-verify (accessed on 6 December 2022).

Kindervag, J and Balaouras, S. (2012) No more chewy centers: Introducing the zero trust model of information security. Forrester Research. Vol 3. pp 234 - 245

Mandal, S. Khan, D.A and Jain, S. (2023) Cloud-based zero trust access control policy: An approach to support work-from-home driven by COVID-19 pandemic. New Generation. Computer. Vol 39, pp 599–622.

Mehraj, S. and Banday, M.T. (2022) Establishing a zero trust strategy in cloud computing environment. In Proceedings of the 2022 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, pp. 1–6.

Patil, A.P., Karkal, G., Wadhwa, J., Sawood, M. and Reddy, K.D. (2022) Design and implementation of a consensus algorithm to build zero trust model. In Proceedings of the 2020 IEEE 17th India Council International Conference (INDICON), New Delhi, India, pp. 1–5.

Rose, S.; Borchert, O., Mitchell, S. and Connelly, S. (2022) Zero Trust Architecture; Technical Report; National Institute of Standards and Technology: Washington, DC, USA,.

Samaniego, M. and Deters, R. (2020) Zero-Trust Hierarchical Management in IoT. In Proceedings of the 2020 IEEE International Congress on Internet of Things (ICIOT), San Francisco, CA, USA, pp. 88–95

Scarfone, K.and Mell, P. (2015) The Common Configuration Scoring System (CCSS): Metrics for Software Security Configuration Vulnerabilities; NIST Interagency Report; NIST: Gaithersburg, MD, USA.

Siosulli. Microsoft Secure Score—Learn.microsoft.com. Available online: https://learn.microsoft.com/en-us/microsoft-365/security/defender/microsoft-secure-score?view=o365-worldwide (accessed on 6 December 2022).

Torkura, K.A., Sukmana, M.I., Meinig, M., Kayem, A.V., Cheng, F.; Graupner, H. and Meinel, C. (2020) Securing cloud storage brokerage systems through threat models. In Proceedings of the 2020 IEEE 34th International Conference on Advanced Information Networking and Applications (AINA), Krakow, Poland, pp. 759–768.

Uehara, M. (2023) Zero Trust Security in the Mist Architecture. In Proceedings of the Complex, Intelligent and Software Intensive Systems: Proceedings of the 15th International Conference on Complex, Intelligent and Software Intensive Systems (CISIS-2023), Asan, Republic of Korea, Springer: Cham, Switzerland, pp. 185–194.

Waizenegger, L, McKenna, B, Cai, W and Bendz, T. (2022) An affordance perspective of team collaboration and enforced working from home during COVID-19. Eur. J. Inf. Syst. Vol 29, pp 429–442.

Wicaksana, A.and Wira, J.C. (2023) Security Analysis of Private Blockchain Implementation for Digital Diploma. International Journal on innovation in Computer and. Information Control, Vol 18, pp1601–1615.

Yu, X., Shu, Z., Li, Q. and Huang, J (2023) BC-BLPM: A multi-level security access control model based on blockchain technology. China Communication. Vol 18, pp110–135.