SECURITY ACCESS CONTROL EFFECTIVENESS DESIGN

D.P. Goncalves[1*]

ARTICLE INFO

Article details
Presented at the 2nd International Conference on Industrial Engineering, Systems Engineering and Engineering Management, held from 2 to 4 October 2023 in Somerset West, South Africa

Available online 17 Nov 2023

Contact details
* Corresponding author
dgoncalv@csir.co.za

Author affiliations
1 Council for Scientific and Industrial Research, Pretoria, South Africa

ORCID® identifiers
D.P. Goncalves
https://orcid.org/0000-0001-7401-9394

DOI
http://dx.doi.org//10.7166/34-3-2954

ABSTRACT

South Africa's infrastructure has faced a barrage of security attacks that has led to the promulgation of the Critical Infrastructure Protection Act (CIPA) No. 8 of 2019. Residual risk (i.e., that which remains after the threats have been mitigated) must be assessed for the critical infrastructure security system as part of the total security system design. One area that requires attention is access control. This paper demonstrates how to approach such a design, with a particular focus on the effectiveness of the access control system and how to choose the biometric or digital key (such as access cards) system. The approach starts by defining access control events that in turn are used to define access control effectiveness in respect of the probability of invalid access and of anomaly detection. The theoretically derived results are validated by a simulation. Based on these models, guidance is provided for the design of access control for critical infrastructure.

OPSOMMING

Suid-Afrika se infrastruktuur het 'n oormaat van sekuriteitsaanvalle in die gesig gestaar wat gelei het tot die promulgering van die Wet op die Beskerming van Kritieke Infrastruktuur No. 8 van 2019. Residuele risiko (d.i. dit wat oorbly nadat die bedreigings aangespreek is) moet beoordeel word vir die kritieke infrastruktuur sekuriteitstelsel as deel van die totale sekuriteitstelselontwerp. Een area wat aandag verg, is toegangsbeheer. Hierdie artikel demonstreer hoe om so 'n ontwerp te benader, met 'n spesifieke fokus op die doeltreffendheid van die toegangsbeheerstelsel en hoe om die biometriese of digitale sleutel (soos toegangskaarte) stelsel te kies. Die benadering begin deur toegangsbeheergebeurtenisse te definieer wat weer gebruik word om toegangsbeheerdoeltreffendheid te definieer ten opsigte van die waarskynlikheid van ongeldige toegang en van anomalie-opsporing. Die teoreties afgeleide resultate word bevestig deur 'n simulasie. Op grond van hierdie modelle word leiding verskaf vir die ontwerp van toegangsbeheer vir kritieke infrastruktuur.

1. INTRODUCTION

New risks to infrastructure in South Africa are emerging beyond vandalism, theft, and organised crime. Orchestrated and synchronised hybrid threats and non-traditional security threats are important trends [1, 2]. It is vital that South Africa develop proactive and preventive approaches and frameworks to counter these threats. This will require protecting critical infrastructure, protecting public health and food security, enhancing cyber security, targeting threat financing, and building resilience against radicalisation and violent extremism. One of the legal mechanisms is the implementation of the Critical Infrastructure Protection Act (CIPA), Act No. 8 of 2019. CIPA requires the evaluation of both strategic and threat risks. The design of security measures for critical infrastructure requires the evaluation of the threat risk and of the residual risk after mitigations have been applied [3].

A critical infrastructure (CI) security system will contain various elements, such as a perimeter fence with intrusion detection, access control, a security operations centre, and response teams. The interaction of these elements reduces the threat risk to CI. The security system may contain multiple nested levels of security. Mitigation is achieved by detecting and delaying the threat from achieving its intent until a response team arrives to interrupt or neutralise the threat actor. However, a response team can only respond in time if a threat is detected and the response team is notified of its presence and location. A CI security system's effectiveness is measured as the risk reduction resulting from the mitigation measures relative to the unmitigated threat risk [3].

The purpose of an access control system is to grant access, based on authentication (identity) and authorisation (permission), and to record access events in support of accountability and security investigations [4, 5][1]. Access is granted if the identified person has permission. For the purposes of this article, an access control system consists of biometric or digital key subsystem(s) that perform the authentication function and a permission subsystem that performs the authorisation function. A mantrap or vehicle trap gives physical access to a person or vehicle. The design of the access control architecture requires that an access control effectiveness model answer these questions:

a. What is the probability of undetected invalid access (whether biometric or digital key)? This is typically the result of a biometric error that grants people access to classified partitions for which they do not have permission and cannot be held accountable. This is the residual access control technology risk that remains and that needs to be qualified when used in CI.
b. What is the probability of detecting an access control anomaly? This is necessary to determine the residual risk of mitigation measures.

There are standards for biometrics used for authentication [6] that define measures of effectiveness for the biometric system that forms part of access control. However, there does not appear to be any work that considers access control effectiveness in respect of authentication effectiveness and authorisation parameters. One of the important reasons for an access control effectiveness model is to specify the biometric identification effectiveness and the digital key effectiveness when used with a permission rule in an access control system.

This effectiveness analysis addresses access control modelling limitations that arise in the interaction of identification and permission technologies. For each of these, a technology-specific attack is possible; this is not addressed here, but could lead to an increased probability of invalid access and a decreased probability of anomaly detection. Biometric attacks and their defences, for example, have been considered elsewhere [7, 8].

2. EVALUATING THE EFFECTIVENESS OF AUTHENTICATION AND AUTHORISATION FUNCTIONS

The access control effectiveness of the following are determined:

1. A biometric system with a permission rule;
2. Digital keys with a permission rule; and
3. A biometric and digital key with a permission rule.

2.1. Effectiveness of a biometric system with a permission rule

The effectiveness of a biometric system based on a structural biometric such as a face or fingerprints with a permission rule in a CI security system is considered for the purpose of designing the architecture of a security system and its specification.

'Invalid access' means that access is granted on the basis of an identity decision that does not match the presenting person's true identity. Invalid access cannot be detected by means of a biometric or digital key and a permission rule (although it might be detected by security investigations). This is important, because people who have been granted invalid access cannot be held accountable. The purpose of this analysis is

[1] In this article, 'authentication' and 'identity' are used interchangeably, as are 'authorisation' and 'permission'.

to determine the theoretical probability of invalid access for the design of access control systems from a security perspective.

Operational authentication may involve several biometric presentations by each person. The biometric authentication effectiveness is quantified in respect of both the false reject rate (FRR) and the false accept rate (FAR) of these transactions [6]. FRR is the proportion of incorrectly identified legitimate people (those with a registered biometric), while FAR is the proportion of people incorrectly identified as someone with a registered biometric but who are impostors. When FRR is low it is an annoyance but not a security risk. FAR is a security risk that is investigated further in this article. These error rates depend on the environment, the number of attempts (e.g., finger placements on the sensor), the sensor itself, the quality of the registration images, the number of fingerprints or irises invoked, and the user's experience with the process [6]. The use of two fingers or irises in all authentication transactions offers substantially improved performance over single-instance authentication.

This author departs from the view of Grother *et al*. that "FAR would be the proportion of impostors *incorrectly allowed access*" [this author's emphasis] [6, p. 40]. The proportion of impostors incorrectly allowed access would certainly be related to FAR, but linking identity and permission prevents a clear analysis. The relationship between the probability of invalid access and FAR will be derived once the possible access control events have been determined.

Suppose that N_{PP} people out of a total number of N_{PR} people registered[2] in the biometric system have access to an access-controlled partition, subject to $1 \leq N_{PP} \leq N_{PR}$ to avoid the case where no one has permission, but limited to those who are registered. Let α_i be the biometric system decision of person i's identity when presenting their biometric, and whose true identity is ω_i[3]. The biometric system makes an error when person i with identity ω_i is classified as α_j, where $j \neq i$. The permission rule for the partition where person i is presenting their identity is

$$\Phi(\omega_i) = \begin{cases} 0, & \text{where } \omega_i \text{ does not have permission and} \\ 1, & \text{where } \omega_i \text{ has permission.} \end{cases} \quad (1)$$

In practice, permission would be granted by management through a permit. When ω_i has permission to enter a partition, access is granted when $\Phi(\alpha_i) = 1$.

Using the proposed notation, the access events can now be defined as sets for the purpose of calculating the probabilities, based on whether permission has been granted to ω_i and on the permission decision for a biometric. The exhaustive set of combinations has been enumerated in Table 1, noting that when $\Phi(\omega_i) = x$ then $\Phi(\alpha_i) = x$ by definition, assuming that a permission attack is excluded. The key event for normal operations is valid access. From a security perspective, anomalies are events that require further investigation to conclude whether or not they are threats. Several anomalies are identified because of biometric errors: two cases of valid denial of access, valid denial of access with an incorrect identity decision, and *two cases of invalid access with an incorrect identity decision*. It is the last-mentioned that are of concern because they cannot be accounted for by access control.

These access control events are summarised as a Venn diagram in **Figure 1**, since this will be important for the probabilistic derivations and validation that follow. The access control events are the union of three mutually exclusive subsets: valid access, detectable anomalies, and invalid access. Access control anomalies consist of the union of detectable anomalies and invalid access, which is undetectable.

[2] 'Registered' means that the person's biometric has been captured in the biometric system. It does not imply that the person has permission to enter any access-controlled area, which is referred to as 'a partition'.

[3] Suppose that the true identity, ω_i, is Fred. When Fred presents a biometric, and the biometric system output is α_i – i.e., Fred – then it is correct. But if the answer is α_j – say, John – then it is incorrect.

Table 1: Definition of access events based on permission granted and the permission decision for a biometric

Permission granted to person i presenting?	Access decision using biometric identity estimate	Access event Key: Detectable anomaly Undetectable anomaly
$\Phi(\omega_i) = 0$	$\Phi(\alpha_i) = 0$	Valid denial of access
	$\Phi(\alpha_j) = 0, j \neq i$	Valid denial of access with an incorrect identity decision
	$\Phi(\alpha_j) = 1, j \neq i$	Invalid access with an incorrect identity decision
$\Phi(\omega_i) = 1$	$\Phi(\alpha_j) = 0, j \neq i$	Valid denial of access with an incorrect identity decision
	$\Phi(\alpha_j) = 1, j \neq i$	Invalid access with an incorrect identity decision
	$\Phi(\alpha_i) = 1$	Valid access

Figure 1: Venn diagram of the access control events following from Table 1

2.1.1. Determining the probability of invalid access for a biometric with a permission rule

An invalid access occurs when any registered person is mapped to one of the N_{PP} people who have permission via an incorrect biometric decision. Before proceeding to the main derivation, an intermediate result is derived that is used in the remainder of the article.

The identities ω_i and the decisions α_i are mutually exclusive for all i. The probability of decision α_i, given person i with identity ω_i, is $P(\alpha_i|\omega_i)$. The conditional probability $P(\alpha_j|\omega_i)$ is the probability of identifying person $j \neq i$ incorrectly. Using the probability axioms [9],

$$\sum_{j=1}^{N_{PP}} P(\alpha_j|\omega_i) = 1. \tag{2}$$

FAR is calculated only on the basis that person j is the incorrectly identified, without concern for which person it is out of the N_{PP} who are registered. From this, it follows that

$$P(\alpha_i|\omega_i) = 1 - \sum_{j=1, j\neq i}^{N_{PP}} P(\alpha_j|\omega_i) \approx 1 - FAR. \tag{3}$$

Invalid access is defined in **Table 1** as two events. The probability of invalid access for person i via decision α_j is

$$P_{IA} = \sum_{j=1, j\neq i}^{N_{PP}} [P(\Phi(\omega_i) = 0 \text{ and } \Phi(\alpha_j) = 1) + P(\Phi(\omega_i) = 1 \text{ and } \Phi(\alpha_j) = 1)]. \tag{4}$$

Assume that permission is granted to people independently, and that the biometric decision is independent of the management decision of granting permission; then

$$P_{IA} = \sum_{j=1, j\neq i}^{N_{PP}} [P(\Phi(\omega_i) = 0) + P(\Phi(\omega_i) = 1)] P(\Phi(\alpha_j) = 1) P(\alpha_j|\omega_i).$$

Since the events *person i has permission* and *person i does not have permission* represent the complete set, the probabilities sum to 1. Thus, since person i is excluded, the probability $P(\Phi(\alpha_j) = 1) = \frac{N_{PP}-1}{N_{PR}}$; and applying (3),

$$P_{IA} = \frac{N_{PP}-1}{N_{PR}} \sum_{j=1, j\neq i}^{N_{PP}} P(\alpha_j|\omega_i)$$

$$P_{IA} = \frac{N_{PP}-1}{N_{PR}} FAR. \quad (5)$$

The probability of invalid access is directly proportional to FAR. The P_{IA} is a maximum when the number of people with access to a partition approaches the number of registered people (**Figure 2**). The outer perimeter of a CI site will have many people with access, and inner partitions will have few people with access. A P_{IA} requirement would drive the selection of the appropriate biometric system, based on the outer perimeter probability of invalid access for a CI. For smaller interior partitions, P_{IA} would be lower, since there are fewer people with permission.

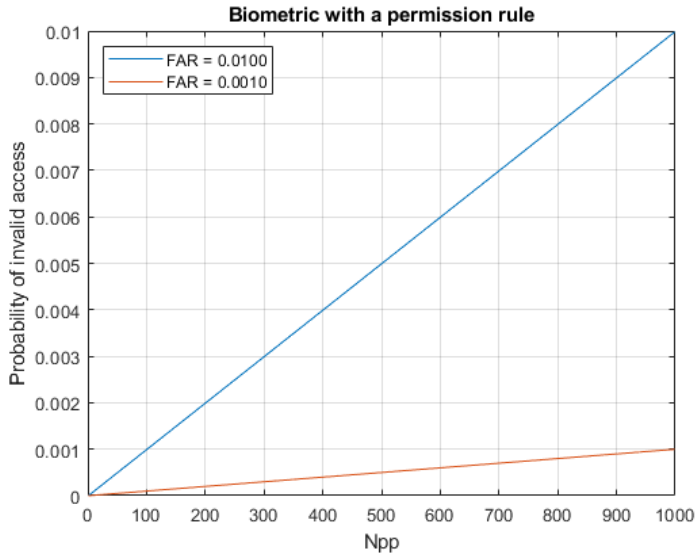

Figure 2: The probability of invalid access for a biometric with a permission rule ($N_{PR} = 1000$)

2.1.2. The probability of anomaly detection for a biometric with a permission rule

The next consideration is the probability of anomaly detection for a biometric system with a permission rule. Access control events (**Table 1**) represent a complete set – or, in other words, the sum of the probabilities of the individual access events is 1. However, not all of these events constitute an anomaly (refer to **Figure 1**). The set of anomalies contains all access events except for the valid access event. The probability of anomaly detection, given an anomaly, is calculated from the conditional probability of invalid access events, given an anomaly – i.e., P_{IA}/P_A – since invalid access events are the only undetectable anomalous events. Given that the probability of valid access is P_{VA}, the probability of an anomaly at an access control point is $P_A = 1 - P_{VA}$. Thus the probability of anomaly detection[4] is

$$P_{ADAC} = 1 - \frac{P_{IA}}{P_A} = 1 - \frac{P_{IA}}{1 - P_{VA}}. \quad (6)$$

P_{VA} is the probability that any one of the N_{PP} (out of a total of N_{PR}) people has permission, and a correct identity decision α_i is made. It is given by

[4] There are other ways of calculating the probability of anomaly detection, but this way has benefits for later sections, and it requires deriving the probability of valid access, which is itself a useful result.

$$P_{VA} = P(\Phi(\omega_i) = 1 \; and \; \Phi(\alpha_i) = 1). \tag{7}$$

Thus

$$P_{VA} = P(\Phi(\omega_i) = 1)P(\alpha_i|\omega_i) = \frac{N_{PP}}{N_{PR}}(1 - FAR). \tag{8}$$

Substituting (5) and (7) into (6),

$$P_{ADAC} = 1 - \frac{\frac{(N_{PP} - 1)}{N_{PR}} FAR}{1 - \frac{N_{PP}}{N_{PR}}(1 - FAR)}$$

and upon simplifying,

$$P_{ADAC} = 1 - \frac{(N_{PP} - 1)FAR}{N_{PR} - N_{PP}(1 - FAR)}. \tag{9}$$

The probability of valid access and the probability of an anomaly detection for a biometric with a permission rule with *FAR* = 0.001 is plotted in **Figure 3**.

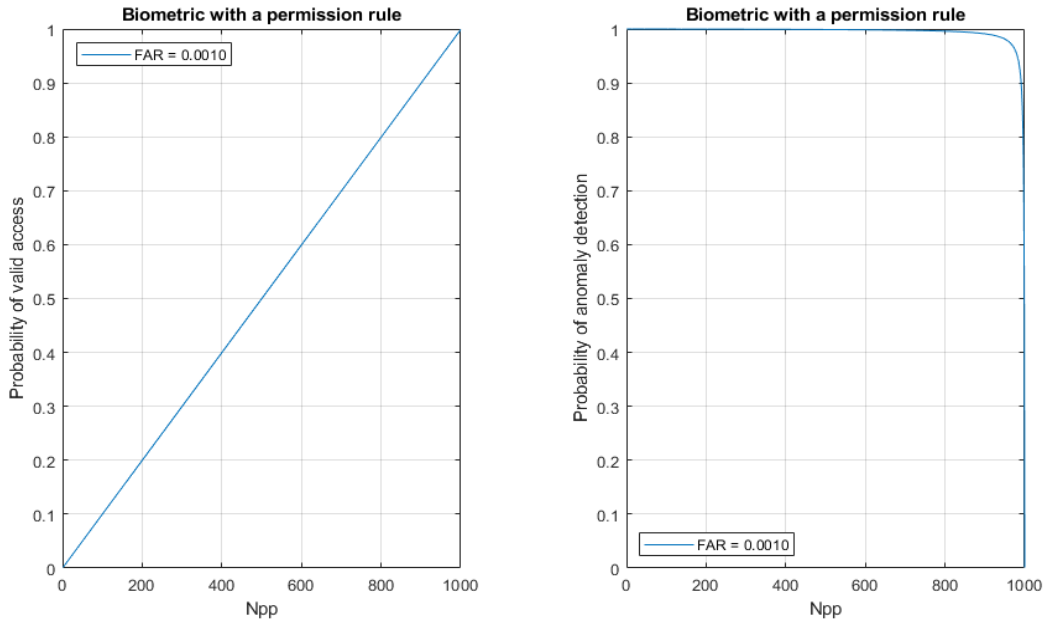

Figure 3: The probability of valid access and the probability of an anomaly detection for a biometric with a permission rule ($N_{PR} = 1000$)

Based on P_{VA} (8), the probability of valid access is directly proportional to N_{PP} with a maximum of 0.999, which is determined by $(1 - FAR)$. The probability of an anomaly detection moves from 1 at $N_{PP} = 1$, with a turning point at about N_{PP}=965 and approaching zero at N_{PP}=1000. For small partitions, anomalies are almost certain to be detected, decreasing to 91% for N_{PP}=990. This is because, as the proportion of people with permission increases, it leads to invalid access when a biometric error is made. Thus biometric identification with permission would not be suitable for partitions where the number of people with permission approaches the number of registered people.

2.2. Effectiveness of digital keys

A digital key, also referred to as 'a token', means any access card or mobile device-based system used for authentication in access control, and it may have static or dynamic codes. Static codes are not preferred for CI protection because they can be duplicated.

Let β_i be the digital key system deterministic mapping of identity when person i presents their digital key, and whose true identity is ω_i. The definition of access events, based on permission granted and the permission decision for a digital key, is the same as for a biometric, except that α_i and α_j are replaced by β_i and β_j respectively (**Table 1**).

Digital keys should have far more codes (1 000 times) than the number of people registered. Where this is not possible, codes must have a limited time validity and increase the number of codes in proportion to the time interval over which the digital key is valid. For CI use, digital keys may not be static with an infinite time validity. Digital keys can also be disabled if they are not used within a certain period. If the digital key identification is implemented on a mobile device, then it is recommended that a password or biometric identification is also implemented on the mobile device to reduce risk when stolen or lost.

2.2.1. Determining the probability of invalid access for a digital key with a permission rule

Digital keys depend on their being in the legitimate possession of a person, and are not fundamentally linked to identity. Digital keys can be lent to others, stolen, or lost. If the digital key is not in the possession of person i, then it is in illegitimate possession (IP) with a probability of P_{IP}. The probability of illegitimate possession is not a function of N_{PR} but of management and culture. With a digital key, the decision β_j is independent of who presents it; it could be the digital key of any of the N_{PR} registered people. The conditional probability of the decision β_j, given ω_i, is $P(\beta_j|\omega_i)$. Following similar reasoning as for the biometric (3),

$$P(\beta_i|\omega_i) = 1 - \sum_{j=1, j\neq i}^{N_{PP}} P(\beta_j|\omega_i) = 1 - P_{IP}. \tag{10}$$

The structure of the permission rule remains the same as when it is used with a biometric. The probability of invalid access with a digital key and a permission rule is

$$\begin{aligned} P_{IA} &= \sum_{j=1, j\neq i}^{N_{PP}} \left[P(\Phi(\omega_i) = 0 \text{ and } \Phi(\beta_j) = 1) + P(\Phi(\omega_i) = 1 \text{ and } \Phi(\beta_j) = 1)\right] \\ P_{IA} &= \sum_{j=1, j\neq i}^{N_{PP}} \left[[P(\Phi(\omega_i) = 0) + P(\Phi(\omega_i) = 1)]P(\Phi(\beta_j) = 1)\, P(\beta_j|\omega_i)\right]. \end{aligned} \tag{11}$$

Since the two events *person i has permission* and *person i does not have permission* represent the complete set, the probabilities sum to 1. Thus

$$P_{IA} = \sum_{j=1, j\neq i}^{N_{PP}} \left[P(\Phi(\alpha_j) = 1)\, P(\beta_j|\omega_i)\right] = \frac{N_{PP} - 1}{N_{PR}} P_{IP}. \tag{12}$$

The form of the probability of invalid access with a digital key is similar to that of a biometric with a permission rule.

2.2.2. Determining the probability of anomaly detection for a digital key with a permission rule

Following a similar approach to the biometric with a permission rule, all access events are considered anomalies except for the valid access event; this constitutes the full anomaly set (Table 1). Thus, given that the probability of valid access is P_{VA}, and on the assumption that invalid access is the only undetectable

event, the probability of anomaly detection is $P_{ADAC} = 1 - \frac{P_{IA}}{1-P_{VA}}$ from (6). To determine the probability of valid access, P_{VA} note that any one of the N_{PP} people with permission requires a correct identity decision β_i.

$$P_{VA} = P(\Phi(\omega_i) = 1 \; and \; \Phi(\beta_i) = 1) = P(\Phi(\omega_i) = 1)P(\beta_i|\omega_i). \tag{13}$$

Substituting (10) results in

$$P_{VA} = \frac{N_{PP}}{N_{PR}}(1 - P_{IP}), \tag{14}$$

Upon substituting (12) and (14) into (6),

$$P_{ADAC} = 1 - \frac{\frac{(N_{PP}-1)}{N_{PR}}P_{IP}}{1 - \frac{N_{PP}}{N_{PR}}(1 - P_{IP})}$$

and simplifying,

$$P_{ADAC} = 1 - \frac{(N_{PP}-1)P_{IP}}{N_{PR} - N_{PP}(1-P_{IP})}. \tag{15}$$

Since these equations have a similar form to those for biometric access with a permission rule, the same conclusions apply here.

2.3. Effectiveness of a combined biometric, digital key, and permission rule

To improve the detection of a biometric error or a digital key in illegitimate possession, the combination of the biometric, digital key, and permission is considered.

The **access rule** for person i is $(\alpha_i = \beta_i) \text{ and } \Phi(\alpha_i)$, based on matching the biometric and the digital key identifiers and permission. Anomaly detection is based on identity mismatches between biometric and digital key decisions, and on when permission is denied. The mismatch between the biometric and the digital key can happen in various ways, as shown in **Table 2**. The detectable anomalies can be used to investigate the illegitimate possession of digital keys or an incorrect biometric match.

There are two cases in which invalid access is granted on the basis of an incorrect biometric match *and* the illegitimate possession of a digital key (indicated by the all-red text in the cells of **Table 2**). **Table 2** also indicates that the number of access events is double that of either a biometric or a digital key individually.

Table 2: Access events for a biometric and a digital key with a permission rule

Permission granted to person i presenting?	**Permission decision based on biometric identity estimate**	**Digital key identity decision**	**Access event** Key: Detectable anomaly Undetectable anomaly
$\Phi(\omega_i) = 0$	$\Phi(\alpha_i) = 0$	β_i	Valid denial of access
		β_j	Valid denial of access Mismatched identifiers Illegitimate possession of digital key
	$\Phi(\alpha_j) = 0,$ $j \neq i$	β_i	Valid denial of access Mismatched identifiers Incorrect biometric match
		β_j	Valid denial of access Incorrect biometric match Illegitimate possession of digital key
	$\Phi(\alpha_j) = 1$	β_i	Valid denial of access Mismatched identifiers

			Incorrect biometric match
		β_j	Invalid access Incorrect biometric match Illegitimate possession of digital key
$\Phi(\omega_i) = 1$	$\Phi(\alpha_j) = 0$	β_i	Valid denial of access Mismatched identifiers Incorrect biometric match
		β_j	Valid denial of access Incorrect biometric match Illegitimate possession of digital key
	$\Phi(\alpha_j) = 1$	β_i	Valid denial of access Mismatched identifiers Incorrect biometric match
		β_j	Invalid access Incorrect biometric match Illegitimate possession of digital key
	$\Phi(\alpha_i) = 1$	β_i	Valid access
		β_j	Valid denial of access Mismatched identifiers Illegitimate possession of digital key

2.3.1. Determining the probability of invalid access for a biometric and a digital key with a permission rule

As indicated by the all-red cells in **Table 2**, there are two cases that meet the access rule but that cannot be detected in practice. The first is invalid access when person i who does not have permission – i.e., $\Phi(\omega_i) = 0$ – is given access because of an incorrect biometric decision α_j – i.e., $\Phi(\alpha_j) = 1$, $j \neq i$ – and, in addition, neither the biometric nor the digital key match the true identity, but $\alpha_j = \beta_j$. This case is significant from a security perspective because the person is granted invalid access, and the person's identity is recorded incorrectly, and they may be in illegitimate possession of a digital key. There is a second concern: when person i has permission – i.e. $\Phi(\omega_i) = 1$ – and is given access because of an incorrect biometric decision α_j – i.e., $\Phi(\alpha_j) = 1$ – and again $\alpha_j = \beta_j$. This case is different from the first because the person had permission, but the person's identity is recorded incorrectly and they may be in illegitimate possession of a digital key.

The probability of invalid access for person i via decisions α_j and β_j, of which there are $N_{PP} - 1$ people with permission, is

$$P_{IA} = P\left(\Phi(\omega_i) = 0 \text{ and } \Phi(\alpha_j) = 1 \; and \; (\alpha_j = \beta_j)\right) + P\left(\Phi(\omega_i) = 1 \text{ and } \Phi(\alpha_j) = 1 \; and \; (\alpha_j = \beta_j)\right). \quad (16)$$

The permission rule, the biometric (linked to physiological identity), and the digital key are independent decisions. Therefore,

$$P_{IA} = [P(\Phi(\omega_i) = 0) + P(\Phi(\omega_i) = 1)]P(\Phi(\alpha_j) = 1)P(\alpha_j = \beta_j)FAR\ P_{IP}.$$

Since the events *person i has permission* and *person i does not have permission* represent the complete set, the probabilities sum to 1. Once the decision α_j has been made, such that $\Phi(\alpha_j) = 1$, then $P(\alpha_j = \beta_j) = P(\beta_j) = \frac{1}{N_{PR}}$. Thus

$$P_{IA} = P(\Phi(\alpha_j) = 1)P(\alpha_j = \beta_j)FAR\ P_{IP} = \frac{N_{PP} - 1}{N_{PR}} \frac{1}{N_{PR}} FAR\ P_{IP}$$

which leads to

$$P_{IA} = \frac{N_{PP} - 1}{N_{PR}^2} FAR\ P_{IP}. \quad (17)$$

This result indicates that, for a well-designed biometric system with $FAR \ll 1$ and a well-managed digital key system with $P_{IP} \ll 1$ and with P_{IA} inversely proportional to the square of the number of registered people, the probability of invalid access is much smaller than with either a biometric or a digital key individually. Such a combined system is worth considering for partitions where a large proportion of people have permission, such as a CI outer perimeter.

2.3.2. Determining the probability of anomaly detection for a biometric and a digital key with a permission rule

Again, following a similar approach to the biometric with a permission rule, all access events are considered anomalies except for the valid access event, which then constitute the full anomaly set (**Table 2**). Thus, given that the probability of valid access is P_{VA}, and on the assumption that invalid access is the only undetectable event, the probability of anomaly detection is $P_{ADAC} = 1 - \frac{P_{IA}}{1-P_{VA}}$ from (6). The probability of valid access for a biometric and a digital key with a permission rule is

$$P_{VA} = P\big(\Phi(\omega_i) = 1 \; and \; (\alpha_i = \beta_i)\big) = P(\Phi(\omega_i) = 1)P(\alpha_i|\omega_i)P(\beta_i|\omega_i)$$
$$P_{VA} = \frac{N_{PP}}{N_{PR}}(1 - FAR)(1 - P_{IP}). \tag{18}$$

Thus, on substituting (17) and (18) into (6),

$$P_{ADAC} = 1 - \frac{\frac{N_{PP} - 1}{N_{PR}^2} FAR \; P_{IP}}{1 - \frac{N_{PP}}{N_{PR}}(1 - FAR)}$$

which simplifies to

$$P_{ADAC} = 1 - \frac{(N_{PP} - 1)FAR \; P_{IP}}{N_{PR}^2 - N_{PR}N_{PP}(1 - FAR)(1 - P_{IP})}. \tag{19}$$

Since both $FAR \ll 1$ and $P_{IP} \ll 1$, P_{ADAC} starts at 1, and practically remains 1 as the number of people with access to the partition approaches the number of registered people (**Figure 4**), which is a much higher value than for a biometric with a permission rule only (shown in **Figure 3**).

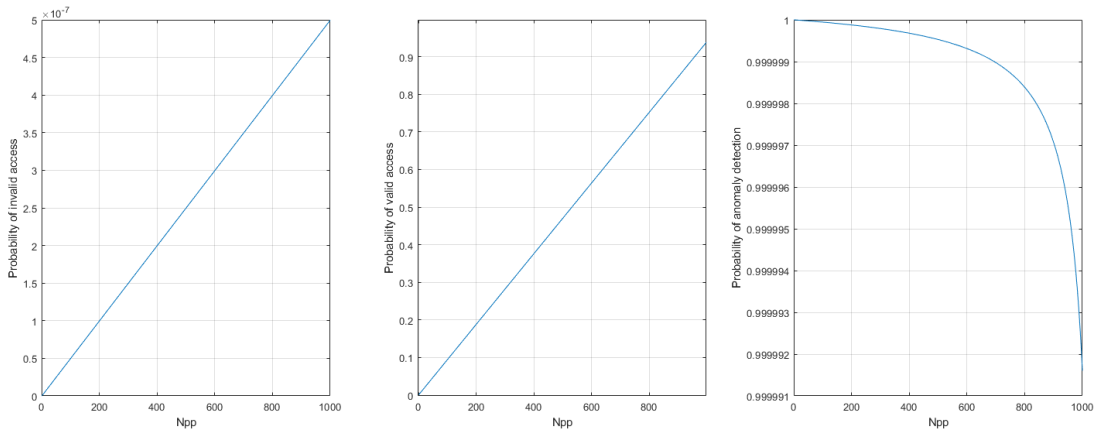

Figure 4: The performance of the combined biometric and digital key with permission

3. VALIDATION OF THE RESULTS

To validate the theoretical results derived earlier, a Monte Carlo simulation was constructed using Matlab to test the concepts and the derived expressions [9]. Three random variables were generated as three vectors: the first with true identities, the second with biometric identity containing errors generated at the biometric false acceptance rate, and a third with digital key identities, including illegitimate possession of P_{IP}. The permission rule was applied to the biometric and digital key vectors to determine access. The conditions constituting the access events of **Table 1** and **Table 2** were used to create statistics to confirm the derived expressions. On the basis that false rejection is an annoyance but not a risk, only access events arising from false acceptance were modelled.

For the combined biometric and digital key with permission, the probability of invalid access can be small, but the probability of valid access approaches 1. The form of equation (17), being the most demanding case, suggests that N should be chosen, such that $N > \frac{N_{PR}^2}{FAR\ P_{IP}}$. To avoid an unduly large N and the associated computational time, the following parameters were used: $FAR = 0.05$, $P_{IP} = 0.01$, and $N_{PR} = 100$, which makes $\frac{N_{PR}^2}{FAR\ P_{IP}} = 2 \times 10^7$. N was chosen to be 40 million. To formulate the hypothesis test, the three categories of access control events involving a biometric or digital key with a permission rule were repeated from **Figure 1**:

- Valid access;
- Invalid access because of an undetectable anomaly; and
- Valid denial of access because of a detectable access control anomaly.

To validate the probability of invalid access using a hypothesis test, the valid access and valid denial events were grouped so that there were effectively only two sets. For each trial the false acceptance rate (or probability of illegitimate possession) was the same; each of the two sets was independent across trials; and the number of trials, N, was fixed by the construction of the Monte Carlo simulation. These were Bernoulli trials with a binomial distribution [10]. Validating the probability of valid access followed the same process, except that sets 2 and 3 were grouped together, while validating the probability of anomaly detection required the *exclusion of valid access*.

The theoretical values of P_{IA}, P_{VA} and P_{ADAC} were tested against the corresponding simulation results using a two-sided binomial distribution test at a significance level of 5% [10]. The test results are presented in **Table 3** and **Table 4** for the two values of $N_{PP} = 10$ and $N_{PP} = 90$ respectively. **All of the results were statistically significant at the 5% level** – i.e., there was a 95% probability that the theoretical values would explain the simulation statistics.

Table 3: Theoretical vs estimated access control probabilities for biometric and digital key combinations with a permission rule[5] **($N_{PP} = 10$)**

	P_{IA}		P_{VA}		P_{ADAC}	
	Theoretical	**Estimated**	**Theoretical**	**Estimated**	**Theoretical**	**Estimated**
Biometric with permission	4.5000e-03	4.9693e-03	9.5000e-02	9.5108e-02	0.99503	0.99451
Digital key with permission	9.0000e-04	9.8980e-04	9.9000e-02	9.9069e-02	0.99900	0.99890
Biometric and digital key with permission	4.5000e-07	5.0000e-07	9.4050e-02	9.4165e-02	1.0000	1.0000

[5] To keep the tables compact, 'e' has been used to denote '10 to the power of' when writing numbers.

What can be seen from the two tables is that the simulation tracks the theoretical values across different values of N_{PP}. The combined identifier access outperforms either the biometric or the digital key on the probability of invalid access, but does worse than either the biometric or the digital key on the probability of valid access whose limit should approach N_{PP}/N_{PR}. This means that more attempts would be required for people with permission to access a partition. Although the biometric and digital key theoretical expressions had a similar form, different values of FAR and P_{IP} were chosen so these two should not be compared directly. This was one of the reasons for the large difference between the biometric and the digital key probability of anomaly detection. The other reason was the asymptotic fall-off of a single identifier. What is notable is that the combined identifier system had a better performance than either identifier individually, confirming the intuitive expectations.

Table 4: Theoretical vs estimated access control probabilities for biometric and digital key combinations with a permission rule ($N_{PP} = 90$)

	P_{IA}		P_{VA}		P_{ADAC}	
	Theoretical	**Estimated**	**Theoretical**	**Estimated**	**Theoretical**	**Estimated**
Biometric with permission	4.4500e-02	4.4536e-02	0.85500	0.85546	0.69310	0.69187
Digital key with permission	8.9000e-03	8.9201e-03	0.89100	0.89108	0.91835	0.91810
Biometric and digital key with permission	4.4500e-06	4.1500e-06	0.84645	0.84699	0.99997	0.99738

4. CONCLUSIONS, RECOMMENDATIONS AND FUTURE WORK

This work has defined all of the access control events for one- and two-factor authentication for the purpose of access control design. Invalid access, the result of identification errors, cannot be detected by access control alone. The expressions for biometric, digital key, and combined biometric and digital key with a permission rule have been derived and validated for:

- probability of invalid access;
- probability of valid access; and
- probability of anomaly detection.

Table 2 shows that a biometric and digital key combination with a permission rule leads to more possible access control events when compared with a biometric with a permission rule (Table 1). However, in the case of invalid access, the combined identifier case has a lower probability of occurrence. These probabilities are important for CI access control design, but cannot be easily measured. This article also provides a framework that can be extended to other cases, such as three-factor authentication.

For a CI enterprise with a $P_{IA} = 0.001$ and 10 000 access control transactions per year, that would mean that 10 people enter with invalid access. The risk profile of the enterprise partition would be required to determine whether this would be acceptable. Exploiting the invalid access vulnerability would require repeated access attempts, since invalid access has a low probability of occurring. Thus detecting many repeated access events that are denied should generate an additional anomaly.

The expressions derived above allow a design for CI security that is based on an effectiveness analysis that has not been possible until now. These models directly support the calculation of CI residual risk. The results indicate the importance that the number of authorised people who have access to a partition be kept small in comparison to the number of registered people when only a biometric or a digital key is used. Where this is not possible, and the secured resource can have separate partitions, more smaller partitions should be added. Alternatively, if this is not feasible, a second authentication factor should be added. This would also mean that certain biometrics may not be suitable for partitions with a large proportion of authorised people but where a low probability of invalid access is required (refer to Table 5).

In this analysis it has been assumed that all of the people were registered. The access control effectiveness with unregistered people has not been considered. However, unregistered people are likely to be visitors or suppliers who have different procedures for authorisation that do not require registration. This analysis has also focused only on the technical limits of identification and permission. The threat actor's modus operandi would influence the access control's effectiveness if vulnerabilities were not adequately mitigated; but that has not been considered in this article.

Table 5: The typical performance of various types of biometric system [11]

Biometric	*False rejection rate (FRR)*	*False acceptance rate (FAR)*
Hand	0.1%	0.1%
Fingerprint	< 1%	0.0001% to 0.00001%
Face	< 1%	0.1%
Iris scanning	0.00066%	0.00078%

Finally, developing multi-factor, multi-modal identification systems without understanding where the bottlenecks are is not productive. Identification systems need to be characterised and the threat's modus operandi understood so that a balanced security system can be designed.

REFERENCES

[1] D. P. Gonçalves and C. J. Serfontein, "Systemic approaches to critical infrastructure risk and security capabilities," *Proceedings of INCOSE SA*, pp.11-26, 2022.

[2] Cullen, P., Juola, C., Karagiannis, G., Kivisoo, K., Normark, M., Rácz, A., Schmid, J. and Schroefl, J., *The landscape of Hybrid Threats: A Conceptual Model* (Public Version), Giannopoulos, G., Smith, H. and Theocharidou, M. editor(s), EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-29819-9, doi:10.2760/44985, JRC123305.

[3] M. L. Garcia, *Design and evaluation of physical protection systems*, 2nd ed. Amsterdam: Elsevier, 2008.

[4] S. Harris, *CISSP exam guide*, 6th ed. New York: McGraw-Hill, 2013.

[5] V. C. Hu, D. Ferraiolo, and D. R. Kuhn, *Assessment of access control systems*, Gaithersburg, MD: National Institute of Standards and Technology Interagency Report, 2006.

[6] P. Grother, W. Salamon, and R. Chandramouli, "Biometric specifications for personal identity verification," *NIST Special Publication 800-76-2,* 2013.

[7] C. Roberts, "Biometric attack vectors and defences," *Computers & Security,* vol. 26, pp. 14–25, 2007.

[8] M. L. Garcia, *Vulnerability assessment of physical protection systems*, Amsterdam: Elsevier, 2005.

[9] M. Bonamente, *Statistics and analysis of scientific data* 2nd ed. Berlin: Springer, 2017.

[10] R. A. Johnson, I. Miller, and J. E. Freund, *Probability and statistics for engineers*, 9th ed. London: Pearson Education, 2018.

[11] D. Verma and S. Ojha, "Performance analysis of biometric systems: A security perspective," *International Journal of Advanced Research in Computer and Communication Engineering,* vol. 8, pp. 104-110, 2019.