NTNU

Norwegian University of
Science and Technology

Access Control in Critical Infrastructure Control Rooms using Continuous Authentication and Face Recognition

Kristian Dragerengen

Master in Information Security
Submission date: June 2018
Supervisor: Sokratis Katsikas, IIK

Norwegian University of Science and Technology
Department of Information Security and Communication Technology

NTNU

Norwegian University of
Science and Technology

Access Control in Critical Infrastructure Control Rooms using Continuous Authentication and Face Recognition

Kristian Dragerengen

01-06-2018

Master's Thesis
Master of Science in Information Security
30 ECTS
Department of Information Security and Communication Technology
Norwegian University of Science and Technology

Supervisor: Prof. Sokratis Katsikas

Preface

This master's thesis concludes two years of study in the field of Information Security (MIS) at the Norwegian University of Science and Technology in Gjøvik. This work was carried out during the spring semester of 2018. The topic for this project was proposed by Statkraft as a way to explore alternatives of authentication in control rooms. This thesis is intended for those with an interest in biometrics and authentication solutions.

Gjøvik, 01.06.2018

Kristian Dragerengen

Acknowledgment

I would like to thank Prof. Sokratis Katsikas as the supervisor. Thanks to Harald Hilde, Eivind Valhov and the Statkraft/Statnet project team. Thanks to Emil Volckmar Ry for feedback and thanks to my current employer Eika for allowing me to focus on this master's thesis.

K.D.

Abstract

Access control solutions in critical infrastructure control rooms do not support needs for availability and traceability. Most solutions rely on usernames and passwords that are used on multiple accounts on different systems. Workstations in control rooms need to be visible and available on a 24-7 basis, enabling operators to monitor the infrastructure and to initiate actions when needed. This is not possible today as logins, logouts and rebooting are a part of daily routines. This thesis presents a prototype of a solution that uses continuous authentication and face recognition for access control, that provides user friendliness, and ensures availability and traceability. At the same time, the solution provides for strict access control to ensure that only the right users are allowed in, and that systems are not left open to anyone. This is achieved by rethinking the architecture of how access control is done, by centralizing it through moving authentication from clients to a central server, and by using biometrics. The solution was tested using multiple virtual clients that receive commands from a server that runs continuously a face recognition application. The solution was tested for usability performing scenario tests and security by performing presentation attacks.

Contents

List of Figures

List of Tables

1 Introduction

Access control for critical infrastructure control rooms is not standardized and is handled in different ways. Over the past years, access control has not been prioritized at the workstations, but as physical access control, so workstations do not need a high level of security mechanisms. A control room is a locked area where personnel need multiple levels of access to enter; this is handled by physical access control to different security zones. A control room usually has one or several workstations where each workstation has multiple clients where operators monitor and control different processes linked to operations such as power, nuclear, chemical, wind and water. The most widely used form of access control is static authentication using username and password. There are several usernames and passwords depending on different systems and different levels of access on each system. This means that each operator has multiple credentials which may be hard to remember and can be shared with other operators even if this is not authorized. Periodic locking is also used to provide the operators to regularly authenticate themselves on the system. There exist policies for passwords based on requirements such as length and variations of passwords. The passwords have a defined lifetime and need to be changed at specific intervals. This means that each operator needs several different passwords for several different systems.

Availability and ready systems are crucial, but today's solutions with username and password do not provide this and are not suited for control room environments. Because of this, authentication mechanisms have been shifted to physical access control instead of focusing on logical access control at the workstation. Physical access control is often implemented by an access card. This opens up for social engineering and piggybacking which allows unauthorized personnel into the control room [8]. The biggest problem inside the control room is visibility; this is not taken into consideration when a workstation's clients are locked. Each workstation has multiple clients which are defined by the infrastructure it is monitoring and not by the operator using it. If the infrastructure is in normal operation there is no need for user-interaction and the operator can monitor the situation. But when values exceed thresholds there is need for user-interaction and accessibility is crucial. Accessibility is important in emergency situations where operators need to perform operations on multiple clients; this requires quick access and readily available systems. This is not possible with today's solutions due to locked clients which require a password to unlock, for each system. Important factors for access control are user friendliness, availability, traceability and strict access control. Current solutions address strict access control, but do not provide availability in an easy to use solution. Traceability is addressed based on the users; this is not a guarantee of who the operator behind an action is.

Critical infrastructure control rooms monitor and operate highly critical processes which need to be watched continuously. Locked screens prevent operators from monitoring and username/-password logins increase the time to access systems. This prevents an operator to execute actions during critical situations or it delays important actions. This can cause damage to the infrastructure, it can cause financial and operational loss for the company and it can affect other parties which depend on the company's operations. Tracing operators on the systems based on user-sessions is not a good solution for traceability based on operators who do not follow policy and use each other's accounts[9]. One operator can perform actions on one client where another operator is logged in. In a worst case scenario, an unauthorized person is able to steal an operator's access card, get access and perform actions on an already logged in system which does not detect unauthorized users. Frequently asking for passwords requires the operator's active participation, it may influence the ongoing activity, and is a disturbing element for the operator. Usernames and passwords are not suited for a control room with multiple systems. A control room will benefit from the automation of the authentication process which would move the job of authentication from the operators to the systems, thus freeing the operators. The research questions that this thesis addresses are as follows:

- Can biometrics be used for improved authentication in critical infrastructure control rooms?
    - Can biometric authentication by face recognition replace static authentication in a control room and at the same time increase availability for the operators and provide strict access control?
    - Can continuous authentication by face recognition be used to provide traceability?

This thesis provides effective authentication for operators which addresses availability as a critical factor. The solution is based on continuous authentication and face recognition, which automates access control at workstations. The contribution of this project is a prototype using state of the art face recognition to perform continuous authentication providing availability, traceability and strict access control in an easy-to-use solution. The solution performs authentication without user-interaction and transfers the process of authentication from humans to machines. The project also contributes to the sectors of critical infrastructure by rethinking how authentication is done in control rooms by representing a new architectural concept for authentication.

1.1 Keywords

Critical Infrastructure, Control Room, Access Control, Authentication, Biometrics, Face Recognition, Continuous Authentication

1.2 Definitions

- Control room: A room with restricted access equipped with one or several workstations used to control operations for a critical infrastructure.
- Workstation: A desk inside the control room with multiple computers and screens, which is monitored by an operator.
- Client: A computer with a connected screen at a workstation.
- Operator: The person which monitors operations at a workstation.

1.3 Thesis outline

- Chapter 2 provides background knowledge on biometrics, critical infrastructure and control room systems.
- Chapter 3 provides the state of the art on control room authentication, face recognition and continuous authentication.
- Chapter 4 presents the ground requirements for the prototype of this solution.
- Chapter 5 presents the architecture for the prototype of this solution.
- Chapter 6 describes the methodology and methods used for this thesis.
- Chapter 7 presents the results and the verification of the solution's prototype.
- Chapter 8 discusses the provided prototype with additional results.
- Chapter 9 concludes the thesis and offers directions for future work.

2 Background

2.1 Authentication

Identification and authentication is something we encounter every day in our lives when using online banking, credit cards, computers and our smart devices. Identification is the process of establishing or claiming an identity (one-to-many comparison). The process of authentication is to verify the claimed identity (one-to-one comparison); according to the biometric vocalbulary this is called verification[10]. There are different types of authentication, such as knowledge based, possession based and biometric based[11]. Figure 1 shows a login form as an example of knowledge based authentication; a smart card, which is an example of possession based authentication; and a representation of a fingerprint, as an example of biometric based authentication. Static authentication is referred to as verification of an claimed identity in the start of a session to gain access[12], this can be a login using password, fingerprint or iris scan.

- Knowledge based: something you know
- Possession based: something you have
- Biometric based: something you are or do

Figure 1: Different types of authentication

2.1.1 Knowledge based

Knowledge based authentication is widely used over the Internet to access accounts, by logging into a phone or a computer. It is also used for credit card payments in terminals by using a PIN-code. The most known form is the password.

Passwords

Passwords are used in many ways to protect data and are used for authentication. There are different forms of passwords, such as a personal identification number (PIN) which is mostly known and used in addition to a card. The word "password" is mostly associated with a passphrase which can be easy to remember, easy to use and works very well if used correctly. The downside is that many different services require a password and people tend to register for multiple services; this leads to multiple passwords. To remember multiple passwords, the quality often decreases or the same passwords are reused; this is often what people do so they will not need to request a new password every time they log into a service because the old password was forgotten. Passwords are alphanumerical phrases and policy often follows best practices, which says passwords should not contain only numbers, lowercase letters, uppercase letters, special characters or personal information, but rather contain a combination of those. They should not be shorter than 8 characters and should not be already used somewhere else. They should not contain dictionary words even when some letters are changed to capitals, numbers or special characters. Avoid reversing of words, adding simple conjugations or using keyboard phrases. A good password can be easy to create, but also hard to remember. Policies usually include several of these best practices to ensure the quality of passwords, but when the users needs to remember several of policy-based passwords, they are easy to take shortcuts[13].

2.1.2 Possession based

Possession based authentication relies on a physical item which can be used to claim access. The most known form of possession based authentication is the key we use to open doors. Other forms of possession based authentication are smart cards. These items are hard to replicate, but expensive to produce, and is not directly connected to a user; this means it can be used by several people.

2.1.3 Biometrics

Biometrics have recently gained popularity and have become part of our daily lives. Biometrics are defined as "automated recognition of individuals based on their behavioral and biological characteristics" [10] where behavioral has to do with some function of the body and biological is about some structure of the body. A biometric modality is evaluated by following the biometric properties[1]:

- Universality: Every person shall have a biometric characteristic.
- Distinctiveness (Uniqueness): Different people shall have different biometric characteristics.
- Performance: Shall be accurate.
- Permanence: The characteristic shall be sufficiently invariant over a period of time.
- Collectability: The characteristic shall be easy to collect.
- Acceptability: How people are willing to use the biometric character.
- Circumvention (Security): Shall not be easy to mimic or easy to spoof.

Biometrics is not as straight forward as a knowledge- or possession-based authentication, whose verdict is either "true" or "false". Biometrics-based verdict is neither "true" nor "false"; it is rather decided based on whether it is "true" or "false" enough, where the tipping-point is called a threshold.

An attempt to gain access needs a score above the threshold, whereas a score below threshold will result in denying access. Since measures are never 100% correct, it is possible to have false positives i.e. when an impostor is granted access; these are measured by the False Match Rate (FMR). False negatives occur when a genuine user is denied access; these are measured by the False Non-Match Rate (FNMR). FNMR and FMR are measures for the comparison algorithm in a biometric system, often reported as Equal Error Rate (EER).

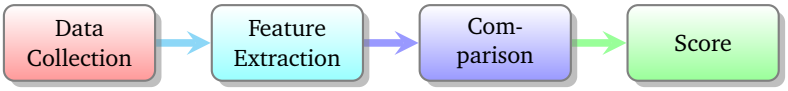


Figure 2: Biometric processing pipeline

- FMR is defined as the set of all impostor scores above threshold divided by all impostor scores in total.
- FNMR is equal to $1 - GMR$. The Genuine Match Rate (GMR) is defined as the set of all genuine scores above threshold divided by all genuine scores in total.

For operational testing of a biometric system, False Acceptance Rate (FAR) and False Reject Rate (FRR) are used. Operational testing gives scores based on the whole biometric processing pipeline (Figure 2). Failure to Capture (FTC) is used on data collection and Failure-to-Extract (FTX) is used for feature extraction. The combination of those is Failure-to-Acquire (FTA).

- $FAR = FMR * (1 - FTA)$
- $FRR = FTA + FNMR * (1 - FTA)$
- $FTA = FTC + FTX * (1 - FTC)$
- $FTC = \frac{N_{tca}+N_{nsq}}{N_{tot}}$ where N_{tca} is the number of terminated capture events, N_{nsq} is the number of images created with insufficient sample quality and N_{tot} is the total number of capture attempts.
- $FTX = \frac{N_{ngt}}{N_{tsub}}$ where N_{ngt} is the number of cases where no template was generated and N_{sub} is the total number of biometric samples being submitted to feature extraction.

Other metrics are the Average Number of Impostor Actions (ANIA) and the Average Number of Genuine Actions (ANGA)[14, 15]; which are used for behavioral biometrics such as keystroke- and mouse dynamics. ANIA and ANGA are used as metrics for continuous authentication (CA) and were developed since FMR and FNMR are not suited to a CA system. In a CA system it is more important to know when an impostor is detected. ANIA and ANGA measure how many actions can be performed before an impostor posing as a genuine user is detected. We want ANIA to be as low as possible and ANGA as high as possible.

Biometrics performs a comparison between a reference and a probe where the reference is one or more templates, samples or models attributed to a biometric data subject. The probe is a sample or feature. Comparison is the process of estimation, calculation or measuring similarity or dissimilarity between reference(s) and probe(s)[10].

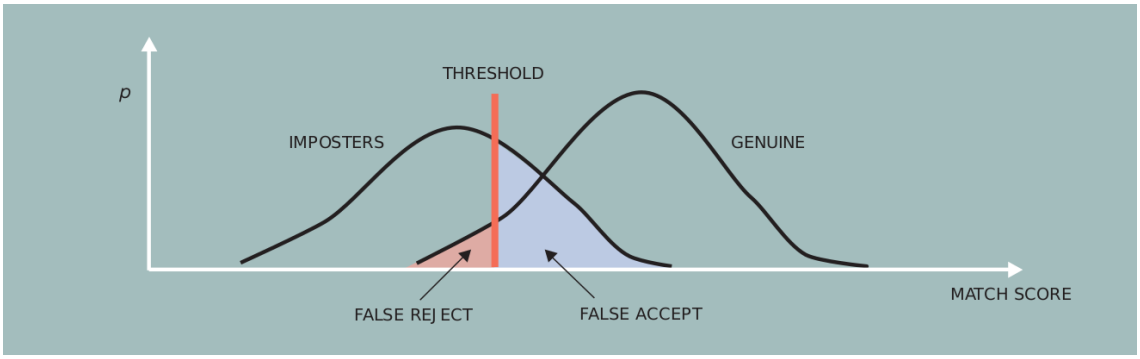


Figure 3: Example of a Receiver Operating Characteristic (ROC) curve[1]

Behavioral biometrics

Behavioral biometrics are based on how a person interacts with something or the way a person does something which generates an identical pattern which can be measured, for example voice[16], gait[17], keystroke dynamics[18, 14] and mouse dynamics[19, 14]. Behavioral biometrics has been known since 1897 when research based on typing behavior was performed with telegraphic writing, which is an early form of keystroke dynamics, by Bryan and Harter[20].

Biological biometrics

Biological biometrics is not based on how a person does something, but is based on what a person is. Biological characteristics have been used since early history and started being used for forensics in the late 1800s, by measuring different body parts. Biological biometrics are based on characteristics of the human being, such as fingerprint[21], veins[22], face recognition[23] and iris[24].

Face recognition

Face recognition uses the variations of the structure in a person's face as features and has been popular due to the potential of usage in different applications[25]. The advantage of such a system is that it only needs a camera -which exists in most of today's devices- and there is no need for physical contact with the subject. Face recognition also has its challenges such as illumination, picture quality, pose, person aging, scars and tattoos[26, 23]. The face is also unique, but there are similarities between siblings, twins and people who are related. Face recognition can be separated into 2D and 3D; 2D measures reference points in a flat surface, while 3D additionally measures depth[23]. Face recognition is often based on input of multiple faces (identification) where face detection needs to be done to isolate the faces. Each face is pre-processed and a low-dimensional representation is obtained which is important for efficient classification. It is important to note that face recognition needs to be resilient from intrapersonal variations such as aging and face expressions, but also able to distinguishing between interpersonal variations (different peoples)[4]. A survey of face recognition techniques up to 2009 has been conducted by Jafri and Arabnia[27] where face recognition research can be categorized as holistic- or feature based. The earliest work is feature based recognition by using distances, areas and angles. Later work is based on the holistic approach by

using statistics and machine learning on datasets of facial images. Principal Component Analysis (PCA) is a statistical approach that is used to represent a set of images as Eigenvectors. Fisher- and Eigenfaces are landmark techniques used in the PCA-based methods. A machine learning approach to face recognition, which uses neural networks to classify a face was proposed by Lawrende et al.[28].

2.2 Critical infrastructure

Critical infrastructure has been around for a long time but the concept is relative new. Critical infrastructure are systems which are essential for the maintenance of vital societal functions such as safety, security, health, economics and the well being of people. The definitions are different between single countries, for the EU and NATO. National and international documents as well as independent researcher- and institutional handbooks and studies differentiates these from country to country. However a broad understanding of critical infrastructure defines a system or a network of vital societal functions where infrastructure are embedded in those functions.

Norway divides critical functions into critical infrastructure and critical societal functions. Critical infrastructure is electronic communication and power, water supply and sewage, transport, oil and gas and satellite-based infrastructure. Examples of critical societal functions are food supply, health services, banking and finance, social services and social security benefit[2]. Critical infrastructure are systems which are essential in order to uphold societal critical functions which safeguard societies basic needs. The Norwegian definition of criticality is shown in figure 4.

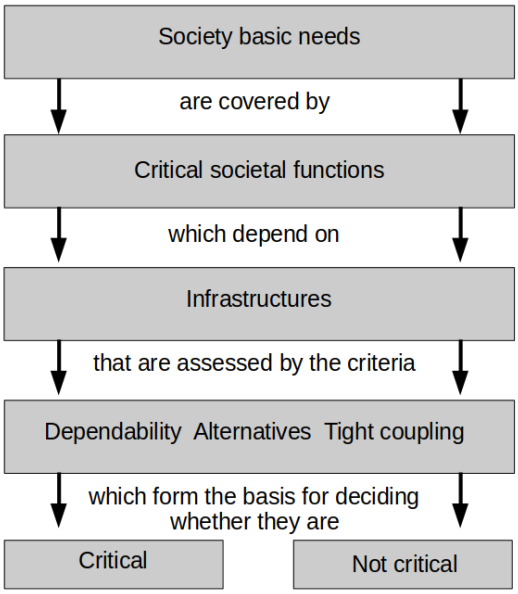


Figure 4: Norwegian definition of criticality [2]

The protection of critical infrastructure is called Critical Infrastructure Protection (CIP) and covers a nation's infrastructure across different sectors. Critical Information Infrastructure Protection (CIIP) is an essential part of CIP which focuses on the protection of underlying information infrastructure that consists of physical components. CIIP focuses on networks, wires, satellites and computers. This also includes the actual information which is transported by, to or through the physical components[3]. CIIP is also a part of Cybersecurity since it is a part of many cyber- and information security strategies. Cybersecurity covers a broad spectrum of information communication technology security issues where CIIP is included.

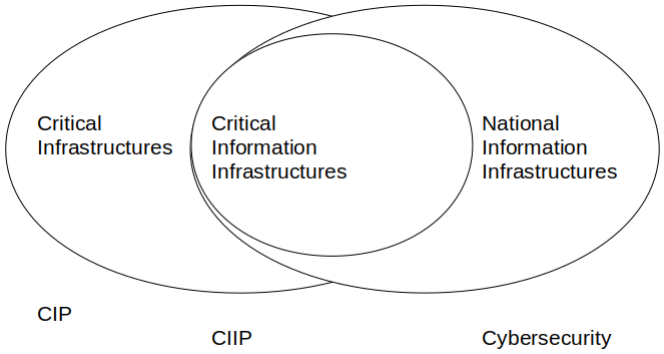


Figure 5: CIP, CIIP and Cybersecurity [3]

2.2.1 Threats and vulnerabilities

The VITA taxonomy is a set of 320 identified threats to critical infrastructure clustered as threats to the operational environment of ICT (Information and communications technology) like natural threats, technical threats, human errors etc. and ICT specific threats such as hacking, malware and denial of service[29]. The VITA taxonomy defines internal human threats as an own category of threats to CII operations which includes unauthorized access to operational systems in addition to a wide range of other physical and operational threats. External human threats such as e.g. intrusion into networks and control systems -theoretically possible on not air-gapped networks- is another category. The ENISA taxonomy[30] includes a large category of nefarious activity where threats such as abuse, misuse, identity fraud and manipulation are present, in addition to eavesdropping/interception/hijacking which is relevant for network based access control solutions. The ICS-CERT (Industrial Control Systems Cyber Emergency Response Team) identified 700 vulnerabilities through design architecture reviews (DAR) and network validation and verification (NAVY) assessments in their annual report from 2016[9]. The ICS-CERT mission is to reduce the risk to CI by strengthening security and resilience of control systems. The report identifies 700 weaknesses; the top 6 are

1. Boundary protection
2. Least functionality
3. Identification and authentication
4. Physical Access Control
5. Audit review, analysis and reporting
6. Authenticator management

The category of identification and authentication is important because those are needed to provide accountability for individual user actions. Weak identification and authentication makes it harder to secure accounts when employees leave the organization, and there are no policies or procedures to handle this[9]. Authenticator management is also part of identification and authentication and focuses on the use of passwords. Passwords can easily be compromised using brute force or pass the hash techniques.

2.3 Access control and control room

A control room is an operational center where the critical infrastructure can be monitored and controlled. The control room is often a restricted area where only authorized personnel can enter. There are usually one or more workstations, each used by an operator. Each workstation usually has multiple clients and monitors. The control rooms are protected by both physical and logical security. Physical access control is handled by dividing a location into 3 different zones. The first zone is an area for public traffic. The middle zone is a building of importance to the operation and management of energy supply. The inner zone are control rooms, server rooms and rooms for communication. The information systems in the control room are classified into operational and administrative. This is in accordance with Norwegian guidance on regulations on precautionary safety and preparedness in energy supply[31]. Figure 6 depicts a typical control room workstation with multiple screens.

Figure 6: Control room workstation

2.3.1 Systems

A control room has different systems such as a working station, an administrative station and a SCADA station. The administrative and working stations are used for production and planning, mail, logging and reporting. SCADA (Supervisory control and data acquisition) is an information- and communication technology which allows the controls of industrial processes. The controls can be performed locally or remotely with devices such as sensors, pumps, motors and valves, through a human machine interface (HMI). The basic SCADA system is built up by programmable logic controllers (PLC) and remote terminal units (RTU) which are microcomputers that are talking to sensors and end-devices which further route information to computers with SCADA software. The SCADA software processes the information, and distributes and displays it for control room operators to support decision making. SCADA systems are mostly used in the industrial sector, but are also used by companies in the public- and private sector for maintaining control and efficiency and to mitigate downtime. SCADA systems can be used on smaller, simple configurations and up to large, complex installations[32]. Security requirements for SCADA systems are based on the confidentiality, integrity and availability triad (CIA-triangle)[33].

- A threat to confidentiality would be an attempt to eavesdrop information.
- A threat to integrity would manipulate information resources, hardware or software.
- A threat to availability would be a threat to performance and unavailable systems and information resources.

This master's thesis is focusing on availability of the human-machine interaction in a control room. Availability means the ability of a system to deliver a service when it is needed at a time instant[34].

2.3.2 Authentication

The current form of authentication for access control on systems in a control room is based on knowledge based authentication by username and password. There are usually multiple account types based on different requirements. As mentioned in section 2.1.1, passwords follow best practices, which leads to passwords which could be hard to remember. The minimum set of user accounts comprises standard accounts and an administrator account. Administrator accounts have more privileges and are inter alia used to create standard accounts; they therefore have more strict requirements than a standard account which usually is used by any employee. In addition, access to SCADA systems usually needs authorization and authentication, i.e. another user account with own requirements.

3 Related research

3.1 Control room authentication

There is limited research based on biometrics used inside control rooms. SUAC3I [8] (Secure User Authentication in Control Centers for Critical Infrastructures) is a project funded by the European Commission which uses a multi-modal biometric solution to provide access control for control room systems. As well as Schiavone et al.[35] which also uses multi-modal biometrics by a fingerprint scanner on the mouse, a web camera for face recognition and keystroke dynamics from the keyboards. This combines behavioral- and biological biometrics based on a level of trust. The trust value are assigned as the user logs on to the system. This value will change during the operator types on the keyboard. If the system discovers unknown behavior, the trust value will decrease, and if it falls below a defined threshold the operator will be logged out. As the operator gets logged out, it is necessary to perform a new login to get the trust level back. The system is based on two different phases, initial phase: the user can start a session based on strong authentication by login with a one-time password, or using biometrics which is based on verification from all biometric subsystems. Maintenance phase: this is also based on all three subsystems to perform continuous authentication. The user can sit in front of the client, type on the keyboard to gain trust. If the trust level decreases, the operator will be notified and needs to be authenticated again. If not the sessions will expire. This concept should be extended to use mouse dynamics as a part of the behavioral biometrics to collect more user data. The interaction between a operator and the terminal in a control room will vary. It can be limited in periods and therefore it is desirable to collect as much user data as possible. This concept of research by Schiavone et al.[35] will lock the user out of the clients, while the driving concept behind SUAC3I[8] is blocking of input. This is handled by an daemon on each client which are able to enable or disable input. This means that the operator at all time can monitor activity on the screen even if logged out.

The research conducted by Schiavone et al.[35] are based on a control room station with a single mouse and keyboard which will cover some control rooms, but since this project allows multiple clients at each workstation it will be problematic using behavioral biometrics by keystroke dynamics or mouse dynamics. The part with fingerprint sensor in the mouse and face recognition is still possible.

3.1.1 SUAC3I

The SUAC3I[8] project is a proposal of focusing on user-authentication at the workstation by using strong biometric authentication instead of focusing on physical access control. The project has used the biometric properties as shown in section 2.1.3 for a control room setting in order to select the most suited biometric modalities. That is fingerprint, hand veins, iris and retina according to table

1 with the values low (L), medium (M) and high (H) which summarized strengths and weaknesses. The chosen biometric modalities for the project is fingerprint and iris.

Biometric	Universality	Collectability	Uniqueness	Permanence	Performance	Acceptability	Circumvention
Fingerprint	M	H	H	M	H	M	H
Hand geometry	M	M	M	H	M	M	M
Face	H	L	L	H	L	H	L
Iris	H	H	H	M	H	L	H
Retina	H	H	M	L	H	L	H
Voice	M	L	L	M	L	H	L
Signature	L	L	L	H	L	H	L
Ear	M	M	H	M	M	H	M
Keystroke	L	L	L	H	L	M	L
Hand vein	M	M	M	M	M	M	H

Table 1: Comparison of biometric properties [8]

As mentioned, the driving concept behind SUAC3I is the blocking of input at the workstation and not the screen. The second concept is traceability which is handled by sending user behavior to a server when a user locks or unlocks at a workstation. The solution has three main elements:

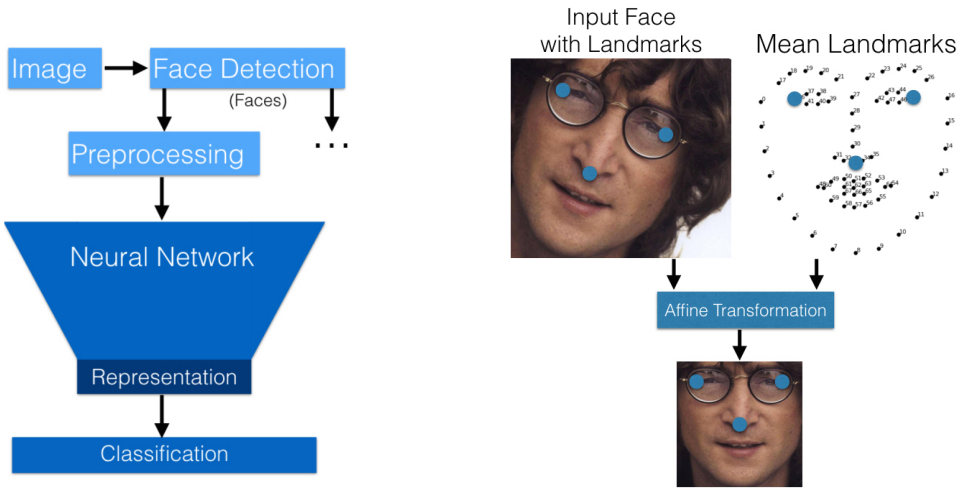
1. An daemon on each workstation capable of disabling input.
2. A server responsible for managing users.
3. Client-Server communication.

The essential part on the client side is the SUAC3I locked process which blocks input from mouse and keyboard and shows a locked message for the operator. The locked process is responsible for preventing the capture of mouse and keyboard event until an operator is successfully authenticated. The operator still needs to monitor activity but also clearly knows about the locked workstation which is displaying a lock symbol on the client screen. The client also communicates directly with the biometric device to perform authentication. The server manages all workstations, users and the access permissions for each workstation. A daemon on the client side is constantly listening to the server awaiting grant or revoke. The daemon also communicates with the biometric device interface. The server is responsible for managing access privileges and store biometric data. SUAC3I opens up for usage of multiple biometric modalities from multiple manufacturers where each manufacturer has its own SDK for the current biometric solution. This is handled by adding a homogenization layer so the solution is not bound to a specific solution but also open for future devices. SUAC3I performs authentication at several biometric devices which communicates directly

to the client which further communicates to the server, there are no direct communication between the biometric devices and the server.

3.2 Face recognition and OpenFace

OpenFace by Amos et al.[4] is a open source library used for face recognition. OpenFace is based on the technology behind Facebook's DeepFace[36] and Google's FaceNet[37] which both uses deep neural networks.



(a) Flow of face recognition with neural network [4]

(b) Affine transformation [4]

Figure 7: OpenFace architecture

Figure 7a highlight the OpenFace implementation. The preprocessing part is based on landmark detection by using bounding boxes on different location on the face as a direct input to the neural network. Normalization by 2D affine transformation to make eyes and nose appear in the same positions as shown in figure 7b. It further resizes and crops images to the edges of the landmarks which leaves 96 x 96 pixel images. The neural network in OpenFace are trained with 500k images (FaceNet[37] with 100-200M and DeepFace[36] with 4.4M images). The neural network structure are based on the FaceNet architecture[4]. OpenFace was developed with the goal to be the state of the art open source face recognition library[4]. FaceNet and DeepFace are the best performing methods today based on accuracy.

Figure 8 presents the results from the LFW benchmark[38]. The best scenario would be having the true positive rate of 1 everywhere which the industry state of the art almost achieves. The graph also shows OpenBR[39] and "Human, Cropped" by Kumar et al.[40] which presents results by human decisions and not a machine. The ROC curve shows that OpenFace are near the performance of today's state of the art deep learning techniques. The best performing algorithm are DeepFace according to to ROC curve. The area under curve (AUC) is the probability that a randomly cho-

sen face of a known person will be ranked higher than a randomly chosen face of other different people[4].

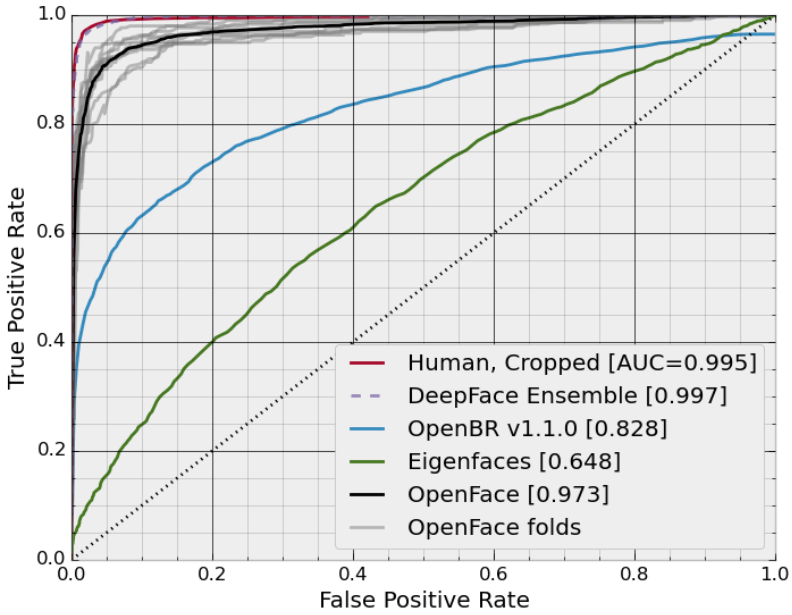


Figure 8: ROC curve of LFW benchmark [4]

3.3 Continuous authentication

Continuous Authentication (CA) is based on continuously verifying that the users are the same as the one who logged into the system, and mostly known using behavioral biometrics. This is different from Periodic Authentication (PA) where users are authenticated frequently at specific times and not continuously and static authentication (SA) which authenticates only once[12]. The big difference is the set of data used for verification. CA uses real-time data and PA uses a bulk of data. In CA, every keystroke or mouse movement is compared against a reference which will decrease or increase the level of trust based on impostor of genuine user actions. This is based on the score of that single action which will identify if the user are classified as genuine user or impostor. This is called penalty (decreased trust) and reward (increased trust)[12, 14]. No person can behave in exactly the same manner at all times so genuine users will sometimes deviate from the normal and decrease the score. But the majority of user-actions will be inside a allowed range based on the reference it is compared against. An impostor could perform actions which are defined as genuine, but the majority of actions would decrease the trust level. When a users logs into a system, he or she will gain 100% of trust. This trust level will decrease based on impostor actions and will increase on genuine actions, but never increase above 100% which is the maximum threshold. There is also

a threshold where the users is locked out and need to authenticate again to reset the trust level. Most of the research are using keystroke- or/and mouse dynamics and based on metrics such as FMR and FNMR. For continuous authentication it is also important to know when an impostor is detected and know what set of actions that has been done before detection. Therefore, ANGA and ANIA are good performance indicators for such as system[14].

3.3.1 Continuous authentication using face recognition

A experiment conducted by Beunder[41] tests continuous authentication by using face recognition. Some requirements was to detect an impostor by 10 seconds and then lock the person out from the system. Authorized users should be identified even if certain conditions are met. Authorized users was tested in a static, busy and concentrated scenario. The experiment used OpenCV with Local Binary Pattern (LBP) as the algorithm for comparison. The experiment failed due to to many false negatives and the average time of detecting an impostor was six times higher than requirements. Change of condition also had a major impact on the trustworthiness such as lightning and face alterations. Resource consumption by CPU and memory were not a problem. This experiment was done using a laptop with integrated camera which tends to have a lower quality than stand alone cameras. The process of registration or enrollment of users was done every time a user logged into the system. While a user were typing a password to log onto the computer, a picture was taken. The quality of the picture was not controlled. Face recognition has also been used for surveillance. Wati and Abadianto[42] uses a PCA based face recognition algorithm and tries to replace the door-lock and key with face recognition. A camera is placed by the door to capture people. Several tests are done to verify the quality of the technology. This will of course depend on the camera and face recognition algorithm, but there were done tests in different conditions. The distance between the subject and camera was able to detect the face when the distance was 80, 160 and 240 cm. There was not possible to detect a face when the distance was 360cm or more. Direct lighting to the face was tested by holding a flashlight directly to the face from different distances which didn't have any effect to the face detection, the same with light from different angels. Testing with various accessories such as cap and hijab cause problems with face detection. Another problem was the use of clothing that had similar color as the skin. The system proposed by Rajiv et al. [43] also uses face recognition for home surveillance but enables email communications which allows an owner to remotely control the doors for possible visitors. Non of these are using continuous authentication by the definition as in section 3.3, but rather variations. The biggest difference for this thesis is the usage of a specifically enrolled reference which needs a large set of genuine user images to be used for comparison.

4 Requirements

This chapter contains requirements which the prototype of the solution is based on. All requirements are based on the SUAC3I project[8]. Requirements are divided into system, user and security requirements. The system requirements are technical while the user requirements are directed towards usage. Requirements for the clients apply to all clients at a workstation. The server includes the biometric devices and handles authentication.

4.1 Main requirements

1. User friendliness: The authentication system needs to be easy to use. The users should not need new knowledge to use the system and the user-interaction should be kept at a minimum level.
2. Strict access control: This means that margins of false positives should be low or zero. The system cannot accept unauthorized users. It also needs to be resistant to physical and logical attacks.
3. Availability: Availability is about providing operators of a control room operational information at any time and ability to perform actions within a short time limit. Authentication has to be as quick as possible and not time consuming.
4. Accountability: The use of unique user-identities where actions of an entity can be traced back to this entity. Sharing of user identities should not be possible.
5. Traceability: Traceability is important to support accountability to have an overview of what types of operations are performed by which operator.

4.2 System requirements

4.2.1 Client

As there are many different forms of control rooms with different numbers of workstations, clients and different sets of technology, the solution must fit different types and variations of control rooms and the technology inside.

Performance

- Client lock: It must take no longer than one second to lock if there is an unknown user. If no one is identified as user or an unknown user is detected, the client must be locked within 1 minute.
- Client unlock: It must take no longer than one second to positively identify a user and grant access.
- CPU usage: max 5%.
- RAM usage: max 5%.

Compatibility

- All clients shall share the same source code.
- The solution shall be implemenetd in a programming language which enables interoperability between different systems.
- The client solution should work on Windows 7.
- The client solution should work on Windows 8.
- The client solution should work on Ubuntu 14.04.

Third party integration

The clients in a control room will have many different applications installed. It is important that the solution does not interfere with other applications.

- The locking mechanism shall not interfere with the screensaver and power-saving tools of the client.

4.2.2 Server

Traceability

- The server shall keep a log of all users and personnel interacting with each workstation.

Services

The server shall be able to communicate with all clients at a workstation.

- Unlock enables input from mouse and keyboard.
- Lock disables input from mouse and keyboard.
- Emergency unlock enables input from mouse and keyboard and disables biometric authentication.
- Emergency lock disables input from mouse and keyboard and disables biometric authentication.
- Timeout disables input from mouse and keyboard.

4.3 User requirements

4.3.1 Client

- Visibility: Screens on every workstation should be visible both when locked and unlocked.
- Disable input: When workstations are locked, input from the keyboard and mouse shall be disabled.
- State indication: Operators shall be aware of the current state at any time.
- Emergency unlock: A single client must be able to unlock all other clients at a workstation.
- Emergency lock: A single client must be able to lock all other clients at a workstation.

4.3.2 Server

- New user: The server shall be capable of adding new users.
- Delete user: The server shall be capable of deleting users.
- List users: The server shall be capable of listing all users.

- Add client: The server shall be capable to add a new client.
- Remove client: The server shall be capable to remove a client.
- List clients: The server shall be capable to list all clients.
- Assign user to client: The server shall be capable to add a new user to a client.
- Remove user from client: The server shall be capable to remove a user from a client.

4.4 Security requirements

- The following operations shall be communicated through encrypted communication:
  - Lock
  - Unlock
  - Emergency unlock
  - Emergency lock
- Client must not have permission to edit log files.
- Client must not have permission to edit files to change time before lockout.
- Client must not have access to interfere with the solution.
- Client must not be able to stop the solution.
- Code audit: A security audit of the source code shall be provided to exclude malicious code or bad code practices.

4.5 Legal considerations

The Norwegian law of privacy does not directly include biometrics but defines that social security numbers and other methods of identification only can be used when there is a need for secure identification.

> "§12 Fødselsnummer og andre entydige identifikasjonsmidler kan bare nyttes i behandlingen når det er saklig behov for sikker identifisering og metoden er nødvendig for å oppnå slik identifisering." [44]

The person responsible for treating data shall satisfy information security with confidentiality, integrity and availability (CIA). The process of storage and the use of data shall also be documented and available to other employees and to the controlling authority.

> "§13 Den behandlingsansvarlige og databehandleren skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger. For å oppnå tilfredsstillende informasjonssikkerhet skal den behandlingsansvarlige og databehandleren dokumentere informasjonssystemet og sikkerhetstiltakene. Dokumentasjonen skal være tilgjengelig for medarbeiderne hos den behandlingsansvarlige og hos databehandleren. Dokumentasjonen skal også være tilgjengelig for Datatilsynet og Personvernnemnda." [44]

A consultative paper has been released by the Department of Justice of the Norwegian government which is intended to include the EU GDPR (The General Data Protection Regulation) into

Norwegian law[45]. As the consultative paper specifies, biometric data shall be handled in the same way as sensitive and personal information. The only difference to previous legislation is that biometrics is specified. Social security numbers and other means of identification should only be used when there is a need for identification and the method is needed to achieve such identification. This includes fingerprints and other biometric data.

5 Architecture of the solution

Figure 9 shows an overview of the solution at a workstation where the server communicates with a biometric device which is used for user authentication. The server also communicates directly with a daemon inside each client at the workstation.

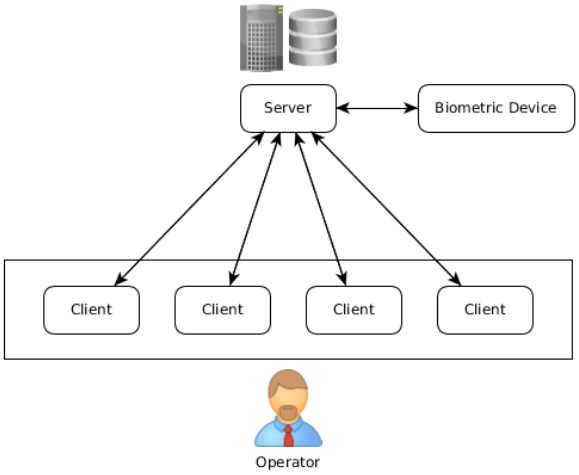


Figure 9: Overview of main architecture

5.1 Client

The main purpose of the client is to grant access to authorized users and to deny access to unauthorized users. A workstation will consist of one or more clients, depending on the control room. Each client will run a daemon which listens to signals from the server to perform lock or unlock on operations. The clients at the workstation will not have any direct interaction with the biometric device; this is handled by the server which manages the process of authentication.

5.1.1 Lock and unlock

The main responsibility at the client side is to enable and disable input from mouse and keyboard based on the lock and unlock signals from the server. This is handled by a daemon running on each client. Figure 10 shows different triggers which will cause a change of state. Biometric authentication is used for operators to gain access to the workstation. Forced lock is triggered when an unknown person is detected. Timeout will lock the clients after a length of time when no authorized operator is detected. Emergency lock and unlock will disable the current solutions and will provide

full availability or full lock depending on the situation. All triggers will not change the state every time, for example the timeout trigger will not change the state if the client is already locked. All states and state changes handled by a state machine.

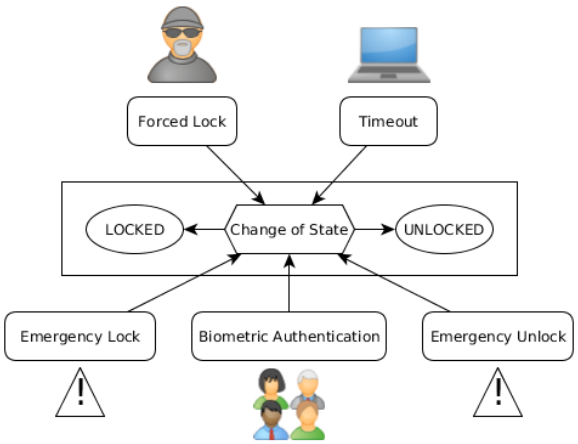


Figure 10: Change of state

State machine

The state machine has two possible states:

- Locked
- Unlocked

This is a deterministic finite automaton which can change between two different states. The actors who can trigger a state transition are the operator, the server and the client. The operator can cause a state transition by the process of authentication. An unknown person can also trigger a state transition by locking the solution. The server can trigger a state transition by locking or unlocking the clients in an emergency situation. The clients can trigger a timeout. Table 2 shows different state transitions depending on the actions in a state transition table.

Current State	Action	Next State	State transition
Locked	Forced lock	Locked	No transitions
	Timeout	Locked	No transitions
	Emergency lock	Locked	No transitions
	Emergency unlock	Unlocked	Locked –> Unlocked
	Biometric authentication	Unlocked	Locked –> Unlocked
Unlocked	Forced lock	Locked	Unlocked –> Locked
	Timeout	Locked	Unlocked –> Locked
	Emergency lock	Locked	Unlocked –> Locked
	Emergency unlock	Unlocked	No transitions
	Biometric authentication	Unlocked	No transitions

Table 2: State transition table

5.1.2 GUI

The graphical user interface only consists of two images, as shown in figure 11 which shows a lock and an unlock symbol. A state transition will trigger a change of the GUI when states are changed from locked to unlocked or unlocked to locked. This is to inform the operator of the current state. The lock or unlock symbol is visible in the upper right corner of the screen on every workstation.

Figure 11: Lock and unlock symbols

5.1.3 Daemon

The daemon on the client side is responsible for receiving state transition commands from the server and also performs the timeout operation. The daemon starts when the session on the workstation clients starts.

5.1.4 User session

Sessions are not defined for each user, but rather one session which is defined as unlocked. The session starts when a user is granted access as unlocked and ends when the state changes to locked. There can be several users in one session, an example would be that one user logs in to the system and another user takes over the monitoring before a timeout occurs. As figure 12 shows, as long as there is one known operator, access is granted and the state is defined as unlocked. An unlocked and granted state will also be the time between an operator is authenticated and timed out.

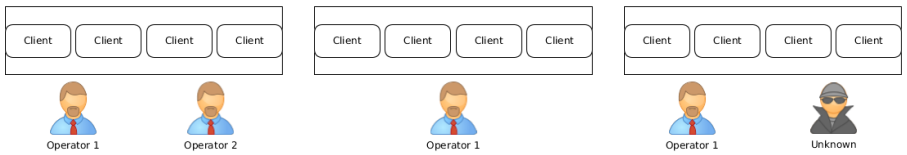


Figure 12: Access granted

Figure 13 shows an unknown person behind the workstation; this will cause a system lock.

Figure 13: Access denied

5.2 Server

The main purpose of the server is to perform authentication and to communicate commands to the client in order to trigger state transitions. The server will also function as an administrator which enables enrollment of new users, edit or removal of old users.

5.2.1 GUI

The server will have a graphical user interface which enables enrollment of users available for administrators of the solution. The GUI will enable the administrator to add a new user by name and further be given the opportunity to upload images of the user which will be stored in a tree-structure at the server where there is one folder for each user and each folder has a set of facial images provided to create a reference for each user. The administrator needs to upload several images in order to meet the requirement to get the highest confidence score possible. The administrator will further be given the possibility to add a user; the solution will then do feature extraction of all the users included in the tree structure. The following functions will be available for the administrator:

- Add user
- Remove user
- Add client
- Remove client

5.2.2 Server authentication

Administrators do not perform biometric authentication. Administrator accounts are using usernames and passwords.

5.3 Emergency lock and unlock

Availability is crucial for operations in control rooms which need mechanisms such as emergency lock and emergency unlock. Each client at the workstation has to be able to perform actions both locally and central.

- Workstation lock: a single client can send an emergency lock signal to the workstation server; this locks all clients at the workstation and disables the biometric authentication.
- Workstation unlock: a single client can send an emergency unlock signal to the workstation server; this unlocks all clients at the workstation and disables the biometric authentication.

The emergency lock cannot be undone after it is locked. This is due to security considerations since it is possible to use the solution where one user is unknown and one user is authorized. This is a measure against burglaries. To unlock an emergency lock a password is needed which should be stored in a safe in another room. The emergency unlock on the other hand can be set back to normal by the operator.

5.4 Traceability and reporting

While the system does continuous authentication, it can record live events of personnel in the control room. A report will be produced for each day with the format as shown in table 3. A new column will be added in the report which is triggered by a state change at the server as shown in figure 11 and table 2. A picture is taken every time an user is defined as "unknown". This can be used for further identification.

Time	Workstation	State	Operator	Picture
1655	1	Unlocked	Ola Nordmann	Nil
1700	1	Locked	Nil	Nil
1755	1	Unlocked	Ola Nordmann	Nil
1803	1	Unlocked	Per Nordmann, Ola Nordmann	Nil
1813	1	Unlocked	Per Nordmann	Nil
1830	1	Locked	Unknown	2018-01-01-18-30
1835	1	Unlocked	Per Nordmann, Unknown	2018-01-01-18-35
2000	1	Emergency Unlocked	Per Nordmann	Nil
2335	1	Emergency Locked	Unknown	2018-01-01-23-35

Table 3: Example of daily user report

5.5 Face recognition

Face recognition is set up by using OpenFace[4] which is running on the server with an own camera at each workstation.

5.6 Continuous authentication

Earlier known CA systems are based on penalty and reward as described in section 3.3. The user starts with a trust level of 100% after authentication; the level of trust increases or decreases based on impostor or genuine user actions. This is handled in a different way using face recognition as CA. The same concept of penalty and reward are basic foundations for CA and are reused in a different approach. On a CA system based on keystroke- or mouse dynamics there is need of a set of genuine user actions to reward a user a trust level of 100%; this is because single keystrokes or mouse movements are not enough to identify a user. One single action will direct the user ± 1 point closer or further away from the threshold; this means that a set of actions to perform identification is needed. But by using face recognition, one single capture is enough to perform identification. This means that the reward of gaining 100% trust can be performed in one capture. Penalty can also be given in a similar way of setting the trust to 0% while an unknown user is detected. Penalty is used in another way when there are no detected personnel in front of the workstation. The system will then count backwards until a threshold is reached. This further leads to locked clients at the workstation which is defined as a timeout. The system is capable of detecting impostors so there is no need to decrease the trust level by the same rate as when no one is detected, but rather lock the clients when an impostor is detected.

1. Genuine user detected: Set trust level to 100% (Full reward)
2. Impostor detected: Set trust level below threshold
3. No person detected: Decrease trust level (Penalty)

5.7 Communication

5.7.1 Client inter-process communication

The are two elements which communicates with each other, as presented in figure 14. There is one process called the receiver which handles all external communication to and from the server where the biometric device is attached. The inter-process communication at the client side is between the receiver and the authenticator and is being done by one way communication using sockets. The authenticator listens to signals from the receiver and makes a binary decision to unlock or lock the client. In an emergency situation the receiver will only send a lock or unlock signal depending on the situation.

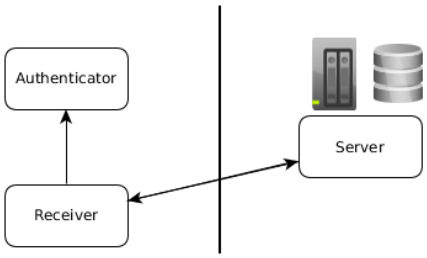


Figure 14: Client inter-process communication

5.7.2 Client-server communication

The only external communication from different nodes is between the server and the client, as figure 15 illustrates. The client can demand the server to perform an emergency lock or unlock if such a situation occurs. Any client can trigger the server to broadcast a lock or unlock command to all clients at a workstation. This is the only situation where the client sends information to the server. Otherwise, the server makes a binary decision whether to unlock or lock, depending on the biometric device. Decisions based on forced lock and timeout are also handled by the server through the biometric device in the same way. Forced lock is triggered when a unknown subject is detected and timeout when no positive authentication can be made.

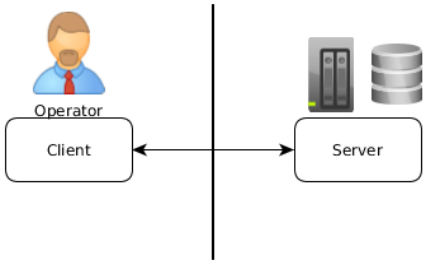


Figure 15: Client-server communication

5.7.3 Secure communication

Given that the solution is providing secure authentication to critical systems, it is important that communication between all nodes is secure. External communication such as between clients and the server is encrypted and will only send lock, unlock and emergency commands. As the architecture is, all entities of the solution are placed in the same room, i.e. a control room that requires a set of security mechanisms. This means that the solution is well protected against physical attacks. On the other hand, the solution needs to be protected against certain attacks. Unencrypted communications allow sniffing of packets which can then be replayed. This means that a potential attacker can listen to traffic and replay packets to the clients on behalf of the server to control when the

clients at the workstation should be locked or unlocked. The communication between nodes in this solution is secured by using the SSL/TLS family protocols. The authentication of trusted nodes in the network is handled by a certificate based approach. Each server works as a certification authority (CA), which uses self signed certificates and needs to sign all client certificates so the clients are valid and usable at the workstation. The reason of choosing a public key infrastructure for this solution is to facilitate for extending the architecture. The solution architecture for this thesis is a prototype based on a single workstation. An extension of this solution may include multiple workstations, which leads to multiple servers which handles authentication and at the top a central server which will work as an administrator and certification authority.

6 Methods

This thesis presents the development of a prototype of a solution which will require use of different methods. The choice of biometric solution is conducted in earlier research[46], where quantitative methods were used to look into different solutions of authentication such as behavioral and biological biometrics, knowledge based authentication, possession based authentication and non-personally identifiable information (Non-PII). Non-PII are data which can be gathered that do not collect personal information such as in the research by Malatras et al.[47] which collects identifiers based on CPU, memory and network activity. Each method of authentication was analyzed up against criteria and main requirements as described in chapter 4. Behavioral and biological biometrics were also analyzed against the biometric properties as shown in section 2.1.3 where each property gives a score of low, medium or high. Based on the analysis, the final choice was the use of facial recognition which requires non or minimal user-interaction and it is possible to perform continuous authentication that enables availability and traceability. The biometric property of security and the requirements of strict access control result in a lower score for face recognition than for example iris, vein or knowledge based authentication.

The choice of modality depends on today's critical need in control rooms which is the availability. Security can be handled by authentication at the workstations or by physical access control to get into the control room. Physical access is often handled by access control at several levels as described in chapter 2. There are many different solutions of face recognition on the market which could be used. Based on cost and quality to build a prototype, OpenFace[4] which is an open source face recognition library with high performance and accuracy is chosen, as a free tool. OpenFace allows face recognition on a video stream and still images.

Face recognition compares templates based on features extracted from the face. The reference is generated by extracting features from several facial images of a person which is compared with features extracted from a probe. The comparison gives a score which uses the threshold to decide if a person is known or unknown. This thesis will use qualitative methods for the process of verification of this technology by testing it on different scenarios. This includes both enrollment of new users and testing the system live by verifying enrolled users. The testing is not done inside a control room, but in a controlled environment using a single computer. The solution should work on one or several clients. The set of multiple clients on a workstation are represented by running multiple virtual machines on the same computer where communication behind are provided by socket-communication. The verification will mostly focus on the biometric device and the use of continuous authentication.

6.1 Prototype hardware

The prototype of the solution is running on a virtual machine by virtualbox on Ubuntu 16.04 with 5GB of RAM and 2 processors are assigned from a physical machine of 8GB RAM and Intel(R) Core(TM) i7-6500U CPU @ 2.50GHz.

6.2 User enrollment and feature extraction

User enrollment is based on feature extraction from images. Different numbers of images were tested to identify the number of images which is necessary to use for each user to enroll on a live system. Different numbers of images of the same person were used and verified against three images to provide an accuracy rate. The goal is to find the amount of images necessary to find the point where the accuracy rate does not change. The facial images are not taken in a specific angle and there or not different poses, just ordinary facial expressions. This is due to OpenFace's[4] feature extraction algorithm which normalizes each face before landmarks are detected and features are extracted, as in the examples shown in figure 16.

Figure 16: Cropped faces

6.3 Live usage and performance

After enrolling and creating a classifier which is used as reference, this is tested against different probes. The reference was first tested live with a subject in front of the camera with the head aligned and eyes looking on the camera in order to capture as many facial features as possible. Different poses are also tested when the subject looked up, down, left and right to test face recognition from different angles. The use of artifacts is also possible in a control room, so the subject was also tested with a cap, cap and glasses, glasses, winter cap, jacket, jacket and hood. The system was also tested with multiple users. Instead of gathering multiple people to stay in front of the camera, a database of images with 76 men and 60 women were used. Each person is represented by 1-4 different images. All these subjects are tested as impostors to see what confidence level impostors get. 65 different images of one genuine user are also used to test against the reference to see what confidence level a genuine users has relative to the impostor. All images of the genuine user were used to create the reference template. Scenario testing was also performed by reconstructing 3 different scenarios given different tasks. Each scenario was captured for 8 minutes.

- Calm scenario: The subject is sitting watching a movie.
- Moderate scenario: The subject is sitting, turning his head talking to co-workers, drinking coffee from a cup and water from a bottle, scratching his face.

- Busy scenario: The subject is standing; sometimes in front of the camera and sometimes in distance. Continuously moving away from the camera.

The CA algorithm is a face recognition algorithm running in an endless loop where performance is measured by the time used in each round. Each round includes capture of a reference which is compared with the probe and given a score. The continuous authentication part of the system defines a maximum trust level of 100 and a threshold at 50 which defines a session as logged in(> 50) or logged out(< 50). Detection of genuine users sets automatically max trust at 100 and detection of impostors sets it at 0. The threshold was set to a confidence level of 90% during testing.

6.4 Security

Simple attacks were performed against the sensors-level of the solution. Presentation attacks were performed where the same images were used for testing classifiers and a part of the probe (figure 17). The same images was tested from a digital screen (iPhone 6S) and as printed paper held up against the camera.

7 Verification

7.1 User enrollment and feature extraction

Table 4 shows the accuracy rate by comparing different enrolled references based on the number of images. All references are compared against three different samples from the same data subject as shown in figure 17. Based on the result, it is easy to see that the more pictures of a data subject are used, the more accurate authentication is, based on the confidence level. The largest span is from 3 to 30 images where the accuracy increases for each image. From 30 images and up to 65, the accuracy stagnates and reaches a top value between 50 to 65 images with an accuracy of 97%. This means that the solution is 97% sure that the reference based on the input of 65 images of the same data subject is the same as the three samples. 97% is also what was expected when looking at the ROC curve in 8 which presents OpenFace with an error rate of 2.7%. This error rate is the probability that the reference will rank randomly chosen faces of the same person higher than randomly chosen faces of different people[4].

Number of images	Sample a (fig. 17a)	Sample b (fig. 17b)	Sample c (fig. 17c)
3	0.73	0.74	0.72
5	0.80	0.81	0.79
10	0.86	0.86	0.84
15	0.88	0.89	0.88
20	0.91	0.92	0.91
25	0.93	0.94	0.93
30	0.95	0.95	0.94
35	0.95	0.96	0.95
40	0.96	0.96	0.96
45	0.96	0.97	0.96
50	0.97	0.97	0.97
55	0.97	0.97	0.97
60	0.97	0.97	0.97
65	0.97	0.98	0.97

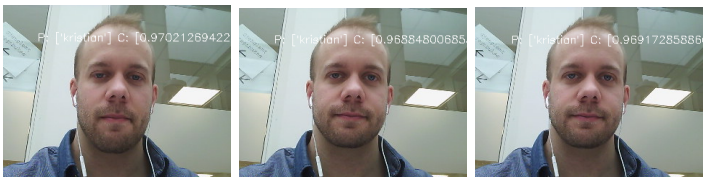
Table 4: Accuracy on reference based on number of images

(a) (b) (c)

Figure 17: Images used for comparison to test classifiers

7.2 Performance

Live usage gives a confidence level in the range 96-97% by looking at the camera where all characteristics from the face are visible, as shown in images in figure 18.



(a) 0.970 (b) 0.968 (c) 0.969

Figure 18: Capturing live data subject

Figure 19 shows an overview of 65 genuine user images which are compared against the enrolled reference of the same 65 images. One image gives a confidence score of 95%, which is the lowest. The mean, median and the most occurrences are at 97%, which is represented by 33 of the genuine user images. There are 18 images at 98% and 13 images at 96%. The outlier at 95% is a lower sized image containing mostly background and the full body of the data subject. The rest of the images are mostly images focusing on the face or upper body.

Figure 20 is an overview of a total of 493 images from 136 different impostor users. 60 of them are women and 76 are men. Each person is mostly represented by 4 images, but some are represented by 3,2 or only 1 image. 1 person which is tested with 4 different images is represented by a confidence level at 95% in 2 images, 1 image at 94% and 1 image at 93%. There are 4 different users of 5 images at 91-92% confidence and 90% are represented by 5 images of 3 different users.

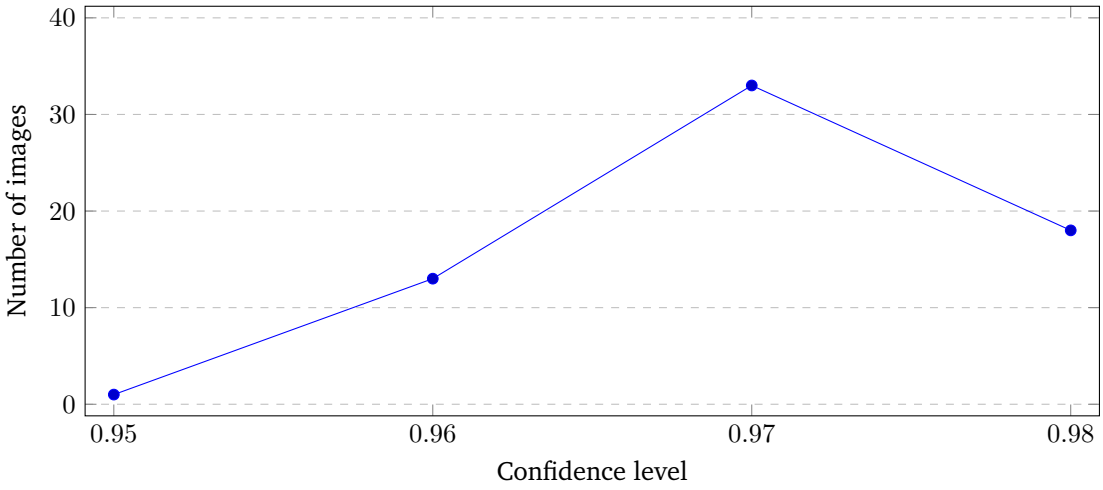


Figure 19: Confidence level from comparison of reference and images of genuine user

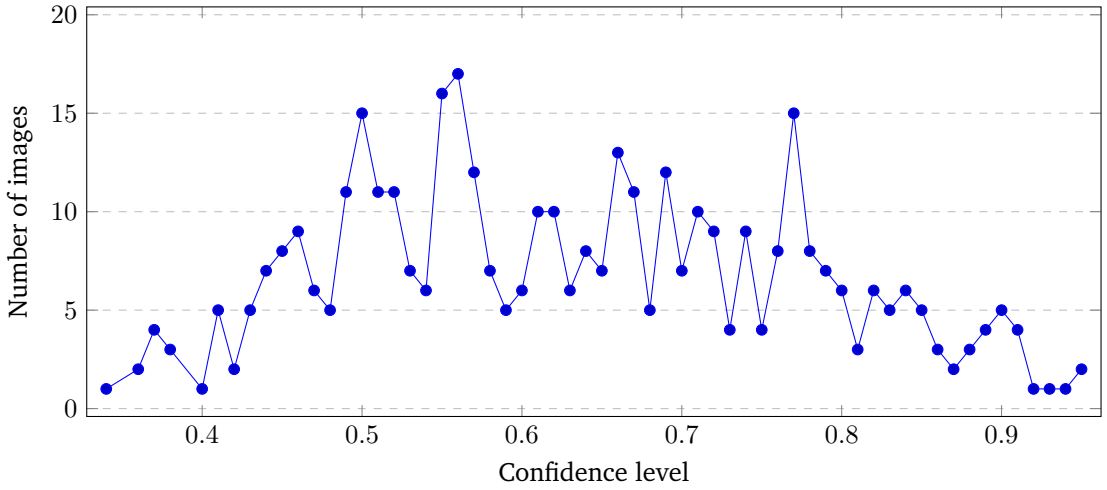


Figure 20: Confidence level from comparison of reference and images of impostors

Figure 21 shows the round time used for each comparison. Each round includes detection of a face from the camera, comparison with a reference and judgments based on identification of a genuine users or detected impostor. The most occurrences are found between 0.50 and 0.69 seconds with an average value of 0.604 seconds. The live usage has a latency of 2-3 second before the system detects changes from the camera; this is not included in the numbers in figure 21.

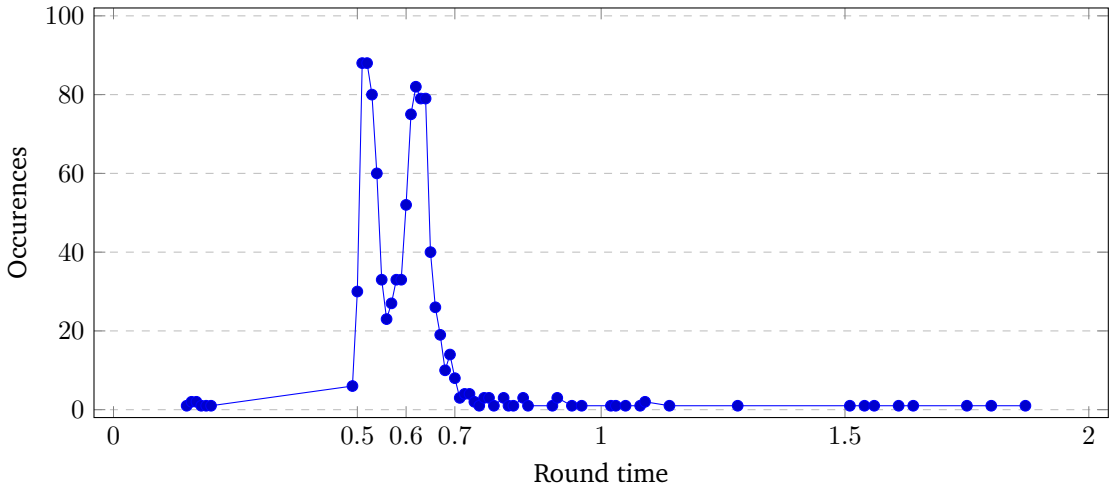


Figure 21: Round time for continuous authentication

Figure 22 shows a graph of around 1000 decisions from a 10 minutes capture of a genuine user. The confidence level ranges from 90% up to 98%, with most occurrences between 96% and 98% and a peak at 97%.

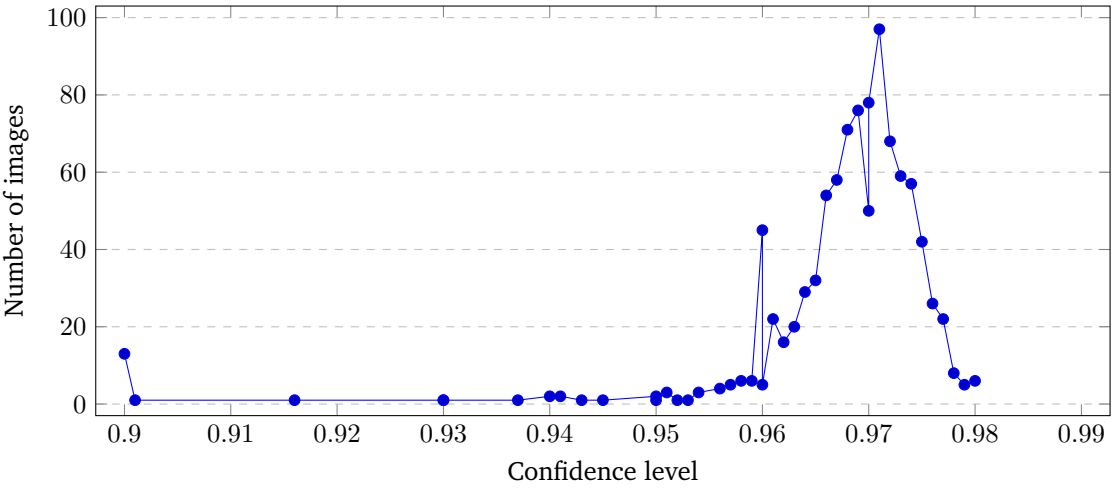


Figure 22: Confidence level from live capture of genuine user

7.2.1 Scenario testing

Figure 23, 24 and 25 shows the confidence level for each round of capturing in a calm, moderate and busy scenario as described in section 6.3. The calm scenario (figure 23) shows a stable confidence level between 98% and 96% with most occurrences between 97% and 98%. There are two drops; one at 530 and 690 rounds where the last are classified as false negative due to low confidence level at 79%. The moderate scenario (figure 24) shows a wider range of confidence level between 98% and 96% with more drops. Penalty occurs when the subject is drinking coffee or water which blocks the camera from capturing needed facial features, but penalty never leads to timeout since its only registered a maximum of 13 rounds which is about 8 seconds. The busy scenario (figure 25) is more unstable since the subject were walking away from the camera which causes a timeout between round 20-110 and 140-260. The rest of the session is defined as unlocked but has many rounds with decreased trust (penalty) since no subject are captured. The calm and moderate scenario also shows 1% higher confidence level than in figure 18. The calm scenario registered 0% rounds where no user was detected, the moderate scenario at 5.88% and the busy at 49.25%. Based on the level of false negatives on all rounds where the users was detected; the calm scenario has 0.13% FNMR, moderate at 2.66% FNMR and the busy scenario at 2.71% FNMR using a 90% confidence level as threshold.

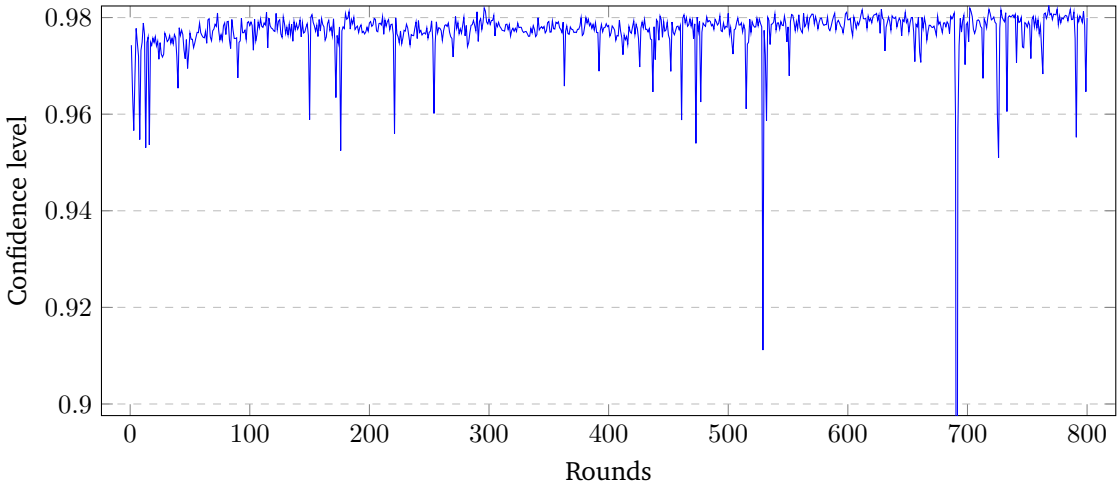


Figure 23: Scenario: calm

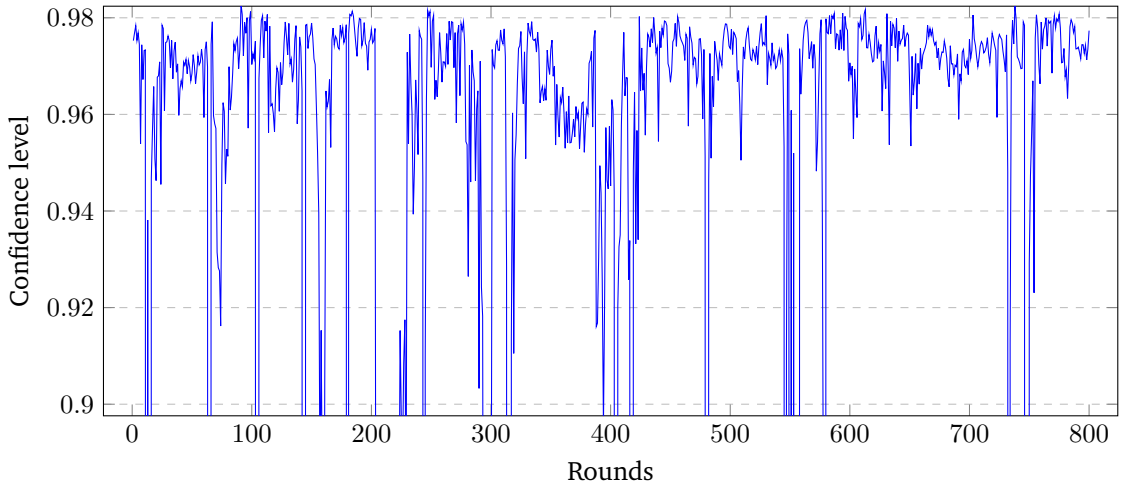


Figure 24: Scenario: moderate

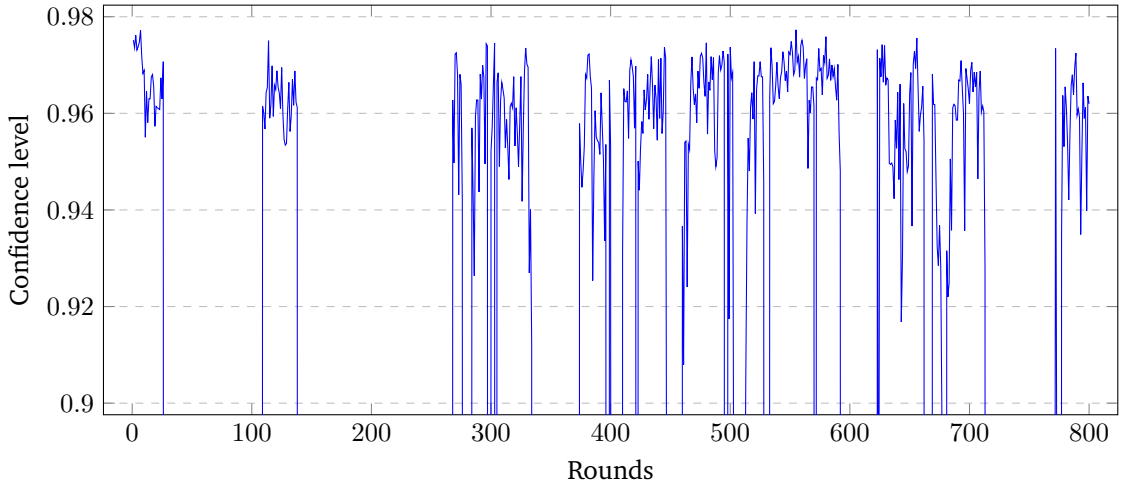


Figure 25: Scenario: busy

7.2.2 Artifacts

Results from different artifacts are shown in table 5 with additional images in figure 26. Results show that clothing such as a winter jacket does not affect the accuracy of face recognition. Neither does a cap or hood which still shows facial landmarks when used. All of those artifacts provide an accuracy of 96-97%, which is the same score as without artifacts. The only artifact which gave a change to the accuracy was the one with glasses and glasses with cap. The glasses will overlap with some facial landmarks and decrease the score around 3-6%, which will affect the decision of

setting the threshold for the solution since using glasses shall be allowed in this solution. The used references are the two best performing in section 7.1.

Figure 26: Genuine user with artifacts

Artifacts	Reference 1	Reference 2
Glasses	0.91	0.90
Glasses and cap	0.91	0.93
Cap	0.97	0.97
Hat	0.97	0.97
Jacket	0.96	0.96
Jacket and hood	0.97	0.96

Table 5: Accuracy based on data subject with artifacts

7.3 Security

7.3.1 Spoofing

The face recognition can easily be spoofed by different methods. Figure 27 shows three images where face recognition was done by a digital image from iPhone 6S which predicts the right user with a confidence of 95-96%, i.e. 1-2% lower than using a real reference. Similar results are also achieved when using printouts.

(a) 0.963 (b) 0.955 (c) 0.957

Figure 27: Spoofing using digital image

8 Discussion

8.1 Access control

Different access control rights has not been the priority or fundamental for this prototype. A workstation consists of multiple clients each running a single session. Each client doesn't have any control of the users since this is handled by the server. The server performs identification and authentication of genuine users and locks out impostors. There is no form of access control done to separate operators with different privileges. Operators working in the same control room and on the same workstations usually have many of the same authorizations which means many of the same systems and accesses can be used within one single session. There are also operational critical systems such as SCADA which usually require authentication of their own. This prototype provides only authentication into level 1 systems such as administrative and working systems which have the same type of requirements. A typical level 2 access system is a SCADA system; these usually employ the same method of authentication (username and password) as level 1, but based on a own policy. All operators need level 2 access to perform actions on SCADA systems. The prototype can also perform level 2 access control based on the same requirements as level 1. This will depend on the organization using the solution based on access control requirements of separation between level 1 and level 2 access. This means that level 2 access has to be included in the same session as level 1 and the overall system needs to be designed to support level 2 requirements. This will provided availability to critical systems but will also remove the access level hierarchy. This means that all operators need clearance and authorization for critical systems and not just for administrative and working systems.

The biggest problem will be users with administrative access or users with special privileges. Such types of access need to be controlled with username and passwords or the type of authentication already in use.

8.2 Continuous authentication and performance

Penalty and reward in this system are defined differently than as in a CA system using behavioral biometrics as described in section 5.6 and does not perform CA in accordance with the definition by e.g not using historical data. Full reward is gained when positive identification is achieved. Penalty takes effect when no person is detected by the system which triggers a timeout by decreasing the trust level (penalty) on each round. This functionality within the timeout is also used a security measure. This is because impostors knowing about the solution could perform an attack by using a paper in front of the face with holes for the eyes so as to be possible to see, without getting detected. The face recognition system will not see this as an impostor, but rather will not detect any face and will trigger a timeout since there are no data subjects to capture. This requires that a

genuine user is already logged in and further switched with an impostor within a short time range. The average round-time as described in 7.2 was 0.604 seconds. The maximum level of trust was set to 100 and the threshold between a locked and unlocked system was set to 50 which means 50 rounds that will take approximately 30 seconds before a timeout is triggered for max trust level. The CA system designed by Beunder[41] failed due to the time limit of detecting an impostor which could not be done within 10 seconds. This solution can detect impostors and genuine users for each round, but based on hardware used for the prototype (as described in section 6.1), the solution experiences a latency of 2-3 seconds. In order to meet requirements based on client performance as mentioned in section 4.2.1, it must take no more than 1 second to detect an impostor and lock the systems. Based on results on round-time and latency, the average round-time is calculated to be 0.604 seconds with some outliers above 1 second; this is within the requirements. The biggest problem is the latency, which keeps this prototype outside the required limit. The requirements are based on the SUAC3I[8] project which uses other biometric modalities for authentication such as fingerprint and iris. Locking of systems within 1 second would decrease the user friendliness of the solution. Based on the requirement of 1 second, the solution can only make one decision based on one frame to decide if the detected person is genuine or an impostor. This will provoke a unstable session causing many state changes from lock to unlock and unlock to lock. According to figure 24 and 25, there are many rounds registered with lower confidence level which could cause false negative. This means that the requirements for such a systems should be using more than 1 second to be able to use multiple rounds for decision making. This could be done by periodic authentication (PA), making decision on a block of data or by keeping the concept of penalty on detected users in addition to timeout.

The project by Beunder[41] has requirements of authentication within 10 seconds which this solution manages. 10 seconds is too much for a control room setting based on strict access control and open systems. 10 seconds allows a possible impostor to initiate actions on the system, possible actions would increase drastically with a total time of 3-4 seconds and especially at 1 second when considering physical actions on the system. The requirement on timeout of one minute can easily be calculated by the round-time and be configured there after. The CPU and RAM-usage for the clients are minimal and will not affect the client's performance; the requirement of 5% will vary depending on the hardware, but on today's computers, the solution works below 5% for the prototype. The performance on the server on the other hand requires computing power and would hopefully perform better in a real scenario on a dedicated and customized server.

8.3 Aging and database updates

Face recognition is based on feature extraction from facial landmarks. The face is not static, but changes during the lifetime of a person. Norwegian requirements for passport renewals is every 10 years for people over 16 years [48]. The need for renewals is because of the changes of the facial structure with aging. Research conducted by Ricanek and Tesafaye[26] shows that aging has a great impact on face recognition. This was tested by enrolling different users at different ages and comparing them to pictures of themselves from one to twenty years old. The age span of enrolled

users was from below 18 and up to 50, divided into four groups. The best results were in the group of 0-5 year old pictures. The PCA algorithm used for recognition performed better on identifying older people than young people. This means that people below 30 should update the reference each fifth year and people above 30 can update every 10 year to avoid false negatives. Updates should also be done when the rate of false negatives is a problem. Database updates are also needed if there are other changes in the facial structure, like scars or tattoos.

8.4 Live usage and threshold

Figure 28 shows impostors in red and the genuine user in blue. Impostors are from a large dataset and the genuine user is only represented by one single subject. Techniques such as over-fitting are not applied. The genuine statics are from only one user recorded live where the confidence level spans from 90% up to 98% as in figure 22. Impostors are not recorded live but are represented as static images as shown in figure 20 which represents a confidence level from 36% up to 95%. In addition testing of genuine users with artifacts had a great impact in scenarios where glasses were used; this decreased the confidence level by 3-6% which will have a great impact on setting the threshold. A high threshold will enable a secure system where acceptance for impostors is low, but the denial for genuine users would be higher; that will have a great impact on the availability, which is one of the main requirements. The threshold should be set by the organization using it based on risk management which focuses on these factors, but also factors such as which personnel can access the control room and which kind of physical protection measures are in place.

The system considers movement of the operator such as drinking coffee or drinking water from a bottle. This triggers penalty and will start counting down towards the level for lockout. The system will not detect a face when a cup or bottle are in front of the face or when the face is turned $45°$ right or left.

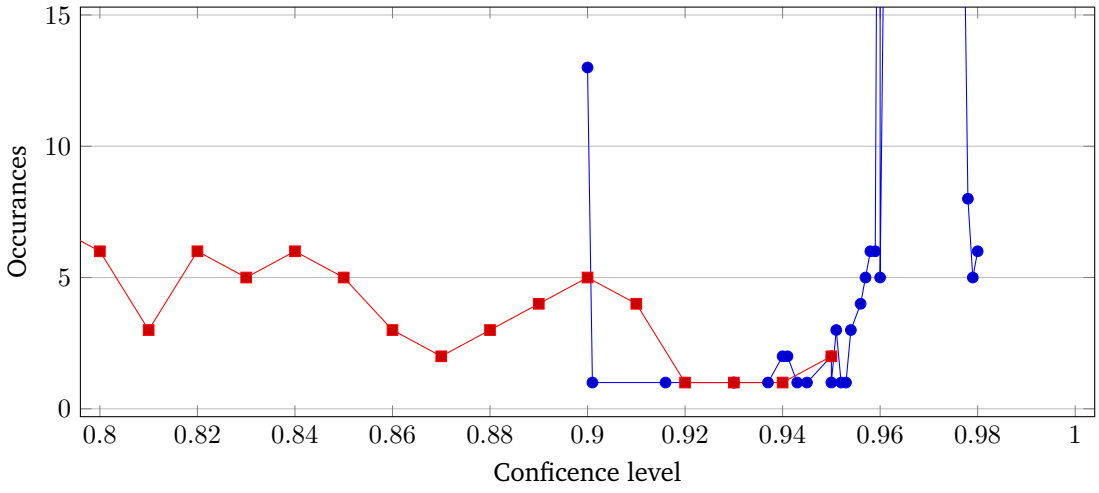


Figure 28: Confidence level of impostors and genuine user

8.5 Security

Security was only tested by performing presentation attacks. This section discusses possible measures such as presentation attack detection and the usage of several biometric modalities.

8.5.1 Presentation attack detection

As shown in chapter 7, the face recognition library OpenFace[4] can easily be spoofed by a 2D printout or another 2D representation of a bona fide image, since the reference point in a flat surface is represented equally on a paper and on a digital screen. Landmarks are shown in figure 29 which will be the same on a real person as in a spoofing attack.

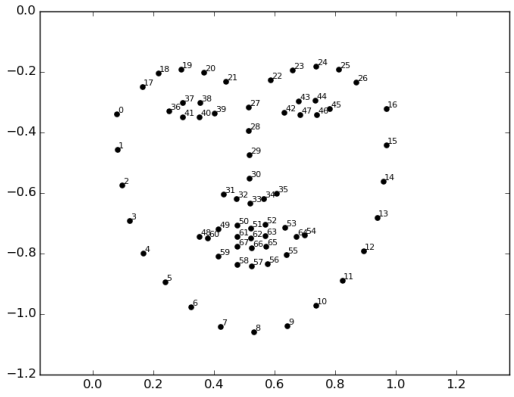


Figure 29: Landmarks [5]

A spoofing attack is when someone tries to masquerade as someone else by inputting false or manipulated data to gain illegal access. Attacks against face recognition systems can be divided into two categories[49].

- Indirect attack: inside the system, bypassing feature extraction(3 in figure 30), matching algorithms(5 in figure 30), manipulating templates(6 in figure 30) or exploiting weak point in the communications channel (2, 4, 7 and 8 in figure 30).
- Direct attack: outside the system at sensor level(1 in figure 30) by spoofing and presentation attack.

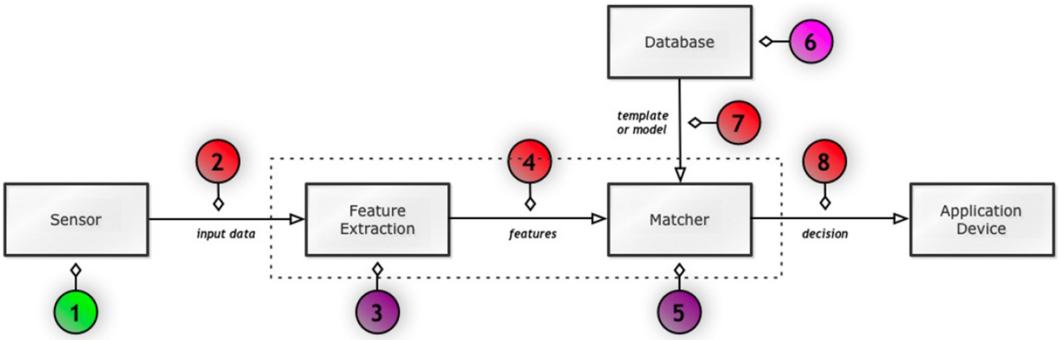


Figure 30: Possible attack vectors in a face recognition system [6]

Face spoofing can be performed as a direct attack by using methods like a printed photo, digital photo/video, 3D mask, sketch, reverse engineered image, makeup lookalike, plastic surgery or a synthetic face. The solution needs further requirements and implementation of presentation attack detection (PAD) which should be based one the following requirements[6].

- Non-invasive: should not affect the users or the users' well being.
- The process should not take too long.
- Should not decrease the performance of the solution.
- Should be simple to integrate into face recognition systems.
- Should need no additional hardware.

Presentation attack detection can further be divided into motion, image quality and hardware based methods shown as static- and dynamics software based approaches and hardware based approach in figure 31 which is from a comprehensive survey on PAD techniques by Ramachandra and Busch[7]. Software based methods involves an algorithm which can determine if the input data originates from a presentation attack of a bona fide presentation.

Static based methods by reproducing a copy of original images often lack details and characteristics such as blur and loss of sharpness. This means that the lack of high frequency information in images can be used for detection. This approach is used on single images, but can also be applied to a video sequence where each frame is analyzed. The static approach can further be divided into texture-based approaches, frequency-based and hybrid approach. The texture-based approach is based on applying filters to detect microtextural patterns in the face. It detects the presence of pigments, specular reflections and shade. This is effective for detecting a photo or display. The most known texture-based method is based on the Local Binary Pattern (LBP) proposed by Maatta et al.[50] and also successfully performed in video[51]. LBP can distinguish artificial faces based on laser print, photo print and display[7]. There also exist variations of LBP and other filtering techniques such as Gabor and Binarized Statistical Image Features (BSIF). The second type of static presentation attack detection includes frequency based analysis, such as Fourier spectrum used to detect head and hair[52], and other techniques for frequency analysis, such as Discrete Cosine

Transforms and different Gaussian filters. The hybrid method combines different methods like the research by Galbally and Marcel[53] which does quality assessment of images.

Dynamic analysis based methods compares differences between frames. A typical countermeasure of anti-spoofing based on motion is liveness detection, such as the detection of eye blinking, facial expressions and movement of the mouth[6], which is described as motion based. Dynamic motion based on texture is also based on LBP, where the change of texture changes across video frames. The combination of motion- and texture based features is the hybrid approach, such as e.g. in the research by Junjie et al.[54] that uses multiple scenic cues.

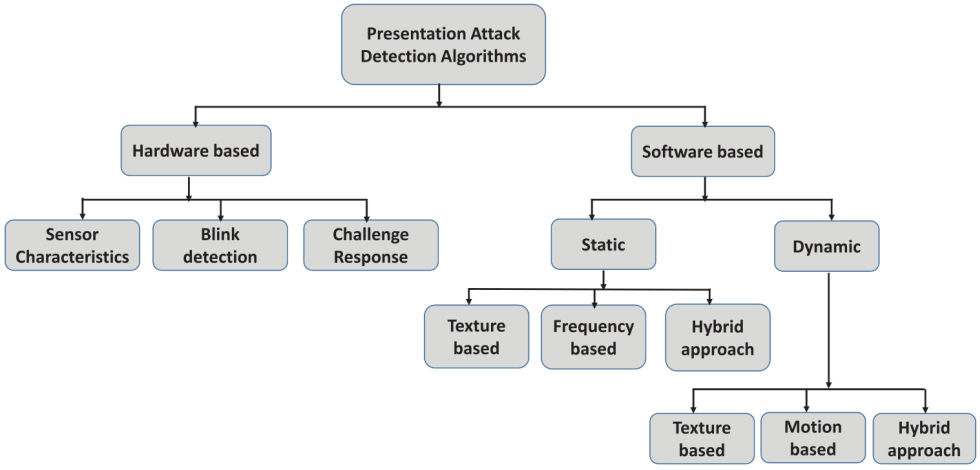


Figure 31: Presentation attack detection methods [7]

Hardware-based methods include non-conventional hardware which is able to acquire information about shapes and reflections from faces. Sensor characteristics are based on using characteristics of the camera. Depth sensors can detect planar surfaces such as a 2D printout or a digital screen. Multi-spectral imaging can be used to distinguish 2D print or 3D mask artifacts from the human skin which has a low property of reflection in the upper-band near infrared spectrum (NIR). Detection of photo and a digital screen can be done by using a light field camera (LFC) which records both direction and intensity of the incoming light rays. This was explored by Ramachandra et al.[55] using a photo print, laser print and a digital screen from an iPad where the focus variation is high when comparing real and artificial images. The multispectral sensor proposed by Li et al.[56] is also tested on real and artificial faces from a 3D mask, photo print, laser print and photo displayed from an iPad. This also helps to detect presentation attacks in a multispectral face recognition system. Use of a multispectral or LFC sensor can detect several attacks, the biggest limitation being the high cost of the sensor and the need for computational power. Eye blinking is described as a dynamic software approach, which can be implemented as hardware and can be effective to detect attacks performed with a static photo, but also easy to attack using a video replay of the user and using a 3D mask with the eye region open. The idea behind the challenge and response method is to give

the user a task like moving the gaze[57]. This method decreases the usability and user friendliness for a face recognition system but is effective against photo and display attacks[7]. It also needs dedicated hardware, user interaction and computational power. Use of hardware based methods may provide presentation attack detection for photo, display and video replay. The common limitations are the need for computational power and the cost.

Implementation of a presentation attack detection system will add additional hardware or increase the computational cost since there always will be something additional to do, like reading images from multiple cameras or adding different filters and further analyzing them. Since the solution uses continuous authentication and face recognition, the critical factor will be the computational cost which will be a factor in all PAD methods already mentioned. Ramachandra and Busch[7] evaluated different software based PAD algorithms against 2D attacks using the CASIA face spoof database[58] which includes low (front camera on a smartphone or low-price webcamera), medium (CCTV, back camera on a midrange smartphone or the frontcamera at a high-end smartphone) and high quality (camera at border controls) images from three different cameras in addition to print, wrap, and digital displayed images. Attack presentation classification error rate (APCER) and Bona fide presentation classification error rate (BPCER) were used as performance metrics. APCER is the proportion of attacks using the same presentation attack instrument (PAI) species incorrectly classified as bona fide presentations. BPCER is the proportion of bona fide presentations incorrectly classified as attacks. There is no single answer and only one perfect algorithm to use, but rather one specific algorithm which gives a better score than another algorithm depending on the specific purpose. Local binary pattern (LBP) by Chingovska et al.[51] gave the best score on print, wrap, and displayed images using low resolution image as input. Binarized Statistical Image Features(BSIF) by Raghavendra and Busch[59] on medium quality and for high quality, multi-level local phase quantization (ML-LPQ) by Benlamoudi et al.[60] had the best score on print and digital images while image distortion analysis by Wen et al.[61] had the best results on wrap photos. Hardware-based algorithms were not tested since they often are tailored to a specific type of hardware. The prototype for this solution uses a medium-level camera where Binarized Statistical Image Features(BSIF) by Raghavendra and Busch[59] would have the best PAD performance in use. Presentation attack detection algorithms are often developed to countermeasure a specific purpose which is the reason why there is not one specific algorithm that works better than others on different type of attacks. There exists a wide range of attacks as described in figure 31 where these algorithm could help to provide more security at the sensor level by detecting 2D attacks, but they are not tested against more sophisticated attacks such as 3D faces and masks.

8.5.2 Multimodal biometric system

A multimodal biometric system is the combination of several biometric modalities used for authentication. The different modalities capture more than one modality e.g. a system which combines iris and face recognition, even when both data are captured with the same device. Both the research conducted by Schiavone et al.[35] and the SUAC3I project[8] are examples of multimodal biometric systems. Both use the modalities separately, which means that the user does not need to

perform authentication by several biometric modalities. This means that the systems does not perform score fusion of different biometric modalities. The use of a multimodal biometric system could increase the security if implemented with score level fusion. This requires use of several modalities to perform authentication, but it could decrease the level of user friendliness and availability for the solution. This is true if the user needs to do a specific task to login, such as scanning the finger for a fingerprint or performing voice recognition. A multimodal solution is also possible using the existing technology by performing both face- and iris recognition using the same camera. This will not work for the prototype with a medium quality camera; this needs to be upgraded to a high quality camera to capture the iris. The solution would also need a backup plan for authentication if something went wrong with the face recognition system.

9 Conclusion

The research objective was to verify whether biometrics can be used to improve authentication in critical infrastructure control rooms and if continuous authentication can provide traceability, in addition to increasing availability for operators and to providing a solution with strict access control which only allows the right users into the systems, all together in a user-friendly, easy to use solution. The solution uses face recognition in combination with continuous authentication to automate access control. OpenFace, an open source face recognition tool was used as the biometric modality. The solution proposed a completely new architecture where access control is performed at one central server instead of locally at each client. The solution provides availability by doing continuously face recognition of operators, and by moving decision-making from the clients to a central server at each workstation. Traceability is enabled by performing identification of users rather than verification of user-accounts, which offers no guarantee of the user being verified. Strict access control is done by setting a high threshold for face recognition, accepting a low number of false positives. Strict access control is also supported by continuous authentication, that decides if a detected user is genuine or an impostor every 0.6 second on average. The solution is easy to use since it doesn't require any form of physical contact or some specific activity to work properly, and the rate of acceptability is high. Emergency lock and unlock is a important part of availability; it completely overrides authentication rules when an emergency situation occurs. The biggest problem of the solution is the possibility of launching presentation attacks which can be done by a digital- or print-out representation of a bona fide image. The outcome of this thesis is a step in the process of re-thinking how access control is managed inside control rooms for critical infrastructures. Focusing on strict requirements is still possible, while having open and available systems. This will hopefully engage other researchers in a new direction of doing authentication and identification in the critical infrastructure sector.

9.1 Future Work

As described in section 6 the prototype was tested by using a single computer with webcam using virtual machines to represent multiple clients. The solution should also be tested in a control room. There should be performed scenario tests to verify the camera position and the type of camera to fit the environment. A classic web-camera will not capture wide enough a picture or the distance will be too large to capture high quality facial features. An operation environment should also be provoked to verify the time before timeout and the friendliness of the solution.

9.1.1 Access control

The prototype of this solution uses one single user session at each client for all users. This means that all users need the same type of clearance and authorization for accessesing the systems. This

could be a problem in a control room with users with multiple different privileges. This problem can be solved by moving the centralized authentication from the server to each client.

9.1.2 Enrollment and template creation

As mentioned in section 8.4, the confidence level is reduced by 3-6% when a genuine user with glasses is compared with the reference where the template is created with facial images without glasses. Such a difference in the confidence level could be critical when setting a strict threshold; this could be necessary depending on the requirements set for control room authentication. This means that operators cannot use glasses at work, as these are in the way for some facial features which cannot in this case be extracted. This problem needs to be addressed on a possible solution to be used in production. This can be tested by generating 3 different templates:

- With glasses
- Without glasses
- Mixture with and without glasses

A genuine user should be compared against all references to see if there are differences in the confidence level between references.

9.1.3 Centralized solution

As the architecture is defined for the prototype in section 5, there exists one server for each workstation which handles the authentication. There is no centralized database for template storage. If a control room has multiple workstations, multiple servers are needed and all references need to be duplicated. The architecture could be expanded, as it is designed as a tree structure. A control room with multiple workstations can have a centralized server and database which handles all references for the authentication server at each workstation. Or an organization with multiple control rooms can expand, by running a centralized server and database which handles user accounts on behalf of every control room.

9.1.4 Presentation attack detection

A complete solution using face recognition should have implemented PAD in its implementation. What type of PAD that should be used will depend on the implementation and what would give best results and performance for the solution. Recommendations and different types of PAD are discussed in section 8.5.1.

Bibliography

[1] Jain, A. K., Ross, A., & Prabhakar, S. Jan 2004. An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1), 4–20. doi:10.1109/TCSVT.2003.818349.

[2] Pursiainen, C., Lindblom, P., & Francke, P. *Towards a Baltic Sea Region Strategy in Critical Infrastructure Protection*, chapter 1, 6–33. Nordregio, 2007.

[3] Anna, S. & Konstantinos, M. *Stocktaking, Analysis and Recommendations on the Protection of CIIs*, chapter 1, 9–15. ENISA.

[4] Amos, B., Bartosz, L., & Satyanarayanan, M. Openface: A general-purpose face recognition library with mobile applications. Technical report, CMU-CS-16-118, CMU School of Computer Science, 2016.

[5] Amos, B. 2017. Openface website. https://cmusatyalab.github.io/openface/. Accessed: 26.02.2018.

[6] Li, L., Correia, P. L., & Hadid, A. 2018. Face recognition under spoofing attacks: countermeasures and research directions. *IET Biometrics*, 7(1), 3–14. doi:10.1049/iet-bmt.2017.0089.

[7] Ramachandra, R. & Busch, C. March 2017. Presentation attack detection methods for face recognition systems: A comprehensive survey. *ACM Comput. Surv.*, 50(1), 8:1–8:37. URL: http://doi.acm.org/10.1145/3038924, doi:10.1145/3038924.

[8] SUAC3I. Secure user authentication in control centers for critical infrastructures. 2011.

[9] Ics-cert annual assessment report 2016. Technical report, NCCIC.

[10] Information technology — vocabulary — part 37: Biometrics. Standard, International Organization for Standardization, Geneva, CH, February 2017.

[11] Ratha, N. K., Connell, J. H., & Bolle, R. M. 2001. Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, 40(3), 614–634. doi:10.1147/sj.403.0614.

[12] Bours, P. 2012. Continuous keystroke dynamics: A different perspective towards biometric evaluation. *Information Security Technical Report*, 17(1), 36 – 43. Human Factors and Biometrics. doi:10.1016/j.istr.2012.02.001.

[13] Nist special publication 800-63b - digital identity guidelines. authentication and lifecycle management. Technical report, NIST.

[14] Mondal, S. & Bours, P. March 2017. A study on continuous authentication using a combination of keystroke and mouse biometrics. *Neurocomput.*, 230(C), 1–22. doi:10.1016/j.neucom.2016.11.031.

[15] Bours, P. & Mondal, S. 2015. Performance evaluation of continuous authentication systems. *IET Biometrics*, 4(4), 220–226. doi:10.1049/iet-bmt.2014.0070.

[16] Singh, S. & Yamini, M. July 2013. Voice based login authentication for linux. In *2013 International Conference on Recent Trends in Information Technology (ICRTIT)*, 619–624. doi:10.1109/ICRTIT.2013.6844272.

[17] Fernandez-Lopez, P., Liu-Jimenez, J., Sanchez-Redondo, C., & Sanchez-Reillo, R. Oct 2016. Gait recognition using smartphone. In *2016 IEEE International Carnahan Conference on Security Technology (ICCST)*, 1–7. doi:10.1109/CCST.2016.7815698.

[18] Messerman, A., Mustafić, T., Camtepe, S. A., & Albayrak, S. Oct 2011. Continuous and non-intrusive identity verification in real-time environments based on free-text keystroke dynamics. In *2011 International Joint Conference on Biometrics (IJCB)*, 1–8. doi:10.1109/IJCB.2011.6117552.

[19] Feher, C., Elovici, Y., Moskovitch, R., Rokach, L., & Schclar, A. 2012. User identity verification via mouse dynamics. *Information Sciences*, 201, 19 – 36. doi:10.1016/j.ins.2012.02.066.

[20] Bryan, W. L. & Harter, N. 1897. Studies in the physiology and psychology of the telegraphic language. 4(1), 27–53.

[21] Pankanti, S., Prabhakar, S., & Jain, A. K. Aug 2002. On the individuality of fingerprints. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 24(8), 1010–1025. doi:10.1109/TPAMI.2002.1023799.

[22] Raghavendra, R. & Busch, C. 2014. Novel image fusion scheme based on dependency measure for robust multispectral palmprint recognition. *Pattern Recognition*, 47(6), 2205 – 2221. doi:10.1016/j.patcog.2013.12.011.

[23] Bowyer, K. W., Chang, K., & Flynn, P. 2006. A survey of approaches and challenges in 3d and multi-modal 3d + 2d face recognition. *Computer Vision and Image Understanding*, 101(1), 1 – 15. doi:10.1016/j.cviu.2005.05.005.

[24] Daugman, J. 2002. How iris recognition works. *IEEE Transactions on Circuits and Systems for Video Technology*, 14, 21–30.

[25] Srivastava, S. & Sudhish, P. S. Dec 2016. Continuous multi-biometric user authentication fusion of face recognition and keystoke dynamics. In *2016 IEEE Region 10 Humanitarian Technology Conference (R10-HTC)*, 1–7. doi:10.1109/R10-HTC.2016.7906823.

[26] Ricanek, K. & Tesafaye, T. April 2006. Morph: a longitudinal image database of normal adult age-progression. In *7th International Conference on Automatic Face and Gesture Recognition (FGR06)*, 341–345. doi:10.1109/FGR.2006.78.

[27] Jafri, R. & Arabnia, H. R. 06 2009. A survey of face recognition techniques. 5, 41–68.

[28] Lawrence, S., Giles, C. L., Tsoi, A. C., & Back, A. D. Jan 1997. Face recognition: a convolutional neural-network approach. *IEEE Transactions on Neural Networks*, 8(1), 98–113. doi:10.1109/72.554195.

[29] Luiijf, E. *Understanding Cyber Threats and Vulnerabilities*, 52–67. Springer Berlin Heidelberg, Berlin, Heidelberg, 2012. doi:10.1007/978-3-642-28920-0_4.

[30] Marinos, L. Enisa threat taxonomy 2016 - a tool for structuring threat information. Technical report, ENISA, January.

[31] Veiledning til forskrift om forebyggende sikkerhet og beredskap i energiforsyningen (beredskapsforskriften). http://publikasjoner.nve.no/veileder/2013/veileder2013_01.pdf. Accessed: 23.04.2018.

[32] Inductive automation: What is scada? https://inductiveautomation.com/what-is-scada. Accessed: 02.02.2018.

[33] Zhu, B., Joseph, A., & Sastry, S. Oct 2011. A taxonomy of cyber attacks on scada systems. In *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*, 380–388. doi:10.1109/iThings/CPSCom.2011.34.

[34] Alcaraz, C. & Zeadally, S. 2015. Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection*, 8, 53 – 66. doi:10.1016/j.ijcip.2014.12.002.

[35] Schiavone, E., Ceccarelli, A., & Bondavalli, A. *Continuous User Identity Verification for Trusted Operators in Control Rooms*, 187–200. Springer International Publishing, Cham, 2015. doi:10.1007/978-3-319-27161-3_17.

[36] Taigman, Y., Yang, M., Ranzato, M., & Wolf, L. June 2014. Deepface: Closing the gap to human-level performance in face verification. In *2014 IEEE Conference on Computer Vision and Pattern Recognition*, 1701–1708. doi:10.1109/CVPR.2014.220.

[37] Schroff, F., Kalenichenko, D., & Philbin, J. June 2015. Facenet: A unified embedding for face recognition and clustering. In *2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 815–823. doi:10.1109/CVPR.2015.7298682.

[38] Huang, G. B., Ramesh, M., Berg, T., & Learned-miller, E. Labeled faces in the wild: A database for studying face recognition in unconstrained environments.

[39] Openbr - open source biometric recognition. https://openbiometrics.org. Accessed: 10.05.2018.

[40] Kumar, N., Berg, A. C., Belhumeur, P. N., & Nayar, S. K. Sept 2009. Attribute and simile classifiers for face verification. In *2009 IEEE 12th International Conference on Computer Vision*, 365–372. doi:10.1109/ICCV.2009.5459250.

[41] Beunder, K. M. 2014. Design of continuous authentication using face recognition. In *Twente Student Conference on IT*.

[42] Wati, D. A. R. & Abadianto, D. Nov 2017. Design of face detection and recognition system for smart home security application. In *2017 2nd International conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE)*, 342–347. doi:10.1109/ICITISEE.2017.8285524.

[43] Rajiv, P., Raj, R., & Chandra, M. 2016. Email based remote access and surveillance system for smart home infrastructure. *Perspectives in Science*, 8, 459 – 461. Recent Trends in Engineering and Material Sciences. doi:10.1016/j.pisc.2016.04.104.

[44] Lov om behandling av personopplysninger (personopplysningsloven). https://lovdata.no/dokument/NL/lov/2000-04-14-31. Accessed: 05.02.2018.

[45] Høringsnotat ny personopplysningslov - gjennomføring av personvernforordningen i norsk rett. Accessed: 05.02.2018. URL: https://www.regjeringen.no/no/dokumenter/horing-om-utkast-til-ny-personopplysningslov--gjennomforing-av-personvernforordningen-i-norsk-rett/id2564300/.

[46] Dragerengen, K. A review of authentication solutions for control rooms in critial infrastructure. Dec 2017.

[47] Malatras, A., Geneiatakis, D., & Vakalis, T. Nov 2017. On the efficiency of user identification: a system-based approach. *International Journal of Information Security*, 16(6), 653–671. doi:10.1007/s10207-016-0340-2.

[48] Norwegian police website. https://www.politiet.no/tjenester/pass/soke-om-pass/. Accessed: 05.03.2018.

[49] Hadid, A. June 2014. Face biometrics under spoofing attacks: Vulnerabilities, countermeasures, open issues, and research directions. In *2014 IEEE Conference on Computer Vision and Pattern Recognition Workshops*, 113–118. doi:10.1109/CVPRW.2014.22.

[50] Määttä, J., Hadid, A., & Pietikäinen, M. Oct 2011. Face spoofing detection from single images using micro-texture analysis. In *2011 International Joint Conference on Biometrics (IJCB)*, 1–7. doi:10.1109/IJCB.2011.6117510.

[51] Chingovska, I., Anjos, A., & Marcel, S. Sept 2012. On the effectiveness of local binary patterns in face anti-spoofing. In *2012 BIOSIG - Proceedings of the International Conference of Biometrics Special Interest Group (BIOSIG)*, 1–7.

[52] Liu, W. July 2014. Face liveness detection using analysis of fourier spectra based on hair. In *2014 International Conference on Wavelet Analysis and Pattern Recognition*, 75–80. doi:10.1109/ICWAPR.2014.6961294.

[53] Galbally, J. & Marcel, S. Aug 2014. Face anti-spoofing based on general image quality assessment. In *2014 22nd International Conference on Pattern Recognition*, 1173–1178. doi:10.1109/ICPR.2014.211.

[54] Yan, J., Zhang, Z., Lei, Z., Yi, D., & Li, S. Z. Dec 2012. Face liveness detection by exploring multiple scenic clues. In *2012 12th International Conference on Control Automation Robotics Vision (ICARCV)*, 188–193. doi:10.1109/ICARCV.2012.6485156.

[55] Ramachandra, R., Raja, K. B., & Busch, C. March 2015. Presentation attack detection for face recognition using light field camera. *IEEE Transactions on Image Processing*, 24(3), 1060–1075. doi:10.1109/TIP.2015.2395951.

[56] Yi, D., Lei, Z., Zhang, Z., & Li, S. Z. *Face Anti-spoofing: Multi-spectral Approach*, 83–102. Springer London, London, 2014. doi:10.1007/978-1-4471-6524-8_5.

[57] Ali, A., Deravi, F., & Hoque, S. 2013. Directional sensitivity of gaze-collinearity features in liveness detection. In *Proceedings of the 2013 Fourth International Conference on Emerging Security Technologies*, EST '13, 8–11, Washington, DC, USA. IEEE Computer Society. doi:10.1109/EST.2013.7.

[58] Zhang, Z., Yan, J., Liu, S., Lei, Z., Yi, D., & Li, S. Z. March 2012. A face antispoofing database with diverse attacks. In *2012 5th IAPR International Conference on Biometrics (ICB)*, 26–31.

[59] Raghavendra, R. & Busch, C. Sept 2014. Presentation attack detection algorithm for face and iris biometrics. In *2014 22nd European Signal Processing Conference (EUSIPCO)*, 1387–1391.

[60] S. Benlamoudi, A. Ouafi, A. B. T.-A. A. & Hadid, A. Nov 2015. Face spoofing detection using multi-level local phase quantization (ml-lpq). doi:10.13140/RG.2.1.3335.6241.

[61] Wen, D., Han, H., & Jain, A. K. April 2015. Face spoof detection with image distortion analysis. *IEEE Transactions on Information Forensics and Security*, 10(4), 746–761. doi:10.1109/TIFS.2015.2400395.