Proximity based authentication mechanisms and their use cases in autonomous factories

Seminar - Offensive and Defensive Measures in Wireless Security

Daniel Christian Mayer
School of Computation, Information and Technology (CIT)
Technical University Munich
Munich, Germany
daniel.ch.mayer@tum.de

***Abstract*—Security in information technology is getting a more relevant topic since the beginning of the first computers. Our modern Information society relies on billions of computer chips worldwide. The massive amounts of consumed goods by over 8 Billion people requires more efficient ways of production. Therefore, Germany introduced the term of Industry 4.0, the fourth Industrial revolution. Computers already revolutionized the way we produce goods, but high connectivity and developments of self-learning and self-optimizing systems are about to revolutionize Industry again.**

Security is a critical topic, due to the high amount of connections and high level integration of computers into our modern production infrastructure. Integrating appropriate authentication mechanisms into the workflows of our infrastructure is a central part of a strong cyber security.

We are analyzing possible requirements in autonomous factories and proximity based authentication mechanisms. Afterwards we will try to integrate proximity based authentication mechanisms with some of those requirements to provide a more secure production environment.

We were able to combine some of the technologies used in autonomous factories with proximity based authentication mechanisms.

Most authentication mechanisms fitting best for machine to machine communication are radio based. On the other hand best fitting mechanisms for human to machine authentication are often biometrics based.

***Index Terms*—IoT, Industry 4.0, Proximity based authentication, Autonomous factories**

I. Introduction

The first question is, what is the problem to deal with? The main problem is to create a flexible and reliable production environment the society can rely on, but why do we need this? Our environment is getting more personalised. For example personalised ads or more possibilities to get special goods more quickly through online shops. Production is getting more streamlined in order to pay less for storage capacity with tactics like "just in time delivery" of raw materials and increasing connectivity. Everyone tries to work more efficient and increase their economics, but even with streamlined production lines the amount of needed goods is still getting estimated by humans. It would be more efficient to produce just the goods which are really needed, so just goods which got ordered. Also it would be more efficient if the production would happen automatically in order to reduce costs for personal and in order to reduce production time. We have now shown why we need a flexible production environment, but why does it need to be reliable? Many goods are necessary to ensure a human standard of living and if an ordered good is not getting delivered, customers will try to buy them somewhere else. An important part of reliability is security. Hackers for example are always trying to attack critical infrastructure. An important part of security is authentication. For this reason we are trying to provide a concept for a more secure production environment.

There are analyses and concepts about proximity based authentication mechanisms and there are analyses and concepts about autonomous factories. To ensure a deep integration of security into a system, the system should be designed with security already in mind. Because of authentication being an important part of security, authentication mechanisms should be already integrated at the concept phase of autonomous factories. In order to make this integration easy to comprehend we will first define autonomous factories and proximity based authentication. Afterwards, a general explanation of the most important attacks is given in order to approach the fusion of technologies from the security side. The contents of the most important related works is presented afterwards. A section about the requirements of autonomous factories and their implications will approach the fusion from the production side, followed by a survey which proximity based authentication mechanisms exist and could be used. After approaching the integration of both technologies we will show possibilities to combine authentication mechanisms into autonomous factories and evaluate said possibilities. A conclusion is given at the end in order to sum up the most important findings.

While most of the analysis are well done for each technology, their combination is not sufficiently researched. We will combine the technologies in the following sections.

II. Background

We have shown why the problem is important, now we will provide the necessary background knowledge in order to make

redd.

empty sentence

so now the focus is on production efficiency?, first it was ads ?

it more easy to understand later sections.

A. Definition of autonomous factories

No general definition of autonomous factories, which generally applies, has been published yet [1].

In this paper we define autonomous factories as facilities, which are working without human interaction within the process of production. In some cases, these facilities are fully self-controlled and self-optimizing.

B. Definition of authentication

We define authentication as the process of identifying an entity. This entity could either be a human or a machine.

C. Definition of proximity based authentication

Really???

We could not find any suitable definition of proximity based authentication in our research, most definitions define proximity based authentication only for persons as users. For this reason we define our own definition of proximity based authentication.

Proximity based authentication is a type of authentication which requires proximity to verify the identity of an entity. This entity could for example be a person or a device.

D. Explanation of Attacks

We will shortly describe the general attack types which are getting mentioned later, in order to make the following sections more easy to understand.

1) Jamming attacks: In general the goal of a Jamming attack is to put a certain system out of function. This is achieved by interrupting the communication of the system at some point. Considering a wireless sensor network, a sensor could be jammed by manipulating the sensor data itself or by interrupting the transmission of the data. Jamming attacks are often part of a larger attack. For example, jamming the signals of sensors of an alarm system could be part of breaching physical security.

2) Eavesdropping attacks: The goal of an Eavesdropping attack is not to directly disturb a system. The goal is to get information about the system, which can later be used to attack the system. Therefore, eavesdropping is also often a part of larger attacks. For example recording a BLE beacon or an RFID Token can later be used for a replay attack.

3) Replay attacks: A replay attack has the goal to deceive a system to do something by presenting a copy of the original entity. An entity could in this context be a BLE Beacon, biometrics or anything which can be copied. For example ~~presenting a copied RFID Token to authenticate to the system would be a replay attack.~~ cloneing attack, so Wrong!

III. Related Work

We have shown the important background knowledge. We will now give a quick overview of already published papers in order to show the new findings of this paper.

The first important paper on a subarea of our topic is a survey on proximity based authentication mechanisms in [2]. It is used as a base for our survey of useful proximity based authentication mechanisms. It sums up most of the proximity based authentication mechanisms in clear categories.

The second paper to mention is the literature review of Industry 4.0 and related technologies [1]. It shows a wide overview of papers related to Industry 4.0 and is used to survey the second subarea.

Another important paper is the overview of current technologies and emerging trends in factory automation [3]. We used this paper to isolate technological areas of autonomous factories which are important for security reasons and therefore need to implement proximity based authentication mechanisms.

We could not find a paper regarding the topic of this paper in our survey. The new findings of this paper are how proximity based authentication mechanisms can be combined with technologies from autonomous factories in order to create a more secure production environment. We will do these combinations in the following section.

IV. Autonomous Factories

We have now provided necessary background knowledge and shown related work. We will now approach the integration of authentication mechanisms from the production side and show necessary requirements and their implications.

We are using [3] to get an overview of interesting technologies and workflows which could require proximity based authentication. We will further analyze and explain the requirements in the next sections.

A. Requirements existing in autonomous factories

According to [3] we isolated the following relevant topics, spitted in technological areas and requirements:

1) Advanced manufacturing processes and technologies
   a) Flexibility — only one source??
   b) Product traceability
   c) Resource efficency
2) Mechatronics for advanced manufacturing systems
   a) Adaptivity
   b) Modularity and re-configurability
3) Information and communication technology
   a) Connectivity
4) Skills and knowledge of workers
   a) Human-Robot interaction
   b) State knowledge for maintenance staff

B. Implications of the above isolated requirements

We are now going to talk about the implications of the above isolated requirements. We will list the implications by requirement.

Flexibility: Machine parameters need to be changed quick. This may be the case because the flow of orders is unpredictable or orders change while they are already in production [3]. Also maintenance staff needs to be able to change parameters from inside a factory in case of technical

errors.

Product traceability: Products need to be traceable ensure quality for example. To accomplish traceability, products must be clearly identifiable.

Resource efficiency: Sensors and actuators are necessary to monitor different parameters and situations, for example available resources or power consumption. These entities need to communicate securely to transfer their collected data.

Adaptivity: Machines need to adapt themselves to new boundary conditions, for example other raw materials. Therefore the boundary conditions need to be verified to avoid unintentional behavior. but is this nec. auth?

Modularity and re-configurability: Systems of machines need to be re-configurable. According to [3] these machines are controlled decentralized and therefore need to communicate with each other, to make decisions, depending on the status of the different production subsystems.

Connectivity: Connections need to be established quickly and securely between mobile entities, for example mobile work piece carriers [3]. We mention this requirement separately because spontaneous communication is meant in particular.

Human-Robot interaction: Humans need to interact with machines sometimes. Therefore the human entity needs to be authenticated before allowing interaction with production systems.

State knowledge for maintenance staff: Maintenance staff needs to be authenticated and granted access to the systems information and controls of the factory.

V. Proximity based authentication mechanisms, a survey

We have approached the integration of authentication mechanisms from the production side and will now approach it from the security side.

In the following we will perform a survey of proximity based authentication mechanisms, which are useful in the context of this paper. We will do the survey based on [2]. In general, proximity based authentication can be part of larger authentication mechanisms. For example multi-factor authentication systems to authenticate a person as user.

In order to evaluate and compare the methods properly and to make the methods easy to understand, we will describe the basic functionality, possible range, required hardware and possible events to disturb the mechanisms. The required Hardware is fitting for most applications, but additional or less required hardware is possible. Also the disturbance can be intended or unintended. The list of disturbances is not exhaustive. We will not use parameters like false positives or false negatives, because we can not provide this data for all reviewed methods properly. An overview of all mechanisms is given in I.

A. Wire based

why?how?

The most reliable way of authenticating is via wire, but this method is not as flexible as all wireless methods. Besides that, this paper concentrates on wireless authentication mechanisms, so we will ignore this method.

B. Radio based

The probably most spreaded technique for wireless authentication is radio based authentication. We will pick out those mechanisms, which work with proximity as authentication factor.

There are many techniques which use radio based proximity as authentication mechanism. The received signal strength (RSS) and the radio channel statistics are often used to prove authenticity [2]. Again only one source!

Radio channel statistics could for example be the signal-to-noise ratio. In general physical parameters of the radio channel are meant. ToF?

Radio frequency identification (RFID) is a technique, which transmits data over very low ranges due to the underlying physics. RFID can either be passive or active, where passive RFID tokens get powered by induction of the RFID reader and active tokens have an own power source. The induction of the power to the token limits the range of the transmission. Also the transmission power of an active token limits the range to authenticate. These physical barriers could be extended from several centimeters to up to 10 meters [2] by using antennas with high gain, either on reader side or token side. However, antennas with high gain can just be used to increase the signal range, passive tokens still need to get powered by induction, which at this point is just possible at up to one meter. Additional security to RFID can be added by using cryptographic mechanisms, such as symetric or asymetric key pairs to encrypt usage data. Near field communication (NFC) is a further development of RFID, so the above described security also applies for NFC. NFC is for example used for credit cards.

Bluetooth low energy (BLE) is a radio based protocol, which transmits on 2,4 GHz with low data rates. It is limited in range due to the low transmission powers. At maximum transmit power, BLE could reach several tens of meters at line of sight. The MASHaBLE Application as described in [4] implements a proximity based authentication mechanism on top of BLE. BLE ist just SRRI!

Another protocol to mention, named AMIGO Authentication is described in [5]. A more basic research is done by [6]. Due to the wireless range, this protocol is also bound to proximity. It combines a Diffie-Hellman Key exchange with a co-location check based on the same ambient

Basic mechanism	Range	Required hardware	Disturbances
Radio (Channel statistics)	several meters	• Same radios	• Jamming • Eavesdropping
Radio (RFID)	up to 10 meters	• Token (passive or active) • Reader	• Jamming • Replay Attacks • Eavesdropping
Radio (MASHaBLE/BLE)	several meters	• 2,4 GHz Radio	• Jamming • Eavesdropping
Radio (Amigo)	several meters	• Same radios	• Jamming • Eavesdropping
Radio (move2auth)	around 20 centimeters	• Same radios	• Jamming
Audio	several meters	• Speakers • Microphone	• Jamming • Replay Attacks • Eavesdropping
Light	almost unlimited	• Light emitter (for example LED, Laser) • Sensor (for example camera)	• Jamming • Replay Attacks • Eavesdropping
Biometrics	several meters	• Light emitters • Sensors (for example camera, ultrasound, microphone)	• Jamming • Replay Attacks (for example Portrait for Facial scanners, printed finger for fingerprint scanner)
Physical access	direct contact	• sensors (for example button, capacitive touch)	• breaching physical security

TABLE I
OVERVIEW OF PROXIMITY BASED AUTHENTICATION MECHANISMS.

radios. These Ambient radios are fluctuating and therefore hard to predict at a certain location.

According to [7], radio based authentication could also be implemented by a motion pattern, detected trough the radios whithin the communicating devices. The implemented method is called move2auth.

C. Audio based

Audio based authentication is a way of authenticating via audio waves through a medium, such as air or water. There are many possibilities to authenticate via audio, for example a special frequency or a pulse sequence. An overview of possible methods is shown in figure 1. Acoustic based authentication is also bound to physical barriers, such as output power of the speakers, ambient noise and quality of the microphone. It can be used up to several meters [2].

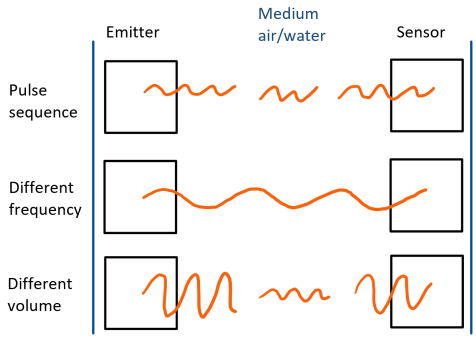

Fig. 1. Possible mechanisms for audio based authentication

D. Light based

Light based authentication uses light waves. These do not require a medium like audio. Depending on the frequency range of the light, the type of light used, like mixed light or lasers and the output power, the range is very different. Light based authentication is very precise due to the direction of the emitting device [2]. Light proximity based authentication mechanisms could be a special light frequency, a pulse

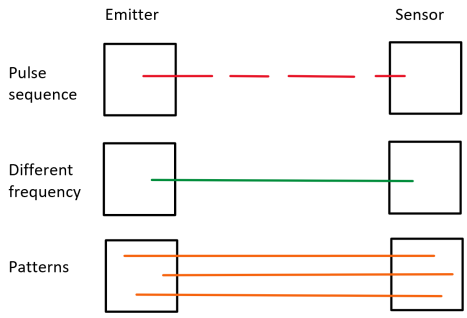

Fig. 2. Possible mechanisms for light based authentication

sequence or a pattern like a quick response (QR) code. An overview of possible mechanisms is shown in figure 2. For example a barcode or a QR code authenticates a product in the supermarket to the cash register. The code on the product is a passive token, which can be read by sending out light, in most cases a laser beam and reading the reflections of the token.

Other subsections of light based authentication would be Image based authentication and gesture based authentication as described in [2].

E. Biometric based

Known biometric based authentication mechanisms are a combination of light and sound based authentication mechanisms. Possible biometric markers would be fingerprints, voice, face and eyes. For all of those markers the above described physical barriers apply. For this reason biometrics is proximity based authentication to a maximum of several meters.

F. Physical based

Proximity based authentication based on physical access is also a method of authenticating. For example Wireless Protected Setup (WPS) is a protocol to initiate wireless local area network (WLAN) connections, which requires the user to push a button on the access point (AP) device. To be able to do this, the user needs physical access to the WLAN AP and therefore, the authentication requires access to the devices.

G. Countermeasures against disturbances

In the following sections we will present general counter-measures against certain disturbances. This should give the reader a better understanding how security measures could be implemented. connection?

1) Countermeasures against Jamming: In order to Jam a system, some kind of physical access is required. Depending on which part of the target system which should be jammed, different access is necessary. For example in case of a wireless sensor network, the attacker has to be close enough to transmit a strong enough noise in order to overlap other radio signals. Two possible countermeasures would be securing a large enough area to prevent this or shielding the facility in order to block radio signals from passing the outer walls or ceilings.

2) Countermeasures against Eavesdropping: To prevent eavesdropping, the attacker must not be allowed to get physically close to the protected systems. Radio signals from a facility should be blocked as described above. BLE Beacons or active RFID Tokens must only be active inside the protected facility and passive RFID Tokens need to get protected by a metal casing before leaving the facility. Also cryptographic protocols could be implemented in order to increase security if physical security breaches. connection?

3) Countermeasures against Replay Attacks: The best countermeasure against replay attacks is to prevent them in advance by preventing eavesdropping, but this is not always possible. For example biometrics cannot always be protected. For these cases scanners with very little false positives are required in order to prevent deceiving the scanners. If these biometric scanners fail to protect the facility additional cryptographic protocols need to be implemented. Also diverse authentication mechanisms should be used in order to prevent a single compromised authentication factor to gain access to all systems of a facility.

VI. Using proximity based authentication mechanisms in autonomous factories

We have now identified requirements of autonomous factories and defined their implications. We also have done a survey about proximity based authentication mechanisms and defined their ranges and hardware requirements. We are now able to combine the requirements of autonomous factories with proximity based authentication mechanisms in order to increase security on the concepts of autonomous factories. In order to do so, we will go through all requirements and implement some authentication mechanisms on them. We will not list all possibilities of implementing authentication mechanisms, just the ones we think best suited for the stated situation.

A. Flexibility

Within section IV-B we defined, flexibility implies quick changes of machine parameters. So from where can machine parameters be changed? Remotely if needed, but with different authentication mechanisms. We are going to just have a look at changes in proximity, so maybe from a control room, directly at the machine or several meters away from another machine. We also need to consider which type of entity tries to change parameters. If the entity is another machine or a human different authentication mechanisms need to be used.

In case of a parameter change from a control room, any authentication requires physical access to this room and therefore is an authentication protected by proximity. We assume only humans are going to change parameters from this room, therefore a biometric based authentication within the room would be applicable. This authentication could be implemented cost effective for example with cameras to perform face recognition

without additional user interaction at entering the room or fingerprint sensors at control terminals. Authentication through key cards or passwords would also be possible, but is not recommended. We do not recommend this, because key cards and passwords are authentication through ownership, so we are not directly authenticating the entity. Authentication through ownership means it is implicitly assumed only authorized entities own a certain hardware token or knowledge to authenticate. This knowledge or hardware token could get lost or compromised and therefore we are not directly authenticating the entity than just a certain ownership is available.

The second case would be authentication directly at the machine in question. Again, we assume this authentication is only for humans and biometric based authentication would be a quick way of authenticating without additional user interaction.

The last case would be machine to machine authentication from several meters away. Depending on already available hardware on those machines, an applicable authentication mechanism can be chosen. We assume all machines are equipped with radios to be able to communicate. In this case, we could use Amigo authentication. In case of an autonomous factory the Amigo authentication should be relatively precise due to the fact there are many ambient radios. MASHaBLE authentication would be another more energy effective possibility to use. weak/none examples

B. Product traceability

We have found, that it is necessary to be able to track production parts, for example in order to be able to ensure product quality, decision making for production queues and resource management. Due to the fact that many production parts are in use, tracking must be cost effective and reliable. Active radio based authentication is not an option, because it requires energy and too many radios at the same frequencies would interfere with each other.

Therefore, light based authentication, more precisely QR codes or barcodes could be used. The QR or barcode markers are cheap, do not need an active energy source and can be read by cheap hardware like cameras or laser scanners. One disadvantage of this approach is the possibility to copy the printed code and insert malicious parts into a factory with this identifier.

Another cost effective authentication method would be radio based RFID authentication with passive tokens. These tokens can be read by cost effective readers at needed points in production and can be secured by additional cryptographic protocols. is this auth or id?

C. Resource efficiency

An important topic is the usage of wireless sensor and actuator networks for resource management. These networks of sensors are necessary to monitor for example the power consumption or other resources or status information. Based on this information autonomous systems are making decisions. Therefore, these status informations needs to be transmitted securely, to avoid manipulation of the transmitted data.

Depending on the boundary conditions of the sensors, different transmission technologies and different authentication mechanisms can be used. We now assume our sensors are built into mobile units which are battery powered and getting charged frequently.

Due to the need to transmit permanently different data, but not at high data rates, MASHaBLE would be applicable to achieve low energy sensor networks.

Another possibility would be to use light frequency to transfer a sensor value. The light source could only be used in fixed situations due to the need to adjust the direction of the light source.

D. Adaptivity

This part is connected to the above described sensor networks for resource efficiency. Autonomous machines are making decisions based on the information provided by sensors. Therefore, this information has to be reliable.

In this case we assume we are using sensors which are not running from battery and need to transmit their information to multiple machines. We are using Radio based authentication, more precisely the Amigo authentication. With this method, we can use high transmit energy and we implicitly verify the location the data is being transmitted from.

E. Modularity and re-configurability

Quick re-configurability requires modularity and therefore also requires communication between modules or more in general, machines.

We assume production machines are connected to a powerful power source, not highly mobile and able to communicate over larger distances. Depending on the use-case and transmitted data, high data throughputs might be necessary. If we consider our assumptions a radio based network would be appropriate. There are multiple ways of authentication for this network, but all of them require maintenance staff to take action.

One possible way would be to use an RFID token to transfer necessary information to initiate a network connection.

Other possibilities would be authentication by a physical action, a QR code, a move2auth challenge or a configuration via BLE.

F. Connectivity

Connectivity is needed everywhere in autonomous factories. The challenging part is the secure communication of mobile entities which know nothing about each other.

In this particular case of for example mobile work piece carriers, move2auth would be an applicable authentication method if they are able to get close enough to each other.

G. Human-Robot interaction

Humans need to interact with machines, therefore an authentication via Biometrics would be applicable, but we already covered these requirements above in the flexibility section.

We said a human could authenticate directly at a machine, but this would require every machine to provide an interface, which is not cost effective. It would be more likely to use a mobile device to control machines and use this mobile device to authenticate. This authentication could be biometric or just the ownage of a certain pre-authenticated device.

H. State knowledge for maintenance staff

Maintenance staff needs to be identified to get access to all necessary information and controls. At best, the maintenance staff does not need to do anything to get authenticated.

Our proposal would be to perform a biometric identification at the entrance to the facility, and track a beacon to be aware of the staffs position. A beacon could be an active RFID token or a BLE beacon transmitted by a mobile device. The advantage of the BLE beacon is, there is no need for an additional RFID token. A mobile device like a configuration tablet is necessary anyways to read sensor data and perform configurations, if the machines do not provide own interfaces.

VII. Evaluation

We have now integrated the concepts of proximity based authentication into the concepts of autonomous factories. We will now evaluate the significance of the findings.

This paper is a hypothetical combination of technologies. Therefore, there is no practical implementation, which could be tested yet. This paper should serve as rough concept for a future, more fine grained research. We could also not find other papers for the same topic with other approaches to compare with.

VIII. Discussion

Due to the fact this paper is just based on hypothetical considerations the impact is not big. This paper also does not do a sufficient research to serve as an implementation basis, so further research has to be done in order to implement prototypes of secure autonomous production facilities.

We will now give additional thoughts about various topics which appeared in the process of this work.

A. Logic checks to improve overall security

why here??

In most cases proximity based authentication mechanisms are working good on their own to prevent attacks. If an authentication mechanism fails nevertheless there could be another layer of security, logic checks in particular. Logic checks means an authentication mechanism is connected to a logging database and checks if an authentication in a certain situation should even be possible.

For example, an employee has authenticated at the entrance of a facility in order to enter the facility. If a second entity would now try to authenticate again at the entrance with a stolen fingerprint for example, the fingerprint sensor could check the database if the employee is already within the facility. In consequence the sensor would deny access for the second entity which tries to authenticate and could also alert security in order to check on the incident.

Another example would be to prevent attacks on inserting malicious parts into production by copying a QR or barcode. If an optical identifier is getting stolen, an arbitrary part could be marked with this identifier and brought into production. This part would be scanned by a certain machine and getting processed as the original part should be. If the scanner on the machine performs a check if a part already passed all steps before and none after this production step and if a part with the same identifier has recently been scanned somewhere else in production those parts would get sorted out and maintenance staff could be informed about the incident. These logic checks are mainly an additional countermeasure against some types or replay attacks.

B. Verifying validity of optical markers by print quality

Scanning and printing graphics, or more basic copying graphics, normally results in a quality loss. We could use this to prevent some tries to copy optical markers. If we print optical markers in high resolution in very little dimensions, a malicious scanner and printer also needs a very high resolution in order to produce a readable copy. One drawback is more little optical markers would also lead to the need of better optical sensors at all machines, and high resolution at all printers. This is not cost effective, because more high end hardware is required.

ideas, but why discu?

C. Advanced biometric authentication procedures

Until now we only mentioned already existing biometric procedures in order to prevent this paper from getting too hypothetical. Medical technology is evolving and therefore advanced biometric authentication procedures will be available within the next years. All of the following procedures are already in use in laboratories but they are not fast neither cost effective at the moment.

Biometric markers like Fingerprint, voice, face and iris are just characteristics built from the entities genetic material, also called DNA. Another marker which could be interesting in the future would be the set of teeth. The teeth are not as exposed as fingerprints or voice and therefore it is harder to obtain information for a replay attack. Scanning the teeth could happen optical, with lasers or in contact. Also the scanner has to be fast and self cleaning afterwards.

As told above, all markers are just manifestations of a certain set of genetic material. As authentication through ownership of a key card or knowledge is indirect authentication of an entity, authentication with biometric markers is also indirect authentication of a certain DNA.

Therefore, it would be the most direct authentication if the DNA itself would be used as authentication factor. At the moment DNA analysis is only done in laboratories and is a very time consuming process. For this reason it is also not very cost effective. Future scanners could be able to perform

DNA can be taken from subject, worse then iris scan!

these analysis more quickly. For an analysis a sample would be necessary. As sample saliva, a hair follicle, blood or a skin cell could be used. In general every cell can be used. These are still possible to steal but the needed effort for a replay attack on a DNA based authentication system would be higher than the benefit.

D. Cryptographic security behind proximity based authentication mechanisms

First we have to find which proximity based authentication mechanisms could get protected by cryptographic protocols in order to prevent eavesdropping and cloning of tokens.

The first group of authentication mechanisms are the radio based authentication mechanisms. Most of these mechanisms are already getting protected by cryptographic protocols. For WiFi Networks for example, different modifications of the WPA2 Protocol could be used. Another example would be RFID tokens which could get protected by using an asymmetric key exchange.

The second group of authentication mechanisms is audio based authentication. Depending if an audio channel is implemented to transmit arbitrary data or just a fixed pattern, different protection is possible. In the case of a fixed pattern, the only protection would be to use very low energy and therefore very close proximity to avoid eavesdropping. If an audio channel can be used to transmit arbitrary data, cryptographic protocols can be used. To protect an audio channel, the same cryptographic protocols as for radio based authentication can be applied.

The last group of proximity based authentication mechanisms which is able to use cryptographic protocols is light based authentication. As already described above, if the light based data channel is implemented to transmit arbitrary data it can use the same cryptographic protocols as radio based authentication.

Biometrics and Physical based authentication could use cryptography behind the sensor to communicate, but the authentication itself is not protected by cryptography.

IX. Conclusion/Future Work

We have shown different possibilities to secure systems of autonomous factories in order to create a more secure production environment. It has shown there are always multiple possibilities to secure certain systems. Often the best fitting algorithms are radio based for machine to machine authentication and biometric based for human to machine authentication. The reason for this is radios are cheap and in most cases already installed at the machines. Biometric based authentication however is not cheaper than using smart cards, but more secure because the ownership can not be lost. It has also shown there are different requirements to the authentication mechanism depending on the situation. For example which type of entity, either a human or a machine wants to authenticate. Still, this work is just a hypothetical rough concept. Deeper research must be done in the future to create concrete implementations of the shown authentication mechanisms and their reliability must be tested. Other questions like the exact structure and system design of an autonomous factory are not researched enough yet.

References

[1] E. Oztemel and S. Gursev, "Literature review of industry 4.0 and related technologies," *Journal of Intelligent Manufacturing*, vol. 31, no. 1, pp. 127–182, Jan 2020. [Online]. Available: https://doi.org/10.1007/s10845-018-1433-8

[2] U. M. Qureshi, G. P. Hancke, T. Gebremichael, U. Jennehag, S. Forsstrm, and M. Gidlund, "Survey of proximity based authentication mechanisms for the industrial internet of things," in *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*, 2018, pp. 5246–5251.

[3] M. Dotoli, A. Fay, M. Mikowicz, and C. Seatzu, "An overview of current technologies and emerging trends in factory automation," *International Journal of Production Research*, vol. 57, no. 15-16, pp. 5047–5067, 2019. [Online]. Available: https://doi.org/10.1080/00207543.2018.1510558

[4] Y. Michalevsky, S. Nath, and J. Liu, "Mashable: Mobile applications of secret handshakes over bluetooth le," in *Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '16. New York, NY, USA: Association for Computing Machinery, 2016, p. 387400. [Online]. Available: https://doi.org/10.1145/2973750.2973778

[5] A. Varshavsky, A. Scannell, A. LaMarca, and E. de Lara, "Amigo: Proximity-based authentication of mobile devices," in *UbiComp 2007: Ubiquitous Computing*, J. Krumm, G. D. Abowd, A. Seneviratne, and T. Strang, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 253–270.

[6] A. Varshavsky, A. LaMarca, and E. de Lara, "Enabling secure and spontaneous communication between mobile devices using common radio environment," in *Eighth IEEE Workshop on Mobile Computing Systems and Applications*, 2007, pp. 9–13.

[7] J. Zhang, Z. Wang, Z. Yang, and Q. Zhang, "Proximity based iot device authentication," in *IEEE INFOCOM 2017 - IEEE Conference on Computer Communications*, 2017, pp. 1–9.