

Securing the Manufacturing Environment using Biometrics

Shimon K. Modi
shimon@purdue.edu
Industrial Technology,
Purdue University
West Lafayette, IN-47906, USA

Stephen J. Elliott, Ph.D.
elliott@purdue.edu
Assistant Professor, Industrial Technology,
Purdue University
West Lafayette, IN-47906, USA

ABSTRACT

Over the past decade, there has been substantial growth in global business, of which the manufacturing industry plays a large part. This, accompanied by an increase in intelligent manufacturing equipment, increased connectivity of equipment and software both internally within a company, and with external partners has led to an increase in the probability of attacks and threats to these systems. Combine this with the current events and the additional requirements of governmental regulation, and several businesses in advanced manufacturing have to increase both physical and logical security. This paper outlines a unique application of biometrics and computer integrated manufacturing systems as part of providing an applied solution to solving security problems for manufacturing and control systems, and adhering to government regulations related to the manufacturing industry.

1. INTRODUCTION

Computer integrated manufacturing systems have changed the interaction of industrial manufacturing equipment with different systems within and outside the manufacturing environment. The increase in the sophistication of the manufacturing equipment, along with increased connectivity with internal and external systems has changed the way that manufacturing security is designed. As manufacturers move towards a more connected collaborative environment in order to compete in global businesses, concerns that their proprietary manufacturing processes and intellectual property could be exposed to damaging compromise on a worldwide scale are increasing. Security in the manufacturing environment has not been able to keep up with the advancement of interconnectivity and sophistication of manufacturing systems. The general problem that the manufacturing environment is facing is that operation of most industrial manufacturing equipment does not require any strong form of authentication or identification when some transaction related to product manufacturing takes place. Most manufacturing systems require a password to log

onto the system, after which the system is open to anyone on the manufacturing floor to operate. The manufacturing systems are sophisticated enough to provide remote operation capability, but most require only a password as a form of authentication. There are no means to ascertain who was operating the machine, and if they were authorized to do so. In an event of a malfunction or accident the audit trail does not provide relevant operator information. Physical access to the manufacturing environment is also an important factor to consider for security infrastructure. Because physical access vulnerabilities have been examined for longer than logical access vulnerabilities in the manufacturing environment, legacy physical access security systems are considered to be sufficient. Designs of security frameworks generally don't try to integrate physical access and logical access security. Biometric systems can incorporate physical and logical access security into a single framework, and provide a more centralized and integrated solution. The rest of this paper describes the different government regulations related to manufacturing security, and the proof of concept implementation that uses commercially available biometric systems to improve physical and logical security for a manufacturing environment.

2. REGULATIONS

The US government has also passed several regulations so that companies take into account general concerns like physical and logical security. The Sarbanes-Oxley Act of 2002 and the Food and Drug Administration's (FDA) 21 CFR Part 11 are two such regulations which require that companies have specific controls to ensure authenticity, integrity and auditability of electronic records. On March 20, 1997, the FDA published the Electronic Records: Electronic Signatures Rule in the Federal Register. This rule became effective on August 20, 1997, and was codified as 21 CFR Part 11. FDA's 21 CFR Part 11 primarily targets the health, and pharmaceutical industries. The initial targeted user community within these industries are the operators of the distributed control systems where the FDA has expressed concern regarding the ability to authenticate an individual who performs any

type of transaction in the manufacturing process, that would be governed by the regulations associated with electronic signatures, and the guidance of 21 CFR Part 11. There are several criteria like validity of records, accuracy of records, audit trails, protection of records, authority checks, system documentation, and operator entry checks that need to be satisfied in order to adhere to the FDA's regulation. Validity is achieved by ensuring the system's accuracy, reliability, consistency, and ability to discern invalid or altered records. Accuracy is achieved by creating adequate means to protect records for accurate and ready retrieval throughout the record retention period. Systems must use secure, computer-generated, and time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Operator entry checks must include some mechanism that determines and records the validity of the source of any data entered manually [1].

At first glance, Sarbanes-Oxley appears to be only concerned with financial information and therefore would have little to do with the manufacturing industry. But manufacturing systems are closely integrated with financial and inventory systems thereby increasing the importance of security in the manufacturing environment.

A security system that depends on usernames and passwords does not provide authenticity, integrity and auditability of records. A stronger authentication system is required in order to comply with these regulations. Biometric systems offer a stronger authentication system compared to traditional username password combinations, or identification tokens. The following sections describe the proof of concept implementation that can improve security in the manufacturing environment, and comply with government regulations.

3. PROOF OF CONCEPT IMPLEMENTATION

The proof of concept design is comprised of physical access security, and logical access security systems. One of the primary goals while creating this proof of concept was to use a wide variety of commercially available biometric systems as possible while keeping in mind the environment that they would be deployed in, matching performance rates, and cost-benefit ratio. The physical access security system uses hand geometry recognition to allow authorized individuals into the manufacturing environment. Access to the manufacturing machines requires the operator to be authenticated using fingerprint recognition. Along with fingerprint recognition, face recognition is used to authenticate the operator. Fingerprint recognition and face recognition make up the logical access security system.

Modern manufacturing equipment allows operators to access the manufacturing equipment from remote locations for maintenance operations. This proof of

concept uses iris recognition to authenticate the operator from a remote location, hand geometry for physical access, and fingerprint and facial recognition for logical access. Fig 1 shows the network diagram of the entire security framework.

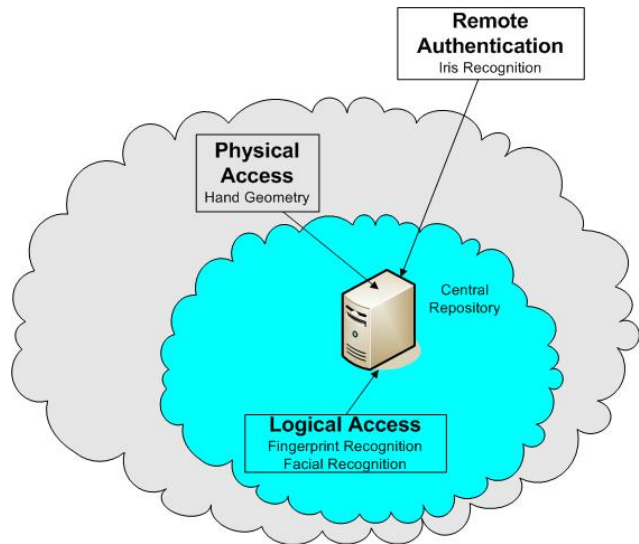


Fig. 1. Network diagram of access framework

A commercially available middleware solution is used to integrate all the different biometric systems, and provides centralized administration capability. The middleware solution manages all the enrolment templates, and provides identity and privileges management capability. A centralized server stores all the enrolment templates, and all queries are made to this server when a particular template is requested. In this particular design, the matching operation is done on the server whenever possible due to certain security, and performance benefits. A centralized system has its benefits over a decentralized system. Data management is easier, since all the data is stored in a central repository. A centralized storage system can be integrated with a decentralized matching system. Different profiles can be setup for machine operators, thus allowing separation of duties for using the manufacturing systems. A centralized architecture also provides the benefit of expanding the authentication to multiple locations without any major changes to the existing infrastructure. When an individual has to be enrolled into the system, they have to provide proper credentials to the administrator or the supervisor before proceeding with the enrolment procedure. It is important to carry out this first step with extreme care because if an incorrect identity is linked to a particular biometric template, all the security measures are rendered useless. If the administrator needs to deny access to an individual it can be done by removing the templates of the individual from the central repository.

3.1. Physical Access

As mentioned earlier, hand geometry recognition is used to authenticate individuals attempting to gain physical access to the manufacturing environment. Commercially available hand geometry systems are designed to withstand environmental and climate changes, making them an ideal choice for an uncontrolled environment. Also, the features of hand geometry are not affected by climate so much that the performance of the system will be affected. Hand geometry recognition systems use a personal identification number (PIN) to pull up the enrolment template linked to that PIN, and performing the matching operation. The use of a PIN reduces the time taken for matching operations, and offers the capability of separating personal information of the individual from the enrolment template repository. For example, the personal information of all the enrolled individuals and their enrolment templates can be kept in separate databases, and the PIN can be used to interlink the two databases. Since the physical access security is the first system the operators interact with all remaining transactions can be done using the PIN as the identifier.

3.2. Logical Access

Fingerprint recognition is used to authorize operators for accessing manufacturing machines. Traditionally username password combinations are used to allow operators to access manufacturing machines. Typing in the username and password every time an operator wants to access the machine can be cumbersome, and lead to loss of productivity. Fingerprint recognition takes less than a few seconds to complete one to many match operation depending on the size of the enrolment database [2], and doesn't require the operator to remember any usernames and passwords. The inside of the manufacturing environment tends to be relatively controlled in terms of temperatures and climate changes, which makes it suitable for fingerprint recognition.

Facial recognition is used in combination with fingerprint recognition to provide an added level of authentication. Also, commercially available facial recognition software's provide capability of tracking faces within a predetermined field of vision. This feature can be used to lock the machine if the operator steps away from the machine, and unlock the machine only if the authorized operator steps back into the field of vision of the facial recognition system. If a situation arises where an audit trail is required for usage of particular machine transactions from the fingerprint recognition system, and visual information can be used to provide accurate details.

Iris recognition performs optimally in a well lit, and controlled environment, which was the reason for using it

for remote authentication. Statistically iris recognition provides among the best matching performance rates when compared to existing biometric systems [3]. An unauthorized operator gaining remote access to a machine could have far reaching implications in terms of human safety, and business liability. Commercially available iris recognition software's can use web cams to capture the image of the iris. Normally operators log on to the machines from their home which makes iris recognition quite suitable because they can control any kind of visual interference that might affect the web cam.

4. WALK THROUGH SCENARIO

This section describes a typical scenario of an operator entering the manufacturing environment, and gaining access to a machine. The operator can enter the manufacturing premises only by using the hand geometry machine. When a positive verification occurs, the central server registers that the operator has entered the premises, shown in Fig 2. For the operator to log onto his/her respective machine, they have to use the fingerprint recognition, and the facial recognition systems. But just a positive match on the fingerprint, and facial recognition systems does not let the operator log onto the machine. If a positive match occurs using the fingerprint machine but the operator did not get registered on the central server because he/she just followed some one through the physical access system, that operator will not be allowed to log onto the machine. In order for the operator to use the machine, he/she has to enter the manufacturing environment using the hand geometry system.

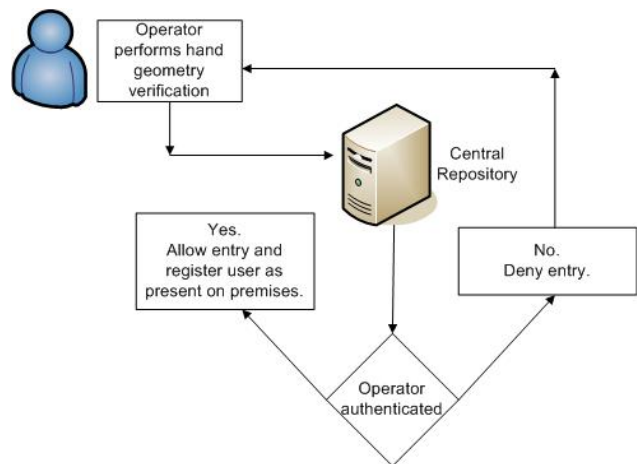


Fig 2. Stages for physical access to manufacturing environment.

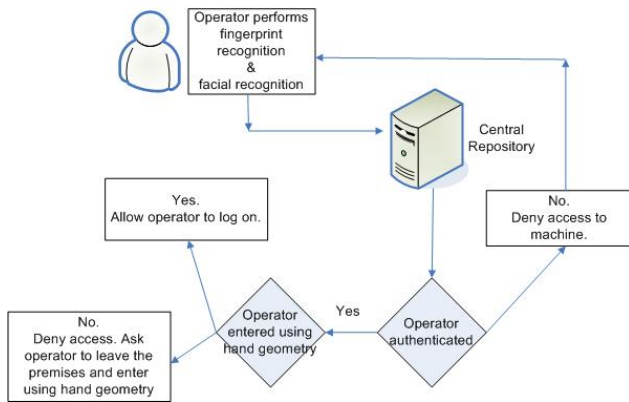


Fig 3. Stages for logical access to manufacturing environment.

This cross referencing prevents an unauthorized individual from entering the premises and using a machine that is not locked, is schematically shown in Fig 3.

The facial recognition system also provides facial tracking capabilities which can be used to lock down a machine when the operator moves away from the field of vision of the camera. This functionality prevents unauthorized operators from using a machine that an authorized operator has logged on to.

5. OTHER CONSIDERATIONS

The proof of concept described in this paper is by no means completely secure. The system was designed to reduce security inadequacies, and indeterministic nature of audit trails in current manufacturing environments. Security in any system is only as strong as its weakest link. Security technology can keep on advancing, but the human interaction with the system is a step that technology cannot replace. Human interaction with the system has to be considered whenever a security system is designed. For example, in the system described in this paper the administrator of the system has to ensure that proper credentialing takes place during enrolment in order to link the correct identity with the biometric template. Awareness and implementation of policies that limit the possibility of malicious actions will help reap the benefits of advancement made by technology.

6. CONCLUSION AND FUTURE WORK

The main aim of this research project was to demonstrate effective use of advanced technologies that keep up the advances made in the manufacturing environment. The proof of concept is designed using commercially available biometric products, and systems. Hand geometry

recognition is used to control physical access, and remove the inadequacies and management issues related to traditional lock and key systems or card based systems. Logical access is secured by using fingerprint recognition in tandem with facial recognition to overcome the weakness of traditional logical access security based on usernames and passwords. Remote authentication is performed using iris recognition as it is best suited to work in controlled environments, and provide a high level of security. The entire framework is centralized to provide ease of management, and increased security.

The current framework does not integrate smart cards or radio frequency identification (RFID) tags in conjunction with biometrics. Smart cards could provide local storage of templates, as well as an additional layer of identification. Similarly RFID tags can be used instead of facial tracking to lock down a machine if the operator steps out of range of the RFID scanner. One of the improvements for the future is to concentrate on developing policies, and procedures which would make the biometric security system more effective. The system in its present form does not record if an operator leaves the manufacturing premises, and then re-enters. Future work should focus on exit protocol so that records can be more accurate. An in depth return on investment study can also be carried out to assess the feasibility of large scale deployments, although long term considerations, and intangible advantages should be measured.

7. REFERENCES

- [1] Haley, T. A., *The Electronic Records Regulation: An Implementation Guide for the Food Industry*, <http://www.ces.purdue.edu/extmedia/FS/FS-12/FS-12W.html>
- [2] <http://www.neurotechnologija.com/verifinger.html>.
- [3] Wildes, R.P., *Iris Recognition: An Emerging Biometric Technology*, Proceedings of IEEE, Sept., 1997.