Volume 6, Issue 12, December 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

How to Enable Security by Managing Identity of Applications

Youssef ZIZA*
RITM LAB ESTC
Hassan II University
Casablanca, Morocco

Nadia AFIFI
RITM LAB ESTC
Hassan II University
Casablanca, Morocco

Hicham BELHADAOUI
RITM LAB ESTC
Hassan II University
Casablanca, Morocco

Mounir RIFI
RITM LAB ESTC
Hassan II University
Casablanca, Morocco

Abstract*— Modern life depends on automating. Virtually every time we open a faucet tap, turn on a light or jump on a train, we rely on the Industrial Control Systems (ICS) to manage processes such as water purification, power generation and mass transit signalling. However, rely on computers for so fundamental tasks requires absolute confidence in their security. The attacks interrupting these basic needs could trigger of financial disaster and the collapse of public health and safety. Contrary to what was done in the past, most of ICS sellers now use standard computer technology for their solutions. They allow companies to connect components such as ICS SCADA to corporate networks and other operational technologies such as Enterprise Resource Planning (ERP) or Manufacturing Execution Systems (MES). While this convergence of technology can improve productivity and profitability, it also greatly increases the risk of ICS cyber attack, creating new vectors for less skilled hackers can launch attacks. Stuxnet, Shamoon Havex are well-known examples of this type of threat, which continues to grow while ac- global initiatives such as smart grids lead to systems increasingly connected to public and private networks. The exploitation of vulnerabilities is a real threat to the state and may lead to disaster. That's why we propose an approach that combines the use of electronic certificates, electronic signature, whitelisting to help secure critical information systems.

***Key Words*— Stuxnet, Strong authentication, TPM, X509, Whitelisting, IDS/IPS, Antivirus.**

I. INTRODUCTION

Despite that industries have set up different modules to ensure the security of their information systems, they are subject to several attacks to which interfere with the proper conduct system. One of the attacks was the subject of several publications and writings is STUXNET [1] [2].

This virus is known and earned his reputation thanks to the sophisticated way of its design, but above all it's recognized by the nature of the systems that it attacks.

Nowadays, to ensure the security of a system, we must ensure the security of the weakest link of this system. Small flaw in its operation may be fatal and lead to a multitude of vulnerabilities in the control command of the system. So an upstream work is essential to secure the system.

Indeed, despite the presence of security modules that are installed and implemented in information systems (antivirus, proxy firewalls, IDS/IPS ...), these systems remain vulnerable and are the subject of several attacks in recent years.

In our paper we will first present the types of solutions generally offered in an information system. After we will analyze them and then propose an approach for ensuring the security and integrity of these systems. This approach will allow us to have more security and improved traceability; to secure information systems in the industry field.

Our paper is organized as follows: Section 2 we'll present the state of the art on the tools allowing to ensure security on the various components of an information system. Section 3 will present a case of Whitelisting use. Our proposal for a new approach will be developed in section 4. In section 5, we present the secured architecture, and we will end up with a conclusion and perspectives.

II. STATE OF THE ART

A. Antivirus

The concept of antivirus protection in the industrial world is unavoidable. Typically, they are used to protect data streams, servers and client computers. We know that there are two types of antivirus scanning: By signature and by heuristic. The antivirus by signature looks for a pattern present in a predetermined antivirus database, while the heuristic analysis consists of detecting the virus by its actions on the system (attempting to access system files, by elevation of privilege, trying to write in registry, etc.).

We can say that an unknown virus (absence of signature in the antivirus database) with normal behaviour can easily infiltrate in the system, this is the case of Stuxnet [3].

B. Whitelisting

The whitelist solutions are designed to protect companies against damage that can be caused by hostile applications and unwanted software. whitelisting solutions can protect: (i) desktops and servers, (ii) industrial robots, (iii) process control systems and monitoring, (iv) ATMs, (v) medical equipment. [4].

© 2016, IJARCSSE All Rights Reserved

The whitelist approach offers an innovative and secure alternative to traditional anti-virus. These solutions controls which applications are allowed to run on a device or system. Anti-virus must check permanently, hundreds of thousands of known threats, unlike the white list which is much faster because it is sufficient to verify each application with a short list approved. Any process that is not part of an authorized application is prohibited before being launched (principle of "default deny"). Therefore, unauthorized software are completely blocked and therefore will never be a threat to an organization.

C. Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)

An intrusion into the network is an attack that comes from outside the LAN, usually over the Internet. IDS / IPS are important elements in the security of networks as they can detect and prevent intrusions.

Intrusion Detection System (IDS), allows to analyze network traffic and generate alerts when malicious activity is discovered. They are usually able to reset TCP connections. Some IDS are able to query the firewall to add rules "OnTheFly".

The limitation of those intrusion detection systems is that they can not anticipate network attacks.

When the Intrusion Prevention System (IPS), they perform the same analysis as IDS, but in addition, can anticipate and prevent against malicious activity.

1) Types des IDS/IPS

There are two types of IDS:(i) IDS Host and (ii) Network IDS.

Host IDS (HIDS): Host IDS should be deployed on each protected machine (server or workstation). It analyzes the local data to the machine such as system log files, system files changes, and sometimes the process and system calls. HIDS alerts the administrator in case of violation of rules.

Network IDS (NIDS): This is a type of IDS is deployed in the network (before the firewall or in various locations in the internal network) to analyze the traffic traversing the network. Several actions can be conceivable in case of an intrusion detection: (i) send an alert to the administrator, (ii) dynamically change the rules of firewall to block the connection (even if it is often very risky because false positive. NIDS can be compared to a sniffer).

All intrusion detection methods (X-IDS) involve the collection and analysis of information from various sectors (computer or network) to identify possible threats from hackers and crackers either of inside or outside the organization. NIDS and HIDS have their respective advantages and limitations. [5] So the most effective protection for a network owner would be ensured by a combination of both technologies.

2) Functioning of IDS/IPS

An IDS can detect intrusion by following two approaches:(i) behavioural or (ii) signature.

The behavioral approach is based on statistics to detect intrusions, several parameters are taken into consideration, thus determining the profiles of users and traffic transiting the network. This type of tool offers a solution against the brute force attack.

The signature approach is based on a database of attack signatures, IDS compares the packets that pass with the signatures of attacks and thus detects intrusions. This kind of solution is susceptible to false positives and depends bases signatures [6].

Specialized teams add IDS signatures in the database, such as Vulnerability Research Team (VRT) and for Snort IPS.

The downside of IPS / IDS is that in case of absence of signature based IDS / IPS. An unknown virus by the system with normal behavior can adversely affect the operation of the latter.

D. Protection by Strong authentication

It has been shown that by adding strong/multi-factor authentication for identifying entities using resources or accessing information increases the security of an information system in terms of availability. We highlighted in our previous work using the OTP (One Time Password) to deal with Hook DLL attacks to alter the normal functioning of a process. [7].

Indeed, strong authentication is a process to identify safe way entities using multiple parameter for the connection (One Time Password, electronic certificate authentication, etc.)

By definition, Authentication is the use of one or more Mechanisms to confirm that you are the authenticated user you pretend to be. Once the identity of the human or machine is validated, access is authorized. There are three authentication factors: (i) what you know like Alphanumeric passwords, Graphical Password (ii) what you-have like ATM card or tokens and (iii) what you are like Finger print, Thumb Print, heart beat called Expired biometrics authentication [13]. While the biometric-based authentication is Relatively expensive and raises privacy Concerns, One Time Passwords (OTP) offers a promising alternative for two factor authentication systems [8].

E. Digital Signature

The digital signature ensures the integrity of a given signature algorithm [9]. It relies on the use of asymmetric key hashing and digital certificates to ensure the integrity and non-repudiation.

In general, the technique of the digital signature is essential for secure transactions over open networks. It is used in a variety of applications to ensure the integrity of data that has been exchanged or stored, and prove the identity of the sender or the entity modified content [10]. The digital signature is mainly used in cryptographic protocols to provide services such as authentication of the entity.

F. Trusted Platform Module

In devices such as PCs and servers, the TPM is typically a microcontroller that securely stores keys and digital certificates that can provide electronic identity. The TPM may be a "chip" separate or an integrated part of another "chip", such as an Ethernet controller. The TPM works with security methods to ensure the deployment of secure applications.

The idea is to offer the highest level of security for access and use of the certificates for the manufacturer, and this obviously requires the use of Trusted Platform Module (TPM) [11].

In the TPM, a cryptographic coprocessor handles operations such as the generation of asymmetric keys, the hash (Secure Hash Algorithm (SHA-1)) and the generation of random numbers (RNG). With increasing cost of security breaches and cost of threats; the TPM ensures the protection and interoperability across multiple platforms.

The use of TPM as cryptographic certificates support, increases the level of security and has not impact on productivity.

III. FUNCTIONING OF CLASSIC WHITELISTING SYSTEM

Most of withelisting solutions have the same functioning, in our example we will explain the proposal by Microsoft and we will see later the approach that we have proposed.

AppLocker whitelisting solution is the one that replaces Software Restriction Policies on recent versions of Windows.

AppLocker helps administrators control the applications and files that can users can run. This includes executables, scripts, files in the Windows installation program, dynamic link libraries (DLLs), packaged applications and packaged application installers.

AppLocker allows you to perform the following tasks:

- Define rules based on file attributes derived from the digital signature.
- Assign a rule to a security group or an individual user.
- Create exceptions to rules.
- Define rules for packaged applications and packaged application installers.
- Manage group policies, and allow the administrator to update these strategies.
- Allow customization of error messages to direct users to a web page to get help.
- Support a set of PowerShell cmdlets to assist in the administration and maintenance.
- Use rules to control the sizes of the files listed: .exe, .com, .ps1, .bat, .cmd, .vbs, .js, .msi, msp, mst, .dll, .ocx, .appx.

However, the control of application behavior after execution is not supported by AppLocker. Applocker can be exceeded with a simple Hook DLL. [12]

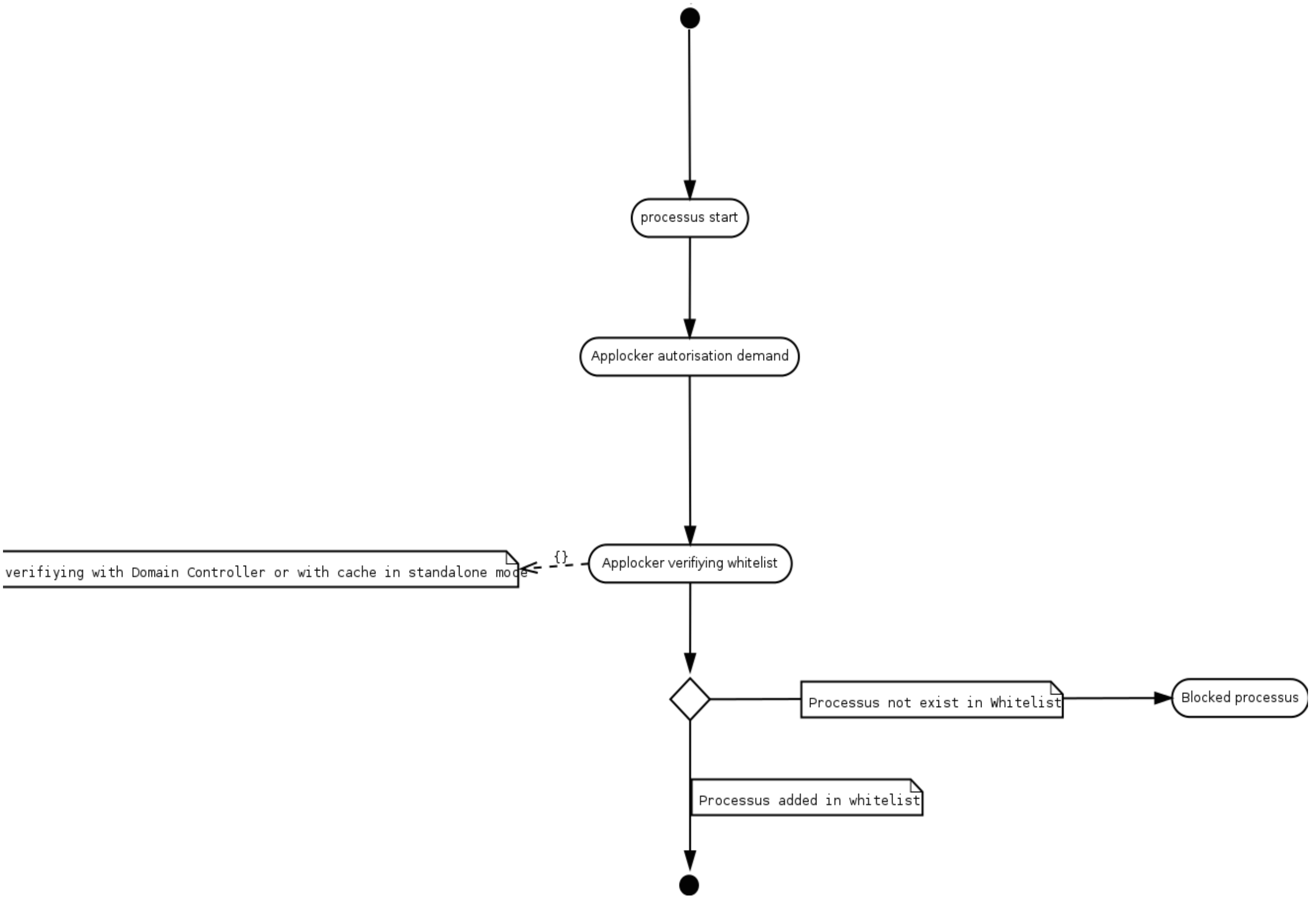
processus start
Applocker autorisation demand
Applocker verifiying whitelist
{}
verifiying with Domain Controller or with cache in standalone mode
Processus not exist in Whitelist
Blocked processus
Processus added in whitelist

Figure 1 : AppLocker functioning

The figure 1 shows how AppLocker verifies that the process to start is included in the whitelist.

The operation of AppLocker whitelisting remains similar to other systems [13].

AppLocker type solutions cannot prevent attacks which concern applications added in the whitelist. Hence the idea to offer an improved system security, by strong authentication proposal for any change in processes started.

IV. APPROACH PROPOSAL

We have seen the limits of whitelisting solutions, antivirus also showed that they are limited and circumvented in case a virus exploits of unknown vulnerabilities. [14]

We also studied in depth the functioning of stuxnet virus and the flaws that he exploited [7] [15], our goal is to propose an approach to cope with these vulnerabilities.

Our approach considers the various existing security components usually present in structures requiring high level of security in their IS. The approach is based on the digital signature, the Trusted Platform Module TPM, the digital certificate, and Whitelisting.

The idea is to ensure the identity of the processes that are running towards the machine and be certain they are launched by the right entities. Digital certificates are the unfalsifiable link between an entity and its digital identity, hence the importance of using these certificates to securely identify performers applications processes. This will ensure that these applications execute only what is allowed, and use only the resources to which they are entitled.

To do this, we have to verify the identity of: (i) the running process, and (ii) the process requesting a modification of system files of an application. This warranty is provided by strong authentication. We propose a digital certificate to authenticate the process; and to request authentication for any use of critical features enabling to bypass the normal behaviour of a process.

We propose the use of standards (X509) deployed on a physical cryptographic module on each machine to identify the process.

To summarize, we will use: (i) strong authentication when calling to critical system features (ii) x509 standard which allows for the attributes of the identity of an entity and its pair keys signed by a trusted third party.

V. ARCHITECTURE AND THE FUNCTIONING

In our previous work [7], we highlighted Stuxnet's exploitation of zero-day attacks (i) CVE 2010-2743 (MS -10-073); (ii) vulnerability in the Windows Task Scheduler on Microsoft OS; allowing it to have all the necessary privileges on the machine. And after, Stuxnet uses a special method to load the DLL. Normally the LoadLibrary function loads the DLL from the ROM. But Stuxnet is able to load the DLL from RAM. This operation is possible thanks to use of Hook DLL; the exploitation of WriteProcessMemory or CreateRemoteThread that allow to Stuxnet to write in a process running, and change the APIs [16].

One of system vulnerabilities is that it does not verify the entity which modifies the process. This is why we propose to secure this process of modification, by adding an authentication request with electronic certificate (strong authentication).

One system vulnerabilities, is that it does not verify the entity modifies the process. This is why we propose to secure this process of change by adding an authentication request with electronic certificate (strong authentication).

A. Approach

Figure 2 shows how the process works after adding the authentication functionality

As explained above, when starting a process, AppLocker checks permissions of the application and verifies the signature of the whiteliste. The critical features of use of calls will always be associated with strong authentication of the entity that requested.

B. Code Example

The initial function syntax "WriteProcessMemory" in C ++ is as follows:

```
BOOL WINAPI WriteProcessMemory(
_In_ HANDLE hProcess,
  _In_ LPVOID lpBaseAddress,
  _In_ LPCVOID lpBuffer,
  _In_ SIZE
  T nSize,
  _Out_ SIZE_T *lpNumberOfBytesWritten
  );
```

We propose to modify by inserting instructions "_IN_ LPSTR hX509_fileVersionInfo" and "_IN_ LPSTR hX509_PID" which allow verification of the two attributes of the certificate process (i) "FileVersionInfo" which provides information about the version of a physical file on the disk and (ii) the process identifier "PID" when strong authentication.

```
BOOL WINAPI WriteProcessMemory(
  _In_ HANDLE hProcess,
  _In_ LPVOID lpBaseAddress,
    _In_ LPCVOID lpBuffer,
    _In_ SIZE_T nSize,
    _In_ LPSTR hX509_fileVersionInfo,
    _In_ LPSTR hX509_PID,
    _Out_ SIZE_T *lpNumberOfBytesWritten
);
```

Parameters

- hProcess [in]

  A handle to the process memory to be modified. The handle must have PROCESS_VM_WRITE and PROCESS_VM_OPERATION access to the process.
- lpBaseAddress [in]

  A pointer to the base address in the specified process to which data is written. Before data transfer occurs, the system verifies that all data in the base address and memory of the specified size is accessible for write access, and if it is not accessible, the function fails.
- lpBuffer [in]

  A pointer to the buffer that contains data to be written in the address space of the specified process.
- nSize [in]

  The number of bytes to be written to the specified process.
- lpNumberOfBytesWritten [out]

A pointer to a variable that receives the number of bytes transferred into the specified process. This parameter is optional. If lpNumberOfBytesWritten is NULL, the parameter is ignored [17].

The same changes are made to the "CreateRemoteThread" function that initially looks like this:

```
    HANDLE WINAPI CreateRemoteThread(
    _In_ HANDLE hProcess,
    _In_ LPSECURITY_ATTRIBUTES
    lpThreadAttributes,
    _In_ SIZE_T dwStackSize,
    _In_ LPTHREAD_START_ROUTINE
    lpStartAddress,
    _In_ LPVOID lpParameter,
    _In_ DWORD dwCreationFlags,
    _Out_  LPDWORD lpThreadId
    );
```

After modification it becomes

```
    HANDLE WINAPI CreateRemoteThread(
    _In_ HANDLE hProcess,
    _In_ LPSECURITY_ATTRIBUTES
    lpThreadAttributes,
    _In_ SIZE_T dwStackSize,
    _In_ LPTHREAD_START_ROUTINE
    lpStartAddress,
    _In_ LPVOID lpParameter,
    _In_ DWORD dwCreationFlags,
    _In_ LPSTR hX509_fileVersionInfo,
    _In_ LPSTR hX509_PID,
    _Out_  LPDWORD lpThreadId
);
```

In case where authentication is not verified, the change in the process is blocked at this level. Thus, simply revoke the certificate that allows the update of the Certification Revocation List (CRL). Knowing that the CRL is verified at each authentication.

C. Deployment of Certificate on TPM

The functionality of deployment of certificates on TPM will be done via the whitelisting agent, which own features of authentication verification

The check will be done via the electronic signature of the whitelist, by the Domain Controller (DC). The certificate of the Certificate Authority has the advantage of being available on all stations.

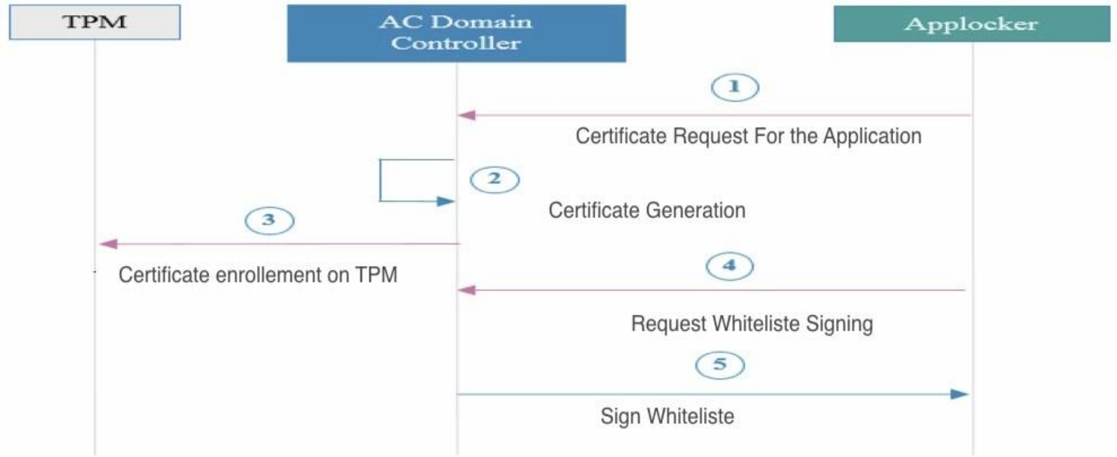
TPM
AC Domain Controller
Applocker
1
Certificate Request For the Application
2
Certificate Generation
3
Certificate enrollement on TPM
4
Request Whiteliste Signing
5
Sign Whiteliste

Fig 3 : Certificates Deployement in TPM

Figure 3 illustrates the deployment of certificates on TPM machines. The whitelisting agent through the Microsoft enrolment interface, initiates the certificate request for a process, and displays the key pair associated with the certificate in the cryptographic module. Thus the safety profile which includes the list of processes allowed to be run on the system is checked. Also, certificate-based authentication is required when use of critical functionalities.

D. Proposal of a certificat gabarit for processus

The electronic certificates allow to identify the process. We offer templates respecting the X509 standards to which we will add following attributes in the "Extended Key Usage": Proess ID via Object ID '

We have specific certificates for authentication process by adding the Extended Key Usage "signing process" with a specific OID.

Table 1: Certificat Procedure

Champ	**Description**
Version	Version 3
Serial Number	Generated by the tool
Issuer	CN: OU: O: C:
NotBefore	Deliverance date
NotAfter	Date of expiration
Subject	
SubjectPublicKeyInfo	(rsaEncryption) 1.2.840.113549.1.1.1
Key Size	2048
Signature (algorithm & OID)	SHA256WithRsaEncryption
Authority Key Identifier	ID Public Key of the CA
keyIdentifier	issuerName+serialNumber
Subject Key Identifier	
Key Usage (Critical)	digitalSignature
CRL Distribution Point	
Distribution point	**URL VERIFICATION CRL**
Authority Information Access	
OCSP	**URL OCSP**

VI. QUALITATIVE STUDY

The aim of this study is to provide guidance on the safety system approach in terms of "confidence". In this perspective, the common criteria define a set of requirements for systems to develop. The Security objectives reflect the desired state to address identified vulnerabilities and/or comply with the rules or constraints. In our case, we will see added value of our approach.

1) Protection Profile (PP)

A Protection Profile is a description in a standardized form of a need for security and how to fulfil the functions from the catalog. PP corresponds to a document containing all the objectives and security requirements for information systems relating to the safety of a tool [18].

This document is used as part of the certification process according to ISO/IEC 15408 and the Common Criteria.

2) Commun Criteria

Common Criteria for Information Technology Security Evaluation is an international standard (ISO / IEC 15408) for the security of information systems.

We based on the functional safety requirements. These are grouped in a catalog for the purpose is to provide a structured language to express what must be a security product:

- Security Audit (FAU)
- Communication (FCO)
- Use of cryptography (FCS)
- Protection of user data (FDP)
- Identification and Authentication (FIA)
- Security Management (FMT)
- Protection of Privacy (FPR)
- Protection of the security functions of the target of evaluation (FPT)
- Use of Resources (FRU)
- Access to target of evaluation (FTA)
- Paths and trust channels (FTP)

3) Target of evaluation

The "TOE" is the product under evaluation. The criteria are intended to be generic but they apply properly if it is a software. In our case we can take the system hosting the SCADA as TOE.

4) Use Case

In general, the security of an information system is measured by several parameters, our study deals with the following parameters: Availability, confidentiality and integrity. We can rely on our approach to propose a new protection profile that takes into account several CLASS of the CC. Therefore increases the level of security. These new protection profiles have security objectives that are different from the protection profiles applied in the information systems used in the industrial sector. These profiles will take into account the various modifications made and therefore bring more security with regard to the use of cryptography, identification and strong authentication. This increases the availability of the system and the integrity of the information.

The table below illustrates the added value of our proposal

Table 2: Added value of our proposal

Actifs	Disponibility	Integrity
Executed Process	++	++
DLL Files	++	++

VII. CONCLUSION AND PERSPECTIVES

The Stuxnet virus types continue to spread, exploiting technical and organizational vulnerabilities. In our paper, the use of strong authentication and application filtering makes it possible to cancel the risk of exploitative threats of the vulnerabilities allowing to take control on a machine by a virus.

The next step is to propose new ways of raising awareness of the security of information systems in the industrial field. The organizational aspect of security remains very critical, thus, we propose in our future works an approach of management of identities, of accesses and authorizations that allows more control and flexibility. This greatly reduces the risk of threats.

REFERENCES

[1] USA DEPATEMENT OF ENERGY 21 Steps to improve cyber security of scada networks available: http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf 11P

[2] Cyber Security of Water SCADA Systems Analysis and Experimentation of Stealthy Deception Attacks IEEE

[3] Stuxnet and the Limits of Cyber Warfare, Jon R. Lindsay, University of California Institute on Global Conflict and Cooperation, p23 & p33, 2013

[4] PROTECT CRITICAL INFRASTRUCTURE COMPUTER SYSTEMS WITH WHITELISTINGGIAC (GSEC) Gold Certification Dwight Anderson, dwight_anderson@selinc.com

[5] Flaws and frauds in the evaluation of IDS/IPS technologies, Stefano Zanero, DEI - Politecnico di Milano via Ponzio 34/5 20133 Milano Italy, 2013

[6] A Survey of Ethernet LAN Security, Timo Kiravuo , Mikko Sa ̈rela ̈ , and Jukka Manner, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 15, NO. 3, THIRD QUARTER 2013

[7] Youssef ZIZA, Hicham BELHADAOUI, Nadia AFIFI, Mounir RIFI, Proposal of Countermeasure against Attacks Similar to Stuxnet, RITM LAB ESTC CED ENSEM Hassan II University, Casablanca, Morocco, 2014

[8] S. Vaithyasubramanian1, A. Christy Sathyabama University, India. Chennai and D. Saravanan, Faculty of Operations and Systems, IBS Hyderabad, India, TWO FACTOR AUTHENTICATIONS FOR SECURED LOGIN IN SUPPORT OF EFFECTIVE INFORMATION PRESERVATION AND NETWORK SECURITY, ARPN Journal of Engineering and Applied Sciences MARCH 2015

[9] Mr. Vinod Saroha, Annu Malik, Madhu Pahal, The Enormous Certificate: Digital Signature Certificate, Computer Science and Engineering. Ijarcsse 2013

[10] Shivendra Singh Student Department of CSE Amity University, Noida, India, Md. Sarfaraz Iqbal Student Department of CSE Amity University, Noida, India, Arunima Jaiswal Asst. Professor Department of CSE Amity University, Noida, India, Survey on Techniques Developed using Digital Signature: Public key Cryptography, International Journal of Computer Applications May 2015

[11] Justin D. Osborn and David C. Challener, JOHNS HOPKINS APL TECHNICAL DIGEST, Trusted Platform Module Evolution, VOLUME 32, NUMBER 2, 2013

[12] Nicolas Falliere, Liam O Murchu, and Eric Chien, W32.Stuxnet Dossier SYMANTEC, SYMANTEC Septermber 2010

[13] Himanshu Pareek, Sandeep Romana and P R L Eswari, Centre for Development of Advanced Computing, Hyderabad, India, APPLICATION WHITELISTING: APPROACHES AND CHALLENGES, International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), October 2012

[14] René Freingruber, A review of SCADA anomaly detection systems, SEC Consult Vulnerability Lab, Vienna

[15] Aleksandr Matrosov, Senior Virus Researcher, Eugene Rodionov, Rootkit Analyst, David Harley, Senior Research Fellow, Juraj Malcho, Head of Virus Laboratory, Stuxnet Under the Microscope, ESET, , P85

[16] Bc. Peter Nemček, Analysis of Malware Classification Schemas, Masarykova univerzita Fakulta informatiky, 2014

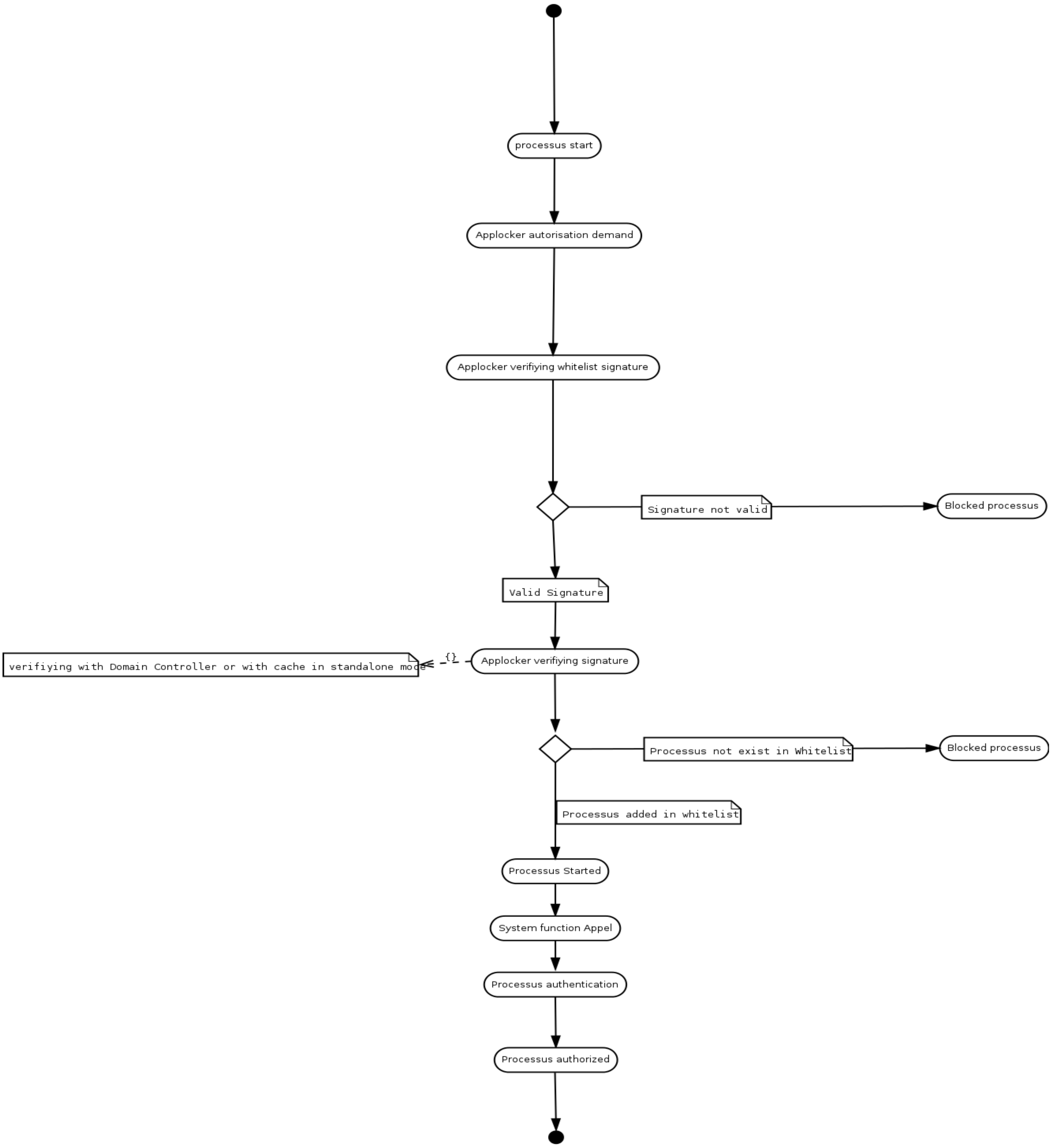
processus start
Applocker autorisation demand
Applocker verifiying whitelist signature
Signature not valid
Blocked processus
Valid Signature
verifiying with Domain Controller or with cache in standalone mode
{}
Applocker verifiying signature
Processus not exist in Whitelist
Blocked processus
Processus added in whitelist
Processus Started
System function Appel
Processus authentication
Processus authorized

FIG 2 : Progress Functioning