# Security Framework for the Semiconductor Supply Chain Environment

Alireza Esfahani[1], Georgios Mantas[1], Mariana Barcelos[1], Firooz B. Saghezchi[2], Victor Sucasas[2], Joaquim Bastos[1] and Jonathan Rodriguez[2]

[1] Instituto de Telecomunicações (IT), P-3810-193 AVEIRO – PORTUGAL
alireza@av.it.pt,gimantas@av.it.pt, m.aleixo@av.it.pt,and jbastos@av.it.pt
[2] University of Aveiro, Aveiro, Portugal
firooz@ua.pt, vsucasas@ua.pt, and jonathan@ua.pt

**Abstract.** This paper proposes a security framework for secure data communications across the partners in the Semiconductor Supply Chain Environment. The security mechanisms of the proposed framework will be based on the SSL/TLS and OAuth 2.0 protocols, which are two standard security protocols. However, both protocols are vulnerable to a number of attacks, and thus more sophisticated security mechanisms based on these protocols should be designed and implemented in order to address the specific security challenges of the Semiconductor Supply Chain in a more effective and efficient manner.

**Keywords:** Industry 4.0, Semiconductor Supply Chain, Network Secure Communications, SSL/TLS, OAuth2.

## 1 Introduction

Nowadays, data communication across the partners in the Semiconductor Supply Chain can be the target of many known and unknown security threats exploiting many security breaches in the internal/external environment of the partners due to its heterogeneous and dynamic nature as well as the fact that non-professional users in security issues usually operate their information systems. Particularly, these vulnerabilities in the Semiconductor Supply Chain Environment can be exploited by attackers with a wide spectrum of motivations ranging from criminal intents aimed at financial gain to industrial espionage and cyber-sabotage. Attackers can compromise the data communication between legitimate parties in the Semiconductor Supply Chain and thus can jeopardize the delivery of services across the partners as well as the continuity of the service provision. As a result, Semiconductor Supply Chain partners will suffer from damaging repercussions, which can cause significant revenue loss, destroy their brand and eventually hinder their advancement. Consequently, a security framework for secure data communications across the partners in the Semiconductor Supply Chain Environment is of utmost importance.

Therefore, the main objective of this paper is to provide a security framework for secure data communications across the partners in the Semiconductor Supply Chain. Towards this direction, in this paper, we firstly consider representative examples of various attacks that have been seen in the wild and can cause potential security issues and challenges in the Semiconductor Supply Chain Environment. The range of the attacks shows how vital is a security framework for secure data communications for the partners in the Supply Chain of the Semiconductor Industry. Moreover, we provide a categorization of the various attack examples based on the intrusion method that they use to compromise the target and gain a persistent foothold in the target's environment. Furthermore, we propose a security framework for secure data communication across the partners in the Supply Chain. The security mechanisms of the proposed framework will be based on the SSL/TLS and OAuth 2.0 protocols, which are two standard security protocols. The SSL/TLS protocol is the de facto standard for secure Internet communications [1]. On the other hand, the OAuth 2.0 protocol is the industry-standard protocol for authorization [2]. However, both the SSL/TLS protocol and the OAuth 2.0 protocol are vulnerable to a number of attacks, and thus more sophisticated security mechanisms based on these protocols should be designed and implemented in order to address the specific security challenges of the Semiconductor Supply Chain in a more effective and efficient manner.

## 2 Cybersecurity Issues and Challenges in the Semiconductor Supply Chain Environment

In this section, we consider representative examples of various attacks in industrial and enterprise domains that have been seen in the wild and can cause potential security issues and challenges in the Semiconductor Supply Chain Environment. We categorize these attack examples into 5 main categories based on the intrusion method that they use to compromise the target and gain a persistent foothold in the target's environment. The 5 main categories that we identified are the following: a) spear phishing attacks, b) watering hole attacks, c) attacks based on "trojanized" third-party software, d) attacks based on malicious code and counterfeit certificates, and e) attacks based on tampered devices.

### 2.1 Spear Phishing Attacks

Phishing is a kind of social-engineering attack where adversaries use spoofed emails to trick people into sharing sensitive information or installing malware on their computers. Indeed, victims perceive these spoofed emails as being associated with a trusted brand. In other words, phishing attacks target the people using the systems instead of targeting directly the systems that people use. Thus, phishing attacks are able to circumvent the majority of an organization's or individual's security measures. Moreover, it is worthwhile to mention that phishing has spread beyond email to include VOIP, SMS, instant messaging, social networking sites, and even massively multiplayer games. Moreover, cyber-criminals have shifted from sending mass-emails,

hoping to trick anyone, to more sophisticated but also more selective "spear-phishing" attacks that use relevant contextual information to trick specific groups of people. In principle, "spear-phishing" attacks are more dangerous than typical phishing attacks [3]. Here are a few examples of "spear-phishing" attacks from the wild.

**Icefog.** In 2011, Kaspersky Lab started to investigate a threat actor called 'Icefog' that attacked many different groups, such as government institutions, military contractors, telecom operators, satellite operators, among others, through their supply chain. This campaign targeted organizations mostly in South Korea and Japan, but it was suspected that it also targeted the United States and Europe [4]. The intrusion method of this attack was phishing e-mails with a malicious attachment or a link to an infected web page. The attacker could compromise the victim's machine either by tricking the victim to install the attached malware or by tricking the victim to visit the malicious web page [5]. Afterwards, the attacker could steal files from the victim's machine, run commands to locate and steal specific information from the victim's machine, and also communicate with local database servers in order to steal information from them. In addition, Icefog was capable of uploading special tools to extend the capabilities of the installed malware, such as tools for stealing cached browser passwords in the infected machine. In 2012, a Mac OS version of Icefog (Macfog) was created [4], but Kaspersky suspected that it was a beta-testing phase to be used in targeted victims later. Finally, it is worth mentioning the "hit and run" nature of Icefog, since the Icefog attackers appeared to know very well what they need from the victims and thus, once the information was obtained, the victim was abandoned.

**Target.** At the end of 2013, Target suffered a cyber-attack that exposed approximately 40 million debit and credit card accounts [6] and 70 million e-mail addresses, phone numbers and other personal information. The hackers started their attack by sending phishing e-mails, including malware, to employees of a third-party vendor, but it was not known if only one vendor was targeted. In addition, it was suspected that the malware in question was Citadel, a password-stealing bot that was a derivative of the ZeuS banking trojan and allowed the attackers to access Target's network by using stolen credentials. It was estimated that the phishing campaign had started at least two months before the main attack carried out. Brian Krebs was the first to break the news about this attack on his security blog followed by Target's Statement, released a day after.

**Home Depot.** In April 2014, just four months after the Target attack, Home Depot was the victim of a data breach. However, they only started investigations on 2nd September, 2014 and released a statement on 8th September, 2014 [7]. It was found that the attackers, similar to the attackers of Target attack, used third party vendor's credentials to access Home Depot's network. After being inside the retailer's network, the attackers exploited a known vulnerability in Windows XP called "zero-days" in order to escape detection [7]. Finally, this attack resulted in the theft of 53 million e-mail addresses and 56 million credit card accounts.

**German Steel Mill.** In late 2014 (no specific date was provided), Germany's Federal Office for Information Security (BSI) released a report communicating that a German steel mill had been attacked. The attackers' point of entry was the plant's business network and the infiltration was made possible with a spear phishing attack [8]. The

phishing emails could have had a malicious attachment or a link to a website from where malware could be downloaded. Once the malware was installed, the attackers were able to take control of the production software. SANS Institute provided the BSI's report, translated to English, where it is mentioned that the attack resulted in an incident where the furnace could not be shut down properly, and as a result, it led to a "massive damage" to the German steel mill.

**Dragonfly - 1st tactic.** A cyber-espionage group, known as Dragonfly or Energetic Bear, began a campaign in late 2010 [9] with the intention of targeting the energy sector and industrial control systems (ICS) through their Supply Chain. In other words, the Dragonfly group attacked the suppliers of the target instead of attacking the target directly.

The Dragonfly group applied at least three different infection tactics against victims in the energy sector. The first one was an email spear-phishing campaign and is examined in this section. However, the Dragonfly group used two main pieces of malware in its attacks. Both are Remote Access Tool (RAT) type malware enabling the attackers to access and control the compromised computers.

The favoured malware tool of the Dragonfly group was Backdoor.Oldrea, which was also known as Havex or the Energetic Bear RAT. Symantec reported that Oldrea was used in around 95% of infections. This malware acted as a back door for the attackers onto the victim's computer, enabling them to extract information and install further malware. In particular, Oldrea, gathered system information such as operating system, computer and user name, country, language, Internet adapter configuration information, available drives, default browser, running processes, desktop file list, My Documents, Internet history, program files, and root of available drives. In addition, Oldrea collected data from Outlook (address book) and ICS related software configuration files [10]. All this data was collected and written to a temporary file in an encrypted form before it was POSTed to the remote C&C (command-and-control) server controlled by the Dragonfly attackers. Moreover, the second main malware tool used by the Dragonfly group was Trojan.Karagany. It was a back door programmed in C/C++ and used mainly for reconnaissance operations. Specifically, it was designed to download and install additional files and exfiltrate data. Moreover, it had plugin capability and its payload was approximately 72 KBs in size. Finally, Trojan.Karagany contained a small embedded DLL file, which monitored WSASend and send APIs for capturing "Basic Authentication" credentials [10].

According to the first approach (i.e., email spear-phishing campaign), selected executives and senior employees in target companies received emails with a malicious PDF attachment. Symantec states that the infected emails had two possible subject lines: "The account" and "Settlement of delivery problem". In addition, all the emails were from a single Gmail address. The email spear-phishing campaign was conducted from February 2013 to June 2013 [10].

### 2.2 Watering Hole Attacks

To attack an organization, cyber criminals "trojanize" a legitimate website often visited by the target company's employees. RSA Advanced Threat Intelligence Team

correlated this behaviour with the one of a lion waiting for its prey at a watering hole, hence the name. RSA was the first to use the term "watering hole", in late July 2012 [11]. Here are a few examples of watering hole attacks from the wild.

**VOHO.** According to [11], "VOHO" campaign targeted Financial Services or Technology Services in Massachusetts and Washington, DC. This campaign worked by inserting JavaScript element in the legitimate website that would redirect the victim (i.e., website visitor) unknowingly to an exploit website. Then, the exploit website would check if the user was running a Windows machine and Internet Explorer browser, and then it would install a version of "gh0st RAT". "gh0st RAT" was a Remote Access Trojan that allowed attackers to control the infected endpoints, log keystrokes, provide live feeds of webcam and microphone as well as download and upload files.

**Dragonfly - 2nd tactic.** As described before in "Dragonfly - 1st tactic" section, the Dragonfly group has used at least three infection tactics against targets in the energy sector. After the earliest tactic (i.e., email spear-phishing campaign) that was described in "Dragonfly - 1st tactic" section, the Dragonfly attackers shifted their focus to watering hole attacks. It was noticed that this shift happened in June 2013 [10]. The Dragonfly attackers compromised a number of energy-related websites and injected an iframe into each of them. Then, this iframe would redirect users to another legitimate, but also compromised, website hosting the Lightsout exploit kit, as shown in **Fig. 1**. This in turn would exploit either Java or Internet Explorer to download Oldrea or Karagny on the target's machine. Besides, in September 2013, the Dragonfly group started using a new version of this exploit kit, known as the Hello exploit kit. The main web page for this kit contained JavaScript that was able to identify installed browser plugins. Then, the victim was redirected to a URL which in turn determined the best exploit to use according to the collected information [10].

**Shylock.** In November 2013, BAE Systems Applied Intelligence announced that a series of legitimate websites had been infected with the Shylock malware [12]. The cyber-criminals infected a legitimate website by inserting a JavaScript file that initially identified when the browser was used and then this JavaScript file was responsible to show a message, in the browser's style, prompting the user to download the malware that, however, was presented as innocent software. BAE Systems gave the following message example: "Additional plugins are required to display all the media on this page", with a button saying "Install Missing Plugins…". In case that the user decided to proceed and install the "missing plugins", the Shylock malware was installed on his/her machine.

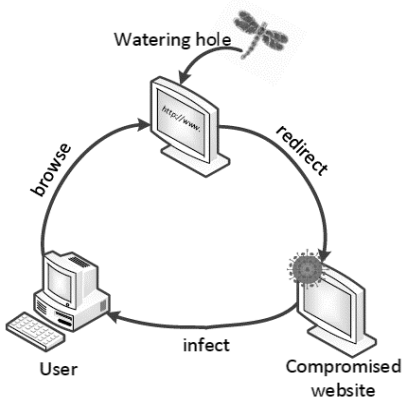


**Fig. 1.** Watering Hole Attack.

### 2.3 Attacks based on "trojanized" third-party software

This section includes a real-life example of attacks based on "trojanized" software of ICS equipment providers.

**Dragonfly - 3rd tactic.** The third tactic of the Dragonfly group was the infection of a number of legitimate software packages. Particularly, three different ICS equipment providers were targeted and the Dragonfly attackers inserted malware into the software bundles that these providers had made available online for download from their websites [10]. The first provider discovered that it was compromised shortly after infection, but the malware had already been downloaded 250 times. The second provider had infected software available for download for at least 6 weeks and the third provider had infected software available online for 10 days, approximately.

### 2.4 Attacks based on Malicious Code and Counterfeit Certificates

This section includes two examples of attacks based on malicious code and counterfeit certificates in industrial environment.

**Stuxnet.** The German Steel Mill attack described earlier is not the first attack that caused physical damage of equipment. The first one was the Stuxnet attack [13] that was designed to target SCADA systems and was responsible for attacking an Iranian nuclear facility. Stuxnet exploited four zero-days vulnerabilities, compromised two digital certificates, injected code into ICS and hid the code from the operator [14]. After implementing the code (process that probably took a long time), the attackers had to steal digital certificates, in order to avoid detection [14]. Stuxnet compromised the system via USB and infected every Windows PC it could find. However, in terms of controllers, it was much pickier. It targeted only controllers from one specific manufacturer (Siemens).

**Meltdown and Spectre.** In the early 2018, researchers revealed that almost every computer chip manufactured in the last 20 years contains fundamental security flaws, with specific variations on those flaws being named Meltdown [15] and Spectre [16]. The flaws arise from features which are built into chips and enable them to run faster. These vulnerabilities allow attackers to use malicious programs to get access to data previously completely protected. It is accomplished by exploiting two important techniques used to speed up computer chips, called speculative execution and caching.

### 2.5 Attacks based on Tampered Devices

This section includes a real-life example of attacks based on tampered devices in business environment.

**Michaels Stores Attack.** In May 2011, Michaels Stores reported an attack that allowed criminals to steal credit and debit cards and the associated PIN codes. To steal this information, attackers tampered at least 70 point of sale (POS) terminals [17]. In a blog entry from Krebs on Security, Krebs explained that there are few ways to tamper with POS terminals. One way is to have pre-compromised terminals ready to be installed at the cash register. In addition, fake POS terminals can also be used to record data from swipe cards and PIN entry. For precaution, Michaels Stores replaced 7,200 PIN pads and trained employees to check regularly if the equipment had been compromised.

## 3 Security Framework for the Semiconductor Supply Chain Environment

### 3.1 Definition of the Security Framework

The security framework for the Semiconductor Supply Chain environment should provide appropriate security mechanisms to address the specific security challenges of the Semiconductor Supply Chain in a more effective and efficient manner. As it is shown in Fig. 2, the security mechanisms of the proposed framework will be based on the SSL/TLS and OAuth 2.0 protocols, which are two standard security protocols. The SSL/TLS protocol is the de facto standard for secure Internet communications and the OAuth 2.0 protocol is the industry-standard protocol for authorization. However, both the SSL/TLS protocol and the OAuth 2.0 protocol are vulnerable to a number of attacks, and thus more sophisticated security mechanisms based on these protocols should be designed and implemented in order to address the specific security challenges of the Semiconductor Supply Chain in a more effective and efficient manner. Specifically, as it is shown in Fig. 2, the proposed framework is focused on security mechanisms for the following two types of communication in the Semiconductor Supply Chain Environment: (i) Client-to-Server communication, and (ii) Server-to-Server communication. Thus, the security framework should include appropriate se-

curity mechanisms ensuring secure data communication between the partners' clients and partners' servers, and appropriate security mechanisms ensuring secure data communication between the servers of the Semiconductor Supply Chain partners. The security mechanisms for the Client-to-Server communication will be based on the SSL/TLS and OAuth 2.0 protocols, and the security mechanisms for the Server-to-Server communication will be based only on SSL/TLS protocol.

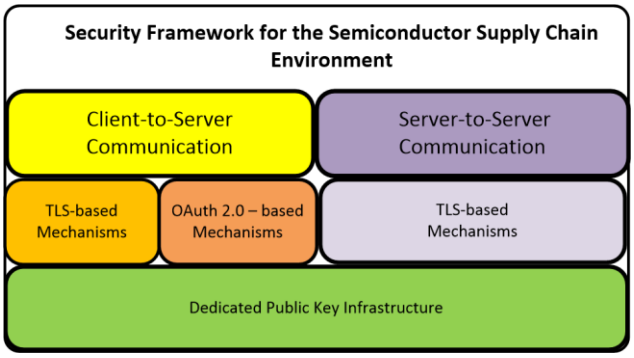


**Fig. 2.** Security Framework.

### 3.2 Dedicated Public Key Infrastructure (PKI) for the Semiconductor Supply Chain Environment

In this section, we provide the description of the dedicated Public Key Infrastructure (PKI) that is an essential component of the Security Framework of the Semiconductor Supply Chain Environment. The dedicated PKI is responsible for issuing and managing all the required digital certificates that will be used by the security mechanisms.

**Public Key Infrastructure.** In principle, a public key infrastructure (PKI) is based on digital certificates. Digital certificates are sometimes also referred to as X.509 certificates or simply as certificates. PKI is defined by RFC 2822 (Internet Security Glossary) as a set of software, hardware, encryption technologies, people and procedures that allow a trusted third party to establish the integrity and ownership of a public key. Furthermore, the trusted third party, called Certification Authority (CA), typically issues the certificates. The CA signs the certificate by using its private key. Moreover, it generates the corresponding public key to all eligible participating parties.

**Dedicated PKI Trust Model.** The dedicated PKI trust model for the Semiconductor Supply Chain Environment follows the traditional hierarchical PKI trust model which is based on the establishment of superior-subordinate CA relationships (See Fig 3). It can be represented as a tree with the root at the top and the branches extending towards the bottom. The elements of the inverted tree are nodes and leaves. The nodes represent the CAs and the leaves represent the end entities. The root (i.e., CA) is the

node located at the top of the inverted tree and below the root CA there are zero or more layers of subordinate CAs. The root CA is the starting point for trust and issues a self-signed certificate as well as certificates to subordinate CAs that are immediately below it but not to the end entities. Subordinate CAs, in turn, issue certificates to the next lower level subordinate CAs or end entities, respectively.

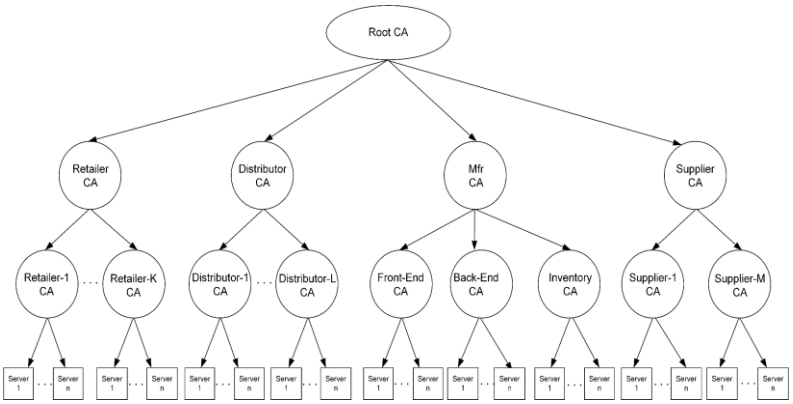


**Fig 3.** Dedicated PKI Trust Model.

According to the dedicated PKI trust model, each of the retailers, distributors, front-end components, back-end components, inventories, and suppliers hosts its own CA that issues the certificates of its registered end-users (i.e., servers). In addition, there is a CA (i.e., Retailer CA) that issues the CA certificates of all the CAs which are set up into the retailers of the specific Semiconductor Supply Chain environment. Moreover, there is a CA (i.e., Distributor CA) that issues the CA certificates of all the CAs which are set up into the distributors' premises. Furthermore, there is a CA (Manufacturing (Mfr) CA) that issues the CA certificates of the CAs which are set up into the front-end component's premises, back-end component's premises and inventory. Similarly, there is a CA (i.e., Supplier CA) that issues the CA certificates of all the CAs which are set up into the suppliers' premises. Finally, there is a CA (i.e., Root CA) that issues the CA certificates of the Retailer CA, Distributor CA, Manufacturing (Mfr) CA, and Supplier CA. It is supposed that the Root CA, Retailer CA, Distributor CA, Manufacturing (Mfr) CA, and Supplier CA are controlled by the main entity (e.g., Infineon) of the specific Semiconductor Supply Chain environment in order to avoid trust concerns associated with subordination between the participating entities belonging to different domains.

## 4 Conclusion and Future Work

In this paper, we provided a number of representative examples of various attacks that have been witnessed in the wild and can cause potential security issues and challenges in the Semiconductor Supply Chain Environment. Furthermore, Moreover, we provided a categorization of the various attack examples based on the intrusion method

that they use to compromise the target and gain a persistent foothold in the target's environment. Furthermore, we proposed a security framework for secure data communication across the partners in the supply chain. The security mechanisms of the proposed framework will be based on the SSL/TLS and OAuth 2.0 protocols, which are two standard security protocols. However, both protocols are vulnerable to a number of attacks. Thus, as future work, we plan to design and implement more sophisticated TLS – based mechanisms and OAuth 2.0 – based mechanisms for the proposed security framework in order to address the specific security challenges of the Semiconductor Supply Chain in a more effective and efficient manner.

## Acknowledgment

The work has been performed in the project Power Semiconductor and Electronics Manufacturing 4.0 (SemI40), under grant agreement No 692466. The project is co-funded by grants from Austria, Germany, Italy, France, Portugal (from the fundação para a ciência e Tecnologia - ECSEL/0009/2015) and - Electronic Component Systems for European Leadership Joint Undertaking (ECSEL JU).

## References

[1] T. Dierks, "The Transport Layer Security (TLS) Protocol Version 1.2," *RFC 5246*, vol. RFC 5246. pp. 1–104, 2008.

[2] D. Hardt, "The OAuth 2.0 Authorization Framework [RFC 6749]," *RFC 6749*, pp. 1–76, 2012.

[3] J. Hong, "The State of Phishing Attacks," *Com. ACM*, vol. 55, no. 1, pp. 74–81, 2012.

[4] GReAT, "The Icefog APT : A Tale of Cloak and Three Daggers," *Kaspersky Labs*. 2013.

[5] G. Mantas, N. Komninos, J. Rodriuez, E. Logota, and H. Marques, "Security for 5G communications," Fundamentals of 5G Mobile Networks, pp. 207–220, 2015.

[6] B. Krebs, "Target Hackers Broke in Via HVAC Company," *Krebs on Security*. 2014.

[7] B. Hawkings, "Case Study: The Home Depot Data Breach," *SANS Institute*. 2015.

[8] B. Krebs, "Sources: Target Investigating Data Breach," *Krebs on Security*. 2013.

[9] N. Nelson, "The Impact of Dragonfly Malware on Industrial Control Systems," 2016.

[10] Symantec, "Dragonfly: Cyberespionage Attacks Against Energy Suppliers," 2014.

[11] Will Gragido, "Lions at the Watering Hole – The 'VOHO' Affair," *RSA*. 2012.

[12] BAE Systems Applied Intelligence, "Shylock. Banking malware. Evolution or revolution?," 2014.

[13] Kim Zetter, "A cyberattack has caused confirmed physical damage for the second time ever," *Wired*. pp. 1–19, 2017.

[14] N. Falliere, L. O. Murchu, and E. Chien, "W32.Stuxnet Dossier," vol. 4, Feb. 2011.

[15] M. Lipp *et al.*, "Meltdown," no. ArXiv eprints. arXiv: 1801.01207, 2018.

[16] P. Kocher *et al.*, "Spectre Attacks: Exploiting Speculative Execution *," no. ArXiv eprints. arXiv:1801.01203, 2018.

[17] B. Krebs, "Breach at Michaels Stores Extends Nationwide," *Krebs on Security*. 2011.