Cybertrust in e-Learning Environment based on Network Time Synchronization

Dmitriy Melnikov, Vladislav Petrov, Natalia Miloslavskaya, Anatoliy Durakovskiy
and Tatiana Kondratyeva
National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
31 Kashirskoye shosse, Moscow, Russia

Keywords: e-Learning, Information Security, Trusted Cyberspace, Trusted e-Learning Environment.

Abstract: The concept of cybertrust as a crucial aspect of cyber security for public electronic interactions and, in particular, distance learning systems (DLSs), is introduced. This concept is the opposite of such well-known terms as cyberattacks and/or cyberespionage and it supports cyber security issues by providing legal significance of a public electronic document interchange. The possibility of cybertrust assurance in an e-Learning environment (ELE) is shown using two proposed methods of network time synchronization.

1 INTRODUCTION

Any computer information system (as an integral part or a degenerate case of cyberspace), even with hardware and software protection of its information resources, remains vulnerable not only to the traditional cybersecurity threats such as loss of connections (unavailability – A), interception (breach of confidentiality – C) and modification (falsification, integrity violation – I) of information circulating in the system, but also to its legal value. The complex nature of the cybersecurity assurance is reflected in the acronym CIA and suggests that a compromise provided by users' trust to the system as a whole is needed for real interrelation between the purpose of the integrated cybersecurity CIA and critical resources (hardware, software and data). The issue of universal trust problem resolution becomes one of the priorities for integrated cybersecurity for all common systems of public computer information infrastructures, and, in particular, for distance learning systems (DLSs) (Pfleeger and Pfleeger, 2003). Therefore, in our opinion, to highlight this issue as a separate study subject it is necessary to introduce the term "cybertrust" as one of the aspects of cybersecurity in e-Learning Environments (ELE).

Thus the paper is organized as follows. Section 2 is devoted to the analysis of the current state of the trust problem in respect of developing of a generalized cybertrust model. Section 3 discusses the main characteristics of cybertrust assurance in ELE. Section 4 shows the practical implementation of the cybertrust through the usage of network time synchronization that allows to increase the reliability and quality of the various kinds of legally significant electronic document interchange. In conclusion main results of the work are outlined and future research is specified.

2 RELATED WORKS

Let us define that any public cyberspace based on the Internet technologies could be perceived as safe and its results are recognized as legally significant iff all its components (such as participants of the information exchange process, communication channels and software and hardware) meet the objectives and requirements of information security (IS) properties (CIA properties).

The basic analysis of principles and public trusted cyberspace organization assumptions, for example, in DLSs based on the evaluation of protection against IS threats (CIA violation threats), suggests that IT does not guarantee the required security level in many cases even by using the traditional information protection tools (IPTs) (Petrov at all, 2015). Thus, the task of cybertrust assurance in ELE continues to be relevant and requires special phrasing (Benzel et al, 2005), (Gritzalis and Lopez, 2009),

Melnikov, D., Petrov, V., Miloslavskaya, N., Durakovskiy, A. and Kondratyeva, T.
Cybertrust in e-Learning Environment based on Network Time Synchronization.
In *Proceedings of the 8th International Conference on Computer Supported Education (CSEDU 2016) - Volume 2*, pages 402-407
ISBN: 978-989-758-179-3

(Gasiorowski-Denis, 2015).

In our opinion the expansion of the so-called “Three trusts” criterion (Petrov at all, 2015), introduced to confirm the required level of ELE’s security (proxy) for any public cyberspace, is quite productive. A generalized cybertrust model (Figure 1) should contain three sub-models: 1) for presentation of the *trust interrelations* among the objects of cyberspace integrally (considered as a whole), 2) for the *hardware and software components* to ensure trust associated with the reference medium, 3) for the *remote user's* (participant of the distance interaction process) trusted perception. The first sub-model for presentation of the trust interrelations among the objects of cyberspace integrally describes the relationship between hardware and software objects of each of the systems participating in the cyberspace. The second sub-model for the hardware and software components shows the trusted characteristics of the interaction between objects and trusted ELE. The third sub-model for the remote users’ perception is a set of conditions directly depending not only on the characteristics of software and hardware but also on the user that affect the trusted cyberspace.

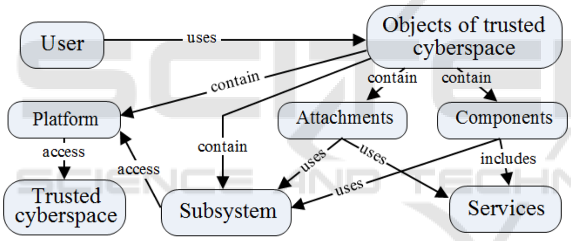

Figure 1: A generalized cybertrust model.

Additionally, a legal user’s model should be constructed. It is assumed that each response directly affects the overall level of trust in the system. However, such a model can be regarded as sufficient for ensuring information exchange’s security only when it is initially supposed that its participant is not a potential insider. To ensure cybertrust in ELE identification and authentication data (i.e. the attributes that differentiate the participants from the others, including the usage of removable media of key information) are supplemented with data related to the continuous user’s presence verification being in a certain place. Only the legal users are obliged to be present at the legally valued electronic document interchange (LVEDI). This can be guaranteed by the continuity of the authentication procedures.

Thus, the cybertrust problem solution lies in the development of generalized integrated requirements establishing the procedures of legal users’ electronic interaction and regulated requirements to their automated working stations (AWSs) as well as to all members of the LVEDI.

3 CYBERTRUST KEY FEATURES

From all the variety of procedures in ELE it is possible to highlight the most critical for ensuring cybertrust. So, it is obvious that identification and authentication, access control and connection protection are such controls for the LVEDI (Miloslavskaya et all, 2014). Most of the existing definitions of trust are applicable to cybertrust. They can be used to formulate the criterion of the trust building. The characteristics of trust, which are important for the formulation of the trust criterion in information systems, are the following: 1) *targeted trust:* trust of oriented relations between the process participants; 2) *subjective trust:* trust is in fact a personal opinion. It is a personal and subjective phenomenon based on various factors or evidence, some of which may have more value than the others; 3) *measurable trust:* the target trust values can be used to assess different levels of trust that an object can have in contact with another object. Therefore, such kind of trust (measurable) provides a framework for trust modeling and for its evaluation; 4) *trust in the dynamics*: trust usually varies nonmonotonically with time. It can be updated periodically or canceled. It should be able to adapt to the changing environmental conditions in which the first trust decision has been made; 5) *conditionally passed trust:* information on trust can be transmitted/received via the interaction network; 6) *trust as a composite property:* trust is a set of different attributes, which should be considered depending on the environment in which the trust is determined (Grandison and Sloman, 2000).

Therefore, we can say that compositionality (as a value of a complex expression is a function of its parts values and the relations between them) it is an important feature for the trusted electronic interaction creation.

Taking into consideration the outlined above, we can assume that the creation of a trusted cyberspace should be based on a combination of factors that directly affect the level of trust, as it is shown in Figure 2. It should be noted that all these factors may be involved in the implementation of the above mentioned criterion of “Three trusts” only in case of network time synchronization. Then, in our opinion, it is reasonable to ensure modular cybersecurity, for example, in the devices of the LVEDI’s participants in order to carry out dynamic prevention, detection, diagnosis, isolation and countermeasures against IS properties violations.

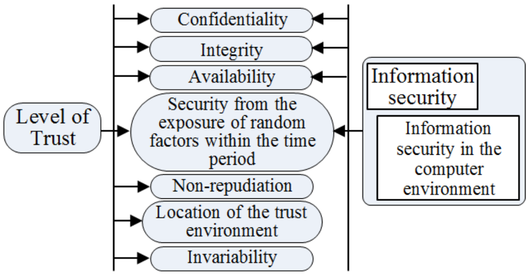
Confidentiality
Integrity
Availability
Security from the exposure of random factors within the time period
Non-repudiation
Location of the trust environment
Invariability
Level of Trust
Information security
Information security in the computer environment

Figure 2: The combination of cybertrust factors for the LVEDI.

4 TIME SYNCHRONIZATION AS A CYBERTRUST ASSURANCE METHOD

A time synchronization system in a cyber environment is an obligatory and extremely important subsystem that affects the functioning of almost every network component and resource. The accuracy of the network time (of synchronization) is not only of great technological importance, but it also becomes a factor affecting the reliability and quality of cryptographic functions and calculations as well as managing the LVEDI based on the timestamps usage. However, maintaining high quality network time synchronization depends on reliability (correctness) of the operation of the following: 1) software and hardware time modules available in the operating system (OS) of each computer, server and network device. The last one depends on the reliability (correctness) of OS functioning; and 2) synchronization subnet (network time infrastructure), which is implemented on the basis of the Network Time Protocol (NTP version 4 – NTPv4) (Mills, 2010).

Compromise of at least one of these components (time modules, OS and synchronization subnet or its segments) may lead to the discrediting of entire application systems and services, and as a result to the loss of cybertrust.

4.1 Creating Timestamps in Software and Hardware

There is a clock in any computing system (CS), which is used for time and synchronization frequency generation. The flowchart of system time generation for timestamps is shown in Figure 3.

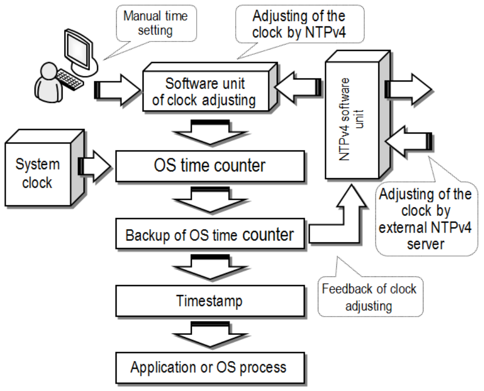
Manual time setting
Adjusting of the clock by NTPv4
Software unit of clock adjusting
NTPv4 software unit
System clock
OS time counter
Adjusting of the clock by external NTPv4 server
Backup of OS time counter
Feedback of clock adjusting
Timestamp
Application or OS process

Figure 3: Cross-functioning flowchart of the system time generation.

In the current CSs the system time is based on the clock pulse generator and two seconds counters (basic and back up). In other words, the date (day, month and year) and time (hours, minutes and seconds) are described by a certain number of seconds (as a power of number 2). The accuracy of the current time is determined by a fractional part, which describes the fraction of a second (Mills, 2010). The main time counter operates continuously, stopping only at correcting the current time value, taking into account the necessary amount of time spent on adjustments. The backup counter repeats the time value, shown by the main counter, and it is used to read the current time for the system and application processes as well as to generate a correction value by NTPv4 (at regular intervals).

In some OSs the fractional seconds of the backup counter is used as a random number generator. In reality the reading of the current time value is a random event, so the fractional part of a second can be seen as a random binary number.

4.2 Cyberespionage Model for CS's Timestamps Modification

One of the requirements (conditions) to ensure a high level of cybersecurity is reliability (warranty) of CSs' functioning, ensuring, in turn, the operation of IPTs. As it was mentioned above, any procedure directly providing the implementation of the security mechanisms or access to security services should be trustful. At present many OSs do not meet this requirement and are untrusted (not reliable). It is very difficult to verify the correct functioning of a certain system and application processes.

We consider the following possible cyberattack model for the current time generation system on the CS (Figure 4).

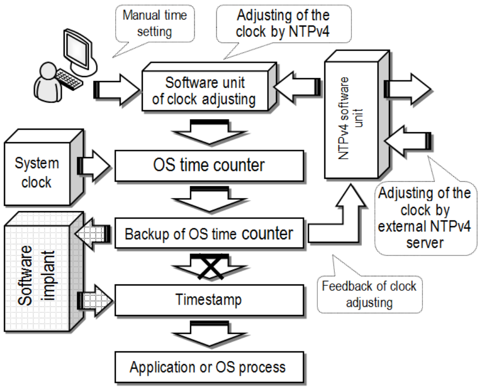
Manual time setting
Adjusting of the clock by NTPv4
Software unit of clock adjusting
NTPv4 software unit
System clock
OS time counter
Adjusting of the clock by external NTPv4 server
Software implant
Backup of OS time counter
Feedback of clock adjusting
Timestamp
Application or OS process

Figure 4: Model of cyberattacks using the IST insertion to modify the current time value.

At the basis of this attack is the introduction of an inset software tool (IST) in a non-trusted OS to modify the current time value. IST functioning content is to change the pre-known algorithm for the fractional part (of a second) of the system time. For example, the algorithm of a fractional part forming may be based on a specific procedure for the conversion of the whole of the current time value. That is, the fractional part of the current time (Ct) will directly depend on (is a function of) the integer part of the Ct. The timestamp formed in this way will consist of the real (true) integer part of Ct and of the modified fractional part (not random and pseudo-random).

An intruder inserting an IST in an untrusted OS knows the algorithm for converting the integer part of Ct into its fractional part. Consequently, s/he does not have to know the geographical location of a compromised CS. It is enough to know the time zone for it. From the viewpoint of the IST detection, it will be extremely difficult to identify a modification of the fractional part of the current time for the following reasons.

1. It is very difficult to distinguish random fractional part of the current time values from the pseudorandom by any external signs, taking into account that the fractional part is composed of milliseconds, microseconds or even nanoseconds, for example, while using the fractional part as the basis for the random numbers generation.

2. Even if one collects a certain statistics of the generated current timestamps, it is unlikely to reveal the algorithm for converting the integer part of Ct into its fractional part, providing that the perpetrator used a cryptographically complex function in his/her IST.

3. If more than one timestamp is demanded for one second, then it is possible to add some relevant complication coefficients in the IST that will make the difference between the timestamp's fractional parts in the modification of the same integer of seconds. The number of these coefficients depends on the execution speed of the compromised CS.

4. In this cyberattack model, the IST operation does not affect the other components of the CS as well as the procedures implemented by NTPv4-module software. In other words, properly integrated IST will not allow to detect itself via any system or application process.

In implementing the cyberattack model considered (based on IST insertion) the following activity of the intruder may result in very "severe" consequences. The main purpose of modifying the system time is a compromise of the secret (private) key of the cyberattack target based on the knowledge of timestamp and the interception of his/her digital signature (DS) in the Public Key Infrastructure (PKI) (Cooper, 2008). In terms of IS compromising the IST insertion provides almost unlimited unauthorized access to the protected information.

The cyberattack essence after the IST insertion is the following.

1. The compromised computer holder's DS interception.

2. The timestamp regeneration in DS. The amount of timestamps options depends on the selected analysis interval for time and the number of complication coefficients. The total number of options will not exceed 3000.

3. Further the "plaintext selection" cryptanalytic attack is implemented. The falsified timestamp appears as a "chosen plaintext" in this attack.

4. The secret (private) key of the cyberattack target can be compromised as a result of decryption (in the event the IST was inserted in his computer).

5. If the cyberattack target exchanges information with the owner of the compromised computer, then it is possible to compromise the key of the cyberattack target by using his/her uncovered secret (private) key.

6. In the future, the secret keys of all users carrying out a protected information exchange with the owner of the compromised computer can be revealed step-by-step.

A more detailed analysis shows that the number of compromised CSs could compromise the entire PKI. Naturally, the compromise will not happen in a moment. It will be a number of targeted and serial successive events as the steps of one cyberattack. But the final result is obvious.

A similar situation may arise with the Kerberos protocol (Kohl and Neuman, 2005), (McNamara, 2003), which is vulnerable to attacks on the systems of network synchronization and time stamping. The one-time password systems are also "powerless" against cyberattacks based on modifying a CS's system time (Haller, 1998).

4.3 Principles of Network Time Reliability Insuring

We worked out the following principles of network time reliability insuring.

The first and fundamental principle of reliable and correct functioning of the network time system (NTS) for modern networks and systems is to achieve the given guarantees of such operation (Mills, 2010). This principle implies the presence of a trusted operating environment that provides services to ensure cybersecurity as well as other software components (modules) supporting NTS operation and provision of the required services.

The second principle is the creation of an internal and independent time source that must operate in stand-alone mode. This principle implies that the time source should receive the original signal generated by a system process of a trusted OS. The output internal clock's signal can be such a signal. Otherwise, the signal coming via a USB-interface may be such a signal.

The third principle means that the whole conversion of the input signal must be carried out only by the time source. Any interference in the work of the time source is not acceptable, since any exposure could affect its reliability.

The fourth principle can be formulated as follows. If necessary (in case of the abnormal events), any adjustment of the time source should be carried out at the user's (client) demand and only in manual mode via the GUI displayed on the computer screen. This principle implies the transfer of a specialized request for certified and protected timestamp from a trusted time source, determined by the appropriate security policy. The implementation of this principle depends on the conditions of the NTS's usage and the corporate (specialized) applied cyberspace. In other words, if such a system is able to provide the timestamp transmission in protected mode (providing its confidentiality and/or integrity), then the client can give a command to automatically update the time. The need to deliver the timestamp in the protected mode can be caused by certain statements of the security policy, aimed at protecting the LVEDI and this entire system against the insiders.

The fifth principle says that the launch of the time source should be carried out only at the command of the NTS's client and only once at the beginning of its work. This principle implies the automatic transfer of a specialized request for certified and protected timestamp from a trusted time source, determined by the appropriate security policy. Otherwise, the initial (current) time value should be entered by the user. The implementation of this principle depends on the conditions of NTS's usage and the corporate (specialized) applied cyberspace. In other words, if such a system is able to provide the timestamp transmission in protected mode (ensuring its confidentiality and/or integrity), then the NTS can give a command to get an initial timestamp during initialization of its work. The need to deliver the timestamp in protected mode can be caused by certain statements of the security policy, aimed at protecting the LVEDI and this entire system against the insiders.

The sixth principle is the two-module construction of the time source, including a main time counter and a back-up counter, wherein the main counter should operate from the start to the end of the session without any interruptions or stops.

The strict implementation of the given principles will prevent any intentional and accidental actions to modify and/or falsify the timestamps.

4.4 Reflection of Cyberattacks against the NTS

The methods proposed (Figures 5 a, b) are actually based on the principles of cyberattacks against the NTS (synchronization) reflection (Melnikov and Jones, 2004). In the first method of reflection of cyberattacks against the NTS the start time is set automatically, while in the second method this time is set manually. The essence of both methods is that the usage of an internal independent time source allows to exclude any possibility of timestamps unauthorized modification and/or tampering. This in turn will considerably (more than twice) complicate the task of cryptanalysis based on plaintext selection, being resolved by a potential intruder (Cooper, 2008), (Kohl and Neuman, 2005).

5 CONCLUSIONS

Thus, from our point of view, the expansion of the "Three trusts" criterion to any public cyberspace together with the usage of an independent source of network time synchronization will allow to implement the standardized cybertrust assurance requirements (being of legal significance) for ELE. It can also become the basis of appropriate legislation, regulations or standards.

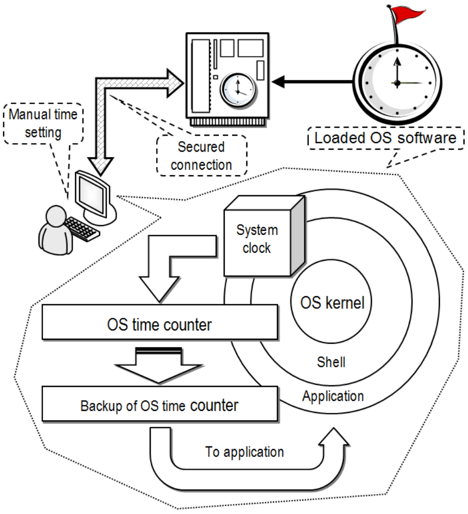

Figure 5a: The first method of reflection of cyberattacks against the NTS with the automatic start time setting.

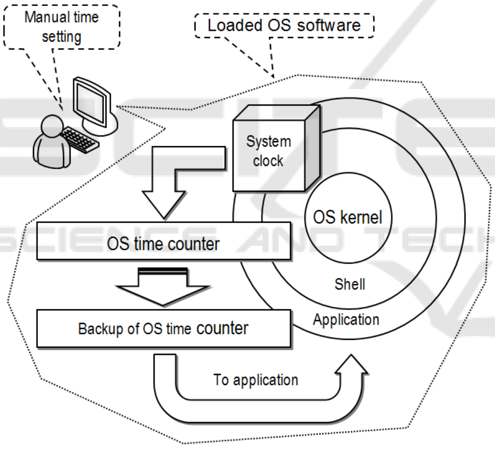

Figure 5b: The second method of reflection of cyberattacks against the NTS with the manual start time setting.

ACKNOWLEDGEMENTS

This research has been performed with the financial support of the Ministry of education and science of the Russian Federation in the framework of the project «Creation of the engineering and technical solutions for high-tech production of innovative software and hardware information protection tools on the basis of perspective high-speed interfaces of information interconnection», jointly with the LLC «OKB SAPR» (the contract N 02.G25.31.0050).

REFERENCES

Benzel, T.V., Irvine, C.E., Levin, T.E., Bhaskara, G., Nguyen, T.D., Clark, P.C., 2005. *Design principles for security. Technical Report NPS-CS-05-010.* http://www.cisr.us/downloads/techpubs/nps_cs_05_010.pdf (access date 05.12.2015).

Cooper, D., 2008. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. RFC-5280, May 2008.

Gasiorowski-Denis, E., 2015. *Trust and confidence in cloud privacy.* http://www.iso.org/iso/news.htm?refid=Ref1921 (access date 27.11.2015).

Grandison, T., Sloman, M., 2000. *A survey of trust in internet applications*. IEEE Communications Surveys and Tutorials, 3(4), pp. 2–16.

Gritzalis, D., Lopez, J., 2009. *In Law We Trust? Trusted Computing and Legal Responsibility for Internet Security*. Emerging Challenges for Security, Privacy and Trust. 24th IFIP TC 11 International Information Security Conference, SEC 2009, Pafos, Cyprus, May 18–20, 2009. Proceedings. 2009. Pp. 399-409.

Haller, N., ed. 1998. *A One-Time Password System*. RFC-2289, February 1998.

Kohl, J., Neuman, C., 2005. *The Kerberos Network Authentication Service (V5)*. RFC-4120 (RFC-4537), July 2005.

McNamara, J., 2003. *Secrets of Computer Espionage: Tactics and Countermeasures*. New York: John Wiley & Sons, Inc.

Melnikov, D., Jones, A., 2004. *"Masquerade" Attacks and a Process for Their Detection*. In *Proceedings of the 3rd European Conference on Information Warfare and Security. Royal Holloway University of London, UK. 28-29 June 2004*. p. 269.

Mills, D., 2010. *Network Time Protocol Version 4: Protocol and Algorithms Specification*. RFC-5905, June 2010.

Miloslavskaya, N., Petrov, V., Tolstoy, A., 2014. *Security Aspects for E-Learning Portals.* In *Proceedings of the 6th International Conference on Computer Supported Education (CSEDU 2014)*. Spain, Barcelona. pp. 427–432.

Petrov, V., Miloslavskaya, N., Gorbatov, V., Durakovskiy, A., 2015. *Problem of Trust in E-Learning Environment*. In *Proceedings of the 7th International Conference on Computer Supported Education (CSEDU 2015)*. Portugal, Lisbon. pp. 424-429.

Pfleeger, C.P., Pfleeger, S.L., 2003. *Security in Computing.* Upper Saddle River, Prentice Hall, NewJersey.