A Mathematical Model of a Trusted Download Violator Process "Hardware Thin Client"

Kirill A. Butsik
ITIZI Dept.
Russia, Rostov-on-Don, RSUE (RINH)
akademik@spark-mail.ru

Evgeniy N. Tishchenko
ITIZI Dept.
Russia, Rostov-on-Don, RSUE (RINH)
celt@inbox.ru

Abstract

The article analyzes a trusted download violator process «hardware thin client» in a typical automation system. The process of loading the operating system into workstation memory both by means of using removable media, and using PXE network boot technology. Analytical modeling of this process from the point of impact of internal and external intruders is being conducted. The formal violator model that is a conditional mathematical representation of their impact on the process of the trusted download is being developed. The factors with increased risk of insider attacks are being determined. The modeling of the ideal process trusted download with a complete opposition to intruders' attack are being conducted. The modeling of the ideal process trusted boot with a complete opposition to intruders' attack are being conducted. The drawbacks of the modern systems of trusted download, based solely on monitoring the status of implementation of protective mechanisms are determined. A list of characteristics that require optimization to develop an alternative method of providing a trusted download «thin client hardware» is presented. It is suggested controlling not the state (reaction) of the defense mechanisms, but the temporal characteristics of the regular download process as an alternative. These specifications are subject to rationing, the preparation and recording of standard values based on the statistics collected during the operation of the automated system in the absence of effects of violators. During each subsequent start of the download process, its temporal characteristics are compared with the normalized value. On the basis of permissible or impermissible difference values it is concluded about the possible impact of insider on the download process. It gives a full control of all stages of the trusted download process, and not only the state of defense mechanisms that occupy only part of the stages.

1 Formal Model of Offender

Modern approaches to the mathematical description of the offenders in the automated (information) systems suggest that any attack of any intruder depends on the following factors: the existence of vulnerabilities in the target system or component of the system (V), the probability of detecting a vulnerability infringer (P) and the ability of the offender to work with the identified vulnerabilities successfully (s) [Ave06, Gol15].

According to the claim that while implementing any automated system (hereinafter - AS) the complete absence of vulnerabilities in its components is fundamentally impossible ($\sum(V) \neq 0$), it is permissible by the use of a binary parameter V = {0,1} transfer to the parameter n - the number of existing vulnerabilities in the attacked AS or its components.

Based on the results of the simulation violators attack outlined in [Gol15] and [Ste12], as well as the claim that any attack could be seen as a set of implementations of attacks on each detected intruder vulnerability it is permissible to submit the resulting ability of the offender to commit a successful attack (S) in the following way:

In: S. Hölldobler, A. Malikov, C. Wernhard (eds.): *YSIP2 – Proceedings of the Second Young Scientist's International Workshop on Trends in Information Processing, Dombai, Russian Federation, May 16–20, 2017*, published at http://ceur-ws.org.

$$S = \sum_{i=1}^{n} (P_i, s_i) \quad (1)$$

It should be noted that in any AS, equipped with complex information protection system (hereinafter - SIS) the task of the offender to identify and exploit of vulnerabilities in the first place is transferred to the space of information protection system itself. That is $S = S_{SIS} + C$, where C - constant, which determines the vulnerability of the AS, is not dependent on the implementation of the information protection system. This idea S_{SIS} is similar to the expression (1).

It should be mentioned that expression (1) and its interpretations in part SIS are true only for the abstract AS.

In the AC built on the basis of "hardware thin client" technology, there is a fundamental division in the direction of the search of vulnerabilities of the violator: the user's workstation (R), communication channels and switching equipment (K) and terminal servers and storage (D) [But15].

Consequently, the success of the attack on the SIS components of such AS is possible to represent as a set of successful attacks in the given directions (without specifying violator's priorities and criticalness of vulnerabilities).

$$S_{SIS} = \sum_{i=1}^{n} S_{Ri} \cup \sum_{i=1}^{n} S_{Ki} \cup \sum_{i=1}^{n} S_{Di} \quad (2)$$

Taking into consideration of advantages of "hardware thin client" technology, one of which is use of terminal operational environment (hereinafter - TOE) it is fair to argue that that only two components are available as part of the SIS on the side of the workstation: trusted download (TD) and the limitation of the software environment of TOE (OPE):

$$S_R = \max\left\{\sum_{i=1}^{n} S_{TDi}; \sum_{i=1}^{n} S_{OPEi}\right\} \quad (3)$$

2 Ideal Model

To describe the ideal model of a trusted download "hardware thin client" it is necessary to determine the functional view (expression) of the trusted download process itself.

The analysis of a typical process of loading of TOE in the workstation memory, as well as the results of the analysis of modern national systems and trusted download algorithms allow us to represent trusted download process by the piecewise function at predetermined variety of intervals – the final stages of the work process of the standard load TOE [But16].

The points of the formula change of such a function are the beginning of the execution of each subsequent stage x_i, где $i \in \{1,2,\dots,7\}$ in case of local download and $i \in \{1,2,\dots,9\}$ – in case of a network. It is important to understand that $x_1 \neq 0$ и $x_i = x_i(t)$, where t – runtime loading stages ($t_0 > 0$).

It means that at zero time and before ($t \leq 0$) function does not exist (not specified) because from a technical point of view, the beginning of the trusted download process coincides with the simultaneous use of all key elements of the AS (workstation, support TOE, switching equipment, etc.). That in general corresponds to the notion "trusted download", adopted by The Russian Federation Federal Service on Technical and Export Control [Inf01].

However, apart from direct dependence on the nominal load stages, the key task of the trusted download process is to confront the violators' attacks. Given the discussed above conditional violator model, it means a reduction of the likelihood and ability of the violator to exploit of vulnerabilities at the each stage of the regular download process to an acceptable minimum. The probability of detection and the violator' ability to operate the vulnerabilities can also be represented by the parametric functions of the execution time at the each stage.

Consequently, the trusted download process can be determined by the function of the success of the violator' attack:

$$S_{TD} \leftrightarrow \begin{cases} f(P,s) \\ P(t) \\ s(t) \end{cases} \quad (4)$$

Then for an ideal case (complete neutralization of the violator' attack): $S_{TD} = 0$ with $\forall t \in x_i$. It is possible to conclude about the about the nature of its continuity and the possibility of its differentiation in any time interval of existence. That is trusted download process is a piecewise smooth function, for which in the ideal case (fig.1).

$$f'(P,s) = \lim_{\Delta t \to 0} \frac{S_{TD}(t + \Delta t) - S_{TD}(t)}{\Delta t} = 0 \quad (5)$$

In turn, the actual process of the trusted download taking into consideration effects (attacks) of the violator is uniquely characterized $f'(P,s) \neq 0$ (fig. 2).

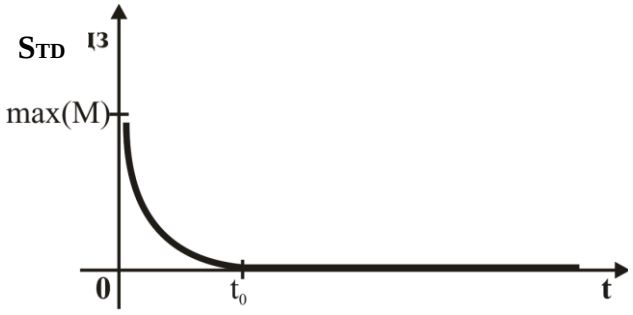

Figure: 1 Conditional representation of perfect trusted download process

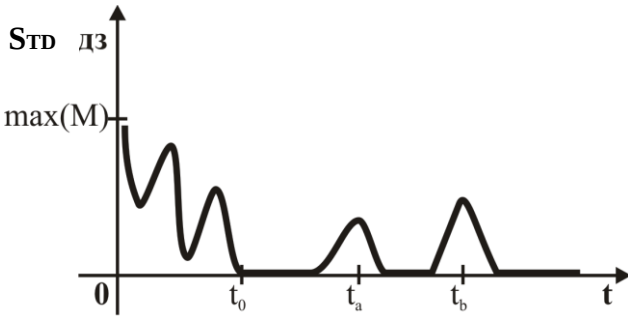

Figure: 2 Conditional representation of actual trusted download process

3 Modern Systems

Based on the data discussed above it is permissible to formulate the basic task of the ideal "trusted download" process as provision a stable neutralization ($S_{TD} = 0$) of violator's possibilities to reveal ($P(t) = 0$) and to exploit ($s(t) = 0$) vulnerabilities in any time period of execution of the each stage of regular download process ($\forall t \in x_i$).

Modern Russian SIS solve this task due to consecutive introduction and exploitation of defense mechanisms (j) [Sch08]. These mechanisms take either a part of a certain stage x_i, or the whole stage. The effectiveness assessment of the trusted download id determined by a total assessment for all introduced defense mechanisms (k) to oppose the violator' attack [Syc15, Zas09]. That is an ideal modern system of trusted download in the frame of the considered above interaction of the violators conditional model can be presented in the following way:

$$S_{TD} = \begin{cases} \sum_{j=1}^{k} f_j(P,s) = 0 \\ f_j'(P,s) = 0 \end{cases} \quad (6)$$

However the expression (6) does not allow to describe the trusted download process where $t \neq t_j$, i.e.in the periods of time which do not connected with the work of the defense mechanisms. Consequently, taking into account the level of the violator's preparation it is possible to conclude that $t \neq t_j \rightarrow 0 < S_{TD}(t) \leq \max(M)$. It can be critical in the cases, when violator's successful attacks on the whole system depend on implementation of indirect (potentially dangerous) attacks on the different stages of the regular download process: $S_{TD} = S(t_a) + S(t_b) = \max(M)$, где $b > a$ и $t_a, t_b \neq t_j$ (fig. 3).

The simplest example is a successful download of an irregular TOE from the third-party removable media after a successful attack on the modification of the software BIOS.

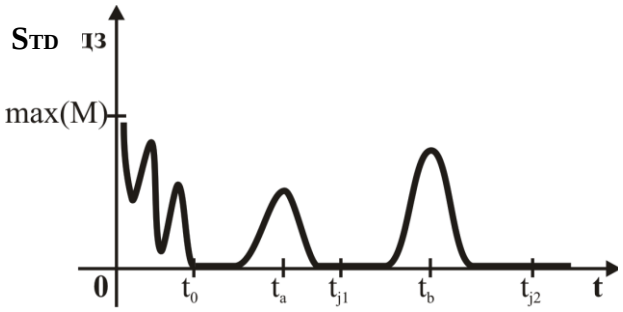

Figure 3: Conditional presentation of modern trusted download systems

Thus, achieving the properties of the ideal model for the modern trusted download systems is possible only due to increase of quality and quantity characteristics of the introduced defense mechanisms to oppose violators' attacks and aimed at revealing and exploiting new (0-day) vulnerabilities both in the components of AS and SIS itself. Game Theory in the presentation of the conflict, "the intruder - administrator" as a directed graph to model the process of "game ahead of the curve" [Zas09, Gor15].

However as soon the violator gets a key advantage connected with the possible exploitation of the revealed vulnerability in the regular download process of TOE regardless vulnerabilities in the defense mechanisms the effectiveness of the implemented trusted download system is to take zero value and the violator's attack success is going to be maximal.

$$S_{TD} = \begin{cases} \sum_{j=1}^{k} f_j(P,s) = 0 \\ f_j'(P,s) = 0 \\ \sum f_i(P,s) = \max(M) \\ f_i'(P,s) \neq 0 \\ t_i \neq t_j \end{cases} \qquad (7)$$

4 Internal Violator

Internal violator in relation to an external one is characterized by a number of distinctive advantages, described in detail in the researches of Russian and foreign experts [Syc15], [Skl04], [Wal13] and [Zag15]:

a) lack of time limits for the attack while dividing it into several independent stages;
b) enough time to study structure and functionality of SIS;
c) possibility to use any components of SIS given to the AS's user in normal manner (e.g. a key media.

It should be mentioned, that depending on implementing the trusted download, the "c" advantage often allows an internal violator to ignore a part of defense mechanisms: $S_{TD} = \max(M)$ при $f_j'(P,s) = 0$.

Given all these advantages it is necessary to specify that expressions (4), (6) and (7) are absolutely applied only for an external violator. In fact while the possibility to reveal $P(t)$ and exploit $s(t)$ vulnerabilities – parametric functions, depending on time to execute the stages of regular download process, the internal violator's advantages «a» and «b» allow it to ignore the stage of revealing of vulnerabilities ($\sum P(t) = 1, \forall t \geq 0$).

Regular download of TOE and, consequently, trusted download are for an internal violator a batch process with actually unlimited period of repeating of stages x_i. In fact it means the lack of time limits inside each stage to reveal vulnerabilities regardless of the value of the end time to execute any stage. Consequently, an internal violator is able to repeat the trusted download" process again and again until it reveal all possible vulnerabilities: $\lim_{T\to\infty} P(t) = 1$, where $T = \sum t,\ t \in x_i$. However in part $s(t)$ the internal violator has no advantages before an external one. This statement is true because the exploitation of any vulnerability is always an active method to influence on the components of the vulnerable system and, consequently, demands some time to execute [Max15, Cap12]. But in case of unsuccessful exploitation of the vulnerability the violator takes risk to be revealed by SIS. Consequently, the number of the repeated

execution of the regular stages is definitely ($T \neq \infty$) for a violator, and an increase of delay on the execution stage follows the growth $s(t)$.

Thus, subject to fixation and subsequent assessment - rationing – of regular run-time values for each stage, the success of the insider's attacks is to be determined by the totality of its operating capacity to exploit the revealed vulnerabilities without going beyond the boundaries of the normalized values of time to execute each stage x_i:

$$S_{TD} = \begin{cases} \sum f(s) \\ s(t) \to 1 \\ t \leq t_{norm} \end{cases} \qquad (8)$$

5 Results and Conclusions

According to the results of the conducted modeling it is fair to argue that the approach based on control over exclusively built-in defense mechanisms in the regular download process is not optimal. The problem of optimization of such an approach is due to lack of control over time characteristic which determine the connection between efficient work of the defense mechanisms and possibility to be revealed and violator's ability to exploit vulnerabilities both in mechanisms themselves and in the regular download structure and in the components of AS. Thus, an attempt to implement a closed technological process by introducing defense mechanisms is doomed on the constant (monotonous) growth of a number of defense mechanisms aimed at maximum coverage of space of the violator's possibilities.

To optimize (modernize) trusted download system "hardware thin client" it is necessary to develop and implement the method which allows:

- fix normalized values of runtime of each stage of regular download process of "thin client" ($x_{norm}(t)$);
- control over the runtime of each stage of regular download process of "thin client" ($x(t),\ t_0 > 0$);
- fix any deviations in the runtime at each stage of regular download process;
- take consistent decisions based on collected data about each case on time deviations;
- pause regular download process if violator's attack is suspected ($f_i'(P, s) \neq 0$);
- refuse from qualitative assessment of defense mechanisms efficiency directly on stages of the regular download process;
- refuse to use defense mechanisms inside the space available for the violator.

The developed method and/or its technical implementation are to take into account the system's condition with $0 \leq t < t_0$, i.e. to control the violator's activity up to the moment the workstation is on.

It is mediated by the violator's possibility to attack before the actual implementation of regular download process ($S_{TD}(t) = \max(M), t < t_0$) – e.g. to connect a third-party workstation with the switching equipment of AS.

References

[Ave06] Avetisov R. S. Mathematical model study of the damage from exposure to the confidential information of internal threats / A. P. Rosenko, R. S. Avetisov // Vestnik of SSU. - 2006. - P. 23-29.

[Gol15] Goldfinches A. Y. Mathematical models and methods of designing formal systems of protection of information systems / A. Y. Goldfinches, K. A. Goldfinches - SPb .: ITMO University, 2015. - 93 p.

[Ste12] Stefarov A. P. Formation standard model violator of the rules restricting access in automated systems / A. P. Stefarov, V. Zhukov // Proceedings of the Southern Federal University. Technical science. - 2012. - Vol. №12, T. 137. - S. 45-54.

[But15] Butsik K. A. Model trusted network boot thin client to neutralize possible insider / E. N. Tishchenko, K. A. Butsik, V. V. Derevyashko // Proceedings of SFU. Engineering - 2015 - Issue 5 (166) - S. 37-47.

[But16] Butsik K. A. Using the "slots" in the system of the trusted network boot thin client / K. A. Butsik, V. V. Derevyashko // Safety of Information Technology - 2016 - Vol. 2016-1 - S. 88-91.

[Inf01] Information Report FSTEC Russia №240 / 24/405 "On Approval of the Requirements for Drugs trusted boot" [Electronic resource]. - Access: http://fstec.ru/component/attachments/download/663. - Title screen.

[Sch08] Schastny D. Y. Building systems of protection against unauthorized access to the terminal system / D. J. Schastny // Information Security - 2008. - Issue 2 - pp 48-49.

[Syc15] Sychev V. M. Formalizing insider information security model / V. M. Sychev // Bulletin of Moscow State Technical University. NE Bauman. Series "Instrument" - Issue number 2 (101) / 2015 - S. 92-106.

[Zas09] Zastrozhnov I. I. Model attacker conflict and protection of information systems / I. I. Zastrozhnov, D. I. Korobkin, A. A. Okrachkov, E. A. Rogozin // Bulletin of Voronezh State Technical University - 2009 - Vol. №6, T. 5 - pp 142-149.

[Gor15] Gorbachev I. E. Modelling of processes of violation of information security of critical infrastructure / I. E. Gorbachev, A. P. Glukhov // SPIIRAN Proceedings - 2015 - Vyp.38 - S. 112-135.

[Skl04] Sklyarov D. V. Protection art and hacking information / D. V. Sklyarov. - SPb .: BHV-Petersburg, 2004 - 288 p.

[Wal13] Wall D. S. ENEMIES WITHIN: Redefining the insider threat in organizational security policy / D. S. Wall // Centre for Criminal Justice Studies. - Security Journal, 2013. - Vol. 26 (2). - P. 107-124.

[Zag15] Zaginaylov Y. N. The theory of information security and information protection methodology / Y. N. Zaginaylov. - M .: DirectMEDIA, 2015. - 253 p.

[Max15] Maximov E. A. Formalization of the information security process in the implementation of insider attacks / E. A. Maksimov, E. A. Vitenburg // Izvestiya of the Tula State University. Technical science. - 2015. - Vol. №8, T. 2. - P. 231-238.

[Cap12] Capelli D. M. The CERT Guide to Insider Threats: How to Prevent, De-tect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud) / D. M. Capelli, A. P. Moore, R. F. Trzeciak. - Addison-Wesley, 2012. - P. 432.