Research on the Classified Protection Model of Information System Based on the Threat Intelligence Technologies

Yuan TAO$^{1,2}$, Ke FAN$^{1,2}$, Feng-ming GUO$^{1,2}$ and Mo-yan LI$^{1,2}$

$^1$The Third Research Institute of Ministry of Public Security, China
$^2$MPS Information Classified Security Protection Evaluation Center, China

**Keywords:** Threat intelligence, Classified protection model, Immune factors network algorithm.

**Abstract.** In order to effectively deal with the APT and 0 day attacks, a new classified protection model of information system is proposed based on the threat intelligence technologies and immune factors network algorithm. So that the useful security threat information can be actively accessed and extracted from a large number of security information. The consequences of the threat information and the effective measures can be timely analysis, and the threat intelligence of classified protection can be timely shared.

**Introduction**

According to the traditional security threats of network, the information system of the defense and detection mechanism is based on feature detection$^{[1]}$, while the existing APT attacks and 0 day attacks cannot be informed in advance of feature information$^{[2,3]}$, and the role of prevention and detection mechanism of traditional cannot be useful$^{[4,5]}$. Through the APT attacks and 0 day attacks continue to grow, the respond of these new threats from the traditional defense are change into active defense, and it provides a new method of monitoring and administrating the networks.

Threat intelligence$^{[6-8]}$ is facing a new threat, and is the inevitable result of evolution method$^{[9,10]}$ based on threat as the center. This paper is the research of the data from threat intelligence of third party, further mining and enhanced the evaluation data of the classified protection. So that the consequences of the threat information and the effective measures can be timely analysis, and the threat intelligence of classified protection can be timely shared.

**The Classified Protection Model Based on Threat Intelligence**

At present, the mainstream of international threat intelligence standards are: CyboX (Cyber Observable eXpression), STIX (Structured Threat Information eXpression) and TAXII (Trusted Automated eXchange of Indicator Information). In this paper, the classified protection model based on threat intelligence is using TAXII to transfer data, using STIX as the information description, and using CyboX as vocabulary. So that the network equipment, security equipment, operating system, database, middleware, honeypot and other equipment are defined as the neuronal factors. The security policy configuration from safety equipment, network equipment, operating system and database are defined as the self-set of immune system.

So the classified protection model based on threat intelligence is defined as ICF model.

$$ICF = \{\Omega, H, D, N, C, K, M, \delta, \Delta, \Pi, \Pi, B, \pi, t, \lambda\}$$

$$IC_i = \{f_i | f_i \in ICF\}$$

$$G = \{g_i | g_i = IC_i\}, \quad |G| \geq 2$$

$$IC_i$$ is one of the factors that constitute classified protection model based on threat intelligence, which is the ICF model, while the $Q = \{q_{ij} | q_{ij} \text{ is the weight of } g_i \text{ to } g_j\}$, $\{g_i, g_j\} \rightarrow q_{ij} \in Q$. 


The security level of the information system is defined as $\Omega$, $\Omega = \{S, A, G\}$, the data security protection level of information systems is defined as $S$, the information system security service security level is defined as $A$, the general safety protection requirements of information systems is defined as $G$.

The operating system security policy of classified protection is defined as $h$, and all the operating system security policy of the information system is defined as the set of $H = \{h_1, h_2, ..., h_n\}$. The information system has database system $w$, so $d_w$ is the security strategy of database system of classified protection, and all database security policy is defined as the set of $D = \{d_1, d_2, ..., d_n\}$. The network equipment (including routers and switches) security strategy of classified protection is defined as $s$, and all network equipment security policy is defined as the set of $N = \{n_1, ..., n_s\}$. Security devices’ (including firewalls, intrusion detection, etc.) security policy of classified protection is defined as $c$, and all safety equipment is defined as the set of $C = \{c_1, ..., c_f\}$.

Security policy for application subsystem of classified protection is defined as $o$, and the security policy for all application subsystems is defined as the set of $O = \{o_1, ..., o_k\}$. Information system security management measures of classified protection is defined as $y$, and all management measures are defined as the set of $Y = \{y_1, ..., y_m\}$. The log information of information system is defined as $\delta(v_j)$ at the $t$ moment. Alarm information is defined as $\Delta(t)$. Threat intelligence of third party from the Internet is defined as $\Pi$. The reliability of the third party threat intelligence is defined as $B$; the timeliness of the third party Threat Intelligence is $\tau$, and time window is $\lambda$.

**The Constraint Condition of the Classified Protection Model**

Zombies, Trojans, worms, viruses, APT and 0 day and other attacks are defined as $v_j$. The damage caused by the attack on the information system is defined as $\chi(v_j)$. The total loss of the information system is defined as $\Lambda(t | \eta(t))$ at t time. All defensive measures are defined as $R$. The response to defense $v_j$ measure is defined as $r_j \in R$.

The measure of the minimize the loss is defined as $\Gamma$. At the t time, the cost of measures $r_j$ is defined as $\alpha$. The total cost of responding at the t time is defined as $\Xi$. The maximum allowable cost of the defense is defined as $\Psi$.

The initial set is defined as $\Phi = \{x | x \ is \ defense \ rules \ of \ network\} \in R$, so that $\chi : \Phi \times T \times R \times W \to \Lambda$, $(x, \chi, w) \to \chi \in \Lambda$.

At the time $t$, the cost of the measure $r_j$, which is to deal with $\alpha$, is defined as $\alpha = \alpha(r_j, t | (H, D, N, C, K, M))$. The total cost of responding to antibody measures is defined as $\Psi$, which is $\Psi = \Psi(\{r_j, t | \alpha(t, \{v_j\})\})$.

So the total loss estimation at t time is defined as $\Lambda(t | \eta(t)) = \sum_{\forall v_j = \eta(t)} \chi(v_j, t)$. 

In each emergency response decision, the choice of defense measures \( \{ r_j \} \) is the criteria of
\[
\arg\min_{\{ r_j \}} \{ c(\Lambda, \Xi) \}.
\]

**Threat Intelligence Analysis Factor Chain of Classified Protection**

The result of network defense is not only related to the system's service setting, system vulnerability and asset value, but also related to the network environment of the defense target and the attack type. At the same time, the effect of defense will change the defense target network system state, so in order to extract the corresponding threat intelligence from a large number of system information, this paper propose the threat intelligence analysis factor chain of classified protection \( I \).

Threat intelligence analysis factor chain of classified protection can provide operational threat intelligence of the information system, which is the defense target. Operational threat intelligence is the information that can be put into action for a particular attack. So \( I \) is defined as
\[
I = \{ \Omega, W, B, \Delta, \delta_j, r_j, t_j, \alpha_s, \chi_s, v_j \}.
\]
Threat intelligence analysis factor chain of classified protection is shown in Figure 1.

![Diagram](attachment:image.png)

Figure 1. Threat intelligence analysis factor chain of classified protection.

\( \Omega \) is the information system security protection level. \( \delta_j \) is the log of the defensive equipment. \( \Delta_j \) is the warning information. \( \alpha_s \) is the cost of defense. \( \chi_s \) is the loss of the defense process.

In the Figure 1, \( L = \{ V, P, E \} \) is the configuration weight of information system. \( V \) is the network vulnerability weights. \( P \) is the importance weight of information system, which is related to the element type, the network services, the data of the network. \( E \) is the weight of network security sensitivity, which is refers to the degree of sensitivity of network information integrity, confidentiality and availability.

The defense costs is definition as \( \alpha_s = \{ e, u \} \). The defense of resource occupancy is defined as \( e \), the risk of defense is defined as \( u \). The loss of defense is defined as \( \chi_s = \{ h, k, e \} \). The loss of
information influence is \( h \), the network attack effect is \( k \). The destruction of information effect is defined as \( \varepsilon \), which is the effect of hardware, software and data loss.

**Threat Intelligence Situational Awareness of Classified Protection**

Threat intelligence situational awareness of classified protection can provide strategic and tactical threat intelligence of the information system and the company. Tactical threat intelligence is used for APT detection and emergency response, the strategic threat intelligence is use for information security bulletins and early warning.

In order to analyses the various factors of the threat intelligence analysis factor chain of classified protection, the threat intelligence situational awareness is established to comprehensive overall performance of information system, which is defined as \( \mathbb{N} \), \( \mathbb{N} = \phi \circ I = (\xi_1, \xi_2, \ldots, \xi_n) \).

\[
\mathbb{N} = \bigcup_{q=1}^{3} \mathbb{N}_q
\]
\[
\mathbb{N}_q = \{I_{q1}, I_{q2}, \ldots, I_{qy}\}, \quad i = 1, 2, \ldots, r_y
\]

(2)

The defense measures set \( R \) is defined as the antibody of bone marrow cells. The defense measures \( r_j \) is defined as antibody defense cells. The maximum allowable cost \( \Psi \) is defined as mature detection cells. So Figure 2 is the chart of the threat intelligence situational awareness of classified protection.

![Figure 2. Chart of threat intelligence situational awareness of classified protection.](image)

In Figure 2, when the threat intelligence analysis factor chain is carried on situation awareness:

1. If mature detection cells will be immune tolerance, \( \xi \) is the product of small operator, so that \( \xi_j = \bigwedge_{i=1}^{n} (\phi_i \land I_{ij}) = \min_{1 \leq i \leq n} \{\phi_i I_{ij}\} \). At this time, tactical threat intelligence is obtained, so that APT and 0 day attack will be detected, and the expected goal of defense is achieved.

2. If marrow cells will be immune activation, \( \xi \) is the bound of sum operator, so that \( \xi_j = \bigoplus_{i=1}^{n} (\phi_i \oplus I_{ij}) = \sum_{i=1}^{n} \phi_i I_{ij} \bigg/ \sum_{i=1}^{n} \phi_i \). At this time, tactical threat intelligence is obtained, so that the appropriate defense measures can be selected, and emergency response can be carried out.
(3) If antibody defense cells will be immune tolerance, $\xi$ is the product of large operator, so that  
$$
\xi_j = \max_{i=1}^n (\phi_i \vee I_{ij}) = \max_{i \leq j \leq n} \{ \phi_i I_{ij} \} .
$$  
At this time, strategic threat intelligence is obtained, through the attack is beyond the constraints of defense, bulletins and early warning should be carried out.

**Summary**

Through the classified protection model of information system is proposed based on threat intelligence, the threat intelligence analysis factor chain and threat intelligence situational awareness of classified protection are built. So that the useful security threat information can active access and extract from a large number of security information. The consequences of the threat information and the effective measures can be timely analysis. And tactical and strategic threat intelligence of the information system can be obtain, and the APT and 0 day attacks can be detected, the appropriate defense measures can be selected to emergency response, bulletins and early warning can be carried out, and the threat intelligence of classified protection can be timely shared.

**Acknowledgement**

This research was financially supported by the National Development and Reform Commission Information security special item “National Engineering Laboratory for Key Technology of Classified Information Security Protection”.

**References**


[8] Information on http://cyboxproject.github.io
