ENSREdm: E-government Network Security Risk Evaluation Method Based on Danger Model

Xiaoting Jin
College of Public Administration, Henan University of Economics and Law, Zhengzhou 450002, China

Abstract: In this study, we propose a danger model based security risk evaluation method to ensure the security of E-government networks. With the concepts and formal definitions of antigen, antibody, danger signal and detection lymphocyte presented, the architecture is given. Following that, the method of E-government network intrusion detection is described. And then, the security risk evaluation method is discussed. Theoretical analysis and experimental results show that the proposed method is valid. Thus, it provides a novel security guarantee solution to E-government networks.

Keywords: Danger model, e-government, risk evaluation

INTRODUCTION

Today, biological principle based methods have become an increasing popular computational intelligence paradigm in the field of information security (Sun, 2010). The problems of computer system are quite similar to those encountered in a Biological Immune System (BIS), since both of them have to maintain stability in a changing environment (Klarreich, 2002; Castro et al., 2003). Inspired by the numerous desirable characteristics of the natural immune system, such as diversity, self tolerance, immune memory, distributed computation, self-organization, self-learning, self-adaptation and robustness, the BIS based Artificial Immune Systems (AIS) have become an increasing popular computational intelligence paradigm within information security (Sun et al., 2008; Li, 2008; Sun and Zhang, 2009; Sun and Xu, 2009; Zhang et al., 2009).

The main task of traditional AIS based method for E-government network security based on antibody concentration (Sun and Wu, 2009) is to discriminate between self and non self and the central challenge of E-government network security is determining the difference between normal and harmful activities. However, it is difficult for AIS to distinguish accurately between self and non self and the size of self library and the time of self tolerance will grow exponentially with time goes by. Moreover, the phenomena of the natural immune system, such as the non self Intestinal Lactobacillus can live within human gastrointestinal, but there is no immune response to them, can’t be explained by the AIS of Self-Non Self (SNS) discrimination.

In this study, we propose a danger model based security risk evaluation method to ensure the security of E-government networks. With the concepts and formal definitions of antigen, antibody, danger signal and detection lymphocyte presented, the architecture is given. Following that, the method of E-government network intrusion detection is described. And then, the security risk evaluation method is discussed. Theoretical analysis and experimental results show that the proposed method is valid. Thus, it provides a novel security guarantee solution to E-government networks.

DANGER MODEL

The danger model is presented and developed by Matzinger (1994), (2001), (2002), Ackelin and Cayzer (2002) and Timmis et al. (2003). Matzinger states that adaptive immune systems can’t distinguish self from non-self but danger signal; immune response will be triggered when danger signals are generated by damaged cells; the cells of the adaptive immune system in danger model are incapable of attacking their host. On the one hand, the immune response of danger model is as a reaction to a stimulus which the body considers harmful, but not the reaction to non-self. On the other hand, the foreign and immune cells of danger model are allowed to exist together and this point is reverse to the traditional AISs. Figure 1 shows the main principles of the danger model.

Figure 1 illustrates that cells distressed or died unnaturally may release an alarm signal which disperses to cover a small area around that cell, Antigen Presenting Cells (APCs) receiving this signal will become stimulated and in turn stimulate cells of the adaptive immune system. Within danger model, the foreign proteins in the injection are not harmful and so
are ignored, likewise tumor cell is not undergoing necrotic cell death and therefore not releasing alarm signals, hence there is no immune reaction occurred. Because of the danger signals only activate APCs, the B and T cells are stimulated into action according to Signal 1 and Signal 2. Signal 1 is the binding of an immune cell to an antigenic pattern or an antigen fragment which is presented by an APC and Signal 2 is either a “help” signal given by a T-helper cell to activate a B-cell or a co-stimulation signal given by APC to activate T-cells.

With the danger model introduced, the danger theory inspired paradigms were proposed for data processing (Secker et al., 2005), worm response and detection (Kim et al., 2005), computer network intrusion detection (Zhang and Liang, 2008), network security threat awareness (Sun et al., 2010a), network security monitoring (Sun et al., 2010b) and so on.

THEORETICAL MODEL

Within ENSREdm, it considers that the computer network attacks, which are dangerous, will induce the generation of danger signals by simulating cellular distress or cell unnatural death and the comparison between danger model and ENSREdm is illustrated in Table 1 (Sun, 2011).

Formal definitions: The state space of ENSREdm is defined with set \( S \) and \( I \subseteq [0,1]^n \), where \( N \) represents the length of a E-government network packet. The antigen (ag) of ENSREdm is regarded as a presented Internet Protocol (IP) packet, which is consisted of the source IP address, destination IP address, source port number, destination port number, protocol type, IP flags, IP overall packet length and IP data. The antibody (ab) is used to recognize antigens. Obviously, the structure of ab is the same as that of ag. Non-self patterns (Nonself) represent IP packets from network attacks and self patterns (Self) are normal network service transactions and non-malicious background clusters, where Nonself \( \cap \) Self = \( \phi \).

Within E-government networks, all IP network packets are composed of the same segments. In point of this fact, the formal definitions of the sets of ag (\( S_{ag} \)) and ab (\( S_{ab} \)) of ENSREdm are respectively defined as follows:

\[
S_{ag} = \left[ \begin{array}{c}
ag_{11} & ag_{12} & \cdots & ag_{1n} \\
ag_{21} & ag_{22} & \cdots & ag_{2n} \\
\vdots & \vdots & \ddots & \vdots \\
ag_{m1} & ag_{m2} & \cdots & ag_{mn}
\end{array} \right]
\]

(1)

\[
S_{ab} = \left[ \begin{array}{c}
ab_{11} & ab_{12} & \cdots & ab_{1n} \\
ab_{21} & ab_{22} & \cdots & ab_{2n} \\
\vdots & \vdots & \ddots & \vdots \\
ab_{p1} & ab_{p2} & ab_{p3} & \cdots & ab_{pn}
\end{array} \right]
\]

(2)

In ENSREdm, each segment of ab and ag can be considered as a gene snippet. According to the principles of AIS, the antigen and antibody organization technique proposed in ENSREdm can fit E-government network well with reason. So, there exists \( S_{ag} \subseteq I \), \( S_{ab} \subseteq I \) and Nonself \( \cup \) Self = \( S_{ag} \).

In ENSREdm, the detection lymphocytes is used for network attacks detection and it is classified into immature, mature and memory detection lymphocyte. The mature detection lymphocyte is the detector that is tolerant to self but not activated by antigens. The memory detection lymphocyte evolves from a mature detection lymphocyte matched enough antigens in its lifecycle. While the immature ones are generated from the process of antigen depository or randomly generation. Let \( S_{imm}, S_{mat} \) and \( S_{mem} \) denote the set of immature detection lymphocytes, mature detection lymphocytes and memory detection lymphocytes, respectively. Therefore, \( S_{imm} \cup S_{mat} \cup S_{mem} = S_{ab} \) and \( S_{imm} \cap S_{mat} \cap S_{mem} = \phi \).

Architecture of ENSREdm: According to the prevalent deployment of AIS, the architecture of ENSREdm is designed by distribution and it is mainly composed of sensors and a risk assessment center. The sensor of ENSREdm can be located in each E-government sub-network and it is in charge of the detection of network attacks. The functions of the risk assessment center include two aspects: bacterin distribution and network security risk evaluation through calculating danger degree.
**Method of intrusion detection:** In ENSREdm, the sensor, which can be located in each host or subnet work, is in charge of the network intrusion detection and it is realized by detection lymphocytes. To describe the intrusion detection methods of the mature and memory detection lymphocytes, formal definitions are defined as below.

Let \( d \) denote detection lymphocyte, a represent the age of \( d \), \( n \) is the antigen number matched by \( d \), \( s \) is the danger degree of network attacks which is detected by \( d \) and the intrusion detector set \( (S_{ab}) \) is defined as follows:

\[
S_{ab} = \{ (d, a, n, s) \mid d \in S, a \in N, n \in N, s \in [0, 1] \} \tag{3}
\]

where, \( N \) represents the set of natural number.

For the convenience using the fields of a lymphocyte \( x \), the operator \( \cdot \) is used to extract a specified field of \( x \), where \( x \) field name represents the value of field fieldname of \( x \). According to the concepts of detection lymphocyte above, the formal definitions of the memory detection lymphocyte, mature detection lymphocyte and immature detection lymphocyte are described as follows:

\[
S_{\text{mem}} = \{ a \mid a \in S_{ab}, \forall b \in \text{Self}(a,n) \geq \beta \land \text{match}(a,b) = 1 \} \tag{4}
\]

\[
S_{\text{mat}} = \{ a \mid a \in S_{ab}, \forall b \in \text{Self}(1 \leq a,n < \beta) \land \text{match}(a,b) = 1 \} \tag{5}
\]

\[
S_{\text{imm}} = \{ a \mid a \in S_{ab}, a.n = 0 \land a.s = 0 \} \tag{6}
\]

where, \( \beta \) denotes the activation threshold and match \( (a, b) \) is a matching function, which can be r-contiguous bits matching function, Hamming distance matching function and etc. In ENSREdm, the matching function is defined as in formula (7):

\[
\text{match}(a,b) = \begin{cases} 1 & \text{otherwise} \\ 0 & \exists i, j (i - j \geq r \land (b_i = a.d_s, y \in S_{ab}, x \in S_{ab}, i \leq k \leq j)) \end{cases} \tag{7}
\]

In ENSREdm, the mature detection lymphocyte simulates a B cell and the memory detector lymphocyte is mapping to a T kill cell. Moreover, the computer network attacks within E-government are detected by memory and mature detection lymphocytes through calculating the affinity between the antibody and the antigen.

The mature detection lymphocytes, which match enough antigens \( (\beta) \) in their lifecycle, will evolve into memory detection lymphocytes and this procedure is illustrated in formula (4). Formula (5) illustrates the generation method of mature detection lymphocytes which generate from immature detection lymphocytes. Please note that the immature detection lymphocyte who matches to any element in Self during the process of negative selection will be eliminated and those immature detection lymphocytes that pass through the negative selection will evolve into mature lymphocytes. The immature detection lymphocytes are generated from antigen depository or randomly generation, so they are described in formula (6).

For \( \forall d_m \in \text{host}_i, D_{\text{mem}} \cup \text{host}_i, D_{\text{mat}}, \) if it detects a network attack (antigen) from time \( t \) to \( t + 1 \), \( d_m, a \rightarrow d_m, a \) and \( d_m, n + 1 \rightarrow d_m, n \). At the same time, the danger degree of \( d_m \) at time \( t + 1 \) is calculated by formula (8) and (9):

\[
d_m.s(t+1) = \eta \times d_m.s(t) + \eta_0 \tag{8}
\]

\[
d_m.s(t) = \frac{d_m.cn(t) - d_m.cn(t-1)}{\Gamma} \tag{9}
\]

where, \( \eta \) represents the encouragement factor which is used to monitor the continuous similar network attacks, \( \eta_0 \) denotes the initial danger degree and \( \Gamma \) represents the period from time \( t \) to \( t + 1 \).

Formula (8) and (9) shows that danger degree of the memory and mature detection lymphocyte will increase persistently with the enhancement of network attack intensity.

On the contrary, for \( \forall s_m \in \text{host}_i, S_{\text{mem}} \cup \text{host}_i, S_{\text{mat}}, \) if it doesn’t detect any non-self antigen during the period of \( \Gamma \) (from time \( t \) to \( t + 1 \)), \( s_m \) will increase 1 if and only if \( s_m \) finishing one time antigen detection and \( s_m \) at time \( t + 1 \) is calculated by formula (10):

\[
s_m.s(t + 1) = s_m.s(t) \times e^{-s_m.a(t + 1)} \tag{10}
\]

To simulate the danger signal of ENSREdm, it is defined that the danger signal of the \( i \)-th host at time \( t \) can be calculated by summation. Let \( V_{\text{host}_i.d_s} \) denote the danger signal of host, and the calculation method of \( V_{\text{host}_i.d_s} \) is defined by formula (11):

\[
V_{\text{host}_i.d_s}(t) = \sum_{j \in \text{host}_i} x_j.d_s(t) \tag{11}
\]

where, \( N \) denotes the total lymphocytes’ number of host, and \( x_j \in \text{host}_i, S_{\text{mem}} \cup \text{host}_i, S_{\text{mat}} \).

**Method of risk assessment:** Because of the distributed architecture of the proposed model, the E-government network security risk assessment includes two parts. One is the host risk calculation which is realized by sensor and the other is completed by the risk assessment center. The detailed computation and assessment methods are described as follows.

There is a sensor in each network host, so the host risk can be calculated by the field of danger degree. In order to exponentially describe the security risk for host, let host, risk \( (t) \) denote the security risk of host, \( ds \) at time \( t \), \( \mu_j \) represent the damage weight, which
denotes the danger degree of the \( j \)th detection lymphocyte. The host \( i \), risk \((t) \) is calculated by formula (12):

\[
hosti_{\text{risk}}(t) = 1 - \frac{1}{1 + L(n) \mu_j \times s_{\text{mem}}(t)}
\]

where, \( n = |\text{host}_i \text{.mem}| \cup |\text{host}_i \text{.mat}| \) and \( \forall S_\text{mem} \in \text{host}_i \text{.mem} \cup \text{host}_i \text{.mat} \).

In formula (12), host \( i \), risk \((t) \) \( \rightarrow 0 \) represents that host \( i \) has no danger at time \( t \) and host \( i \), risk \((t) \) \( \rightarrow 1 \) denotes the host host \( i \) is in extremely danger.

From the above, the algorithm for E-government Network Security Risk Evaluation (ENSRE) for host \( i \) at time \( t \) is described as follows:

**Algorithm 1: ENSRE**

*Begin*

Loop: capture a network packet;

Present \( ag \);

For each \( d_m (d_m \in \text{host}_i \text{.mem} \cup \text{host}_i \text{.mat}) \)

If (match \((d_m, ag) = 1\))

\{ Compute \( V_{\text{hosti.ds}}(t) \geq \theta \);
If \( V_{\text{hosti.ds}}(t) \geq \theta \) then

\{ Give an alarm;
Goto Loop;
\}

Else
Goto Loop;

*End.*

In ENSREdm, the whole network risk at time \( t \) is realized by the assessment center through averaging the risk of all the network hosts.

**Theoretical analysis:** In the abstract, ENSREdm is feasible and the theoretical analysis is given as follows.

Firstly, according to the formal definitions of \( S_\text{ab} \), \( S_\text{mem} \) and \( S_\text{mat} \), the artificial immune detection lymphocyte simulates the detection rule of the traditional network intrusion detection systems. So, network attacks can be detected in real-time; the more the lymphocyte, the more accurate the result.

Secondly, from the distributed framework of the proposed model and host-based deployment of sensors, it can be concluded that each host of the tested network can detect what “disease” it suffers (by checking the type of the artificial immune detection lymphocyte). Furthermore, by the risk assessment center of ENSREdm, network managers can know where the “disease” occurs (by checking the IP address of the host) and what the current “epidemics” are (by checking the maximal \( n \) of the detectors).

Finally, formula (8), (9), (10) and (11) illustrate that the danger signal of hosts is calculated quantitatively and the computation method is exponential. Equation (12) shows that when network attacks occur and the attack intensity increases, the danger signal also increases and follows the trend of the real attack intensity; as the real attack intensity decreases, the perceived attack intensity decreases as well.

In a word, ENSREdm is feasible; not only can it find out where the most serious disastrous area is, but also it can perceive the current situation of the local hosts and the whole network in quantification. Moreover, the higher attack frequency and intensity, the higher the danger signal and the situation awareness result of the network security is sensitive whether the “disease” is serious or not.

**SIMULATION AND EXPERIMENTAL RESULTS**

In order to verify the validity of ENSREdm, simulations were carried out and the topology structure is illustrated in Fig. 2.

In the experiments, the antigen is extracted from network packets, including destination IP, source IP, port number and protocol type. Therefore, the length of antigen is fixed. The match function used in ENSREdm was \( r \)-contiguous-bits matching rule and we defined \( r = 8 \). As limited by the size of our computer memory, computation speed and etc., the number of lymphocytes in ENSREdm was restrained, the proportional under 600 (theoretically, the more the lymphocytes, the more accurate the result).

Within the simulations, the values of activation threshold \( \beta \) were used as in the method of Forrest et al. (1997), where \( \mu_j = \mu_k = 1 \) \((j \neq k)\), \( \eta = 1 \), \( \eta_0 = 0 \). Within the experiments, the network intrusion of land, teardrop and smurf attacks were tested, there was one non-self packet among 20 packets and the network attacks were from 192.168.0.1 to 192.168.0.2 and 192.168.0.3. Partly experimental results are listed as follows.

The land attack intensity (packets per second) of the simulations was listed in Table 2 and the
Table 2: Land attack intensity (packets per second)

<table>
<thead>
<tr>
<th>Time (second)</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>111</td>
</tr>
<tr>
<td>2</td>
<td>121</td>
</tr>
<tr>
<td>3</td>
<td>134</td>
</tr>
<tr>
<td>4</td>
<td>148</td>
</tr>
<tr>
<td>5</td>
<td>162</td>
</tr>
<tr>
<td>6</td>
<td>171</td>
</tr>
<tr>
<td>7</td>
<td>181</td>
</tr>
<tr>
<td>8</td>
<td>191</td>
</tr>
<tr>
<td>9</td>
<td>201</td>
</tr>
<tr>
<td>10</td>
<td>211</td>
</tr>
<tr>
<td>11</td>
<td>221</td>
</tr>
<tr>
<td>12</td>
<td>231</td>
</tr>
</tbody>
</table>

Table 3: Teardrop attack intensity (packets per second)

<table>
<thead>
<tr>
<th>Time (second)</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>121</td>
</tr>
<tr>
<td>2</td>
<td>132</td>
</tr>
<tr>
<td>3</td>
<td>143</td>
</tr>
<tr>
<td>4</td>
<td>154</td>
</tr>
<tr>
<td>5</td>
<td>165</td>
</tr>
<tr>
<td>6</td>
<td>176</td>
</tr>
<tr>
<td>7</td>
<td>187</td>
</tr>
<tr>
<td>8</td>
<td>198</td>
</tr>
<tr>
<td>9</td>
<td>209</td>
</tr>
<tr>
<td>10</td>
<td>210</td>
</tr>
<tr>
<td>11</td>
<td>221</td>
</tr>
<tr>
<td>12</td>
<td>232</td>
</tr>
</tbody>
</table>

Table 4: Attack intensity (packet per minute)

<table>
<thead>
<tr>
<th>Time (second)</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>111</td>
</tr>
<tr>
<td>2</td>
<td>122</td>
</tr>
<tr>
<td>3</td>
<td>133</td>
</tr>
<tr>
<td>4</td>
<td>144</td>
</tr>
<tr>
<td>5</td>
<td>155</td>
</tr>
<tr>
<td>6</td>
<td>166</td>
</tr>
<tr>
<td>7</td>
<td>177</td>
</tr>
<tr>
<td>8</td>
<td>188</td>
</tr>
<tr>
<td>9</td>
<td>199</td>
</tr>
<tr>
<td>10</td>
<td>209</td>
</tr>
<tr>
<td>11</td>
<td>210</td>
</tr>
<tr>
<td>12</td>
<td>221</td>
</tr>
</tbody>
</table>

Fig. 3: Risk of land attack

Fig. 4: Risk of teardrop attack

Fig. 5: Risk of smurf attack

The teardrop attack intensity of the simulations was listed in Table 3 and the experiment results apperceived by the proposed method were illustrated in Fig. 4.

The smurf attack intensity (packets per second) of the simulations was listed in Table 4 and the experiment results apperceived by ENSREdm were illustrated in Fig. 5.

Theoretical analysis and the experimental results show that ENSREdm can aware security threats, which are caused by the network attacks, for E-government networks. Therefore, the proposed model is valid.
CONCLUSION AND RECOMMENDATIONS

This study proposes a danger model based method for E-government network security risk evaluation, which develops the concept of danger degree for network security risk evaluation, improves the formal definitions of the traditional immune detectors, describes the model architecture and gives the principles of network intrusion detection and security risk assessment. Theoretical analysis and experimental results show that the proposed method is valid, it can evaluate the security risk for E-government networks, which is caused by network attacks. The higher attack frequency and intensity, the more dangerous the network faces. ENSREdm can detect wha"disease" that E-government networks suffering, whether the "disease" is serious or not.

However, the current research of ENSREdm is mainly focus on network attacks frequency and intensity. In future work, the theory of ENSREdm should be perfected. Moreover, the activation threshold value (\(\beta\)), the matching function, encouragement factor value (\(\eta\)), the initial danger signal (\(\eta_0\)) and the damage weight (\(\mu_i\)) should be tested in detailed.

ACKNOWLEDGMENT

This study was supported in part by a grant from Key Technologies R & D Program of Henan Province (No. 102102210509).

REFERENCES