Journal of the Nigerian Association of Mathematical Physics
Volume **18 (May, 2011), pp 401 – 406**

Evaluating the Security Risks of System Using Hidden Markov Models

[1]Onibere Emmanuel A. and [2]Egwali Annie. O.

[1, 2]Department of Computer Science
Faculty of Physical Sciences
University of Benin P.M.B 1154,
Benin City, Nigeria.

Abstract

System security assessment tools are either restricted to manual risk evaluation methodologies that are not appropriate for real-time application or used to determine the impact of certain events on the security status of networked systems. In this paper, we determine the strength of computer systems from the perspective of the authentication models employed at the user interface domain by introducing a novel approach to system risk assessment. We first establish the risk of a system as the composition of the risks of individual authentication factors employed for user authentication processes, providing a more formally defined model. Using Hidden Markov Models (HMMs) we characterize the likelihood of transitions between security states of systems with different levels of authentication factors and we provide soft evidence on the states of these systems by applying our security assessment tool to an existing multifactor authentication model. The results of the analysis and the empirical study provide insights into the authentication model design problem and establish a foundation for future research in system authentication application.

1. Introduction:

The complexity of today's system architecture makes the process of establishing the choice of authentication factors and system security management from an authenticating perspective increasingly difficult. The amount of attacks targeted at systems, especially in a connected environment can be overwhelming, and prioritization and selection of appropriate level of authentication factors that will respond effectively and swiftly to attacks is generally difficult. Also security assessment tools are either restricted to manual risk evaluation methodologies that are not appropriate for real-time application, or are mainly used to determine the impact of certain events on the security status of networked systems. Page [1] proposed system change detection HMMs procedure, in which system alteration due to intrusion is detected using the distribution of observations before and after an unknown time. Baum, et. al., [2] proposed a real-time risk assessment method that is limited to risk assessment for individual computing systems. Phillip et al [3] present a knowledge base model that takes into account the impact of alerts on the overall security task that a network infrastructure supports and the model describes the security-relevant characteristics of the protected network in order to prioritize the alerts. In [4] a knowledge-based system that ascertains the security level when a risk alert reaction is received from a networked system was developed. Coras [5] developed a methodology for evaluating networked system risk processes. Kruegel and Robertson [6] proposed a security alert verification model that operate either offline or online. In an offline mode, the systems perform periodic vulnerability scans of the protected network and store the result in a database. Shelby et al [7] proposed a risk-based systems security engineering framework aimed at stopping attacks with intention. Ashish and Gershon [8] proposed a real-time risk assessment method for individual systems. Arnes et al [9] use HMMs as a method for estimating the risk of a network of systems.

1.0 HMMs Terminology and Model Scenario

HMMs are utilized because they are a principal method for modeling stochastic processes and for estimating the risk of a system [9], which are ideal ways to make inferences about how system attacks evolve. HMMs are also used to evaluate the probability of a sequence of events, to establish the most likely state transition path, and parameters for the exceptional representation of likely path. It is a structure or inference based on the forward or forward-backward algorithm that can model the

[2]Corresponding authors: Egwali Annie. O A: E-mail: egwali@yahoo.com; Tel. 07033247730

evolution of a transaction space, and process new information every time a transaction occurs. Any presence of an HMM from among ambient data is easily detected including the probability of false positives and false negatives associated with the observations.

Our HMMs is used to facilitate the effective modeling of the *time evolution* of attack patterns and the *attacks penetration* levels for systems with varied levels of authentication factors. This is a novel approach because current authentication applications are usually implemented with little insight into how the selection of credentials may impact the

resulting level of assurance statistically and the system risk level. We assume that each system *Sys* can be modeled by N different states *Q*, which is defined as $Q = \{s_1, \ldots, s_N\}$. We also assume that the volumes of attackers surveying and attempting to compromise each *Sys* is eminent. Thus at different instances the security state of *Sys* will vary, which depicts a transition from one state at time t to a different state. Besides, the security state of *Sys* changes with time *t*, thus the sequence of states *Sys* which can be at time *t* is denoted as $Z = z_1, \ldots, z_T$, where $z_t \in Q$.

Generally, HMM is parameterized by:

$$\lambda = (S, O, \pi), \tag{1}$$

Each *Sys* consists of:

- *S* a state transition probability matrix which describes the probabilities of transitions between *N* finite number of states of the model, denoted as:

$$S = a_{ij} = P(u_{t+1} = \mathrm{q}_i \mid x_t = \mathrm{q}_j), \ (i, j = 1, \cdots, N) \tag{2}$$

- *O* the observation probability matrix which describes the probabilities of receiving different observations for *M* finite alphabet of observations given that the system is in a certain state, is denoted as:

$$O = b_{ij} = P(u_t = \mathrm{q}_i \mid x_t = \mathrm{q}_i), \ i = 1, \cdots, N; j = 1, \cdots, M \tag{3}$$

- π the initial probability distribution of the Markov states, is symbolized by:

$$\pi = \pi_i = P(u_1 = \mathrm{q}_i), i = 1, \cdots, N \tag{4}$$

To compute the likelihood function of an HMM within a given time frame, the defining property of the joint probability is represented as:

$$\mathrm{P}(\mathrm{x}_1, \ldots, \mathrm{x}_n, \quad \mathrm{u}_1, \ldots, \mathrm{u}_n) = \pi_{x_1}\left[\prod_{t=1}^{n-1} a_{s_t s_{t+1}}\right]\left[\prod_{i=1}^{n} b_{s_t u_t}\right] \tag{5}$$

To evaluate the likelihood of a sequence of observation, the following recursion holds:

$$\propto_{t+1}(j) = \left[\sum_{i=1}^{N} \propto_t (i) a_{ij}\right] b_{j u_{t+1}} \tag{6}$$

with initial condition expressed as:

$$\propto_{t+1}(j) = \pi(j)(j) b_{j u_1} \tag{7}$$

and a forward variable defined as:

$$\alpha_t(i) = P(\mathrm{u}_1, u_2, \cdots, u_t, x_t = i \mid \lambda).$$

The various *Sys* modeled are assumed to have two possible security states $L = \{S_e, V\}$, which are defined as:

- *Secured* (S_e): The system is in a secured state if the authentication factors in place are not compromised thus preventing an attacker from logging in through the user interface.
- *Vulnerability (V):* The system is in a vulnerable state if an attacker has already compromised one of the authentication factors in place and has a high chance of compromising the system.

Figure 1 shows the graph representing the Markov model for the security states of the systems. The edge from one node to another represents the fact that when a system is in the state indicated by the source node it can transition to the state indicated by the destination node. The full connectivity of the graph indicates that it is possible to transit from one state to another.

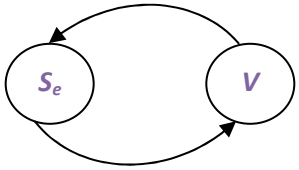


Figure 1: Markov Model for Systems Security States

Our proposed systems comprise three varied levels of authentication factors:

- Sys_1: This system consists of a single-factor authentication model. In this case we represent the factor with M (see figure 2). The state of Sys_1 is defined as:

$$Sys_1 (L) = \{M, 0\} \quad (8)$$

Where at the security level S_e, Sys_1 is represented as *M* and at security level *V*, Sys_1 is represented as *0*.

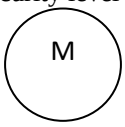


Figure 2: Markov model for the single-factor authentication security state

- Sys_2: This system consists of two factors authentication model. In this case we represent the factors with *M* and *F* (see figure 3). The state of Sys_2 is defined as:

$$Sys_2 (L) = \{MF, F0\} \quad (9)$$

Where at the security level S_e, Sys_2 is represented as *MF* and at security level *V*, Sys_2 is represented as *F0*.

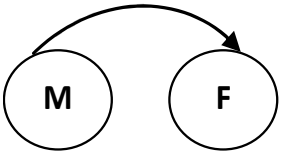


Figure 3: Markov model for the two factors authentication security states

- Sys_3: This is a system comprising of three-factor authentication model. In this case we represent the factors with *G*, *M* and *F* (see figure 4). The state of Sys_3 is defined as:

$$Sys_3 (L) = \{FMG, FM0, F00\} \quad (10)$$

Where at the security level S_e, Sys_3 is represented as *FMG*, while at security level *V*, Sys_3 is represented as *FM0* and *F00*.

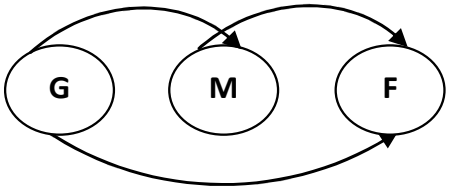


Figure 4: Markov model for the three factors authentication security states

2.0 Experiments

S, O and π represents the probability of transiting from the current secure state to another state that is less secured, the probability of observing authentication attack operation given the current state, and the initial system risk respectively. In our attack instance, we can assume that there are high volumes of probing and a fair amount of attack attempts. The security level for each *Sys* is relative and varying, and a system compromise is a likely scenario for some *Sys*. Therefore, the transitions (represented by the matrix *S*) to state S_e, and *V* are relatively likely. Hence, we have to assume that there is a high number of false positives and negatives. This is modeled by increasing the probabilities of receiving an observation that indicates a false positive or a false negative and decreasing the probability of receiving an accurate observation in the matrix *O*. The fact that the graphs are not fully connected denotes the fact that for any *Sys* with more than one authentication factor employed, after compromising an initial factor, it is not possible to return back to it.

To evaluate the system's attack modalities, the probability of each *Sys* state is associated with its corresponding values. The following sets of rules were used to determine the values of the HMM parameters used in the simulation model. Generally, if a *Sys* is not subject to attack, depicting the fact that none of its authentication factors have been compromised or that an attack did not succeed, then the *Sys* attack value should be very close to 0, and the probability of the system being in state S_e should be close to 1. Due to the fact that the systems are expected to have a higher level of security, the probability of transition to state *V* from S_e should be enormously low. The following is an example of the transition probability matrices employed, while $S(Sys_1)$ is a single variable factor:

S_3 = {FMG, FOO, FMO} where FMG is A_1, FOO is A_2 and FMO is A_3 and S_2 = {FM, FO} where FM is A_1 and FO is A_2.

$$S(Sys_3) = \begin{pmatrix} W_{A_1A_1} & W_{A_1A_2} & W_{A_1A_3} \\ W_{A_2A_1} & W_{A_2A_2} & W_{A_2A_3} \\ W_{A_3A_1} & W_{A_3A_2} & W_{A_3A_3} \end{pmatrix} = \begin{pmatrix} 0.995 & 0.002 & 0.003 \\ 0.02 & 0.959 & 0.021 \\ 0.02 & 0.022 & 0.958 \end{pmatrix}$$

$$S(Sys_2) = \begin{pmatrix} W_{A_1A_1} & W_{A_1A_2} \\ W_{A_2A_1} & W_{A_2A_2} \end{pmatrix} = \begin{pmatrix} 0.999 & 0.001 \\ 0.001 & 0.999 \end{pmatrix}$$

In determining values for matrix *S*, we will have to amplify the probabilities of receiving a false positive or a false negative and reduce the probability of receiving an accurate observation, this is because in a organizational setting, there will certainly be a high level of attack attempts and it is possible for some systems to be compromised, thus there will be a high rate of false positives and false negatives. Taking the aforementioned status of *S* into consideration, we delineate the various *Sys* and their corresponding parameter values into the following Markov algorithm.

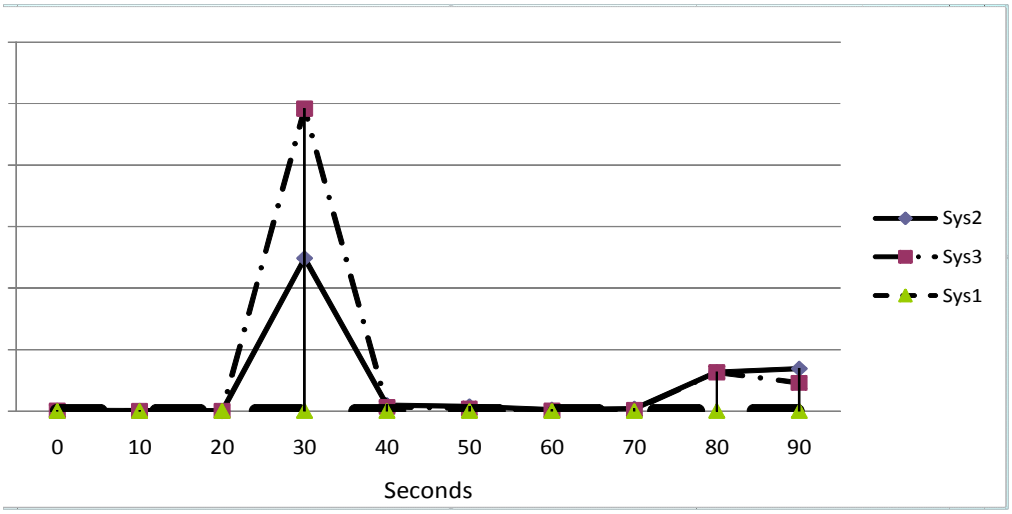
```
π; i;
while (π ^(i-1)~= π ^i)
   π ^i

   i=i+1;

end
        S = π ^i;
        O = π ^(i-1);
for n=1:i
   Z= π ^n;
```

```
D(n)=Z(1,1);

end

        n=1:i;

        plot(n,D)

        S; O; i
```

Where *S*, *O*, and π holds as previously defined, Z denotes the instance of a systems risk to attack, *n* denotes the individual systems risk iterations, *D* denotes the final observed plotting attack flow and *i* the total number of systems risk executed before convergence. $S(Sys_1)$ remains a single variable factor and the value of the initial state for all three systems is presumed to be:

$$\pi(Sys_3) = \{1, 0, 0\}, \pi(Sys_2) = \{1, 0\}, \pi(Sys_1) = \{1\}. \qquad (11)$$

The attack time frame and penetration levels of the varied levels of authentication factors embedded in each system was determined by the HMM parameters $\lambda = (S, O, \pi)$, which was verified based on the aforementioned factors and from experimental experience. We used design–level knowledge about each system to plan and execute attacks. Although attackers can likely use different attack strategies to access a system, our complete data set contains automated attacks on the three systems implemented in nine phases. Each of the codified HMMs represents an attack zone, which might alter the attacker's strategies. A system is stronger if the time for an attacker's success is significantly delayed in comparison to the response time of the other systems.



Number of attack attempts for Sys_1, Sys_2, and Sys_3

3.0 Findings and Discussions

Figure 5 shows the number of attack attempt for Sys_1, Sys_2, and Sys_3 and the compromising time respectively. Sys_1 could counter an attack only to the minimum level (about level 1) within the stipulated time frame of 90 seconds. Sys_2 delayed the attack penetration level and could increase it to about 2486 attack attempts before the system could be compromised. Sys_3 produced maximum delay penetration level and could delay the cracking level to about 4919 attempts. It is evident that the attack penetration level for the different systems differs depending on the number of authentication factors employed in the systems. A three factors authentication process will counter an attack more quickly or cause a more prolonged delay than one factor or two factors authentication model.

4.0 Conclusion

The findings of this preliminary research indicate that HMMs could be an efficient and powerful tool for comparative analysis of security risk of systems and solutions. By deliberately restricting the variety of possible states and selecting the number of authentication factors as strategies rather than exhaustive lists, the model allows reasonable comparisons for decision-making purposes. The selection of time as the unit of measurement is paramount to the model's strength. Time intervals are useful for intelligently comparing and selecting from a broad range of mitigating actions. The advantage of initiating the utilization of HMMs to establishing the level of assurance of authentication models and the strength of different levels of authentication factor models against identity attacks is that existing and proprietary authentication models can easily be integrated into a multifactor model in computing systems so that some level of increase strength is provided by these existing systems. The needed information to ascertain system security risk in this case, does not expose any of the internal operations of the systems. An authentication system can be considered robust if it can effectively counter more attackers' attempts to compromise it. The security risk evaluation tool can also identify how hard or weak a system is as seen by the attacker compared with peer systems in the same establishment. Attack modeling is therefore a necessary first step to clarifying a system's robustness: against what attack, on what scale, and with what system knowledge [10]. Our effort aimed at increasing the resources available to security analysts and policy makers will have enhanced information when developing counterattack measures.

References

[1]. Page, E. "Continuous Inspection Schemes", Biometrika, Vol 41. (1954) p100-115.

[2]. Baum, L., Petrie, T., Soules, G. and Weiss, N. "A Maximization technique occurring in the statistical analysis of probabilistic functions of Markov chains," Ann. Of Math. Stat., vol. 41. (1970) p 164-171.

[3]. Phillip A. Porras, Martin W. Fong, and Alfonso Valdes. A mission-impact-based approach to infosec alarm correlation. In Proceedings of the International Symposium on the Recent Advances in Intrusion Detection (RAID 2002). 2002). p 95–114.

[4]. Porras P. A., Fong M. W., and Valdes A. A mission-impact-based approach to infosec alarm correlation. In Proceedings of the International Symposium on the Recent Advances in Intrusion Detection (RAID 2002) Zurich, Switzerland. (2002). p 95–114.

[5]. CORAS IST-2000-25031. (2003). Available at: http://www.nr.no/coras.

[6]. Kruegel C. and Robertson W. (2004). Alert verification: Determining the success of intrusion attempts. In Proceedings of the 1st Workshop on the Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA 2004).

[7]. Shelby E., Heinbuch D., Kyule, E., Piorkowski, J. and Wallner J. Risk-based systems security engineering: Stopping attacks with intention. IEEE Security and Privacy, 02 (6). (2004). p 59 – 62.

[8]. Ashish G. and Gershon K. Rheostat: Real-time risk management. In Recent Advances in Intrusion Detection: Proceedings of the 7th International Symposium, (RAID 2004), Sophia Antipolis, France, September 15-17. (2004). p 296 – 314.

[9]. Arnes, A., Sallhammar K., Kjetil H., Tonnes B., Gaup, M., Marie E., and Knapskog S. Real-time risk assessment with network sensors and intrusion detection systems. In International Conference on Computational Intelligence and Security. (2005).

[10]. Burke, R., Mobasher, B., Zabicki, R and Bhaumik, R. Identifying attack models for secure recommendation. In Beyound Personification. A workshop on the Next generation of Recommender Systems. (2005).