Томского политехнического университета. – 2012. – Т. 321. – №. 5. – С. 113–116.9

OPTIMAL INFORMATION SECURITY INVESTMENT IN MODERN SOCIAL NETWORKING

KinashN., BerestnevaO., TikhomirovA., TrufanovA., RossodivitaA.
Irkutsk National Research Technical University
troufan@istu.edu

Introduction

In the current study, the modern social network compositions (SNC) include social networks (S – networks) per se, systems of information sharing (communication components, C- networks), and tool platforms providing the processes of sharing (P-networks). Generally each component of these socio-cyber systems has non-trivial characteristics to be in focus of many explorers. Following the concept of combined stem network [1], we suppose that actors from each of P-, C - and S – ensembles, integrated in triples - "bouquets". Just for this study there is no necessity to consider more than one layer case for the P, C and S networks. Thus such actors as a computer device, information resource, and individual comprise a bouquet of social network composition. Then, in graphG_q of q components ofsocial network composition

$$G_q = (V_q, E_q),$$

where V_q – a set of nodes (vertices), E_q– a set of links (edges), and a set of V_q - includes all participants of information sharing processes in the component

$$q = \{S, I, P\}.$$

Formal models [2,3] have considered economic aspects of information security and have revealed features and importance of optimal investment into information security. Topological measures to mitigate system risks have been stated in [4]. Nevertheless, researchers have been faced so far by a number of the intricate problems in information security of social networking compositions.

Model of social networking security

Probabilistic nature of the processes that bring damages allows to define risk, R - the main security measure - as:

$$R = P \times Damage,$$

where P - probability of the successful attack, *Damage* - damage caused by impact of an attack. As a classic attack on network structure is focused on removal of nodes which is result of coordinated threat, one has:

$$\mathcal{R} = \mathcal{P}_{tN} \times \mathcal{P}_{vN} \times (1 - \mathcal{P}_{cN}) \times \mathcal{L}_N$$

here $P_{t\,N}$, P_{vN} , 1- P_{cN} corresponding probabilities of threat, vulnerability and overcoming of counter-measures, L_N – cost of topological damage, caused by attack on node set $N_a \in V$.In the proposed model, similar to [4], the attacks are revealed through the detailed description of triplets – threats, vulnerabilities and counter-measures for separate nodes. Within the research network structural losses L, are estimated by calculations of a portion g of the nodes which have been disconnected with giant cluster after successful attacks which were carried out against targets – nodes:

$$\mathcal{L} = 1 - g$$

In case of emerging threats, with topological features close to real, the model gives means to investigate network system risks in more complex environment, if compare to traditional one. So, if follow [2], the probability of a successful attack will be connected with the investment in line with power and exponential expressions:

$$\mathcal{P}_{vi} = f^{I}(F_i) = 1/(\mu F_i + 1)$$

$$\mathcal{P}_{vi} = f^{II}(F_i) = v^{(\mu F_i + 1)}$$

where v – is initial vulnerability, $P_{vi0} = v$ for F_i =0, and μ - a coefficient which sets efficiency of financial means. In the study it was suggested that probability of a successful attack on node depends only on P_{vi} , which decreases exponentially with increasing of protection barrier "thickness" d. This thickness is connected with the value of expenses: $d_i \sim F_i$. In this case:

$$\mathcal{P}_{vi} = f^{III}(F_i) = \exp(-\mu \times F_i)$$

Security level of a separate element of a network is defined by the value:

$$SL_i = (1 - P_i) = 1 - \exp(-\mu \times F_i)$$

$$\mathcal{F} = \sum_n F_i$$

n- is power of a set V.

It seems reasonable to determine axiomatic parameter –security level of a network structure- by probability that any of elements won't be successfully attacked. If the probability to choose an attacked element i is 1/n then:

$$\mathcal{SL} = 1 - \sum_n \mathcal{P}_i = 1 - [\sum_n \exp(-\mu \times F_i)/n]$$

A specialized generator of network in the Python programming language has been created for analyzing the network structure exposed to risks.

Results

In this paper we study some networks of P-, C-and S- character in the field of coordinated the most dangerous threats for complex networks [5] to understand their information security investment sensitivity. For this research we have concentrated our choice on the following real networks (see Table. 1): m is number of links, <k> - average connectivity of nodes, γ – degree in a power distribution of node connectivity.For the modeling research two protective strategies are considered

Table 1. Social networks (S), Communication networks (C), and networks of computer platform (P)

Type	Code	Name	*n*	*m*	<*k*>	γ	Reference
P	CA	CAIDA	26,475	53,381	4.032	~2	[6]
P	AS	Route views	6,474	13,895	4.292	~2	[6]
C	HA	Haggle	274	28,244	206.1	1.5	[7]
S	FB	Facebook	63,731	817,035	25.64	~3	[8]
S	AP	Astro Physics	18,772	198,110	21.10	~3	[6]
S	JZ	Jazz musicians	198	2,742	27.70	5.3	[9]

Strategy 1. All the financing amount of counter-measures is uniformly distributed on nodes, i.e., in simple words, all nodes are protected equally:

$$F_i = F1_i = Const1 = 1/n$$

Strategy 2. In suggestion that the strategy of security governs distribution of financial resources between nodes, we have investigated reaction of the networks to threats for a case when investment into protection of nodes is proportional to their connectivities. The total volume of investment into protection is the same, as for Strategy 1:

$$F2_i(k_i) = Const2 \times k_i / \mu$$

$$\sum_{i=1}^{|V|} F1_i = \sum_{i=1}^{|V|} F2_i(k_i) = \mathcal{F}$$

It was supposed, as before, that the offensive party carries out the intentional successive choice of targets- nodes with maximum connectivity.P-components of social network compositions-computer networks CAIDA and Route views – both have properties of scale-free networks with power degree ~ 2, and low value of average connectivity ~ 4. We find that removal more than 1 % of nodes causes essential damage to these unprotected network structures. Dependences of loss L in real P- C-and S-networks countering to destruction of 10% nodes are presented in Figure 1a. Values of the necessary financial volumes of protection measures which are uniformly distributed among nodes (in $1/\mu$ units) to provide necessary network security level SL are manifested as well.

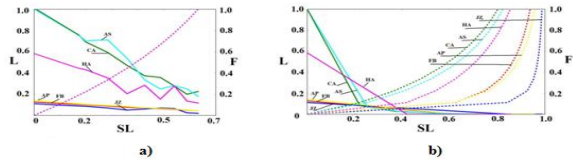

Figure 1. Loss of failures in network security (L, continuos line) and expenses on providing of protection counter - measures (F, dashed line) at different network security level (SL) according to Strategy 1 (a) and Strategy 2 (b) for the set of networks (Table 1)

Results of calculations confirm that intentional (coordinated) threats of SNC disintegration are especially dangerous concerning a computer component (CAIDA and Route views networks). Loss as functions of security level for social networks FB friendships, AP network and JZ has similar behavior. Communication network Haggle demonstrates its intermediate character. Estimations of topological loss and protection costs for the networks with 10% of nodes - targets due to distribution of protection investment proportional to node degree (Strategy 2) are given on Figure 1b. The results indicates that the strategy with protection of nodes in proportional dependence on connectivity (i.e. $F_i \sim k_i$)is more effective, than the strategy with uniform distribution of investment. And it is clear as counter-measures reduce probability of inactivation of the nodes representing the main targets for the classical strategy of coordinated threats.

Conclusion

We show that among social networking components computer networks manifest their greatest sensitivities to the most dangerous – coordinated threats of disintegration. Also it is found that network security level with optimal investment does not exceed 0.4 ~ 1/e for both strategies of net-work protection.

References

1. Barabási A-L, Albert R., Jeong H. Mean-field theory for scale-free random networks. // Physica A. – 1999. – no. 272. – P. 173–187.

2. Gordon L., Loeb M. The Economics of Information Security Investment. // ACM Transactions on Information and System Security. – 2002. – no. 4. – P. 438–457.

3. Huang D., Behara R., Goo J. Optimal Information Security Investment in a Healthcare Information Exchange: An Economic Analysis. // Decision Support Systems. – 2014. – no. 61. – P. 1–11.

4. Helbing D. Globally networked risks and how to respond. // Nature. – 2013. – no. 497. – P. 51–59.

5. Plum M.M., Gertman D.I. Novel threat-risk index using probabilistic risk assessment and human reliability analysis // Report No. INEEL/EXT-03-01117, Idaho National Engineering and Environmental Laboratory. – 2004. – P. 39.

6. Leskovec J., Kleinberg J., Faloutsos C. Graph Evolution: Densification and Shrinking Diameters //

ACM Trans. Knowledge Discovery from Data. – 2007. – no. 1. – P. 1–40.

7. Chaintreau A., Hui P., Crowcroft J. Impact of human mobility on opportunistic forwarding algorithms // IEEE Trans. on Mobile Computing. – 2007. – no. 6. – P. 606–620.

8. Viswanath B., Mislove A. On the evolution of user interaction in facebook // WOSN'09 Proc. Workshop on Online Social Networks. – 2009. – P. 6.

9. Gleiser P., Danon L. Community Structure in Jazz // Advances in Complex Systems. – 2003. – no. 4. – P. 565–573.