INFORMATION SECURITY

Information Assets Survivability Property Analysis

Yurii Garasym[1], Volodymyr Romaka[2], Mariana Rybiy[3], Taras Stetsiak [4]

[1]Information Security Department, LLC "IT Capital", UKRAINE, Kiev, Svobody avenue 4, E-mail: Iurii.Garasym@it-capital.com.ua

[2]Information Security Department, Lviv Polytechnic National University, UKRAINE, Lviv, S. Bandery street 12, E-mail: vromaka@polynet.lviv.ua

[3]Information Security Department, Lviv Polytechnic National University, UKRAINE, Lviv, S. Bandery street 12, E-mail: rybiy.mm@gmail.com

[4]Information Security Department, Lviv Polytechnic National University, UKRAINE, Lviv, S. Bandery street 12, E-mail: stecyaktb@gmail.com

Abstract – It's important to ensure the information assets survivability property for the effective and secure highly distributed networked systems operation. In order to do this the authors of the paper have improved the information assets survivability property analysis approach. As the result they received effective methodology of the survivability property analysis. It gives opportunity to more detail review and analyse survivability property attacks.

Key words – survivability property, information security, risk management, attack tree, information assets.

I. Introduction

The results of previous researches [1, 2], in particular:

- information security systems (ISS) continuity functioning methodology improvement,
- establishing dependences between ISS survivability parameter, recovery time and ISS risk level

allow us to analyse and describe the ISS survivability property ensuring process and show the ISS risk assessment importance as one of the steps to ensure ISS survivability property.

Today's large-scale, highly distributed networked systems improve the efficiency and effectiveness of organizations by permitting whole new levels of organizational integration. However, such integration is accompanied by elevated risks of intrusion and compromise. Incorporating survivability capabilities into an organization's systems can mitigate these risks [3].

A widely accepted definition of survivability given in literature defines survivability as the capability of a system to fulfill its mission in a timely manner, in the presence of attacks, failures or accidents [4].

The authors of the paper defined in [5] the ISS survivability property as a new concept that integrates IT security sector developments and risk management to protect distributed information flows and assets.

That's why information assets survivability property analysis should be done in relation to the organization mission. Survivability solutions are the best understood as a risk-management strategies that first depend on an intimate knowledge of the mission being protected [6].

At the current stage of the progress, companies have to ensure key properties of the information assets survivability, develop and implement business survivability strategies using the following means (Table I).

TABLE 1

THE KEY PROPERTIES OF THE INFORMATION ASSETS SURVIVABILITY AND SURVIVABILITY STRATEGIES

Key Properties	Ensuring of the Key Properties
Resistance - Ability to repel attacks	Strategies for repelling attacks (e.g. firewalls, user authentication, diversification)
Recognition - Ability to detect an attack or a probe - Ability to react or adapt during an attack	Strategies for detecting attacks and evaluating damage (e.g. intrusion detection systems, internal integrity checks)
Recovery - Provide essential services during attack - Store services following an attack	Strategies for limiting damage, restoring compromised information or functionality, maintaining or restoring essential services within mission time constraints, restoring full services (e.g. incident response, replication, system backup, contingency planning)
Redress - Ability to hold intruders accountable in a court of law - Ability to retaliate	Strategies of accountability and retaliating (e.g. computer forensics, legal remedies, active defense)

So, we present information security (IS) risk management methodology in relation to the survivability as the information assets survivability property analysis.

II. Information Assets Survivability Property Analysis

The information assets survivability property analysis detects whether the property above is ensured. For this process it is needed to determine which threats can damage survivability property and which type of the protection should be implemented. A widely accepted definition of this process is known as IS risk management.

Authors of the paper developed IS risk management methodology in relation to the survivability [1] in order to ensure the information assets survivability property. We implement this methodology as the part of the information assets survivability property analysis approach.

General algorithm of the analysis approach above is presented on the Fig. 1.

The authors present the IS risk analysis (Step 3 on the Fig. 1) by using Attack Tree Method. Attack tree models

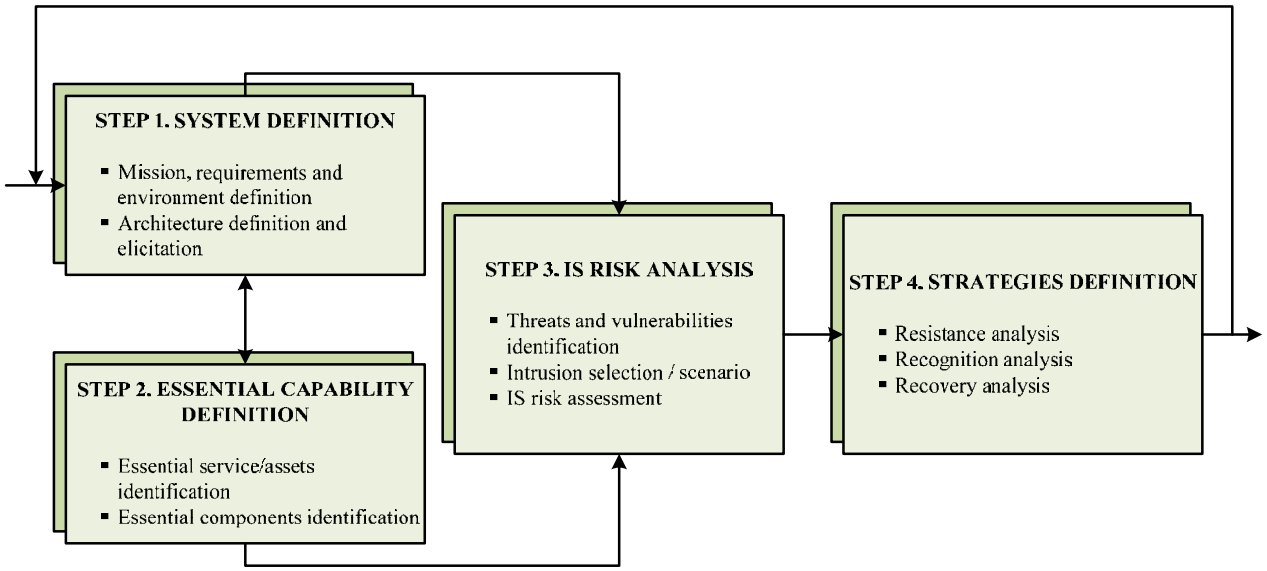

Fig. 1. Algorithm of the Information Assets Survivability Property Analyses Approach

and scenario analysis show which situations are likely to arise and how much damage will result. The analysis can then incorporate various mitigation mechanisms and demonstrate the costs and savings that will occur [7].

Attack trees are multi-leveled diagrams consisting of one root, leaves, and children. From the bottom up, child nodes are conditions which must be satisfied to make the direct parent node true; when the root is satisfied, the attack is complete. Each node may be satisfied only by its direct child nodes. A node may be the child of another node; in such a case, it becomes logical that multiple steps must be taken to carry out an attack. Note also that an attack described in a node may require one or more of many attacks described in child nodes to be satisfied [8].

So, for the information assets survivability property analysis we decompose a node of an attack tree either as

- a set of attack sub-goals, all of which must be achieved for the attack on survivability property to succeed, that are represented as an AND-decomposition, or
- a set of attack sub-goals, any one of which must be achieved for the attack on survivability property to succeed, that are represented as an OR-decomposition.

In our analysis approach attack trees can be represented graphically or textually. The main rules of the representation are presented on the Figs. 2 and 3.

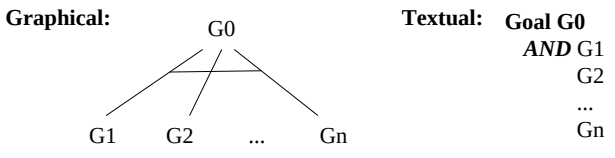

Fig. 2 AND-Decomposition

Fig. 2 represents a goal G_0 that can be achieved if the attacker achieves each of G_1 through G_n. Fig. 3 represents a goal G_0 that can be achieved if the attacker achieves any one of G_1 through G_n.

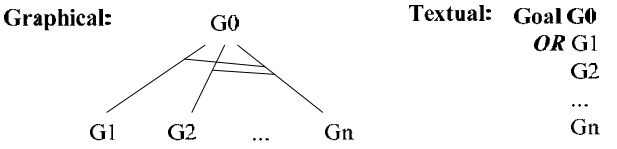

Fig. 3. OR-Decomposition

During the performing of the information assets survivability property analysis attack trees allow the refinement of attacks to a level of detail chosen by the analyser. This property permits an analyser to explore certain attack paths in more depth than others, while still allowing an analyser to generate survivability property intrusion scenarios that make sense. In addition, refining the branches of the attack tree generates new branches, resulting in intrusion scenarios at the new lower level of abstraction [9].

To apply Attack Tree Method during the performing of the Step 3 from survivability analysis approach it's necessary to perform five steps process [7]:

- Create an attack tree model showing possible ways to attack the information assets survivability property.
- Predict how adversaries will attack using Capability-based Analysis.
- Identify the impact associated with each survivability property attack scenario. An attack scenario is the set of events that characterize a particular survivability property attack.
- Determine the level of risk associated with each survivability property attack scenario.
- Monitor the system for signs that the survivability property attack scenario is in progress.

The Capability-based Analysis [7] that we are using for the information assets survivability property analysis determine the risk of survivability property damage R as

$$R = P \times I \ , \qquad (1)$$

where P – is probability of the survivability property attack implementation;

I – is the impact caused by the survivability property attack implementation.

If the probability of the survivability property attack implementation P equal to the multiplication of the threat T and vulnerability V

$$P = T \times V , \quad (2)$$

and

$$T = C \times M , \quad (3)$$

where C – is the capability of the survivability property attack implementation; M – is the attacker motivation;

which for a motivated attacker reduced to

$$T = C , \quad (4)$$

then we will have that risk can be determined as

$$R = (T \times V) \times I \quad (5)$$

As the result to prove the effectiveness of the Attack Tree Method in relation to the information assets survivability property analysis we suggest to review the example of the survivability property attack scenario, which presents the implementation of the method above.

For the investigation the authors of the paper chose one of the most unprofitable in financial and secure meaning attacks which can damage the survivability property – Distributed Denial of Service (DDoS) attack. DDoS attack is a malicious attempt to make a server or a network resource unavailable to users, usually by temporarily interrupting or suspending the services of a host connected to the Internet [10].

DDoS attack methods commonly deployed are Smurf, ICMP, TCP SYN, UDP, TCP floods and combinations thereof.

Smurf Floods is a reflector attack. Attacker floods the network with ICMP ECHO requests to broadcast address. For the ICMP Floods the attacker generates a flood of ICMP ECHO packets directed at the victim. The victim replies to each ICMP request, consuming its CPU resources and network resources. UDP floods send a large number of UDP packets to the target system, effectively tying up the available network bandwidth. TCP floods are similar to UDP floods. Attackers use TCP packets instead of UDP packets. TCP SYN attack is a vulnerability attack that uses the TCP protocol design to perpetrate a TCP SYN flooding attack. It works by exploiting the way the servers handle the setup of a TCP connection [11].

DDoS attack tree example developed by authors of the paper textually is presented bellow. The graphical form of it is presented on the Fig. 4.

DDoS Attack (Textual Form of the Attack Tree)

OR 1. Performing Vulnerability Attack (TCP SYN Attack)
- **AND** 1. Attacker spoofs IP source address.
  2. Attacker sends a flood of TCP/SYN packets.

2. Performing Flooding Attack
- **OR** 1. Smurf Floods Attack
  - **AND** 1. Attacker spoofs IP source address.
    2. Attacker floods the network with ICMP ECHO requests to broadcast address.

  2. ICMP Floods Attack
  - **AND** 1. The attacker generates a flood of ICMP ECHO packets directed at the victim.
    2. The victim replies to each ICMP request, consuming its CPU resources and network resources.

3. UDP Floods Attack
- **AND** 1. Attacker spoofs IP address of the UDP Packets
  2. Attacker sends a large number of UDP packets to random ports on a remote host.
  3. The victim host replies by sending many ICMP packets, eventually leading it to be unreachable by other clients

4. TCP Floods Attack
- **AND** 1. Attacker spoofs IP address of the TCP Packets.
  2. Attacker sends a large number of TCP packets to random ports on a remote host.
  3. The victim host replies by sending many ICMP packets, eventually leading it to be unreachable by other clients.

Conclusion

As the result of the research process:

1) the information assets survivability property analysis approach was improved, which allows effective survivability property ensuring;
2) the general algorithm of the improved analysis approach was developed, which gives visual representation of the every approach step;
3) the Attack Tree Method was used as the IS risk analysis step in relation to the survivability property, which permitted an analyser to explore certain attack paths in more depth than others, while still allowing an analyser to generate survivability property intrusion scenarios that make sense;
4) the textual and graphical forms of DDoS attack trees were developed, which showed the effectiveness of the using Attack Tree Method as the IS risk analysis step of the information assets survivability property analysis approach.

The authors of the paper notice that improved approach has certain limitations, the resolution of which will be the subject of further research.

References

[1] I. R. Garasym, V. A. Romaka, M. M. Rybiy, “Zabezpechennia zhyvuchosti ta neperervnosti funktsionuvannia system zakhystu informatsii” [“Information Security Systems Survivability Property and Continuity Functioning Ensuring”], Visnyk NU «Lvivska politechnika» «Avtomatyka, vymiriuvannia ta keruvannia», no. 741, pp. 105-112, 2012.

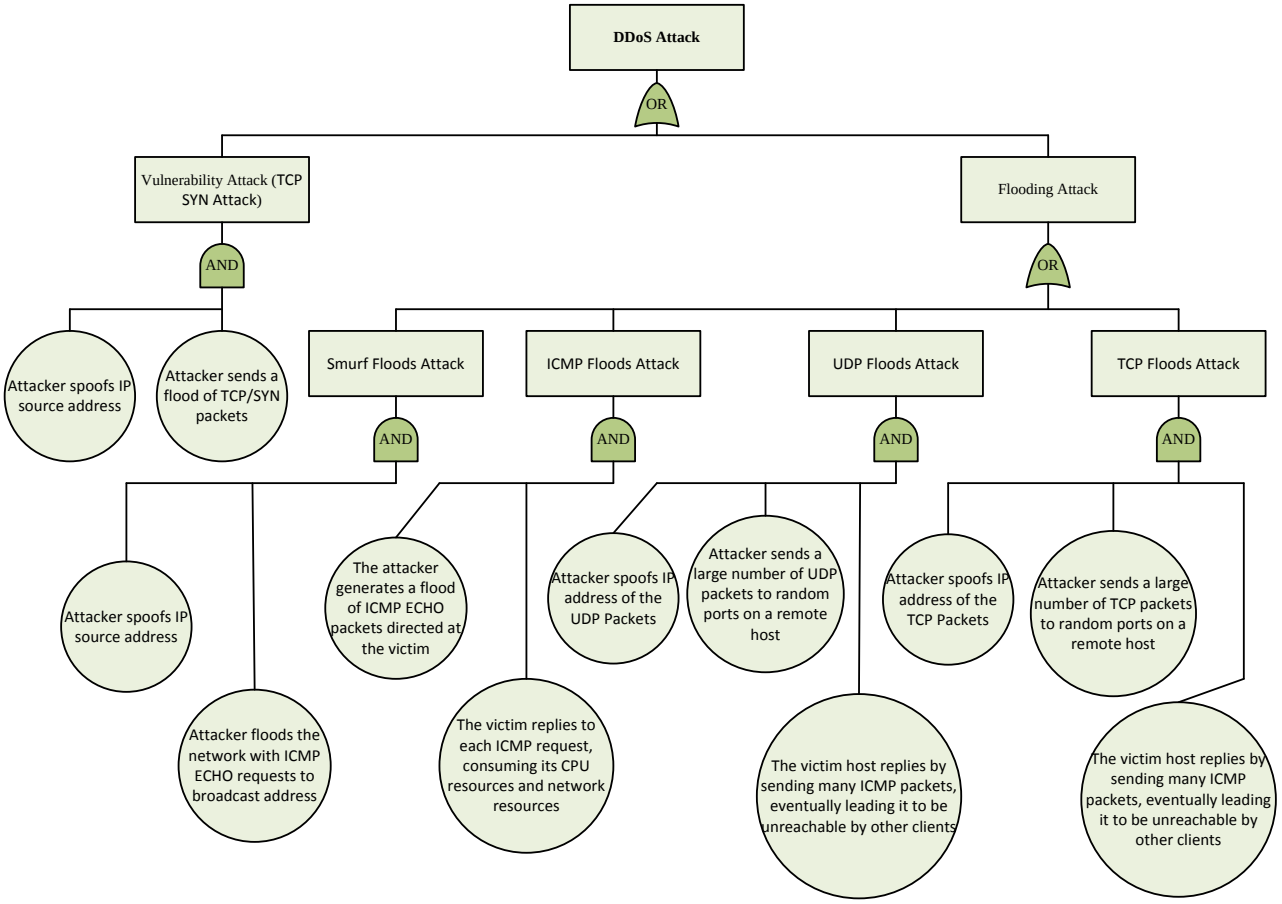

Fig. 4. Graphical Form of the Attack Tree Method

[2] I. Garasym, V. Romaka, M. Rybiy, "Information Security System Survivability Property Research in Emergency Operating Conditions", in Proceedings of the 12-th International Conference "The Experience of Designing and Application of CAD Systems in Microelectronics": CADSM 2013, February 19-23, 2013, Polyana Svalyava, Ukraine. Lviv: Vydavnyts-tvo Lvivskoi politekhniky Publ., 2013. pp. 95-96.

[3] Nancy R. Mead, Robert J. Ellison, Richard C. Linger, Thomas Longstaff, John McHughP, "Survivable Network Analysis Method", Sept. 2000. [Online]. Available:http://www.sei.cmu.edu. [Accessed: Sept. 10, 2013].

[4] Song Huang, "Survivability Strategies for the Next Generation Network", Information Systems Control Journal, ISACA, vol. 6, 2006. [Online]. Available: http://www.isaca.org. [Accessed: Sept. 10, 2013].

[5] I. R. Garasym, V. A. Romaka, M. M. Rybiy, "Analiz ryzykiv pry zabezpechenni zhyvuchosti ta neperervnosti funktsionuvannia system zakhystu informatsii" ["Risk Analysis during the Information Security Systems Survivability Property and Continuity Functioning Ensuring"], in Proceedings of the 16-th Ukrainian Scientific Internet Conference "Research is a tool for resolving key economy problems", Novembre 28-29, 2012, Ternopil, Ukraine. Ternopil: Taip, 2012. pp. 3-5.

[6] Howard F. Lipson, David A. Fisher, "Survivability – A New Technical and Business Perspective on Security", NSPW '99, pp. 33-39, 2000. [Online]. Available: http://delivery.acm.org. [Accessed: Sept. 10, 2013].

[7] Amenaza Technologies Limited, "Understanding Risk Through Attack Tree Analysis", 2003. [Online]. Available: http://www.amenaza.com. [Accessed: Sept. 20, 2013].

[8] Dilip Thomas, K.S.M. Panicker, "Data Security Architecture using Embedded Chip", International Journal of Computer Science and Network Security, IJCSNS, vol. 11, no 5, May 2011. [Online]. Available: http://paper.ijcsns.org. [Accessed: Sept. 29, 2013].

[9] Andrew P. Moore, Robert J. Ellison, Richard C. Linger, "Attack Modeling for Information Security and Survivability", March 2001. [Online]. Available: http://citeseerx.ist.psu.edu. [Accessed: Sept. 23, 2013].

[10] "Distributed Denial of Service Attacks". [Online]. Available: http://www.incapsula.com. [Accessed: Sept. 29, 2013].

[11] S.Karthik, V.P. Arunachalam, T.Ravichandran "An Analysis of DDos attack methods, threats, tools and defense mechanisms". [Online]. Available: http://www.academia.edu. [Accessed: Sept. 29, 2013]