Modeling Analysis of Advanced Persistent Threat – Based on UML

Bin Dong[1,a], Wentao Zhao[1], Jianglong Song[1]

[1]National University of Defense Technology, Changsha, China

[a]dobi110@qq.com

Keywords: advanced persistent threat attack, attacking processes, UML modeling.

Abstract. This paper reveals the inherent features of advanced persistent threat (APT), and summarizes its general attacking processes, attacking means and methods. The attacking steps model of APT which is based on UML effectively describes the application principles of APT and its behavior features, mode features and target features. Therefore, a series of methods to defend APT are proposed.

The Features of APT

Advanced Persistent Threat (APT) is a compound network attack with a specific target launched by some hackers or political groups in recent years. It uses many advanced attacking means and social engineering methods and penetrates into the target network step by step. Its ultimate goal is to get the target's important assets information or some sensitive information. The attacking target is generally military institutions, large enterprises or national government agencies. The attack aims to destroy industrial infrastructures, theft the important data which is related to national security and the people's livelihood. In March 2011, RSA Company, a subsidiary of EMC Corporation, suffered ongoing invasion. A part of RSA SecureID technology and some related customers' information were stolen, which directly lead to the fact that many companies with VPN network which was established with SecurID as its authentication credentials were attacked and much important information was stolen, including Lockheed Martin, Northrop Grumman and other American defense contractors [1].

APT is often very complex and diverse. APT has three essential features: a) High-class: In APT attacks, generally, single attack means (such as RAT, SQL injection and back door, etc.) cannot succeed in actions. Therefore, the intrusion team will use a full range of various intrusion technologies and dynamically adjust them, which aim to successfully infiltrate into the target. [2] b) Continuity: The attacker will continuously invade and infiltrate into the target over a long period with various attacking means. The incubation period is generally a few months or even a year. After the successful invasion, a three-to-five-years' detection is also common. c) Menace: Instead of using automatic code to launch attacks, APT attack is a manmade attack which is commanded and coordinated by the organizers. Its ultimate goal is to destroy and steal important assets information, which may even cause a threat to social stability and national security.

Through the study of many attacks and the attacking processes, it was found that APT is difficult to prevent and its high risk is mainly due to its three features:

a) Targeted: APT attack has a clear goal. All the attacks are launched with a specific target, a piece of confidential document (RSA SecureID stealing attack), or programmable logic controller of industrial control system (Stuxnet) [3], or a specific organization (Night dragon attacks). The attacker driven by interests (for instance, enterprise interest or national interest) will carry out various network attacks to achieve the specific purpose. Perhaps, a phishing attack is just to download a trigger, but it is an important step during the penetration of APT attack. The targeted APT also must make detailed detection of a specific object before each attack. Even if two different attacks happened are not directly connected in time, their goals must be interlocked in space. Therefore, the attack would move on.

b) Diversity: The various methods adopted by an attacker are closely related to the development of network technology. Therefore, the update of network technology also reflects the upgrade of the attacking means used by hacker. APT includes the spreading of virus, Trojan horse virus and other

traditional means, as well as SQL injection, zero-day vulnerabilities, hardware deficiency and operating system vulnerabilities, etc. The attacker even can adopt auxiliary means which is combined with social engineering and psychology to collect data and succeed to attack. [4] Such an attack makes it difficult for the target to prevent. Therefore, the success rate of attack is greatly improved. In addition, it splits the target's attention and helps to covert attacking intent.

c) Invisibility: The target host is generally installed in a relatively perfect intrusion detection system. Therefore, the conventional hacker attack is difficult to achieve the purpose. The dynamic behaviors of APT and the concealment of its static file are significantly better than the conventional hacker attack. By carrying out some approaches (for instance, an encrypted channel, a hidden shell connection, a low profile attack, fake and forged digital signature, etc.), APT makes traditional security equipments and detection methods which are based on signature cannot distinguish between the true and the false. [5] In fact, Stuxnet attack can incredibly lurk in the target system for years after its invasion. Meanwhile, Night dragon attacks can even cheat the firewall of the target system and transfer much sensitive information after its invasion. The malicious code of Operation Shady RAT is carefully camouflaged and cannot be identified by security equipments for several years. In addition, the traditional detection is based on real-time monitoring at single time point. It is difficult to carry out effective tracking of APT with large time span.

Through the above feature analysis, we made a comparison between APT and traditional hacker attack. The results were shown in table 1-1:

Table 1-1 The comparison of APT and traditional hacker attack

	Traditional hacker attack	APT
Goal specificity	Large spreading of Botnets	Clear attacking target
Attacking group	Personnel or hacker team	Professional team
The features of attacking targets	Not targeted, but with large range	Strong targeted, with small range
Network destroy	Network destroy with certain target	No network destroy
Attacking frequency	Only once	Frequent over a long period
Attacking targets	Economic benefits	To steal vital confidential information and Intelligence
The features of attacking means	Fast and single	Various and low profile
Common methods	Various common hacktools Malicious URL Trojan software	Social Engineering approaches Many zero-day vulnerabilities Various Backdoor Trojan Various RAT

APT Attack Modeling

The Process of APT Attack. Though APT attacks use different methods, they are goal-oriented. The general process of APT attack can be obtained through summarizing regularities. As shown in Figure 2-1, intruders take advantage of social engineering science to detect first. And they scan targeted network with the help of various scanning tools, collecting all kinds of information against the target, such as network segment, public website information and higher staffs' daily schedule within the target system in order to make preparation for following attack. Next, intruders infiltrate the targets by using websites embodied by Trojan or SQL injection for the purpose of approaching targeted network; afterwards, they install back door into the host computers which have direct relation with targeted network by the means of Trojan virus; then intruders can get access to the host computers in brute-force way to make Botnet so as to launch comprehensive attack; finally they can collect valuable information by spreading malicious code within targeted network, and package the

encrypted data into the local machine controlled by intruders. Finally, intruder hides in targeted host computer to wait for next attack. [6]

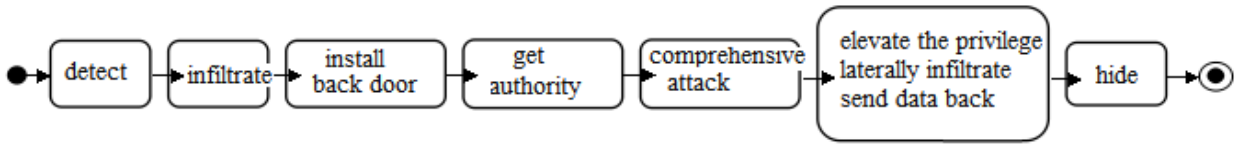

Figure 2-1 The process of APT attack

To make a more detailed description of the process of APT attack, this paper will use UML to build models for APT attack, mainly covering Use Case Diagram, Sequence Diagram and Activity Diagram. In light of the process of APT attack, the attacked targets can be categorized into three: ordinary network objects, interior objects of important targets and important targets. Ordinary network objects refer specifically to those controlled puppet computers or networks, not belonging to targeted network; interior objects of important network are users or equipments within the network of important targets; important targets are intranets of important departments, often including kinds of valuable information, which are the ultimate goals of APT attack.

Use Case Diagram of APT Attack. The major participants attacked by APT involve sponsor, intruder, ordinary network object and interior objects of important targets. Sponsor is in the decision-making level of APT attack, mainly checking attack scheme and giving attack orders during the whole process; intruder is executor, chiefly working out attack plan, detecting and infiltrating network, and controlling ordinary network objects, etc; while ordinary network objects, known as controlled puppet computers or networks, invade and control targeted network through launching comprehensive attack. [7] Interior object of important targets is the last of APT attack, primarily being used to steal and pass sensitive data back to local machine controlled by invaders. In line with above task allocation, Use case diagram shown in Figure 2-2 can be reached. UML uses this figure to clearly express functions of each participant, making a systematical description of APT attack and invaders' deeds.

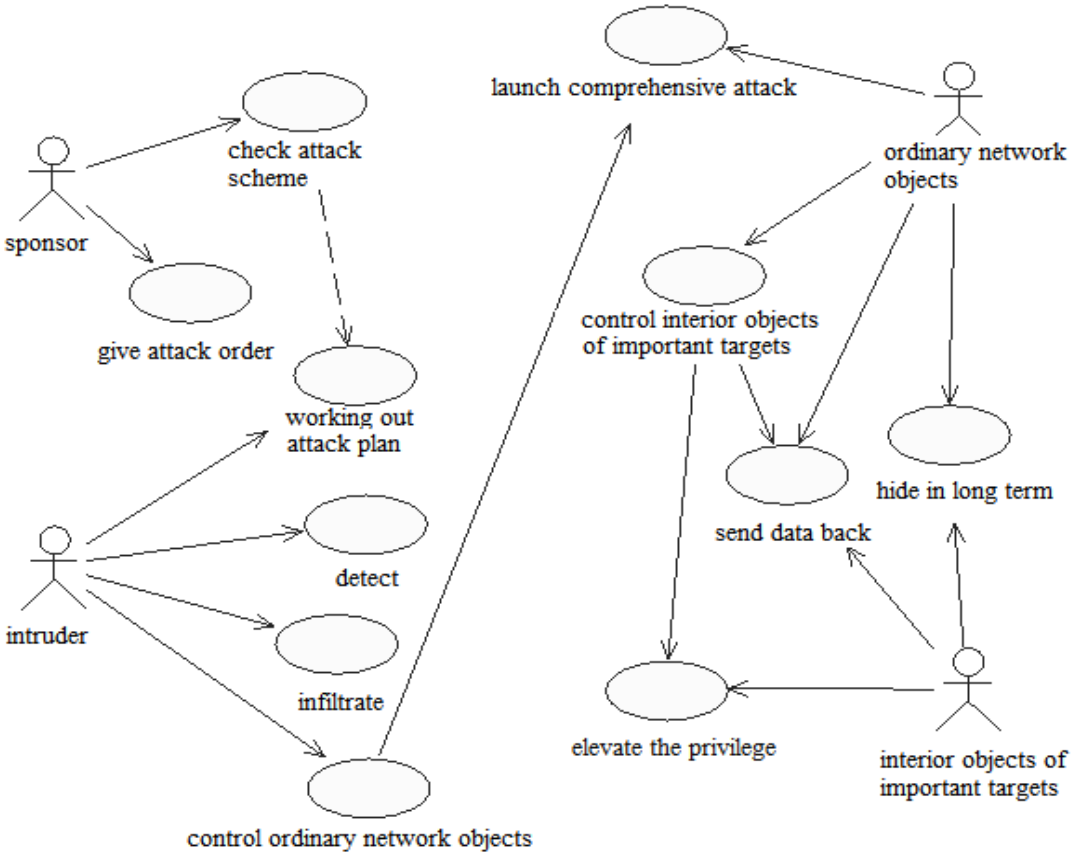

Figure 2-2 Use Case Diagram of APT attack

Sequence Diagram of APT Attack. Based on different tasks, intruders can be refined as sponsor, attacker, scout and infiltrator. Sequence diagram of APT attack describes its visual track over time. [8] Interaction among objects is indicated through directed line segments of which the dotted lines signify information feedback. Sequence diagram of APT attack represents the realization process of the cases of each attacked object, showing these objects' interactive action and message transmission developed in chronological order, as shown in Figure 2-3.

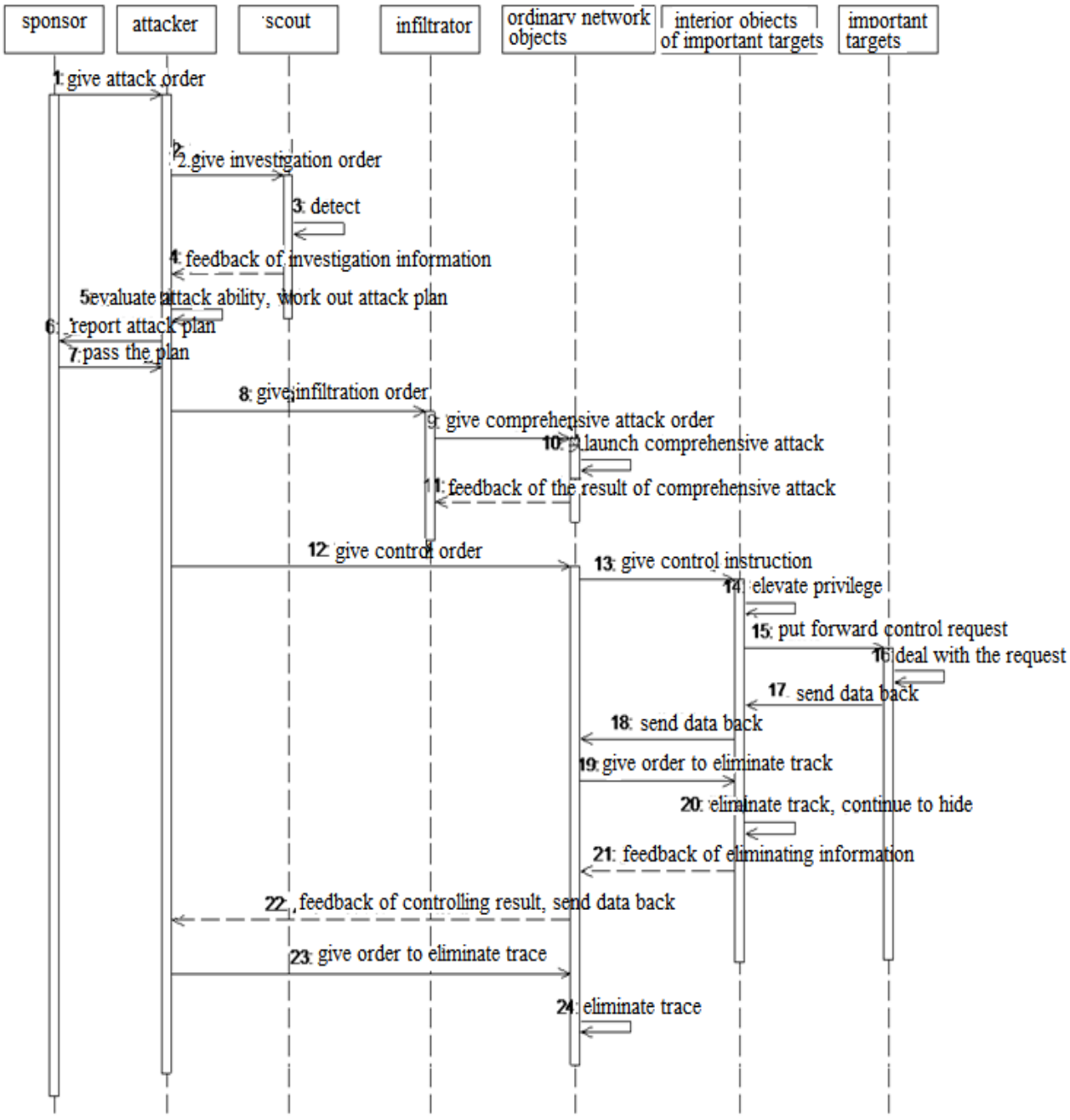

Figure 2-3 Sequence Diagram of APT attack

Activity Diagram of APT Attack. In order to present the spatial relationship among all attacking means, Activity diagram of APT attack is depicted on the basis of Sequence diagram. Activity diagram reveals fully the whole procedure of APT attack, organizing all objects through activities, which has described the dynamic behavior of APT attack. [9]Serial and parallel relation among activities also can be clearly revealed, which provides reference for the organization of APT attack. As shown in Figure 2-4, there are three key activities during APT attack: infiltrating network, controlling ordinary network objects and conducting comprehensive attack, expressed as three cycle-judged circuits.

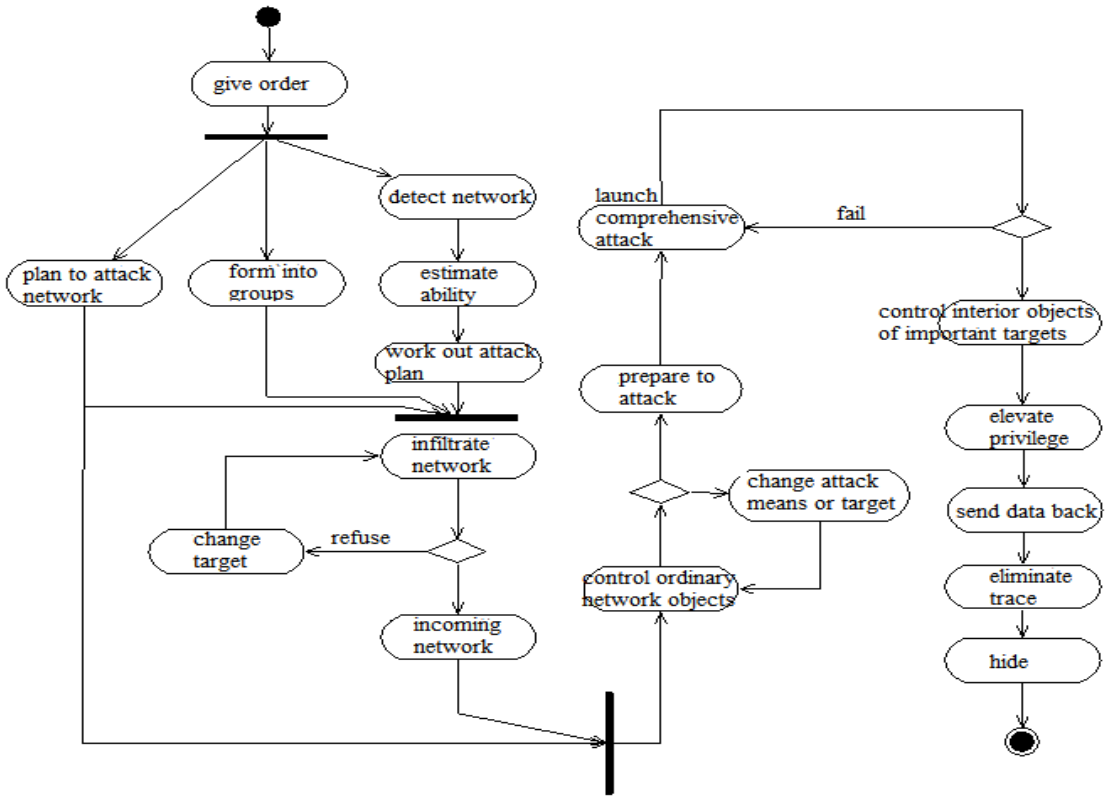

Figure 2-4 Activity Diagram of APT attack

Conclusions

This paper analyzed the features of APT behaviors. Through the UML modeling analysis, it compared the traditional defense system and the present one. The present paper also summarized several methods of APT defense system: a) the security defense of web application programs; b) the security defense of server and network equipments; c) the security defense of the operation and maintenance center; d) the security defense of internal network; e) the social engineering attacking prevention; f) to improve the response capability of network security emergency. [10].

References

[1] Dan Sullivan. Beyond the Hype: Advanced Persistent Threats [R]. Realtime, 2011.

[2] Symantec. W32. Stuxnet dossier version. 3[EB/OL]. http://www.trendmicro.com, 2010.

[3] David Helan. Stuxnet: analysis, myths and realities [J]. Actusecu 27. 2010, 14:23-25.

[4] A. Nicholson, S. Webber, S. Dyer, T. Patel, and H. Janicke. SCADA security in the light of cyber-warfare [J].Computers & Security.2012, 31(4): 418 – 436.

[5] Dmitri Alperovitch. Revealed: Operation Shady RAT [R]. McAfee. 2011.

[6] Lau, H. The truth behind the shady rat [R]. 2011.

[7] Gross, M. J. Exclusive: Operation shady rat-unprecedented cyber-espionage campaign and intellectual-property bonanza [R]. 2011.

[8] Larsson, S. Microsoft excel 'featheader' record remote code execution vulnerability [R]. 2009.

[9] Nusca, A. Operation shady rat: Five things to know [R]. 2011.

[10] Wikipedia，Advanced Packaging Tool.