The Situational Awareness Based on Trusted Measurement

Jie Qiang[1,a], Qing Pan[1,] and Fei Wang [1]

[1]Equipment Academy, BeiJing, 101416, China;

[a]easyravan@163.com

Keywords: Trusted Measurement, Mass Data, Situational Awareness, D-S Evidence Theory

Abstract. With the rapid development of network technology, how to ensure information security is r a severe test. In this paper, The experimental environment is based on the enhanced by trusted or trusted network equipment, with trusted measurement evaluation index for the data source assess the situation of the specific network, and provide support for the development and application of trusted computing. Finally, the paper puts forward a method that how to deal with massive amounts of data in the future.

1. The Trusted Measurement

There is an important concept --- trusted chain in trusted computing. TCG think if the chain is from an initial "trusted root", trusted relationship can be maintained by way of passing down and not be destroyed, then the platform computing environment is always a trusted, when the computing environment of platform for each conversion, then the computing environment is to be trusted all the time, and the trusted computing environment represents the trusted entity[1]. Starting from the idea, we need to implement the trusted chain transfer in the trusted computing environment. To achieve trusted chain transfer, we must build “trusted root" on the computing platform, the integrity of the trusted root was totally trusted. On this basis, in the process of the establishment of a trusted chain, any entity that will transfer the control (the ring before the trusted chain), before the control is transferred to an entity (the ring after trusted chain), the entity must be trusted measurement, if it meets some requirements, such as the value is consistent with a previously stored expected metric, then the control can shift, so the trust if from a previous entity to the next entity

The establishment of the trusted chain is made by trusted measurement. Measurement can be divided into static and dynamic measurement metrics. In the theory of trusted chain, before the system is trusted to run, whether it is at the bottom of the BIOS setup module or in the top of the application, all need to measure, that is, a measurement or the certification process. Data integrity measurement technology is based on the Message Authentication Code MAC (Message Authentication Code) of the consistency check to realize the measurement function. This way ensures the trusted chain is passed from the source up.

In this paper, the security events by measuring are as follows:

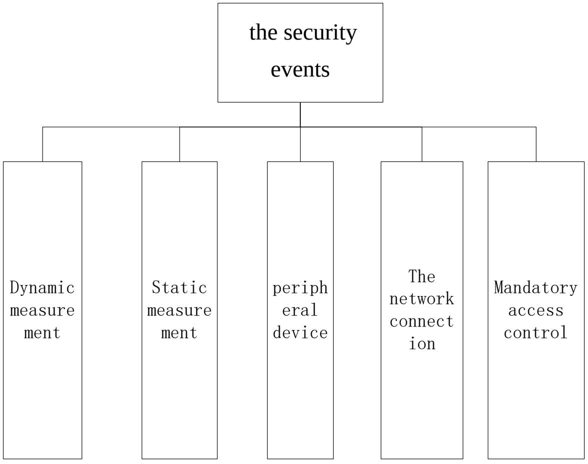


Fig. 1 the security events

2. Situational Awareness

D-S evidence theory is an uncertainty reasoning approach to meet the conditions of weaker than probability, can distinguish between "uncertainty" and "I don't know", and can deal with uncertainty caused by "I don't know", and has great flexibility, it has great advantages in the expression of uncertain information and synthesis.[2] First to set up the logical relationship between evidence and proposition, namely the way to gather the situational factors to situation state, and determine a basic probability distribution; Then according to the arrival of the evidence, that is, each an incident reporting information, the use of evidence combination rule of evidence synthesis, get a new basic probability distribution, and send the results of the synthetic to decision logic to judge, it will have the biggest confidence proposition as alternative proposition. When the event occurs constantly, this process will be continued until the final integration is completed.

In this paper, the device will be divided into categories serial device, terminal device and server class

Here's terminal device class as an example to show the calculation process

Security event represented by the above five categories A_1, A_2, A_3, A_4, A_5

Framework for the recognition $U = \{A_1, A_2, A_3, A_4, A_5\}$

$m(A_1)_j, m(A_2)_j, m(A_3)_j, m(A_4)_j, m(A_5)_j$ expressed confidence terminal equipment distribution function, j represents the number of times that the measure appears

The fusion $m(A) = K^{-1}\sum_{\bigcap A_i = A}\prod m(A_i)_j, 1 \le i \le 5并且1 \le j$ (1)

$$K = 1\text{-}(m(A_1)m(A_2)m(A_3)m(A_4)m(A_5)) \tag{2}$$

Situation can be derived for the contribution of a single device, and the calculation is also available on the contribution of the terminal device class and server class.

Provided equipment for the above three categories A,B,C

Framework for the recognition $U = \{A,B,C\}$

Through the above calculated probability assignment of a single device posture contribution, the result will be calculated as an overall trend calculation.

$m(A_i), m(B_i), m(C_i)$

According to Dempster combination rule

$$m(all) = \mathrm{T}^{-1}\sum\prod m(A_i)m(B_i)m(C_i) \tag{3}$$

$$T = 1\text{-}\sum_{C_i \cap B_i \cap A_i = \varnothing,}(m(A_i)m(B_i)m(C_i)) \tag{4}$$

Finally ,calculat the result of fusion and obtain the probability assignment of the whole network, to determine the trend. The flow chart is as follows:

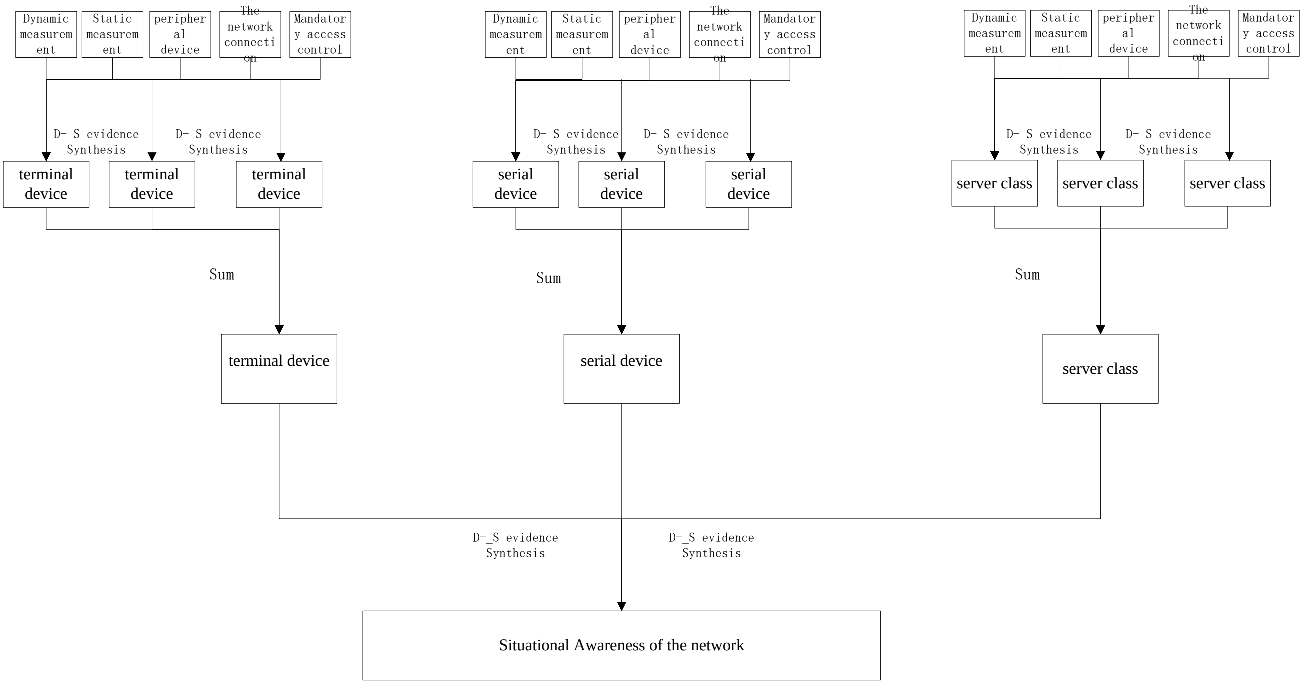
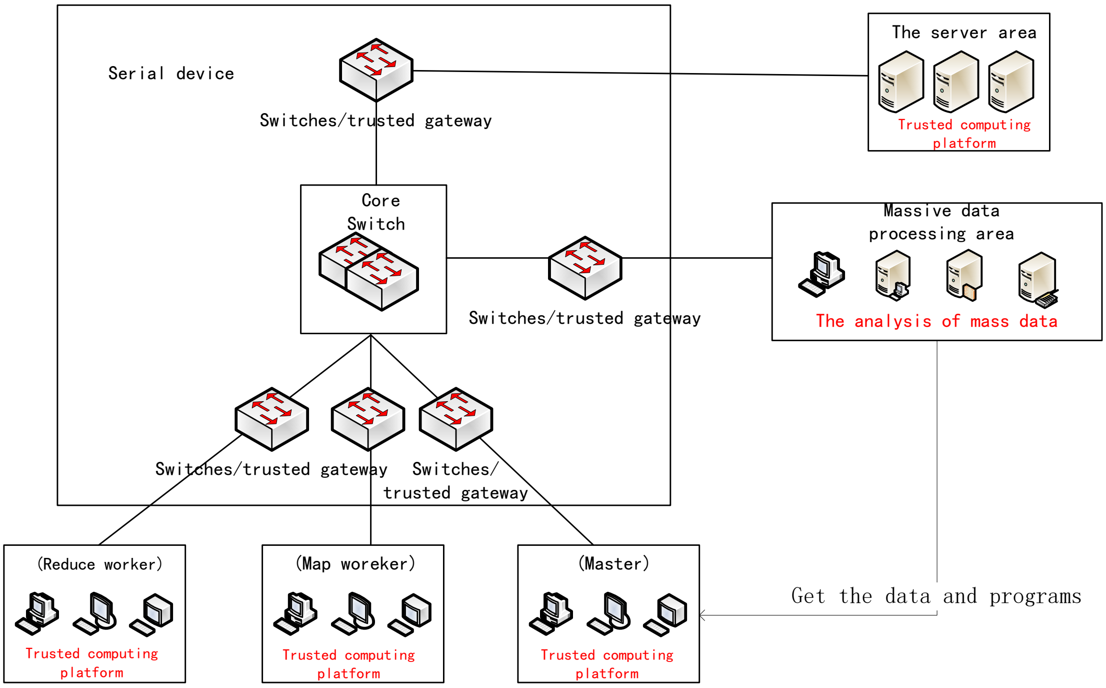


Fig. 2 The fusion process

3. Mass Data Processing and Deployment

Considering the number of devices, the evidence fusion will be quite a large amount of calculation, so we joined the model and the actual deployment environment for mass data computing. The mapreduce model is popular model now. So given the deployment diagrams



Serial device
Switches/trusted gateway
The server area
Trusted computing platform
Core Switch
Massive data processing area
Switches/trusted gateway
The analysis of mass data
Switches/trusted gateway
Switches/ trusted gateway
(Reduce worker)
Trusted computing platform
(Map woreker)
Trusted computing platform
(Master)
Trusted computing platform
Get the data and programs

Fig. 3 the deployment of network

In this paper, the key is represented by the three categories of equipment classification; the value is represented by each device to calculate the trusted of the distribution.

The control program---master, the rest of the executable program are as the master worker to dispatch work. There are M map tasks and R Reduce tasks to dispatch. Master chooses free worker to share the map tasks or reduce task. The work of assigned map task is to block calculation; the work of assigned reduce task is to calculated the result of map task.

4. Summary

In this paper, to evaluate the network situation awareness that is made up of trusted or trusted enhanced equipment achieved good results; provide support for the development and application of trusted computing.

References

[1]. Trusted Computing Group. TCG PC Specific Implementation Specification Version 1.1[DB/OL],https://www.trustedcomputinggroup.org.

[2]. DenceuxT. Analysis of evidence theoretic decision rules for pattern classification.Pattern Recognition，1997, 30 (7): 1095-1108.