Security Situation Assessment Method Based on States Transition

CSTCERT，CNIC，CAS

March, 2018

中国科学院
计算机网络信息中心
Computer Network Information Center,
Chinese Academy of Sciences

OUTLINE

INTRODUCTION

中国科学院
计算机网络信息中心
Computer Network Information Center,
Chinese Academy of Sciences

BACKGROUND

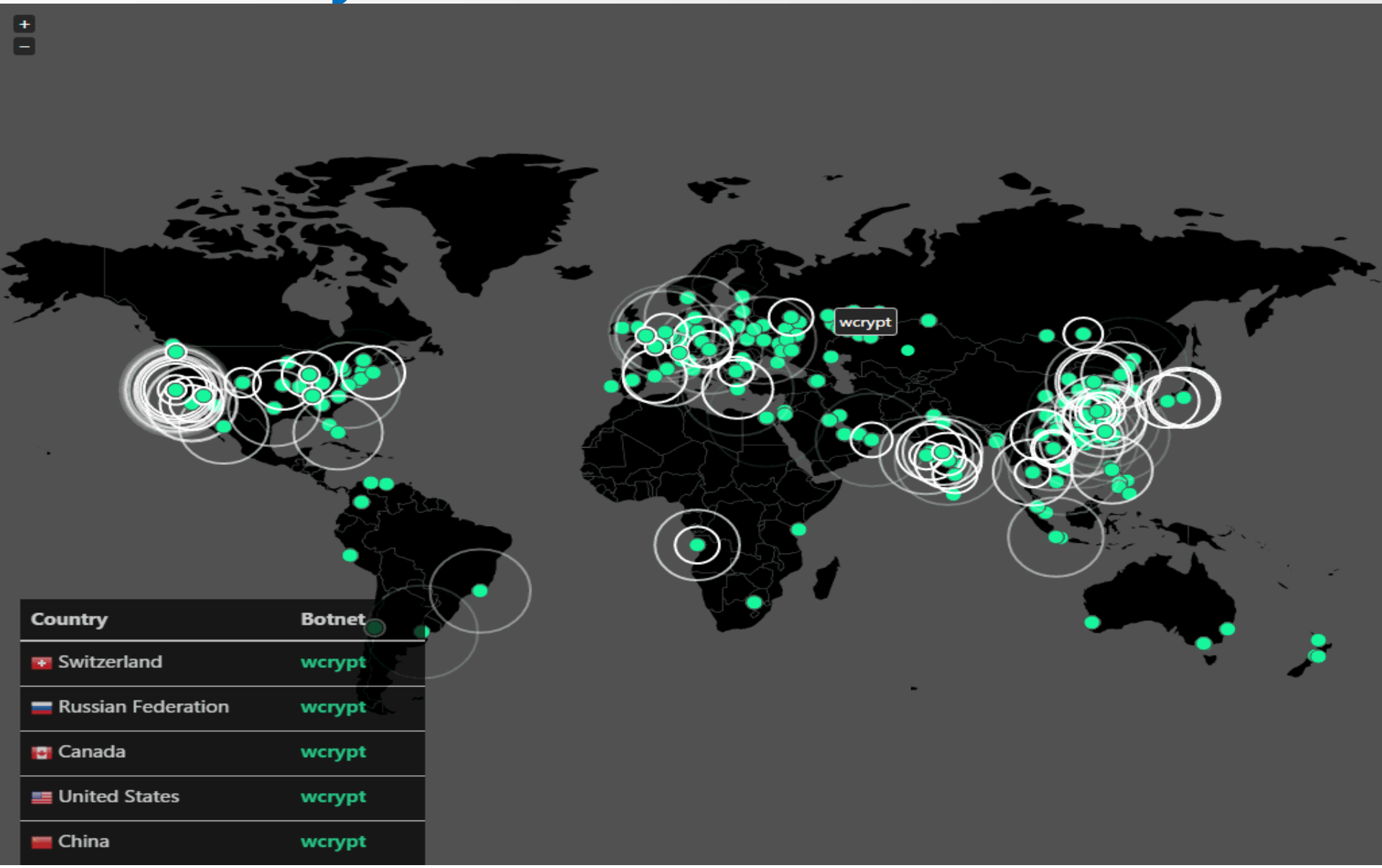
Increasing network security problems in the repaid popularization of network technology applications.

2015, nearly *200,000,000* victims in China controlled by Botnet or Trojans. *25,000* phishing pages webpages in China has been monitored.
2016, increasing *10822* vulnerabilities. High-risk vulnerabilities accounted for *38.3%* mainly covered worldwide vendors.

SECURITY SITUATION OF LARGE-SCALE NETWORK

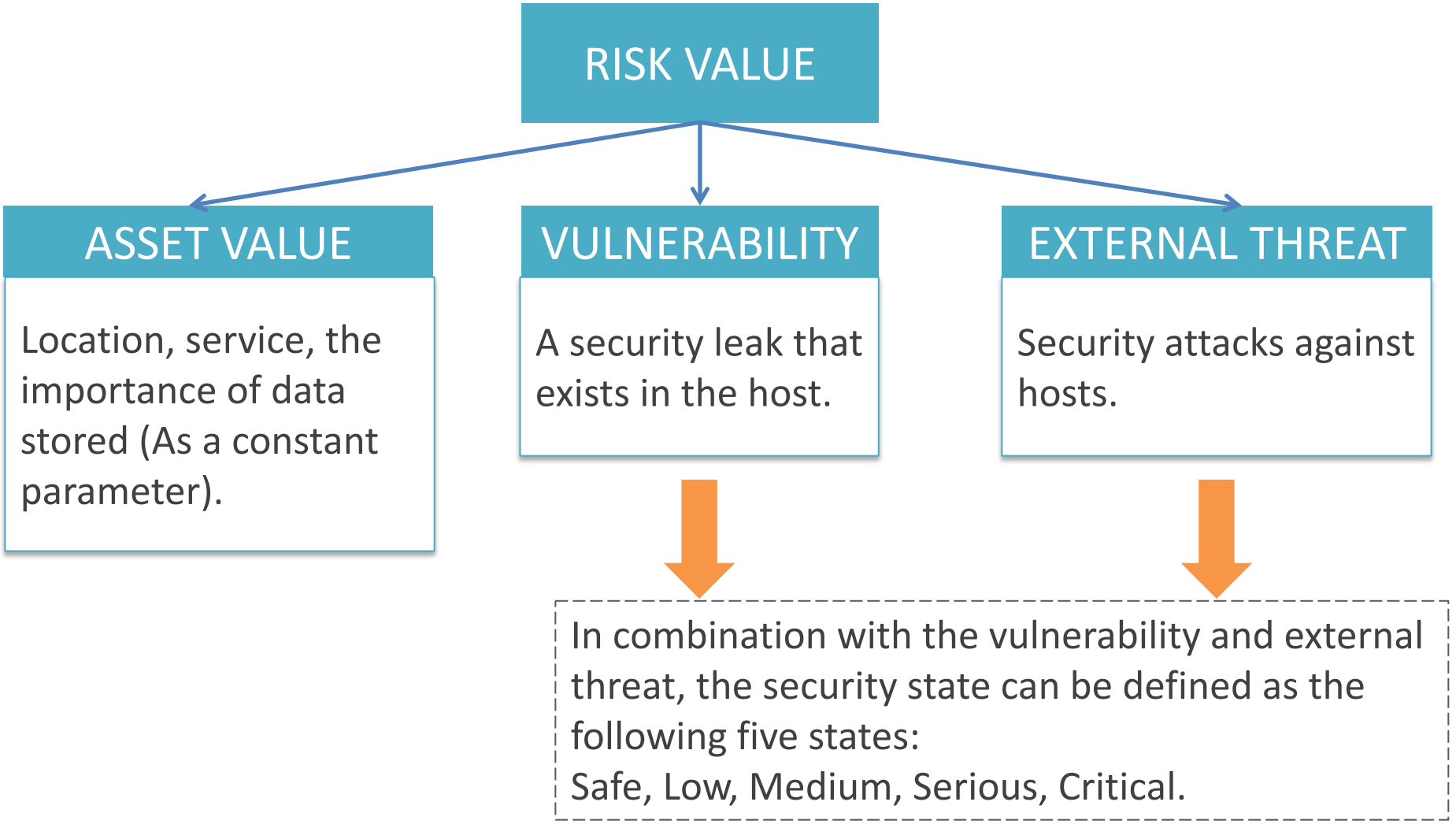
- A large-scale network consists of an exit, a core, a convergence, an exchange and a terminal layer.
- The security state is a static concept that describes the security status of the asset at a given moment.
- Security situation value of large-scale network can be calculated on the basis of the security situation analyzing of each asset.

WannaCry



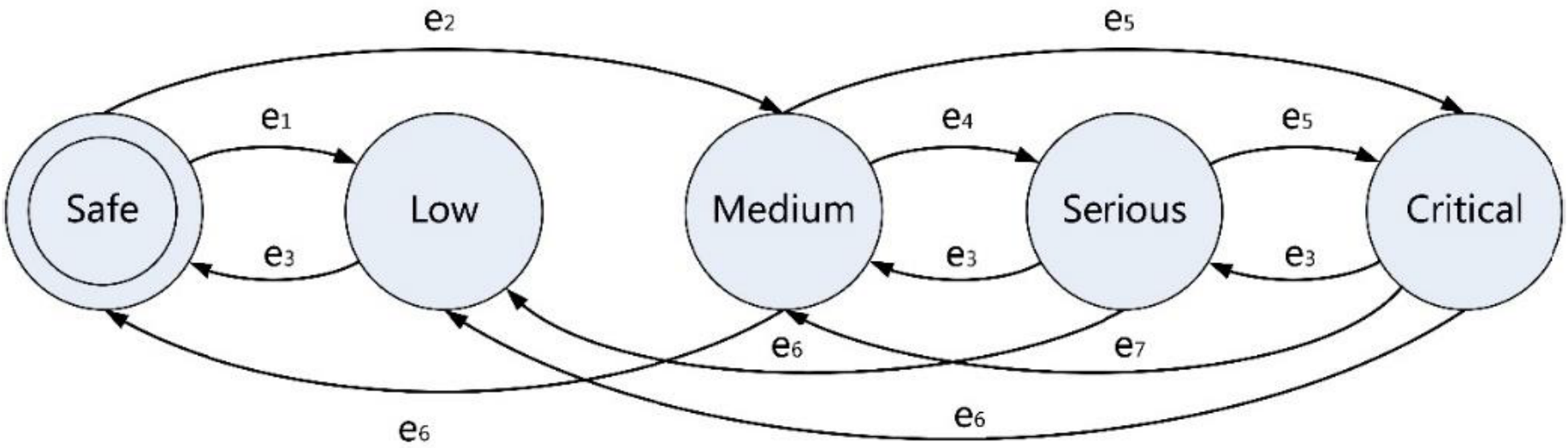
ref：https://intel.malwaretech.com/WannaCrypt.html

SECURITY STATES ANALYSIS



SECURITY STATES ANALYSIS

中国科学院
计算机网络信息中心
Computer Network Information Center,
Chinese Academy of Sciences



SAFE

No any known vulnerabilities and exposed external attacks.

LOW

No any known vulnerabilities, but subject to an external attacks.

MEDIUM

One or more vulnerabilities, but not subject to any external attacks.

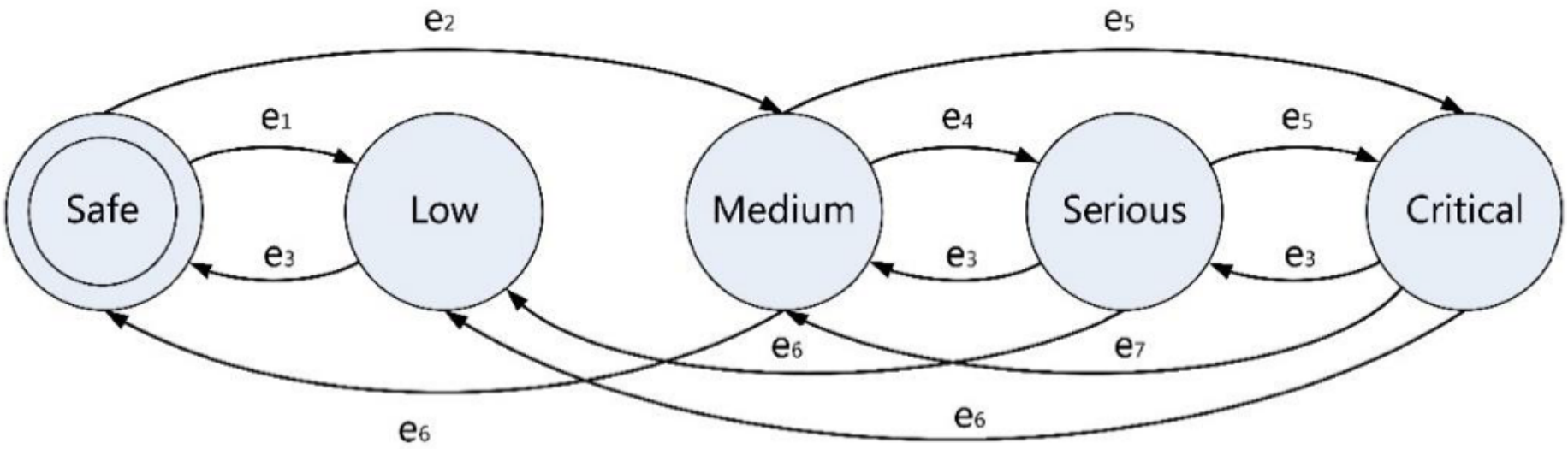
SERIOUS

One or more vulnerabilities, and cannot fully use the vulnerability under attacks.

CRITICAL

One or more vulnerabilities, and under attacks that can fully use the vulnerability.

SECURITY STATES ANALYSIS



Detailed security states changes as bellows:

Event ID	Description
e_1	The host is under any external attacks.
e_2	The host found a new security vulnerability.
e_3	All attacks are ended or blocked.
e_4	The host is under attack but cannot be exploited.
e_5	The host is under attack and can be exploited.
e_6	The host vulnerability is repaired.
e_7	The attack that exploited vulnerability is ended or blocked.

SECURITY SITUATION ASSESSMENT MODEL

ASSESSMENT MODEL ESTABLISHMENT

Observable information obtained by tools

Vulnerabilities,
Various security events

Host 1
security risk analysis

Host 2
security risk analysis

.....

Host N
security risk analysis

Further calculating the risk value of the host.

SECURITY SITUATION ASSESSMENT MODEL

COMBINED WITH HIDDEN MARKOV MODELS(HMM)

HOST SECURITY STATUS
As a hidden state set(safe, low, medium, serious, critical), transfer under the certain conditions.

$\lambda = (S.V.A.B.\Pi)$

SECURITY EVENT SEQUENCE
As a random process, each security event has a certain impact on the changes in the security status

λ, the security situation assessment model based on the states transition.
S, the collection of security states of the host.
V, the collection of event type.
O, is the observability vector sequence based on V.
A, the host security state transition conditional probability matrix.
B, collection of probabilities of attack types that can be observed in a secure state.
Π, the initial security state vector.

CALCULATION METHOD OF SECURITY SITUATION

SECURITY SITUATION CALCULATION METHOD

- Host asset risk vector: $K = \{k_i\}$ ($i \in [1, N]$, k_i, risk value of the host state s_i)

  According to the definition of the forward backward algorithm,

$$\alpha_t(j) = \begin{cases} b_j(o_1)\pi_j, & t = 1 \\ b_j(o_t)\sum_{i=1}^{N}\alpha_{t-1}(i)a_{ij}, & t > 1 \end{cases} \quad (1)$$

$$\beta_t(i) = \begin{cases} 1, & t = T \\ \sum_{j=1}^{N} a_{ij}b_j(o_{t+1})\beta_{t+1}(j), & 1 \le t < T \end{cases} \quad (2)$$

$a_i(j)$: the probability that the state is s_j at t moment.
$\beta_t(i) = \mathrm{P}(o_{i+1}o_{i+2} \ldots o_r | q_t = s_i)$: the probability that the hidden state is s_i at t moment; the observability vector sequence is $o_{i+1}o_{i+2} \ldots o_r$ after t moment.

CALCULATION METHOD OF SECURITY SITUATION

- The probability of state $\gamma_t(i) = P(q_t = s_i)$ is defined to represents the probability that the state is s_i at t moment.

$$\gamma_t(i) = \frac{\alpha_t(i)\beta_t(i)}{\sum_{i=1}^{N} \alpha_t(i)\beta_t(i)} \tag{3}$$

- The security situation vector of the host is defined as $R = \{r_i\}, i \in [1, N]$. r_i represents the security situation value of the host in the state s_i. Hence, the security situation value of the host at t moment is:

$$r_i = k_i \gamma_t(i), i \in [1, N] \tag{4}$$

$$\Rightarrow \quad R^{(network)} = \frac{\sum_{l=1}^{L} c_l R_l^{(host)}}{\sum_{l=1}^{L} c_l} \tag{5}$$

$R^{(network)}$: the security situation value of the whole network.
L: L assets in a large-scale network
$C = \{c_l\}, l \in [1, L]$: asset value vector

CALCULATION METHOD OF SECURITY SITUATION

METHOD FOR DETERMINING MODEL PARAMETERS

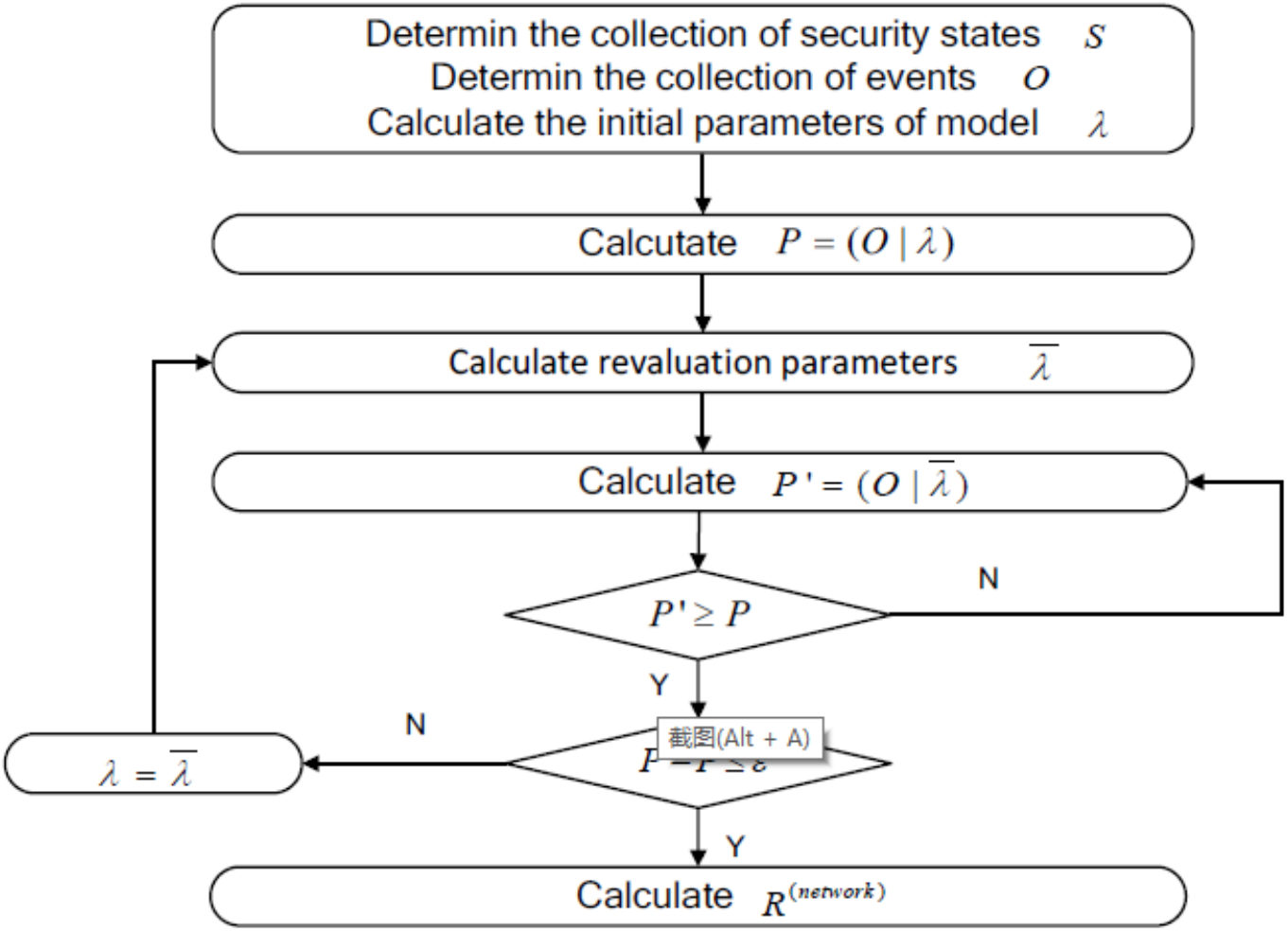
- When calculating the situation value, the selected parameters are static which cannot reflect the trend of changing with time and state. Therefore, the parameters of the security situation assessment model are dynamically adjusted by solving the learning algorithm of the HMM.
- The parameters should be iterated over until the parameter converges to a suitable value.

$P(O\|\bar{\lambda}) \geq P(O\|\lambda)$ is calculated according to the new parameter $\bar{\lambda}$	→	Replace the λ with $\bar{\lambda}$
$P(O\|\bar{\lambda}) < P(O\|\lambda)$ is calculated according to the new parameter $\bar{\lambda}$	→	λ remains

Until the difference between $P(O|\bar{\lambda})$ and $P(O|\lambda)$ tends to be constant

CALCULATION METHOD OF SECURITY SITUATION

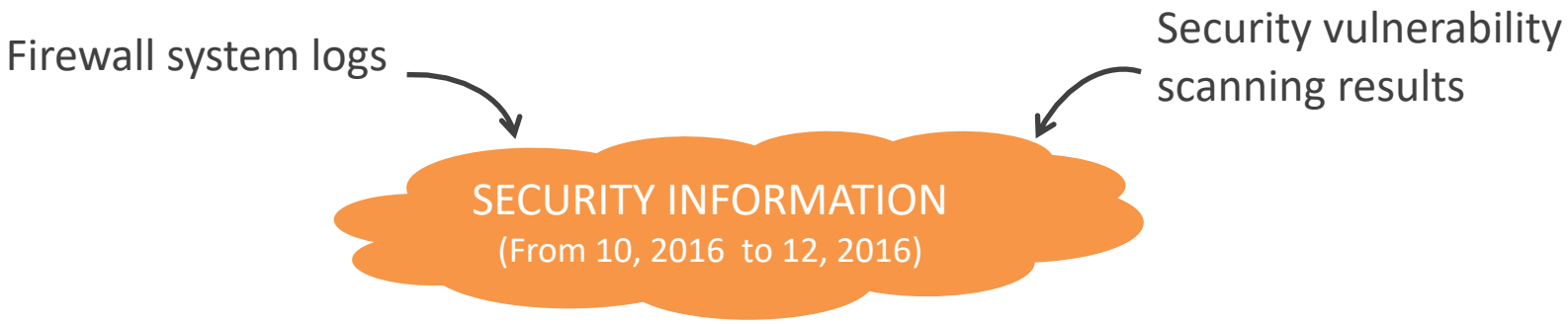
FLOW CHART OF SECURITY SITUATION CALCULATION



EXPERIMENT RESULT ANALYSIS

中国科学院 计算机网络信息中心 Computer Network Information Center, Chinese Academy of Sciences

Data Pre-treated	Data Processed	Data Stored
- Unifying security information - Filtering and merging the redundant data - Cutting out irrelevant attributes	- Processing data in accordance with 7 categories of security events	- Storing data - Fine-turning the parameters and comparing with the iterative results of the original present parameters

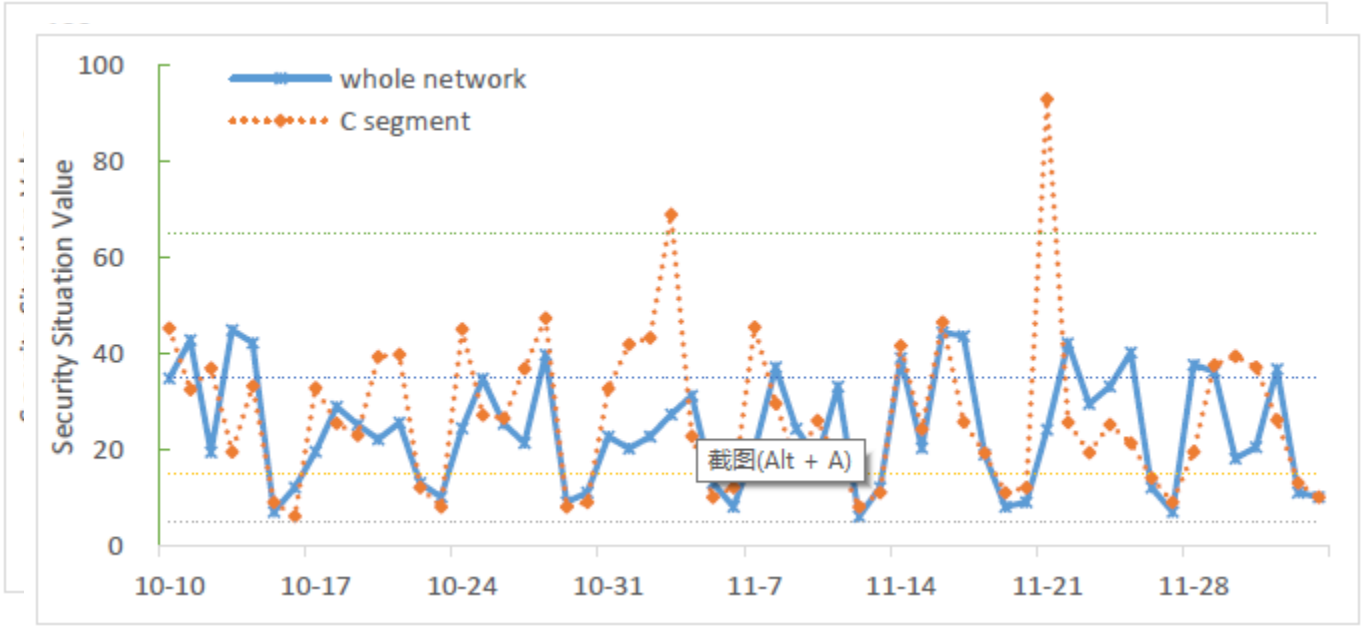


EXPERIMENT RESULT ANALYSIS

中国科学院
计算机网络信息中心
Computer Network Information Center,
Chinese Academy of Sciences

SECURITY SITUATION VALUE

- Calculating the security situation value of the whole network in a given period (from 10.10 to 11.28).
- Next, summarizing each day's security situation and normalizing it to 0-100 interval to get the daily security situation value.
- The security situation value is divided into 5 grades, which correspond to 5 security situation: Excellent, Good, Medium, Dangerous, Bad.



EXPERIMENT RESULT ANALYSIS

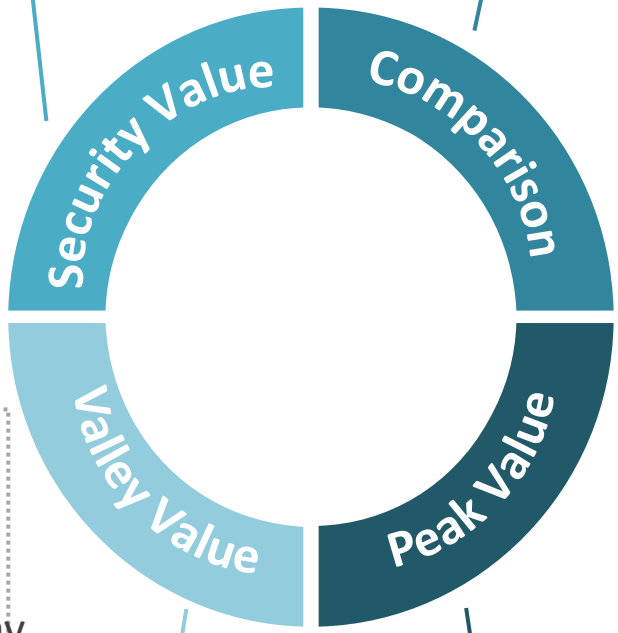
FURTHER ANALYSIS

Security situation value

Most of the whole network s and one of the address segments security situation value remain between 15-40.

Whole network & Address section

The whole network security situation curve is basically consistent with an address section. Therefore, the whole network security state in the security state.



Valley value analysis

- Periodic low situation values and same cycle
- Valley value appeared in time for two days (Saturday and Sunday)
- Basic security situation is “Good”

Peak value analysis

- Two peaks in the security situation of an address section
- Two security events are individual phenomenon
- The whole network overall security situation is stable

CONCLUSION

BENEFITS

- Comprehensive factors considered in the evaluation model
- The calculation result are relatively accurate and credible

FURTHER IMPROVEMENT

- Needs a lot of preparatory work because the security information from intrusion detection system, firewall system, vulnerability scanning system needs to be integrated and analyzed.
- Not real-time

Introduction of CSTCERT

4 Directions

Security Engineering

Related to the security construction, including projects, cloud computing security, mobile terminal security and penetration test.

Monitoring and Support

Daily security incident detection and handling, emergency response, security incident, special affairs, etc..

System operation and maintenance

Security system, equipment, hardware and software resources management.

Security Service

Security project service, security design, service support.

5 Abilities

Project Management

Resource Coordination and Communication

Security event handling

Security Protection

Thank you

Tel: 8610-58812935

Email：cert@cnic.cn