Identification Method of Attack Path Based on Immune Intrusion Detection

Huang Wenhua
School of Telecommunications and Information Engineering, Xi’an University of Posts and Telecommunications, Xi’an, China

Yishuang Geng
Center of Wireless Information Network Studies (CWINS), Worcester Polytechnic Institute, Worcester, MA, 01609, USA
Email: yugeng@wpi.edu

Abstract—This thesis takes researches on the immune intrusion detection and IP trace back technology. To find out the network data features of the real-time analyses, the distributed immune intrusion detection system and the packet marking theory are used; to guide the dynamically processing of path signs technology, the immune intrusion detection system is used; what’s more, to dynamically adaptive different methods of characteristics of network data, the path signs technology is adopted. After that, the attack paths can be quickly identified to provide path information for feature detector on attack path in the immune intrusion detection system. Experiment results show that this scheme can quickly reconstruct the attack path information, and the performance on the aspects of the convergence is with efficiency rate and false positive rate, which is superior to the current probabilistic packet marking algorithm and can provide characteristic path information for immune intrusion detection system.

Index Terms—IP Packet Marking; IP Trace Back; Adaptive Mechanism; Artificial Immune

I. INTRODUCTION

Computer network security technology is a multi-disciplinary, multi-disciplinary comprehensive discipline, including traditional firewall technology, access control technology, encryption technology, intrusion detection technology, IP trace back technology and so on [1]. Network security technology research includes dual nature, that is, offensive and defensive, in which the immune intrusion detection and IP trace back technology represent the technology of both ends of the network security technology. Although it is not ripe yet at this stage, as an important direction of development network security technology, it received sustained attention by experts and scholars. The thought of immune intrusion detection system derives from the recognition and treatment of the “non-self” material in biological immune system [2-4]; this system does not rely on a large number of signatures to determine whether invaded or not, but the characteristics of normal network flow are modeled; once the current network characteristics are not within the normal range, the system will consider that the potential attacks are discovered. So the immune intrusion detection system has a good dynamically adaptive capacity and high sensitivity for unknown attacks, and it is very suitable for the current changing network environment [5]. On the other hand, in order to find the perpetrators of cyber attacks and to punish them, and making the deterrent effect on the potential attackers, attack source tracing technology has steadily developed [6].

All along, the attack source tracing technology has always been researched as a stand-alone network security technology, but it is difficult to apply the results of their research. Among the reason, firstly, it is the flaw when the IP protocol is designed, because the current tracking technology just relies on changing the IP protocol, which is difficult to increase their effectiveness; secondly, it is the tracking strategy for relatively fixed algorithm adopted by tracing algorithm, and in order to improve this strategy, the artificial immune intrusion detection technology has been used as a typical anomaly-based intrusion detection system study since proposed in 1994 [7-9]. This technology does not rely on signatures, but has the ability to detect new, potential network attacks to protect the host against invasion. Since then, the American University of Memphis proposes a multi-agent detection system based on artificial immune intrusion, in which the intrusion detection system is no longer confined to the local host and the each agent can co-process to improve the robustness of the system, but there is a problem of not fully covered [10]. Gonzalez firstly proposed using the real value to represent the network data flow characteristics, in which the extracted features can be easy for people to understand and be easier to classify data [11]. In 2010, Dr. Jamie Twycross proposed the concept of second-generation artificial immune, which tries to combine the innate immunity and adaptive immunity and proposed the model to assess and test the immune algorithm, but the model is still difficult for practical application [12]. There are some problems of current immune intrusion detection system like inadequate autologous collection, overburdened local intrusion detection systems and so on, but it has a highly
sensitive for unknown new attacks, a rapid response capability for the known attacks, and a strong change characteristic to adapt the network characteristics, which has the application value [13-14].

Probability p; when the attacking the host sends a large number of attack packets to the victims host, the victim host can refractor the attack path through the receiving information on data packets [15-16], but the method presents the problem of the weakest chain [17], and the reconstruction requires a lot of data packets with a lot 2000 or so, Trace back technique began to receive the academic attention [18]. In the same year, Stone R. proposed a technology through the recursion method to trace back the attack source, but this technology needs to get a router management authority, and at the same time only able to launch the attack when attacking, which has application value. Then, Burch H. proposed a link test tracking strategy method based on denial of service, but this method itself is a huge burden to the network [19].

Thereafter, Bellovin proposed IP trace back technology based on ICMP protocol, which applies a new "iTrace Report" to trace back attack source, and through the router sending these messages to help the victim host identifying attack paths, but this method will make the overload router load, which affects its normal performance, and the ICMP report is easy to be filtered by the security policy [20]. The current researched IP trace back technology mainly focuses on the improvement of marking method to the probabilistic packet, which is proposed by the Savage. Routers are required to mark its own address information for each passing packet with a fixed efficiency high false alarm rate and poor immunity. Although the passive tracking algorithm represented by packets marking has been conducting improvement, there are various restrictions for used alone packet marking algorithm or improved packet marking algorithm due to the inherent flaws and fixed format of IP protocol, while the "iTrace" method based on ICMP protocol implementation provides a good idea, and the implementation based on router needs to be improved.

In general, all the existing intrusion detection systems focus on the discovery and prevention of attacks. Although most network-based attacks can be detected, all of them can not provide a real source tracking of attack. In order to avoid exposure the usual approach of the attacker firstly break a system, and then use it as a platform to use the approach of network jump (H () P) to attack another system. Because it is difficult to track the invasion, many cases are attacked after many jumps before reaching the real target. Additionally, currently tracing algorithm do not with dynamic adaptability. Packet marking algorithm is not based on packet characteristics, or the characteristic dynamic detection and tracking of data traffic, but always uses a fixed markup policy, which led to a large number of normal data packets are marked. On the other hand, when the host is tracing attacked it seems that the approach is inefficient.

In addition, the current tracing algorithm does not have the dynamic adaptability. Packet marking algorithm is not based on packet characteristics or the detection and tracking of dynamic characteristics of the data flow, but always adopts a fixed marking policy, which marks a lot of normal data packets, but inefficient when the attack host is tracing.

Innovations in this thesis:

(1) Many researches for immune intrusion detection and combined technology of IP trace back are studied. By using the distributed immune intrusion detection system and packet marking theory, network data features of the real-time analyses in immune intrusion detection system is used to guide the dynamically processing of path signs technology, and then the path signs technology can dynamically adaptive different methods of characteristics of network data.

(2) Through consulting the distributed processing ideas of IDRA and DDoS, combined with a distributed immune intrusion detection systems theory, this design implements of a path signs technology based on distributed open-immune intrusion detection system. Technology implementation relies on immune response server located in switched networks. On one hand, this server can make immune processing to the passing attack packets; on the other hand, it can make path marking to the suspected potential attacks, so the IP trace back algorithm is dynamic, adaptability and resources saving.

(3) Model and algorithm of attacking path signs based on distributed open-immune intrusion detection can further mark passing the data packet path to provide technical foundation for immune feature detector aimed at the single attack in the immune intrusion detection system. Thus this can deal with the attack packet in the attacking path and avoid the situation that victim host suffers the big attack packet and then refuses to serve. Experimental results show that the proposed scheme is better than the traditional tracking algorithms in convergence efficiency, false alarm rate and so on. Although supports of the immune response server are needed, the server is not located for the path signs, and its main function is an immune node to process the attack packets in switched network.

II. PROPOSED SCHEME

The combination of distributed immune intrusion detection system and IP trace back technology will place distributed open-immune response servers in the key path location in the switched network to serve the local immune intrusion detection system. On one hand, network data features of real-time analysis in immune intrusion detection system can be used to unfold the IP trace back algorithm, and then the algorithm has a dynamic adaptability, which can quickly find out the specific attack path. On the other hand, since the characteristics of a single attack in the shape-space are relatively continuous, just as shown in Figure 2-1, and the subsequent packets will be marked with a specific path signs, so that the immune intrusion detection system can attack data for a specific path selection method with a
positive culture to generate immunoassay device, and the path makes response to processing attack packets of the subsequent.

For the convenience of discussion and research of the algorithm and model, the prerequisites are as follows:
a. The data packet may be lost or out of order during transmission.
b. The data packets path of the same source hosts and the destination host are basically stable.
c. The attacker can generate any desired packets.
d. The router is credible, but limited resources.

The design of model and algorithm of the attack path signs based on distributed open-immune intrusion detection is mainly divided into the following three steps:
1) Modeling and building the overall framework to determine the location of the immune response server.
2) Determining the steps of the module and specific work.
3) Redefining IPv4 packet header and using packet to mark.
4) Designing algorithms in each module.

A. System Model and Module Design

Technical models building and core concept of the path sign based on immune intrusion detection system are locating the analysis of the immune intrusion detection system and response module into the transmission network, and after the real-time analysis of network data, the attack source trace back algorithm module are dynamically used according to the data characteristics of decision-making.

By referring to the “Distributed Intrusion Detection System and Distribution open intrusion detection and response framework” IDRA technology [12] and DDoS distributed processing thinking [13], an open track-type immune response server is located in the critical path in the transmission network (such as network border routers) shown in Figure 2-2: the server does not belong to a separate intrusion detection system, but can provide services for any immune intrusion detection system and work together; the server match the passing packets with the immune detector, which is used to determine whether the packet needs to respond, to treatment or trace back attack path, and then cooperate with the existing various routers to realize route signs; tracing algorithm is converged quickly and promptly traced to the desired position.

In addition, the set of this server can release a heavy relay on the route resources of previous various algorithms, which makes the router is only in collaborative work, rather than proactive, high loading trace back status, so the network status can be better guaranteed.

Attack source tracing algorithm based on immune Intrusion detection system can be divided into tracking / responding server algorithms, router algorithm and path reconstruction algorithm. The module design is shown in Figure 2-3:

Tracing algorithm only trace back unusual packet. Though to achieve synergies algorithm needed by routers is seemingly relatively complex, the vast majority of normal packets transmitting in the network will not be processed. Compared to other tracing algorithm it can reduce the load of routers and network, however, immune response server needs to have better performance, and can identify attacks path to provide the path packet information for the immune intrusion detection systems.
4) Downstream router identifies the packet itself should be labeled and records the IP into the two packets.
5) Victim host verifies the packets and reconstruct the path from the immune response server to its own point.
6) Victim host informs the immune response server that the reconstruction is completed, and accepts the attack marked and traced by the improved probabilistic packet out of the “control zone”.
7) Victim host informs immune response server among the reconstructed paths that the packets marked as F not be marked repeat.
8) Thereafter, the immune response servers mark all the packets through themselves and sending to the victim host as path marker F, so that the local immune intrusion detection system can generate the immune feature detectors for this path.
9) Immune intrusion detection system of the victim host distinguishes and marks packets as autologous (normal) or non-autologous (attack) data.
10) Immune intrusion detection system of the victim host generates the immune feature detector to non-autologous attack data through negative selection algorithm.
11) The generated attack immune feature detector is sent back to feature library of immune response server, and recognizes it in its life cycle and deals with the subsequent attack packets. After the life cycle of immune feature detector is over, it will be placed into the memory abnormality detector for detection to find the potential attacks.

Wherein, 1-8 steps are designed for the path signs algorithm based on immune intrusion detection system and they are the key points of this paper.

B. Algorithm Design

1) Immune Response Algorithm

The algorithm is used in the immune response module of immune response server. Algorithm uses the “memory” immune detector and “characteristic” immune detector in the immune nodes to compare with the passing packets, in where the “memory” immune detector is the further heritable variation of “characteristic” immune detector after its life cycle is over, while the “characteristic” immune detector comes from the training and submitting of the private immune intrusion detection system of attack host. Once the packet is matched with the “characteristic” immune detector, it considers that the packet belongs to attack behavior, which can be deleted; if it matched with the “memory” immune detector, it considers that the current packet is similar with the previous attack behavior, which belongs to the potential attack and can be traced.

Of course, in order to further improve the recognition abilities of the immune response nodes to the potential attack, “memory” detector can accept this immune response server via local data features to establish a long-term normal model, and after that via the “positive selection” algorithm to generate the “non-self” immune characteristics, which can be processed by the specific situations of the dealing performance of the immune response server and feature modeling. This thesis will not discuss further here.

Immune response algorithm is as follows:
Step1 Processing the next packet and controlling the packet in regional location
Step2 Extracting the features in the packet
Step3 Matching the features of the packet and immune features detector submitted in the immune intrusion detection system with the same destination IP, which successfully delete the packet and back to Step 1, otherwise the progress continues
Step4 Matching the characteristics of the packet and the set of the memory detector; if fail, back to Step 5, or to Step 7
Step5 Checking to find out whether exists the path sign F with the same destination IP; if exist, F will be marked into the path and be forwarded; if not, it will be directly forwarded.
Step6 Back to Step1
Step7 the packet information is recorded and then submitting it to the tracking module for processing path signs via controlling the tracking algorithm.
Step8. Back to Step1
2) Controlling Tracing Algorithm

The algorithm is used in the tracking module, which can be called by the immune response module. For safety, controllability and feasibility considerations, routers within the control area are not active sign address, but it will generate a particular packet for the cooperating of the downstream routers by the immune response server. It can be called as “path tracing packets”, and it is recognized and marked its address in turns by router. Since there are only 16-space in each “path tracing packets” any host to victim host, there are only 64 “path tracing data packets” are need for the immune response serve can carry address information, there are two packets for each route to mark itself address, and via the current monitoring of network packets it is learned that there are less than 32 routes in the path from. In order to enable the downstream router determining its own IP address to which the trace data packet marker, a contrast marker is needed in the tracing packet. Because there is no need for compared market after the IP is marked, the compared market and marked IP can share a head, that is, head marking segment. Controlling and tracking algorithm uses the TTL decrement feature to compare with the TTL via setting the marking segment TTL, which determines whether it need to be marked or not.

The specific algorithm is as follows:
Step1. Applying random path marker F to the immune intrusion detection system with the tracing destination IP address and submitting the abnormal packet information which second causes this tracing algorithm
Step2. Waiting for the path marker; if it is timeout or reject, it comes to the end; if it is successful, it will be continued
Step3. Generating 64 path tracing packets, in which one set of two, and in total there are 32 group; the TTL compared segment of two packets’ IP header in each set are the same, in which from top to bottom 32 groups are
decreasing from 33 to 1; the IP offsets of two packets in each set are different, in which one is for 0 and the other is for 1; the tracing marker of the all 64 packets is set as 1, in which the distance between segments set as 0; the part of data in the packet are loaded into the path marker F.

Step4. Sending the 64 packets to the destination IP

3) Router Collaborative Algorithm

Collaborative algorithm on downstream routers is based on the different state of the data packets makes different movements. Firstly, the routes determine the controlling zone bits. If the bit is equal to 0 (not considered the forgery case), the packet do not enter the control area and can’t control the tracing algorithm to track; in order to compensate the deficiency of the tracing algorithm in this segment (usually the first few jump in full path and no more than 5 jumps), the router with algorithm marked by the improved probabilistic packet marks the packets [14], and the tracing algorithm will be conducted when it is through by the first immune response server and can be sent to the victim host, thus the victim host will conduct the entire path.

Once the packet P are into the control area, collaborative routers judges P via tracking markers as a normal data packet or the tracing packet needed to be co-processed; when P is the tracking packet, compared the read TTL marked segment of the read P with the TTL of P, if it is different and its distance is not as 0, which indicates that the package has been marked by the upstream router, and it can be forwarded by adding 1 distance; otherwise, it will be directly forwarded.

When the read TTL marked segment of the read P and the TTL are the same, the router via IP offsets marks the first 16-bit or the last 16-bit of their own IP address into the compared field TTL, that is, the mark field. Since the IP is marked as the mark field, the meaning of the mark field changes from TTL comparison to IP marker. Meanwhile, the odd-even check of P mark the IP location via the filled markers. At this point, the router completes its coordination algorithms.

It is can be known from the above description that the value of the mark field is less than 32, and it should be as the comparing value of TTL value than the right; in order to prevent conflict, 10 hexadecimal value of the 16 random markers allocated by the victim host should be larger than 32.

Routers collaborative algorithm is as follows:

Step1. Dealing with the next data packet

Step2. If the packet control area bit is as 0, the packet is traced by the improved probabilistic packet marking algorithm and forwarded to Step 1; otherwise, the process is continuing.

Step3. If tracing mark bit of the packet is 0, the packet is forwarded; otherwise the process is continuing.

Step4. If the distance between the fields of the packet is not as 0, the distance between the fields will plus 1 and then the packet is forwarded; otherwise the progress is continuing.

Step5. If the compared field TTL of the packet is different with TTL, the packet is forwarded; otherwise the progress is continuing.

Step6. If the offset field of the IP in the packet is 0, the router mark its high 16-bit of into the marked IP field of the packet, and then the distance between the fields is set as 1 and the IP verifying field is filled in the verifying bit and be forwarded and then it is returned to Step 1.

Step7. Routers mark its low 16-bit of IP into the marked IP field of the packet, and the distance field is set as 1; the IP verifying field is filled in the verifying bit and be forwarded and then it is returned to Step 1.

After the victim host receiving 64 tracks packet, firstly it verifies if the random mark in the data field is sent by itself or not, quickly builds this path according to the contents of the packet and sends a confirmed report to the immune response server to inform that its tracking is complete.

When the immune response server receives the confirmed report, it is indicates that the controlling and tracking algorithm is complete. Thereafter, the immune response server can mark the generated path of the pass by probabilistic packet out of the controlling area and inform the victim host to conduct full path. More importantly, after that, the immune response server write the previous obtained 16-bit markers through the packet sending to the victim host, in which the victim host knows where these packets are derived from, so it is convenient to deal with or the specific immune detector is trained.

Since there is one or several immune response servers in a path, if all of them mark the random marker to the packet, it is only can be retained by the reserve closest to the victim host. In order to solve this problem, the victim host is needed to conduct a complete path tree according to the received packet locally; once several immune response servers are found in a path, the victim host sends packet to the middle of the servers and not repeats the futhest random markers. The method can effectively prevent the situation that all of the immune response servers don’t mark the packets in the path caused by forged random markers by the attacker, makes the longest path tracing and has a more obvious characteristic of marking packet. In addition, when a random marker is no longer used in a certain period of time, the victim host empties all the information of this marker, and re-allocates this marker out.

III. ALGORITHMS ANALYSIS AND EXPERIMENTS

A. Algorithm Analysis

In the current mainstream tracking algorithm, the performance and behavior of router cause various shortcomings of tracking algorithm, such as heavy refactoring packets, high false alarm rate and other issues. Since the router needs to forward a lot of data, it is not suitable for a large number of computing and storing and the router can only operate the header of the IP packet. All of these make all the routers address mark limited in the header; what’s more, marking a router address requires large amounts of data packet (header option is not practical). While the presence of The immune response server can solve or improve the above problem: based on this algorithm the normal packet will not be
In this paper, we propose a Senior PPM (PPMSenior) IP trace back algorithm based on the immune path marking scheme. The algorithm uses a probabilistic packet, which can be used for marking the path information carrier, but use "path tracing data packets" generated by the trace response server to forward the IP, which increases difficulties for the attacker to forge the path tracing information. The algorithm is used to mark the path and the immunity of the IP trace back algorithm will be theoretically analyzed based on the immune intrusion detection system as follows.

1) Convergence Experiments. The algorithm needs to satisfy the convergence both of the path tracing algorithm in "control area" and the path tracing algorithm out of "control area". In the "control area", the convergence begins when the algorithm sends the 64-th data packets. The trace back algorithm begins when the feature similarity between a packet with the normal packet is small, i.e., the affinity of a "autologous Detector" in the tracking response server is less than a given threshold. Out of the "control area", the improved marking algorithm of probabilistic packet is adopted, there is less than 5 hops between the attacker and the first boundary router hops, and then the probability can be marked as \( p = 1/5 \). For an attack path of 5 hops out of "control area", there are only a few dozen packets are required to conduct. On the other hand, the router out of the "control area" should belong to the unique ISP, and through log files recorded by the ISP, the packet sender can be easily found out.

2) False Alarm Rate. The unique random marker of a 16-bit is used in the algorithm to track the path from the tracking response server to the victim host, as long as there are less than 216-32 tracking response servers in the attack path, i.e. the 65504, the situation of false positives or false negatives will not exist. But once the hosts are suffered more than 65,504 tracking response servers' attacks, the victim host can't allocate the random markers to complete the trace, and then the situation of omissions is appeared. According to the practical attack experience, the attacking hosts are usually no more than a few hundred units even the DDOS attacks. The proposed program can completely avoid the appearance of false paths.

3) Immunity IP trace back algorithm based on immune intrusin detection does not use common data packet as the path information carrier, but use "path tracing data package" generated by the trace response server to forward the IP, which increases difficulties for the attacker to forge the path tracing information. The path marking algorithm based on the immune can mark the TTL value of the packet in the immune response host corresponding to the records of the victim host. Thus if the attacker want to interfere a path refactoring it should be satisfied that the "random identifier" and the corresponding "TTL hops" are the same with the records of the victim host. It is very difficult for an attacker, and the probability of successfully forge a "path tracing data packets" is about \( \frac{1}{2^{16} \times 2^{32}} \); even it is forged successful, the attacker is difficult to know. Therefore, anti-interference performance of this algorithm is really strong.

Through the using of simulations like NS-2, C-language and so on under Linux, the core parts of the algorithm are used to make experiment analysis, which will observe the algorithm’s performance of convergence time, false alarm rate and so on.

**B. Convergence Experiments**

In experiment 1 under the attack of a single path, the convergence time of the tracking algorithm is compared with different situation of the distance between the attack host and the victim host from 1 to 30. If the immune response server is located in the position of the five hops, the improved probabilistic packet out of the control area is adopted for tracking. The results are shown in Figure 4.

![Figure 4. Distance and convergence of attack path](image-url)

From the experimental results it can be seen that the existence of the immune response server can assist the system to mark the attack path; when the proposed marking algorithm of immune path are attacking, the convergence time is reduced to constant level compared to the other two algorithms; as long as the distance between the first immune response server in the attack path and the victim host does not exceeds 32 hops, the attack path can be quickly found. Although the convergence algorithm out of the control area is still using the marking improved program in probabilistic packet, it can be seen from the experimental results that the algorithm can converge quickly because of relatively small number of hops. The two kinds of marking schemes in probabilistic packet are in direct proportion of the number of hops on the convergence time; when the distance of the between the attack host victim and host is increased, the issue of weakest chain will stand out slowly; although the senior probabilistic packet is greatly improved on the convergence time compared to the marking scheme of basic probabilistic packet, it is really hard to apply in practice for it need to know the network topology.
C. Experimental of False Positives Rate

In experiment 2 there is a simulation on the false positive rate condition to three path marking algorithms in the multi attack paths. According to the actual attack situation, even if large-scale distributed denial services are attacking, the attack path is not more than 1000, so the experiment makes situation simulation within 1000 attack paths. The results are shown in Figure 5.

As can be seen from the experimental results, because there is no way to be taken against the problem of false positives, false positives situation based on PPM is very serious; when several attack paths are attacking, it is completely unable to reconstruct the attack path correctly. There is a great improvement of the advanced PPM on the aspect of false positives, but when the attack paths increase, the false alarm rate is rising rapidly. In the proposed immune-based path marking algorithm, because the immune response server is connected with the victim host and the marker of a unique path is determined, there is no false positives within the control area and false positive rate out of the control area is discussed according to different used methods. Low false positive rate makes the higher information entropy of the tracing path information. It has a reference value for the pertinence treatment of the subsequent immune intrusion detection system.

![Figure 5. Experiment on the false positive with several attack paths](image)

D. Experimental Conclusions

Through the above discussion and experiments it can be seen that the path marking technology based on immune intrusion detection has a better efficiency in searching the source of attack packets compared with other existing probabilistic packet parking. It can find out the source of the attack packets in a relatively fixed time, and the authenticity and credibility of the path information can be guaranteed; compared with the other two tracking algorithms it has more practical value.

IV. CONCLUSION

By reference to distributed processing ideas of IDRA and DDOS, combined with a distributed immune intrusion detection systems theory this thesis designs the path marking technology based on distributed open-immune intrusion detection system. The implementation of this technology relies on the located immune response server in switched networks. On the one hand, the server can make immune processing to the passing attack packets; on the other hand, it can launch path marking against the suspected potential attacks, and thus the making IP trace back algorithm has a dynamic and adaptability, which save resources. In addition, this path marking technology can further mark the passing packets to provide technological base for the immune intrusion detection system to generate immune feature detector after a single attack and to process attack packets in the attack path, which can avoid denial of service condition caused by the great regularity attack packet aggregation on victim host.

Experimental results show that the proposed scheme is superior to the traditional tracking algorithms on the aspects of convergence efficiency, false positive rate and so on. Although the immune response server is needed to support the processing, the server is not only located for the path marker, but for processing attack packets as an immune node in the switched network.

ACKNOWLEDGMENT


REFERENCES


Huang Wen-hua (1980.5-) female, Master degree, lecture. Her interests are in network security & information security, especially security evaluation.