Internet Early Warning Systems - Overview and Architecture

Sascha Bastke Mathias Deml Sebastian Schmidt

Institute for Internet-Security
University of Applied Sciences Gelsenkirchen
{bastke,deml,schmidt}@internet-sicherheit.de

December 15, 2009

Abstract

In the last two decades the Internet has become more and more important to our live and economy. Also the number of threats to the Internet is rising. Actual security systems that are used to protect the infrastructure are insufficient. For this reason Internet Early Warning Systems have gain a more and more important position in research. Such systems have a lot of aspects that must be bear in mind. These are technical and organisational aspects. In this work we give an overview of such aspects to define the term Internet Early Warning Systems in detail.

1 Introduction

In order to protect the critical infrastructure Internet, Internet Early Warning Systems have gain a more and more important position in the research area. The objective of these systems is the early detection of threats. Early means before a threat can cause any damage or before the threat cause the maximum damage. A second objective is Situation Awareness, these systems should generate a picture of the actual security situation which can serve as a help for decisions. These systems follow a global utilization, which protect not only one local network, but give an estimation of the whole situation with combination of different information from different local networks and give advice on how to prevent the threats.

To build an Internet Early Warning System many different aspects must be considered. These are not only technical aspects but also organisational and legal aspects. In the next paragraphs we try to identify such aspects and try to take conclusions about the realisation of such systems.

2 Related Work

Some work is done on Internet Early Warning Systems. Systems developed are introduced in [1], [3], [26] or [25]. The last two are based on honeypots. The first one gather statistical data from network traffic. The second one collect data

from different type of sensors, e.g. netflow. A system specialized in malware is shown in [30]. This work introduce a method for end-to-end worm containment by using a p2p network and automated filter generation. In [] a system for distributing security updates on an Internet wide level has been introduced. The authors use a overlay structure for this.

At lot of work was done that deals with single aspects of an Internet Early Warning System. Especially for the analysis of early warning times, e.g. modeling of malware propagation: [4], [5] and [6]. A model based on cellular automates theory is introduced in [7]. Publications that deal with the question of confining the spread of malware are [6] and [8]. Another work deals with the question how malware looks like in the future and what is the propagation speed [9].

Communication of botnets is analyzed in [10], [11], [12] and [13]. The publications [10] and [11] give a deeper insight into the efficiency and resiliency of botnets.

Attacks on BGP are introduced in [14]. An analysis of the behavior of BGP is carried out in [15] and [16]. Information to the propagation speed of packages in the Internet can be taken from [17], [18] and [19].

In the fields of detection and reaction to attacks their exists a lot of work. Most of this comes from the field of intrusion detection/prevention. A survey of anomaly detection can be found in [34]. Methods for anomaly detection can for example be found [31], [32] and [33]. Work on misuse detection is described in [35], [36] and [37]. Correlation methods were described in [38], [39] and [40].

Work on reaction to attacks are found in [41], [42], [43] and [44]. The first one introduce a cost-based model for Intrusion Response Systems. The second introduce a taxonomy for such systems. The use of machine learning to counter flooding attacks is described in [43]. A survey of methods to counter DoS and (D)Dos is given in [44].

3 Objectives of an Internet Early Warning System

The goal of an Internet Early Warning System is to protect and uphold the functionality of the Internet. This means to protect and uphold the systems that are part of this infrastructure or build this infrastructure. For this two aspects are relevant:

- The early detection of threats and the initiation of countermeasures.
- The improvement of the information infrastructure to deal with future requirements.

Based on this, one can identify the objectives of an Internet Early Warning System as to build a situation awareness and generate countermeasures to actual threats based in this situation awareness, so an early reaction is possible. A second objective is the collection and analysis of information, so that an assessment of future developments will be possible.

4 Definition of Early Warning

A definition for early warning in the area of natural catastrophe is following:

Early warning is the warning of a menacing natural phenomenon which occurs so early that the potentially concerned persons have the possibility to react so that personal injury can be avoided or reduced. ([24])

Basically this definition can also be transferred to the area of early warning in the Internet. But normally there is no personal damage in terms of injuries of the people.

The word "early" in early warning can have many different meanings. To explain this in more detail, we define an attack as a sequence of preparative actions v_i to the attack and the attack actions a_j itself (equation 1). The preparative actions for the attack can be for example scanning or password cracking.

$$A = \langle v_1, v_2, \cdots, v_n, a_1, a_2, \cdots, a_m \rangle \tag{1}$$

Based on this definition we define the different types of early warning as following:

Type 1: before the start of an attack Such a warning can only be generated in two cases. In one case, one or more preparative actions (v_i) are detected. Then a warning can be generated before the sequence of attack actions begin. In the second case, an attack is detected at a hop between origin of the attack and target of the attack. In this case there is a chance to warn the target before the attack reaches the target. The attack can be identified both in the preparative steps (v_i) and the attack steps itself (a_i).

Type 2: with beginning of/during the attack The attack has already begun, one or several steps a_i were already executed, but the attack has not finished yet, so the attack either doesn't cause any damage until this point or has not yet reached the maximal potential damage. The detection can take place at the attacked system or a hop on the way.

Type 3: before a possible threat Under this category, situations are summarized that can lead to a concrete problem but that must not be the case. Here are two different situations. The first situation deals with propagation phenomena. This can be e.g., the propagation of a malware using an HTTP-server security gap. As long as the security gap in own system is not patched and the local protection system such as Intrusion Detection System (IDS) and virus scanners are not updated, there exists the danger that own system can be a victim. But this must not be the case if the malware never tries to infect the own system or doesn't try until an effective protection is installed. This is similar for SPAM or Phishing attempts. There is potential threat, which doesn't lead directly to an attack and maybe it never come to an attack at all. However, the danger exists basically. In this situation a warning is provided for threat that need some time to spread globally. At the time of warning, a number of potential victims can already be affected and the main goal of the warning is to warn the rest of the not affected victims.

The second situation is about security gaps which are discovered, but are not yet used by an attacker. These can be discovered for example by

reviewing the code of a manufacturer. In this situation all affected ones can be warned early theoretically.

5 Threat Scenarios

An important questions is what kind of thread scenarios must be considered by an Internet Early Warning System? For this work different threat scenarios were analysed. To decide what is a important scenario is relatively hard and we need a definition of the critical infrastructure. A communication-technically oriented definition would draw the line at the routers and wires, i.e. the infrastructure which is required for transport of network packages. The question is here, however, whether such a definition is purposeful. It can be argued that DNS is an important protection-worth component of the infrastructure, because without DNS a reasonable use of the Internet is not possible. The same can be stated for the email service or for HTTP, because these services are used by a lot of people. So a threat is then relevant when it causes a great damage in terms of cost to the infrastructure.

But based on this the decision if a threat scenario is relevant or not is not easy. For this we give an example: A (D)DoS-attack that affects the global Internet traffic by his strength can be stated as relevant. What is, however, with a single exploit attempt which can lead, at the end, to a DoS on a target system? The things become much more complicated now. It is absolutely not relevant if only a simple workstation is crashed, but what when the system is an important server, e.g. a DNS root server? At this moment this scenario becomes relevant to the Internet Early Warning System. It is also relevant when the same exploit is used on thousands of systems. At this moment you can't ignore the event because it can bring the Internet into a state where it is not usable anymore. Based on these considerations following scenarios were investigated: (D)DoS, exploits, malware spreading, botnets, Routing.

5.1 (D)DoS

First consider a DoS scenario. Assume an attacker performs an SYN-flood on a target. This leads to a rise of the number of network packets with set TCP-SYN flag on the routes to the target and at the target. When we use threshold based attack detection, we will get an alarm after a threshold value is reached. This means with a certain packet a threshold is exceeded. Let T_{total} be the overall time for a packet on his way from source to destination. This time is the sum of the transmission times between the hops t_{trans} and the processing times on the hops t_{proc}. See equation 2.

$$T_{total} = \sum_{i=1}^{N} (t_{trans,i} + t_{proc,i}) \tag{2}$$

The early warning time T_{EW} is the difference between the overall time T_{total} and the transmission time to the hop where the attack was detected (T_D). See equation 3. We assume here that the detections on the hop and on the target of the attack are similar, so there is no difference caused by different detection methods or parameters.

$$
\begin{aligned}
T_{EW} = T_{total} - T_D &= \sum_{i=1}^{N}(t_{trans,i} + t_{proc,i}) - \sum_{i=1}^{D}(t_{trans,i} + t_{proc,i}) \\
&= \sum_{i=D+1}^{N}(t_{trans,i} + t_{proc,i})
\end{aligned}
\tag{3}
$$

The data from [19] shows the latency between different tier one providers. From this the latency can be assumed to be less than 100 ms. From measurements with a system called InternetVerfügbarkeitsSystem ([2]) we know that the round trip time to different servers in the Internet is also under 100 ms in average. Based on these data we can expect only a few seconds as early warning time in the best case. As the warning is delivered over the same network we can not expect to generate an early warning that reaches the victim in an appropriate time. This means there is no advantage compared to detection at the victim. In principle the same can be applied to (D)DoS-Attacks.

5.2 Exploits

Exploits use security gaps in software to crash a system (DoS) or to get the access to the system. For example this can be done by provoking a buffer overflow. Such exploits are used by malware to spread over the Internet, so that they are relevant for Internet Early Warning Systems. There are two different approaches to analyze this scenario:

- To protect from an concrete attack (early warning of type 1 or 2)
- General determination of the threat level of exploits (early warning of type 3)

The first approach is similar to the (D)DoS scenario. The exploit consists of one or more network packages that will be exchanged between attacker and victim. A hop on the way can detect the exploit with help of a signature and can send a warning to the destination. If we assume a one packet exploit we will get the same early warning time which is shown in equation 3 section 5.1.

Because of the fast transmission of packets in the Internet (see section 5.1), there is no significant speed up in reaction time compared to a local security system. This means there is no advantage in using an Internet Early Warning System. An early warning of type 1 is not possible.

The second approach is to warn not from a concrete attack, but from a potential threat. In this case the Internet Early Warning System determines information which exploits are currently used and try to identify new exploits which are unknown so far (Zero-Day-exploits). Such information can be e.g gathered by honeypots. Based on these information warnings can be given and be used to create countermeasures. Because of the fact that not all vulnerable systems will be attacked at the same time we are able to give an early warning (type 3) and to generate an effective protection against the exploit. An example is the spreading of a malware. The time we have for early warning strongly depends on the kind of threat. It can be minutes up to hours. Whether an early warning is really possible depends on the situation.

5.3 Malware Spreading

There are many publications to the modeling of the propagation of autonomous spreading malware, examples are [4], [5] and [6]. Most of them use an epidemic propagation model which is also used for the modeling of spreading of biological viruses. These models are called SIR-Models. He spreading is than described by an exponential spreading curve.

By an infection the question is how many time is still there for the reaction before it has only a minor effect, i.e. since when should a reaction begin so that it is still effective and since when the reaction is just a limitation to the damage. In [6] and [8] this aspect is investigated. The results there show that a reaction has to begin very early during the spreading process. The earlier the countermeasures are seized, the less the malware spread.

This results show that the reaction should begin before the outbreak reaches the exponential part of the curve. If this happens there is no chance to have a significant impact on the spreading. The possible early warning time depends basically on the worm. After [21] code red has reached his biggest spread within 14 hours. An reaction within the first 5 hours would make sense . Another example is the Witty worm. This has infected all potential hosts within 45 minutes. The worm SQL-Slammer was even quicker and needs only 15 minutes to infect all potential hosts ([22]). In [9] it is analyzed how fast a worm can theoretically spread. The article comes to the result that propagation is possible within 15 minutes even if with bigger potential populations. This means we have only a very short time span for reaction. In the best case there are several hours available. However, at least a warning can be provided in both case which corresponds to an early warning of type 3.

5.4 Botnets

Botnets are one of the biggest threats in the Internet. Using it, the potential victims can be scanned, an attack can started, SPAM can be sent and other harmful activities can be done. By the mass of the computers on such networks (several Thousand to Hundred Thousand or even Millions) the threat potential is very high.

In the past botnets owned a central aligned structure with one or several Command and Control servers (C & C) that control the botnet. These had a very simple structure but were very vulnerable to attacks against their C & C servers. Switching off the C & C server, switches off the botnet. Meanwhile the number of botnets that are organized decentralized is increasing. These are based on P2P technologies. An example of such a botnet is the StormWorm botnet [13]. These are not so easy to switch off because it is not enough to switch of a few nodes. An analysis of this aspect for decentralized botnets is given in [10] or [11]. The result shows that it is very hart to switch off a decentralized botnet. One of the best methods is to stop it during the creation phase but this is also very difficult. However, this alone is not enough, more effort must be done to detect and disinfect the infected systems.

Instead of switching off the botnets, man can also try to sniff their communication to get information of the threats which go out currently from them. Based on this information warnings could be generated and countermeasures be developed.

How fast botnets commands can be distributed inside botnet, this specifies the reaction time for countermeasures. In [10] this question is investigated for different botnet structures. The authors come to the result that propagation within a few minutes is possible, e.g. 6 minutes for a botnet with million nodes and 1 MB commands. With more worse assumptions the authors ([11]) think a time of approximately an hour is realistic. This is the time to reach every zombie in the botnet. But this is not necessary for the successful realization, e.g. (D)DoS attack. For this kind of attack, potentially fewer hosts are needed than the number of hosts in the botnet, which means the time for early warning becomes shorter.

Again in this scenario an effective early warning of the type 1 is difficult. However, with slow communicating botnets, it is possible.

5.5 Routing

The routing infrastructure builds the basis for a well working Internet. Core of this infrastructure is the BGP protocol. There are a series of attacks to this protocol. [14] gives an overview for it. A part of these attacks are targeted at a single router and the goal is to switch off this router by exploits. This has only limited influence on the whole routing infrastructure. More interesting are the attacks that try to redirect data by influencing the routing data.

Let's assume that an attacker give wrong routing information to a router. An analysis how long a route announcement need to spread in the routing infrastructure is introduced as a part of [15] and [16]. Based on it, a convergence time of few minutes can be assumed. In more than 90 % of the cases a convergence is reached after approximately 2 minutes. A deletion of a route needs longer, approximately 180 seconds.

A concrete example of such a scenario is the incident from the 24.02.2008 which is described in [20]. Pakistani Telekom has a new Prefix announced for ip addresses that belong to YouTube. Within a few minutes (approx. 2 minutes) this prefix had been distributed in a big part of the routing system and the requests to YouTube have been directed to Pakistani Telekom. This problem could be solved by a suitable reaction.

The early warning time is in this scenario also very short. By the quick propagation of routing information only few minutes left for the reaction. Therefore a direct warning before the threat and also the reaction is very difficult.

5.6 Summary

From the analysis above we cans see that an distributed sensor system have only limited use in countering an concrete attack (early warning of type 1 or 2). We can get some useful information from it but for early warning of this types the period of time from detection to hitting the target of the attack is to short. So the main objective of an Internet Early Warning System should be to detect new threats, so it can generate early warnings of type 3. This does not mean that no components needed to detect concrete attacks, it only means that such components are not very helpful located somewhere outside the target of an attack.

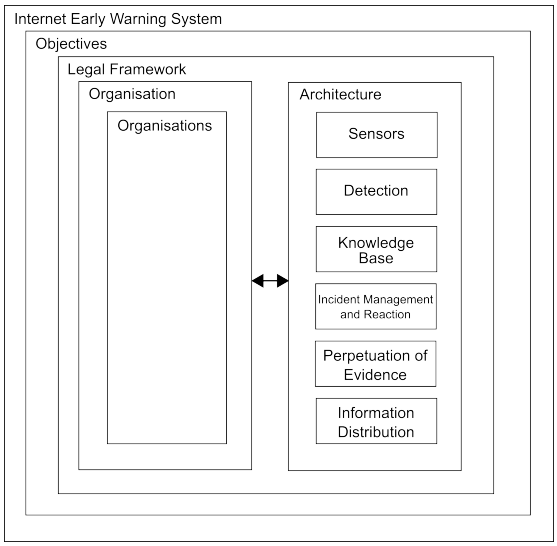

Figure 1: Building blocks of an Internet Early Warning System.

6 Definition of the Term Internet Early Warning System

Abstract an Internet Early Warning System can be defined as a six tuple of the form:

$$F = (N, P, O, L, G, C)$$

$$\begin{aligned} N &:= \text{Network, that would be monitored.} \\ P &:= \text{Organisations, that are part of the early warning system.} \\ O &:= \text{Definition of the organisational structures and processes necessary to run a early warning system.} \\ L &:= \text{Legal framework, necessary for the operation of an Internet Early Warning System.} \\ G &:= \text{Objectives, that should be achieved by an Internet Early Warning System.} \\ C &:= \text{Technical components of an Internet Early Warning System.} \end{aligned} \tag{4}$$

Figure 1 shows this components and their relations. They will be described in more detail in the next paragraphs.

6.1 Network (N)

This element describes the monitored network. In case of an Internet Early Warning System the Internet. The knowledge of the underlying network is used to place the sensors and helps to estimate the propagation of faults. But its not

only important for technical aspects it have also influence on the organisational, legal and architectural aspects of an Internet Early Warning System.

The Internet is composed by autonomous systems that are managed by different organisations. This is important because that means there is no global control over the Internet. The building blocks of the Internet are managed locally and underlie different legal frameworks. This shows that a centralized approach for an Internet Early Warning System for the whole Internet is not suitable. Most of the decisions are better made at the local organisation based on the environmental conditions.

6.2 Organisations (P)

The component P is the set of organisations / people involved in the early warning system. Involved stand here for actively involved or passively involved. Active partners are involved in the construction and operation of the Internet Early Warning System, e.g. as operator of sensors or by the initiation of countermeasures.

The group of the active partners must suitably chosen. An unfavorable composition of this group reduces the effectiveness of the early warning system. It is important to get all the information needed for early warning.

Under the term passive partners fall everybody which do not help actively in the operation of the Internet Early Warning System, but profiting from the information which the Internet Early Warning System generates. These can be different institutions or people. Examples are manufacturers of anti-virus software who can provide new signatures for worms or administrators which can improve the security of their networks. It is important to find suitable communication channels. They must be fast and resilient enough.

6.3 Organisation (O)

The component O describes the organisation of an Internet Early Warning System. The organisation can be divided in the organisational structure and the operational structure. The organisational structure defines the organizational units of the Internet Early Warning System and their relations to each other. The operational structure defines the processes that are necessary for the operation of an Internet Early Warning System, e.g., the kind of information must be defined that are sent to the situation center or it must be defined how to react to different threat situations. Important for the organisation are:

- Short decision making process
- Efficient information distribution
- Clearly defined responsibilities

By this requirement a strictly hierarchically built up organisation with many levels are not well suited. Rather it is necessary that the organisations communicate directly with each other. In some cases it might be necessary to coordinate the reaction on a global level. This can be necessary in case of an (D)DoS that affects a big part of the infrastructure. But most of the time its more important to distribute information as quickly as possible and trigger a local reaction. This

has different reasons as, e.g. different policies for handling incidents, different system architectures or different laws.

6.4 Legal framework (L)

This aspect deals with the question to what extent the existing laws support the operation of an early warning system. Different aspects of law are touched, e.g. data protection or contract law.

7 Technical Components (C)

From a technical point of view an Internet Early Warning System consists of a bunch of components. These components are Sensors, Detection, Knowledge Base, Incident Management and Reaction, Perpetuation of evidence, Information distribution.

7.1 Sensors

The sensors of an Internet Early Warning System are needed to:

- To generate an overview of the actual situation, this means to generate a situation awareness.
- To identify new threats, e.g. new malware spreading over the Internet.
- To identify concrete attacks actual running.

The sensors needed for an Internet Early Warning Systems are of different types. Most important are sensors that identify new threats. Most important an Internet Early Warning System need to use honeypots and honeyclients to identify malware and new exploits. As the analysis above shows it can also be helpful to monitor botnet traffic. This can be a chance to react before a attack starts. For this one method is to be part of a botnet by using modified bot code. Also sensors that monitor the routing and naming infrastructure are needed. But it must be stated that a reaction is difficult because of the short time spans. A Internet Early Warning System should also generate information on SPAM and Phishing. This can be done automated or by the input of Internet users (swarm intelligence).

The detection of concrete attacks on a network intrusion detection systems like snort can be used. For detection of (D)DoS attacks it needs to use sensors that give information about the amount of traffic in the Internet. This can be a system like the one described in [1] or other systems.

7.2 Detection Component

Core of an early warning system is the detection of threats. In general this component can be divided in two layers, the signal layer and the event layer. This is shown in figure 2.

On the signal layer data from network or log data is analysed by anomaly and misuse detection methods and generates events. For this a knowledge base is used which includes models for normal behavior or signatures for threats.

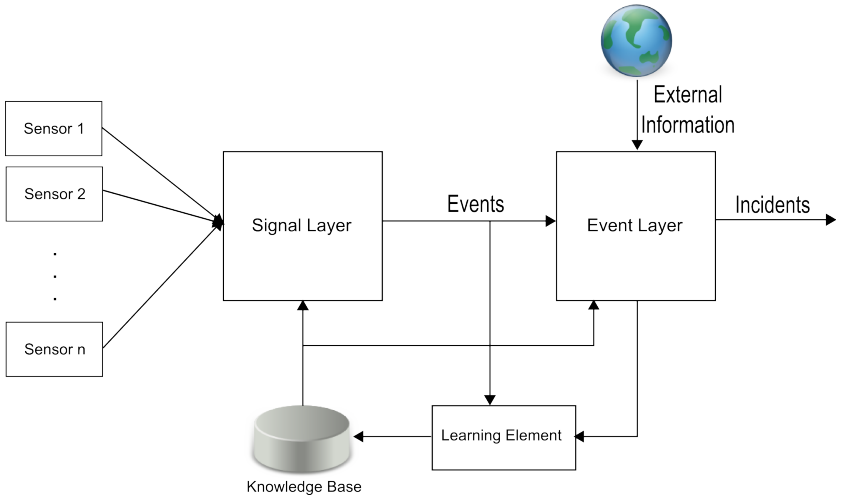

Figure 2: Detection component.

This layer only use technical information sources that monitor the network infrastructure. The knowledge base must be updated on a regular basis to capture changes in network behaviour and new threats. Methods for detection for example introduced in [31], [32] and [33].

On the event layer tries to correlate the events from the signal level and information from external sources like CERTs or other security systems, e.g. Intrusion Detection Systems. The information from external sources may be also events but can also be other information like the information that a new exploit is used by malware. Methods for event correlation are for example introduced in [38], [39] and [40].

Another task of this component is the prediction of incidents. This means based on events detected by the signal layer the most probable incident should be predicted and which kind of events will happen next.

7.3 Knowledge Base

The knowledge base include knowledge to different aspects of an Internet Early Warning System. In detail this includes knowledge of normal behaviour and signatures for threats, knowledge about incidents, knowledge about countermeasures to incidents, knowledge about environmental conditions (technical aspects, organisation aspects, legal aspects, ...).

The knowledge must be updated on a regular basis because of new threats, changes in network infrastructure and behaviour, improvement of countermeasures and changes in the environmental conditions.

7.4 Incident Management and Reaction

This is a kind of an expert system that support the users by the processing of incidents. It is connected to the knowledge base and supports the user in its decision process by suggesting steps for further analysis to decide what kind

of incident the actual situation is and what kind of countermeasures should be used.

In the best cases countermeasures should be initiated automatically based on information collected locally and information from the outside, because of the short early warning times. The countermeasure component must generate the best countermeasure based on the incident information and the environmental conditions. The problem is to decide what is the best countermeasure. A metric must be defined that helps to decide this question. In some cases it can be the best decision to do nothing and wait until a better countermeasure can be used. This is the case when the countermeasure produces a higher cost than the damage caused by the threat would do. Because it is very hard to decide what countermeasure to use, a human interaction is required to authorize the chosen countermeasure.

In some cases it may be necessary to initiate coordinated countermeasures. This means countermeasures that are initiated not by one but by many users of the Internet Early Warning System. This can be useful for example in cases of (D)DoS.

7.5 Perpetuation of Evidence

In the case of the recognition of an attack this component is used for the perpetuation of evidence which can be used in the criminal proceedings. The objective is to collect data that allows to take evidence that an attack happened and who has started the attack.

The access to these data must be limited and may occur only in reasonable cases. The application of cryptographic procedures is necessary here. These protect the data against unauthorized access. In the easiest case the data can be the complete recording of the network traffic or data from log files.

7.6 Information Distribution

This component is needed to distribute information to the users of the Internet Early Warning System. The information can be of different kind, e.g. warnings/alerts, countermeasures, description about threats, information about SPAM and Phishing sites.

The distribution system must be fast and resilient. An import end question is how to deal with the injection of wrong information. This leads to the assumption that information distributed in the system must be verified.

8 Architecture of an Internet Early Warning System

A big question is how to combine the different components in one system. Based on the analysis of threats and conditions above we propose a distributed architecture. The reasons for this are:

- Different policies at the local system for incident handling and initiation of countermeasures

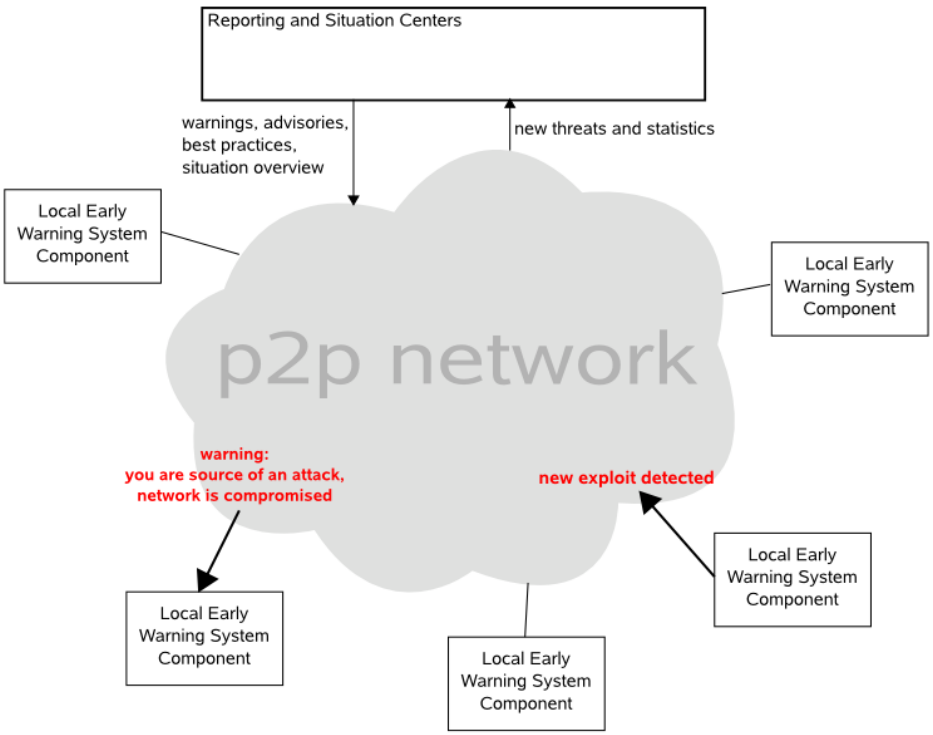

Figure 3: General structure of an Internet Early Warning System.

- Different environmental conditions, so that not every countermeasure can applied to every network
- Fast distribution of threats
- In future more use of cryptography, so that deep packet inspection is only usable at the target systems of the traffic
- Different legal conditions at different countries

Core of the system are strong local security systems that are connected by an efficient information sharing network. Over this network the local system share information about threats and countermeasures. An situation center is part of this network and can generate statistical information and help in coordinating countermeasures. This structure is shown in figure 3.

For the information sharing network we propose the use of a p2p network. This is because we need a fast and resilient possibility to share information. P2P networks have been shown to fulfill this requirements. An example is the analysis in [10], that show how efficient and resilient different botnet structures are. Another example is shown in [30] that uses a p2p network for worm containment.

The local security components consists of the other components mentioned in section 7. At the local system the different kind of sensors will be operated. The information of this sensors will be analysed by the detection component to

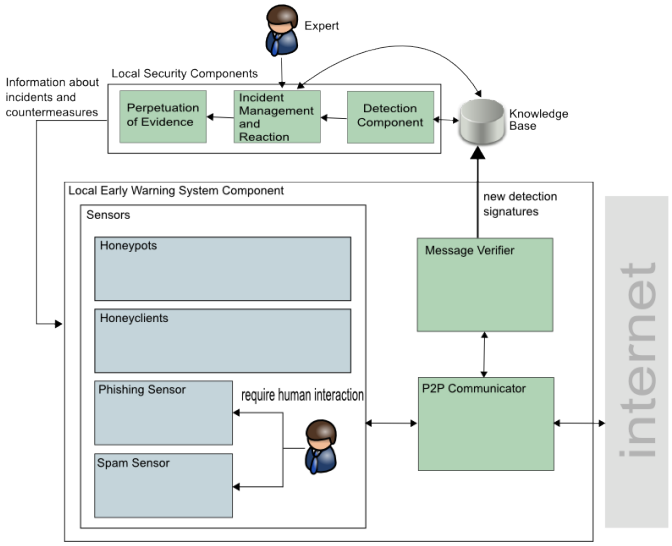

Figure 4: Architecture of the local Internet Early Warning System components.

detect attacks on the local system and new threats that can be interesting for other users of the Internet Early Warning System. For this not only the information of the local sensors are used but also the information distributed by the information sharing network and the information of the knowledge base component. The Incident management and reaction component than try to initiate countermeasures and can decide to give information to other partners of the Internet Early Warning System. In the best case this works automatic but we believe that a human interaction is necessary. For this to work a connection to the information sharing network is needed that can receive and verify messages from the network and send messages over the network. In the local security system also the component for perpetuation of evidence is located. This structure is shown in figure 4.

9 Conclusion

In this work we have defined the term Internet Early Warning System and analyzed what kind of early warning is possible. We concluded that an early warning of type 1 is not possible. The network packages are sent too fast through the network, so that there is no significant speed up compared to the warning directly generated by a local security system. In principle, this argument is also valid for identify the attack at the preparative steps.

It seems more reasonable to use the early warning type 3. This means the detection of threats that propagate through the Internet, such as malware, SPAM or something similar. A certain time span is available for early warning because of the propagation character of the threats. The above analysis shows that only a few scenarios are of this kind but it shows also that even in this cases the early warning time is sometimes very short, see section 5.5 or 5.4.

This leads to the second conclusion. Most of the detection and countermeasures to attacks must be initiated at the local systems that are target of the attacks. This is not only because of the short period of tome for reaction but also because of the different law situations depending on the location of the targeted system and different policies in administration of the systems. The Internet Early Warning System can only give helpful information to generate such countermeasures. As we see from the analysis an Internet Early Warning System in most cases can provide additional information, which can be used to analyze the actual situation and can also help to make decisions on countermeasures. Therefore another important character of an Internet Early Warning System is the aspect of situation awareness. This can help to judge the actual situation and make decisions.

From this we can conclude that a key component of an Internet Early Warning System is an efficient information sharing network. This network must be able to distribute information very fast to a high number of clients. It also must be resilient in case of attacks or damages to components of this network. A good structure to achieve this goals can be a p2p structure as it is used in actual botnets or for example in [30] for worm containment.

Another key component must be installed at the client that get information from the local network. This is a strong local security component that does the work at the local systems. This component must be able to generate countermeasures automatically based on the data from the Internet Early Warning System and on the environmental conditions.

This implies that a Internet Early Warning Systems is in a big part an information sharing network and only the local components are like intrusion detection system. It only distribute information as fast as possible to help the clients to protect their systems. The reaction must than be generated at the local systems. This leads to another observation. A situation center is only a client of this network that collects the data to give an overview what actual happens and helps in the analysis and reaction. In some cases a situation center can try to coordinate countermeasures, e.g. in case of massive (D)DoS attacks but in most cases it collects statistics and give hints about countermeasures back into a network. It does not have special position in such a network compared to the other clients.

For this kind of Internet Early Warning System further research is necessary. One must answer the question what kind of sensors and how many of them are needed. What kind of network structure is best used for information sharing, how many clients such a network has to service, what kind of information should distributed and how we can secure such a network. Also there must be some kind of normalization on the information shared.

References

[1] Pohlmann, N., Proest, M.:Internet Early Warning System: The Global View. ISSE 2006 Securing Electronic Business Process, Vieweg, 2006

[2] Pohlmann, N., Hommelsbach, K., Bastke, S.: Messen und Warnen, ¡kes¿ Die Fachzeitschrift für InformationsSicherheit, Augabe 5, 2008

[3] Sander, J., Jedlicka, H.-P.: Carmentis - Frühe Warnung im deutschen Internet -. 14. DFN-CERT Workshop, 2007

[4] Liljenstam, M., Yuan, Y., Premore, B.J., Nicol, D.: A mixed abstraction level simulation model of large-scale Internet worm infestations. Modeling, Analysis and Simulation of Computer and Telecommunications Systems, 2002

[5] Zou, C., Gong, W., Towsley, D.: Code Red Worm Propagation Modeling and Analysis. IEEE, 2003

[6] Yiran Gu, Yurong Song, Guoping Jiang, Suoping Wang: A New Susceptible-Infected Model of Malware Propagation in the Internet. Proceedings of the 9th International Conference for Young Computer Scientists, ICYCS 2008, Zhang Jia Jie, Hunan, China, November 18-21, 2008

[7] Yurong Song, Guo-Ping Jiang, Yiran Gu: Modeling Malware Propagation in Complex Networks Based on Cellular Automata. IEEE, 2008

[8] Wen-Jie Bai, Tao Zhou, Bing-Hong Wang: Immunization of susceptible-infected model on scale-free networks. Physica A: Statistical Mechanics and its Applications, 2007

[9] Staniford, Stuart, Paxson, Vern, Weaver, Nicholas: How to Own the Internet in Your Spare Time. Proceedings of the 11th USENIX Security Symposium, 2002

[10] Li, Jun and Ehrenkranz, Toby and Kuenning, Geoff and Reiher, Peter: Simulation and Analysis on the Resiliency and Efficiency of Malnets. PADS '05: Proceedings of the 19th Workshop on Principles of Advanced and Distributed Simulation, 2005

[11] Reiher, P., Li, J., and Kuenning, G. Midgard Worms: Sudden Nasty Surprises from a Large Resilient Zombie Army. Tech. Rep. CSD-TR040019, University of Oregon, 2006

[12] Dave Dittrich, Sven Dietrich: P2P as botnet command and control: a deeper insight, 3rd International Conference on Malicious and Unwanted Software (Malware), 2008

[13] Ruitenbeek, Elizabeth Van, Sanders, William H.: Modeling Peer-to-Peer Botnets. QEST '08: Proceedings of the 2008 Fifth International Conference on Quantitative Evaluation of Systems, IEEE Computer Society, 2008

[14] Toni Farley, Patrick Mcdaniel, Kevin Butler: A Survey of BGP Security Issues and Solutions. AT&T Labs - Research, Florham Park, NJ, 2004

[15] Labovitz, Craig, Ahuja, Abha, Bose, Abhijit, Jahanian, Farnam: Delayed Internet routing convergence, IEEE/ACM Trans. Netw., IEEE Press, 2001

[16] Mao, Z. Morley, Bush, Randy, Griffin, Timothy G., Roughan, Matthew: BGP beacons. IMC '03: Proceedings of the 3rd ACM SIGCOMM conference on Internet measurement, ACM, 2003

[17] Aiguo Fei, Guangyu Pei, Roy Liu, Lixia Zhang: Measurements On Delay And Hop-Count Of The Internet. in IEEE GLOBECOM'98 - Internet Mini-Conference, 1998

[18] Edoardo Biagioni, Peter Hinely, Chun Liu, Xinmin Wang: Internet Size Measurements, 2000, Available at http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.24.9061

[19] The Internet Health Report. Available at http://www.internetpulse.net

[20] YouTube Hijacking: A RIPE NCC RIS case study, RIPE NCC News & Announcements, February 2008, Available at http://www.ripe.net/news/study-youtube-hijacking.html

[21] The Spread of the CodeRed Worm (CRv2). November 2008, Available at http://www.caida.org/research/security/codered/coderedv2_analysis.xml

[22] The Spread of the Witty Worm. November 2008, Available at http://www.caida.org/research/security/witty/

[23] Provos, Niels: A virtual honeypot framework, SSYM'04: Proceedings of the 13th conference on USENIX Security Symposium, USENIX Association, 2004

[24] Frühwarnung bei Naturkatastrophen. Wikipedia - Die freie Enzyklopädie, Januar 2009, Available at http://de.wikipedia.org/wiki/Frühwarnung_bei_Naturkatastrophen

[25] Engelberth,M., Freiling, F., Göbel, J., Gorecki, C., Holz, T. Willems, C.: Frühe Warnung durch Beobachten und Verfolgen von bösartiger Software im deutschen Internet: Das Internet-Malware-Analyse-System (InMAS). Procceding of the 11. Deutscher IT-Sicherheitskongress, SecuMedia, 2009

[26] E. Markatos and K. Anagnostakis: NoAH: A European Network of Affined Honeypots for Cyber-Attack Tracking and Alerting. The Parliament Magazine, Issue 262, 3 Mar 2008

[27] Moore, D., Shannon, C.: The Spread of the CodeRed Worm (CRv2). Available at http://www.caida.org/research/security/code-red/coderedv2_analysis.xml

[28] AV-Test release latest results. Available at http://www.virusbtn.com/news/2008/09_02

[29] Update Frequency of Anti-Virus Software. Available at http://www.av-test.org/index.php?menue=7&lang=0

[30] Costa, Manuel and Crowcroft, Jon and Castro, Miguel and Rowstron, Antony and Zhou, Lidong and Zhang, Lintao and Barham, Paul: Vigilante: End-to-end containment of Internet worm epidemics. ACM Trans. Comput. Syst., ACM, 2004

[31] Marina Thottan and Chuanyi Ji: Anomaly Detection in IP Networks. IEEE Transaction on Signal Processing, 2003

[32] Bastke, Sascha and Deml, Mathias and Schmidt, Sebastian: Combining statistical network data, probabilistic neural networks and the computational power of GPUs for anomaly detection in computer networks. Workshop Intelligent Security (SecArt 2009), 2009.

[33] Morteza Amini and Rasool Jalili: Network-Based Intrusion Detection Using Unsupervised Adaptive Resonance Theory (ART). Proceedings of the 4th Conference on Engineering of Intelligent Systems (EIS 2004), 2004.

[34] Chandola, Varun and Banerjee, Arindam and Kumar, Vipin: Anomaly detection: A survey. ACM Comput. Surv., ACM, 2009.

[35] Tylman, Wojciech: Misuse-Based Intrusion Detection Using Bayesian Networks. DEPCOS-RELCOMEX '08: Proceedings of the 2008 Third International Conference on Dependability of Computer Systems DepCoS-RELCOMEX, IEEE Computer Society, 2008.

[36] Yang, Yahui and Huang, Chunfang and Qin, Zhijing: A Network Misuse Detection Mechanism Based on Traffic Log. NSWCTC '09: Proceedings of the 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing, IEEE Computer Society, 2009.

[37] Mosqueira-Rey, Eduardo and Alonso-Betanzos, Amparo and Río, Belen Baldonedo and Pi neiro, Jesús Lago: A Misuse Detection Agent for Intrusion Detection in a Multi-agent Architecture, KES-AMSTA '07: Proceedings of the 1st KES International Symposium on Agent and Multi-Agent Systems, Springer-Verlag, 2007.

[38] Krügel, Christopher and Toth, Thomas and Kerer, Clemens: Decentralized Event Correlation for Intrusion Detection. ICISC '01: Proceedings of the 4th International Conference Seoul on Information Security and Cryptology, Springer-Verlag, 2002.

[39] Aboelela, Emad and Douligeris, Christos: Fuzzy Temporal Reasoning Model for Event Correlation in Network Management. LCN '99: Proceedings of the 24th Annual IEEE Conference on Local Computer Networks, IEEE Computer Society, 1999.

[40] Holub, Viliam and Parsons, Trevor and O'Sullivan, Patrick and Murphy, John: Run-time correlation engine for system monitoring and testing, ICAC-INDST '09: Proceedings of the 6th international conference industry session on Autonomic computing and communications industry session, ACM, 2009.

[41] Stakhanova, Natalia and Basu, Samik and Wong, Johnny: A Cost-Sensitive Model for Preemptive Intrusion Response Systems. AINA '07: Proceedings of the 21st International Conference on Advanced Networking and Applications, IEEE Computer Society, 2007.

[42] Stakhanova, Natalia and Basu, Samik and Wong, Johnny: A taxonomy of intrusion response systems. Int. J. Inf. Comput. Secur., Inderscience Publishers, 2007.

[43] Berral, Josep L. and Poggi, Nicolas and Alonso, Javier and Gavaldà, Ricard and Torres, Jordi and Parashar, Manish: Adaptive distributed mechanism against flooding network attacks based on machine learning. AISec '08: Proceedings of the 1st ACM workshop on Workshop on AISec, ACM, 2008.

[44] Peng, Tao and Leckie, Christopher and Ramamohanarao, Kotagiri: Survey of network-based defense mechanisms countering the DoS and DDoS problems. ACM Comput. Surv., ACM, 2007.

[45] Li, Jun and Popek, Gerald J. and Reiher, Peter: Disseminating Security Updates at Internet Scale. Kluwer Academic Publishers, 2002.