DAI-Labor
TU Berlin

Karsten Bsufka, Olaf Kroll-Peters, Sahin Albayrak:

Intelligent Network-Based Early Warning Systems

Zuerst erschienen in:

Proc. Of Critical Information Infrasturctures Security First International Workshop, CRITICS 2006, Samos Island, Greece, August 31 - September 1, 2006. Lecture Notes in Computer Science (LNCS) 4347. Editor Javier Lopez. 2006. Springer

http://dx.doi.org/10.1007/11962977_9

DAI-Labor, Technische Universität Berlin
Fakultät IV für Elektrotechnik und Informatik
www.dai-labor.de

Intelligent Network-Based Early Warning Systems*

Karsten Bsufka, Olaf Kroll-Peters, and Sahin Albayrak

Technische Universität Berlin, DAI-Labor
(karsten.bsufka|olaf.kroll-peters|sahin.albayrak)@dai-labor.de

Abstract. In this paper we present an approach for an agent-based early warning system (A-EWS) for critical infrastructures. In our approach we combine existing security infrastructures, e.g. firewalls or intrusion detection systems, with new detection approaches to create a global view and to determine the current threat state.

Key words: critical infrastructures, early warning system, multi agent systems, intrusion detection

1 Introduction

Modern societies depend heavily on certain infrastructures, which are critical for existence and smooth operation of society. Examples for these critical infrastructures are:

- Transportation and traffic
- Telecommunications and information technology
- Finance and insurance services
- Supplies
  - Health care
  - Emergency services
  - Water supply
  - Energy supply
- Public administration and legal system [2]

With the dawning information age these infrastructures lose the independent character. The main reason for this loss of independence lies within the emergence of information technology infrastructures and the Internet.

Every critical infrastructure is based on its underlying networks. These separate networks are connected by Internet provider networks, see Figure 1.

Figure 1 is similar to a figure presented in [5], which shows how *bounded* networks reside within an *unbounded* domain. Generally speaking bounded networks are under single administrative control and adhere to known security policies.

* J. Lopez (Ed.): CRITIS 2006, LNCS 4347, pp. 103 – 111, 2006. http://dx.doi.org/10.1007/11962977_9

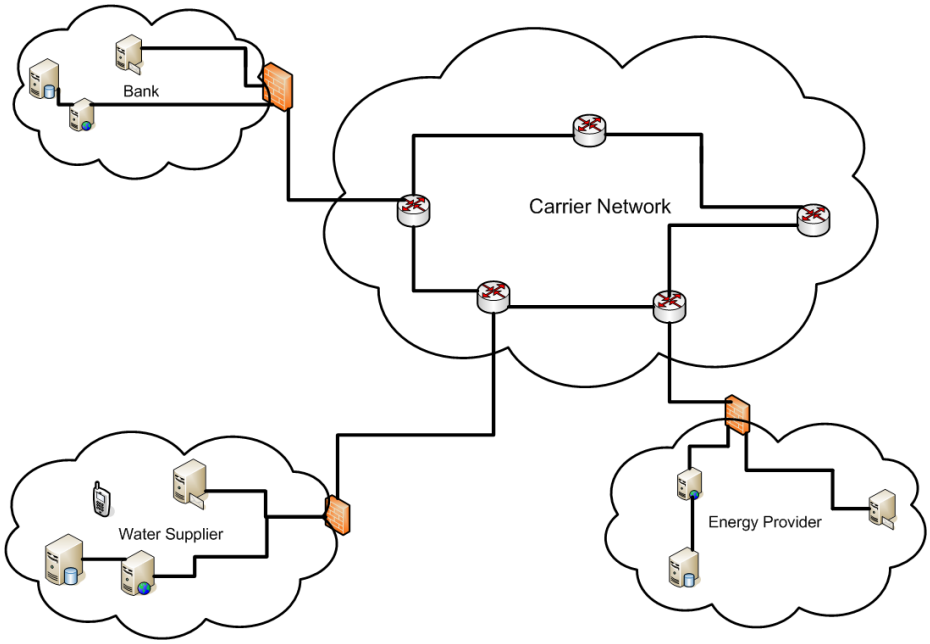

Fig. 1. Overview of CRITIS networks

Unbounded networks on the other hand are under different administrative controls and there is no global visibility of the network. As a consequence, problems occurring within one critical infrastructure, e.g. power failures caused by natural disasters or attacks are carried out against transport systems, will not be communicated to other critical infrastructures.

We propose an early warning system for critical infrastructures, which helps to relay information about threatened critical infrastructures. Before we go into details about our proposed agent-based early warning system for critical infrastructures, we first describe some potential scenarios for a breakdown of critical infrastructures, the role of IT systems and the potential effects in these situations.

2 Breakdown Scenarios For Critical Infrastructures

There are several potential causes for a breakdown or limited availability of a critical infrastructure. Obvious causes would be attacks (cyber or physical) or natural disasters, other reasons may include (labor) strikes, erroneous use or technical failures of IT systems or other systems. A detailed discussion of critical infrastructures can be found in [9].

The threats to critical infrastructures can be classified into the following different categories.

– Financial threats
– Material threats
– Immaterial threats
– Threats of living
– Social threats

We chose the following scenarios as examples for the effect on IT systems. First, we describe the dependence of other critical infrastructures from the telecommunication systems. Subsequently, we will describe possible threat scenarios for the chosen infrastructures.

2.1 Financial Payment Systems

Nowadays, financial transactions without IT support are unthinkable. IT systems are the foundation for processing global business (e.g. stock market transactions) and private business such as online banking or online tax declaration. IT systems are a fundamental infrastructure in this field.

Attackers can have different motivations for attacking a financial payment system. Foremost there is the possibility of gaining monetary benefits for themselves by attacking the infrastructure. For example, a potential attacker could transfer rounding errors from stock transactions to his own account.

2.2 Electric Power Systems

In contrast to financial payment systems, an electric power system is more susceptible to natural disasters and attacks, which try to damage the physical part of the infrastructure. As an example for natural disasters serves the winter of 2005/2006, where parts of Germany were without any electric power, because extremely cold temperatures caused power lines to collapse.

Electronic devices are employed in most activities of everyday life. In case of power failure all energy-dependent processes cease to function. Therefore power supply is also considered to be a basic infrastructure. Power failure will also cause the breakdown of other critical infrastructures, a general power failure for example would also cause the traffic systems to fail.

The effects of a power failure can be reduced by back-up systems, but they will only provide a reduced amount of electric power.

2.3 IT and Telecommunications

IT and Telecommunication infrastructure can be indirectly targeted by attacking the underlying electric power systems, but they also can be attacked directly. In both cases this will affect other critical infrastructures that use or are built upon an attacked IT or telecommunication infrastructure.

Control devices and communication in all other critical infrastructures require an underlying operational telecommunication network. In case of an attack, this infrastructure can be utilized to take preventive measures, issue an alert or initiate a responsive action.

For instance, if an attacker plans to reduce the market value of a company, he could spread falsified rumors about the company. Another possibility would be to cut off the access for customers to the e-business portal.

2.4 Common Themes In Attacks

All the aforementioned critical infrastructures exhibit the following characteristics: they require a running IT infrastructure, energy and they are all distributed systems. All fields require electric power for operation consequently a running power infrastructure. They also need a running IT infrastructure to deliver results, to be controlled and coordinated. Distributed sensors, which include the fields of IT and power supply, have to be employed to control and protect the systems. Therefore we describe an approach which is distributed as well.

3 Agent-based Early Warning System

Currently, operators of a critical infrastructures are on their own when dealing with attacks or natural disasters. This may work as long as a problem, natural disaster or cyber attack, affects only his infrastructure. Generally, critical infrastructures are interconnected. It certainly would enhance the survivability of critical infrastructures if early warnings of approaching problems could be issued, received and exchanged.

We propose an agent-based early warning system (A-EWS) for this task, see Figure 2 for high-level overview.

The general architecture depicted in Figure 2 is similar to the architecture presented in [12], but our proposed systems does not focus on networks alone, but also on hosts.

Currently, our research focuses solely on detecting cyber attacks, and we will describe the A-EWS in this context. Yet, we believe our approach can be extended to cover natural disasters and technical failures as well. We are aware that an A-EWS raises a lot of privacy and policy issues for the co-operation between different entities. We decided to focus our research on the technical aspects and to use the results of the technical solutions to identify specific privacy and policy requirements. These requirements will then be used for a revised A-EWS version.

The foundation of an A-EWS is its capability to detect attacks as early as possible. Known attacks can be detected by IDS, firewalls and anti-virus software. In general, these applications inform users or system administrators about detected events. Sometimes they do even less and store the knowledge about occurring attacks in log files.

An A-EWS will not help the current victim of an attack. If information concerning detected attacks is spread beyond the border of a single local network, it can help others in preparing for an attack. If, for example, anti-virus software attached to e-mail servers detects several e-mails with an attached viruses, it currently only cleans the e-mails. If it would also propagate the information

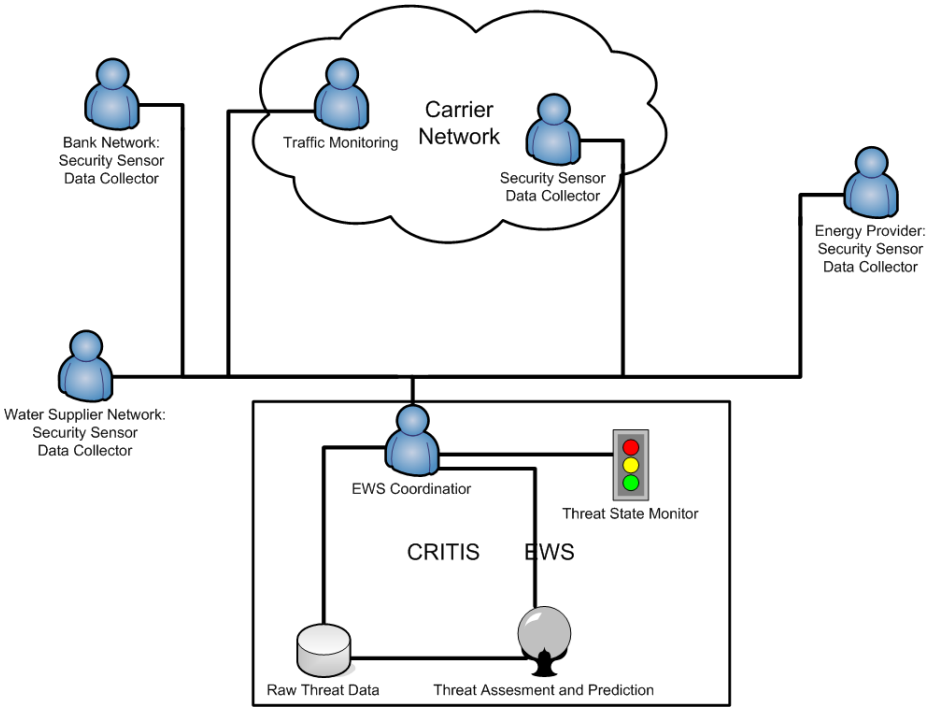

Fig. 2. Proposed agent-based EWS

about the virus attacks to other e-mail servers, they could start updating the anti-virus softwares signature database ahead of time.

To this end, one type of sensor in an A-EWS should be a wrapper for current security products capable of interpreting and reporting the detection results in a common attack ontology. Another kind of sensor would use honey pots or honey nets as a sensor [8]. Sensors will be represented by agents that share common ontologies and use services for interaction with the A-EWS.

Our research focus is on three other types of sensors:

- Anomaly Sensors,
- Network Traffic Sensors and
- Attack Pattern Sensors.

3.1 Anomaly Sensors

In our work anomaly sensors are used to observe the behavior of hosts. Although the basic ideas and concepts could also be used to realize network traffic anomaly sensors, we are currently do not investigate that direction. For detecting anomalies we use two different approaches.

One approach uses unsupervised learning (Self Organizing Map — SOM) algorithms to learn the "normal" behavior of hosts [1]. Here we measure a selected

set of features on host systems. For this approach to work well, the behavior of hosts should not be too erratic. It will be much more complicated to detect anomalies on PCs, used by students in a PC pool, than observing a PC used by a single secretary. The other approach is a host-based artificial immune systems (AIS). Both approaches work on the same set of observed features and can simultaneously observe the same host. Supervisor agents are capable or correlating observation results for one host produced by the AIS and SOM components. To reach a certain belief of the current threat state of a host, these agents also consider their beliefs and the known measurements results from neighboring hosts.

In general, the supervisor agents will act as the anomaly sensors for a critical infrastructure. Depending on the current global threat state or the local threat state, it should also be possible to propagate all anomaly sensor events to the global A-EWS system.

3.2 Network Traffic Sensors

Anomaly sensors can only report attacks, which have reached or breached a target system. Furthermore, the impact on the (global) threat state is very low for small numbers of breached systems. Unfortunately, it is be more or less to be expected, that a small number of systems will be infected.

It would make more sense to detect ongoing attacks before they fully reach their targets. A field of application for this is the network level. Here it is possible to detect threats during transmission and react to them. A carrier network, that connects critical infrastructures, would be very suitable. Networks for a specific critical infrastructure would be less suitable but still acceptable.

There are two types of network traffic sensors. One simply observes the traffic flow and could be used to detect denial-of-service attacks. The other type analyzes the traffic content, trying to identify known malware signatures. Currently our researches focuses on the latter.

The realization of network traffic sensors faces technical and social challenges. When the traffic content is analyzed, privacy considerations have to be taken into account. Current privacy laws prevent the use of network traffic sensors for analyzing traffic content in some countries. Legislators must weigh the gain in critical infrastructure survivability and security against the loss of privacy. Technically there are two main problems to address. In large networks it is infeasible to analyze traffic at every possible server and router. This means a method for identifying the minimum number of observation points and their locations must be found. The question of a minimum number of observation points is closely related to the second challenge, which deals with performance issues. Network traffic sensors must be capable of handling a huge amount of traffic in relatively short time frames. The amount of traffic and the time-frame of traffic analysis depends not only on technically issues, but also on the security and survivability goals for a critical infrastructure.

3.3 Attack Pattern Sensors

Sophisticated attacks contain a sequence of steps, where each step produces some sort of effects. Attack pattern sensors know a formal description of attack steps or effects [10]. An example for the former is an IP fragmentation attack on an IDS [11], were the order and properties of the IP fragments can be described; an example for the latter would be the installation (modifies the file system) and execution of a Trojan horse (increases the number of running processes and opens new network connections) by exploiting different bugs in e-mails and/or web browsers. These two very short examples also illustrate the fact that attack pattern sensors either can be deployed to monitor hosts or to monitor network traffic.

3.4 Sensor placement and cooperation

When selecting a location where a sensor is to be placed, its detection abilities must be taken into account. If a sensor agent is responsible for interpreting firewall log files, it should be attached to a firewall. It is not necessary to place network traffic sensor agents on every node in the network. They only need to be placed on nodes, which add additional information to their knowledge about the current network traffic flow. We are currently working with game–theoretic approaches for determining the optimal placement of sensors in a network.

One defining aspect of placement algorithms is whether sensors need communicate with other sensors. In general, our sensors do not need to cooperate directly with each other, they only need to report relevant events to coordinator or collector agents. We plan to build this A-EWS up on the JIAC framework [6]. JIAC is a Java-based environment for developing agent-based applications. It already offers yellow–page, security and communication services, which allow the discovery of other agents and the secure communication between agents. In order to build an early warning system with JIAC, the global EWS part will be connected to trusted remote platforms (at least one per connected critical infrastructure IT system), which will in turn host sensors in specific critical infrastructure IT systems. The concept of trusted remote platforms for JIAC, was introduced in the security target [4] for Common Criteria evaluation of JIAC [7, 3].

3.5 Countermeasures

Anomaly sensors, network traffic sensors and attack pattern sensors are used by A-EWS to detect ongoing attacks. The simplest reaction to detected attacks is to inform human operators about it, e.g. by sending e-mails to a threat state monitoring tool.

We envision that an A-EWS also contains a prediction unit, capable of making educated guesses about the future development of the attack. These guesses will be used to send warnings and advices to administrators, prepare alternative transport mechanisms for important messages, e.g. converting e-mails to

SMS messages if normal e-mail transport is not possible, or disconnect hosts or sub-networks.

4 Conclusions and Future Work

In order to enhance the survivability of IT systems for critical infrastructures. It is important to detect failures and attacks as early as possible. To this end, we propose an agent-based early warning systems, that on one hand builds upon already existing security products and on the other hand uses new agent-based sensors for hosts and networks.

Currently our work is conducted in an industry endorsed research project, which focuses on the development of the described agent-based sensors and the sensor placement. We envision the described A-EWS as an application and extension of our current work. An especially interesting research aspect, will be the correlation of anomaly detection results, with events from security appliances. At the moment we are only working on different correlation strategies between anomaly sensors.

Acknowledgments

The authors wish to thank Katja Luther, Danie Christelle Mouapi Tientcheu, Rainer Bye, Christian Scheel, Stephan Schmidt, Tuvshintur Tserendorj, Robert Wetzker, Volker Eckert, Sebastian Linkiewicz, Thorsten Rimkus, Aubrey-Derrick Schmidt and Tansu Alpcan for supporting them during the creation of this paper and the productive work on the malware filtering project funded by the Deutsche Telekom AG.

References

1. Sahin Albayrak, Achim Müller, Christian Scheel, and Dragan Milosevic. Combining Self-Organizing Map Algorithms for Robust and Scalable Intrusion Detection. In M. Mohammadian, editor, *Proceedings of InternationaInternational Conference on Computational Intelligence for Modelling Control and Automation (CIMCA 2005 Book 2)*, pages 123–130, Vienna, Austria, 2005.
2. Bundesamt für Sicherheit in der Informationstechnik. Critical infrastructures in state and society. `http://www.bsi.de/fachthem/kritis/kritis_e.htm` (2006-05-16).
3. Bundesamt für Sicherheit in der Informationstechnik. Certification Report BSI-DSZ-CC-0248-2005 for Java Intelligent Agent Componentware IV Version 4.3.11 from DAI- Labor Technische Universität Berlin. `http://www.bsi.de/zertifiz/zert/reporte/0248a.pdf`, 2005.
4. DAI-Labor. Security Target Java Intelligent Agent Componentware IV. `http://www.bsi.de/zertifiz/zert/reporte/0248b.pdf`, 2004.
5. R.J. Ellison, D.A. Fisher, R.C. Linger, H.F. Lipson, T. Longstaff, and N.R. Mead. Survivable Network Systems: An Emerging Discipline. Technical Report

CMU/SEI-97-TR-013 ESC-97-013, Software Engineering Institute, Software Engineering Institute. Carnegie Mellon University. Pittsburg, PA 15213 USA, November 1997.

6. Stefan Fricke, Karsten Bsufka, Jan Keiser, Torge Schmidt, Ralf Sesseler, and Sahin Albayrak. Agent-based telematic services and telecom applications. *Communications of the ACM*, 44(4):43–48, April 2001.
7. Tim Geissler and Olaf Kroll-Peters. Applying Security Standards to Multi Agent Systems. In *The First International Workshop on Safety and Security in Multiagent Systems (SASEMAS) Part of AAMAS held at Columbia University New York City, 20 July 2004*, July 2004.
8. Cristine Hoepers, Klaus Steding-Jessen, Luiz E. R. Cordeiro, and Marcelo H. P. C. Chaves. A National Early Warning Capability Based on a Network of Distributed Honeypots. In *Proceedings of the 17th Annual FIRST Conference on Computer Security Incident Handling*, Singapore, June 2005.
9. John C. Knight, Matthew C. Elder, James Flinn, and Patrick Marx. Analysis of Four Critical Infrastructure Applications. Technical Report Computer Science Report No. CS-97-27, Department of Computer Science, University of Virginia, September 1998.
10. I. Kotenko. Active vulnerability assessment of computer networks by simulation of complex remote attacks. In *International Conference on Computer Networks and Mobile Computing, 2003. ICCNMC 2003*, pages 40–47, October 2003.
11. Antonio Merola. Intrusion Detection Systems-Interna. *hakin9*, (4), 2005. `http://www.hakin9.org`.
12. C. Zou, L. Gao, W. Gong, and D. Towsley. Monitoring and early warning for internet worms. In *Proceedings of the 10th ACM conference on Computer and communication security, ACM Press (2003)*, pages 190–199, 2003.