Network Attack Detection and Defense

Dagstuhl Perspective Workshop 08102, March 02-06, 2008

Executive Summary

From March 2nd to 6th, 2008, the Dagstuhl Perspective Workshop 08102 *Network Attack Detection and Defense* was held at the International Conference and Research Center (IBFI), Schloss Dagstuhl. The objective of the workshop was to work out a manifesto that identifies past shortcomings and future directions for the field. During the workshop, several participants presented their perspective on the development of the area. Furthermore, ongoing work and on open problems were discussed. Six working groups were formed to discuss the state of the art and the challenges of future research directions. The *Executive Summary* describes the workshop topics and goals in general, and gives an overview of its course. Abstracts of the presentations given during the workshop, the outcomes of the working groups, and the manifesto are put together in the online proceedings.

1. Motivation

The increasing dependence of human society on information technology (IT) systems requires appropriate measures to cope with their misuse. The growing potential of threats, which make these systems more and more vulnerable, is caused by the complexity of the technologies themselves and by the growing number of individuals which are able to abuse the systems. Subversive insiders, hackers, and terrorists get better and better opportunities for attacks. In industrial countries this concerns both numerous companies and the critical infrastructures, e.g. the health care system, the traffic system, power supply, trade (in particular e-commerce), or the military protection.

In today's Internet there is a ubiquitous threat of attacks for each user. Most well-known examples are denial of service attacks and spam mails. However, the range of threats to the Internet and its users has become meanwhile much broader. It ranges from worm attacks via the infiltration of malware till sophisticated intrusions into dedicated computer systems. The Internet itself provides the means to automate attack execution and to make them more and more sophisticated. The protection against these threats and the mitigation of their effects has become a crucial issue for the use of the Internet. Complementary to preventive security measures, reactive approaches are increasingly applied to counter these threats. Reactive approaches allow detecting

Dagstuhl Seminar Proceedings 08102
Perspectives Workshop: Network Attack Detection and Defense
http://drops.dagstuhl.de/opus/volltexte/2008/1492

ongoing attacks and to trigger responses and counter measures to prevent further damage.

Reactive measures comprise beside the classical virus scanner intrusion detection and flow analysis. The development of intrusion detection systems began already in the eighties. Intrusion detection systems possess a prime importance as reactive measures. They pursue two complementary approaches: anomaly detection, which aims at the exposure of abnormal user behavior, and misuse detection, which focuses on the detection of attacks in audit trails described by patterns of known security violations. A wide range of commercial intrusion detection products has been offered meanwhile; especially for misuse detection. The deployment of the intrusion detection technology still evokes a lot of unsolved problems. These concern among others the still high false positive rate in practical use, the scalability of the supervised domains, and explanatory power of anomaly-based intrusion indications. In recent years intrusion detection has received a wider research interest which increased the efficiency of the technology, in particular in connection with other approaches e.g. firewalling, honeypots, intrusion prevention.

In recent years network monitoring and flow analysis has been developed as complementary approach for the detection of network attacks. Flow analysis aims at the detection of network anomalies based on traffic measurements. Their importance arose with the increasing appearance of denial of service attacks and worm evasions which are less efficient to detect with intrusion detection systems. The flow analysis community developed two approaches for high speed data collection: flow monitoring and packet sampling. Flow monitoring aims to collect statistical information about specific portions of the overall network traffic, e.g. information about end-to-end transport layer connections. On the other hand, packet sampling reduces the traffic using explicit filters or statistical sampling algorithms.

There is an urgent need to coordinate the research activities in intrusion detection and network monitoring. For example, sampling and flow monitoring have been developed as important methods in the network monitoring field (for accounting, charging, and security). They are more and more applied for attack detection (anomaly detection, flow based signatures). This, however, requires a close cooperation of the two communities. The same applies to the intrusion detection community for the detection of worm epidemics and denial of service attacks. Here traffic analysis can help to make the detection procedure more effective. This objective makes the subject of the seminar to be rather cross-disciplinary.

2. Goals and Content of the Workshop

The object of the workshop was to discuss future challenges in reactive security, in particular in intrusion detection and network monitoring. New challenges arise as the functionality of network monitoring, attack detection and mitigation must be suitable for a large variety of attacks, and has to be scalable for high data rates and numbers of flows. Event correlation techniques can be used to combine results from both worlds. The workshop was the first one devoted to this topic in Dagstuhl. A particular objective of this event was to bring together the both communities of intrusion detection and network monitoring which still do their research relatively separated and are organized in different communities (e.g. WGs SIDAR and KUVS in the German Society of Informatics (GI) for reactive security and communication systems, respectively).

Thus we saw the Dagstuhl workshop as providing a forum where researchers of both communities (intrusion detection, network monitoring) could discuss common problems and coordinate their activities to benefit from research on related problems in the other area. Hence for the Dagstuhl workshop, we felt that there would be valuable interactions and contributions that would be facilitated by bringing people together in both areas.

The main objective of the workshop was to work out a manifesto that identifies past shortcomings and future directions for the field. For this, six working groups were formed to discuss the state of the art and the challenges of future research directions. The outcomes of the working groups as well as the manifesto are contained in the online proceedings of the workshop.

3. The participants

The seminar gathered 35 researchers, among them 6 participants from industry, from the following countries:

> Austria (2), France (3), Germany (24), Norway (1), Switzerland (2), United Kingdom (1), United States (2).

Around half of the participants came from the intrusion detection and networking monitoring community each. The different backgrounds of the researchers resulted in stimulating discussions on various issues.

4. The program

We organized the program in 6 sessions to present participants' individual perspective opinion on the area and six working groups which discussed in several sessions the respective topic.

The speakers of the first day (*Monday, March 3rd*) were

Keynote talk: **Richard Kemmerer** (Univ. California - Santa Barbara, USA)
Intrusion Detection - Yesterday, Today, and Tomorrow

Georg Carle (University of Tuebingen, GER)
On Network Attack Detection and Response

Tanja Zseby (Fraunhofer Institute FOKUS Berlin, GER)
Expect the Unexpected! The importance of passive measurements for Network Security

Tobias Limmer (University of Nueremberg/Erlangen, GER)
Requirements and State of the Art for Seamless Reconfiguration of Flow Meters

Marc Dacier (Institut Eurécom, Sophia-Antipolis Cedex, F)
From intrusion detection to attack attribution vs. from error detection to fault diagnosis

Pavel Laskov (Fraunhofer Institut FIRST Berlin, GER)
Similarity-based anomaly detection for network security

Anja Feldmann (Technical University Berlin, GER)
Enhancing NIDS with Time Travel - NIDS Autoconfiguration

The speakers of the second day (*Tuesday, March 4th*) were

Joachim Biskup / Michael Meier (University of Dortmund, GER)
Specification and Enforcement of Availability and Confidentiality Policies as Enabler of Cooperative Security Surveillance

Peter Herrmann (Univ. of Science & Technology Trondheim, N)
Making Distributed Services Security-Aware – Desires of a Software Engineer

James Sterbenz (Univ. of Kansas - Lawrence, USA)
Multilevel Defensive Network Architecture

Christopher Kruegel (Technical University Vienna, A)
Still doing intrusion detection research after all these years

Stephan Wolthusen (RHUL – London, UK)
Concurrent Probabilistic Attack Detection and Self-Defense

Sebastian Schmerl / Hartmut Koenig (BTU Cottbus, GER)
Speed up the modeling process of Snort signatures by reuse

Norbert Luttenberger (University of Kiel, GER)
Upper Layer DoS attacks

The speakers of the third day (*Wednesday, March 5th*) were

Thorsten Holz (University of Mannheim, GER)
The Future of Honeypots

Markus Jahnke/Jens Toelle (FGAN Wartenberg, GER)
Practical Challenges for Intrusion Detection and Response in tactical MANETs

Radu State (INRIA Nancy, F)
Advanced vulnerability searching with fuzzing

The speakers of the forth day (*Thursday, March 6th*) were

Ulrich Flegel (SAP Karlsruhe, GER)
Intrusion and Fraud Detection for the Internet of (Web) Services

Hervé Debar (France Telecom R&D Caen, F)
Past and future perspectives of network security research and its application to the real world

Besides the individual perspective talks which were held in the auditorium 6 working groups met several times to discuss new research directions. The topics considered were

- Early warning systems
- Situation awareness
- Attack taxonomy
- Measurement requirements
- Requirements for network monitoring from an IDS perspective
- Intrusion and fraud detection for web services

The results of these working groups are documented in the proceedings. They form the input for the manifesto.

5. Conclusions

We assess the workshop as successful and very useful for all participants. This was expressed several times to the organizers by the participants. There are two main achievements of the workshop: (1) the meeting made participants aware of a commonality of interests across both areas and (2) it suggested new directions for research that will probably be taken up by some of the participants in the next couple of years.

Where is the field going? We can identify the following trends:

- The potential of threats in networked systems will further grow as well as the number of individuals which are able to abuse these systems. Increased efforts in research and society are required to protect critical infrastructures such as the health care system, the traffic system, power supply, trade, military networks and others in industrial countries.
- Reactive measures will further turn out as the most efficient countermeasures to ward off these threats in future. Intrusion detection and network monitoring as complementary approaches will remain the most important approaches in this context.
- It turned out that specific functionality of intrusion detection can be accelerated or improved by moving operations into the monitoring environment. Such cross-domain optimizations need to be adaptive in terms network load and attack awareness.

For the future, we plan another workshop in 2 – 3 years to discuss the development under the perspective of this workshop and to encourage continued interdisciplinary interactions.

The organizers

Georg Carle
Falko Dressler
Richard Kemmerer
Hartmut Koenig
Chris Kruegel