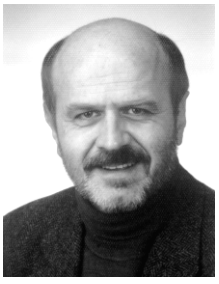
K.G. Saur Verlag, München, 2004

M. Meier, U. Flegel, and H. König

Reactive Security – Intrusion Detection, Honeypots, and Vulnerability Assessment

Michael Meier studied computer science from 1993 to 1998 at the Brandenburg University of Technology Cottbus (Germany). After his graduation he joined the Network Security group of the chair Computer Networks and Communication Systems at the Computer Science Department of the same university, where he is working as research and teaching assistant. His research interests include security aspects of information technology. His current research focus is intrusion detection. He is a founder member of the special interest group SIDAR "Security – Intrusion Detection and Response" of the German Informatics Society (GI) and member of the steering committee of the group.

Ulrich Flegel graduated at the Computer Science Department at the Technical University at Brunswick, Germany, and now is member of the research staff at the Information Systems and Security group at the Computer Science Department of the University of Dortmund, Germany. His research focus is on aspects of privacy and reactive security and their interplay, more specifically on identity management and intrusion detection systems. He is a founder member of the special interest group SIDAR "Security – Intrusion Detection and Response" of the German Informatics Society (GI) and is in charge of the chair position of the group.



Hartmut Koenig completed his diploma in physics at the Technical University of Dresden (Germany) in 1972. He received his Dr.-Ing. and Dr.-Ing.habil. in computer science from the same university in 1979 and 1987, respectively. In 1988 he became associate professor at the Department of Computer Science of the Otto-von-Guericke University of Magdeburg. Since 1993 he has been a full professor at the Department of Computer Science of the Brandenburg University of Technology at Cottbus. His research interests include network protocols, protocol engineering, video-conferencing, network security, intrusion detection, and grid computing. Prof. Koenig was guest professor at the University of Montreal, at La Trobe University Melbourne, at INT Evry, and at the University of Helsinki. He was co-chair of IFIP TC 6 working conferences DAIS '97, DAIS '99, TestCom 2002, and FORTE 2003, and general chair of the IEEE ICNP 2004 held October 2004 in Berlin. Prof. Koenig is member of IFIP TC 6 WG 6.1 and 6.7.

The rapid advance of communication technologies in many areas of the human society accelerates the displacement of many social processes on such systems, in particular on the Internet. This brings numerous benefits to the users, but it also increases their dependencies on these technologies. These dependencies create a growing potential of threats, while the increasing technological complexity of the systems makes them more and more vulnerable.

Security has, therefore, become a crucial feature in the development and acceptance of the Internet. The growing dependency of human society on information technology (IT) systems and in particular on the Internet has moved IT security in the focus of interest. Large efforts are made to preserve the confidentiality and integrity of data, to ensure the authorization of accesses to resources, and to avoid misuse of the Internet. The majority of the procedures applied and the approaches investigated focus on preventive measures that try to avoid a harmful behavior of the users. Less attention is paid to reactive measures which are triggered when intruders succeed to circumvent all security barriers. The rapidly increasing number of attacks – alone in 2003[1] about 137529 security incidents have been registered by the Coordination Center of the US Computer Emergency Response Team (CERT/CC) – makes it more and more apparent that IT security cannot be achieved by prevention alone. Only reactive measures are capable to respond appropriately to hinder an attacker, to avoid harm, or to prevent future intrusions. Therefore, future IT security measures should be more complementary taking into account both aspects.

The enforcement of research activities in this area is the objective of the special interest group SIDAR (*Security – Intrusion Detection and Response*) which was recently founded as part of the Security and Safety division of the German Informatics Society (GI). SIDAR focuses on reactive aspects of IT security and related areas. The main topics of interest are Intrusion Detection and Prevention, Incident Response, and Computer Forensic. SIDAR addresses both academic research and industrial development and deployment. It provides a forum for researchers and users to review, discuss, and learn about new approaches, concepts, and experiences in the field of reactive

1 CERT/CC annotates regarding these statistics: "Given the widespread use of automated attack tools, attacks against Internet-connected systems have become so commonplace that counts of the number of incidents reported provide little information with regard to assessing the scope and impact of attacks. Therefore, as of 2004, we will no longer publish the number of incidents reported. Instead, we will be working with others in the community to develop and report on more meaningful metrics, …".

security measures. More information about SIDAR is available on the website of the group: http://www.gi-fb-sicherheit.de/fg/sidar/.

One of the first activities of SIDAR was the organization of the DIMVA 2004 which was held July 6th-7th, 2004 in Dortmund. DIMVA is an annual workshop in the German-speaking area dedicated to Intrusion Detection, Malicious Agents, and Vulnerability Assessment. The next event will take place 2005 in Vienna. DIMVA will increase the public awareness of reactive aspects in IT security. It focuses on the discussion and the exchange of opinions on recent advances and developments in the area. The workshop addresses active players working on reactive IT security in industry, government, and research.

In 2004 authors from twelve countries on three continents submitted 41 papers to the workshop. More than a hundred participants from academia (54%), industry (36%) and government (10%) from six countries attended DIMVA 2004. This issue contains extended versions of the best and most interesting papers of this year's workshop. We selected papers covering different topics of reactive security measures to illustrate the broad range of activities in this field. In the sequel we give an overview of the subjects discussed in the contributions.

In order to efficiently and adequately increase the security of our systems by mounting preventive barriers and arranging for reactive measures, we need to know what the actual threat is that our systems are facing. Recently emerging endeavors look into an experimental honeypot approach to assessing the current threat. The honeypot or even honeynet approach is based on the idea to place one or more different instances of electronic bait together with one or more sensors within the network environment for which the attack potential should be determined. In this issue we present three contributions introducing various aspects concerning honeynets and delivering insights into the current threat our systems are facing when connected to the Internet.

The contribution "Honeynet Operation within the German Research Network – A Case Study" describes the requirements for the operation of honeynets, an operational honeynet at the Leibniz-Supercomputing Center within the German Research Network (DFN) and presents the experiences made over a period of two months. The contribution "Vulnerability Assessment using Honepots" describes an operational honeynet within the University of Aachen and basically corroborates the aforementioned experiences. More importantly, the paper elaborates on the technical details of honeypots and brings up ethical, legal and economical aspects related to this technology.

One might be tempted to object the significance of the presented threat assessments, which may be limited to the respective honeynet environments. The contribution "A Network of IDS Sensors for Attack Statistics" may reconcile this argument. The paper describes a network of internationally distributed honeypots and presents an evaluation of the data delivered by the honeypots. While confirming the previous results, the distributed approach particularly provides new insights into the scanning range of the attackers.

After the threat we are facing is determined we need to assess the vulnerabilities that the systems exhibit. While the threat analysis helps us to adjust our security priorities, the vulnerability assessment points us to the existing problems that we need to solve in our systems according to our security priorities. The contribution "Foundations for Intrusion Prevention" proposes an Intrusion Prevention Infrastructure as a systematic approach to efficiently close existing vulnerabilities by ranking them based on the knowledge about the local system as well as about the threat the system confronts.

Knowledge about the vulnerabilities of a system can also be exploited to improve the accuracy of intrusion detection results. Intrusion detection systems generate a number of non-relevant alerts which correspond to unsuccessful attack attempts and therefore should be assigned a low priority or should be suppressed. The contribution "Using Alert Verification to Identify Successful Intrusion Attempts" discusses techniques to verify the relevance of alerts. The authors present a tool that integrates vulnerability assessment mechanisms into an intrusion detection system to verify alerts regarding the vulnerability that the associated attack aims to exploit.

One of the main approaches in intrusion detection is anomaly detection that focuses on deviations from usual activity patterns. Since classical anomaly detection systems require knowledge about usual activity they need to be trained with data representing usual and security-compliant behavior. Unfortunately it is difficult to produce clean, attack-free training data. To overcome this issue methods for so-called unsupervised anomaly detection have been recently proposed. These approaches do not require training data that are free of attack manifestations. The contribution "Intrusion detection in unlabeled data with quarter-sphere Support Vector Machines" proposes and evaluates a new method for unsupervised anomaly detection.

One of the current software development trends is the construction of systems by assembling software components of possibly competing software vendors. This trend generates new security threats e.g. maliciously acting components. The contribution "Trust-Based Monitoring of Component-Structured Software" introduces an approach to address the threats that detects misbehaving components by comparing activities at the interfaces of components against application-specific security policies.

Another future trend is the application of small, mobile and networked devices. These new technologies such as mobile adhoc networks (MANETs) raise new security challenges. MANETs rely on the cooperation of all participating nodes. The problem of uncooperative nodes trying to save their resources is addressed by the contribution "Sensors for Detection of Misbehaving Nodes in MANETs". They propose and evaluate an approach for detecting and excluding such nodes.

We hope that the contributions of this special issue will not only give the reader a broad overview on the variety and complexity of reactive countermeasures in the Internet, but will be also helpful for future work.

The Editors