Dimva 2006

Welcome

You never know what lurks behind the code! Viruses, worms, spyware, „trojan horses“ and hidden vulnerabilities have become part of an everyday concern of system administrators as well as ordinary users. To counter an imminent threat of hacker attacks, security mechanisms should be able to adapt to constantly changing environments and promptly react to incidents. By bringing together experts in reactive security representing academic, governmental and commercial institutions, DIMVA strives to facilitate development of novel security approaches and their smooth transfer into practice.

Conceived as a compact and dynamic forum, DIMVA has achieved a recognized place in the international IT-Security calendar. Now in its third year, DIMVA has received 41 submissions from 21 countries. 11 contributions from 9 countries have been selected for publication in a competitive selection process (27% acceptance rate). We extend sincere appreciation to authors and reviewers for their hard work in strengthening the scientific quality of this meeting.

On behalf of the DIMVA Steering Committee, welcome to DIMVA in Berlin!

Pavel Laskov and Roland Büschkes

In cooperation with:

Kindly supported by:

Program

Thursday, 13.7.2006

8:30 - 9:30	Registration
9:30 - 9:45	Opening Remarks
9:45 - 11:00	**Keynote** Reaction: The internet security paradox. J. McHugh, Dalhousie University
11:00 - 11:30	Coffee Break
11:30 - 12:30	**Code Analysis** Type qualifiers to analyze untrusted integers and detecting security flaws in C programs. Ebrima N. Ceesay, Jingmin Zhou, Matt Bishop, Michael Gertz and Karl Levitt Using static program analysis to aid intrusion detection. Manuel Egele, Martin Szydlowski, Engin Kirda, Christopher Kruegel
12:30 - 14:00	Lunch Break
14:00 - 15:30	**Intrusion Detection** An SVM-based masquerade detection method with online update using co-occurrence matrix. Liangwen Chen and Masayoshi Aritsugi Network-level polymorphic shellcode detection using emulation. Michalis Polychronakis, Kostas G. Anagnostakis, Evangelos P. Markatos Detecting unknown network attacks using language models. Konrad Rieck and Pavel Laskov
15:30 - 16:00	Coffee Break
16:00 - 17:00	**Threat Protection and Response** Using labeling to prevent cross-service attacks against smart phones. Collin Mulliner, Giovanni Vigna, David Dagon, Wenke Lee Using contextual security policies for threat response. Hervé Debar, Yohann Thomas, Nora Boulahia-Cuppens and Frédéric Cuppens
17:15 - 18:00	Meeting of the GI Special Interest Group SIDAR
19:00 - 23:00	Boat tour on the Spree / Conference dinner

Program

Friday, 14.7.2006

9:00-10:15	**Keynote** Security Management - 5000 events/sec, half an engineer, and automation discouraged. M. Behringer, Cisco Systems
10:15-10:45	Coffee Break
10:45-11:45	**Malware and Forensics** Detecting self-mutating malware using control-flow graph matching. Danilo Bruschi, Lorenzo Martignoni, Mattia Monga Digital forensic reconstruction and the virtual security testbed ViSe. André Årnes, Paul Haas, Giovanni Vigna, Richard A. Kemmerer
11:45-12:30	**Rump Session** Informal presentations of recent results
12:30-14:00	Lunch Break
14:00-15:00	**Deployment Scenarios** A robust SNMP based infrastructure for intrusion detection and response in tactical MANETs. Marko Jahnke, Sascha Lettgen, Jens Tölle, Michael Bussmann, Uwe Weddige A fast worm scan detection tool for VPN congestion avoidance. Arno Wagner, Thomas Dübendorfer, Roman Hiestand, Christoph Göldi, Bernhard Plattner
15:00-15:30	Coffee Break
15:30-16:30	**Best Practice** Analysing privacy-invasive software using computer forensic methods. Martin Boldt and Bengt Carlsson Subverting J2EE security with malicious serialized payload. Marc Schönefeld
16:30-17:00	Overview and results of the 2nd Capture-The-Flag contest CIPHER Lexi Pimenidis
17:00-17:15	Closing Remarks

Special Events

CIPHER

The second Capture-The-Flag (CTF) contest CIPHER, organized by the GI Special Interest Group SIDAR and the Security and Privacy Research Group of RWTH Aachen, features several student groups exercising defense and penetration techniques in a virtual environment. The goal of CIPHER is to provide students of participating teams with practical experience in security administration. Each team will be provided with an image of a vulnerable server running various services. The team's task is to protect its server against attacks from competing teams while trying to compromise the systems of their opponents. Points will be given for various successful penetrations and for the duration of keeping the own server uncompromised. The contest will run on 14.7.2006 from 9.00 to 16.00. The scoreboard will be broadcast live and results will be summarized at the end of the second day of DIMVA.

www.cipher-ctf.org

SPRING

The GI Special Interest Group SIDAR invites young researchers in the field of reactive security to present their recent results in an informal one-day workshop to be held on 12.7.2006 at the same premises as DIMVA. Participation in the workshop is free.

www.gi-fg-sidar.de/spring/spring1

Organization

Program Committee

Phil Attfield, Northwest Security Institute, USA
Thomas Biege, SUSE LINUX AG, Germany
Marc Dacier, Institut Eurécom, France
Herve Debar, France Telecom R&D, France
Luca Deri, ntop.org, Italy
Sven Dietrich, Carnegie Mellon University, USA
Toralv Dirro, McAfee, Germany
Ulrich Flegel, University of Dortmund, Germany
Dirk Häger, BSI, Germany
Bernhard Hämmerli, HTA Luzern, Switzerland
Oliver Heinz, arago AG, Germany
Peter Herrmann, NTNU Trondheim, Norway
Marc Heuse, n.runs GmbH, Germany
Erland Jonsson, Chalmers University of Technology, Sweden
Klaus Julisch, IBM Research, USA
Engin Kirda, Technical University Vienna, Austria
Hartmut König, Technical University of Cottbus, Germany
Klaus-Peter Kossakowski, DFN-Cert, Germany
Christopher Kruegel, Technical University Vienna, Austria
Jens Meggers, Symantec, USA
Michael Meier, University of Dortmund, Germany
Achim Müller, Deutsche Telekom Laboratories, Germany
Martin Naedele, ABB Corporate Research, Switzerland
Dirk Schadt, Computer Associates, Germany
Robin Sommer, ICIR/ICSI, USA
Axel Tanner, IBM Research, Switzerland
Marco Thorbruegge, ENISA, Greece
Stephen Wolthusen, Gjovik University College, Norway

Steering Committee

Ulrich Flegel, University of Dortmund, Germany
Michael Meier, University of Dortmund, Germany
Roland Büschkes, RWE AG, Germany
Marc Heuse, n.runs, Germany
Klaus Julisch, IBM Research, USA
Christopher Kruegel, Vienna University of Technology, Austria

Organization

Organizing Committee

General Chair: Pavel Laskov, Fraunhofer FIRST, Germany
Program Chair: Roland Büschkes, RWE AG, Germany
Sponsoring Chair: Marc Heuse, n.runs GmbH, Germany
Publicity Chair: Ulrich Flegel, University of Dortmund, Germany

Conference Fees and Registration

	until 12.06.2006	after 12.06.2006
Regular Fee	295 Euro	345 Euro
Reduced Fee[1]	195 Euro	245 Euro
Student Fee	75 Euro	90 Euro
Extra Dinner Ticket	40 Euro	40 Euro

[1] The reduced fee is valid for members of GI and affiliated scientific societies.

The Conference Fee includes:

- Admission to the technical program
- Conference proceedings
- Admission to the conference dinner (tickets for accompanying persons can be purchased additionally)
- Lunch and refreshments on both days
- Conference gifts

For online registration and travel information visit the conference web site: **www.dimva.org/dimva2006**

Contact

Fraunhofer Institute for Computer Architecture
and Software Technology FIRST
Pavel Laskov
Kekuléstraße 7, 12489 Berlin
Phone: +49 (0) 30 / 63 92 – 18 00
Fax: +49 (0) 30 / 63 92 – 18 05
E-Mail: first@first.fraunhofer.de
www.first.fraunhofer.de

Location

Conference Venue

Conference and Event Centre
of Berlin-Brandenburg Academy of Sciences and Humanities
Markgrafenstraße 38
10117 Berlin

Conference Dinner

Conference dinner will be held during the boat tour on the Spree. The boat „Comtesse" will start at 19:00 from the landing stage located at the crossing of Märkisches Ufer and Am Köllnischen Park.

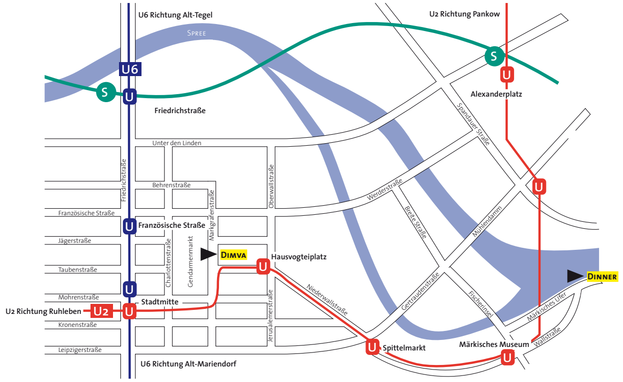
Directions from the Conference Venue

Using public transportation:

- Take U2 from the station „Hausvogteiplatz" two stops in the direction of Pankow to the station „Märkisches Museum".
- Walk along the Wallstraße ca. 300 m in the direction of Spree until the crossing of Märkisches Ufer and Am Köllnischen Park.

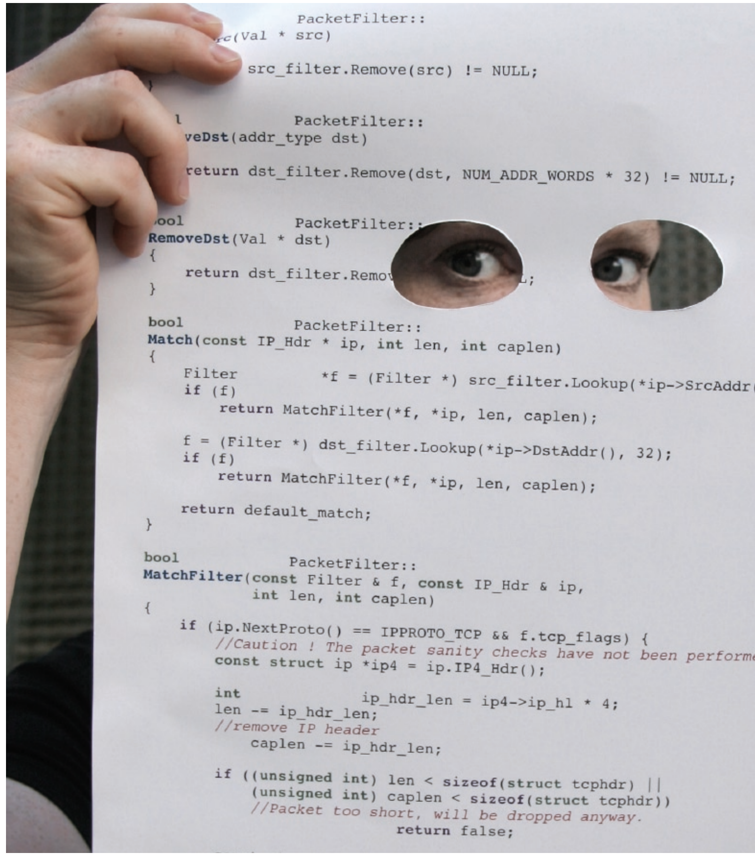
On foot:

- Follow the Taubenstraße ca. 200 m until the crossing with the Niederwallstraße.
- Turn right onto the Niederwallstraße and follow ca. 300m until the crossing with the Leipzigerstraße (Spittelmarkt).
- From Spittelmarkt follow the Wallstraße ca. 800m until the crossing of Märkisches Ufer and Am Köllnischen Park.



German Informatics Society (GI)

Special Interest Group SIDAR



```
                    PacketFilter::
  c(Val * src)

      src_filter.Remove(src) != NULL;
}

l                   PacketFilter::
veDst(addr_type dst)

  return dst_filter.Remove(dst, NUM_ADDR_WORDS * 32) != NULL;


ool                 PacketFilter::
RemoveDst(Val * dst)
{
    return dst_filter.Remo                ;
}

bool                PacketFilter::
Match(const IP_Hdr * ip, int len, int caplen)
{
    Filter          *f = (Filter *) src_filter.Lookup(*ip->SrcAddr
    if (f)
        return MatchFilter(*f, *ip, len, caplen);

    f = (Filter *) dst_filter.Lookup(*ip->DstAddr(), 32);
    if (f)
        return MatchFilter(*f, *ip, len, caplen);

    return default_match;
}

bool                PacketFilter::
MatchFilter(const Filter & f, const IP_Hdr & ip,
            int len, int caplen)
{
    if (ip.NextProto() == IPPROTO_TCP && f.tcp_flags) {
        //Caution ! The packet sanity checks have not been performe
        const struct ip *ip4 = ip.IP4_Hdr();

        int             ip_hdr_len = ip4->ip_hl * 4;
        len -= ip_hdr_len;
        //remove IP header
            caplen -= ip_hdr_len;

        if ((unsigned int) len < sizeof(struct tcphdr) ||
            (unsigned int) caplen < sizeof(struct tcphdr))
            //Packet too short, will be dropped anyway.
                        return false;
```

Dimva 2006

Detection of Intrusions and Malware & Vulnerability Assessment

July 13-14, 2006
Berlin, Germany