



## Sentinels year report 2005

---

Rik D.T. Janssen  
Technology Foundation STW  
Version 1.0, February 14, 2006

[www.sentinels.nl](http://www.sentinels.nl)  
[info@sentinels.nl](mailto:info@sentinels.nl)



Sentinels is being financed by Technology Foundation STW, NWO and the Ministry of Economic Affairs



## Sentinels year report 2005

---

The Sentinels year report 2005 can be obtained from [www.sentinels.nl/library/yearreport2005.pdf](http://www.sentinels.nl/library/yearreport2005.pdf).

PO Box 3021  
3502 GA Utrecht  
The Netherlands

Visiting address:  
Van Vollenhovelaan 661  
3527 JP Utrecht

Phone +31 (0)30 6001211  
Fax +31 (0)30 6014408

[www.sentinels.nl](http://www.sentinels.nl)  
[info@sentinels.nl](mailto:info@sentinels.nl)

ABN-AMRO 55 57 54 855

## Contents

---

|   |           |
|---|-----------|
| <b>Preface</b> . . . . .  | <b>4</b>  |
| <b>Introduction</b> . . . . .   | <b>5</b>  |
| <b>1 The year 2005 at a glance</b> . . . . .  | <b>6</b>  |
| 1.1 Projects granted in 2004 . . . . .  | 6         |
| 1.2 Sentinels Vici-position . . . . .   | 6         |
| 1.3 Sentinels ambassador . . . . .  | 6         |
| 1.4 Sentinels Security day, September 29, 2005 . . . . .                                | 6         |
| 1.5 Preparation and start of the second round of Sentinels proposals in 2006 . . . . .  | 7         |
| 1.6 Press coverage in 2005 . . . . .  | 7         |
| <b>2 The financial year 2005</b> . . . . .  | <b>8</b>  |
| 2.1 Overall program budget . . . . .  | 8         |
| 2.2 Expenses for project costs in 2005 . . . . .  | 8         |
| 2.3 Expenses for knowledge exchange in 2005 . . . . .                                   | 9         |
| 2.4 Expenses for office costs & program management in 2005 . . . . .                    | 9         |
| <b>3 Program management in 2005</b> . . . . .   | <b>10</b> |
| 3.1 Steering Group members . . . . .  | 10        |
| 3.2 Program Committee members . . . . .   | 10        |
| 3.3 Daily Board members . . . . .   | 11        |
| 3.4 Program Office . . . . .  | 11        |
| <b>4 Sentinels Security day, Thursday, September 29, 2005</b> . . . . .                 | <b>12</b> |
| 4.1 Inleiding . . . . .   | 12        |
| 4.2 Over Sentinels . . . . .  | 12        |
| 4.3 Noodzaak . . . . .  | 12        |
| 4.4 Plenaire sessies . . . . .  | 13        |
| 4.5 Interactieve workshops . . . . .  | 13        |
| 4.6 Kennismarkt . . . . .   | 14        |
| 4.7 Conclusies . . . . .  | 14        |
| <b>5 Year report from the Sentinels ambassador</b> . . . . .                            | <b>15</b> |
| 5.1 Inleiding . . . . .   | 15        |
| 5.2 Algemeen . . . . .  | 15        |
| 5.3 Specifiek 2005 . . . . .  | 16        |
| <b>6 Year reports for each Sentinels project</b> . . . . .                              | <b>18</b> |
| <b>7 NIT.6677, JASON, A Generic Architecture for Secure Remote Management</b> . . . . . | <b>19</b> |
| 7.1 Administrative details . . . . .  | 19        |
| 7.2 Research report for the previous year . . . . .                                     | 19        |
| 7.3 Utilization report for the previous year . . . . .                                  | 19        |

---

|           |   |           |
|-----------|---|-----------|
| 7.4       | Contacts with third parties . . . . .   | 20        |
| 7.5       | Time line and events . . . . .  | 20        |
| 7.6       | Press coverage . . . . .  | 20        |
| <b>8</b>  | <b>TIT.6679, IPID, Integrated Policy-based Intrusion Detection . . . . .</b>                    | <b>21</b> |
| 8.1       | Administrative details . . . . .  | 21        |
| 8.2       | Research report for the previous year . . . . .   | 21        |
| 8.3       | Utilization report for the previous year . . . . .  | 22        |
| 8.4       | Contacts with third parties . . . . .   | 23        |
| 8.5       | Time line and events . . . . .  | 23        |
| 8.6       | Press coverage . . . . .  | 24        |
| <b>9</b>  | <b>CIT.6680 Practical Approaches to Secure Computation . . . . .</b>                            | <b>25</b> |
| 9.1       | Administrative details . . . . .  | 25        |
| 9.2       | Research report and utilization report for the previous year . . . . .                          | 26        |
| 9.3       | Contacts with third parties . . . . .   | 26        |
| 9.4       | Press coverage . . . . .  | 26        |
| <b>10</b> | <b>TIT.6682, ProBiTe, Protection of Biometric Templates . . . . .</b>                           | <b>27</b> |
| 10.1      | Administrative details . . . . .  | 27        |
| 10.2      | Research report for the previous year . . . . .   | 27        |
| 10.2.1    | Template Protection . . . . .   | 27        |
| 10.2.2    | Biometric Identification . . . . .  | 28        |
| 10.2.3    | Demonstrator . . . . .  | 28        |
| 10.3      | Utilization report for the previous year . . . . .  | 28        |
| 10.4      | Contacts with third parties . . . . .   | 29        |
| 10.5      | Press coverage . . . . .  | 29        |
| 10.6      | Publications . . . . .  | 29        |
| <b>11</b> | <b>VIT.6684, DeWorm, Worm monitoring on Internet backbones . . . . .</b>                        | <b>30</b> |
| 11.1      | Administrative details . . . . .  | 30        |
| 11.2      | Research report for the previous year . . . . .   | 30        |
| 11.3      | Utilization report for the previous year . . . . .  | 32        |
| 11.4      | Contacts with third parties . . . . .   | 33        |
| 11.5      | Time line and events . . . . .  | 33        |
| 11.6      | Press coverage . . . . .  | 33        |
| <b>12</b> | <b>TIF.6687, PINPAS JC, Program INferred Power-Analysis in Software for Java Card . . . . .</b> | <b>35</b> |
| 12.1      | Administrative details . . . . .  | 35        |
| 12.2      | Research report for the previous year . . . . .   | 35        |
| 12.3      | Utilization report for the previous year . . . . .  | 36        |
| 12.4      | Contacts with third parties . . . . .   | 36        |
| 12.5      | Time line and events . . . . .  | 36        |
| 12.6      | Press coverage . . . . .  | 36        |

---

|                             |           |
|-----------------------------|-----------|
| <b>References</b> . . . . . | <b>37</b> |
|-----------------------------|-----------|

## Preface

---

The year 2005 was an important year for the Sentinels program in that the first projects under the program have become operational. We currently have six projects running:

- JASON, Generic and Secure Remote Management Infrastructure;
- IPID, Integrated Policy-based Intrusion Detection;
- Practical Approaches to Secure Computation;
- ProBiTe, Protection of Biometric Templates;
- DeWorm, Worm monitoring on Internet backbones;
- PINPAS JC, Program INferred Power-Analysis in Software for Java Card.

These projects lead to a well balanced portfolio of security research in the Netherlands. Next to this we also installed our Sentinels ambassador who is already very active in promoting Sentinels towards the Dutch industry. And, in addition, we had our 'kick-off' for the next proposal round starting with a very successful Sentinels security day in Amsterdam. And last but not least we are starting the process for the appointment of a Vici-style Sentinels professor. All in all a busy year with a lot of activity.

Prof. Dr. Willem Jonker  
Chairman Sentinels

## Introduction

---

In the years 2002 and 2003 the Sentinels research program [2] was written. This program aims to improve ICT, networks and information systems security, including PCs, corporate and home networks, hand held devices, smart cards, and wireless networks. It targets the technical aspects of security through scientific research in close collaboration between academia and industry. After quite some activity to obtain funding for this program, it started in February 2004.

In 2004 the main Sentinels activity was the selection of research projects. This selection process has been concluded with the meeting of the Steering Group on November 24, 2004. In that meeting, the Steering Group granted six projects out of 15 submitted.

All of these projects have started in 2005. For most of them, a user committee has been formed. For the few remaining projects, this will be done in the first half of 2006.

For Sentinels, 2005 consisted of four main activities: activities of the Sentinels ambassador, the organisation with SenterNovem of the Sentinels Securitydag on September 29, 2005, in which industry and universities were brought together to learn to know each other for writing pre-proposals, the deadline for pre-proposals in December 2005, and the preparation for the Sentinels Vici-position.

More information about the Sentinels research program can be found in the document "Sentinels in a nutshell" [1] or more extensively in the research program text [2] and the year plans for 2004 [3], 2005 [4] and 2006 [5], and in the year report for 2004 [6].

This document describes the year report 2005 for Sentinels. Chapter 1 describes the year 2005 at a glance, chapter 2 describes the financial year 2005 for the program, and chapter 3 lists the members of the Steering Group, the Program Committee, the Daily Board, and the program management in 2005. Then, there are chapters about the Sentinels Securitydag (chapter 4) and the activities of the Sentinels ambassador (chapter 5). Next, the year reports for each project are given (chapters 7 to 12).

## 1 The year 2005 at a glance

---

### 1.1 Projects granted in 2004

In 2004, the first round of Sentinels proposals has been granted. The following proposals have been granted:

- NIT.6677, Erik Poll, JASON, Generic and Secure Remote Management Infrastructure.
- TIT.6679, Prof.dr. Roel Wieringa, IPID, Integrated Policy-based Intrusion Detection.
- CIT.6680, Dr. Ronald Cramer, Practical Approaches to Secure Computation.
- TIT.6682, Dr.ir. Raymond N.J. Veldhuis, ProBiTe, Protection of Biometric Templates.
- VIT.6684, Herbert Bos, DeWorm, Worm monitoring on Internet backbones.
- TIF.6687, Erik de Vink, PINPAS JC, Program INferred Power-Analysis in Software for Java Card.

Short outlines of these projects can be found on the Sentinels website, [www.sentinels.nl/projects](http://www.sentinels.nl/projects), as well as in the chapters with year reports for each individual project, chapters 7 to 12.

### 1.2 Sentinels Vici-position

Sentinels has planned funding for a Vici-position in information security at a Dutch university. This form of grant is directed at senior researchers who have shown that they have the ability to successfully develop their own innovative lines of research and to act as coaches for young researchers. They will be able to build up their own research teams, often in advance of a regular professorial appointment. Their lines of research will be given a structural place within the research institution. The maximum amount of grant will be 1.2 M€ for a period of five years.

If possible, in 2006 the NWO Vici procedure will be joined. Part of 2005 has been spent in determining the best procedure how to do this and by getting approval from the Sentinels Board. By using budget from Sentinels, we ensure anchoring and that the person appointed (a.o.) collaborates with all kinds of Sentinels activities such as knowledge exchange activities, and that he/she promotes the Sentinels vision and range of ideas.

### 1.3 Sentinels ambassador

The security ambassador is, just as the Sentinels Vici-researcher, one of the important instruments to ensure that security research results from Sentinels remain visible and accessible even when the program has ended. He/she is someone who is very capable in promoting the Sentinels range of ideas.

Ideally, such a person should be from industry, so that Sentinels vision and research is actively promoted by both an expert from a university (the Vici-researcher) and an expert from industry. The security ambassador is *the* central point of access for anyone in need of security expertise.

In 2005 the Sentinels ambassador has started his work. His name is drs. Fred Eisner. Fred's year report can be found in chapter 5.

### 1.4 Sentinels Security day, September 29, 2005

On September 29, 2005, Sentinels has organized a Sentinels Security day. This has been done in cooperation with SenterNovem. The most important aim of that day was to bring

together industry and universities so they could start writing Sentinels proposals together for the second round of Sentinels proposals in 2006.

An extensive description of the Sentinels Security day can be found in chapter 4.

### 1.5 Preparation and start of the second round of Sentinels proposals in 2006

On the Sentinels Security day on September 29, 2005, the Sentinels call for pre-proposals for the second round of Sentinels proposals 2006, was released. The deadline for that call was December 15, 2005. 17 Pre-proposals have been received, from 7 different universities and 24 different companies. The decision how many are invited to submit a full proposal will be taken during a meeting of the Program Committee on January 26, 2006, and will be described more extensively in the year report 2006.

### 1.6 Press coverage in 2005

As far as is known to the author of this document, Sentinels, Sentinels related activities, or persons involved with Sentinels have generated the following press coverage in 2005. This section does not include press coverage of individual Sentinels projects, these can be found in the year report chapters for each project (chapters 7 to 12).

- Jan. 19, 2005: “Persbericht: VU-informatici starten groot onderzoek: Zeven ton voor jacht op Internetwormen en -virussen”, [www.vu.nl/Nieuws/index.cfm/home\\_subsection.cfm/subsectionid/314163C5-E34F-4175-B0650AAEDC6D2D8F](http://www.vu.nl/Nieuws/index.cfm/home_subsection.cfm/subsectionid/314163C5-E34F-4175-B0650AAEDC6D2D8F).
- Jan. 20, 2005: “Grootscheeps computervirusonderzoek bij de VU”, Computable webeditie, [www.computable.nl/nieuws.htm?id=437709](http://www.computable.nl/nieuws.htm?id=437709).
- Jan. 20, 2005: “VU begint onderzoek naar computervirussen”, Volkskrant.
- Feb. 25, 2005: “Condoom voor het netwerk”, Computable, p. 11.
- Feb. 28, 2005: “VU jaagt op internet wormen en -virussen” IT Monitor.
- Apr. 7, 2005: “Virussen lusten Windows rauw”, Intermediair 14, p. 45–47.
- June 2005: “Securitydag op 29 september 2005”, Rik D.T. Janssen, I/O InformaticaOnderzoek, jaargang 2, nummer 2, p. 12–13.
- July 19, 2005: “Bedrijfsgeheimen surfen de achterdeur uit”, Volkskrant.
- Dec. 2005: “Verbeter veiligheid van computersystemen, Sentinels Securitydag, donderdag 29 september 2005”, Rik D.T. Janssen, Informatiebeveiliging, nummer 8, p. 6–7. [www.sentinels.nl/library/Sentinels-Informatiebeveiliging-dec2005](http://www.sentinels.nl/library/Sentinels-Informatiebeveiliging-dec2005).
- Dec. 2005: “Sentinels Securitydag – Verbeter veiligheid van computersystemen”, Rik D.T. Janssen, I/O InformaticaOnderzoek, jaargang 2, nummer 4, p. 9. [www.sentinels.nl/library/Sentinels-Securitydag-IO-dec05](http://www.sentinels.nl/library/Sentinels-Securitydag-IO-dec05).

## 2 The financial year 2005

### 2.1 Overall program budget

Table 2.1(a) lists the revenues and table 2.1(b) lists the total expenses for the Sentinels research program. There are three main types of expenses: expenses for project costs (see section 2.2), expenses for knowledge exchange (see section 2.3), and expenses for office costs & program management (see section 2.4). This grouping originates from table 2.1(b) and can also be recognized in table 2.3.

Table 2.2 lists the total expenses per year. Both the table with revenues and expenses and the table with expenses per year are the same as in the year report 2004 [6] and have been discussed in that document.

### 2.2 Expenses for project costs in 2005

The projects which have been granted in the first round of the Sentinels program require a reservation of (rounded up) 3.0 M€ (for details see table 1.3 in the year plan 2005 [4]). This 3.0 M€ consists of (rounded) 2.2 M€ financial support from Sentinels en 0.7 M€ material, personnel and/or financial support from industry (the reason these do not add up to 3.0 M€ is due to the rounding up).

The total expenses for project costs in 2005 are € 38 099.79, with a total industrial contribution of € 13 890 (218 hours). (see table 2.3). Expenses for individual projects are not given in this year report for confidentiality reasons, but may be requested from the Sentinels secretariat.

Two reservations have been made to cover future project costs (see table 2.3): one of € 1 608 500 for financing projects before their continuation request<sup>1</sup>, and one of € 620 000 for financing projects after their continuation request, for a total of € 2 228 500. Note that

<sup>1</sup>The budget granted for a Sentinels project is divided in two parts, one part available directly after granting and the other part only after approval of the continuation request. This is done to ensure the quality of the research. A project leader has to do a continuation request within 18 months after start of his/her project.

| contributor                             | amount (M€) | expenses  | %  | amount (M€) |
|---|-------------|---|----|-------------|
| Public contributions:                   |             |   |    |             |
| Technology Foundation STW               | 2.5         | Research (incl. Vici-style professor)   | 80 | 8.0         |
| NWO                                     | 2.5         | Knowledge exchange (a.o. security ambassador, workshops, symposia, publ., comm.act., web portal (safe-nl, www.sentinel.nl)) | 10 | 1.0         |
| Ministry of Economic Affairs            | 2.5         | Office costs & program management   | 10 | 1.0         |
| <i>Total public contributions</i>       | <i>7.5</i>  | <b>total expenses</b>   |    | <b>10.0</b> |
| Matching funds:                         |             | (b) Overall expenses  |    |             |
| Industry (research, knowledge exchange) | 2.1         |   |    |             |
| University (Vici-style professor)       | 0.4         |   |    |             |
| Universities (research)                 | p.m.        |   |    |             |
| <i>Total matching contributions</i>     | <i>2.5</i>  |   |    |             |
| <b>total revenues</b>                   | <b>10.0</b> |   |    |             |
| (a) Revenues                            |             |   |    |             |

Table 2.1: Revenues and overall expenses

| amounts in M€                     | 2004 | 2005  | 2006  | 2007 | 2008  | 2009 | 2010 | 2011 | total       |
|-----------------------------------|------|-------|-------|------|-------|------|------|------|-------------|
| Projects round 1                  |      | 3.0   | ..... |      |       |      |      |      | 3.0         |
| Projects round 2                  |      |       |       | 3.8  | ..... |      |      |      | 3.8         |
| Vici-style professor              |      |       |       | 1.2  | ..... |      |      |      | 1.2         |
| Knowledge exchange                | 1.0  | ..... |       |      |       |      |      |      | 1.0         |
| Office costs & program management | 1.0  | ..... |       |      |       |      |      |      | 1.0         |
| <b>total expenses</b>             |      |       |       |      |       |      |      |      | <b>10.0</b> |

Table 2.2: Expenses per year as planned on December 31, 2005.

|   | research            | knowledge exchange | office costs & prog. man. | totaal              |
|---|---------------------|--------------------|---------------------------|---------------------|
| aangegane verplichtingen                                      |                     |                    |                           |                     |
| office costs & program management (in 2004)                   |                     |                    | 1.000.000,00              |                     |
| gehonoreerde projecten ronde 2004 voor voortzetting (in 2004) | 1.608.500,00        |                    |                           |                     |
| <b>totaal aangegane verplichtingen</b>                        | <b>1.608.500,00</b> | <b>0,00</b>        | <b>1.000.000,00</b>       | <b>2.608.500,00</b> |
| <b>totaal uitgaven in 2004</b>                                | <b>0,00</b>         | <b>0,00</b>        | <b>80.850,53</b>          | <b>80.850,53</b>    |
| <b>totaal uitgaven in 2005</b>                                | <b>38.099,79</b>    | <b>36.415,84</b>   | <b>59.933,60</b>          | <b>134.449,23</b>   |
| <b>beschikbaar op 1-1-2006</b>                                | <b>1.570.400,21</b> | <b>-36.415,84</b>  | <b>859.215,87</b>         | <b>2.393.200,24</b> |
| reserveringen   |                     |                    |                           |                     |
| gehonoreerde projecten ronde 2004 na voortzetting             | 620.000,00          |                    |                           |                     |
| <b>totaal verwachte bedrijfsbijdrage projecten ronde 2004</b> | <b>703.528,00</b>   |                    |                           |                     |
| gerealliseerde bedrijfsbijdrage in 2005                       | 13.890,00           | (218 uur)          |                           |                     |
| nog te verwachten bedrijfsbijdrage projecten ronde 2004       | 689.638,00          |                    |                           |                     |
| <b>totale projectkosten ronde 2004</b>                        | <b>2.932.028,00</b> |                    |                           |                     |

Table 2.3: Financial overview of 2005. For explanation see the text.

these two amounts do not include the contribution from industry. This is estimated to be € 703 528.

### 2.3 Expenses for knowledge exchange in 2005

In 2005, there were two types of expenses for knowledge exchange activities: the Sentinels Security day and the Sentinels ambassador. The expenses for knowledge exchange in 2005 are € 36 415.84 (see table 2.3). Specific expenses for the Sentinels Security day and the Sentinels ambassador are not given in this year report for confidentiality reasons, but may be requested from the Sentinels secretariat.

### 2.4 Expenses for office costs & program management in 2005

The expenses for office costs & program management in 2005 are € 59 933,60 (see table 2.3). Almost all of this was spent on personnel costs.

## 3 Program management in 2005

---

The members of the Steering Group have been appointed by the participants providing funds for Sentinels. Approval from the Steering Group for the members of the Program Committee and the Daily Board has been obtained before new members joined the Program Committee or the Daily Board. For tasks and responsibilities of the Steering Group, Program Committee and the Daily Board, see the research program [2, chapter 6].

### 3.1 Steering Group members

The Sentinels Steering Group members as of December 31, 2005, are:

- Prof.dr. W. Jonker, Philips Research Laboratories & University of Twente (chairman) (from start of the program)
- Dr. R.D.T. Janssen, Technology Foundation STW (secretariat) (from start)
- Dr.ir. A.A.J.M. Franken MBA, Technology Foundation STW & Netherlands Organization for Scientific Research (from November 1, 2004)
- Drs. H.J.T. Nieuwenhuis, Ministry of Economic Affairs (from March 15, 2004)

The following person was member of the Steering Group in 2005:

- Ir. A.A.J. Reuver, IBM Nederland N.V. (from April 1, 2004 – December 1, 2005)

The observers for the Steering Group as of December 31, 2004, are:

- A.L. Levisson, Ministry of Economic Affairs (from November 1, 2004)
- Dr. F. Zuijdam, Netherlands Organization for Scientific Research (from December 1, 2004)

### 3.2 Program Committee members

The Sentinels Program Committee members as of December 31, 2004, are:

- Prof.dr. W. Jonker, Philips Research Laboratories & University of Twente (chairman) (from start of the program)
- Dr. R.D.T. Janssen, Technology Foundation STW (secretariat) (from start)
- Dr.ir. A.M. Bos, Chess Information Technology BV (from start)
- Ing. B.E. Elsinga, Capgemini Nederland B.V. (from May 1, 2005)
- Prof.dr. W.J. Fokkink, Centrum voor Wiskunde en Informatica & Vrije Universiteit Amsterdam (from start)
- Dr.ir. L.J.N. Franken, ABN-AMRO Bank N.V. (from April 1, 2004)
- Prof.dr. P.H. Hartel, University of Twente (from start)
- Prof.dr. B.P.F. Jacobs, Radboud University Nijmegen (from start)
- Dr.ir. P. de Jager, TNO ICT (from start – June 1, 2004 and from November 1, 2004)
- Dr. J.C. de Jong, SenterNovem (from September 1, 2005)
- E.R. de Lange, Ministry of Economic Affairs (from start)
- Dr.ir. J.C.A. van der Lubbe, Delft University of Technology (from start)
- Ir. H.A.M. Luijff, TNO Defence, Security and Safety (from start)
- Prof.ir. E.F. Michiels, Ernst & Young EDP Audit & University of Twente (from start)
- Prof.dr.ir. B. Preneel, Katholieke Universiteit Leuven (from start)
- Ing. B. Snel, Comsec Consulting B.V. (from May 1, 2005)

- 
- L.A.M. Strous, De Nederlandsche Bank N.V. (from April 1, 2004)
  - Prof.dr. A.S. Tanenbaum, Vrije Universiteit Amsterdam (from start)
  - Prof.dr.ir. H.C.A. van Tilborg, Technische Universiteit Eindhoven (from start)
  - E. Verheul, PricewaterhouseCoopers & Radboud University Nijmegen (from May 1, 2005)
  - Dr. E.P. de Vink, Technische Universiteit Eindhoven & Leiden University (from start)

The following person was members of the Program Committee in 2005:

- Drs. J.T. Bisseling, SenterNovem (from April 1, 2004 – September 1, 2005)

The observer for the Program Committee as of December 31, 2005, is:

- Dr. F. Zuijdam, Netherlands Organization for Scientific Research (from December 1, 2004)

### **3.3 Daily Board members**

The Sentinels Daily Board members as of December 31, 2005, are:

- Prof.dr. W. Jonker, Philips Research Laboratories & University of Twente (chairman) (from start of the program)
- Dr. R.D.T. Janssen, Technology Foundation STW (secretariat) (from start)
- Prof.dr. B.P.F. Jacobs, Radboud University Nijmegen (from start)
- Dr.ir. P. de Jager, TNO ICT (from start – June 1, 2004 and from November 1, 2004)

### **3.4 Program Office**

The Technology Foundation STW acts as the Program Office for Sentinels. The Program Office is run by the following person as of December 31, 2005:

- Dr. R.D.T. Janssen, Technology Foundation STW (from start of the program)

## 4 Sentinels Security day, Thursday, September 29, 2005

---

Author: Rik D.T. Janssen. This chapter has been written in Dutch.

Dit hoofdstuk is als artikel verschenen in het tijdschrift Informatiebeveiling: Verbeter veiligheid van computersystemen, Sentinels Securitydag, donderdag 29 september 2005, door Rik D.T. Janssen, Informatiebeveiling, december 2005, nummer 8, pagina 6-7. [www.sentinels.nl/library/Sentinels-Informatiebeveiling-dec2005/view](http://www.sentinels.nl/library/Sentinels-Informatiebeveiling-dec2005/view).

Een verkorte versie is verschenen in het tijdschrift I/O InformaticaOnderzoek: Sentinels Securitydag - Verbeter veiligheid van computersystemen, door Rik D.T. Janssen, I/O InformaticaOnderzoek, Jaargang 2, nummer 4, december 2005, pagina 9. [www.sentinels.nl/library/Sentinels-Securitydag-IO-deco5/view](http://www.sentinels.nl/library/Sentinels-Securitydag-IO-deco5/view).

### 4.1 Inleiding

Sentinels, het Nederlandse onderzoeksprogramma op het gebied van informatiebeveiliging, veiligheid van ICT, netwerken en informatiesystemen, heeft op donderdag 29 september 2005 een Securitydag georganiseerd. Belangrijk onderdeel van deze dag was het koppelen van mensen met een securityvraag aan mensen met een securityoplossing. Deze dag werd bezocht door ca. 90 mensen, ongeveer 50 uit de industrie, 40 van universiteiten en 10 overige. Dit artikel geeft een kort verslag van deze dag.

### 4.2 Over Sentinels

Het doel van het Sentinels onderzoeksprogramma is om alle soorten informatiesystemen en netwerken veiliger te maken. Hieronder vallen zowel de standaard systemen zoals pc's en netwerken, als ook hand held devices, embedded systemen en draadloze en on-chip netwerken. Sentinels wil ook bijdragen aan een alomvattend framework voor secure systems engineering. Zo'n framework helpt security-engineers in het ontwerpen en bouwen van veilige systemen. Sentinels is al in een aantal publicaties beschreven, bijvoorbeeld in het jubileumnummer van Informatiebeveiling (december 2004, [www.sentinels.nl/library/sentinels-informatiebeveiling-2004](http://www.sentinels.nl/library/sentinels-informatiebeveiling-2004)). Voor de laatste ronde onderzoeksvoorstellen is 3,8 miljoen euro (inclusief geschatte bedrijfsbijdrage) beschikbaar. Deadline voor deze ronde was 15 december 2005.

De resultaten van het onderzoek zijn direct bruikbaar voor industrie en overheid in Nederland en leveren zodoende een aanzienlijke, direct inzetbare, bijdrage voor de verschillende branches. Door deelname aan de securitydag kunnen ook projecten met specifiek voor de deelnemer interessante behoefte aan ICT-security-onderzoek ontstaan.

### 4.3 Noodzaak

Er wordt door kennisinstellingen, overheid én door het bedrijfsleven veel geld en tijd gestoken in de ontwikkeling van (beveiligingssystemen voor) ICT-security. Allerlei bedrijven, instellingen en ministeries zijn hierbij betrokken. Een belangrijk doel van Sentinels is dan ook het coördineren hiervan en het verbeteren en stimuleren van de samenhang. Daarom zijn deze partijen bij elkaar gebracht op 29 september 2005 om kennis te delen, van elkaars projecten te leren en vooral om toekomstige projecten op te zetten.

---

Op de Sentinels website is een overzicht van security expertise aan Nederlandse universiteiten en kennisinstellingen beschikbaar: "Security expertise aan universiteiten en kennisinstellingen in Nederland" ([www.sentinels.nl/library/SecurityExpertiseInNL.pdf](http://www.sentinels.nl/library/SecurityExpertiseInNL.pdf)). Tijdens de securitydag in het Olympisch Stadion in Amsterdam zijn de deelnemers door vooraanstaande sprekers in korte tijd op de hoogte gebracht van actuele en toekomstige ontwikkelingen. Er waren workshops waarin in drie fasen naar concrete onderzoeksvoorstellen werd gewerkt en er was een kennismarkt waarin wetenschappers, ontwikkelaars en toepassers hun producten, diensten en kennis presenteerden. Het werken naar synergetische relaties stond voorop. Er was ook alle ruimte voor informeel overleg en advisering.

#### 4.4 Plenaire sessies

In de morgen waren er plenaire presentaties door de volgende heren:

- Drs. E.R. Buddenbaum, Ministerie van Economische Zaken, Dir.-Gen. Telecommunicatie en Post;
- Prof.dr. M. Rem, Nationaal Regieorgaan ICT-onderzoek en Innovatie;
- Prof.dr. P.H. Hartel, Universiteit Twente;
- Prof.dr. W. Jonker, Philips Research & Technische Universiteit Twente, voorzitter Sentinels.

De heer Buddenbaum gaf een presentatie over overheidsbeleid en beveiliging van ICT. Vier punten kwamen daarin naar voren: vertrouwen van bedrijven en burgers in ICT, voorbereiding op verstoringen van de continuïteit van ICT-voorzieningen, ondersteuning opsporingsdiensten en verdienen aan innovatie van ICT-veiligheid.

De heer Rem sprak over het Nationaal regieorgaan ICT-onderzoek en -innovatie, een model om onderzoek en innovatie in ICT in Nederland te koesteren. Belangrijk voor het ICT-regieorgaan is om de onderzoekspositie van Nederland in de ICT te versterken en om die positie zodanig te gebruiken zodat nieuwe ICT producten en diensten ontwikkeld kunnen worden.

De heer Hartel vroeg aandacht voor security in het grote kader: let op dat beveiliging niet gebagatelliseerd wordt, het is een echt probleem. Innovatieve oplossingen kunnen ontstaan door gokwerk te vermijden en door het bedenken van onalledaagse oplossingen.

De heer Jonker beschreef het belang van security in consumentenproducten. Aspecten zijn bijvoorbeeld bescherming van digitale rechten (op bijvoorbeeld muziek of beeld) en hoe waardedocumenten te beschermen tegen vervalsing.

#### 4.5 Interactieve workshops

De rest van de dag was opgebouwd rond vier verschillende workshops. Elke workshop was onderverdeeld in drie fasen zodat tussendoor uitgebreid de ruimte was om verder met elkaar kennis te maken. Bij elke workshop waren twee sprekers, een moderator en een verslaglegger aanwezig. Belangrijk doel van de workshops was om bedrijven en onderzoekinstellingen bij elkaar te brengen. Daarnaast was het versterken van de vraagarticulatie vanuit het bedrijfsleven en bevorderen van de omzetting hiervan in projectvoorstellen voor de

---

volgende Sentinels call een belangrijk aspect. Sprekers gaven een overzicht van de actuele stand van zaken op het gebied van securityonderzoek in Nederland.

De vier workshops waren:

- Network Security (Security protocols, Mobile security, PKI, Authentication)
- Device Security (Smartcards, Secure tokens, Software-hardware tamper-resistance)
- Secure Identification Technology (Biometrics, Content identification, Privacy enhancing technologies, Value-paper protection)
- Content Security (Copy protection, Digital rights management, Conditional access, Access control)

Presentaties op de workshops en de verslagen van de workshops zijn terug te vinden op de Sentinels website ([www.sentinels.nl/workshops/20050929-securitydag](http://www.sentinels.nl/workshops/20050929-securitydag)).

#### **4.6 Kennismarkt**

Gedurende de lunch was er een kennismarkt met informatie over de Sentinelsprojecten die eind 2004 gestart zijn, over securitygerelateerde BSIK projecten en over het Nationaal Samenwerkingsverband Securityonderzoek. Ook waren er een tweetal commerciële presentaties.

#### **4.7 Conclusies**

De dag is goed bezocht en werd door de deelnemers goed ervaren. Veel mensen hebben nieuwe contacten opgedaan en er is voldoende grond voor vervolcontacten. We verwachten een groot aantal voorstellen voor de volgende Sentinels ronde. Aan beide doeleinden van de dag is dus zeker voldaan. Foto's en alle presentaties en verslagen zijn terug te vinden op de Sentinels website ([www.sentinels.nl/workshops/20050929-securitydag](http://www.sentinels.nl/workshops/20050929-securitydag)).

## 5 Year report from the Sentinels ambassador

---

Author: Fred Eisner. This chapter has been written in Dutch.

### 5.1 Inleiding

Met ingang van 11 juli 2005 is de eerste ambassadeur voor Sentinels werkzaam geweest op contractbasis, gemiddeld zo'n 6 uur per week (max. 12, min. 4). Bestede uren: 130 uren (in 22 weken effectief, dus 5,9 uur/week)

Ambassadeur in deze periode was drs. A. Eisner.

Drs. A. (Fred) Eisner (1953) is a well known national and international expert on technical and societal issues. He studied Public Administration, University of Twente in Enschede (NL), and worked in Government, Healthcare, Higher Education, and ICT-Industry. In the internet-industry he was partner and CTO (Chief Technical & Security Officer) with one of the first ISP's in NL. After that he served as president/CEO of NLIP (Dutch ISP Association) and board member of EuroISPA and led several national and European industry-working groups on security and continuity.

Fred wrote several policy-recommendations, on cybercrime, on e-business, on e-government, SPAM, critical infrastructure protection, etc. He advised government as well as industry, in NL and EU. Was member of the Dutch delegation to OECD-ministerial conference on E-Commerce in Ottawa/Canada in 1998. Since more then 10 years now working as an independent consultant and researcher, mostly on Internet Security (cybercrime, "illegal content") and on "Protection of Critical Infrastructures".

He is Guest-lecturer ICT & Security at Saxion Polytechnic Enschede. Member Supervisory Board of SIDN (.nl domain-name-registry). Experienced evaluator and rapporteur for EU, mostly in Safer Internet Action Plan, also for Security Research (as a national expert) and ENISA. International ambassador for INHOPE (combating illegal content on the Internet). Member Advisory Board of Bits of Freedom (BOF).

De ambassadeur doet z'n werk in overleg met de programmasecretaris bij STW en met de voorzitter van het Sentinels Dagelijks Bestuur.

### 5.2 Algemeen

In z'n algemeenheid is "kennisuitwisseling" de doelstelling voor de ambassadeursfunctie in Sentinels: het bevorderen van im- en export van Sentinelskennis. De functie, ingevuld door iemand met een bedrijfsleven-achtergrond, is wat dat betreft complementair aan die van de Sentinelshoogleraar die kennisuitwisseling bevordert vanuit de wetenschappelijke invalshoek.

Deze algemene kennisuitwisseling kan, voorzover de ambassadeur betrokken is, meer specifiek worden onderscheiden in:

- zwaartepuntvorming;
- netwerkvorming;

- kennisoverdrachtactiviteiten;
- kennisverankering.

Daarnaast is natuurlijk het vergroten van de naamsbekendheid van Sentinels zowel een doel als een middel. Ook het mede sturen/beïnvloeden van de toekomstige onderzoek-sagenda en -organisatie is voor ons onderzoek en onze onderzoekers van groot belang.

### 5.3 Specifiek 2005

Medio 2005 startte voor het eerst de Sentinels ambassadeur. De drie benoemde taakclusters waren:

1. Het actief promoten van het Sentinels onderzoeksprogramma en -resultaten onder relevante Nederlandse actoren, zoals industrie, (semi-)overheid en koepelorganisaties. Het bevorderen van deelname van genoemde actoren aan Sentinels:
  - Het belang van Sentinels voor o.a. het Nederlandse bedrijfsleven versterken.
  - Inventariseer i.o.m. sleutelpersonen in de security-communities en bij koepelorganisaties wie de in aanmerking komende bedrijven en personen zijn.
  - Contacten leggen, Sentinels promoten, reacties mee terugnemen.
2. Het actief deelnemen aan en helpen met organiseren van de securitydag op 29 september 2005 voor de hele Nederlandse security gemeenschap:
  - Ondersteunen van programmering, organisatie en inviteren.
  - Parallel daaraan het bevorderen van voldoende deelname van relevante bedrijven.
  - Aanwezig zijn op 29 september om o.a. te helpen bij het leggen van contacten en het organiseren van projectvoorstellen.
3. Na afloop van de securitydag op 29 september 2005:
  - Leggen, stimuleren, opvolgen en onderhouden van contacten tussen bedrijven en onderzoekers opdat bedrijven materiële, financiële of personele steun bijdragen aan voorstellen in de volgende Sentinels ronde.
  - Dit moet resulteren in pre-proposals en proposals waarbij een aanzienlijk aantal bedrijven steun bijdraagt.

Gezien de zowel korte als beperkte tijd is gekozen voor een indirecte aanpak. Dus niet domweg bedrijven gaan bezoeken, maar veeleer via grootschaliger activiteiten en brancheverenigingen werken, om op die manier Sentinels bij veel bedrijven tegelijk onder de aandacht te kunnen brengen, met daarbij de toegevoegde waarde van de activiteit en/of de branche. Als extra voordeel werd Sentinels zo ook zelf weer in de aandacht van brancheverenigingen en beleidsbeïnvloeders geplaatst.

Met name in de eerste drie maanden is relatief veel tijd besteed aan de securitydag. Een goed programma en een goede deelname door bedrijven zou diverse Sentinels doelstellingen bevorderen. De meeste tijd ging zitten in enerzijds programma-voorbereiding en anderzijds het promoten van Sentinels en de Securitydag bij brancheverenigingen en enkele grote "spelers". Denk aan VNO-NCW, Vereniging van Nederlandse Banken, MKB-Nederland, KPN, etc. Na de evaluatie van die dag kan worden gesteld dat beide doelen bereikt zijn.

De tweede periode van drie maanden is vooral besteed aan het verder promoten en bekend maken van Sentinels bij het enkele individuele bedrijven, met de mogelijkheden voor het

---

bedrijfsleven om te participeren in onderzoek. Ook de NVSO-kick-off in Twente is daarvoor nog gebruikt. Tevens werd actief ingespeeld op ontwikkelingen rondom toekomstig onderzoek, zoals die speelden bij o.a. NVSO, ICT-Regie, en EZ.

Terugkijkend kan worden geconcludeerd dat Sentinels bij velen goed op de kaart staat, en bij vele spelers ook aanzien geniet. Sentinels onderzoek en onderzoekers zullen hier ook in de toekomst van kunnen profiteren. Het gewenste “aanzienlijk aantal bedrijven” dat participeert in onderzoeksvoorstellen in de recente call is in deze korte periode niet gehaald. Met het actief uitdragen van Sentinels kennis naar het bedrijfsleven (ook een opdracht van Sentinels) kon zelfs maar nauwelijks een begin worden gemaakt (nieuwsbrief, website, bedrijfsbezoeken, “dagen”, etc.)

## 6 Year reports for each Sentinels project

---

The following chapters contain the year reports for each Sentinels project. In order, the following year reports will be presented:

- NIT.6677, JASON, Generic and Secure Remote Management Infrastructure.
- TIT.6679, IPID, Integrated Policy-based Intrusion Detection.
- CIT.6680, Practical Approaches to Secure Computation.
- TIT.6682, ProBiTe, Protection of Biometric Templates.
- VIT.6684, DeWorm, Worm monitoring on Internet backbones.
- TIF.6687, PINPAS JC, Program INferred Power-Analysis in Software for Java Card.

## 7 NIT.6677, JASON, A Generic Architecture for Secure Remote Management

---

Author: dr. Jaap-Henk Hoepman

The core of the practical problem in this project is to build remotely manageable devices, that are owned, controlled and/or accessed by several different parties with different, sometimes even conflicting interests. Several applications of such devices will appear in the near future. For these devices to be successful, they will have to satisfy strong security and privacy guarantees.

To this end, the JASON project develops a secure, object oriented, distributed programming platform for smart cards and embedded systems that provides

- separation of concerns: application programmer only needs to specify the security properties, not implement them, and
- generic secure access to objects and their methods, irrespective of their current location.

### 7.1 Administrative details

- project number: NIT.6677
- title of the project: JASON, A Generic Architecture for Secure Remote Management
- name project leader: dr. Erik Poll, Radboud University Nijmegen
- website: [www.cs.ru.nl/jason](http://www.cs.ru.nl/jason)
- names and fte's of personnel on the project:
  - Funded by Sentinels:
    - \* Thanh Son Nguyen, AIO, RUN, 1 fte, since 15-8-2005
    - \* Łukasz Chmielewski, AIO, RUN, 1 fte, since 1-11-2005
  - Funded by other sources:
    - \* dr. Jaap-Henk Hoepman, RUN
    - \* dr. Erik Poll, RUN
    - \* ir. Bert Bos, Chess IT
- the user committee will be formed in 2006.

### 7.2 Research report for the previous year

The two Ph.D. students have been appointed in the fall of 2005. A kick-off meeting took place at Chess IT, Haarlem on Monday November 14, shortly after the appointment of the second Ph.D. student. The Ph.D. students visit Chess IT weekly, every thursday.

Both Ph.D. students attended the IPA (Institute for Programming research and Algorithms) Fall School on Security from 21 to 25 November 2005 at Hotel Zwartewater, Zwartsluis.

Research started on collecting usage scenarios and security requirements from remote management related projects running or foreseen at Chess IT.

### 7.3 Utilization report for the previous year

Creation and expansion of networks (in Dutch: "netwerkvorming")  
 Several companies have been approached to join the user committee.

---

Knowledge dissemination (in Dutch: "kennisoverdracht")

A website for the JASON project has been established, see [www.cs.ru.nl/jason](http://www.cs.ru.nl/jason).

A poster presentation of the JASON project was given on the Sentinels Security day on September 29, 2005.

Anchoring of knowledge resulting from the program (in Dutch: "verankering")

At the kickoff meeting (and subsequent meetings), several key project managers of Chess IT described running and future Chess IT projects. Goal of these presentations was to establish potential synergy with and utilisation of the JASON project goals and aims.

#### **7.4 Contacts with third parties**

None.

#### **7.5 Time line and events**

- 15-8-2005 appointed Thanh Son Nguyen as Ph.D. student.
- 29-9-2005: poster presentation Sentinels Security day.
- 1-11-2005: appointed Łukasz Chmielewski as Ph.D. student.
- 14-11-2005: project kickoff at Chess IT, Haarlem.

#### **7.6 Press coverage**

None.

## 8 TIT.6679, IPID, Integrated Policy-based Intrusion Detection

---

Author: dr. Pascal A.T. van Eck

Currently available intrusion detection tools monitor events at a relatively low level of abstraction. Due to the large number of events that occur at that level, and due to the low abstraction level, these tools are either ineffective (by generating a large number of false negatives) or inefficient (by generating a large number of false positives). The objective of IPID is to increase both effectiveness and efficiency of these tools by relating low-level events to a smaller number of events at a high level that are meaningful to the business.

### 8.1 Administrative details

- project number: TIT.6679
- title of the project: Integrated Policy-Based Intrusion Detection (IPID)
- name project leader: prof.dr. R.J. (Roel) Wieringa
- website: [www.cs.utwente.nl/~patveck/?page=IPID](http://www.cs.utwente.nl/~patveck/?page=IPID).
- names and fte's of personnel on the project:
  - Funded by Sentinels:
    - \* Virginia Nunes Leal Franqueira, AIO, UT, 1 fte, since 1-8-2005
    - \* Damiano Bolzoni, AIO, UT, 1 fte, since 1-7-2005
  - Funded by other sources:
    - \* prof.dr. R.J. (Roel) Wieringa, Promotor, UT, 0.1 fte
    - \* prof.dr. P.H. (Pieter) Hartel, Promotor, UT, 0.1 fte
    - \* dr. P.A.T. (Pascal) van Eck, Daily supervisor, UT, 0.2 fte
    - \* dr. S. (Sandro) Etalle, Daily supervisor, UT, 0.2 fte
- user committee:
  - \* TNO
  - \* Rabobank
  - \* Fox-IT
  - \* Telindus
- user committee has not met yet; this is scheduled for early February 2006.

### 8.2 Research report for the previous year

As can be seen in the timeline in Section 8.5 below, the IPID Ph.D. candidates started only in the second half of 2005. The activities in 2005 are therefore best seen as first steps in executing the activities planned for 2006, which will be the first full year for IPID. These activities are derived from the IPID research questions as identified in the IPID project plan. There are two groups of research questions: those relating to the policy aspect of IPID and those relating to the technical aspect of IPID.

Policy aspects of IPID:

- Which techniques can be used or combined to express security policies at different levels in the organization hierarchy?
- How to maintain policy compliance when top-down and bottom-up changes occur?

- Is it feasible to bring access control and network infrastructure environments together in terms of policy specification?

These questions have mainly been addressed by Franqueira by performing an extensive literature study. This will be reported in 2006.

Technical aspects of IPID:

- Is it possible to devise new intrusion detection techniques which improve on present ones, in particular by being more easily linkable with the right policies?
- Which techniques can be used to translate policy-based rules into low-level rules for the intrusion detection system?
- Which techniques can be used to trigger the right policy(ies) after an attack(s) has been detected by the detection engine?
- Is it possible to build a general middleware (abstraction layer) or use a common language to translate high-level rules for every intrusion detection system?

On the technical side of IPID, Ph.D. candidate Bolzoni has concentrated on the first question. This has resulted in a proposal<sup>1</sup> for a new kind of anomaly-based intrusion detection system called Poseidon. Poseidon is payload-based, and presents a two-tier architecture: the first stage consists of a Self-Organizing Map, while the second one is a modified PAYL system. Our benchmarks on the 1999 DARPA data set show a higher detection rate and lower number of false positives than PAYL and PHAD.

### 8.3 Utilization report for the previous year

Development of knowledge (in Dutch: "kennisontwikkeling")

By definition, knowledge is developed in the IPID project by performing research, so see Section 8.2.

IPID Ph.D. candidates are members of the national graduate schools: SIKS (Franqueira) and IPA (Bolzoni) respectively. Franqueira took part in the SIKS basic course "Research methods and methodology for IKS". Bolzoni took part in the IPA Security School.

IPID researcher Van Eck has participated in a seminar on security aspects of IT governance organized and hosted by Computer Associates Netherlands.

Development of competence core areas (in Dutch: "zwaartepuntvorming")

IPID is embedded in the work of other security researchers in the chairs of Information Systems and Distributed and Embedded Systems. Thus, IPID researchers benefit from the other security researchers in these chairs as well as contribute to the shared knowledge accumulated in these chairs. This takes, for instance, the form of participation in chair-level weekly research seminars: both the DIES group as well as the IS group have weekly seminars. In 2005, there have been three talks delivered by IPID researchers in these weekly seminars.

<sup>1</sup>Damiano Bolzoni, Emmanuele Zambon, Sandro Etalle, Pieter Hartel (2005). *Poseidon: a 2-tier Anomaly-based Intrusion Detection System*. CTIT Technical Report TR-CTIT-05-53, Centre for Telematics and Information Technology, University of Twente, Enschede, The Netherlands. arxiv:cs.CR/0511043.

A key organizational principle of the University of Twente is that creation and expansion of networks is centralized in Strategic Research Orientations (SROs) of the six UT research institutes. The relevant SRO for IPID is ISTRICE, which is managed by IPID researcher Etalle. All IPID researchers are part of the multidisciplinary ISTRICE SRO-team, which consists of approx. 40 researchers. In 2005, IPID delivered a presentation in one of the ISTRICE lunch meetings.

#### Creation and expansion of networks (in Dutch: "netwerkvorming")

IPID researchers actively participate in creation and expansion of security-related networks:

- IPID researcher Etalle is a founding board member of the NVSO (*Nationaal samenwerkingsVerband Security Onderzoek*).
- IPID researchers contributed to establishing the Sentinels research agenda by participation in the Sentinels 2005 security event.

Industry contacts took the form of meetings with the following organizations: Belastingdienst Centrum voor ICT, Getronics, MediaPlaza, and Telindus.

#### Knowledge dissemination (in Dutch: "kennisoverdracht")

IPID-researchers Etalle and Van Eck led a “food for thought” session on security organized by Apeldoorn-IT, a foundation established by five IT-related organizations from Apeldoorn (Belastingdienst Centrum voor ICT, Gemeente Apeldoorn, Getronics PinkRocade, Kadaster, and Wegener).

#### Anchoring of knowledge resulting from the program (in Dutch: "verankering")

To “ensure that security research results from Sentinels remain visible and accessible even when the program has ended” (Sentinels research program, [2, p. 37]), IPID has:

- created a public web page;
- created a shared workspace on a document server for archiving of research results and making them available to IPID participants (such as the user committee);
- IPID also participates in open archiving.

### 8.4 Contacts with third parties

See the utilization report above.

### 8.5 Time line and events

- February: official acceptance letter from Sentinels received, start of Ph.D. application procedure.
- July 1: Arrival and start of first Ph.D. candidate (Bolzoni). Start of project.
- Augustus 1: Arrival of second Ph.D. candidate (Franqueira).
- September 29: Participation in Sentinels event; IPID presented a poster.
- November 8: Etalle and Van Eck lead a “food for thought” session on security organized by Apeldoorn-IT.

---

## 8.6 Press coverage

IPID was covered by “Campus magazine”, the University of Twente magazine for prospective students (high school kids).

## 9 CIT.6680 Practical Approaches to Secure Computation

---

Author: prof. dr. Ronald Cramer

This project focuses on cryptographic primitives and methods which do not yet belong to the standard toolkit of the security engineer, as opposed to methods for establishing private or authentic channels. We strongly believe that there is now a need to further strengthen the efforts to modernise the existing and very well traveled bridge between cryptography research and the real world, so that more security tools of a fundamental nature can be transferred across it.

It is especially worthwhile when this concerns tools that enable enhanced security levels or new security sensitive applications that could otherwise not be realized satisfactorily by a combination of already more standard security tools. Our project intends to contribute in that direction.

Concretely, in this project we apply this philosophy to elements from the area of *Secure Computation*, a very broad, active and fundamental field of cryptographic research. This area is fairly well understood in the cryptographic literature, at least in its basic incarnations and in a theoretical sense.

As opposed to the situation where two trusting parties wish to secure their communication channel from *malicious outsiders*, Secure Computation can deal with a fundamentally different scenario of two or more parties who wish to achieve some given joint task securely even though they are *mutually distrusting* and wish to keep sensitive, private information secret from each other. This is sometimes called *multi-lateral security*, as opposed to *unilateral security* in the case of secure communications.

We zero in on those methods and applications of Secure Computation which we see most fit for transfer to the real world in a short or medium time-frame. This presents an interesting and important research challenge, with a possible impact on security engineering in the near future. Example application areas include Digital Rights Management and Biometric Authentication, Threshold Cryptography, Profile Matching and Secure Datamining. As a starting point for our research, we will take general results on Secure Computation, including recent results by the members of our project team, and study the possibilities of suitably specializing them to our practical applications. Our expectation is that we will design attractive solutions of practical value, thereby contributing to opening up a new area of practical security applications.

### 9.1 Administrative details

- project number: CIT.6680
- title of the project: Practical Approaches to Secure Computation
- name project leader: Prof. Dr. Ronald Cramer, CWI/UL
- website: no website yet
- names and fte's of personnel on the project:
  - Funded by Sentinels:
    - \* Dr Eike Kiltz, postdoc, CWI, 1 fte, since 1-10-2005
    - \* José Villegas, AIO, TU/e, 1 fte, since 1-1-2006
    - \* n.n., TU/e, 1 fte.

---

Funded by other sources:

- \* Prof. Dr. Ronald J.F. Cramer, CWI/UL
- \* Dr. Berry Schoenmakers, TU/e
- \* Dr. Pim Tuyls, Philips Research
- the user committee will be formed in 2006.

## **9.2 Research report and utilization report for the previous year**

Since the project has only started recently, there are no results for 2005.

## **9.3 Contacts with third parties**

None.

## **9.4 Press coverage**

None.

## 10 TIT.6682, ProBiTe, Protection of Biometric Templates

---

Author: Raymond Veldhuis

ProBiTe concerns the integration of biometric identification in security systems. A considerable research effort has been spent on the individual topics of biometric identification and security, but their combination has led to new research questions. In particular, ProBiTe focusses on the problems of combining biometric identification and template protection.

Storing biometric templates in a database introduces security and privacy risks, which increase if the database is part of a network. A solution is to apply template-protection techniques, which make it impossible to recover the biometric data from the templates. The project's goals are (a) to solve the problems of combining biometric identification and template protection and (b) to validate the solutions in a home-network demonstrator, to be developed at Philips Research. Fingerprint recognition will be used to identify the user and to control the access to content and devices. Template protection will be used to protect biometric data.

### 10.1 Administrative details

- project number: TIT.6682
- title of the project: ProBiTe (Protection of Biometric Templates)
- name project leader: Raymond Veldhuis
- website: under construction
- names and fte's of personnel on the project:
  - Funded by Sentinels:
    - \* Haiyun Xu, AIO, UT, 1 fte, since 1-8-2005
    - \* Chen Chun, AIO, UT, 1 fte, since 1-9-2005
  - Funded by other sources:
    - \* Tom Kevenaer, Researcher, Philips Research, 0.5 fte, since 1-8-2005
    - \* Raymond Veldhuis, UT-SAS
- names and affiliations of members of the user committee:
  - \* Ton Akkermans, Researcher, Philips Research, since 01-08-2005
- dates of the user committee meetings: NA

### 10.2 Research report for the previous year

The project is divided into 3 work packages. The results are listed per work package. For clarity a brief description of each work package is included.

#### 10.2.1 Template Protection

This WP is targeted at developing and optimizing template-protection schemes that enhance security and do not degrade the performance of the biometric recognition. Template protection schemes will be developed and improved such that a maximum number of secret bits, guaranteeing the highest secrecy, are extracted from biometric features while retaining robustness against system noise and intra-class variability.

---

**Progress** From September 1, 2005 until end 2005 Chen Chun has familiarized herself with the theory of template protection by studying the literature on this topic and by having discussions with experts in this area from Philips research.

As a result, a plan for the next year has been made, in which it was decided to focus on the so-called helper-data method for template protection. In the variant of that method that is currently used at Philips Research, the biometric features are quantized very coarsely with one bit. It has been decided to investigate the possibilities of a finer quantization, which is expected to result in a higher degree of security.

### 10.2.2 Biometric Identification

Biometric template protection requires fixed-length feature vectors with known statistics. Therefore, two problems are addressed. First, this WP investigates the extraction of robust well-discriminating new types of fixed-length feature vectors. Fingerprint recognition is often based on variable-length feature vectors, describing characteristic points called minutiae. The work package investigates methods to encode minutiae sets in fixed-length feature vectors that can be used as a basis for template protection. The new feature vectors may also be based on other characteristics, such as (multi-resolution) shape and (transformations of) gray-scale information.

The second topic of this work package is to address the problem of estimating the relevant statistics given a limited number of training examples. Two classes of solutions to this problem can be identified. The first is to develop classifiers that are less sensitive to this problem. The second is to optimize the transform prior to classification.

**Progress** From August 1, 2005 until end 2005 Haiyun Xu has studied the concept of spectral-minutiae matching, which is a method for generating fixed-length feature vectors from variable-size minutiae sets. This is a candidate method to be used in combination with template protection, but it requires some improvement and refinement in order to achieve the recognition performance of standard minutiae-based fingerprint recognition. Possible points of improvement have been identified and a plan for further investigation of the method has been made.

### 10.2.3 Demonstrator

The results of WPs 1 and 2 will be validated in a home-network demonstrator, which will be realized at Philips Research. This will connect devices such as DVD players, TV sets, etc.

**Progress** At Philips Research, Tom Kevenaer has been working on this demonstrator. A version running on a notebook computer, demonstrating the combination of template protection and fingerprint recognition has been finalized.

## 10.3 Utilization report for the previous year

Development of knowledge (in Dutch: "kennisontwikkeling")

A better understanding of template protection has been achieved. A potential method to generate fixed-length feature vectors from variable-size minutiae sets has been identified.

---

Development of competence core areas (in Dutch: "zwaartepuntvorming")

Philips Research and the University of Twente are in the process of intensifying their cooperation. For this purpose, an additional research proposal has been submitted to the Sentinels program. The topic is biometric recognition with a substantially lower false-accept rate at a given false-reject rate. This is prerequisite for good-working template protection.

Creation and expansion of networks (in Dutch: "netwerkvorming")

Both UT and Philips take part in the Dutch and European Networks in the areas of Biometrics and Template Protection, e.g. NBF, BioSecure. Contacts within these networks will, of course, be maintained and, when necessary, be intensified and extended.

Knowledge dissemination (in Dutch: "kennisoverdracht")

Several presentations on template protection have been given by Ton Akkermans and Tom Kevenaer (Philips Research), and by Haiyun Xu and Chun Chen (UT). One paper, describing the concept of template protection, has been published [1].

Anchoring of knowledge resulting from the program (in Dutch: "verankering")

The knowledge will (have to) be anchored in the permanent staff of Philips Research, because Philips has the intention to use the results from the Sentinels project for privacy enhancing in digital rights management (DRM) systems in the home, but wants to implement these techniques also in stand-alone CE devices.

#### **10.4 Contacts with third parties**

None, except the regular contacts with Philips Research.

#### **10.5 Press coverage**

None.

#### **10.6 Publications**

- [1] P. Tuyls, A.H.M. Akkermans, T.A.M. Kevenaer, G.-J. Schrijen, A.M. Bazen, and R.N.J. Veldhuis. Practical biometric authentication with template protection. In *Proceedings of the 5th International Conference on Audio- and Video-Based Personal Authentication (AVBPA)*, pages 436–441, Rye Brook, NY, July 2005.

## 11 VIT.6684, DeWorm, Worm monitoring on Internet backbones

---

Author: Herbert Bos

DeWorm is aimed at developing an automated response system that is capable of (1) detecting zero-day worms on the Internet, (2) generating signatures for the attacks, and (3) using these signatures to block malicious traffic. The goal is to make it fast enough to react to fast-spreading worms. We do this by means of two tiers. In tier I, traffic on fast links that is considered (somewhat) suspect is steered towards a deep scan node (Tier II) for detailed analysis. The deep scan node analyses the traffic and generates signatures if it finds the traffic malicious.

### 11.1 Administrative details

- project number: VIT.6684
- title of the project: DeWorm, Worm monitoring on Internet backbones
- name project leader: Herbert Bos
- website: [www.cs.vu.nl/~herbertb/projects/deworm](http://www.cs.vu.nl/~herbertb/projects/deworm)
- names and fte's of personnel on the project:
  - Funded by Sentinels:
    - \* Georgios Portokalidis, AIO, VU, 1 fte, since 15-4-2005
  - Funded by other sources:
    - \* dr. ir. Herbert Bos, VU
    - \* Joanna Slowinska, AIO, VU, funded by the FP6 Noah project that collaborates with DeWorm
- names and affiliations of members of the user committee: we have invited the following people:
  - \* Hedy van der Ende (GOVCERT.nl)
  - \* Rogier Spoor (SURFnet)
  - \* Rutger Coolen (TNO Telecom)
- dates of the user committee meetings: we have had meetings with TNO about DeWorm, but no official user committee meeting.

### 11.2 Research report for the previous year

As the two-tier approach has gained some popularity since the project was accepted, we decided to focus primarily on the task of detecting the attacks and generating signatures in the initial phases. The reason for doing so, is that we believe that there is much to contribute in this area. It is clear that there are some important constraints for our work. For example, we believe that avoiding false positives is of the essence if the architecture is to be used as an automated response system. Also, we need to beat fast-spreading worms, so the system would need to be able to respond within minutes to a zero-day attack.

The motivation for the above constraints and our approach to deal with them is two-fold. The rate at which self-propagating attacks spread across the Internet has prompted a wealth of research in automated response systems (ARS). We have already encountered worms that spread across the Internet in as little as ten minutes, and researchers claim that even faster worms are just around the corner. For such outbreaks human intervention is

---

too slow and automated response systems are needed. Important criteria for such systems in practice are: (a) reliable *detection* of a wide variety of zero-day attacks, (b) reliable and timely generation of *signatures* that can be used to stop the attacks, and (c) *cost-effective* deployment.

However, even though a fair amount of effort was spent on developing ARS architectures, the industry has been slow or even reluctant to pick them up. The reason is that existing automated response systems tend to incur a fairly large ratio of false positives in attack detection and use of signatures. A large share of false positives violates the first two criteria. Although these systems may play an important role in intrusion detection systems (IDS), it is problematic to apply them in fully automated response systems.

One approach that attempts to avoid false positives altogether is known as dynamic taint analysis. Briefly, untrusted data from the network is tagged and an alert is generated (only) if and when an exploit takes place, e.g., when data coming from the network are executed. This technique proved to be very reliable and to generate few, if any, false positives.

Current work in this area is at a level that is either too low (e.g., in the hardware: Minos), or too high (e.g., at the process level: Vigilante). When one deploys the detection mechanism in the hardware it becomes harder to spot high-level events (e.g., virtual addresses, process-specific information, etc.) and thus to generate signatures. Similarly, when one deploys the detection mechanism on a per-process basis one does not spot low-level aspects, such as physical addresses. Because of this it is difficult to deal with memory that is mapped in multiple address spaces, DMA, etc. Moreover, protection at the process-level leaves the kernel vulnerable to attacks. This is unacceptable as we have already seen kernel exploits in practice.

In this first year we developed a prototype architecture, known as Argos (co-funded by the EU FP6 Lobster project), that explores another extreme in the design space for automated response systems. First, like Minos we offer whole-system protection in software by way of a modified x86 emulator which runs our own version of dynamic taint analysis. In other words, we automatically protect any (unmodified) OS and all its processes, drivers, etc. Second, we want to take into account complex memory operations, such as memory mapping and DMA (commonly ignored by other projects), while at the same time we want to be capable of handling complex exploits (such as register springs). For this we need to be able to handle both virtual and physical addresses. Third, buffer overflow and format string/code injection exploits trigger alerts that will eventually result in the automatic generation of signatures (initially based on the correlation of the exploit's memory footprint and its network trace). The third point is still work in progress.

As these goals are ambitious and because we want the research to have real impact, we collaborate with the EU FP6 Noah project to develop a joint containment environment based on the above description. Since the Vrije Universiteit is responsible for this task in both projects, this is relatively easy to accomplish. The EU FP6 has now chosen Argos as the architecture of choice for building a honeypot.

Note that for DeWorm the containment environment is the first, albeit very important, step in the development. It represents what we have termed Tier II above. The next phase

---

of the project will also look at Tier I.

### 11.3 Utilization report for the previous year

We released our first prototype just before Christmas in 2005. In this short time, the Argos prototype has been picked up and deployed at several sites worldwide. SURFnet is in the process of installing it. And we received feedback from both the HoneyNet project and the Nepenthes team (both provide well-known honeypot systems).

#### Development of knowledge (in Dutch: "kennisontwikkeling")

We have studied the taint analysis method to see how well it can be applied to an emulator-based ARS, which provides full-system protection but by its nature has no knowledge about processes (after all, it sits underneath the operating system). The conclusion is that it seems well-suited. An idea that we are still exploring (both in the EU FP6 Noah project and in the Sentinels DeWorm project) is to perform process-specific forensics at the time of detecting an attack. This is a novel idea that would help the system gather around the problems in systems such as Minos, where the 'viewpoint' is inherently too low.

#### Development of competence core areas (in Dutch: "zwaartepuntvorming")

We expect to develop knowledge that is beyond state of the art especially in the area of network intrusion detection and signature generation. Our approach should help us develop honeypots that generate with extreme accuracy signatures for new attacks.

#### Creation and expansion of networks (in Dutch: "netwerkvorming")

The DeWorm project has attracted attention from a number of external parties. Besides TNO, we have serious interest from various NRENs. For example, SURFnet in the Netherlands has requested collaboration and they are in the process of installing an Argos node. In addition, other honeypot teams around the world have responded enthusiastically. In particular, the Nepenthes and HoneyNet development teams have tested Argos. The feedback has been quite positive.

In addition, after presenting our thoughts on worm containment, the EU FP6 Noah project agreed to co-develop Argos. This is extremely important as it allows us to tackle many more issues than would have been possible in a smaller setting. Also, it knits close ties with a large number of leading European research organisations. In addition, it ensures a greater impact of the work. In both projects, the Vrije Universiteit leads the development effort.

#### Knowledge dissemination (in Dutch: "kennisoverdracht")

There has been extensive coverage in the popular press of the security projects by the PI, which also included coverage of the DeWorm project.

There were several interviews and news items on national radio (Radio 1, 3FM, and 747 AM), interviews in the magazine 'Computable', and the online magazine 'EduSite'. Recent interest was shown by national newspapers and more radio stations, but the publication occurs in the beginning of 2006.

---

Recently, we wrote an article for the Dutch computer magazine 'Informatie' which featured the approach taken by DeWorm. Smaller items appeared in various papers and computer magazines. We also presented the DeWorm approach by means of a poster session at the Sentinels Security Dag in September and a presentation at a NoAH project meeting. In addition, we have submitted a paper on the containment architecture to the EuroSys conference. Finally, we plan to have a user committee meeting to distribute knowledge to the organisations that are closely associated with DeWorm, as well as to request feedback. Finally, Argos featured in discussion lists on the Internet, and an installation guide was written by the Nepenthes development team which is now online.

Anchoring of knowledge resulting from the program (in Dutch: "verankering")

The expertise generated by the program is already making its way in several projects. In turn, it is itself embedded in the security research conducted at the Vrije Universiteit, SURFnet, and TNO. The VU has a strong track record in systems work for security, as witnessed for example by Prof. Tanenbaum's keynote speech at the SOSPC conference in October this year, where he highlighted a push to create safe operating systems, and the problems of security in RFID tags. The DeWorm project fits nicely in this research domain as it tries to guarantee safety in the world of legacy operating systems (whether they use RFID or other devices is immaterial), and its methods of detection may fit the development of secure operating systems. Moreover, an important research effort by the PI in recent years has been the monitoring of network traffic for worm signatures. For instance, we developed a fast intrusion detection system on a network card and an efficient and flexible network monitoring system that allows one to detect signatures and filter traffic. In addition, TNO has its own network-based intrusion detection system (NERD) that could be conveniently used to steer traffic towards our containment environment. The containment environment that is currently being designed is therefore complementary to what is provided by NERD and may help to increase NERD's fidelity.

#### **11.4 Contacts with third parties**

We have close contacts with all parties in the EU FP6 NOAH project which is co-developing DeWorm's Argos architecture. In particular there are ties with FORTH in Greece, DFNCert in Germany, TNO in the Netherlands, and ETH in Zurich. In the Netherlands we also have strong links with SURFnet (which is installing an Argos node) and GOVCERT.nl.

#### **11.5 Time line and events**

- 04/2005: Start
- 2005: Study of literature and initial design of a containment environment (done).
- 01/2006: Core implementation of detection (done).

#### **11.6 Press coverage**

There were several interviews and news items on national radio (Radio 1, 3FM, and 747 AM), interviews in the magazine 'Computable', and the online magazine 'EduSite'.

---

Recent interest was shown by national newspapers and more radio stations, but the publication occurs in the beginning of 2006.

Recently, we wrote an article for the Dutch computer magazine 'Informatie' which featured the approach taken by DeWorm. Smaller items appeared in various papers and computer magazines (see e.g. in chapter 1).

## 12 TIF.6687, PINPAS JC, Program INferred Power-Analysis in Software for Java Card

---

Author: dr. E.P. de Vink

The PINPAS JC project studies side-channel attacks on smartcards, in particular fault attacks for the JavaCard platform. Various fault-based and related attacks will be assessed on their impact for JavaCard, both at the source code as well as the byte code level. The formal method JML will be used to specify security requirements and to prove safety of reference applets. In order to facilitate experiments a software environment will be constructed. This tool can also be exploited for the validation of the impact rating and counter measures developed during the project.

### 12.1 Administrative details

- project number: TIF.6687
- title of the project: PINPAS JC, Program INferred Power-Analysis in Software for Java Card
- name project leader: dr. E.P. de Vink
- website: [www.win.tue.nl/pinpasjc](http://www.win.tue.nl/pinpasjc)
- names and fte's of personnel on the project:
  - Funded by Sentinels:
    - \* Wojciech Mostowski, postdoc, RUN, 1 fte, since 1-9-2005
    - \* Jing Pan, AIO, TU/e, 1 fte, since 1-10-2005
    - \* Srikanth Akkiraju, AIO, UT, 1 fte
  - The Ph.D.-student at UT has been selected and is expected to start March 2006.
  - Funded by other sources:
    - \* J. den Hartog, UT, 0.1 fte
    - \* E. Poll, RUN, 0.1 fte
    - \* E. de Vink, TU/e, 0.1 fte
    - \* J. de Vos, TNO ITSEF, 0.2 fte
    - \* J. Daemen, ST MicroElectronics, p.m.
    - \* P. Dumoulin, ST MicroElectronics, p.m.
- the user committee will be formed in 2006.

### 12.2 Research report for the previous year

Wojciech Mostowski and Jing Pan have been working on two conference submissions and a journal paper on verification of security properties of JavaCard using dynamic logic. This work is in part based on the two researchers' Ph.D. thesis and Masters thesis, respectively. Experiments have been started with the source code analyser FingBugs to explore the possibility of automating enforcement of industry security guidelines for Java Card programs. The initial goals are to find out which guidelines could be enforced by such static analysis and how much effort it is to develop such automated support.

Initial investigations have been launched for the assessment of side-channel vulnerability of quasigroup based cryptographic algorithms as proposed by Smile Markovski (Sts. Cyril and Methodius University Skopje) and co-workers. The research will focus on the block cipher representative from the Edon family and DPA.

---

### **12.3 Utilization report for the previous year**

#### Creation and expansion of networks

Erik Poll and Erik de Vink have joined the board of IFIP Working Group 11.2 on Small Systems Security.

#### Knowledge dissemination

Erik Poll gave a tutorial at the “Smart University”, which was organised as part of the industry conference e-Smart’2005 held in Sophia-Antipolis, France on September 21-23, 2005. This initiative is aimed to participants from industry. The tutorial was in the track “Advanced Java Technologies” and was on the topic “Formal Methods and Java Card Modelisation”.

### **12.4 Contacts with third parties**

On December 12, 2005 the project team visited Riscure in Delft.

### **12.5 Time line and events**

An informal kick-off with academic partners was held on November 9, 2005 in Eindhoven.

### **12.6 Press coverage**

None.

## References

---

1. Rik D.T. Janssen, "Sentinels in a nutshell". [www.sentinel.nl/sentinelsnutshell.pdf](http://www.sentinel.nl/sentinelsnutshell.pdf).
2. P. Hartel, R.D.T. Janssen and B. Jacobs, "Sentinels, Security in ICT, networks and information systems", Version 3.1, August 27, 2003. [www.sentinel.nl/sentinels.pdf](http://www.sentinel.nl/sentinels.pdf).
3. R.D.T. Janssen, "Sentinels year plan 2004". [www.sentinel.nl/library/yearplan2004.pdf](http://www.sentinel.nl/library/yearplan2004.pdf).
4. R.D.T. Janssen, "Sentinels year plan 2005". [www.sentinel.nl/library/yearplan2005.pdf](http://www.sentinel.nl/library/yearplan2005.pdf).
5. R.D.T. Janssen, "Sentinels year plan 2006". [www.sentinel.nl/library/yearplan2006.pdf](http://www.sentinel.nl/library/yearplan2006.pdf).
6. R.D.T. Janssen, "Sentinels year report 2004". [www.sentinel.nl/library/yearreport2004.pdf](http://www.sentinel.nl/library/yearreport2004.pdf).