

Application for Incident Response Teams

<http://www.uvt.nl/infolab/airt>
airt-dev@uvt.nl

Kees Leune
Tilburg University
Infolab, room B 738
P.O. Box 90153
5000 LE Tilburg

Presentation outline

- > **Outline**
- > Goals and Design Philosophy
- > Features
- > Demonstration
- > Q&A

- Presentation Outline
- AIRT Goals and Design Philosophy
- Features: Available and planned
- Demonstration
- Q & A

AIRT Goals

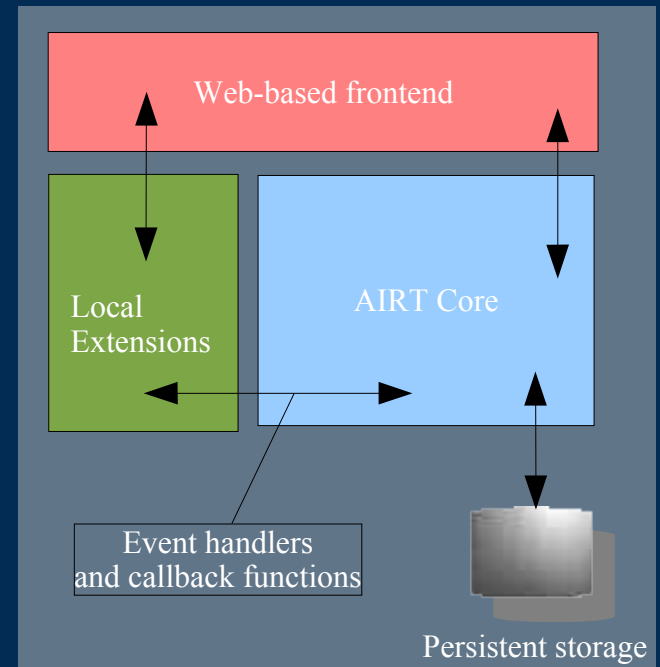
- > Outline
- > **Goals and Design**
- > **Philosophy**
- > Features
- > Demonstration
- > Q&A

- Developed as a collection of separate tools for use by UvT-CERT
- Goal: to develop a support system for incident handling which meets the following criteria:
 - > Creation of new incident in under 30 sec
 - > Comprehensive overview of open incidents
 - > Integration with existing tools
 - > Support for *outgoing* email via templates

Design Philosophy

- > Outline
- > Goals and Design Philosophy
- > Features
- > Demonstration
- > Q&A

- Open
- AIRT-core providing application logic and extension points
- Database-driven
- Extensions which *add* functionality
- Extensions which *alter* functionality
- Human-usable
- Machine-usable



- Community-driven development
- GNU General Public License

AIRT Core Features

- > Outline
- > Goals and Design
- > Philosophy
- > **Features**
- > Demonstration
- > Q&A

- Incident management console
- Networks, constituencies and constituency contacts
- Incident types, states and statuses
- Email templates with PGP GnuPG signing support
- Import queue
- Asynchronous command execution

- > Outline
- > Goals and Design
- > Philosophy
- > **Features**
- > Demonstration
- > Q&A

- Automatic importers: Cymru/Flitspaal, MyNetwatchman, Spamcop, Honeyd logging, nmap logging, Nessus logging, other AIRT installations
- Router/firewall/switchport configuration, DHCP server configuration
- Integrated RSS Reader and Wiki environment in management console
- XML SOAP interface to AIRT-Core
- Integration with A-Select for Single Sign-On
- Authentication with client certificates

- > Outline
- > Goals and Design
- > Philosophy
- > Features
- > **Demonstration**
- > Q&A

Honeyd logging indicated a portscan (output generated by local Perl script)

```
Source ip   : 202.116.160.60
Source name: ftp1.scau.edu.cn
time=2005-08-01-13:04:27+0200 proto=tcp dstip=137.56.127.119 dstport=3306
time=2005-08-01-13:04:27+0200 proto=tcp dstip=137.56.127.118 dstport=3306
time=2005-08-01-13:04:27+0200 proto=tcp dstip=137.56.127.120 dstport=3306
time=2005-08-01-13:04:27+0200 proto=tcp dstip=137.56.127.121 dstport=3306
time=2005-08-01-13:04:28+0200 proto=tcp dstip=137.56.127.121 dstport=3306
time=2005-08-01-13:04:28+0200 proto=tcp dstip=137.56.127.120 dstport=3306
time=2005-08-01-13:04:28+0200 proto=tcp dstip=137.56.127.118 dstport=3306
time=2005-08-01-13:04:29+0200 proto=tcp dstip=137.56.127.121 dstport=3306
time=2005-08-01-13:04:29+0200 proto=tcp dstip=137.56.127.120 dstport=3306
time=2005-08-01-13:04:29+0200 proto=tcp dstip=137.56.127.118 dstport=3306
time=2005-08-01-13:04:30+0200 proto=tcp dstip=137.56.127.119 dstport=3306
```

- > Outline
- > Goals and Design
- > Philosophy
- > Features
- > Demonstration
- > Q&A

- Additional Questions and Answers?

Kees Leune
Tilburg University
Infolab, room B 738
P.O. Box 90153
5000 LE Tilburg

kees@uvt.nl
PGP Key: 2FBA3620