

# Curriculum Vitae

NAME	Arthur Donkers
DATE OF BIRTH	April 13, 1963
NATIONALITY	Dutch
LANGUAGES	Dutch (native) English (written and spoken) French, German (both spoken)
LAST UPDATE CV	December 1, 2004

---

## Education

Technical University of Delft, department Electrical Engineering, Specialisation Computer Architecture.

Independent entrepreneur since 1991, founder and owner of *Le Reseau netwerksystemen BV*, an independent bureau for (technical) Intrusion testing, education and research. Since February 1, 2003 operating as an independent architect, auditor and tester for *Arthur Donkers Informatiebeveiliging*.

RedHat Certified Engineer (RHCE) registration number 803004154312365

## General information

Because of his entrepreneurship Arthur is able to prioritise, work independently or in a team and separate details from main issues. He is a good communicator (both for technical as well as management issues) and very stress resistant.

For all projects described below the technical challenges have been important as well as the project management, proper reporting and presentation of the results to the customer.

Because of his vast technical experience and architectural skills, Arthur is capable of focussing both on the fine details and the global design level.

Arthur has been using Linux and developing for Linux for more than 9 years. He is one of the early adaptors in the Netherlands and has participated in promoting Linux and OpenSource.

Currently Arthur is preparing for his CISSP and CEH exams via self study and test exams.

## Skills

- Project management, reporting of complex security issues in large scale organisations, translating technical security risks into business risks.
- Network, System and Security Architectures, Firewalls, Intrusion Detection Systems, cryptography, PKI, smartcards, LDAP.
- Performing Intrusion tests, Risk assessments, network audits and organisational EDP audits.

- Drafting and implementing Security Policies, Standards and procedures, both on the tactical and operational level.
- Drafting and reviewing Security Architectures.
- Operating systems (Solaris, \*BSD, HP-UX, Linux, AIX, VMS), network components (switches, routers, especially Cisco), extensive knowledge of TCP/IP protocols (Internet and Web based technologies).
- Windows (Windows NT4, Windows 2000, Windows 2003, XP), Active Directory, SQL server, Information Server, ISA server, Exchange, Clustering.
- Application environments based on Apache, PHP and MySQL, VMware applications, honeypots.
- Safe programming techniques (C(++), Java, Perl, shell-scripts).
- Code reviews on Java, C(++), Perl applications.
- Programming Perl, C, C++, Unix Shells, AWK, Visual Studio 6, Visual Studio .NET, i386 assembler.
- Forensics.
- Tool development, especially for performing specific intrusion tests (on the spot development) throughout most of the intrusion tests.
- Exploit analysis and adaptation for specific intrusion tests, and for the alerting service.

### Working history

- Independent contractor for Security, Architecture and Management. 2003 – current
- Senior Security consultant for *Le Reseau netwerksystemen BV*, 1995 – 2002  
Groningen/ Amsterdam, The Netherlands.
- Freelance system specialist for UNIX, VMS en TCP/IP. 1992 – 1995
- Partner in system integration company for UNIX and Microsoft 1991 – 1992  
solutions.
- System analyst and developer for BSO-AT/Rotterdam, The 1988 – 1991  
Netherlands.
- System developer for ICT Novotech, Rotterdam, The Netherlands 1986 – 1988

### Recent projects

- |                  |   |
|------------------|---|
| September 2004 – | Designing and implementing an Intrusion Detection Network with multiple sensors (based on Snort) and one management console (based on ACID). This management console can be used to generate reports and monitor the proper functioning of the sensors. |
| December 2004    | Security review of new IT Architecture proposal and RFP documents for hospital, focussing on security and management issues.  |
| October 2004     | Security assessment of a Windows 2003 domain based network with Active Directory using covert techniques while working from the inside. For this same customer an Intrusion test on their web server  |

- environment was performed as well, as part of this project.
- July 2004 – Building a firewall infrastructure based on a Linux solution. These  
September firewalls are managed from a central management station using  
2004 FWBuilder. The installation of the firewalls has been automated and documented so they can be deployed quickly and reliably.
- January 2004 – Design, development and deployment of a generic tool to perform  
December system security hardening and control on Windows NT, 2000 and 2003.  
2004 Using this tool, vulnerabilities in a server can be detected, removed and checked. Using company specific policy compliance to the security standards can thus be enforced and maintained.
- July 2003 – Global Security Architect for the Command and Control Support Centre  
March 2004 (C2SC) of NLMOD. The goal of the project is to develop and deploy a new architecture, C3IA (Command, Control, Communications and Information Architecture), for the concept of Network Centric Warfare.
- June – July Classified assessment for NLMOD of an internal application.  
2003
- May 2003 Intrusion test on the new multivendor global network of SWIFT. This network is based on a VPN architecture using IPsec to build secure tunnels over unsafe networks. Using a complex Man in the Middle setup, it was possible to intercept and manipulate communications.
- May 2003 Installation and configuration of Windows 2000 Advanced Server cluster using Linux and VMware. A powerful Linux server with plenty of RAM and Hard disk storage can be used as a platform for running a number of virtual PC's in parallel using VMware. These virtual PC's can run a large number of different operating systems. The emulation of the virtual hardware is very good indeed. Using two of these virtual PC's and an emulated shared SCSI disk and network interface one can build a cluster with 2 Windows 2000 servers. This can then be used for demonstration and training purposes.
- January 1998 – Design, implementation and management of a great variety of multi  
January 2003 vendor networks using a combination of Linux, Solaris, Windows and OpenBSD for office automation, safe Internet and intrusion testing for Le Réseau and her customers. Using a combination of xDSL and IPsec for secure connections over the Internet. A large variety of systems and applications is being used in this environment, Linux and Samba (using Windows authentication), Apache and PHP, different versions of Windows (NT4, 2000 and 2003) with Terminal Services, and Solaris (2.6 t/m 9).
- April 2003 – Internal research project with Windows 2003 (RC1 and RC2), focussing  
April 2003 on new features and security.
- April 2003 – Intrusion test on the new global office network of SWIFT. The

- April 2003 architecture of this network is based on a Windows 2000 domain infrastructure, using Active Directory.
- February 2003 – March 2003 Designing and deploying a secure Terminal Server solution using .NET server (RC1/RC2) and XP/2000 systems (internal use). Using a secure web server, users authenticate themselves and are then transferred via a tunnel to the terminal server. This enables them to work wherever they want without sacrificing security.
- February 2003 – March 2003 Performed a number of reviews on the architecture of the new VPN network of SWIFT. This network enables SWIFT's customers to perform transactions over public networks in a secure and controlled manner.
- January 2003 – January 2003 Participated in a tender and performed pre audits for a large Intrusion test on the pilot environment for an integrated network for police, fire-fighters and ambulances. Le Reseau has operated as a subcontractor for Getronics where all technical aspects were the responsibility of Le Reseau. Especially for this project a screening by ITO (central IT department of the Dutch Police force) has been done.
- January 2003 – January 2003 Performing a risk assessment on the Wide Area Network for the Dutch Royal Navy. This was a follow up audit that focussed on the security of the management systems and network. This management network uses IPsec and an AAA solution to make sure only authorized systems managers are allowed access. This assessment has been performed on behalf of Defac (Defensie Accountantsdienst, the auditing department of the Dutch Ministry of Defence).
- August 2002 – January 2003 Performing a risk assessment on the LAN 2000 environment of the NLMOD (NL Ministry of Defence). LAN 2000 is the new office automation system that is based on a combination of NT4 and different supporting tools. This is a completion of the assessment done earlier.
- January 2002 – December 2002 Development of a number of applications for internal use at Le Reseau. These applications are based on a combination of Apache, PHP(4), MySQL, Perl and OpenLDAP and are used as a central alerting service and knowledge base. Customers of Le Reseau could take a subscription to this service and be alerted of new threats and exploits.
- August 2002 – November 2002 Performing a risk assessment on the LAN 2000 environment of the NLMOD (NL Ministry of Defence). LAN 2000 is the new office automation system that is based on a combination of NT4 and different supporting tools. This is a completion of the assessment done earlier.
- October 2001 – June 2002 Security advisor in a project for building an ePortal for students in the Netherlands. All students are registered to be able to claim financial support during their studies. This central administration is done by IBG (Informatie Beheer Groep, the agency responsible for student loans). The IBG wanted to be able to deliver personal information to students via a

- web portal. To build such a portal a special project was started and this project needed a security architect/advisor. It was decided to build an authentication system based on a combination of LDAP and GSM phones. Each student can register his or her phone number and whenever he or she wants to connect to the portal a password is sent to the phone using SMS.
- January 2000 – Performing dozens of audits, assessments and intrusion tests on Internet  
December applications, firewalls web servers, external and internal networks.  
2002 These ‘targets’ were based on Linux, Windows, Novell and/or VMS, ranging from small to large networks.
- August 2002 – Performing an Intrusion test on the new Internet firewall of NLMOD,  
October 2002 based on a combination of Firewall-1, Raptor and proxy systems. Both the technical implementation has been tested using advanced Intrusion testing techniques (firewalking, source port manipulation, fragmentation, ICMP tunnelling) as well as the architecture has been reviewed.
- May 2002 – For a number of banks analyses have been done on the use of  
August 2002 cryptography in their Internet banking applications. Code reviews have been performed and the management of certificates (PKI) have been analysed.
- November A risk assessment has been done for NLMOD on the new ‘Internet at the  
2001 – April office’ system. This system is based on a Citrix, Firewall-1 and Cache  
2002 flow proxies. Both the architecture has been reviewed as a number of advanced Intrusion tests have been performed.
- April 2001 – A risk assessment has been done for NLMOD on their new ‘VPN  
October 2001 gateway’ firewall. This will become their standard solution for connecting different networks with different classifications. Apart from a number of advanced Intrusion tests, also a code review on the crypto part of the Firewall-1 source code has been done in Israel at CheckPoint’s office.
- January 2000 – A large number of classified audits for NLMOD.  
December  
2002
- January 2000 – Intrusion test on an Internet banking application. The use of SSL in both  
April 2000 the web server as the Java applet was the focus of this test. As it turned out a number of bugs in the Netscape browser were discovered that enabled an attacker to spoof a server certificate and perform a Man in the Middle attack. From the reverse compilation and subsequent code review of the Java applet it was proven that the certificate handling in the applet was flawed as well.

**Relevant presentations/workshops**

- October 2004 – Teaching a 2 day workshop (split up in four sessions of 4 hours each) to introduce security awareness into an IT company. This workshop has been developed and given in-house and covers the basic disciplines of Policy Management, Measures and Enforcement, Control and Testing.
- November 2004
- May 2001 *Hoe vang ik een Linux worm (dutch, How to catch a Linux worm) ?*, presentation at the Linux 2001 symposium about building and maintaining a honeypot for luring hackers, Reehorst Ede, The Netherlands.
- May 2001 *Bedreigingen in perspectief (Dutch, threats in perspective)*, presentation at the NGN theme day on security, Jaarbeurs Utrecht, The Netherlands.
- 2001 – 2002 Developer of a course on *VPN* and course on *Web Security*. These courses were developed for IIR training, Maarsssen, The Netherlands.
- April 2001 *Hackers in e-Commerce*, presentation for Global E-Commerce Masters education at Erasmus Universiteit, Rotterdam, The Netherlands.
- 2000 – 2002 Trainer 3 day course *Netwerkbeveiliging (Network security)*. This course is given by IIR Training, Maarsssen, The Netherlands.
- 1998 – 2002 Developer and trainer for a number of different hands-on security workshops, focussing on the security of Internet and web environments.
- 2000 – 2002 Developer and trainer for the *Anti-Hacking (Advanced) Workshop*, a hands-on security workshop.
- 2002 Developer and trainer for a dedicated *Anti-Hacking (Advanced) Workshop*, for DNB (De Nederlandse Bank), the Dutch National Bank.

**Publications**

- 2000 – 2001 *Different articles on security (Dutch), Automatiseringsgids*
- 1995 – 2000 *Many articles on Unix, Linux and Security (English), Sysadmin magazine, USA*

**Other**

Screened by NLMOD for level A (top secret), very familiar with NLMOD organisation.  
Screened by ITO (police ICT department).

Member of PI workgroup on *Encryption* and member of workgroup on *Windows 2000*.  
Former member workgroup on *Internet security* of PI. PI is “*Platform Informatiebeveiliging*”, a Dutch association of companies which is dedicated to drafting standards and handouts on different issues relating to information security.

Arthur is currently preparing for his CISSP exam in December.

