

DNSSCurve Analysis

J. Scheerder*

jeroenscheerder@on2it.eu

November 10, 2008

1 Introduction

In the recent past fundamental design flaws in the DNS protocol have been exposed¹.

DNSSCurve² is a proposal to address these fundamental problems. It promises to guarantee confidentiality and integrity of DNS traffic, as well as protect against attacks on service availability. It should be possible to add DNSSCurve functionality unobtrusively: as a forwarder to front DNS servers, and as a recursive DNS-resolver for DNS clients.

2 Goal

Achieve a deep grasp of DNSSCurve, and a clear and concrete path for DNSSCurve adoption.

3 Task

Analyze the DNSSCurve architecture, implementation status and issues, inventarize implementation and deployment requirements, and discuss a 'governance model' that encourages widespread DNSSCurve deployment.

*ON2IT b.v., Waardenburg, The Netherlands.

¹Widely reported as the "Kaminsky Bug".

²See <http://dnsscurve.org/>.

ON2IT Company Profile

J. Scheerder*

jeroenscheerder@on2it.eu

L.J. Koning*

lieuwejankoning@on2it.eu

October 25, 2007

1 Inleiding

ON2IT is a young, rapidly growing specialist in information security. It operates in close relation with a select few prominent security vendors. The product portfolio comprises Unified Threat Management solutions (i.e. next-generation firewall technology), Intrusion Detection and Intrusion Prevention Systems, Anomaly Detection Systems and Network Access Control.

The primary technology supplier is Internet Security Systems (ISS), recently acquired by IBM. ISS operates as an autonomous division within the IBM ISS Global Services group. ON2IT is one of only five worldwide Tier 1 technology partners, with direct access to ISS' researchers and developers in Atlanta.

Location: Waardenburg.

We seek students that

- have a passion for innovation;
- like living on the cutting edge;
- strive for excellence in the field.

We offer :

- a pleasant work environment;
- a possibility to get hands-on experience in the field with cutting edge security technology;
- great variety;
- a monthly fee;
- a position prospect;
- daily or weekly guidance, dependent on person and project.

2 Projects

Projects are defined in close cooperation between student and ON2IT, in a clear, precise and concise manner. Tasks vary from research into market trends to implementing integral security-related systems. Examples of typical tasks:

- developing extensions to security analysis software;
- portal development using AJAX, etc.;
- implementation of reporting mechanisms and technology for HIPAA, SOX, ...;
- advancing technical infrastructure for mail security, VPN, authentication, ...;
- impact-analysis of Intrusion Detection en Prevention in the context of Managed Security, with respect to SOX (ISO17799, BS7799, NEN27001), HIPAA (NEN7510/11/12), ...;
- examining aspects of desktop security management using common software mechanisms and packages in relation to structural Network Access Control;
- strengthening security by deploying Intrusion Detection en Prevention for entire network infrastructure, or partially – e.g. only for a web site of an E-commerce company.

3 We require

- basic skills and knowledge in general networking, TCP/IP, routing, VPN;
- solid command of Dutch and English;
- extensive hands-on familiarity with Unix/Linux and the usual bunch of scripting languages.

*ON2IT b.v., Waardenburg, The Netherlands.