

Curve25519 Cryptanalysis

J. Scheerder*

jeroenscheerder@on2it.eu

December 1, 2008

1 Introduction

In the recent past fundamental design flaws in the DNS protocol have been exposed. DNSCurve¹ is a proposal to improve upon the current situation.

Essential to DNSCurve is Curve25519, which is claimed to be a high-speed, high-security elliptic-curve-Diffie-Hellman function².

Now consider the following definition of the so-called *safety factor*:

Let n be the number of rounds of the full cipher, and b be the largest number of rounds that has been broken. The safety factor σ is defined as $\sigma := n/b$.³

2 Goal

Analyze the Curve25519 algorithm to assess its security claims. Describe the best attacks against it, as currently known, and determine its safety factor.

3 Task

Perform a cryptanalysis of the Curve25519 design and implementation. Formulate and implement attack strategies and specific attacks.

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

¹See <http://dnscurve.org/>.

²"Curve25519: new Diffie-Hellman speed records", Daniel J. Bernstein, 2006 – <http://cr.yp.to/ecdh/curve25519-20060209.pdf>.

³Taken from "The Twofish Team's Final Comments on AES Selection", Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson, Tadayoshi Kohno, and Mike Stay, 2000.

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.