Next-generation elliptic-curve cryptography (ECC)

Daniel J. Bernstein

Cryptographic Implementations group:

eindhoven.cr.yp.to

working closely with the

Coding Theory and Cryptology group:

www.win.tue.nl/cc/

Remote Timing Attacks are Still Practical*

Billy Bob Brumley and Nicola Tuveri

Aalto University School of Science, Finland
{bbrumley,ntuveri}@tcs.hut.fi

Abstract. For over two decades, timing attacks have been an active area of research within applied cryptography. These attacks exploit cryptosystem or protocol implementations that do not run in constant time. When implementing an elliptic curve cryptosystem with a goal to provide side-channel resistance, the scalar multiplication routine is a critical component. In such instances, one attractive method often suggested in the literature is Montgomery's ladder that performs a fixed sequence of curve and field operations. This paper describes a timing attack vulnerability in OpenSSL's ladder implementation for curves over binary fields. We use this vulnerability to steal the private key of a TLS server where the server authenticates with ECDSA signatures. Using the timing of the exchanged messages, the messages themselves, and the signatures, we mount a lattice attack that recovers the private key. Finally, we de-

More security failures in ECC standards

Search

OCHUM

A-Z | OVERVIEW | SEARCH | CONTACT

TWORK AND DATA SECURITY

RU

lications

PRACTICAL INVALID CURVE ATTACKS ON TLS-ECDH

Tibor Jager, Jörg Schwenk, Juraj Somorovsky

ESORICS 2015

ABSTRACT

Elliptic Curve Cryptography (ECC) is based on cyclic groups, where group elements are represented as points in a finite plane. All ECC cryptosystems implicitly assume that only valid group elements will be processed by the differ- ent cryptographic algorithms. It is well-known that a check for group membership of given points in the plane should be performed before processing.

However, in several widely used cryptographic libraries we analyzed, this check was missing, in particular in the popular ECC implementations of Oracle and Bouncy Castle. We analyze the effect of this missing check on Oracle's default Java TLS implementation (JSSE with a SunEC provider) and TLS servers using the Bouncy Castle library. It turns out that the effect on the security of TLS-ECDH is devastating. We describe an attack that allows to extract the long-term private key from a TLS server that uses such a vulnerable library. This allows an attacker to impersonate the legitimate server to any communication partner, after performing the attack only once.

The math splits into cases handled differently in software

JOURNAL OF NUMBER THEORY **53**, 229–240 (1995)

Complete Systems of Two Addition Laws for Elliptic Curves

W. BOSMA*

Department of Pure Mathematics, University of Sydney, Sydney, New South Wales 2006, Australia

AND

H. W. LENSTRA, JR.†

Department of Mathematics, University of California, Berkeley, California 94720-3840

The math splits into cases handled differently in software

laws on E exists. Indeed, a complete system of three addition laws, each consisting of bihomogeneous polynomials of bidegree $(2, 2)$, was exhibited explicitly by Lange and Ruppert [2; cf. 1]. In the present paper we show that there are complete systems consisting of *two* addition laws, and that both addition laws in such a system are necessarily of bidegree $(2, 2)$.

THEOREM 1. *The smallest cardinality of a complete system of addition laws on E equals two, and if two addition laws form a complete system then each of them has bidegree* $(2, 2)$.

We can describe all addition laws of bidegree $(2, 2)$. To do this, we omit the zero addition law, for which *all* pairs P_1, P_2 are exceptional, and we call two addition laws *equivalent* if there exists a non-zero element $d \in k$ such that the three polynomials in the first addition law are d times those in the second.

THEOREM 2. *There is a bijection between* $\mathbf{P}^2(k)$ *and the set of equivalence classes of non-zero addition laws of bidegree* $(2, 2)$ *on E that has the following property. If* $(a : b : c) \in \mathbf{P}^2(k)$ *and* P_1, P_2 *are points in* $E(K)$ *for some*

. . . or does it?

2007 Bernstein–Lange, for any non-square d:

The Edwards addition law

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}\right)$$

is a complete addition law on $E : x^2 + y^2 = 1 + dx^2y^2$.

. . . or does it?

2007 Bernstein–Lange, for any non-square d:

The Edwards addition law

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2}\right)$$

is a complete addition law on $E : x^2 + y^2 = 1 + dx^2y^2$.

This is one part of next-generation ECC. For more: see 2016 Bernstein–Lange paper “Failures in NIST’s ECC standards”.

Building next-generation ECC

2005 Bernstein:
X25519 encryption scheme
using new elliptic curve **Curve25519**.

Building next-generation ECC

2005 Bernstein:
X25519 encryption scheme
using new elliptic curve **Curve25519**.

2011 Bernstein–Duif–Lange–Schwabe–Yang: EdDSA signatures (generalized by 2015 Bernstein–Josefsson–Lange–Schwabe–Yang), and in particular **Ed25519** using Curve25519.

Building next-generation ECC

2005 Bernstein:
X25519 encryption scheme
using new elliptic curve **Curve25519**.

2011 Bernstein–Duif–Lange–Schwabe–Yang: EdDSA signatures (generalized by 2015 Bernstein–Josefsson–Lange–Schwabe–Yang), and in particular **Ed25519** using Curve25519.

2006, 2007, 2009, 2011, 2012, 2013, 2014, 2014, 2015, 2015, 2015: Curve25519 implementation papers from 23 authors setting speed records for conservative ECC on many different platforms.

Building next-generation ECC

2005 Bernstein:
X25519 encryption scheme
using new elliptic curve **Curve25519**.

2011 Bernstein–Duif–Lange–Schwabe–Yang: EdDSA signatures (generalized by 2015 Bernstein–Josefsson–Lange–Schwabe–Yang), and in particular **Ed25519** using Curve25519.

2006, 2007, 2009, 2011, 2012, 2013, 2014, 2014, 2015, 2015, 2015: Curve25519 implementation papers from 23 authors setting speed records for conservative ECC on many different platforms.

Also: new crypto library, new verification tools, . . .

Deployment: iOS, Signal, OpenSSH, Tor, QUIC, more

Things that use Ed2... ×

https://ianix.com/pub/ed25519-deployment.html

IANIX

Home About Public Services Privacy

Things that use Ed25519

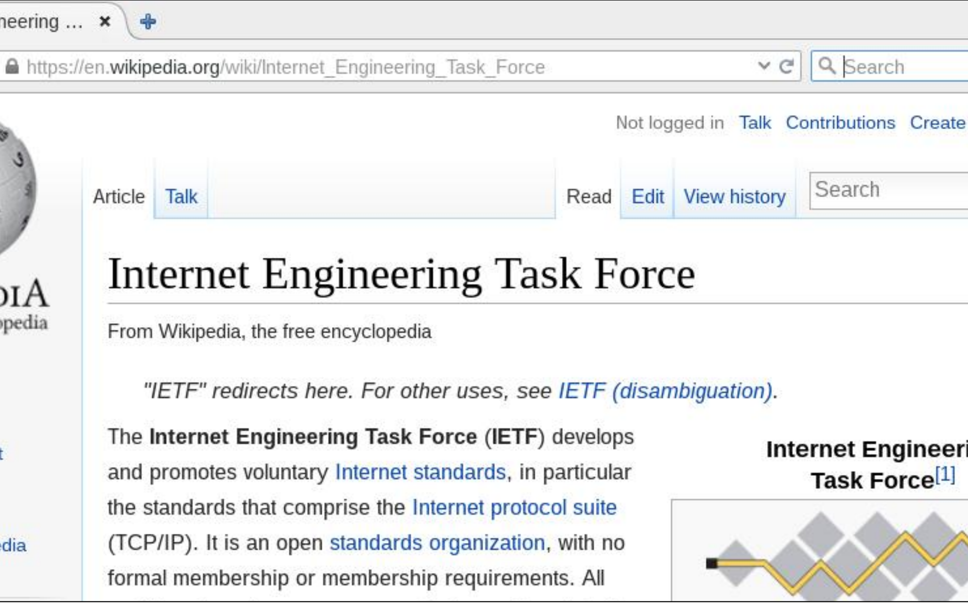
Updated: February 18, 2016

Here's a list of protocols and software that use or support the superfast, super secure Ed25519 public-key signature system from Daniel J. Bernstein, Niels Duif, Tanja Lange, Peter Schwabe, and Bo-Yin Yang.

You may also be interested in this list of Curve25519 ECDH deployment.

- **Protocols**
  - SSH — thanks to work done by the OpenSSH team, adopted also by TinySSH
  - RAET — (Reliable Asynchronous Event Transport) Protocol

The Internet standards committees start paying attention



. . . and delegate to their crypto unit, IRTF CFRG

earch Ta... ✖ ✚

https://en.wikipedia.org/wiki/Internet_Research_Task_Force

Search

Not logged in Talk Contributions Create

Article Talk Read Edit View history Search

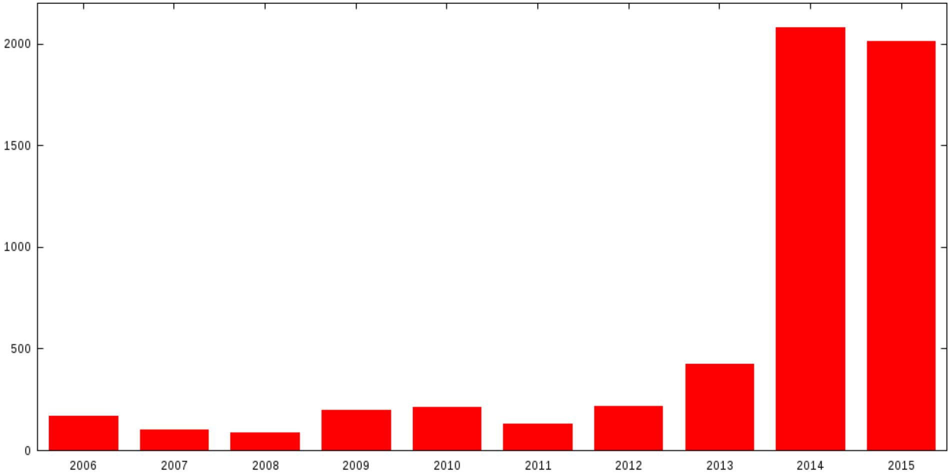
Internet Research Task Force

From Wikipedia, the free encyclopedia

The **Internet Research Task Force** (**IRTF**) focuses on longer term research issues related to the Internet while the parallel organization, the Internet Engineering Task Force (IETF), focuses on the shorter term issues of engineering and standards making. The Internet Research Task Force (IRTF) promotes research of importance to the evolution of the Internet by creating

Internet Researc Task Force

CFRG 2014+2015: >4000 messages, mostly on ECC



January 2016: RFC with next-gen curves + encryption

RFC 7748 - Elliptic C...

https://tools.ietf.org/html/rfc7748

Search

[Docs] [txt|pdf] [draft-irtf-cfrg-c...] [Diff1] [Diff2]

INFORMATIONAL

```
Internet Research Task Force (IRTF)                           A. Langley
Request for Comments: 7748                                        Google
Category: Informational                                       M. Hamburg
ISSN: 2070-1721                            Rambus Cryptography Research
                                                               S. Turner
                                                                   sn3rd
                                                            January 2016
```

Elliptic Curves for Security

Abstract

This memo specifies two elliptic curves over prime fields that offer a high level of practical security in cryptographic applications, including Transport Layer Security (TLS). These curves are intended to operate at the ~128-bit and ~224-bit security level, respectively.

Coming soon: RFC with next-gen signature system

draft-irtf-cfrg-eddsa-...

https://tools.ietf.org/html/draft-irtf-cfrg-eddsa-02

Search

[Docs] [txt|pdf] [Tracker] [WG] [Email] [Diff1] [Diff2] [Nits]

Versions: (draft-josefsson-eddsa-ed25519) 00
01 02

Network Working Group S. Josefsson
Internet-Draft SJD AB
Intended status: Informational I. Liusvaara
Expires: July 22, 2016 Independent
January 19, 2016

Edwards-curve Digital Signature Algorithm (EdDSA)
draft-irtf-cfrg-eddsa-02

Abstract

The elliptic curve signature scheme Edwards-curve Digital Signature Algorithm (EdDSA) is described. The algorithm is instantiated with recommended parameters for the Curve25519 and Curve448 curves. An

Coming soon: standardizing next-gen ECC for TLS

draft-ietf-tls-rfc4492b...

https://tools.ietf.org/html/draft-ietf-tls-rfc4492bis-06

[Docs] [txt|pdf|xml] [Tracker] [WG] [Email] [Diff1] [Diff2] [Nits]

Versions: (draft-nir-tls-rfc4492bis) 00 01 02
03 04 05 06

TLS Working Group — Y. Nir
Internet-Draft — Check Point
Obsoletes: 4492 (if approved) — S. Josefsson
Intended status: Standards Track — SJD AB
Expires: August 5, 2016 — M. Pegourie-Gonnard
Independent / PolarSSL
February 2, 2016

Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer
Security (TLS) Versions 1.2 and Earlier
draft-ietf-tls-rfc4492bis-06

Abstract