User:Sergio Demian Lerner

Contents

Who am I?

Sergio Demian Lerner

- Bitcoin security researcher
- Master in Computer Science
- Reporter of Bitcoin vulnerabilities CVE-2012-3789, CVE-2012-4682, CVE-2012-4683, CVE-2012-4684, CVE-2013-2272, CVE-2013-2292 and CVE-2013-2293
- Designer of Mental Poker protocol MPF.
- My Blog: bitslog.wordpress.com
- My Tweets: @SDLerner
- My company: http://www.certimix.com/

Bitcoin related publications

- MPF: A new family of practical and secure Mental Poker protocols (http://www.dc.uba.ar/inv/tesis/licenciatura/2010/lerner)

Tesis de Licenciatura en Ciencias de la Computación, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires November 15, 2010

In this thesis we propose a new family of practical and secure mental poker protocols, which are efficient enough to achieve real-time performance to security play Texas Hold-em over the Internet, for up to ten players, using personal computers.

- MAVE: Digital Signature Protocol for Massive bulk verifications (http://bitslog.wordpress.com/2012/04/09/mave-digital-signature-protocol-for-massive-bulk-verifications/)

April 9, 2012

In this paper we propose new decentralized digital signature protocols to allow massive bulk verifications (MAVE). The protocols satisfies very tight requirements of performance and storage. MAVE requires a third party with no special trust and a broadcast medium. MAVE can be used for groups of millions of users or autonomous agents that generate thousands of signatures per second that must...more

- MAVEPAY: a new lightweight payment scheme for peer to peer currency networks (http://bitslog.wordpress.com/2012/04/16/mavepay-a-new-lightweight-payment-scheme-for-peer-to-peer-currency-networks/)

April 16, 2012

In this paper we propose a new payment scheme based on the MAVE digital signature protocol, for use in peer to peer currency networks based on a block chain. The proposed payment scheme requires less resources for the users than Bitcoin and can be used to create a truly lightweight peer to peer currency network that stands 700 payments/second, and 5 million new user accounts/year, on an...more

- Destination Address Anonymization in Bitcoin (http://bitslog.wordpress.com/2012/08/06/destination-address-anonymization-in-bitcoin/)

August 6, 2012

Protocol proposal for anonymous customer-merchant relations in Bitcoin.

- Bitmessage v1.0: completely broken crypto (http://bitslog.wordpress.com/2012/11/30/bitmessage-completely-broken-crypto/)

November 30, 2012

Description of security vulnerabilities of the Bitmessage protocol 1.0

- The Bitcoin transaction fetch memory exhaustion attack (TFMEA) (http://bitslog.wordpress.com/2013/01/23/the-bitcoin-trasaction-fetch-memory-exhaustion-attack-tfmea/)

January 23, 2013

Disclosure of a DoS vulnerability in Bitcoin clients.

- Get your peer public addresses (http://bitslog.wordpress.com/2013/01/23/new-bitcoin-vulnerability-get-your-peer-public-addresses/)

January 23, 2013

Disclosure of a vulnerability in Bitcoin that breaks its pseudo - anonymization.

- CVE-2012-3789 disclosure (http://bitslog.wordpress.com/2013/01/08/cve-2012-3789-disclosure/)

January 8, 2013

Disclosure of 3 DoS vulnerabilities I found in Bitcoin.

- Vulnerability in BouncyCastle ECDSA signature verification (http://www.bouncycastle.org/jira/browse/BJB-22)

February 19, 2013

Disclosure of a security vulnerability found in BouncyCastle ECDSA signature verification code that, in applications that must verify other people's signatures, can result in remote application terminations and DoS attack. If affects Bitcoin nodes coded in Java/C# that uses the Bouncycastle cryptographic library.

My Patents

- METHOD AND APPARATUS FOR EFFICIENT AND SECURE CREATING, TRANSFERRING, AND REVEALING OF MESSAGES OVER A NETWORK

United States 12/904,033 Filed October 13, 2009

The patent describes a new realtime peer to peer method for playing with cards over a network with cryptographic security (a **Mental Poker protocol**)

- METHOD AND APPARATUS FOR EFFICIENT AND SECURE CREATING, TRANSFERRING, AND REVEALING OF MESSAGES OVER A NETWORK

Europe PCT/US10/52550 Filed October 13, 2009

See also

- Research

Retrieved from "https://en.bitcoin.it/w/index.php?title=User:Sergio_Demian_Lerner&oldid=35879"
