



# Los Angeles Chapter

## TOOL TALK

TRUECRYPT

FREE OPEN-SOURCE ON-THE-FLY ENCRYPTION

Presented by ISSA LA  
January, 2011



# Los Angeles Chapter

What we are going to talk about today.

- Why did we start Tool Talk?
- What is TrueCrypt?
- How is it used?
- TrueCrypt vs Other free\* encryption tool?
- Additional Information



## Los Angeles Chapter

### What is TrueCrypt?

**TrueCrypt** has been around as an OpenSource encryption tool for a few years. Its main application was the creation of so-called ***encrypted containers*** to store files in a secure manner. Containers can even be mounted as Windows drives in recent versions of the tool. With the introduction of TrueCrypt 6.0, the tool was given the ability to encrypt an existing Windows installation on the fly, which means adding the extra layer of security by encrypting the entire system drive or partition.



# Los Angeles Chapter

## What is TrueCrypt?

**TrueCrypt** is FREE

**TrueCrypt** can run on multiple systems

- **Windows** 7, Windows 7 x64 (64-bit) Edition, Windows Vista (SP1 or later), Windows Vista x64 (64-bit) Edition (SP1 or later), Windows XP, Windows XP x64 (64-bit) Edition, Windows Server 2008, Windows Server 2008 x64 (64-bit), Windows Server 2003, Windows Server 2003 x64 (64-bit), Windows 2000 SP4
- **Mac OS X** 10.6 Snow Leopard (32-bit) , Mac OS X 10.5 Leopard , Mac OS X 10.4 Tiger,
- **Linux** (32-bit and 64-bit versions, kernel 2.4, 2.6 or compatible)

**Note:** The following operating systems (among others) are not supported: Windows 2003 IA-64, Windows 2008 IA-64, Windows XP IA-64, Windows 95/98/ME/NT

**TrueCrypt** supports multiple encryption algorithms



# Los Angeles Chapter

## TrueCrypt :Main Features

- Creation of an encrypted container**, which can be mounted as a real drive.
- Encryption of an entire partition**, such as one on a hard drive or a USB thumb drive.
- On-the-fly encryption** of a Windows installation with pre-boot authentication
- Support for hidden volumes** and unidentifiable volumes (data appears as random).
- Support of various encryption** algorithms and nested double encryption.
- Performance:**
  - Automatic, real-time and transparent encryption
  - Multi-threaded design scales well on multi-core processors



# Los Angeles Chapter

## TrueCrypt supports multiple algorithms

Serpent

Twofish

AES-Twofish

AES-Twofish-Serpent

Serpent-AES

Serpent-Twofish-AES

Twofish-Serpent

All have 256 bit keys

For more information please visit: <http://www.truecrypt.org/docs/?s=version-history>



# Los Angeles Chapter

TrueCrypt vs. Other Free\*Encryption Tool



# Los Angeles Chapter

## What is BitLocker?

**BitLocker Drive Encryption** is a full disk encryption feature included with the Ultimate and Enterprise editions of Microsoft's Windows Vista and Windows 7 desktop operating systems, as well as the Windows Server 2008 and Windows Server 2008 R2 server platforms.

**BitLocker** is designed to protect data by providing encryption for entire volumes. By default it uses the AES encryption algorithm in CBC mode with a 128 bit key, combined with the *Elephant* diffuser for additional disk encryption specific security not provided by AES

For more information please visit: [http://en.wikipedia.org/wiki/BitLocker\\_Drive\\_Encryption](http://en.wikipedia.org/wiki/BitLocker_Drive_Encryption)  
<http://www.microsoft.com/windows/windows-7/features/bitlocker.aspx>



# Los Angeles Chapter

## What is BitLocker?

### Good

**BitLocker** is pre-installed on the your laptop/desktop\*

**BitLocker** is a full disk encryption tool

**BitLocker** is free\*

**BitLocker** creates recovery key

### Bad

**BitLocker** is a full disk encryption tool

BitLocker was designed to be a logical volume encryption solution, which means that you deploy it across entire volumes, whether they span multiple drives or only a fraction of one drive.

**BitLocker based on 128 bit key (compares to TrueCrypt)**

### Ugly

**BitLocker available only on FOUR Windows versions\***

**NOTE:\***-Enterprise and Ultimate editions of Windows Vista and Windows 7



# Los Angeles Chapter

## Resources

<http://www.truecrypt.org/>

<http://www.truecrypt.org/docs/?s=version-history>

<http://www.microsoft.com/windows/windows-7/features/bitlocker.aspx>

[http://en.wikipedia.org/wiki/BitLocker\\_Drive\\_Encryption](http://en.wikipedia.org/wiki/BitLocker_Drive_Encryption)

<http://www.tomshardware.com/reviews/bitlocker-truecrypt-encryption,2587.html>

<http://www.tomshardware.com/reviews/truecrypt-security-hdd,2125-2.html>