Verifying Downloads

Paul Waring
paul@xk7.net

whoami

Two step process:

1. Verify the source
2. Verify the contents

Verify the source

Check the hostname

But… DNS can be changed

Change the nameservers

Poison the DNS cache

http://youtu.be/1d1tUefYn4U

SSL and DNSSEC

Useful but rare and have overheads

Verify the contents

Checksums

String representing block of data

md5sum

(also sha*sum)

Usage:
md5sum [FILE]

Also -c to check

An unmodified file

a30a7d0126cbb23faa8f18b57399a407

An unmodified file.

1f048e1b12e368f917d1c92381b6d2e4

Requirements

1. Cheap to compute
2. One-way
3. Collision-free

Broken in?

Just change the checksums...

Checksum summary

+1 for content

-1 for security

File signing

Used by Debian

Questions?

www.yanone.de
tinyurl.com/slide-design-dev