



Privacy through Technology

(don't drink the kool-aid yet!)

Aldert Hazenberg
<aldert@rotz.org>

Paul Wouters
<paul@cypherpunks.ca>



Introduction

Using encryption USED to be difficult

With software today it is EASY

You will know how easy it is in an hour

Spread the software and the knowledge

A slideshow of this presentation will be at:
<http://chameleon.cypherpunks.ca/>



Trust

Only you can guarantee your privacy!

Do not trust the network

Do not trust proprietary (blackbox)
cryptographic software



Protecting your Communication

We will talk about:

- 1) Instant Messenger
- 2) Email
- 3) Internet browsing
- 4) Voice over IP (if we have time)

We will not talk about:

- 5) Disk encryption
- 6) VPN
- 7) Wifi encryption



Protection against?

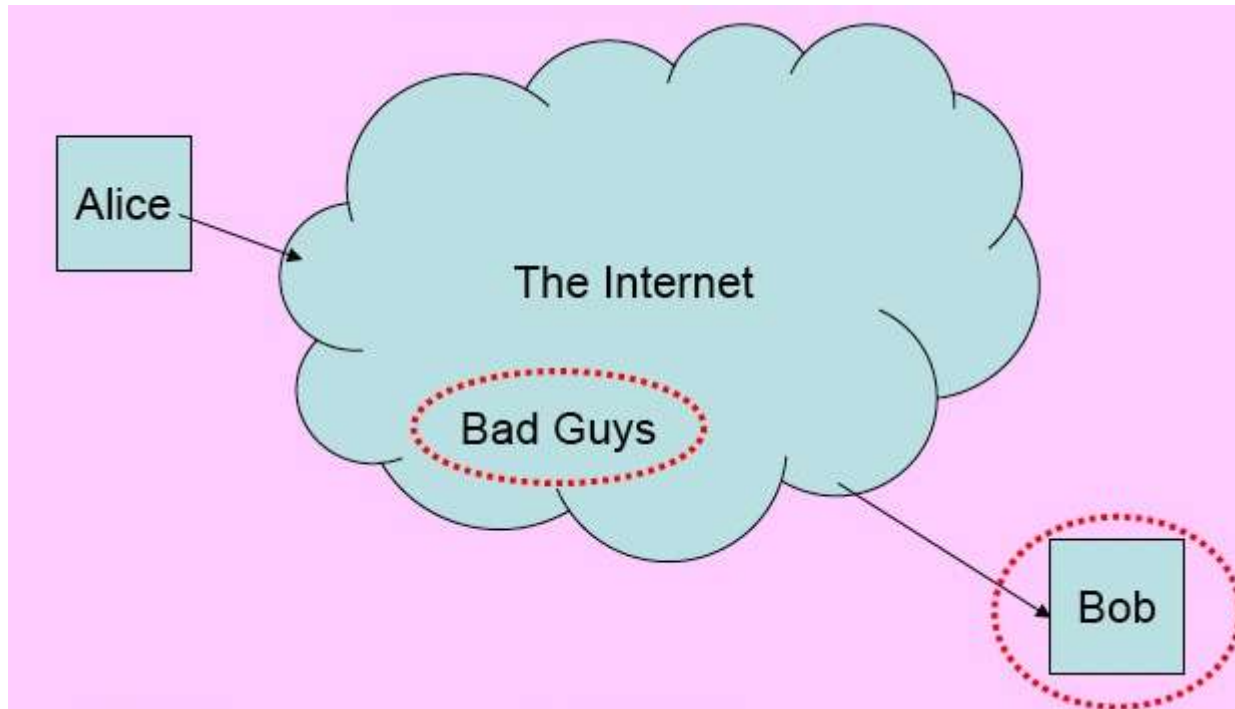
In principle, all encryption software we use in this presentation is “military strength”

In practise, your protection depends on other things, such as physical security, computer security, and any special interest groups that are after you

(and human error)



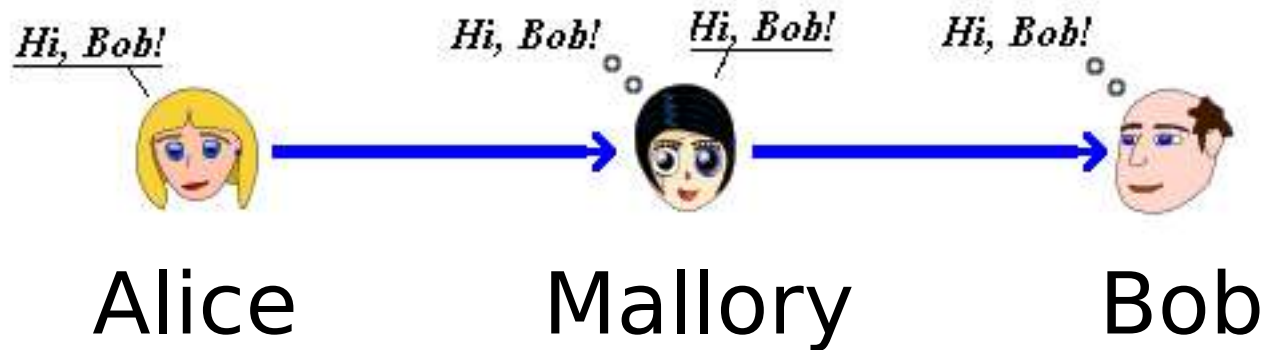
Threat 1: Bob?



Can Alice trust Bob?



Threat 2: Man in the middle



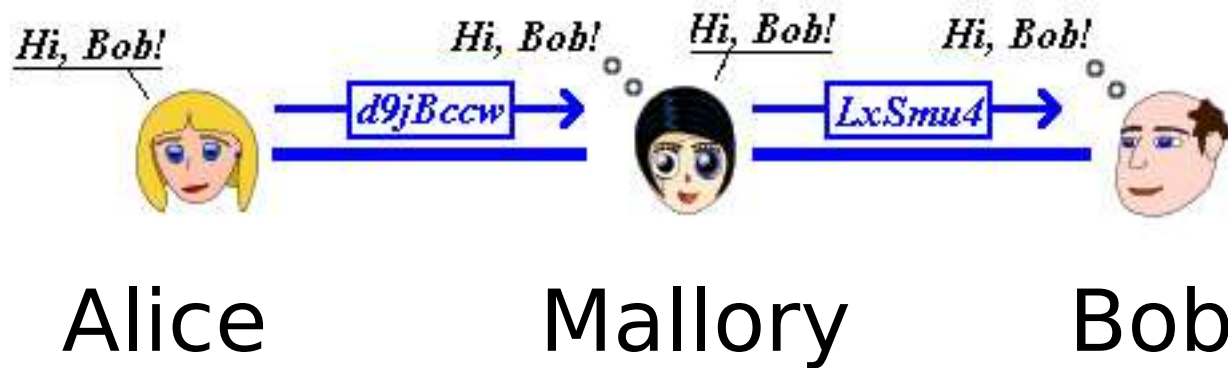
How can we detect this “Man in the middle” attack?



Diffie-Hellman

Solution: The Diffie-Hellman key exchange

Using a DH key exchange, you can guarantee and verify that you are only talking to **one** other party. You can detect someone pretending to be someone else:

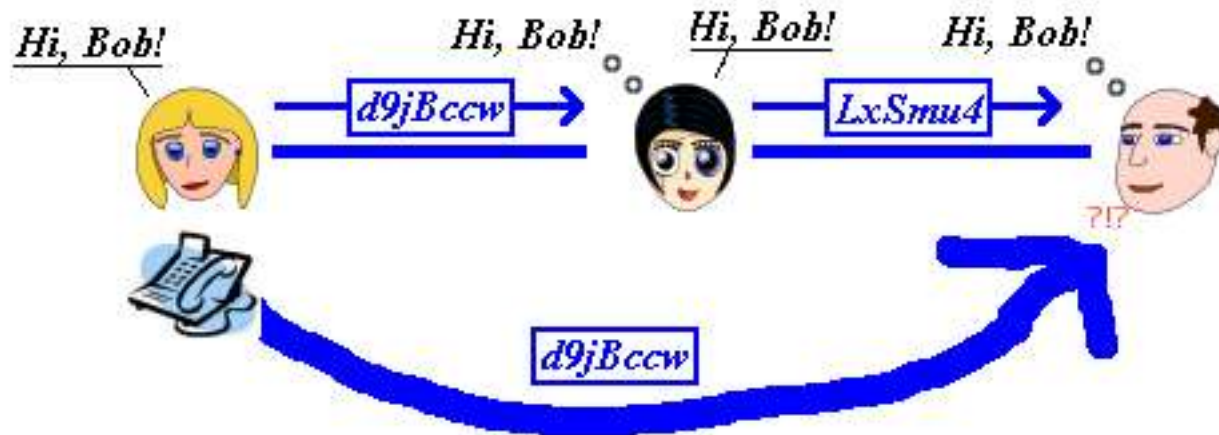


Warning: You know you can detect the MITM. You still need to actually check for that MITM!



Trusted third party

Example TTP: voice recognition





Trusted Third Party

You can NEVER guarantee you are talking privately and securely over a cryptographic channel, unless you have confirmation OUTSIDE that cryptographic channel.

Such outside method is called a "Trusted Third Party"

There is **NO EXCEPTION** to this rule!!!



Threat 3: Future danger

Mallory captures all encrypted traffic between Alice and Bob

Mallory compromises Alice's or Bob's computer

Mallory can now decrypt all captured traffic sent between Alice and Bob



Two defenses against compromised machines

- 1) Only store the private key encrypted with a symmetric encryption key.

This is called "pin" or "password" or "passphrase".

Used mostly to protect private keys by encrypting them (eg: disk encryption, PGP private key, X.509 private key)

This is not super-safe. symmetric ciphers can be broken by brute force, especially short keys and non-random keys such as words or names.

- 2) Use short lived session keys that are NEVER stored on disk.

This is called "Perfect Forward Secrecy" (PFS).

(used by IPsec, SSH, OTR)



Instant Messenger

IM encryption: Off-the-record (“OTR”)
<http://otr.cypherpunks.ca/>

Available on OSX via:

- Adium
- iChat (via OTRproxy)

Available on Windows via:

- Gaim for Windows with gaim-otr
- Miranda via otr.dll plugin
- Trillian Pro via a plugin (non-free!)

Available on Linux via:

- Gaim for Linux with gaim-otr
- Other IM's supporting proxies via otrproxy

(cave-at: OTRproxy does not support the MSN protocol)



Email

PGP and GPG

Available on OSX via:

- iMail with GPGmail
- Thunderbird with Enigmail

Available on Windows via:

- Thunderbird with Enigmail
- Outlook with PGP (proprietary!)

Available on Linux via:

- Thunderbird with Enigmail
- Many command-line mail clients



Web browsing

Privoxy plus TOR

Available on OSX, Windows and Linux



Live Demos

[this space left blank intentionally]