

**zdc**

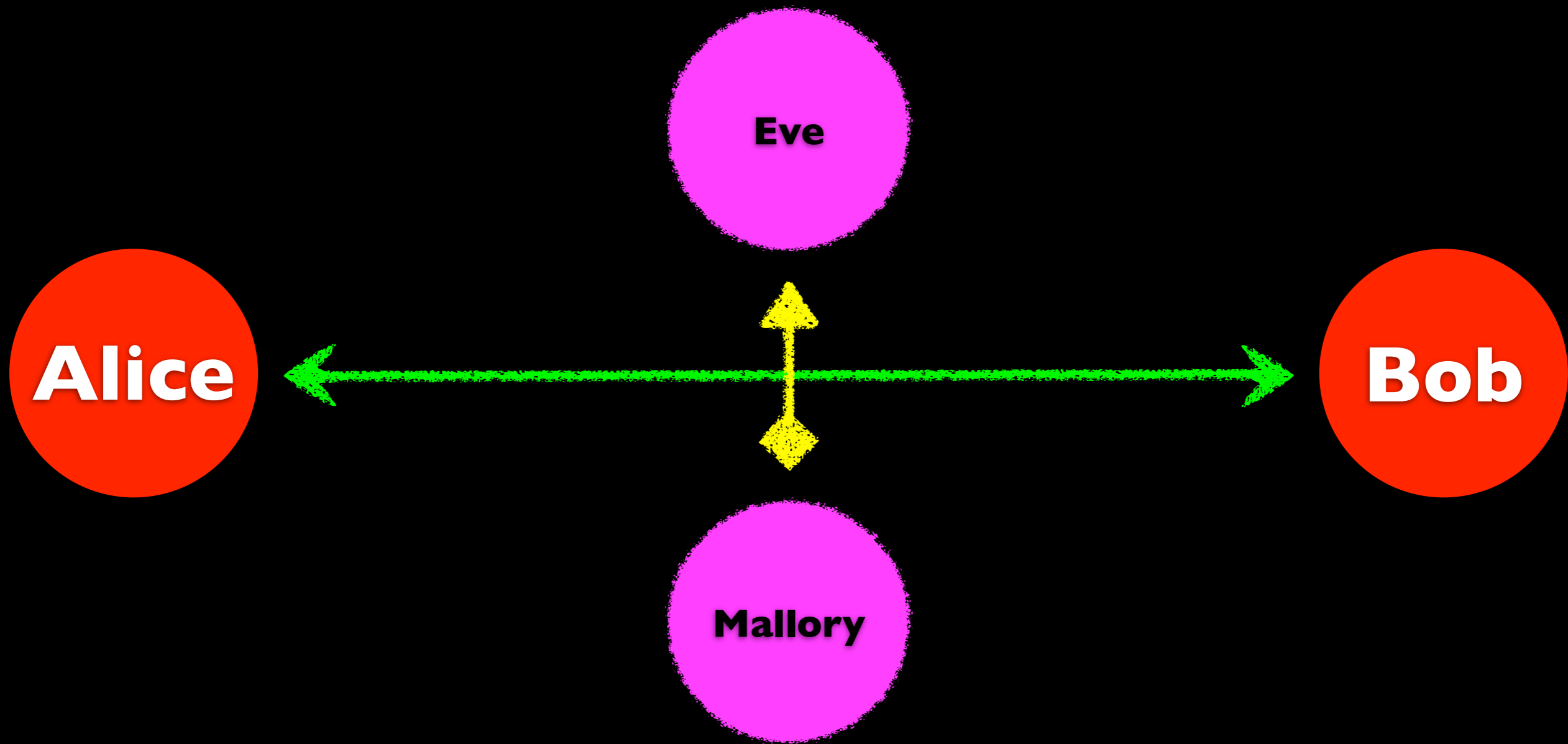
# Zdc

*Pharo Conference May 2012*  
*Sven Van Caekenberghe*

**stfx**

Smalltalk is the Red Pill

# Zodiac TLS/SSL Streams



# Problems

- Eavesdropping
  - listing in
- Tampering
  - changing communication
- Posing
  - acting on behalf of

# TLS/SSL

- Transport Layer Security
- Secure Socket Layer
- Mostly Transparent

# TLS/SSL

- Setup Handshake
- Setup Session
- Communicate

# Setup Handshake

- Exchange parameters
- Negotiate versions, algorithms



# Setup Session

- Use asymmetric public/private cryptography to exchange random session key
- Verify certificates using chain of trust

# Communicate

- Use symmetric encryption on padded message blocks
- Use message authentication codes

**Hard !**

**Fall back  
to  
OS Library**

# SocketStream ?

# Zodiac Streams

# Buffer Management

# Zodiac Streams

- *ZdcAbstractSocketStream*
  - ZdcSimpleSocketStream
    - ZdcOptimizedSocketStream
      - ZdcSocketStream
- ZdcIOBuffer



**OK !**

# ZdcSecureSocketStream

# Plugin

# Plugin

- *ZdcAbstractSSLSession*
  - ZdcPluginSSLSession
- VM Plugin
  - native OS library interface

# ZdcSecureSocketStream

- readBuffer & writeBuffer [plain]
- in & out [encrypted]
- framing

# ZdcSecureSocketStream

- #connect
- #accept
- certificates

**Use**

# HTTPS Client



# Secure POP

## incl STARTTLS

# Secure SMTP

# HTTPS Server

<http://zdc.stfx.eu>

Zodiac TLS/SSL Streams

**zdc**