Two-factor authentication

Ian Durkacz
Development Meeting, 20th August 2014
Project #279

- ‘Examine the options for two-factor authentication’
- [http://devproj.inf.ed.ac.uk/show/279](http://devproj.inf.ed.ac.uk/show/279) – general statement of overall aspiration
- [https://wiki.inf.ed.ac.uk/viewauth/DICE/Project279InitialCallForRequirements](https://wiki.inf.ed.ac.uk/viewauth/DICE/Project279InitialCallForRequirements) – an attempt to unpick the above
General requirements

• Anything we provide has to be:
  – Simple to use
  – Optional: whether or not users want to be involved is up to them
  – Client platform independent
    (Question: in view of recent discussions here, are we including mobile phones, tablets etc. in the list of clients we undertake to support?)
One specific idea: Yubikey

- Hardware OTP generator
- Presents as a USB keyboard – so works on anything which has a USB port
- Easy for people to use; cheap – US$20 each
- Several possible modes of operation:
  - Default: embeds an ever-increasing integer into an encrypted packet. Both Yubikey and the remote authentication server know the symmetric encryption key
  - OATH-HOTP also supported
- More info: http://www.yubico.com/
Yubikey and ssh (1/2)

- Using Yubikey in default mode, this is working (cue demo ...)
- Could be deployed on staff.ssh etc.
- Simple to use
- Optional per user (via pam_succeed_if)
- Client platform independent agnostic (but: does require USB)
Yubikey and ssh (2/2)

- ‘... could be deployed on staff.ssh etc ...’

- In practice, in default mode need to:
  - Integrate (Yubikey serial number, uuid) pairs in LDAP
  - Describe Yubikey users as a (net)group
  - Have procedures to maintain the above
  - Have procedures to allocate the actual Yubikeys
  - [Important] Set up an Inf authentication server
  - Further wrangle with Yubico s/w builds to support the above
That’s all great, but:

• Assumption is that user’s password has been compromised, so:

• If Yubikey/ssh is to be useful, then we need all external access to be similarly restricted:
  – Cosign (definitely feasible; required effort not clear)
  – OpenVPN (don’t know about this)
  – Git? Subversion? CVS?
  – Anything/everything else we might ever use.

• I might need some help here ...
My questions

- Does Yubikey/ssh as presented here solve (any of) our actual requirements?
- Do we want to proceed with this?
  - It will require further investment in time – probably not just by me.
- Should we be looking for a solution which also covers things like mobile phones?
  - Configuring support for Yubikeys in OATH-HOTP mode (rather than default mode) might get us that – but needs work and testing.