Phishing Panel

Richard Clayton

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

FC'05
Roseau, Dominica

28th February 2005

Why does phishing work?

- Con artists are really, really good at persuading people to do dumb things.
- Almost no context to an email, or a website; so you no longer need an Intaglio-capable printing press to produce plausible props.
- The underlying protocols and procedures are pretty rubbish…

Authentication(?) protocols

- Password (or 1-time password, or SecurID)

  A→B: A, S_n

  & hence Man-In-The-Middle attack

  A→P: A, S_n

  P→B: A, S_n

- Even if Alice proves her identity (& liveness) in every message there is no binding of that to the type of transaction (or the amount)

Surely, we can fix it with Crypto?

$A \rightarrow B: \quad \{A, B, nonce, Transaction_n\}_{K_A^{-1}}$

This is fine if Alice trusts the program she is using to do the crypto. So what if the phisher invites her to download a new improved version from **`www.bankname.newsoftware.com`** ?

note that *bankname* doesn't see this being registered! So policing the DNS won't help

What about Client Certificates ?

- Client Certificates fix Man-in-the-Middle
  - also kills off account aggregation, and stops you doing your banking from a cybercafe…
- and if phishers now offer you an updated Client Certificate (“and please email back the previous copies for secure destruction”)
  - or if the next virus targets Certificates ?
  - exactly what is the binding to the Certificate ?

What about browser pop-ups?

- Phishers already overwrite padlocks, the URL being visited and the URL asked for…
  - with current browser "security" models you cannot really rely on *anything* on the screen being in the least bit valid
  - it is not credible to insist consumers check for the browser patches every day **and** also turn off Java, JavaScript, ActiveX and Flash…

    ...besides, the banking site probably needs them!

So what will work ?

- Lots of small improvements are possible
  - One-time passwords
  - Client Certificates
  - Real-time browser checks on websites
  - Validation of incoming IP address
  - Multiple levels of authentication by the bank
  - etc etc
- All can be overcome one-by-one, but if introduced all at once they may be daunting!

Who’d climb Kilimanjaro just to go phishing ?