Insecure Real-World Authentication Protocols

(or Why Phishing is so Profitable)

Richard Clayton

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

Thirteenth Cambridge
Protocols Workshop

20th April 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…

Bank "authentication" protocol

- Alice signs on using her password(s)

  $A \rightarrow B: \quad A, S_n$

- Hence there is a Man-In-The-Middle attack

  $A \rightarrow P: \quad A, S_n$

  and then later on

  $P \rightarrow B: \quad A, S_n$

Fixing freshness

- Alice signs on using SecurID, or a one-time password from a booklet, or a token value provided by an SMS message, or some other two-factor time-based authentication token...

  $A \rightarrow B$: A, S_n

- MITM **still possible**, albeit only in real time

  $A \rightarrow P$: A, S_n

  $P \rightarrow B$: A, S_n

Session extension attack

- Alice signs on and does her transactions

  $A \rightarrow B$: A, T_1

  $A \rightarrow B$: A, T_2

- Phisher extends the session…

  $A \rightarrow P \rightarrow B$: A, T_1

  $A \rightarrow P \rightarrow B$: A, T_2

  $P \rightarrow B$: A, T_3

Defeating session extension

- Asking for (fresh, one-time) password on every transaction avoids session extension
- So phisher replaces transactions…

  $A \rightarrow P$: A, T_1, S_n

  $P \rightarrow B$: A, X_1, S_n

  … more complex, but entirely viable

Secure channels

- SMS, or email are secure (in comparison)
- But are slower (else we'd always use them!)
- Why not summarise completed sessions?

  $B \rightarrow A$: $A, T_1, T_2, T_3, T_4, \ldots$
- Will work, and dumps the problem on Alice!
- However, phisher can use a stolen key to change the email address and then fake the email summaries…

What about `https:` ?

- SSL (or TLS) provides protection against eavesdropping and tampering
- Will also authenticate identity of remote site
- But this is no big win

$$P \rightarrow A: \quad \{\text{I am site-P}\}_{K^{-1}_{\text{Certifier}}}$$

and unless A concentrates she thinks she has just been told that the other end is “B”

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…
- but 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 ?

Surely, we can fix it with crypto?

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

Academic community will be delighted to assist in analysing what is within the brackets, ensuring that sufficient information is being signed, checking that you can't use multiple simultaneous protocol runs to mount an attack.. that's what this workshop addresses!

Crypto doesn't provide trust

- Alice must completely trust the program she is using to do the crypto (because she will not be able to do PKI sums in her head)
- 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

Crypto isn’t a complete solution

- We’ve only really punted – how does the crypto program authenticate Alice?
- How does Alice handle all the “user friendly” indirections?

`PAY GAS COMPANY £100`

is, in actuality, the hard to check

`TRANSFER 100.00GBP to 06-07-08 12346789`

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!

Is “authentication” the problem?

- Schneier 2005: *If we’re ever going to manage the risks and effects of electronic impersonation, we must concentrate on preventing and detecting fraudulent transactions.*
- His proposes to make financial institutions responsible for all fraudulent transactions...
  - not a solution; but a mechanism to find one

So what will work ?

- Lots of small improvements <u>are</u> possible
  - One-time passwords force real-time MITM
  - Client certificates change the attack surface
  - Browsers could do real-time checks on websites
  - Websites could assess risk based on incoming IP address
  - Bank could have multiple levels of authentication
  - 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 ?