Royal Holloway University of London

Information Security Group

Using HIPs to secure human-machine interactions via untrusted intermediaries

Chris Mitchell

http://www.isg.rhul.ac.uk/~cjm

Royal Holloway University of London

Information Security Group

Agenda

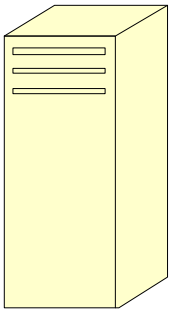
1. **The problem**
2. HIPs
3. Using HIPs
4. Use scenarios
5. Conclusions

Royal Holloway University of London

Information Security Group

Model

Communications enabled by untrusted third party



User

Machine (no user interface)

Royal Holloway University of London

Information Security Group

Examples

- Access to a smart card using a merchant terminal. Must rely on terminal to correctly display amount of transaction (and not record PIN).
- Access to email server (or other Internet service) using Internet café PC – must rely on terminal not to record password.

Royal Holloway University of London

Information Security Group

Prior art

- Prior art has mostly addressed the smart card/user interaction issue.
  - Gobioff, Smith, Tygar and Yee (1996) considered theoretical aspects of the problem.
  - Stabell-Kulø, Arild and Myrvang (1999) looked at solutions using a third party verification server.
  - Berta, Buttyan and Vajda (2004) proposed the use of a special type of signatures.

Royal Holloway University of London

Information Security Group

Agenda

1. The problem
2. **HIPs**
3. Using HIPs
4. Use scenarios
5. Conclusions

Royal Holloway University of London

Information Security Group

What are HIPs?

- Human Interactive Proofs (HIPs) – otherwise known as CAPTCHAs (Completely Automated Public Turing tests to tell Computers and Humans Apart) – are basically tests set by computers which only humans can solve.
- One simple and widely used example of a HIP is to display characters (e.g. letters and/or numbers) in a form that humans can read them but image processing software cannot.

7

Royal Holloway University of London

Information Security Group

Example

This CAPTCHA of ‘smwm’ obscures its message from computer interpretation by twisting the letters and adding a background colour gradient.

It is taken from Wikipedia.

8

Royal Holloway University of London

Information Security Group

Techniques

- Motivation is to choose probloems which are known to be hard for computers to solve.
- As previously mentioned, one method is to display distorted characters. [This is the basis of this paper].
- Many other techniques have been proposed, e.g. to choose images showing the same person, or to count objects of a particular type in a scene.

9

Royal Holloway University of London

Information Security Group

Agenda

1. The problem
2. HIPs
3. **Using HIPs**
4. Use scenarios
5. Conclusions

10

Royal Holloway University of London

Information Security Group

Applications

- Many applications have been proposed.
- Probably the best known is the use by Yahoo to protect free email accounts.
- Here, a user must solve a HIP before obtaining an email account – this prevents automatic harvesting of HIPs for use by spammers.

11

Royal Holloway University of London

Information Security Group

A new use

- In some sense, a HIP provides a (low bandwidth) communications channel between the computer and the human, which no other computer can intercept.
- This is because the human readable symbols shown by the computer are not readable by any other computer.
- This is a confidentiality-protected but not authenticated channel.

12

Royal Holloway University of London

Information Security Group

A reverse channel

- We can also use HIPs to provide a confidential but unauthenticated reverse channel.
- One approach involves the target machine sending a sequence of distorted messages, of which the user chooses one (or more).
- This could, for example, enable the user to enter a PIN in an unobservable (to a computer) fashion, e.g. by pressing a button next to a distorted digit.
- More generally, for password entry, the target machine could ask a password-related question (in distorted text) and get the answer via the selection of one of a series of distorted images.

13

Royal Holloway University of London

Information Security Group

Using the secure channels

- The use of HIPs therefore allows us to establish a two-way confidential channel between user and computer, even when communications pass via an untrusted intermediary.
- However, this channel is:
  - unauthenticated;
  - only confidential against machine eavesdroppers (also can be read by humans if exchanges are recorded).
- What can we do with this?

14

Royal Holloway University of London

Information Security Group

Agenda

1. The problem
2. HIPs
3. Using HIPs
4. **Use scenarios**
5. Conclusions

Royal Holloway University of London

Information Security Group

General remark

- In all the scenarios, the use of the confidential channel by no means solves all security issues (since channel always observable by a human).
- However, it does offer an additional layer of protection against machine-only attacks.

Royal Holloway University of London

Information Security Group

A. Smart card PIN entry

- PIN could be sent to card via a confidential channel, e.g. by displaying concealed digits next to buttons.
- However:
  - channel unauthenticated – so the terminal could put up its own images and learn the PIN; however it could not tell the card the PIN.
  - PIN could be learnt by humans processing a recorded transaction.

17

Royal Holloway University of London

Information Security Group

PIN entry: continued

- Another option would be for the card to provide a PIN offset in a distorted image, which the user simply adds to his PIN before entering it.
- This again has the problem that, because the channel is unauthenticated, the user does not know where the offset comes from.
- However, perhaps the distorted images sent by the card could be combined with the visual authentication notions of Dhamija and Tygar (2005).

18

Royal Holloway University of London

Information Security Group

B. Smart card transaction authorisation

- The smart card could enable the user to enter the transaction amount (to be authorised) via the selection of distorted digits.
- The card would then display a distorted image of the total value to be authorised.
- The authorisation process (e.g. involving PIN entry) could then be managed in the context of the authorisation image.

19

Royal Holloway University of London

Information Security Group

C. Context establishment

- It may be possible to use the confidential unauthenticated channel to enhance the security of 'imprinting' of mobile devices.
- This involves setting up a security context between two devices (which may not have their own user interfaces).
- It might be possible to combine human entry of PINs into two devices (via untrusted intermediaries) with a Diffie-Hellman key exchange.

20

Context establishment: continued

- Use of a Diffie-Hellman key exchange should protect against later inspection of the (recorded) exchange by a human.
- However, as previously, the fact that the human-machine channel is unauthenticated may present security problems.

Agenda

1. The problem
2. HIPs
3. Using HIPs
4. Use scenarios
5. **Conclusions**

Royal Holloway University of London

Information Security Group

Enhancing the channels

- What bandwidth can be achieved?
- What are the best HIPs to use for this purpose?
- Most importantly, can HIPs (perhaps with visual authentication) be used to provide an authenticated human/machine channel?

23

Royal Holloway University of London

Information Security Group

Addressing the scenarios

- Can the confidential channels provided by HIPs be used more effectively in the identified use scenarios?
- Are there other more appropriate use scenarios?

24