UNIVERSITY OF
OXFORD

HCBK:security technology for the mobile generation

Oxford University Computing Laboratory

Content

Introduction to HCBK

HCBK is a new type of security protocol which allows humans to create strong security easily without relying on existing infrastructure or third parties.

It was invented by researchers from Oxford University Computing Lab, and we have formalised and specified a concrete set of solutions based on HCBK to satisfy various kinds of requirements.

The term HCBK in this document represents the technologies we've developed based on the HCBK protocol family.

Hash Commitment Before Knowledge is the principle on which the protocols operate.

Research Team

Professor Bill Roscoe has been a leading security researcher for 15 years. He has been head of Oxford University Computing Laboratory for over six years.
He has worked on security projects sponsored by Industry and UK and US governments and is a member of the steering committee on the KTN on cyber security.

Dr Long Nguyen has worked in this area for 5 years is a research assistant working on the theory of HCBK protocols and associated cryptography.

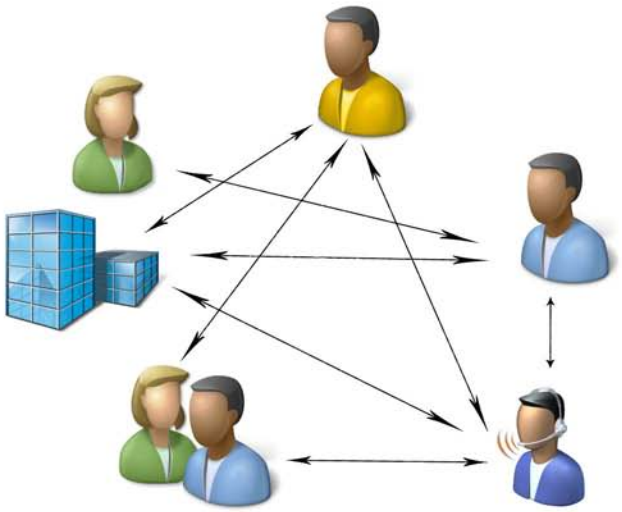
Bangdao Chen is a doctoral student and works on implementation and application issues.

Ronald Kainda is a doctoral student researching human interface issues.

Concept

HCBK builds security between two or more devices that human(s) wish to connect without any pre-existing secrets or infrastructure.

Requires a minimum of expensive cryptography. And a minimum of human effort, using any way of transmitting information that can't be forged such as conversation or observation.



How it works

The devices make an insecure connection.

They send each other ID and security information such as a one-time uncertificated "public" key.

They agree on a one-time hash key in a two-stage process that means it is pointless for an attacker to interfere: see papers.

No point in attacker searching for collisions on this hash because the parties are already committed to what they are going to hash.

Parties then check that the hashes agree.

So only prospect for attacker is to send fake information before the hash key is decided: a single guess that will almost certainly fail: probability 1-1/H where H is the number of possible hash values.

It is a test for the existence of a man-in-the middle.

Applications

Anywhere where a human wants to create security between devices, or where a group need a secure network connecting their devices.

- Payments (see later)
- Participants in a meeting or teleconference
- Secure email, texts, telephone calls, radio
- Sensor networks
- Medical devices: personal sensors, doctor-to-patient.
- Key creation and distribution
- Inter-organisation collaboration (no existing security)
- Temporary and long-term security.

Virtues

1. Requires no pre-existing infrastructure: can be run on mass-produced identical items (no separate identities) and highly heterogeneous networks.

2. Easy to create strong security.

3. Users have confidence in security since they have designed it themselves rather than relying on an infrastructure they don't understand.

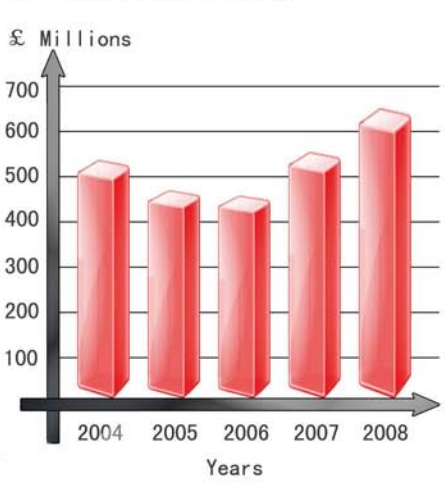
4. Low processing requirement.

5. Technology independent: works over any communication medium.

We can exploit these virtues to create new models of financial transactions.

The threat

Online banking fraud losses up 55% in 2009. Online attacks are constantly growing.



Phishing, pharming and Trojans represent one of the most sophisticated technological crime waves worldwide. Online criminals work day and night to steal identities, online credentials, credit card information, or any other information that they can efficiently monetise. They target organizations in all sectors, as well as any person who uses the Internet at work or at home.

More Attacks

Advanced attacks like man-in-the-middle, man-in-the-browser, session-hijack, and new Trojans make the current security incompetent. For example, the relatively new CAP protocol announced by banks has been recently cracked by a Cambridge research team.

Man-in-the-middle-attack

Wireless applications give opportunities for new attacks which are hard to deal with, for example, mobile network traffic interception, phone spying or cloning.

Necessity

The use of mobile payment was always certain to grow, but...

The announcement on 16 December 2009 by the UK Payments Council that cheques are to be phased out by 2018 has heightened the need for more secure e-payment systems.

Mobile phones are the most obvious technological platform for replacements.

We need innovative solutions for payments supported by convenient but strong security.

Mobile payment

We want the payer to be able to bootstrap an electronic connection to the payee (whether merchant or person, whether online on telephone or in person).

If we knew the connection was secure then payment could be so easy and flexible. Because we can trust a high bandwidth channel between them.

Reverse Authentication!

Authentication of payee precedes the usual authentication of payer, which is thereby made simpler.

HCBK is not a single method of mobile payment. Rather, it is the key to inventing a number of secure and convenient methods for

- e-cash
- Online banking
- Credit card payment

That work over a wide variety of media:

- Telephony/SMS/data calls
- Bluetooth/WiFi
- Internet

At Point of Sale, online or by telephone call.

Payment virtues

HCBK builds strong security between devices of the user's choice. The user is in charge and can clearly identify with the simple process of building security.

We can force compliance by the user: payer cannot bypass security by complacently saying "yes".

It can create security in a stand-alone manner, it can re-inforce other modes of security or it can be backed up by secondary security.

Uniform interface for payer across a wide variety of payment scenarios.

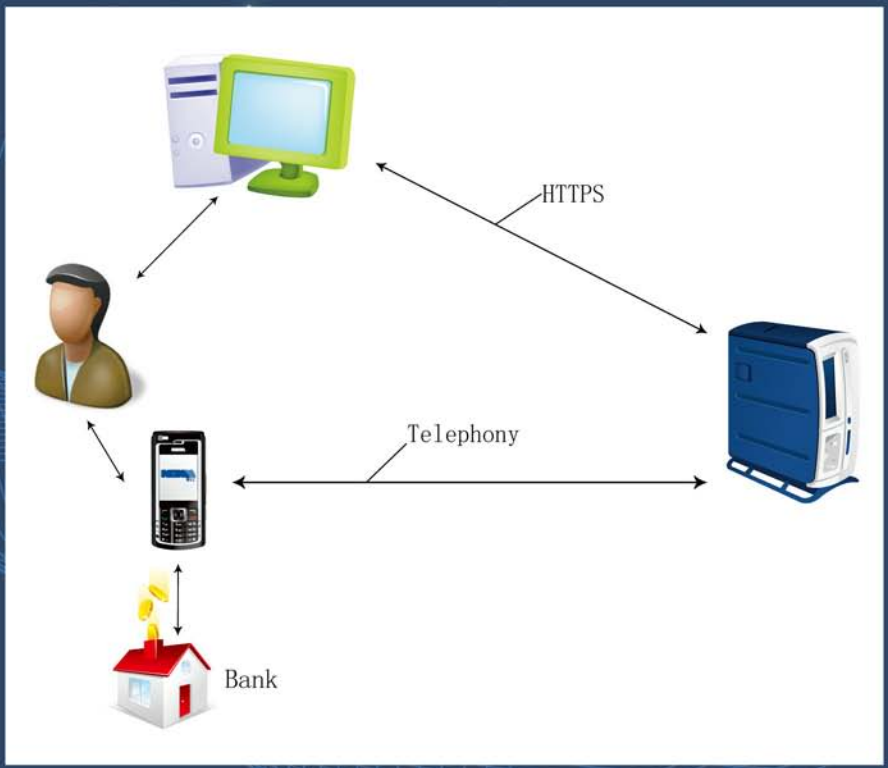
Example: extending mobile banking

Many banks offer mobile banking: looking at accounts, transfers to known payees. Suppose you want to pay some other party: you need their name, A/C number, bank details, amount to pay and perhaps other transaction details. Too much to key into your mobile!

But make an HCBK connection with the payee (and so knowing it is the desired payee within the intended transaction) and the payee can send you all this information to display on your phone and approve.

This information (in particular the name and maybe logo) acts as strong secondary security for HCBK, and the use of HCBK ensures (i) secrecy of the transaction and (ii) that a complacent payer cannot say "yes" to an unintended payment.

Example: person-to-business online payment by mobile banking



All of this also works peer-to-peer, though we may well make the payer rather than payee specify the payment amount in this case.

So you can pay your plumber, your friend or anyone else who has this sort of mobile banking installed.

You can pay them in person, via a telephone call, and set up security for future payments in advance (e.g. for regular payments or birthday presents!)

An interesting replacement for paper cheques!

Scenario of person-to-business online payment by mobile banking

This example is also used as the demonstration of remote mobile payment.

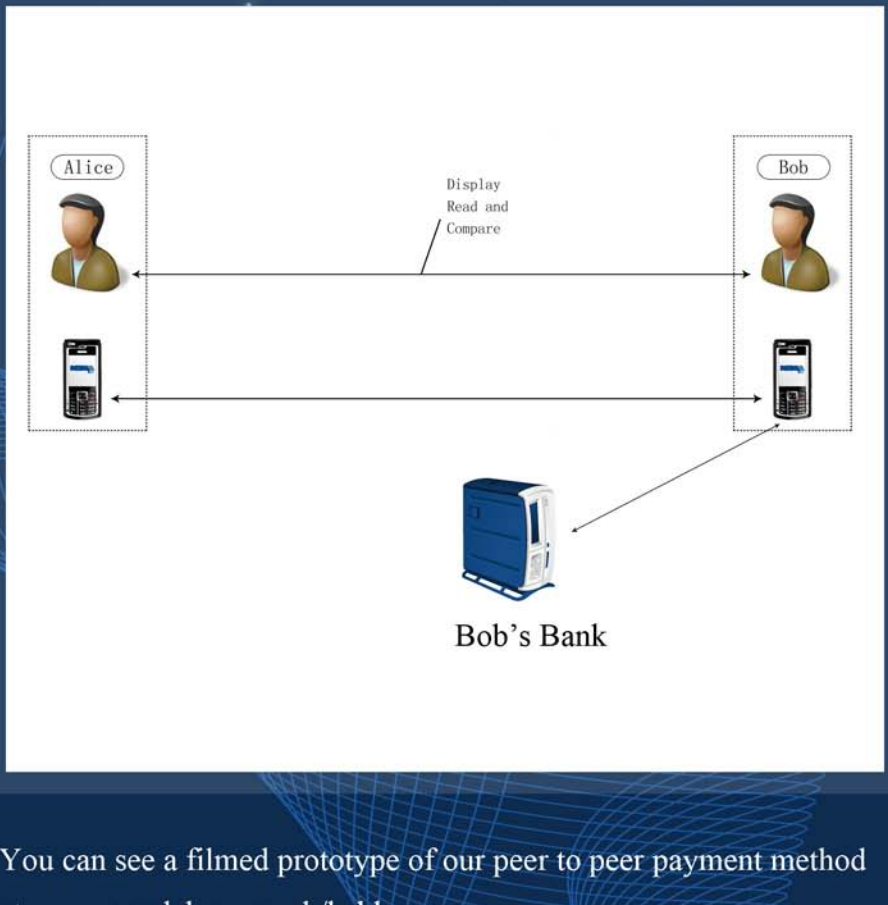
A general description of how it works:

1. The customer C has come to the point of paying on an internet session and is confident that the HTTPS session is connected to the merchant M.
2. C presses a button on the website for mobile payment and starts (*) the payment application on his mobile phone. The button gives C's phone payment number to M securely via HTTPS.
3. M calls C's mobile phone and runs the initial messages of the protocol with it.
4. M calculates the digest and displays it on existing HTTPS window.
5. Assuming C wishes to carry on; he types this number into phone which then decides if numbers agree. Agreement gives secure connection.
6. M sends details of the payment it wants over the secure (authenticated and encrypted) connection including amount, name, possible logo and bank information.
7. The payment is displayed on mobile phone (in our implementation, in the form of a cheque) and C is asked to confirm payment (*).
8. Payment is processed by e-banking, which generates a "receipt" to send to M.

it will be necessary in practice to have the customer prove his/her identity as part of this process. One or both of the points marked (*) are appropriate.

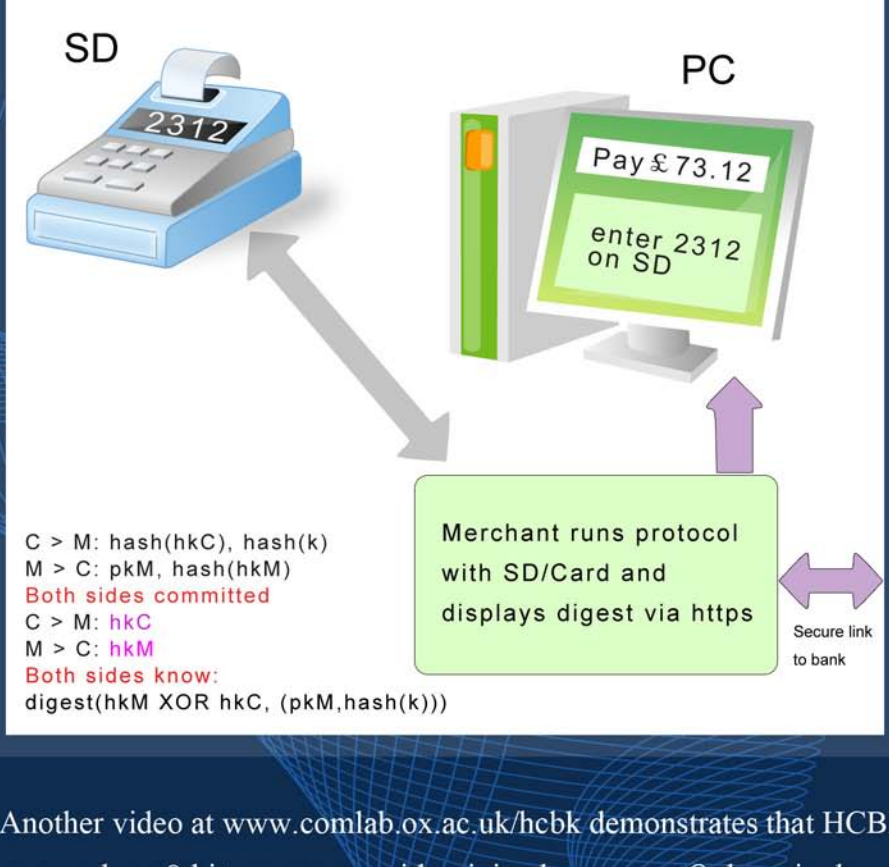
See video “On-line payment” on http://comlab.ox.ac.uk/hcbk

Example: person-to-person mobile payment



You can see a filmed prototype of our peer to peer payment method at www.comlab.ox.ac.uk/hcbk.

Example: Secure online payment



Another video at www.comlab.ox.ac.uk/hcbk demonstrates that HCBK can work on 8-bit processors with minimal memory. Only a single asymmetric encryption is required by a one-time key.

Therefore it can be run on credit cards or give-away devices.

Q&A

Is it safe to run the protocol on an insecure connection/network?

Yes, it is. The messages of the protocol can be made public to everyone, for example, you could send them by broadcasting, by posting on the internet, etc. A hacker can overhear all the messages of the protocol: this does not improve his chances.

Do the applications need to be installed on smart phones or high end mobile phones only?

The applications we have presented are built in Java, and the computation cost of them has been carefully examined and designed. One of the applications is implemented on an 8-bit cheap processor with only 2 Kb of memory and 64 Kb of code space. We are confident that our technology can be implemented on most types of mobile phones with or without Java support.

How can your applications work together with the existing banking system?

Our technology supports multiple payment models. One of the most interesting of these is to extend the functionality of mobile banking (running internet banking on a phone). In this, the secure channel our technology develops is used to upload payment details (name, amount, bank details etc) from the payee's system to the payer's phone. The payment can then proceed through the banking system using existing methods.

In addition, the examples you have seen only demonstrate some features of our technology, they do not define how the underlying technology operates, nor are they intended to represent how the final implementations would function or appear. We can prove the flexibility of our technology against any specific requirements.

Q&A

Are the mobile payment demos EMV (Euro Card, Master Card, and Visa Card) enabled?

We haven't incorporate those functions into our implementations, but it is clear that EMV could be implemented by providing necessary interfaces on mobile phones, either by applying a card reader, the integrated SIM card or hardwired information within the application.

Your demonstration doesn't show how money is actually transferred. Is the money stored on the phone, come from a credit card, a bank?

It could be any of these; our technology is highly flexible which could be swiftly adapted against concrete requirements.

Does the application need to use any information that has been stored on the mobile phone?

No. To establish security, there is no need to store any information or any key on the device. Although there are some keys as part of the cryptography used in the protocol, they are generated on the fly and one time only. However, based on different concrete scenarios (e.g. the use of mobile banking), it could be necessary to use some sort of stored keys or information in order to provide the overall service.

What kind of connection is used to communicate data in the applications?

We do not rely on any particular technology of communication, therefore, any kind of connection can be used in our applications, for example, Bluetooth, WIFI, GSM, CDMA, GPRS, 3G, etc.

Q&A

What's the difference between Near Field Communication (NFC) enabled mobile payment system and HCBK enabled mobile payment system?

HCBK enabled mobile payment system does not rely on any specific kind of technology as it can establish security out from human trust. It can swiftly incorporate new technology like NFC either as the normal connection or one authentication factor. HCBK enabled mobile payment system can be installed on any kind of mobile phones while NFC enabled mobile payment system can only be installed on mobile phones with NFC: a small fragment of the existing market.

What is the value you have seen in the videos that the user has to input on his device?

It is called digest value, which is calculated by taking all the information that has been communicated in the protocol. It is used to verify the authenticity of the data that has been communicated in the protocol. For more details, please refer to the academic papers we have published.

Is the digest value needed to be made secret or to be encrypted?

No. The digest value can be made public to everyone, as long as the participants are assured that this value comes from the correct person, for example: by reading it out (recognize the voice), by displaying it directly (seeing is believing), etc.

Where does the security actually come from?

Please refer to the academic papers listed on:
http://www.comlab.ox.ac.uk/hcbk/papers.html

Contact

If you are interested in this new technology, please contact

Brendan Spillane

Isis Innovation Limited

Ewert House, Ewert Place

Summertown

Oxford

OX2 7SG

Tel:+44(0)1865614423

Fax:+44(0)1865280831

Isis was established by Oxford University in 1988 as its wholly owned technology transfer company. Isis has developed substantially over the years in a number of phases, as the technology transfer activity has grown, and with the formation of Oxford University Consulting and Isis Enterprise.

Isis manages the University's intellectual property portfolio, working with University researchers on identifying, protecting and marketing technologies through licensing, spin-out company formation, consulting and material sales. Isis funds patent applications and legal costs, negotiates exploitation and spin-out company agreements, and identifies and manages consultancy opportunities. Isis works on projects from all areas of the University's research activities: life sciences, physical sciences, social sciences and humanities. Isis provides access to Oxford's expertise and provides researchers with advice on commercialisation.