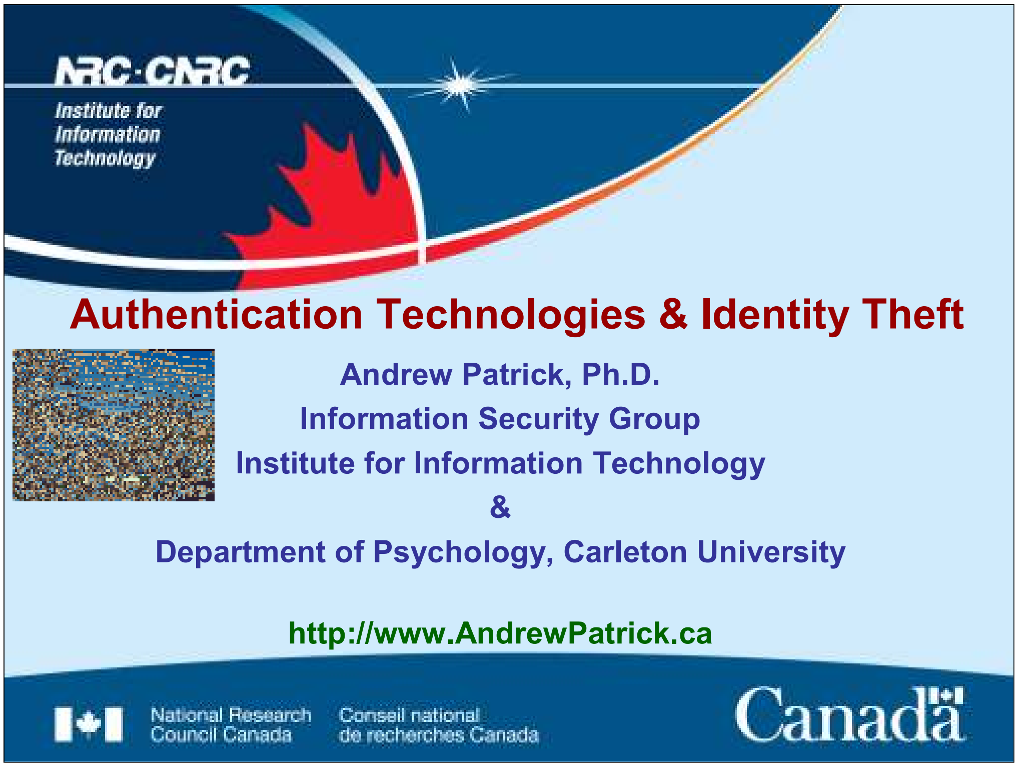


NRC·CNRC
Institute for
Information
Technology

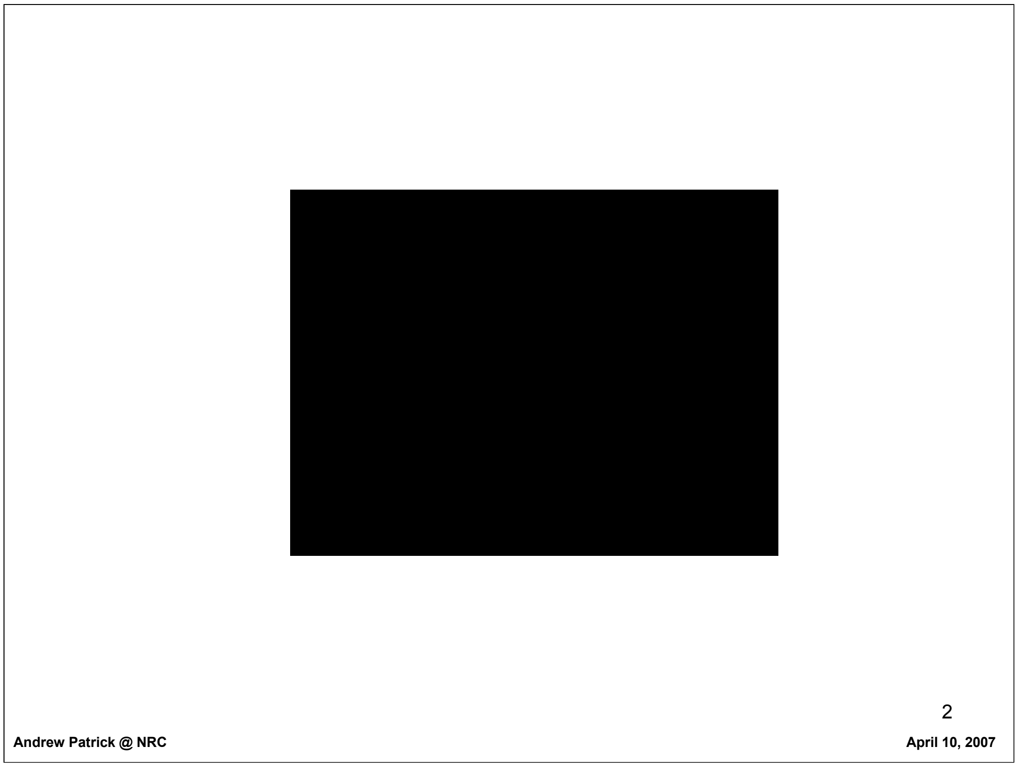
Authentication Technologies & Identity Theft

Andrew Patrick, Ph.D.
Information Security Group
Institute for Information Technology
&
Department of Psychology, Carleton University

http://www.AndrewPatrick.ca

National Research Council Canada
Conseil national de recherches Canada

Canada



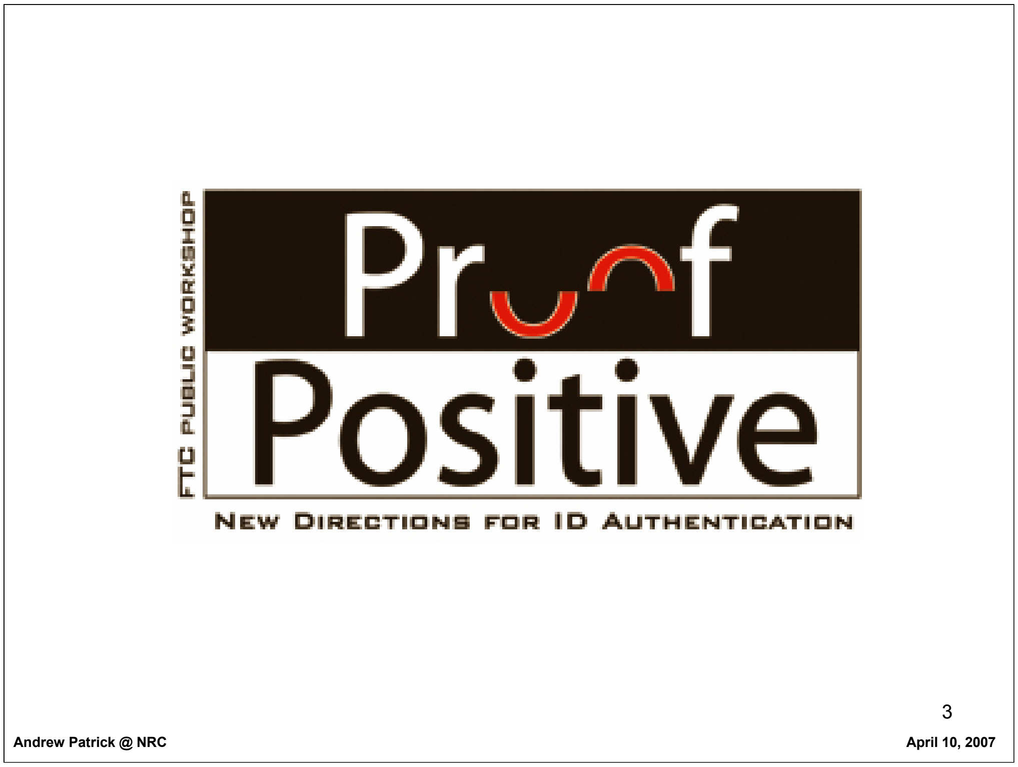
2

Andrew Patrick @ NRC

April 10, 2007

Video from Citibank advertisement

Identity theft is a very large personal and financial problem (2006 estimates are $56 billion per year in the USA).



3

Andrew Patrick @ NRC

April 10, 2007

FTC Workshop, April 23-24 2007

The US FTC and other participating agencies are planning to host a two-day public workshop to explore the role of authentication processes in preventing identity theft. The workshop will provide a forum for discussion among public sector, private sector, and consumer representatives about better ways to authenticate the identities of individuals.

The Identity Theft Task Force was established by Executive Order of the US President on May 10, 2006. The Order directed the Task Force to deliver a strategic plan to the President on the federal government's response to identity theft. The Task Force delivered an interim set of recommendations on September 19, 2006 that included the recommendation to hold a workshop focused on promoting improved means of authenticating the identities of individuals. To implement the Task Force's recommendation and to begin greater study of this area, the FTC and other Task Force agencies will hold a workshop to explore the means by which identity theft can be prevented through better authentication of individuals. The workshop will facilitate a discussion among public sector, private sector, and consumer representatives and will focus on technological and policy requirements for developing better authentication processes, including the incorporation of privacy standards and consideration of consumer usability.

identity theft

4

Andrew Patrick @ NRC

April 10, 2007

Identity theft is a term used to describe a variety of forms of impersonation and fraud.

Here we will concentrate on financial fraud done to obtain money from bank accounts and/or to commit credit card, loan, and mortgage fraud.

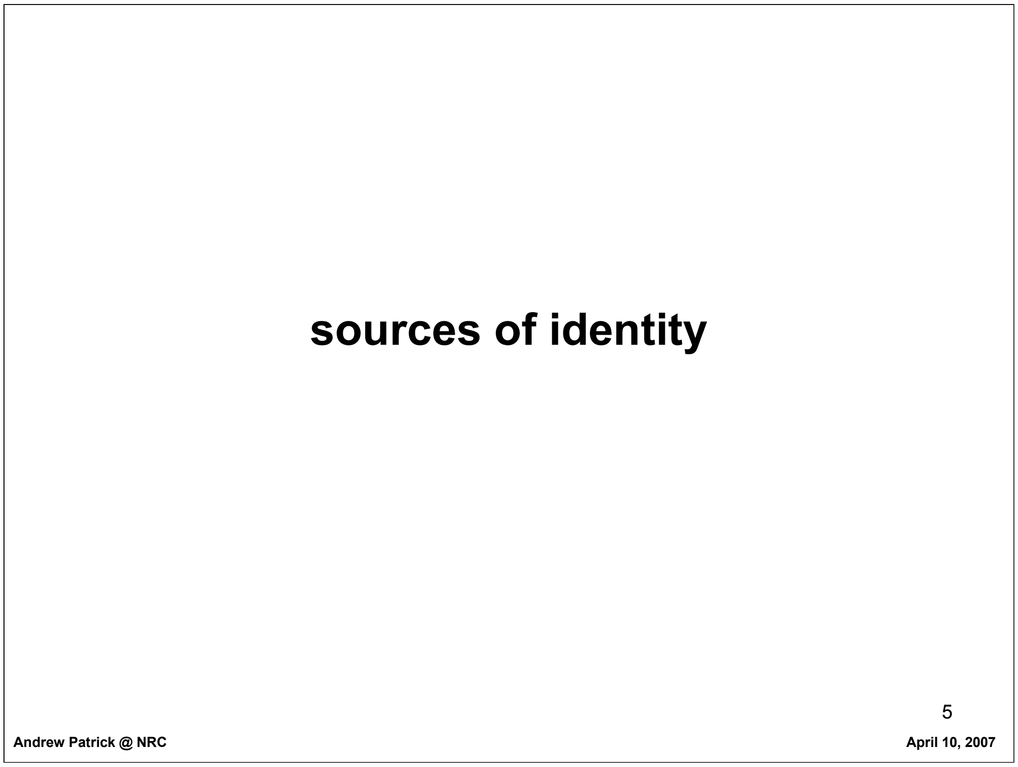
In a strict sense, someone's identity cannot really be stolen, but their money can be and their reputation and credit worthiness can be damaged so that making repairs can be costly, time-consuming, and frustrating.

Low-risk Identity Theft

- Cloning a credit card and making fraudulant purchases
- Cloning an ATM card and making fraudulant withdrawls

High-Risk Identity Theft

- cheque fraud
- Impersonating another person to obtain a bank loan



sources of identity

5

Andrew Patrick @ NRC

April 10, 2007

So where do the theives get the identity information:

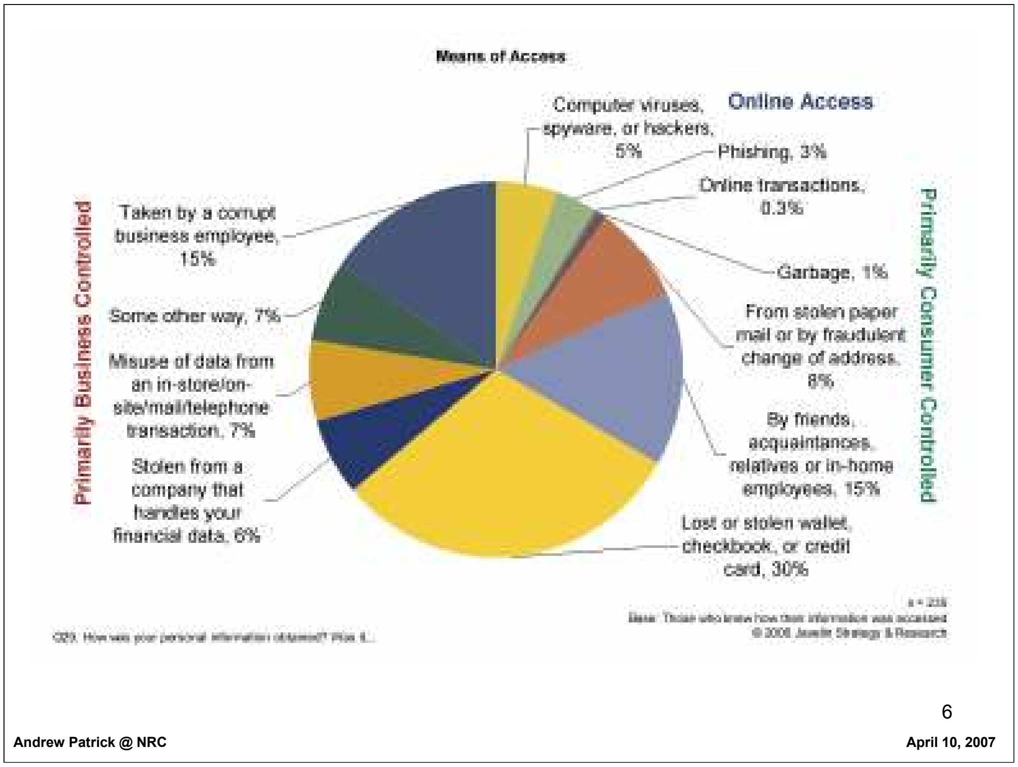
Old School

- stealing postal mail
- dumpster diving

New School

- phishing, pharming, etc.
- trojans
- bank card skimming
- data breaches

In many cases, they don’t have to gather the credentials themselves, they can buy them on the “open” market



n = 235
Base: Those who knew how their information was accessed
© 2006 Javelin Strategy & Research

Q29. How was your personal information obtained? Was it...

6

Andrew Patrick @ NRC

April 10, 2007

Of the cases where the source of

information breach was known, 63% were initiated by breaches of information that were

within the consumer's control. These fell into four major categories: 30% lost or stolen

wallets, credit/debit cards and checkbooks, 15% trusted associates, i.e., friends, family,

in-home employees and neighbors, 9% stolen mail or garbage and 9% home computers

(hacking, viruses and phishing). Fraud amounts from these cases encompass 73% of

the total fraud amount or $41.5 billion.

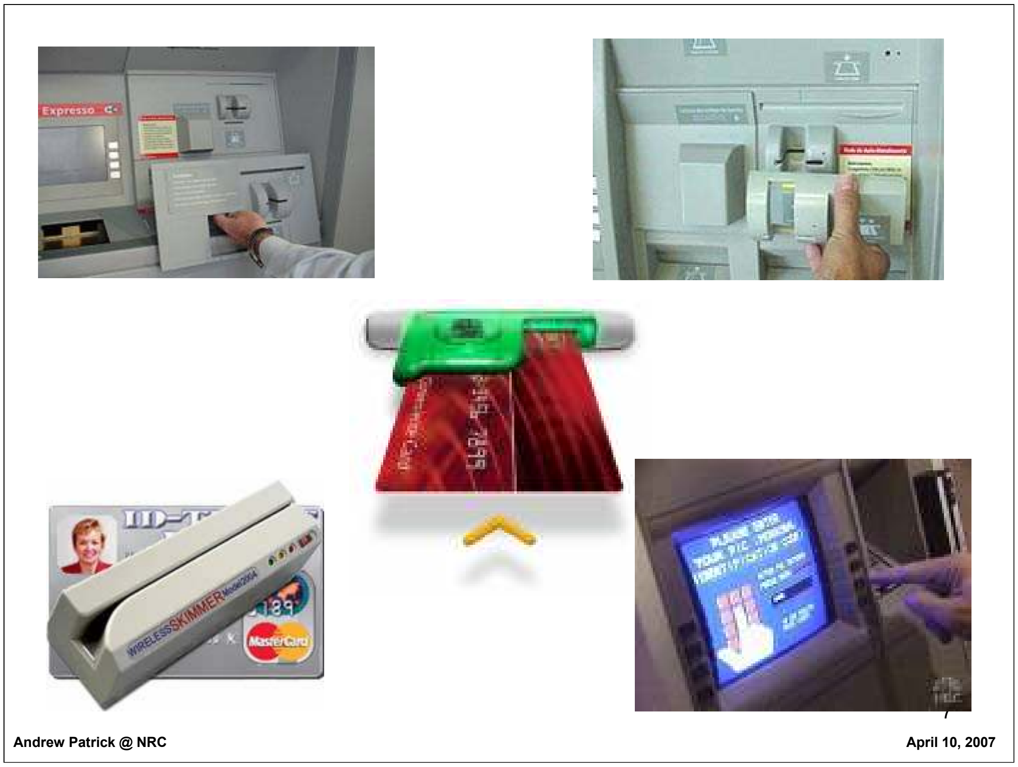
2006 Identity Fraud Survey

Report

January, 2006

Javelin Strategy and Research

http://www.javelinstrategy.com/products/99DEBA/27/delivery.pdf



7

Andrew Patrick @ NRC

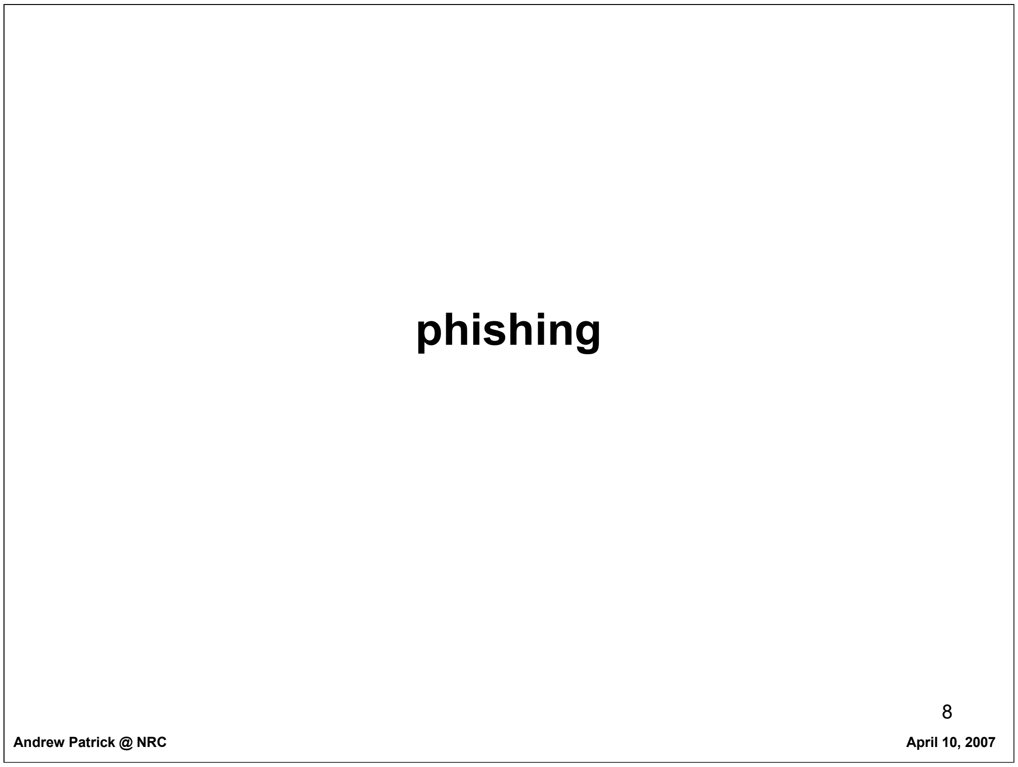
April 10, 2007

Card skimming

For ATM banking, there are various forms of fraud that have been encountered. Fake or doctored ATMs and point-of-sale terminals can be installed and, when a customer attempts to use the machine, the cards themselves or information stored on the cards (on the magnetic strip on the back of the card) can be obtained. The false machines can also record the PINs that are entered by the customers, and these can later be used to withdraw funds. ATM cards can also be cloned by obtained the card number or information from the magnetic strip. If the PIN can also be obtained, either by covert observation (shoulder surfing or hidden cameras), or by tricking the user into revealing it, then the false card can be used. Using fraudulent, or fraudulently obtained, ATM cards and PINs to withdraw cash from bank accounts is commonly called “cashing” and, as we will see, it is an important step in many of today’s successful identity thefts.

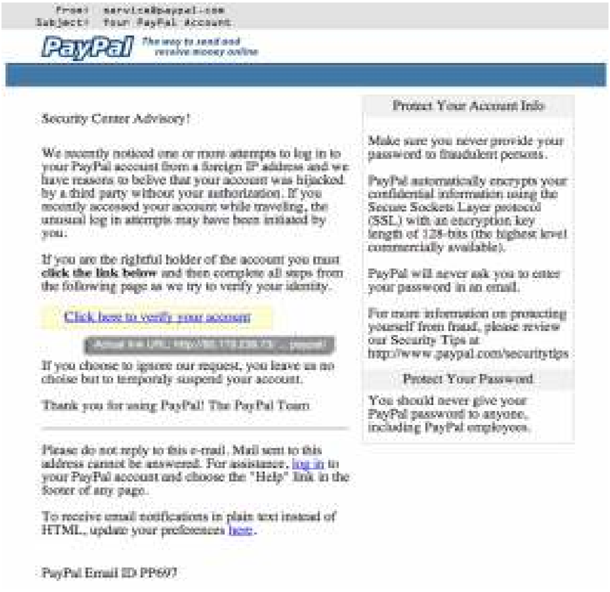
http://news.bbc.co.uk/1/low/business/3256799.stm

http://news.bbc.co.uk/2/hi/uk_news/england/3929549.stm



phishing

The most common method of identity theft related to online banking today is phishing. In phishing, a customer is tricked into revealing their identification information, which is then used for fraudulent transactions. Typically, phishing is done by sending email messages that claim to be from a financial institution. For some reason, usually related to protecting the customers’ security, the message instructs the recipient to verify their identification information. The messages provide a convenient link for the user to follow when updating their information. The problem is that the link is not to the authentic financial institution, but instead to a forged website. Here the identification information is collected and later used to commit impersonation and fraud. Various techniques have been used to create authentic-looking forgeries of financial web sites, and the authentication-related information provided within web browsers (such as the padlock icon) can also be forged.



From: service@paypal.com
Subject: Your PayPal Account

Security Center Advisory!

We recently noticed one or more attempts to log in to your PayPal account from a foreign IP address and we have reasons to belive that your account was hijacked by a third party without your authorization. If you recently accessed your account while traveling, the unusual log in attempts may have been initiated by you.

If you are the rightful holder of the account you must **click the link below** and then complete all steps from the following page as we try to verify your identity.

Click here to verify your account

Actual link URL: http://80.170.238.73 ... paypal/

If you choose to ignore our request, you leave us no choise but to temporaly suspend your account.

Thank you for using PayPal! The PayPal Team

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your PayPal account and choose the "Help" link in the footer of any page.

To receive email notifications in plain text instead of HTML, update your preferences here.

PayPal Email ID PP697

Protect Your Account Info

Make sure you never provide your password to fraudulent persons.

PayPal automatically encrypts your confidential information using the Secure Sockets Layer protocol (SSL) with an encryption key length of 128-bits (the highest level commercially available).

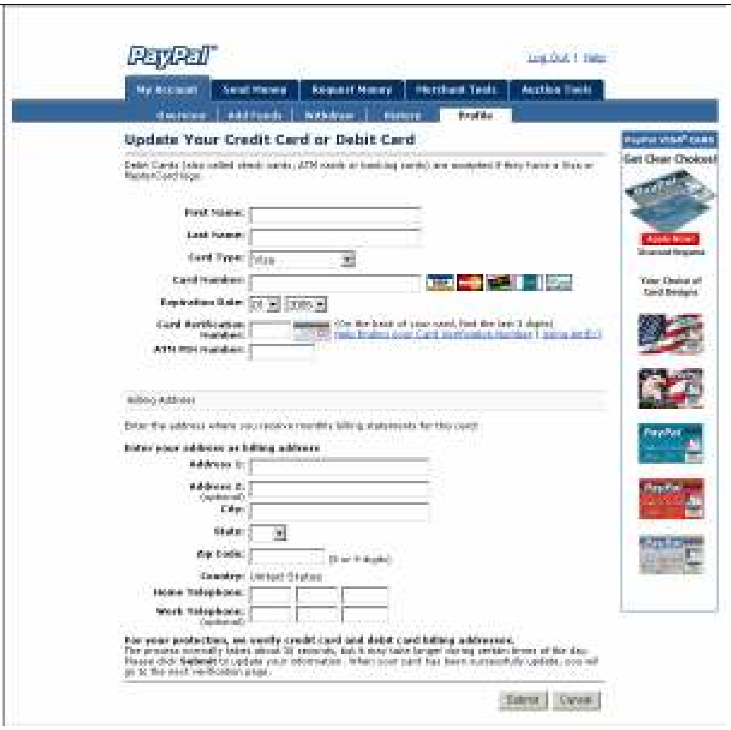
PayPal will never ask you to enter your password in an email.

For more information on protecting yourself from fraud, please review our Security Tips at http://www.paypal.com/securitytips

Protect Your Password

You should never give your PayPal password to anyone, including PayPal employees.

Link in the email does not lead to Paypal, but instead to a server in China.



Update Your Credit Card or Debit Card

Debit Cards (also called check cards, ATM cards or banking cards) are accepted if they have a Visa or MasterCard logo.

First Name:
Last Name:
Card Type: Visa
Card Number:
Expiration Date: 01 2005
Card Verification Number: (On the back of your card, find the last 3 digits)
Help finding your Card Verification Number | [illegible]
ATM PIN Number:

Billing Address

Enter the address where you receive monthly billing statements for this card.

Enter your address or billing address
Address 1:
Address 2: (optional)
City:
State:
Zip Code: (5 or 9 digits)
Country: United States
Home Telephone:
Work Telephone: (optional)

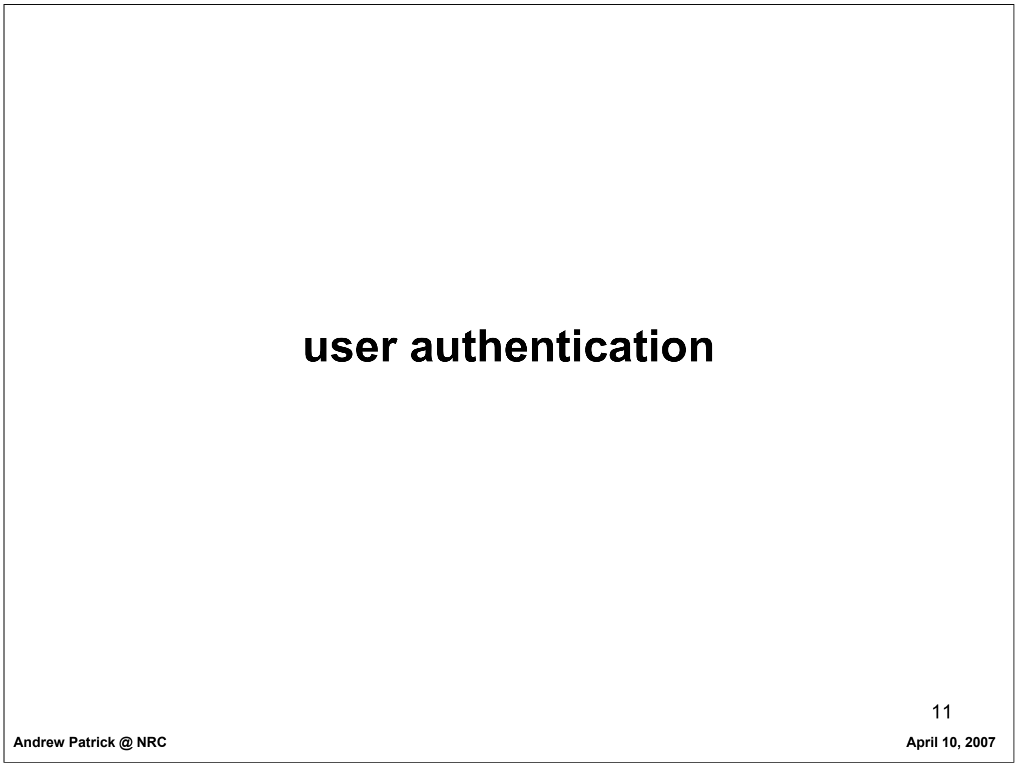
For your protection, we verify credit card and debit card billing addresses.
The process normally takes about 30 seconds, but it may take longer during certain times of the day. Please click **Submit** to update your information. When your card has been successfully update, you will go to the next verification page.

Submit Cancel

This attacks actually writes the address bar, making it harder to recognize as a scam.

- **Notice that the user is asked for their PIN for their bank card!**
- **This is the most common type of phishing attack because of the ease of “cashing” (to be discussed later).**

From the Anti-Phishing Working Group



user authentication

11

Andrew Patrick @ NRC

April 10, 2007

traditionally has been the username and password

Historically, we have used a variety of authentication factors. Most common was personal recognition and introductions among a network of people. When communicating at a distance, signatures and wax seals have been used to leave a mark or impression on documents so that they can be recognized as being authentic or not. The term indentured refers to an ancient practice where contracts could be cut into two pieces using a jagged (or toothed) pattern so that the two parts could be refitted to confirm authenticity. Secret passwords have also been used to confirm identity of individuals or groups, such as by sentries guarding a location. Today, the types of information and the forms of authentication have changed, but the fundamental issues remain.

passwords and PINs

12

Andrew Patrick @ NRC

April 10, 2007

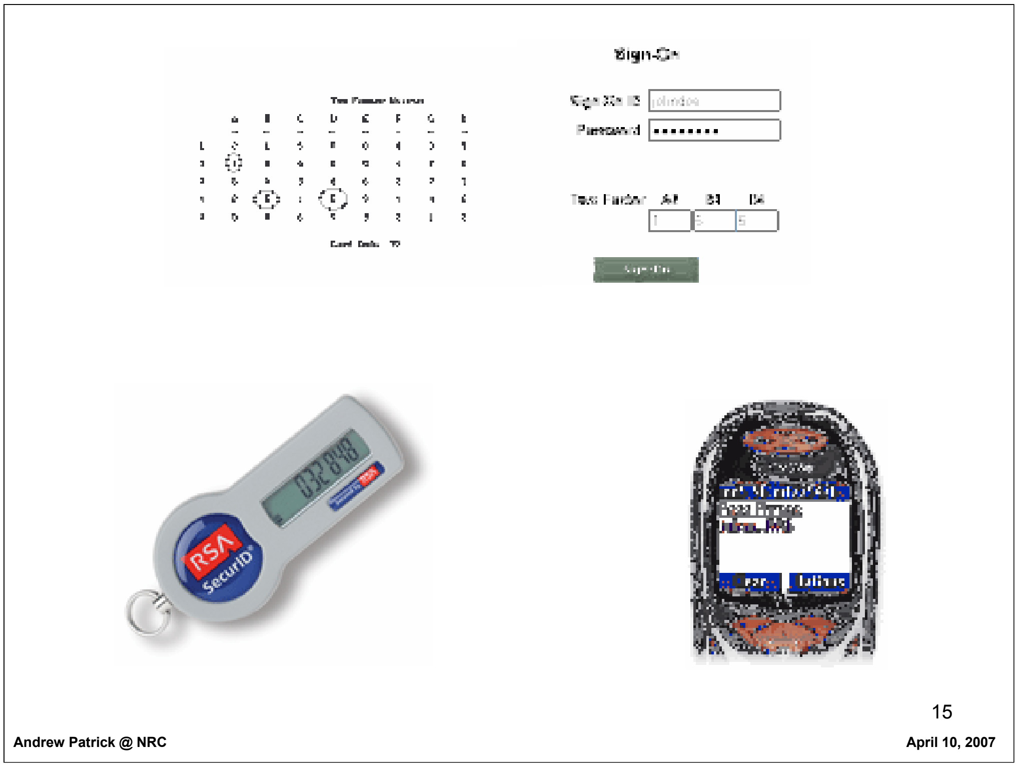
The primary method for authentication for online banking is a username and password. The username may be a person's given name, their bank account number, or the number on a bank card. The password is usually a string of characters (letters, numbers, and perhaps punctuation and symbols) assigned by the institution or, more commonly, chosen by the customer. So, online authentication uses a single authentication factor based on something you know. For authentication at ATM machines, the most common form of authentication is a bank or credit card and a PIN, where the PIN is again assigned or chosen by the customer. Thus, ATM banking involves two-factor authentication based on something you have (the card) and something you know (the PIN).

two-factor authentication

something you have (card, token)
something you know (password, PIN)
something you are or do (biometric, signature)

US banks

- Federal Financial Institutions Examination Council
- new requirements to implement two-factor authentication for Internet banking for high risk transactions



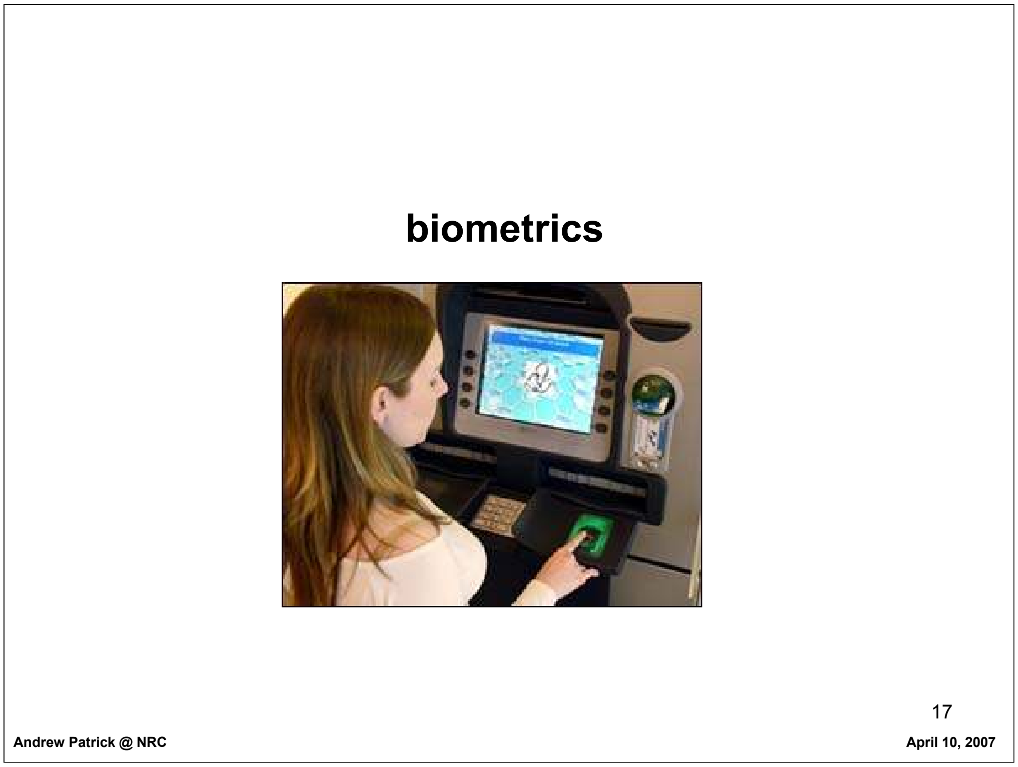
15

Andrew Patrick @ NRC

April 10, 2007

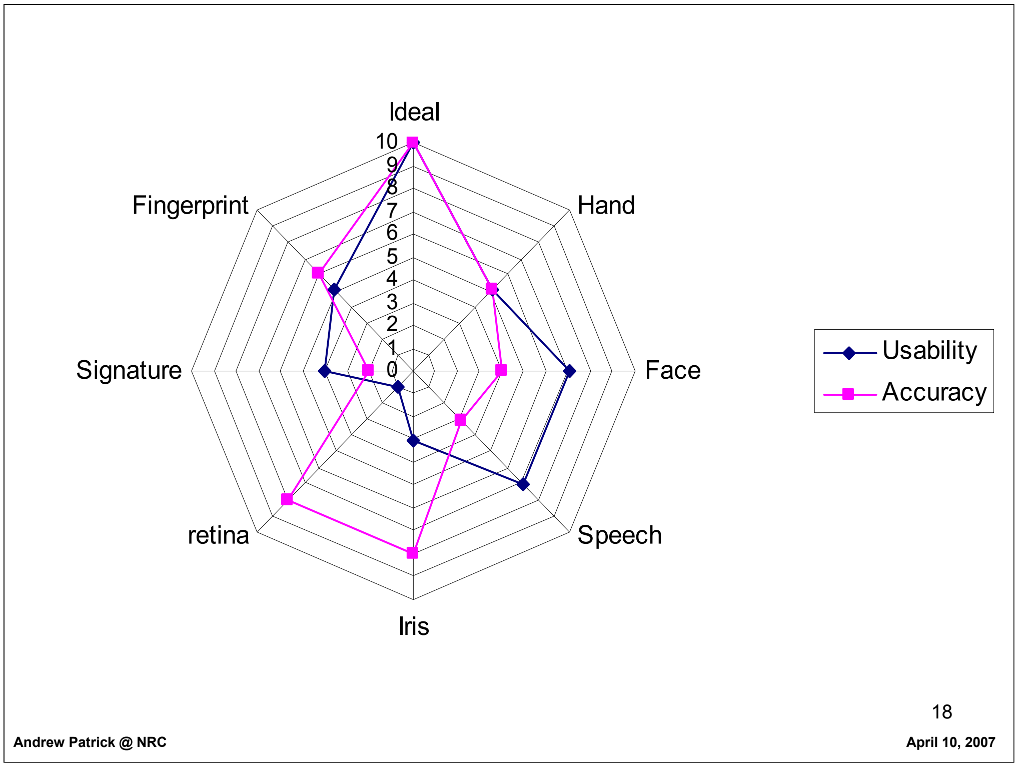
one-time passwords

challenge questions



biometrics

NEW TOPIC: biometrics

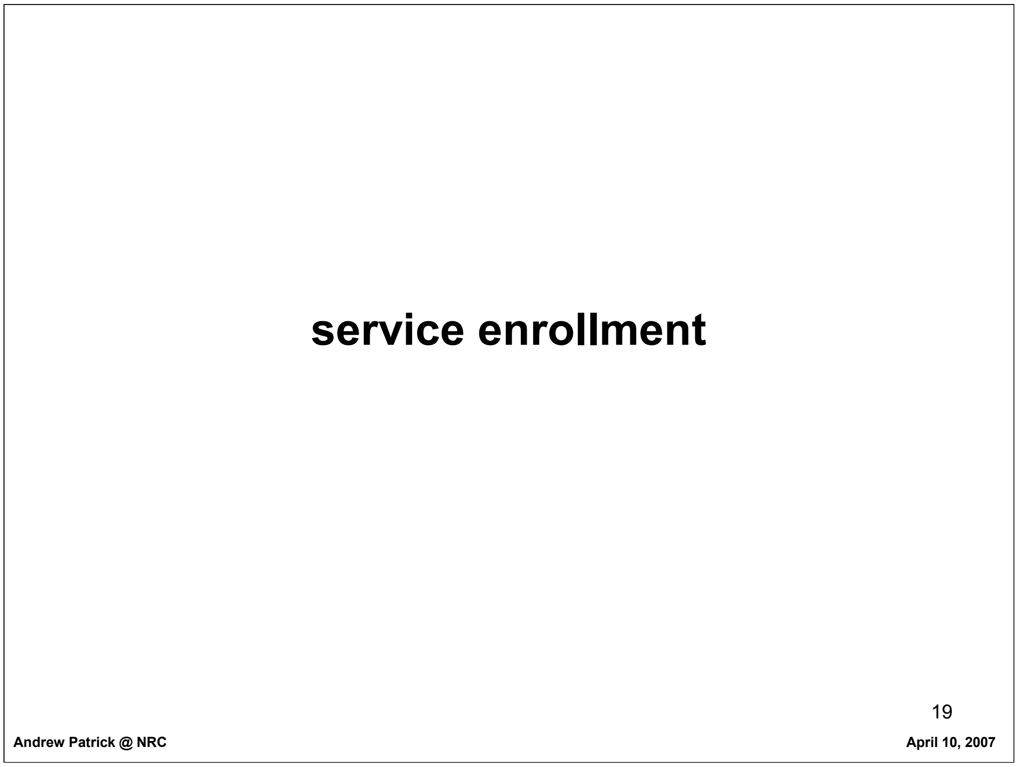


18

Andrew Patrick @ NRC

April 10, 2007

from Coventry book chapter



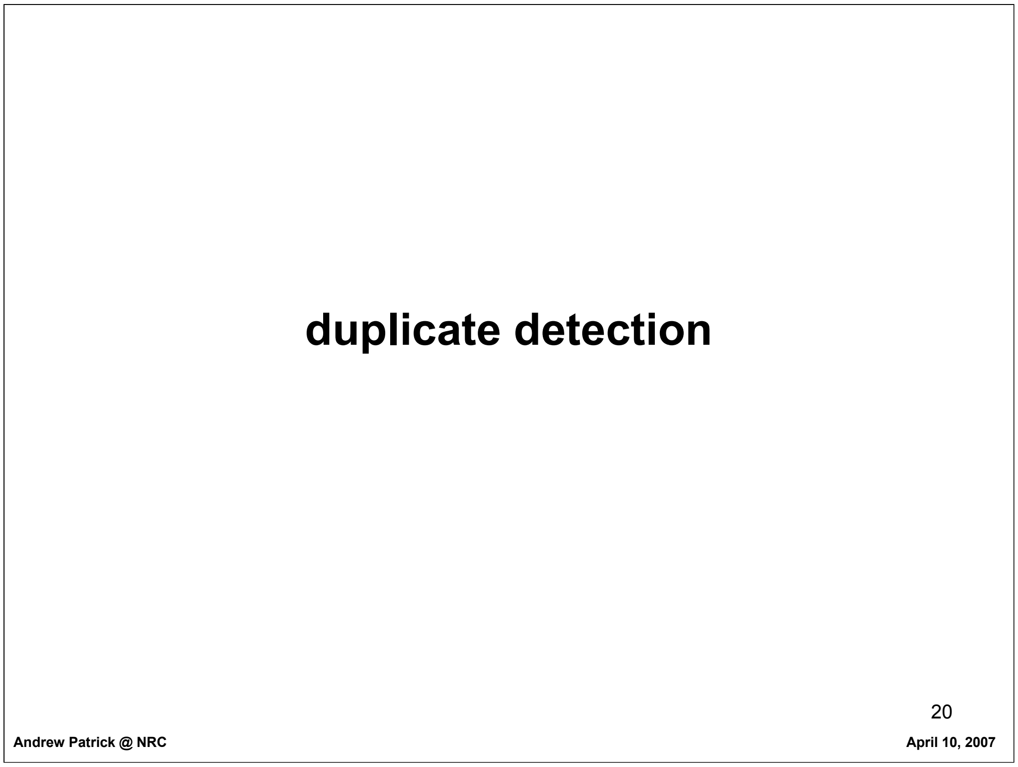
service enrollment

19

Andrew Patrick @ NRC

April 10, 2007

So, using biometrics during service enrollment is limited by the lack of biometric databases. Biometrics can be used, however, for authenticating any documents that are used to support an identity claim. If a document, such as a driver's license, is linked with biometric information, such as a fingerprint, then an authentication decision can be made about whether a particular customer's fingerprint matches the one associated with the driver's license. This really represents someone using the driver's license service as a form of authentication, and we will discuss using biometrics for service use below.



duplicate detection

The Government Accountability Office recently reported that the Federal Emergency Management Agency (FEMA) may have improperly disbursed more than $1 billion by not validating the identity of aid registrants in the wake of hurricanes Katrina and Rita. The GAO cited the example of one person receiving $139,000 in aid by registering 13 times using different Social Security numbers. Other recipients altered their own names or addresses or borrowed names from children or prisoners to obtain extra aid.

The state of California, and others, are using biometric technologies to prevent such fraud. The California database used for social programs contains 6 million fingerprint images and photographs (2004 data) and is believed to be responsible for annual savings of $68 million.

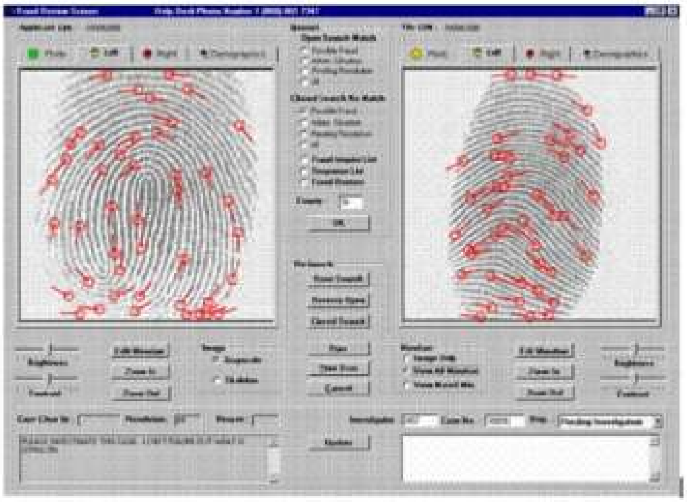
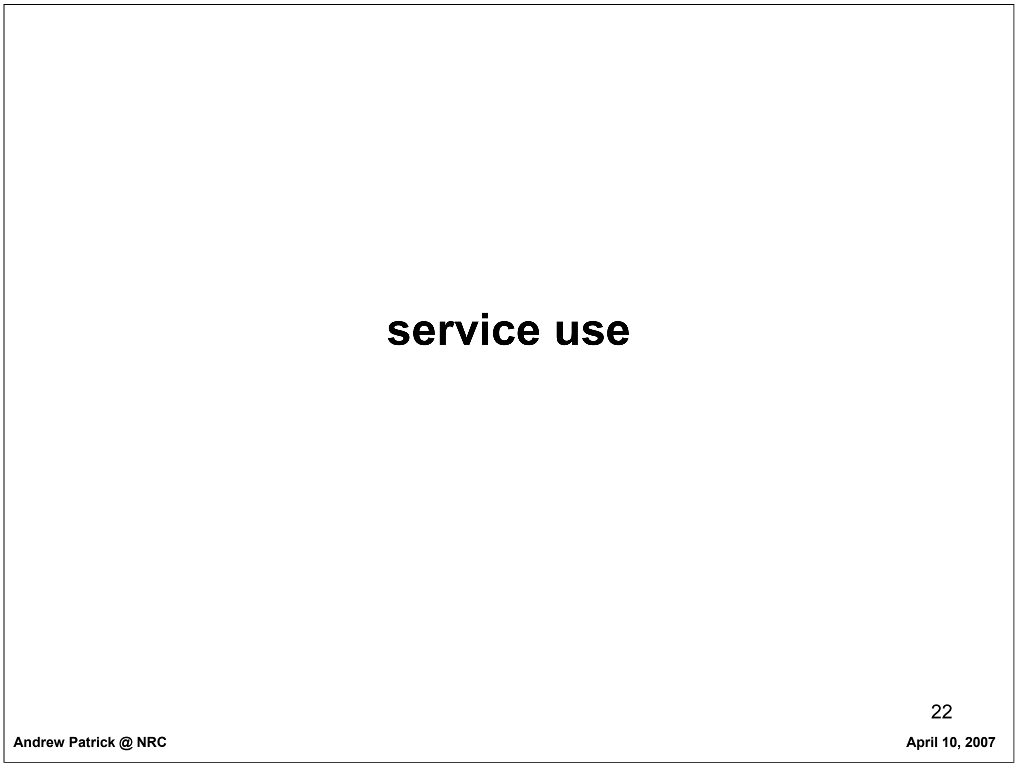


Exhibit: Fraud Review Screen View All or Mated Minutiae

Using biometrics for duplicate detection is not easy, however. Each comparison of biometric information has a chance of producing an error. Errors can come about by failing to match a database record when there should have been a match (a false non-match), or by matching a database record when there should not have been a match (a false match). Vendors of biometric systems strive to have the lowest possible error rates, but no system is perfect. Moreover, as the size of the database grows, the chances of making errors can increase.

The result is that for serious biometric applications, such as detecting welfare fraud, there needs to be a human component added to the automatic biometric matching. In California, for example, all cases where a new applicant is matched to an existing record in the database, which could be fraud or a false match, are referred to a trained Fraud Investigator. The investigator does a side-by-side comparison of the fingerprints, photographs, and demographic information before making any conclusions about possible fraud. The same process is also done in cases where an apparent returning applicant fails to match their existing record in the database, which could be fraud or a false non-match. Depending on the system error rates, the fraud investigations can be time-consuming and costly.



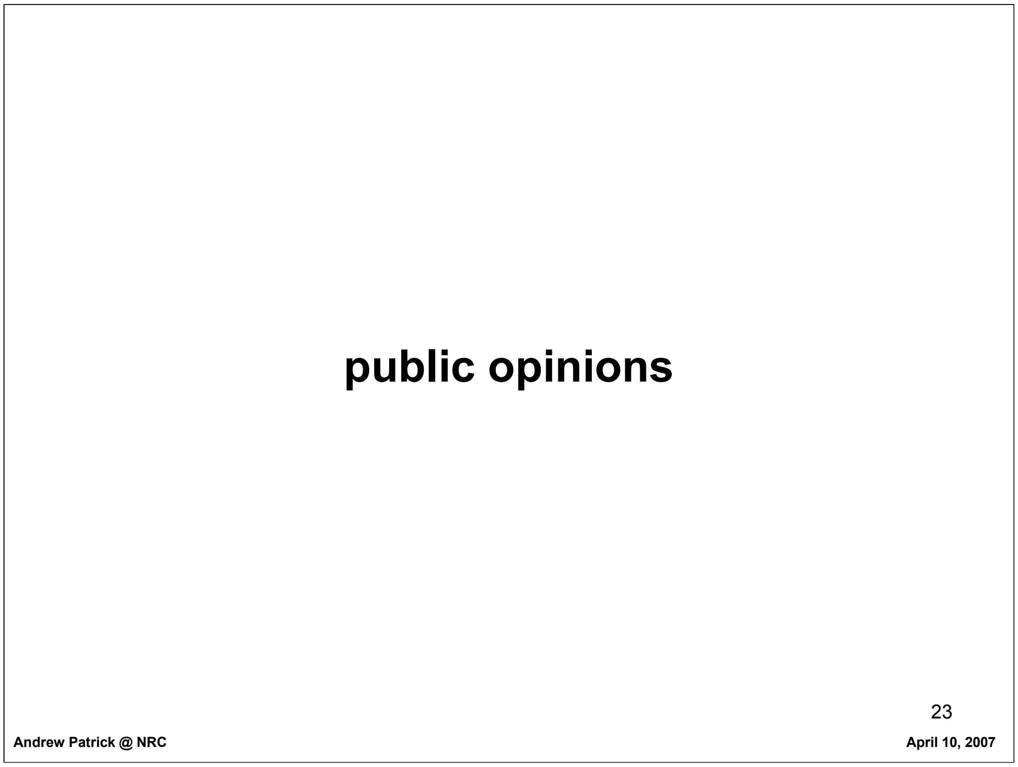
service use

22

Andrew Patrick @ NRC

April 10, 2007

This form of authentication is often being used to verify the accuracy of some kind of document or credential. So, for example, biometric passports (or e-passports) can contain stored information about faces or fingerprints, and the authenticity of the claim that this is an individual’s passport can be made by a 1:1 biometric comparison. Since there is only one comparison being made, the accuracy for authentication decisions can be higher than that for service enrollment. (A service might still choose to use 1:N comparisons if they want to perform authentication using the biometric alone, but the size of the N would probably be limited to the list of current customers rather than an entire population.)



public opinions

23

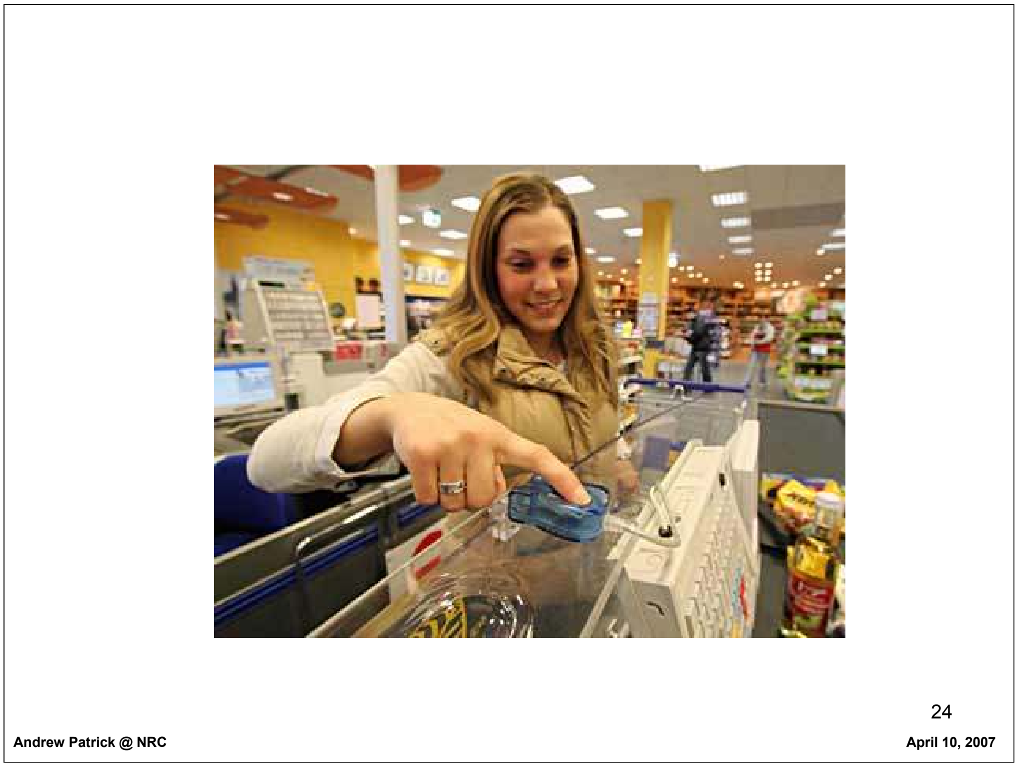
Andrew Patrick @ NRC

April 10, 2007

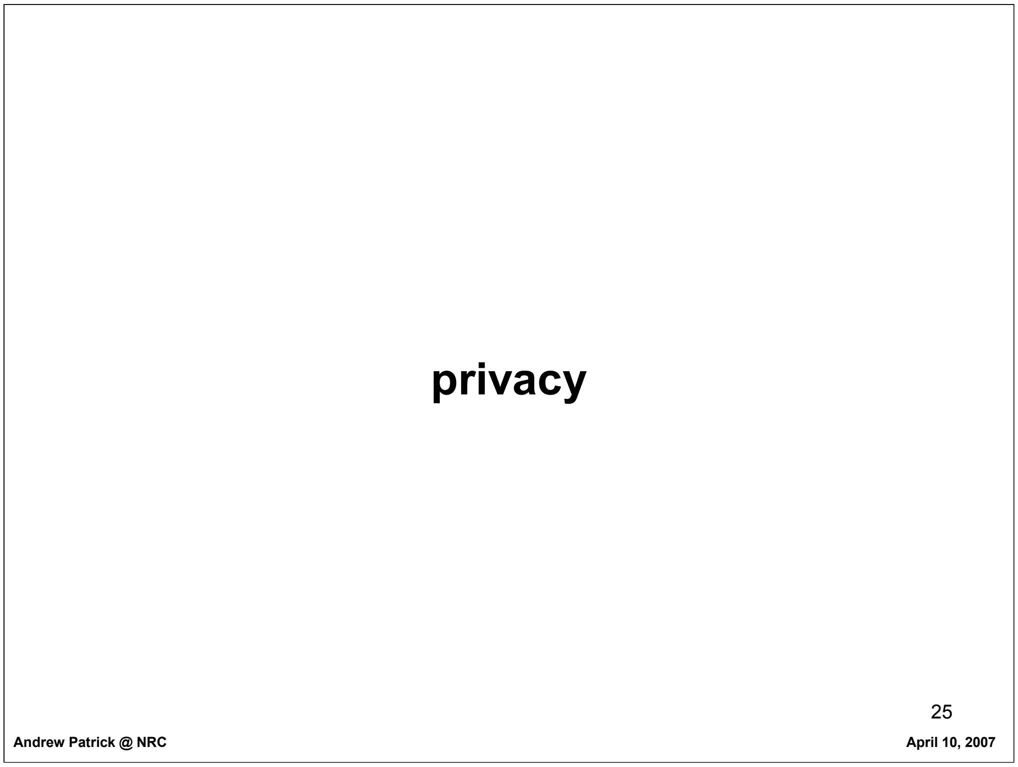
- opinion polls show growing support
    - According to a recent poll by Truste, 82 percent of Americans "support the use of
      biometric identification on passports," 75 percent support adding biometrics to driver's licenses, and 73 percent support adding it to social-security cards.

But there are problems:

- security as an “enabling task” that gets in the way (Sasse)
- biometrics can be seen as unhygienic, stressful (Coventry)
- some fear of bodily harm to obtain biometric information (movies)
    - union at Pearson airport objecting to iris recognition due to infra-red light
- lack of understanding about biometric templates and storage mechanisms
- some cross-cultural differences (within Europe; US/Canada)



http://www.byz.org/~rbanks/movableType/webLog/trends/archives/cat_6_business_workspace.html



privacy

25

Andrew Patrick @ NRC

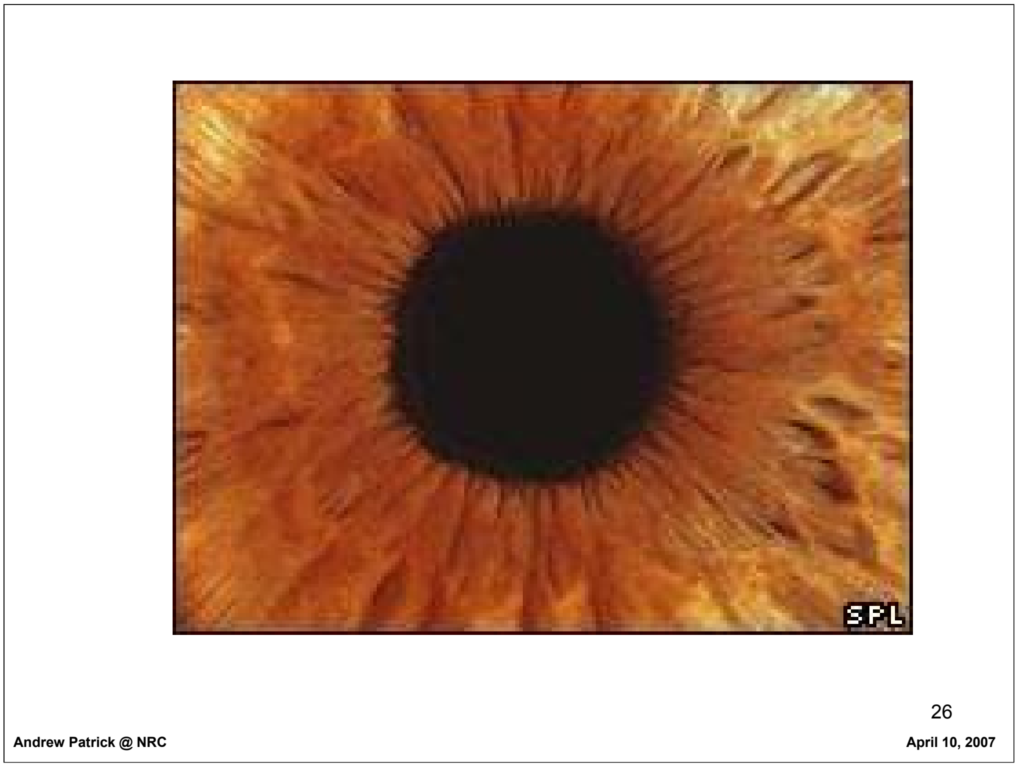
April 10, 2007

- deployments likely covered by provincial and/or federal **privacy legislation**

- **privacy impact assessments** would be required

- some **tools** and **guidelines** are emerging
  - bioprivacy.org
  - Ontario Privacy Commissioner recommendations for possible Toronto anti double-dipping deployment

- **require**: encryption, single use, no match to latents, strict access controls, separate storage of personal information



26

Andrew Patrick @ NRC

April 10, 2007

Researchers have conducted a study looking at certain structural patterns in the iris and self-report personality characteristics. Prior research has shown that genetic differences may influence both brain and iris development, so a correlation between iris appearance and behavior is possible. Although the correlations found in this study were small, they do appear to be consistent and specifically related to some iris characteristics but not others. An analysis of effect size showed that the personality differences were “much larger than, for example, women’s tendency to be more emotional than men.”

The implication for iris-based authentication mechanisms is interesting. If iris characteristics are possibly related to personality, then privacy concerns about who gets to capture, examine, and store iris images become more important. What might a government agency or an insurance company due with information that someone possesses personality characteristics (and perhaps genetic markers) related to approachability or impulsiveness?

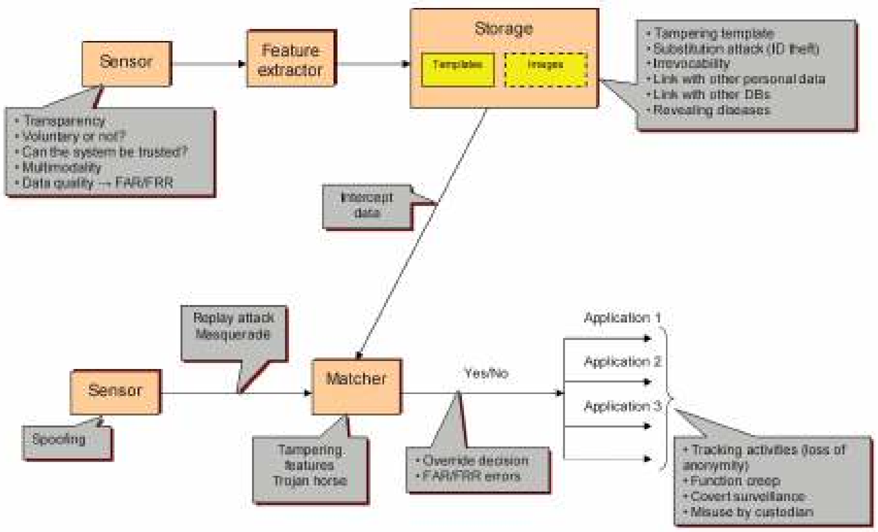
How irises ‘reveal personalities’

The team, led by Dr Matt Larsson a behavioural scientist, said: “These findings support the notion that people with different iris configurations tend to develop along different trajectories in regards to personality. “Differences in the iris can be used as a biomarker that reflects differences between people.”

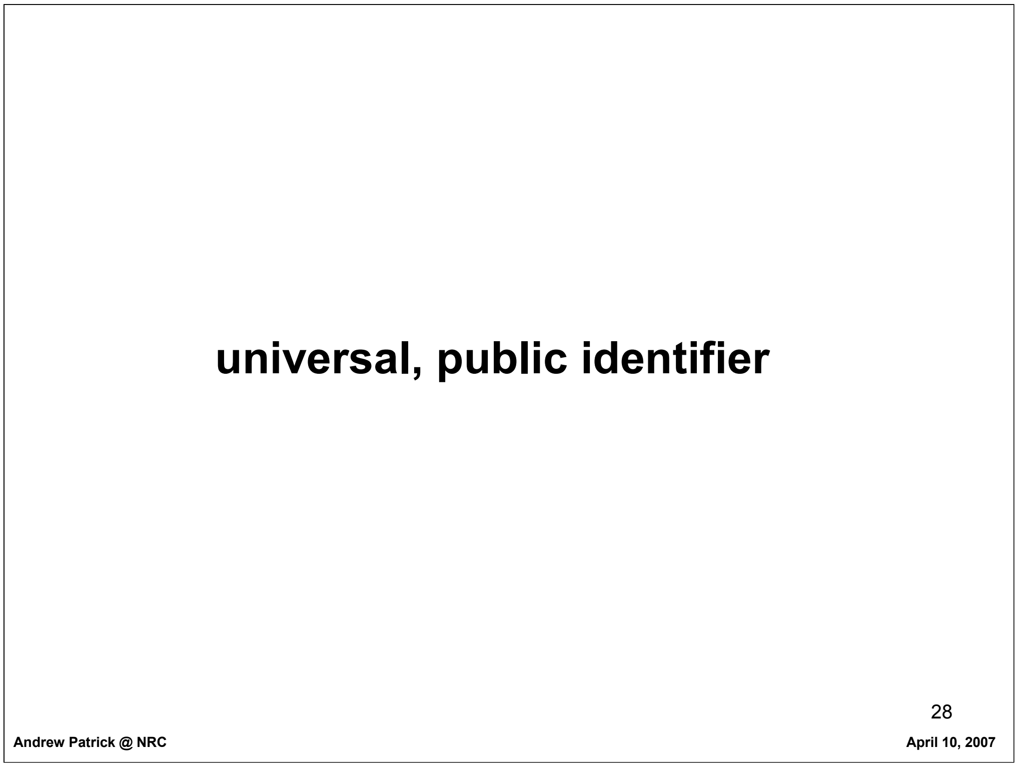
The article is available at

ScienceDirect

Figure 1: Privacy and security issues involving a biometric system



Ann Cavoukian and Alex Stoinov, Biometric encryption. March 2007



universal, public identifier

28

Andrew Patrick @ NRC

April 10, 2007

- biometrics provides a universal, public identifier
- this leads to universal risk
- what is usually needed is a specific, secret identifier

Clip from the film Minority Report, starring Tom Cruise

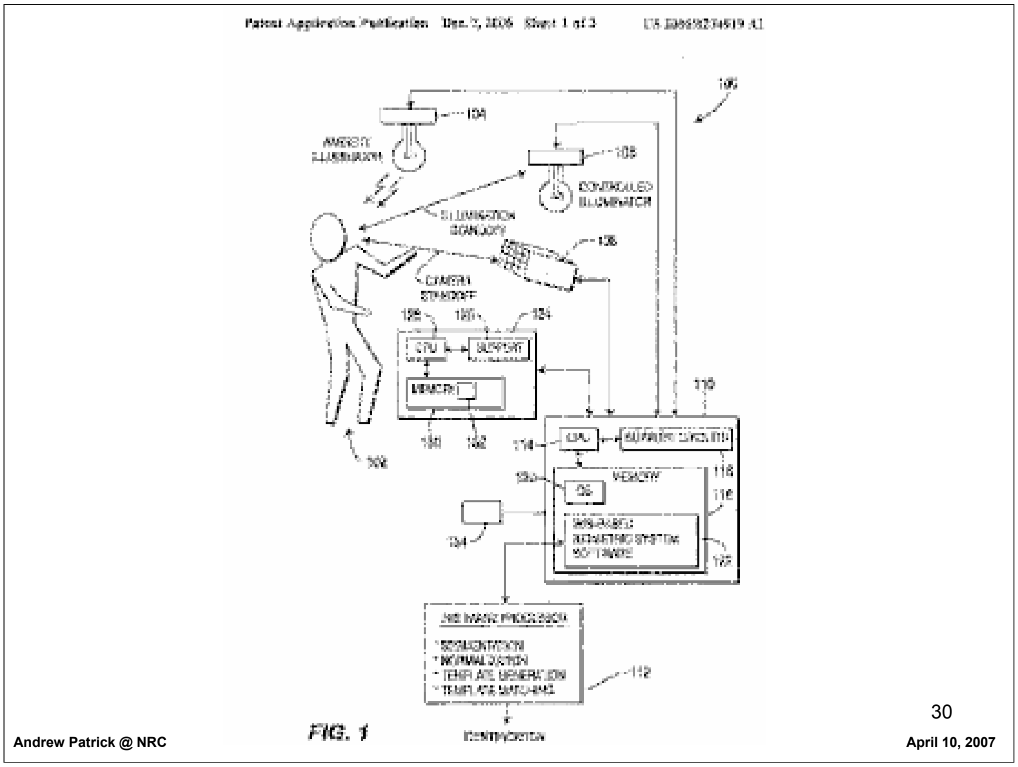

Patent Application Publication Dec. 7, 2006 Sheet 1 of 3 US 2006/0274919 A1

FIG. 1

30

Andrew Patrick @ NRC

April 10, 2007

Sarnoff patent application for iris biometric information from moving subject

similar to Minority Report

array of cameras that capture multiple images until at least one good one is obtained

increased risk

31

Andrew Patrick @ NRC

April 10, 2007

- biometrics only as good as the registration process and the security mechanisms
- violations can lead to increased risk if there is a false sense of security
- can lead to a false sense of confidence in the authenticity of transactions

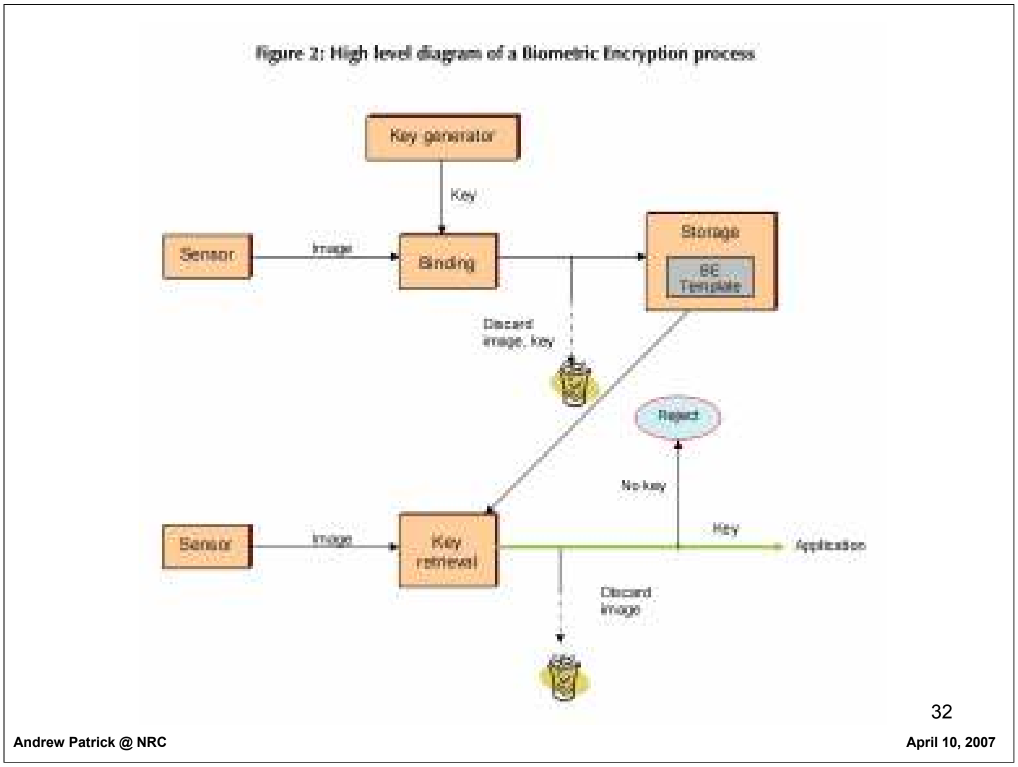


Figure 2: High level diagram of a Biometric Encryption process

32

Andrew Patrick @ NRC

April 10, 2007

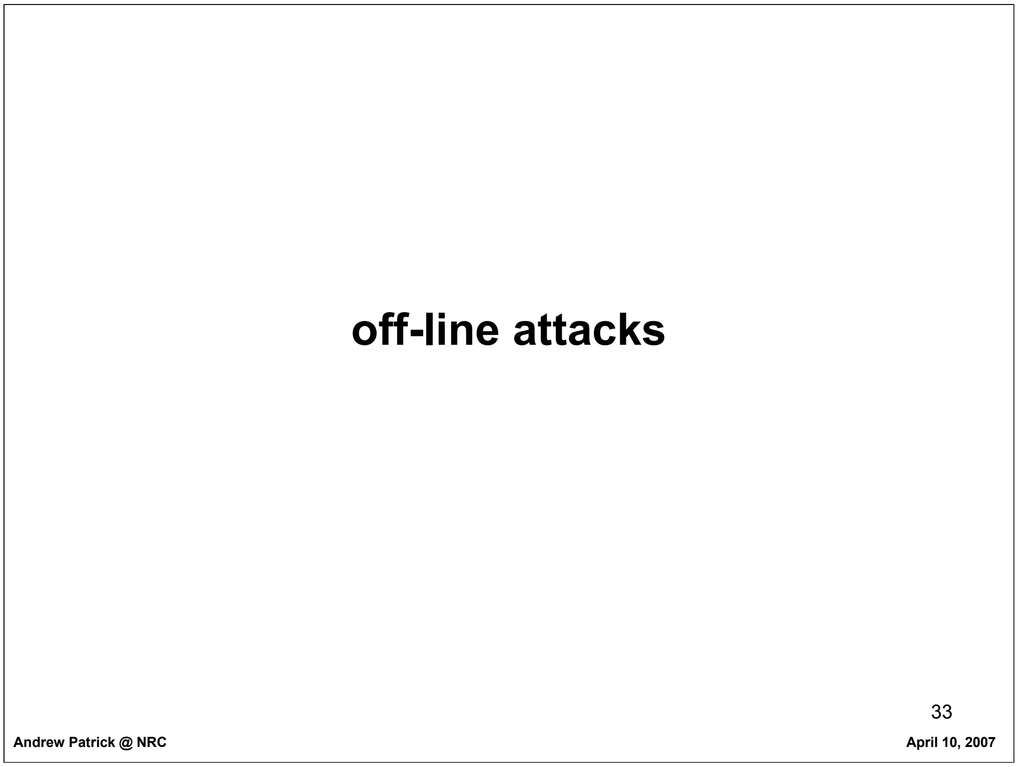
Ann Cavoukian and Alex Stoianov, Biometric encryption, March 2007

A third approach is to transform the biometric information so that it is unique to the application context. In the “cancelable biometric” scheme proposed by IBM, a fingerprint image might be systematically distorted or scrambled in some secret way before it is stored and used. If the fingerprint information is every stolen, it will be useless without knowing the kind of distortion that was used.

A related technology is “biometric encryption,” where biometric information, such as a fingerprint, is mathematically combined with a complex password or key and the resulting “private template” is stored. After enrollment, the fingerprint and the password are destroyed and only the private template is kept. During service use, the fingerprint is presented again and it is used to process the private template and regenerate the key. Again, the fingerprint is immediately destroyed, but the extracted key can now be used to gain access to a system or to unencrypted data.

The Ontario Privacy Commissioner has recently reviewed the privacy-enhancing characteristics of biometric encryption. With biometric encryption the biometric information is not saved, either as an image or a traditional template, so the risk of privacy breaches is eliminated. Also, since the complex key that is bound to the biometric can be unique to each application, there is no possibility for linking database records and function creep.

Biometric encryption does present some technical challenges. In order for the key to be successful recreated during authentication, the biometric information (e.g., the fingerprint) has to be very similar to the information used during enrollment to create the private template. Since each biometric sample will differ because of orientation on the reader, environmental conditions, dirt, sweat, etc., biometric encryption systems have to be designed to have some tolerance for “fuzzy” biometric matches. The current evidence suggests that iris images may provide the most consistent biometric samples that are needed for biometric encryption, and more research is underway.



off-line attacks

33

Andrew Patrick @ NRC

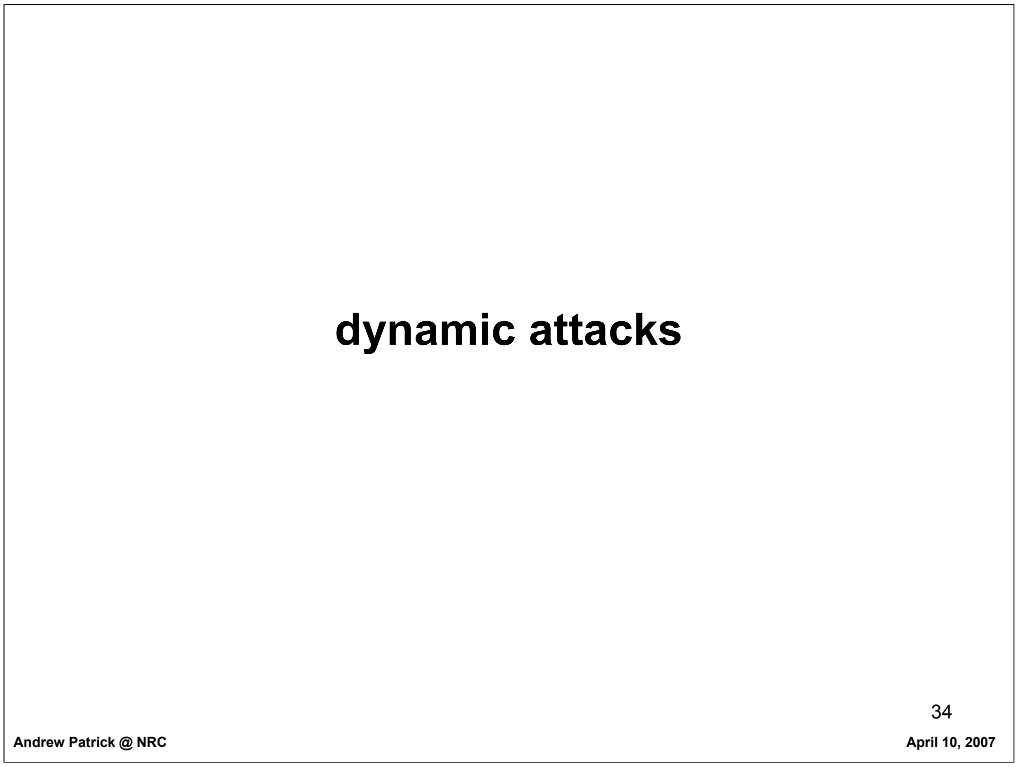
April 10, 2007

these authentication methods work against simple off-line attacks where credentials obtained by

•data breaches,

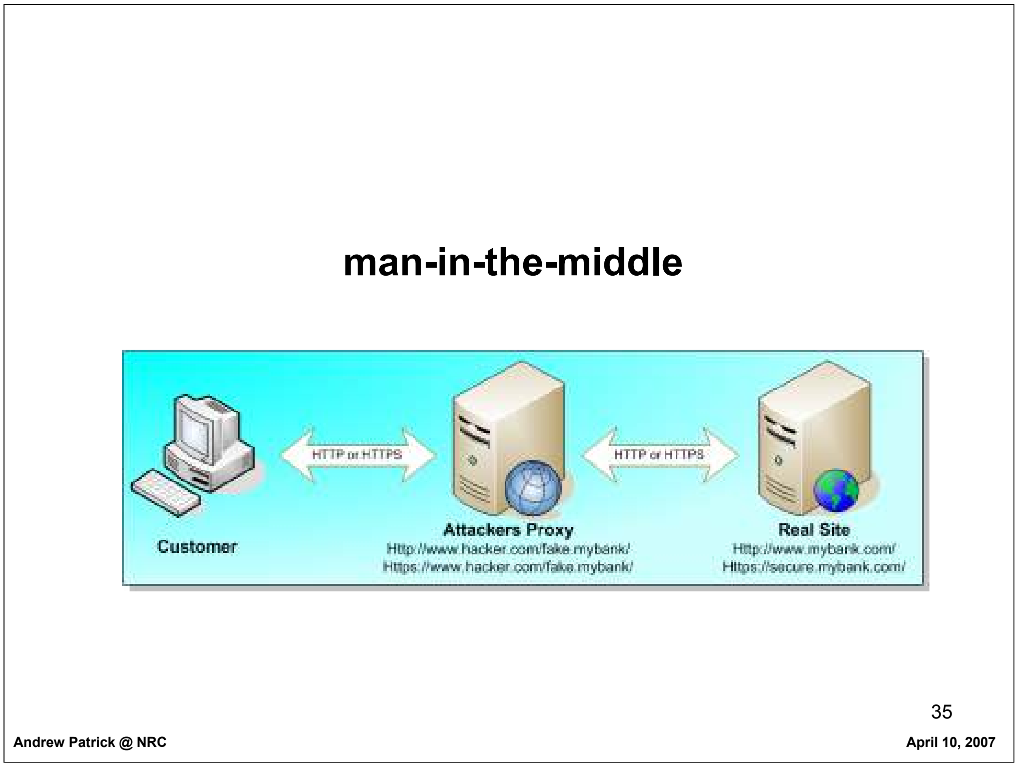
•simple phishing,

•key loggers



dynamic attacks

does not work against dynamic attacks



man-in-the-middle

HTTP or HTTPS
HTTP or HTTPS
Customer
Attackers Proxy
Http://www.hacker.com/fake.mybank/
Https://www.hacker.com/fake.mybank/
Real Site
Http://www.mybank.com/
Https://secure.mybank.com/

35

Andrew Patrick @ NRC

April 10, 2007

the user does all the authentication

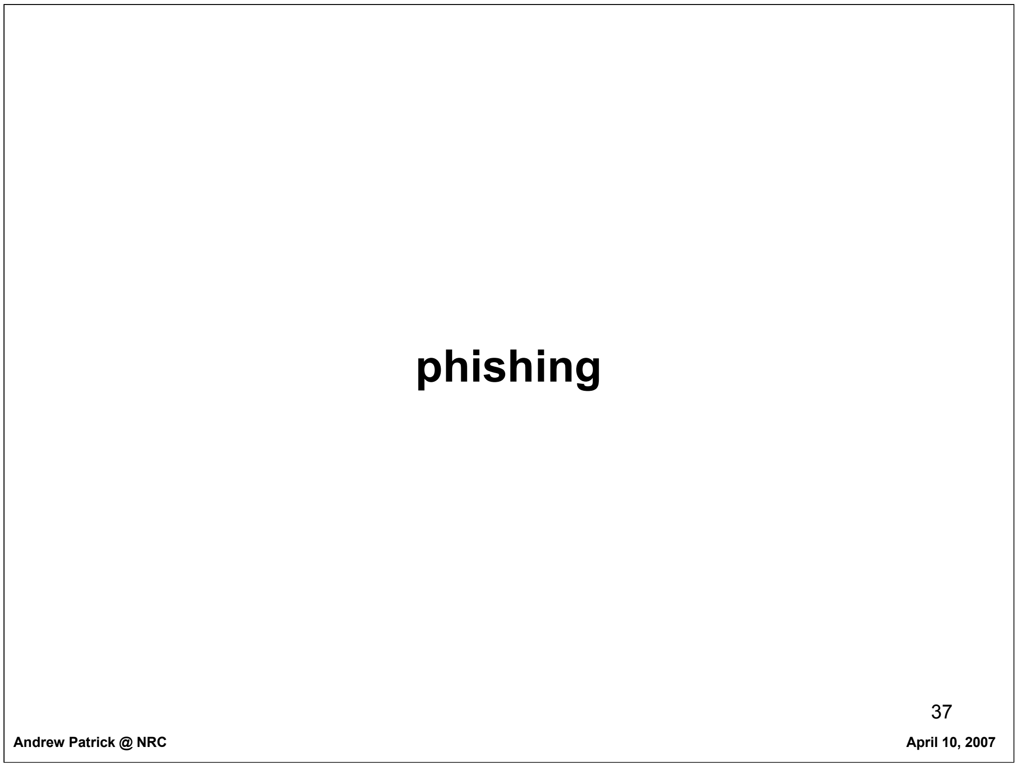
site authentication

36

Andrew Patrick @ NRC

April 10, 2007

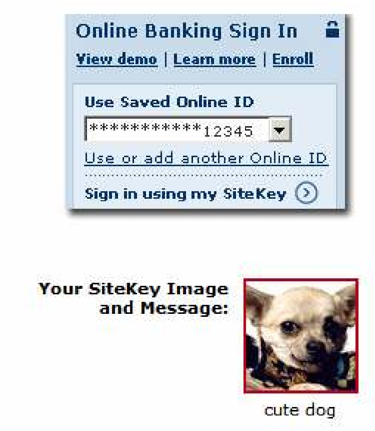
- authenticating the site to the user
- used to prevent phishing attacks



phishing

SSL certificates

- •supposed to provide site authentication
- •but, we have seen, anybody can buy a certificate
- •and many web sites don’t use them properly (e.g., http on page with login form)
    - •see Canadian Internet Registration Authority, cira.ca
- •and browsers/users not good at checking certificates



Online Banking Sign In

Use Saved Online ID

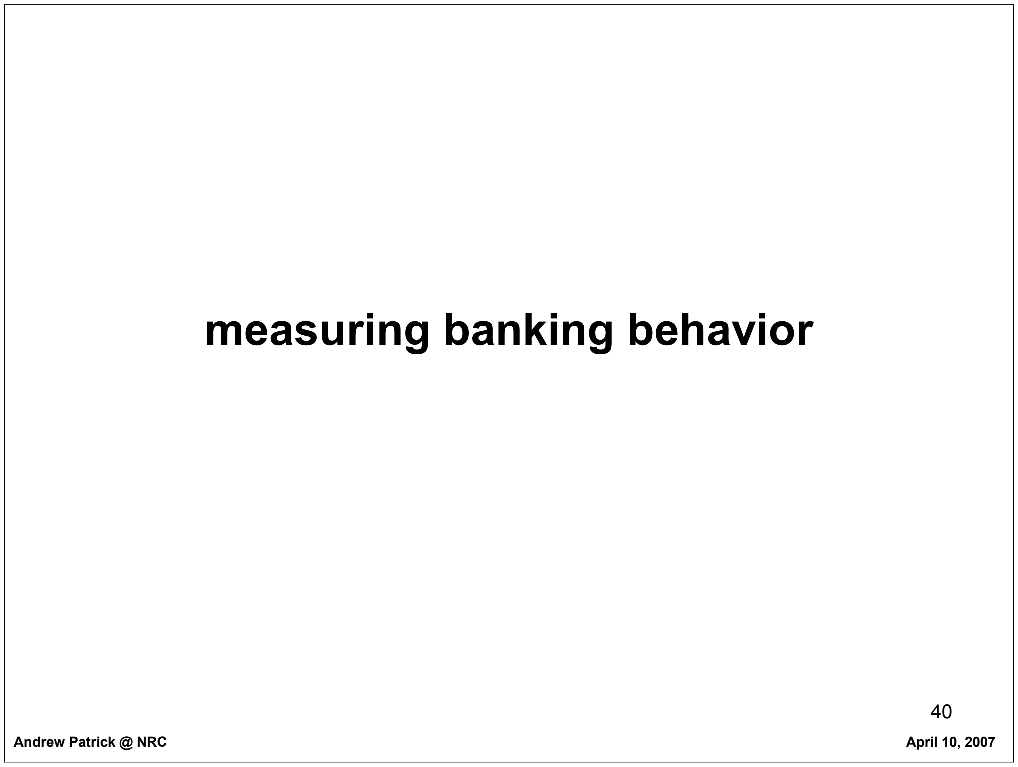
***********12345

Your SiteKey Image and Message:

cute dog

SiteKey

- •method used by Bank of America to identify site
- •requires users to notice that the personalized keys are not present during this transaction
- •combined with machine fingerprinting, so challenge question presented if login from new machine
- •does not protect against bad user behavior (see Schecter article and my critique)
- •does not project against man-in-the-middle attacks and trojans
- •at least one man-in-the-middle attack against SiteKey seen in the wild!



measuring banking behavior

Stuart Schechter, Rachna Dhamija, Andy Ozment, and Ian Fischer, working at MIT and Harvard, reported is a study that involved having people repeatedly login into an unnamed bank (presumably Bank of America) that has recently installed new security indicators to help prevent phishing attacks. The bank is using SiteKey, which is a system that allows a user to choose an image and piece of text at registration time, and they are instructed to check for that image again each time they access their bank account.

•biased sampling for participants – those with privacy concerns eliminated

•demand characteristics – expectations set by setting and researchers

•task focus – users asked to complete banking tasks

•obedience to authority – participants surprisingly compliant with many requests

1

Andrew Patrick @ NRC

April 10, 2007

•bad software running on the client computer

•installed via luring, piggy backing, viruses (e.g., Super Bowl web site used JavaScript exploit in unpatched computers)

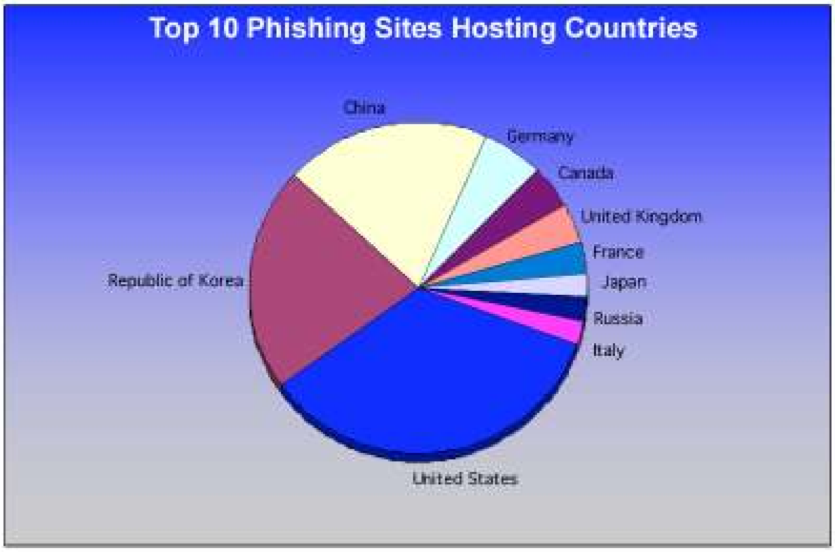
•most common Trojans are shells designed to download specific software

•can hijack secure financial sessions and insert fraudulent transactions

•relies on the user to do all the authentication for it

•part of Greek mythology

•The Greek siege of Troy had lasted for ten years. The Greeks devised a new ruse: a giant hollow wooden horse. It was built by Epeius and filled with Greek warriors led by Odysseus. The rest of the Greek army appeared to leave, but actually hid behind Tenedos. Meanwhile, a Greek spy, Sinon, convinced the Trojans that the horse was a gift despite the warnings of Laocoon and Cassandra; Helen and Deiphobus even investigated the horse; in the end, the Trojans accepted the gift. In ancient times it was customary for a defeated general to surrender his horse to the victorious general in a sign of respect. It should be noted here that the horse was the sacred animal of Poseidon; during the contest with Athena over the patronage of Athens, Poseidon gave men the horse, and Athena gave the olive tree.


Top 10 Phishing Sites Hosting Countries

From the Anti-Phishing Working Group, December 2006 data.

The most common host for fake phishing sites is the USA, because of trojans and “zombie” computers.

43

Andrew Patrick @ NRC

April 10, 2007

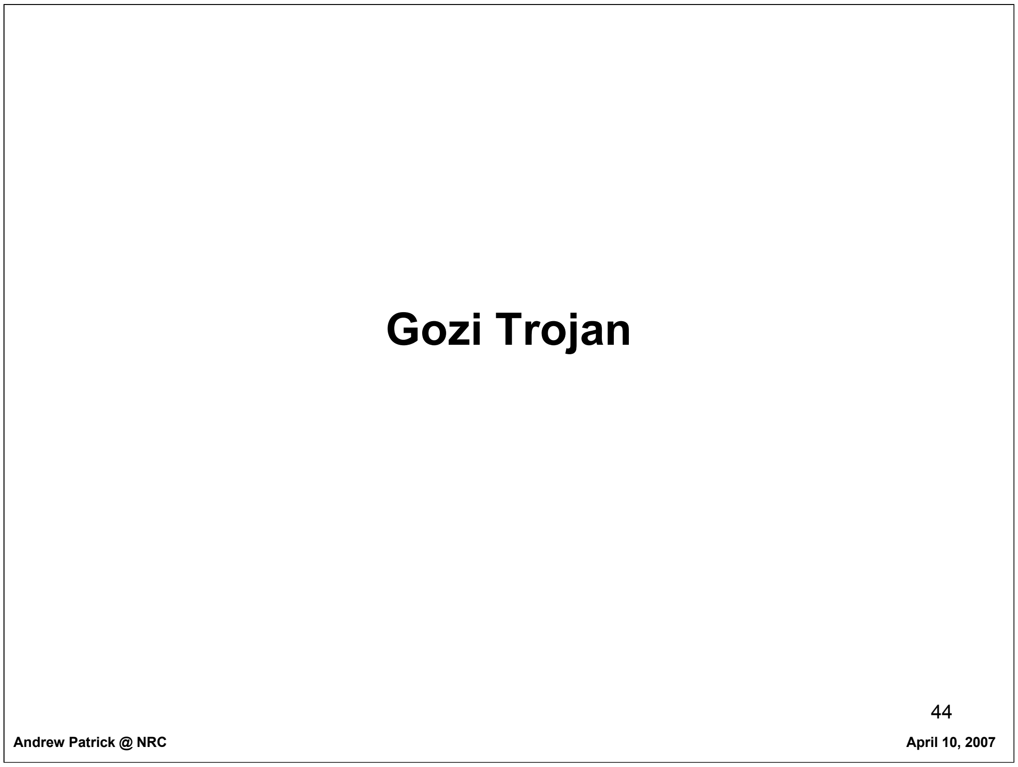
“Zombies” are computers that are being controlled remotely in order to do malicious tasks.

Zombies organized together into “botnets” for efficient control. These are often rented out to cyber criminals.

Estimates are that 80% of spam email is sent by Zombies. New zombies believed to responsible for the massive increases in spam over the past 3-4 months

Zombies also used for phishing, distributed denial of service attacks, and click fraud.

•distributed denial of service attacks are often against anti-spam organizations and other spammers



Gozi Trojan

http://www.secureworks.com/research/threats/gozi/

- **is installed automatically simply by visiting an infected web site**
- **is invisible to the user**
- **is often missed by anti-virus software**
- **is able to steal identity information even if it is encrypted using https**
- **efficiently collects large amounts of information and sends it to a “mother ship”**
- **provides an interface for fraudsters to easily purchase the stolen data**
- **is been used to collect thousands of login credentials at major banks and government agencies**
- **has not been shut down**
- **is only one of many such programs that are now offered as kits**

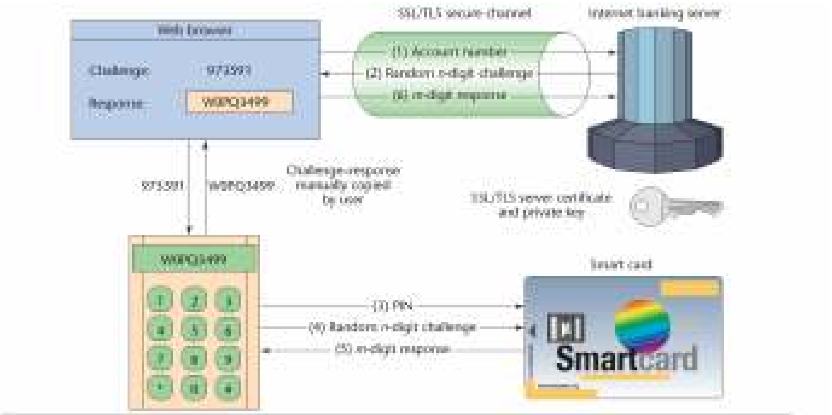


Figure 4. Overview of the short-time password solution. This authentication scheme uses an offline card reader and a smart card to produce short-lived passwords on demand.

Alain Hiltgen, Thorsten Kramp, Thomas Weigold, "Secure Internet Banking Authentication," ***IEEE Security and Privacy*****, vol. 04, no. 2, pp. 21-29, Mar/Apr, 2006.**

chip and PIN

46

Andrew Patrick @ NRC

April 10, 2007

A similar enhancement to equipment security is happening with bank cards used in ATMs and point-of-sale terminals. Since the current cards provide little protection of the information stored on the magnetic strip, and it is easy to produce forged cards, banks are turning to smart cards that contain microchips. EMV cards, also called “chip and PIN” in the UK, contain a chip that is capable of encryption and authentication functions. The chips and associated cryptographic keys are difficult to reproduce, reducing the chances of forgery. The solution is not fool-proof, however, because if the card is stolen and the PIN fraudulently obtained, perhaps by observation or coercion, than fraud can still take place. Also, to ease the transition to the new equipment, most new cards contain both a chip and the magnetic strip. So, as long as some ATMs only use the magnetic strip, the risk of forged cards still remains.

Image: http://www.chipandpin.co.uk/media/resources/

identity theft

47

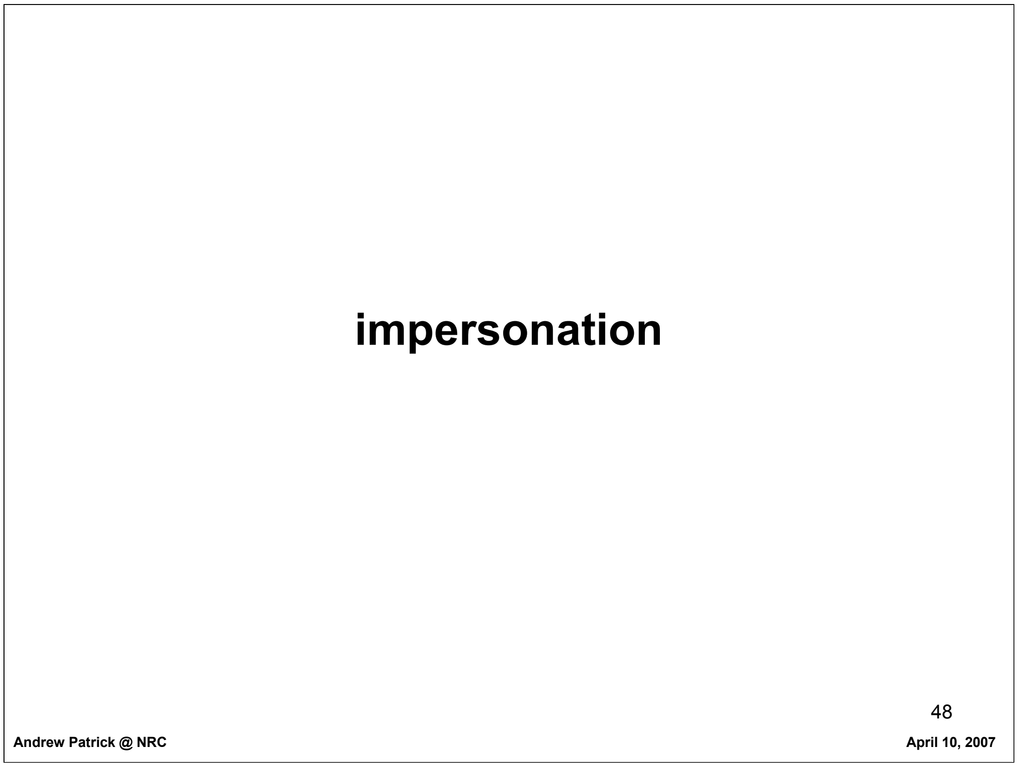
Andrew Patrick @ NRC

April 10, 2007

NEW TOPIC:

The term "identity theft" is an oxymoron.[3] It is not possible to steal a human identity. Human identity is a psychological thing, or the subject of philosophical conversation.[4]. (Wikipedia)

see Bruce Schneier’s essays for good insights



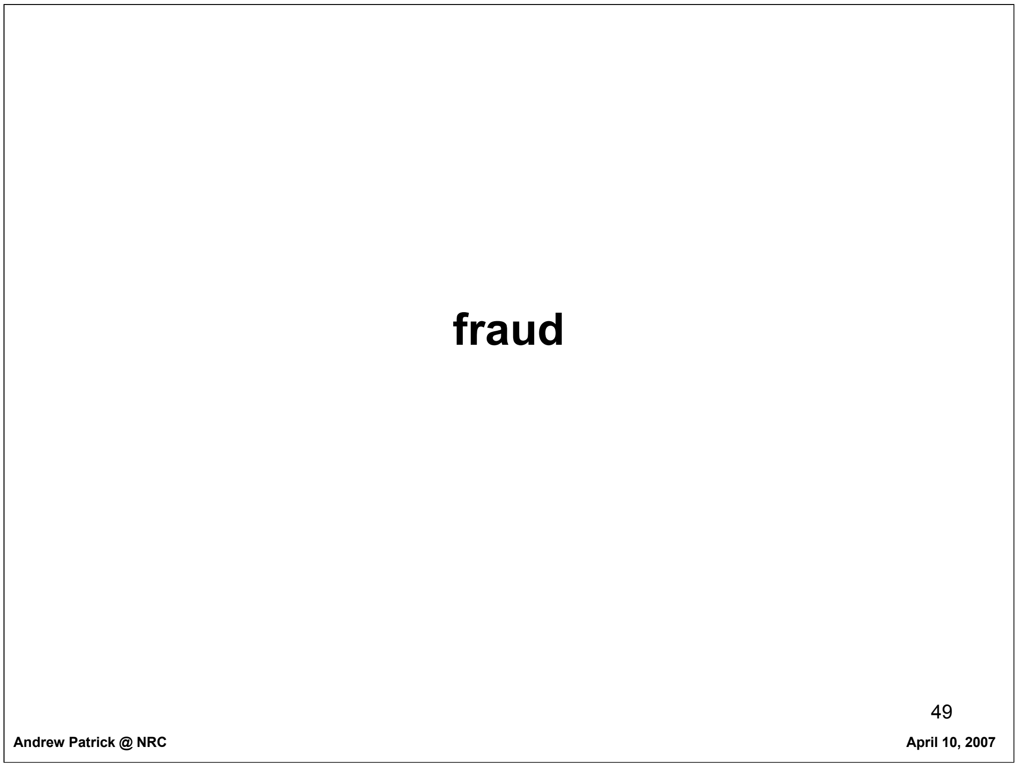
impersonation

48

Andrew Patrick @ NRC

April 10, 2007

The real crime of identity theft is impersonation – using some credentials to claim you are someone else



fraud

49

Andrew Patrick @ NRC

April 10, 2007

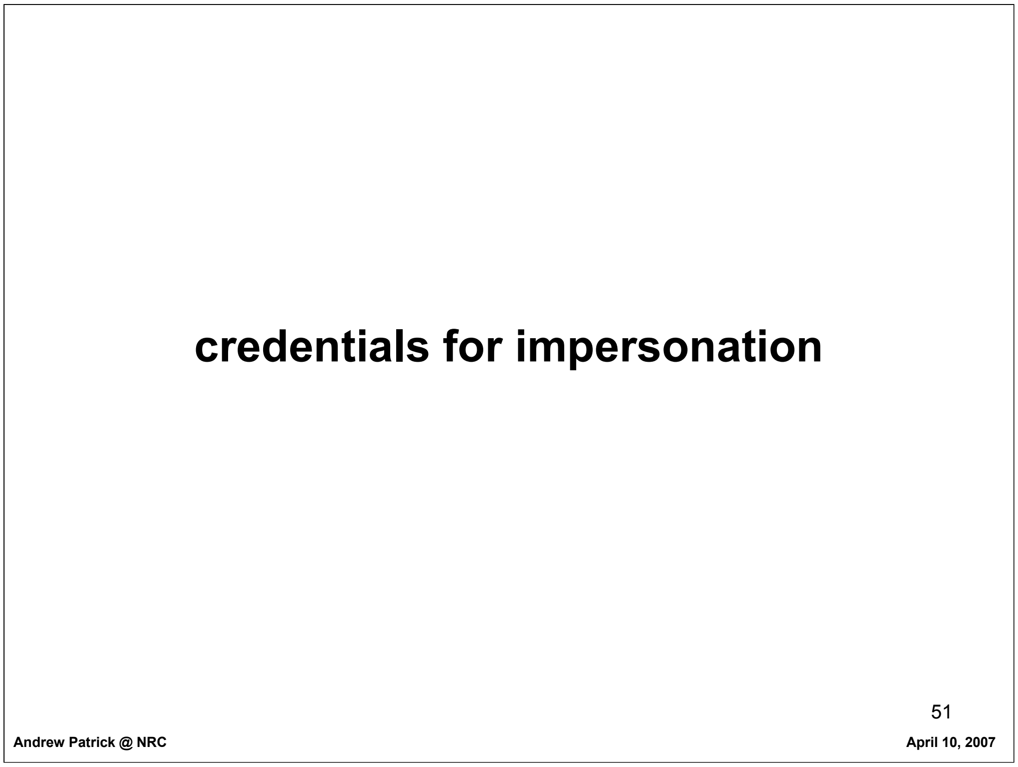
… and then the impersonator commits fraud, which is defined as deception for persona gain

This is not a new crime.

authentic user not present

It is important to note that when the fraud takes place, the authentic user is not present.

So attempts to train users, or provide strong authentication, are not going to do any good.

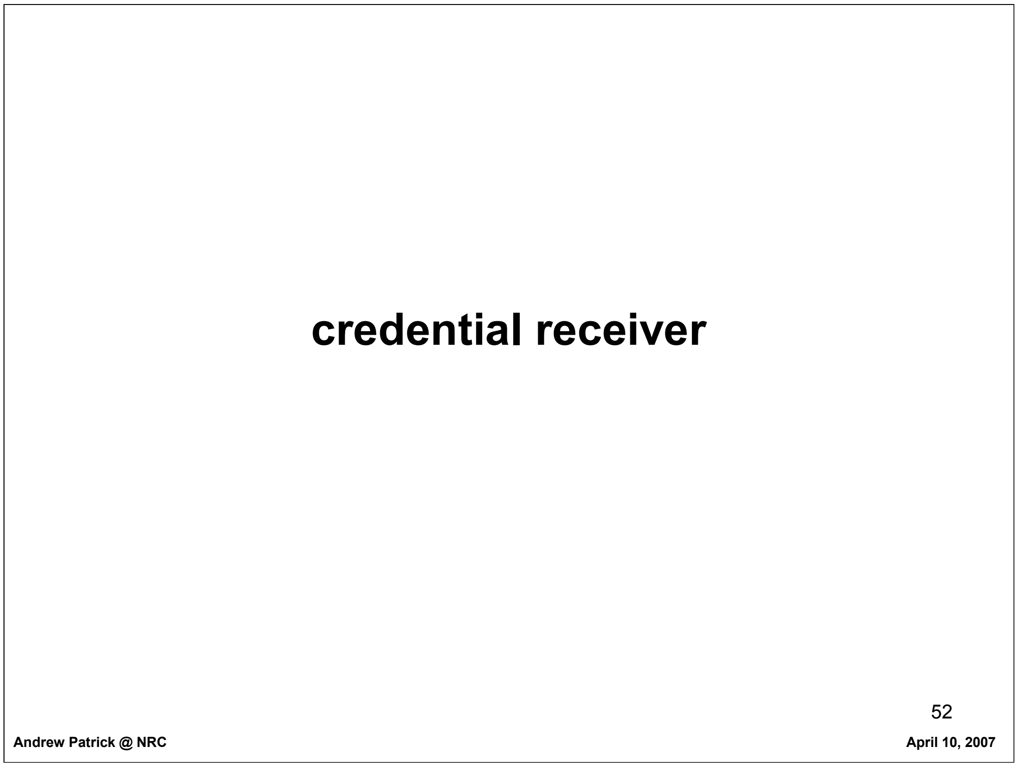


credentials for impersonation

51

Andrew Patrick @ NRC April 10, 2007

The credentials used for the impersonation are not in the hands of the user, and may have been obtained without any involvement of the user (e.g., database breach)



credential receiver

The credential receiver (bank or other institution) is the only one in a position to catch and prevent fraud

wrong incentives

53

Andrew Patrick @ NRC

April 10, 2007

•but the institutions do not have the incentives to prevent fraud

•positive incentive to allow transactions

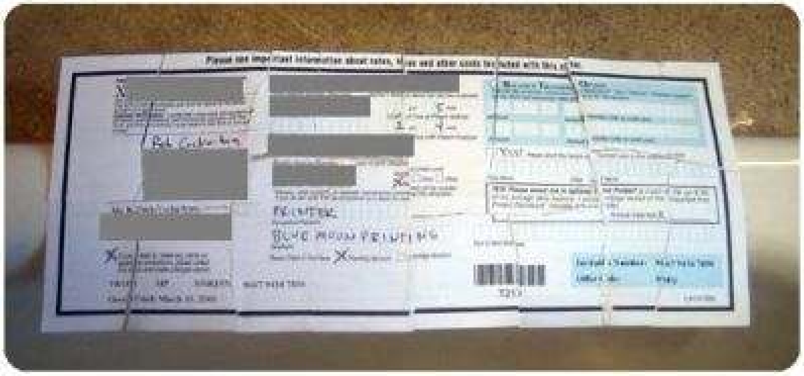
•little or no negative incentives if fraud is committed

•e.g., recent case of mortgage fraud – default is that fraudster or the bank gets the property

•In a 2005 ruling -- Household Realty v. Liu -- the court said that a fraudulent home sale was nonetheless valid once the land title has been registered. The Liu case involved a woman who sold the family home without the consent or knowledge of her husband.

•The Ontario Court of Appeal Feb 6 2007 closed a loophole that had allowed fraudsters to sell homes from under the unsuspecting feet of those who owned them. In a 5-0 ruling, the court said that banks and other lenders will pay a painful price if they do not diligently research mortgage applications to ensure that they are not being made unwitting parties to a swindle.

• financial institutions not required to report ID theft statistics



PRINTER

BLUE MOON PRINTING

Consider the dozens of pre-approved credit card applications that many of use receive each year. Each one is an opportunity for identity theft, and the banks are motivated by high interest rate returns and limited liability to continue the practice. Just how risky these credit applications are was dramatically demonstrated by Rob Cockerham. Rob took an application for a new MasterCard and tore it into small bits. He then haphazardly taped the pieces together and completed the form. He even chose the option of changing the mailing address for the new card to an address that was not his, and he provided a cell phone number as a contact point. He then sent the application to the bank in the postage-paid envelope they provided.

The torn, taped, and completed credit card application. (http://www.cockeyed.com/citizen/creditcard/application.shtml)

A few weeks later, a new card was delivered to the fraudulent address, and it was easily activated using the cell phone. Because of the authentication practices of this bank, identity theft can be that easy.

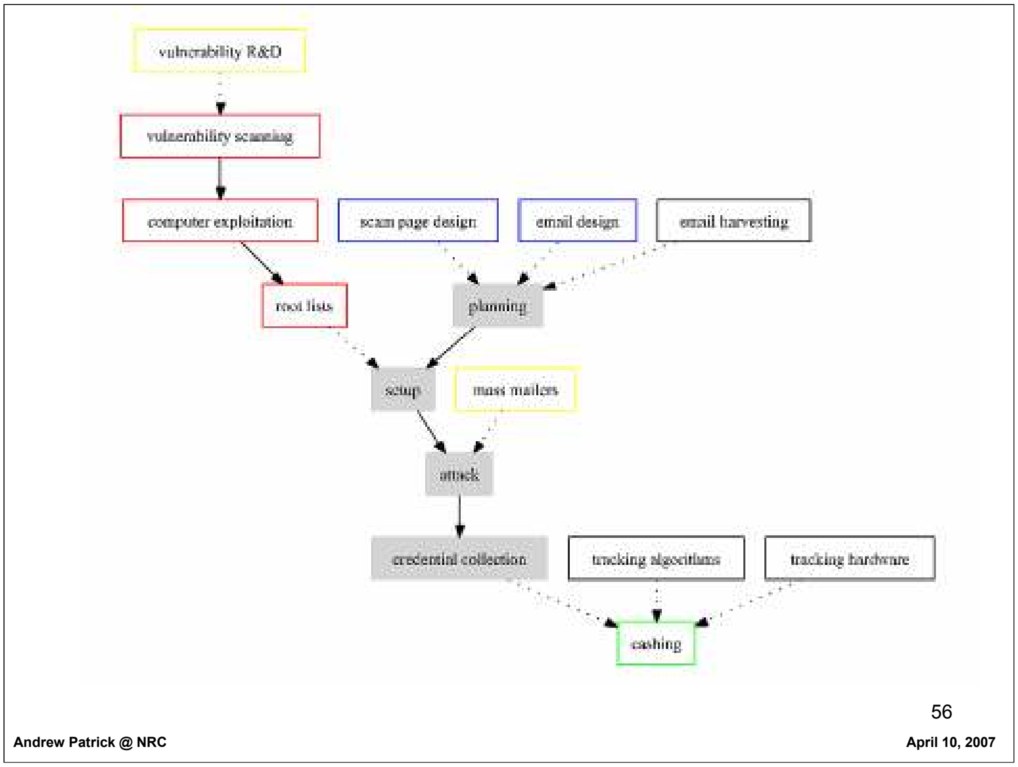
protect the transaction

55

Andrew Patrick @ NRC

April 10, 2007

- the fraud occurs at the time of the transaction (“cashing” after “phishing”)
- the solution is to protect the transaction, not the credential
- why do I not keep my credit card information secret – because the bank protects the transactions
- verify the transaction based on risk parameters (see RSA solution)
- limit possible transactions (e.g., view and internal transfers only)



56

Andrew Patrick @ NRC

April 10, 2007

The Economy of Phishing
Christopher Abad, Cloudmark

Note that the user is only involved in one stage: the attack

With database breaches, the user is not involved at all