

# Biometrics - Practical Issues In Privacy and Security

Terrance E. Boulton & Walter Scheirer

University of Colorado at Colorado Springs  
and  
Securics Inc

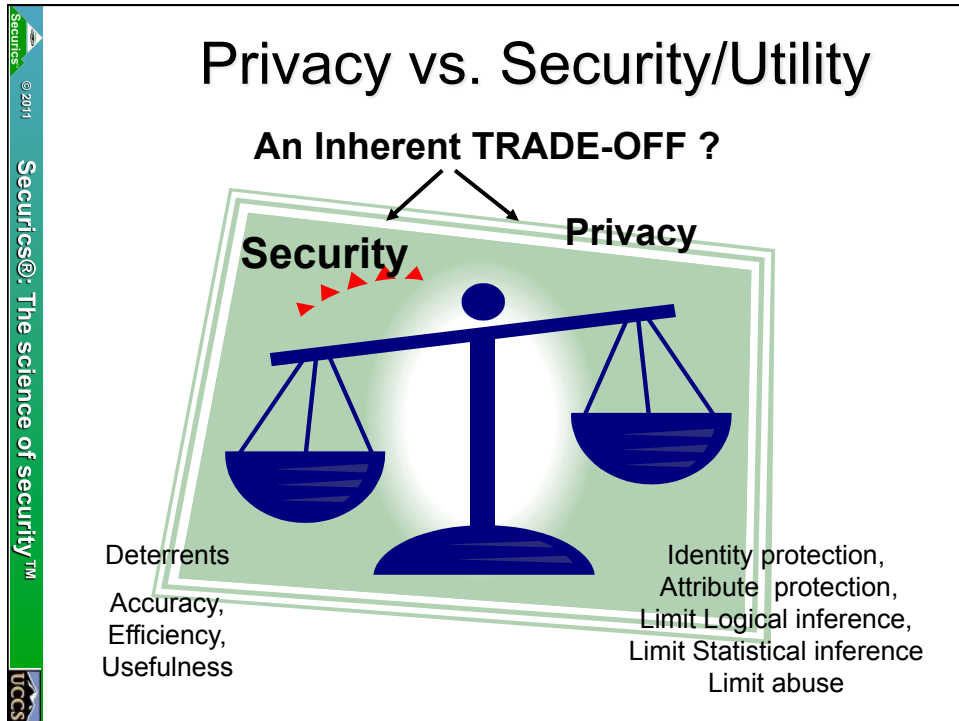
tboulton@vast.uccs.edu wscheirer@securics.com



University of Colorado  
Colorado Springs  
Bachelor of Innovation™

## Outline

- Introduction/Background
  - Privacy vs Security
  - Asymmetric information & Markets
- Privacy Issues for biometrics
- Security Models/Issues
- Biometrics Dilemma
- Limits of standard protection
- Multi-factor solutions
- Revocable biometric templates



**Security  $\neq$  Privacy**

“the right to exercise control  
over your personal  
information.” Ann Cavoukian

“the right to be let alone”  
Warren & Brandeis

“Privacy is at the heart of liberty in  
the modern state.” Alan Westin

Securics®: The science of security™  
© 2011  
UCCS

**Privacy = choice &  
control over use and  
disclosure of our identity  
and our information**

**...including our biometrics**

## **Unfortunate Privacy truisms:**

- 1. Most people don't value their privacy until it is threatened/lost**
- 2. Once invaded/lost, you will need to regain your privacy over and over and over again...**

Security	vs.	Privacy
<ul style="list-style-type: none"> <li>➤ Accountable to Commander, President or Board of Directors.</li> <li>➤ Access and use controls <i>defined by the system owner</i>.</li> <li>➤ Generally focused on protecting against “outsiders”.</li> <li>➤ Short term risk based assessment. (How likely is it?)</li> </ul>		<ul style="list-style-type: none"> <li>➤ Accountable to the subject of the data.</li> <li>➤ Access and use controls defined by <i>design, use limitation, subject consent and legislation</i>.</li> <li>➤ Requires protecting against outsiders, insiders and system owner.</li> <li>➤ Long term capabilities based assessment. (Is it possible?)</li> </ul>

➤ **“A man without privacy is a man without dignity; the fear that Big Brother is watching and listening threatens the freedom of the individual no less than the prison bars”**

➤ Professor Zelman Cowen, 1969  
“The Private Man”, ABC Boyer Lectures

## Competing views on Biometrics

- “Simply put, it’s getting harder and harder to preserve personal privacy without using biometrics...”
  - Richard E Norton, IBIA
- “...Biometrics are among the most threatening of all surveillance technologies, and herald the severe curtailment of freedoms, and the repression of ‘different thinkers’, public interest advocates and ‘troublemakers’.”
  - Roger Clarke

## Privacy risks determined by:

- use of technology
- collection methods – (covert or intrusive)
- system model – storage and security of data
- unique identifiers
- function creep
- Capturing/linking extra data – health, racial, disability, emotional ...
- inaccuracy – false acceptances or rejections
- Ability to validate/challenge data

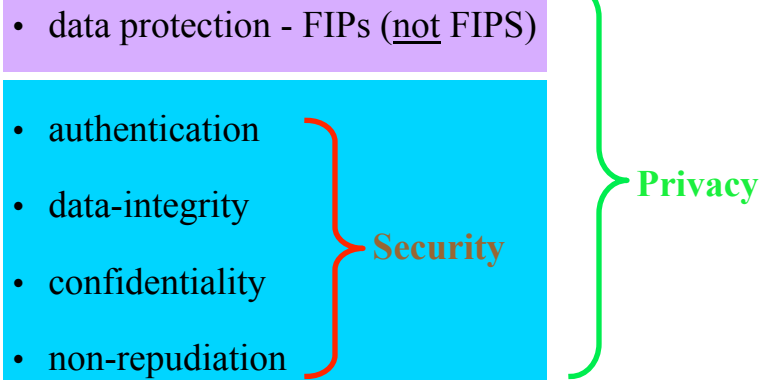
## Biometrics – the benefits to individuals and society

- privacy enhancing capabilities
- convenience
- efficiency
- improved access
  - remote access to e-records
  - access for those with disability (bringing the marginalised back into mainstream)
- Improved security if done properly

## Relationships between Privacy and Security

- In theory, privacy and security may be completely different elements of a system
- In practice, security is a facilitator of privacy and an important foundation to it
- No matter how excellent security may be, it is never, in and of itself, sufficient to ensure privacy
- Not protecting privacy often impacts security.

# Security is a foundation to Privacy



## Fair Information Practices

### “The Ten Commandments”

- |  |                                     |
|--|-------------------------------------|
| ➤ <b>Accountability</b>                          | ➤ <b>Accuracy</b>                   |
| ➤ <b>Identifying Purpose</b>                     | ➤ <b>Safeguards</b>                 |
| ➤ <b>Consent</b>                                 | ➤ <b>Openness</b>                   |
| ➤ <b>Limiting Collection</b>                     | ➤ <b>Individual Access</b>          |
| ➤ <b>Limiting Use,<br/>Disclosure, Retention</b> | ➤ <b>Challenging<br/>Compliance</b> |

## Biometrics Privacy Problems

- Unique Identifier
- Infrastructure for Surveillance
- Consent/Control
  - Infrastructure
  - Template Storage
  - Biometric Acquisition
  - Usage

## Different Approaches to Privacy

- Central Repository/Decision Model – Fort Knox syndrome
- Divide and Conquer – strategic pseudonymisation/anonymisation
- Build in elements of personal Consent and Control
- Smart Hardware
  - Privacy Rules Embedded in Hardware
- Smart Data
  - Encapsulate Methods inside the data

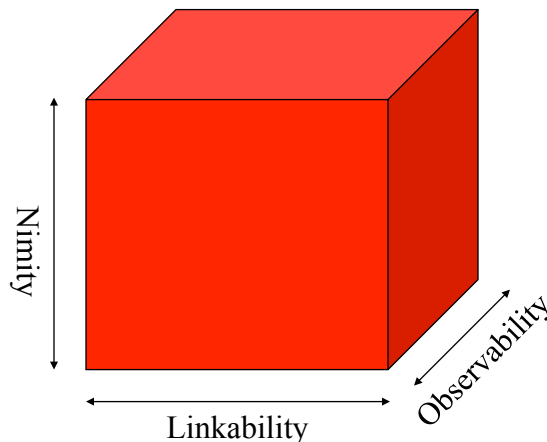


## How do we measure privacy?

- Nimiety or Identifiably
  - Measures the degree to which information is personally identifiable.
- Linkability
  - Measures the degree to which data tuples or transactions are linked to each other.
- Observability
  - Measures the degree to which identity or linkability may be impacted from the use of a system.

With thanks and apologies to the Common Criteria and Peter Hope-Tindall

## Privacy Dimensions



## Interoperability vs privacy

- Governments/Markets want to reuse to reduce costs and improve efficiencies. They want Interoperability.
- What is its impact on privacy?
  - Discussion time..

## Privacy and Biometrics (as sold today)

- Claims of “privacy” since cannot recover fingerprint from template
- Government Officials Statements that biometrics are public information
- Border/Passports and National ID
- ± Biometric access control to facilities
- ± Biometric for computer/file access and data encryption
- ± Personal/home biometric devices

## Why Technology for Privacy

- Policies to protect privacy must be followed by everyone to be effective. They are important, but technology can add confidence that policies are being followed.
- Policies “evolve” to allow/support function creep
- Biometrics are long lived data and once privacy is violated its hard to “fix”.
- Biometrics can be abused without our knowledge
- If we help build the technology, its our social responsibility to make sure it is used properly.
- Given more technological choices we may simultaneously increase privacy and security.

## Security by Obscurity is not Real Security

- Many people think that a security system becomes more secure if its internal structure is secret
  - Example: A secret encryption algorithm
- BUT: The exact opposite is the case
  - Open and standardised systems are subject to constant analysis by the international research community
  - Secret systems can only be analysed by internal specialists
    - Unless an agency or company has a huge budget, severe and constant analysis of internal security systems is not possible
- Kerckhoffs' principle
  - The security of a cryptographic system shall always and only depend on the secrecy of the key. Everything about the algorithm except for the keys shall be open

## Extending Kerckhoffs' principle

- Bruce Schneier: "Kerckhoffs' principle applies beyond codes and ciphers to security systems in general: every secret creates a potential failure point. Secrecy, in other words, is a prime cause of brittleness—and therefore something likely to make a system prone to catastrophic collapse. Conversely, openness provides ductility."
- Any system whose security depends on keeping the details of the system secret is not secure in the long run.
- Defense in depths suggests layers, some of which can have secrets/obscuration but the core must be secure without secrets.
- Keeping "algorithm" and key concepts secret increase the asymmetric information, potentially keeping even experts from evaluating system without significant efforts.

## Market Failure Under Asymmetric Information

In 1970, George Akerlof, published

### **The Market for "Lemons": Quality Uncertainty and the Market Mechanism**

*The Quarterly Journal of Economics*,  
Vol. 84, No. 3. (Aug., 1970)

It won him the 2001 Nobel Prize in Economics

# Lemon Markets

## Criteria for a lemon market

1. Asymmetry of information
  - buyers cannot accurately assess the value of a product through examination before sale is made
  - sellers can more accurately assess the value of a product prior to sale
2. An incentive exists for some sellers to pass off a low quality product as higher quality
3. Sellers have no credible disclosure technology (e.g. sellers with a great car have no way to credibly disclose this to buyers)
4. Deficiency of effective public quality assurances (by reputation or regulation)
5. Deficiency of effective guarantees / warranties

## Fixed quality Lemons market

- Many potential buyers for product
- Buyers are willing to pay
  - \$1,000 for low quality (lemon)



\$2,000 for good quality product



- Sellers choice is sell or not

## Only two possible equilibrium

- Only lemons sell for a price equal to the value that buyers place on lemons (bad drives out good)
- All products sell at average price, e.g. \$1,500 in the example. Sellers of good products are effectively subsidizing sellers of lemons.
- Either is inefficient market and collapses.



## Privacy/Security is a lemon market

### The Privacy Game: Matrix

	Respects	Defects
Buys	$+X, +Y$	$+X - V, +Y + I$
Doesn't	0, 0	0, 0

Bob, Inc. should defect (weakly dominant strategy).

Alice can buy (costing X) or not (cost 0)

Bob can sell (earn Y) or not.

Alice can use only vendors that respect privacy (0) or sell it for “V”

Bob can respect privacy or defect (earning I)

*Why we can't be bothered to read privacy policies: models of privacy economics as a lemons market* by: Tony Vila, Rachel Greenstadt, David Molnar

In ICEC '03: Proceedings of the 5th Int. Conf. on Electronic commerce (2003), pp. 403-407. (Also in ECONOMICS OF INFORMATION SECURITY, Advances in Information Security, 2004, Volume 12, pp143-153)

## Lemons market with variable quality

- In the long run choice is not just sell or not, firms can vary quality of their products
- If consumers cannot identify quality
  - all goods sell at about the same price
  - raising your quality raises price and either raises average price of all firms or cuts your profits
  - This provides inadequate incentive to produce high quality, but more incentive to “sell well”
  - Market still fails because social value of raising the quality is ignored because of uncertain information

## Privacy With Signaling

Signal can be Tech or 3<sup>rd</sup> party

- Bob, Inc. pays  $S$  to send a signal
- Alice pays  $T$  to read Bob, Inc.'s signal (to test)

	Respects	Defects
Tests	$+X - T, +Y - S$	$-T, -S$
Doesn't	$+X, +Y$	$-V, +Y + I$

Alice can buy (costing  $X$ ) or not (cost  $0$ )

Bob can sell (earn  $Y$ ) or not. Can defect and sell info for  $I$

Alice can “test” vendors for cost  $T$ . Loss of privacy still “ $V$ ”

Bob can spend “ $S$ ” to signal he respects/protects privacy

This shifts Equilibrium depending on relative values.

*Why we can't be bothered to read privacy policies: models of privacy economics as a lemons market* by: Tony Vila, Rachel Greenstadt, David Molnar  
 In ICEC '03: Proceedings of the 5th Int. Conf. on Electronic commerce (2003), pp. 403-407. (Also in ECONOMICS OF INFORMATION SECURITY, Advances in Information Security, 2004, Volume 12, pp143-153)

## Lemon Markets with “experts”

- In reality there will generally be some “experts” that can tell quality. How does it change the results?
- “No” expert case
  - The market collapses to only trading low quality items
- Expert case
  - Externality of information and product evaluation is key
  - Handful of experts prevent the market from collapsing
    - Partial collapse occurs up to “expert ratio” = 0.3
    - Even at 0.01, no total collapse
  - More experts mean more information
  - With “expert information” at 60%, market is almost back to “ideal”

From a 1998 talk by J.C. Kim (KAIST) on Lemon Markets

## Avoiding market failure

- The primary tenants of “asymmetric information” and the overall IT Company economic models apply in biometrics and security. It **will** likely happen in biometrics/security if left to basic market forces.
- To provide improved value to society (and avoid market failure) we need to push for “equalization of information” and signaling
- We must be evaluating or at least advise the “experts” to keep the system in check.



## Limiting Lemons

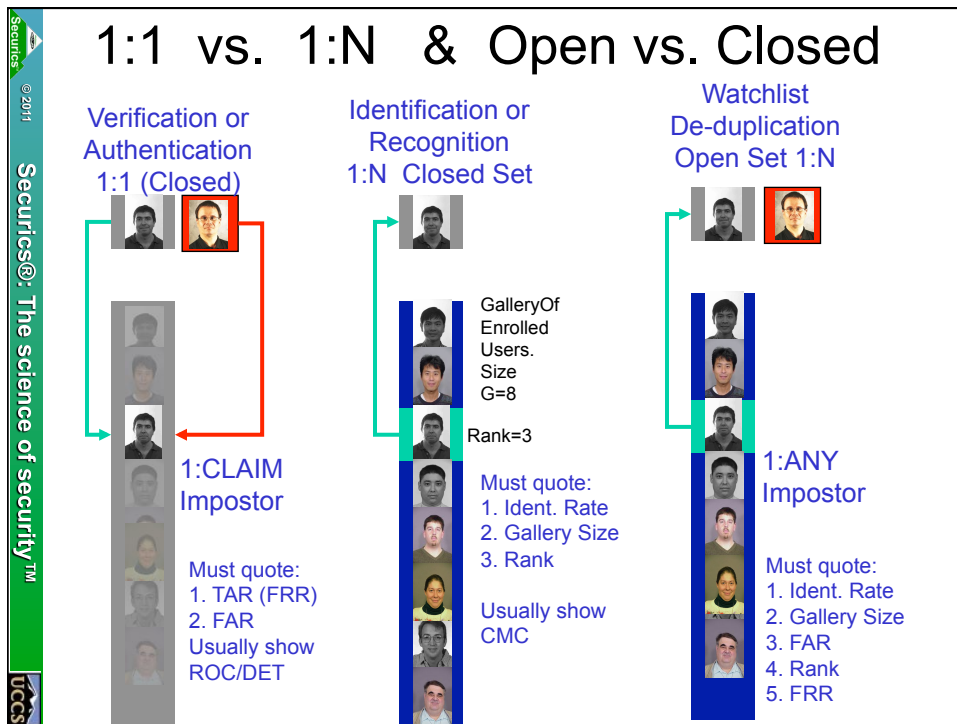
### Means of equalizing information

- Third-party/Expert comparisons
- Pushing Kerckhoffs' principles force Full Disclosure
- Standards and certification
  - *standard*: metric or scale for evaluating the quality of a particular product (e.g., R-value of insulation)
  - *certification*: report that a particular product meets or exceeds a given standard level
- “Company” signaling by firms
  - Free test drives
  - guarantees and warranties
  - brand name
- Laws to prevent opportunism, require standards
- Consumer screening, e.g. test drives



## Outline

- Introduction/Background
- Privacy Issues for biometrics
- Security Models/Issues
- Biometrics Dilemma
- Limits of standard protection
- Multi-factor solutions
- Revocable biometric templates
- *id*-privacy



## Measurement Trade-Offs

*We must balance the FAR and the FRR*

- Lower FAR = Fewer successful attacks
  - Less tolerant of close matches by attackers
  - Also less tolerant of authentic matches
  - Therefore – increases the FRR
- Lower FRR = Easier to use
  - Recognizes a legitimate user the first time
  - More tolerant of poor matches
  - Also more tolerant of matches by attackers
  - Therefore – increases the FAR

Securics®: The science of security™  
© 2011  
UCCS

## Issue 1: Biometric Verification – Why does it reject me?

**Large throughput volume a problem.**

- **Example:** <TrustedTravler smart card with single fingerprint>
- Assume a system where each person is 1-1 verified to a smartcard or a networked database with 5000 people per hour (14hr/day) requesting access (Newark airport hourly passenger volume). Assume 2% FRR for .01%FAR

*100 people per hour will fail to be verified*

*1400 people per day*

*Strong impetus to runs at lower security than a .0001 FAR*

## Issue 2: Biometric (Mis)Identification – Why am I delayed as “suspect”?

**Example:** <fingerprint check vs. government database>

- Assume a system that checks each person's fingerprint against a watch-list database of 1000 suspects. Again airport: 5000 people per hour/ 14hr day, with FAR=.01%
- *over 7000 people per day are likely to match some suspect from 1K WatchDB:*
  - Individual chance of match is  $.0001 * 1000 = .1$ ;*
  - $.1 * 5000 * 14 = 7000$*
- What happens with DB of suspects is 10K people? (Note: current US watch list > 50K)

## Issue 3: Biometric Identification – “Who can I be today”

- **Issues with large scale searchable database..**

**Example 3:** <fingerprint check vs. government database>

- A group somehow gains access to a large Fingerprint DB, and starts looking for someone their “gang” can steal an identity.
- With a 2-print match at high accuracy levels (FAR=.01%) a single print will match  $.0001 * 6,000,000 = 600$  people in the DC area. With a “gang” of 10 or 100 what can they do?
- Since Biometric DB’s often contain lots of other info (e.g. CO DMV records have fingerprint, photo and all driving information), the gang would have strong potential to find the ideal new identity.

## Outline

- Introduction/Background
- Privacy Issues for biometrics
- Security Models/Issues
- Biometrics Dilemma
- Limits of standard protection
- Multi-factor solutions
- Revocable biometric templates
- *id*-privacy

## Critical 5D's of security

#1 goal of security: keep bad things from occurring  
***Address these by Analysis and Design***

- **Deter:** Make people not want to try
- **Detect:**
  - If they do, you need to detect it (else little deterrent)
- **Dispatch**
  - If you cannot respond, it keeps happening. Deterrent?
- **Depose:**
  - If you cannot take it to court, not much of a deterrent
- **Depth:**
  - There should multiple layers to mitigate one layer's failure

**In biometrics “security” its almost all  
Deter and Detect**

## Security/Privacy Threats

- |  |   |
|--|---|
| 1. Live Biometric capture, theft                         | 1. Device tampering   |
| 2. Live Biometric simulation                             | 2. Environmental tampering (e.g. lighting, jamming)           |
| 3. Live Biometric substitution                           | 3. Infrastructure manipulation (e.g. power-outage)            |
| 4. Reference Biometric substitution                      | 4. Device or System override/backdoor/trojan utilisation      |
| 5. Reference Biometric forgery                           | 5. <b>Exception-Handling Procedures manipulation</b>          |
| 6. Message interception, modification, insertion         | 6. <b>Fallback procedures for the Unenrollable subversion</b> |
| 7. Stored Biometric capture, theft, change, substitution | 7. <b>Insider collusion</b>                                   |
| 8. Threshold manipulation                                |   |

## Watch list added attacks

- Don't have to become someone, just not match the watchlist data. Means system cannot partition on biographic or country.
- In addition to the traditional attack points, for watch-list applications user can actually modify their biometric to try to defeat detection, e.g. abrasion on prints, facial surgery, etc.. We call this "failure to detect" (which is same as false-reject, but people often view that parameters a user convenience issue, not security issue).
- Already documented cases of applying facial surgery and others using fake-prints to try to defeat watch-lists.
- Stronger if they also try to find a doppelganger

Page last updated at 18:27 GMT, Monday, 7 December 2009  
E-mail this to a friend    Printable version

### 'Fake fingerprint' Chinese woman fools Japan controls

**Woman fools Japan's airport security fingerprint system**  
January 2, 2009

A Chinese woman managed to enter Japan illegally by having plastic surgery to alter her fingerprints, thus fooling immigration controls, police claim.

Lin Rong, 27, had previously been deported from Japan for overstaying her visa. She was only discovered when she was arrested on separate charges.

Tokyo police said she had paid \$15,000 (£9,000) to have the surgery in China.

It is Japan's first case of alleged biometric fraud, but police believe the practice may be widespread.

Japanese police suspect Chinese brokers of taking huge sums to modify fingerprints surgically.

All foreigners are fingerprinted when they arrive in Japan.

A South Korean woman barred from entering Japan last year has reportedly passed through its immigration screening system by using tape on her fingers to fool a fingerprint reading machine.

The biometric system was installed in 30 airports in 2007 to improve security and prevent terrorists from entering into Japan, the Yomiuri Shimbun newspaper said.

The woman, who has a deportation record, told investigators that she placed special tapes on her fingers to pass through a fingerprint reader, according to Kyodo News.

Japan spent more than ¥4 billion (\$464 million) to install the system, which reads the index fingerprints of visitors and instantly cross-checks them with a database of international fugitives and foreigners with deportation records, the Yomiuri Shimbun said.

### Japanese immigration checks miss fake fingerprints

At least 8 have entered Japan from South Korea using special tapes. -The Yomiuri Shimbun/ANN

Sun, May 16, 2010  
The Yomiuri Shimbun/Asia News Network

AT LEAST eight people arriving in Japan from South Korea have used fake fingerprints to evade the biometric checks at immigration control and enter this country illegally since January 2008, it has been learned.

In May last year, two South Korean hostesses at a South Korean bar in Yamato, Kanagawa Prefecture

## Security programs “dirty secret” Biometrics “security” its mostly “deter”

But once its found ineffective its no longer a deterrent then we traded privacy for the short term security theater.



## The [U.S.] Fingerprinting of Foreigners Bruce Schneier, 15 January 2004

According to the Bush administration, the [fingerprinting of foreigners is] designed to combat terrorism. As a security expert, it's hard for me to see how. The 9/11 terrorists would not have been deterred by this system; many of them entered the country legally on valid passports and visas. ...Capturing the biometric information of everyone entering the country doesn't make us safer. ... even if we could completely seal our borders, fingerprinting everyone still wouldn't keep terrorists out. ... **there is no comprehensive fingerprint database for suspected terrorists.**

## Would it be effective Security?

The hardest problem is the false alarms ....

**Suppose a magically effective biometric terrorist detection that is 99.99%**

**accurate.** That is, if someone is a terrorist, there is a 99.99% chance that the software indicates "terrorist," and if someone is not a terrorist, there is a 99.99% chance that the software indicates "non-terrorist."

Assume that 1 in 100 million Border crossing, on average, is a terrorist. (I.e. about 5 terrorist enter the US per year)

## The boy who cried wolf 10000 times

**Probably not effective. Even that magical system would generate 10000 false alarms for every real terrorist. That is 30 false alarms a day, every day.** And every false alarm means that all the security people go through all of their security procedures. How many false alarm before they stop taking it seriously?

**Because the population of non-terrorists is so much larger than the number of terrorists, the test is practically useless.**

And of course we don't have a biometric list of most terrorists

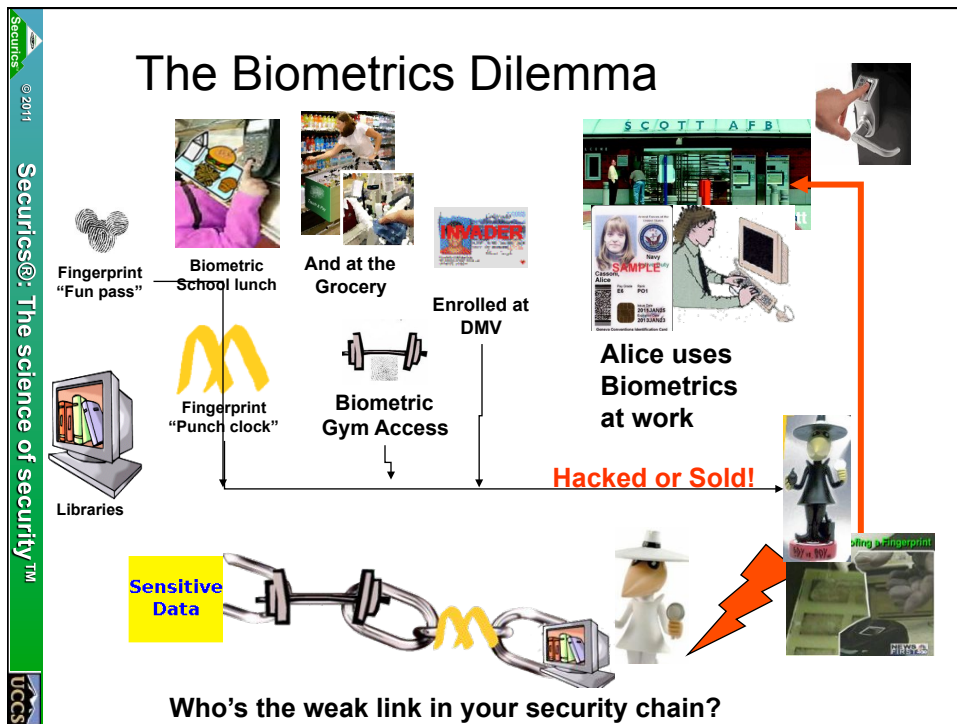


## Security Biometrics and Single-Mission Terrorists

- **“Biometrics ... can’t reduce the threat of the suicide bomber or suicide hijacker on his virgin mission.** The contemporary hazard is a terrorist who travels under his own name, his own passport, posing as an innocent student or visitor until the moment he ignites his shoe-bomb or pulls out his box-cutter” (Jonas G., National Post, 19 Jan 2004)
- **“it is difficult to avoid the conclusion that the chief motivation for deploying biometrics is not so much to provide security, but to provide the appearance of security”** (The Economist, 4 Dec 2003)

## Outline

- Introduction/Background
- Privacy Issues for biometrics
- Security Models/Issues
- Biometrics Dilemma
- Limits of standard protection
- Multi-factor solutions
- *id*-privacy



© 2011 Securesis®: The science of security™ UCCE

## Vendors False Claims

Cappelli et al. PAMI, Sept. 2007

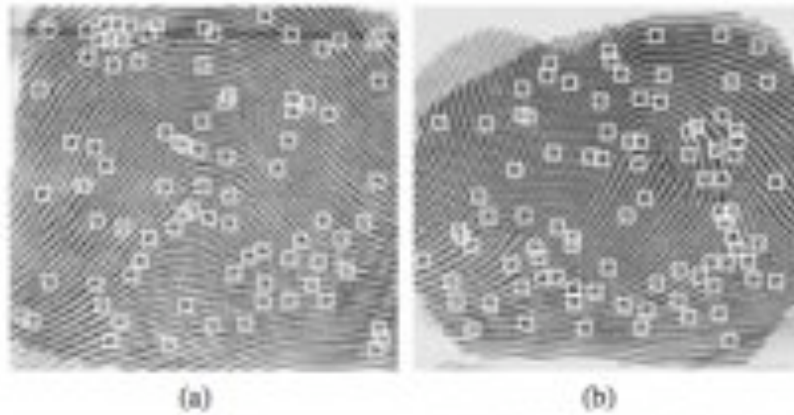
Original Image

Average successful attacks against nine different systems

- 81% high security

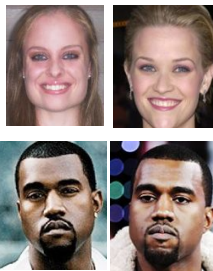
Templates ARE effectively invertible!  
And fakes keep getting better. (e.g. Jain-et-al ICB'09)

## And “recovery from templates” keeps getting better



Prints reconstructed using the technique of Feng and Jain (ICB09), overlaying the original prints. Reconstructions matched >95% of the time!

## “Doppelganger Danger”



Find your Celebrity look-a-like at  
[Myheritage.com](http://Myheritage.com)

Given a DB with 50 Million users, with systems operating at FAR of 1 in 1000 a buyer may be given a choice from approximately 50000 identities!

At a FAR of 1 in million, they still get 50 choices!

At a FAR of 1 in 10 million, they still get 5 choices!

What happens when a terrorist buys the identity of a doppelganger ?

## Cost/Risk model

- A motivated individual might follow someone around at a direct cost  $c_f$ , and following has some risk of being caught, with the cost  $r_f$ .
- Once obtained, the expected value **over the persons lifetime** for using it for spoofing is  $v_s$  and the risk cost of using the spoof is  $r_s$ .
- With probability  $p_d$ , the acquired data could provide for doppelganger, so there is also potential doppelganger value/risk, which we represent as  $v_d$  and  $r_d$  respectively

## The fallacy of secrecy

- Some claim that since Biometrics cannot be secret they don't need to be protected. Credit card numbers are not secret either, but require protection by law!
- The real risk is Databases. Following people is far more risky than hacking a DB, and yields less data.
- A centralized biometric DB of size  $N$  is at risk if:

$$v_s > r_s \text{ or } v_d > r_d \text{ and } N > \frac{(c_h + r_h)}{\max(v_s - r_s, p_d(v_d - r_d))}.$$

where  $v$  is value,  $c$  is direct cost,  $r$  is "risk costs", subscripts  $s$  and  $d$  are for spoofing and doppelganger attacks respectively,  $h$  for DB hacking, and  $p_d$  is the per-person probability of finding a doppelganger.

**Secret or not, biometric DBs must be protected !**

*Hundreds of millions of financial/personal records compromised or “lost” since 2005! Features like fingerprints are permanent and much easier to spoof/match than most want to admit.*



No one serious about security would use accounts, or tokens that could not be revoked.

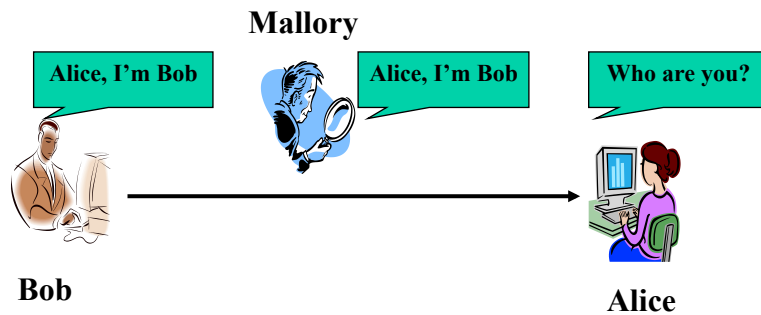
***Why accept less from biometric-based solutions?***

## Outline

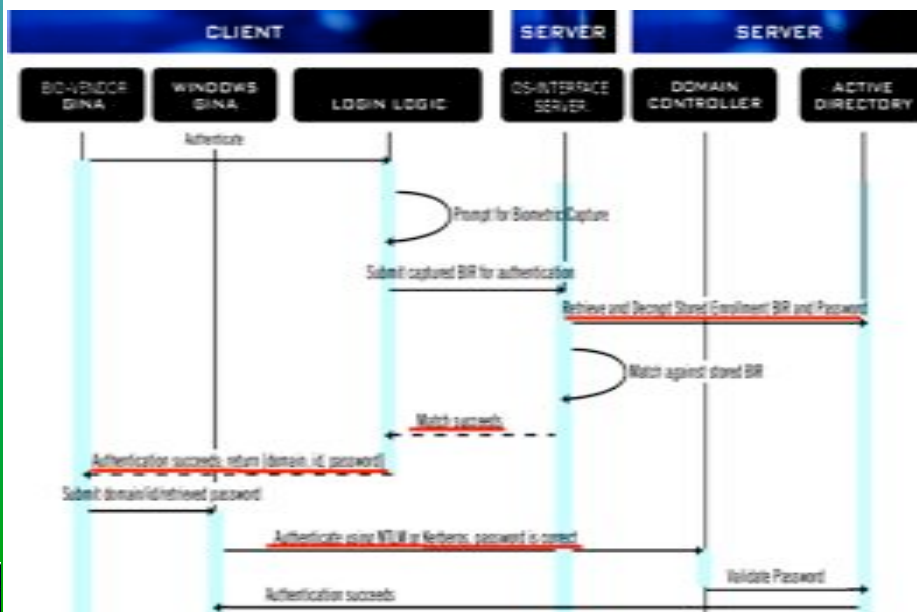
- Introduction/Background
- Privacy Issues for biometrics
- Biometrics Dilemma
- Security Models/Issues
- Limits of standard protection
- Multi-factor solutions
- Revocable biometric templates
- *id*-privacy

# Protecting resources requires authentication of identity.

- How does Bob prove/authenticate to Alice?
- How do we stop impersonation in cyber-space?

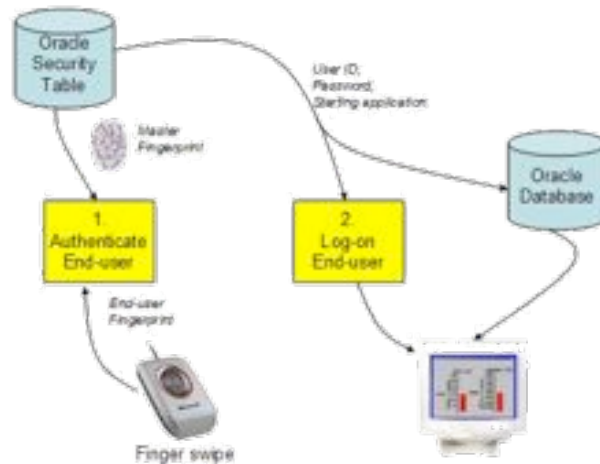


## Classic Biologin



## Another example “Biometric Login”

Oracle database biometric sign-on



To be secure standard biometrics need shared secret, then they authenticate using Kerberos/password anyhow!

## Using Cryptography/Hashing help

➤ Hashing/Crypto great for passwords.

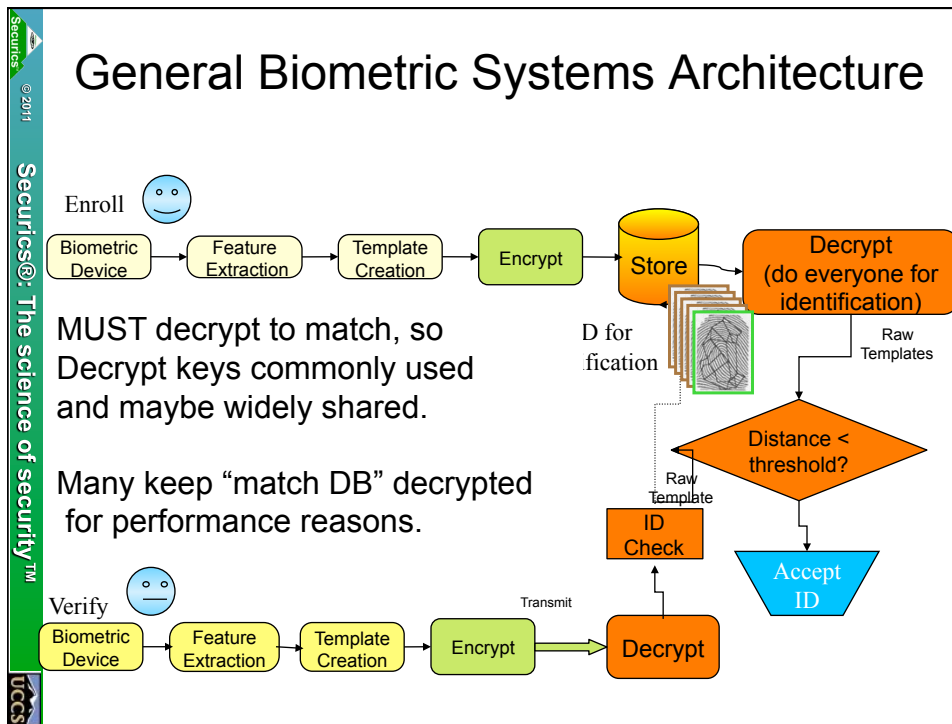
Hire Only IEEE Members      1fc486d4b30dd490e044e40a35b6535c

Fire Only IEEE Members      53cc18345f93c390c7469e38c126a13f

Hire Only IEE Members      dfa9d634376d51d311ee55d40722950c

Minor Change results is radically different crypto string (no match)

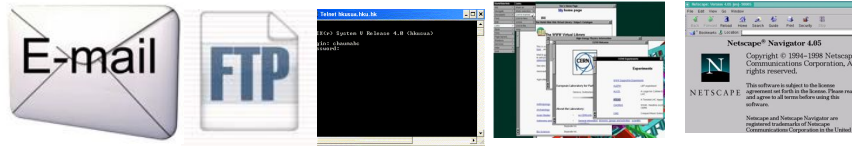
**What does this suggest about potential for Biometrics?**



- Problems with classic "biometrics" network security**
- Biometric authentication is independent of other checks so if attacker can compromise "authentication response", they don't need to compromise biometrics. Must trust matcher for both security and privacy.
  - Does not solve key-exchange. In fact, it needs its keys/encryption to protect biometric data.
  - Biometrics subject to man-in-middle and phishing, but not changeable is lost.
  - It's really what you "have".. And it's easier to fake/reuse than many believe.



## Remember the 80s and 90s?

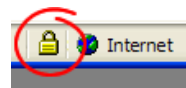


- Huge explosion in new Internet protocols
  - Email, Remote Connections, The Web,...
- Security of these protocols was an afterthought!
  - We need cryptography to protect insecure channels
  - How can Alice verify a server?
  - How do we share encryption keys?

**Solution: Public Key Infrastructure**

## Online Identity Problems...

- Public Key Infrastructure enabled early e-commerce through secure communication
- But Identity and transactions are between people, not machines. How do we “certify” parties in a transaction? ID/Passwords?
- Certificates help machines, few people.
- How many people even know what is a valid certificate?
- Malware/Bot attacks directly capture passwords from machine and browser, sidestepping PKI certificates



**PKI resolve Identity by what you have**

# Identity Limitations of PKI

- Ellison and Schneier (2000)\*
  - “Risk #1: Who do we trust, and for what?”
  - “Risk #2: Who is using my key?”
  - “Risk #4: Which John Robinson is he?”
  - “Risk #6: Is the user part of the security design?”
  - “Risk #8: How did the CA identify the certificate holder”?

\*C. Ellison and B. Schneier, “Ten Risks of PKI: What You’re Not Being Told About Public Key Infrastructure,” *Computer Security Journal*, 16(1):1-7, 2000.

SEPTEMBER 08, 2011

## Certificate hacks: PKI didn't fail us, humans did

After latest attack, GlobalSign stopped issuing SSL certificates. But the real problem is that few pay attention to warnings anyway

By Roger A. Grimes | InfoWorld

Follow @rogeragrimes

Print

With the high likelihood that [GlobalSign](#) has been hacked, this brings to at least three the number of popular public PKI certification authorities (CAs) attacked in recent months by a single hacker. The other CAs are [Comodo](#) and [DigiNotar](#).

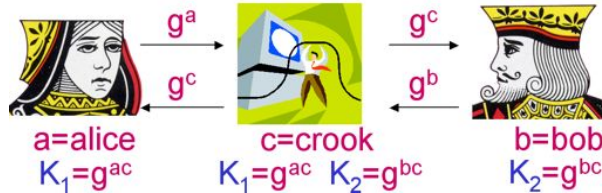
The computer security world is aflutter because hundreds of bogus digital certificates have been issued. “It’s a massive failure of PKI,” they say. “It proves that there’s too much trust spread around,” say others.

But it’s hard for me to get worked up about any public CA or PKI compromise. Here’s why: Almost nobody pays serious attention to digital certificate warning messages in the first place.



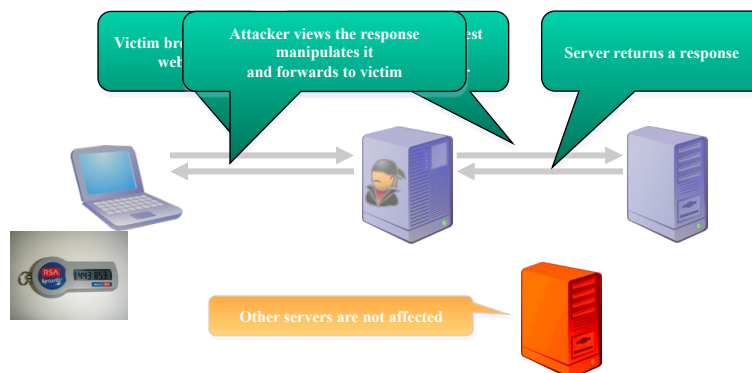
## Man-in-the-middle attacks

- Most Key Exchanges have vulnerabilities,  
Eg. DH is



- With PKI people don't know how certificates work, and some accept bad ones.
- PKI certificates have issues of revocation list maintenance, especially offline.
- Private key of cert is sometimes hard coded, as in MS RDP ☹
- MIM even works against RSA SecureID

## Passive Man in the Middle Attacks



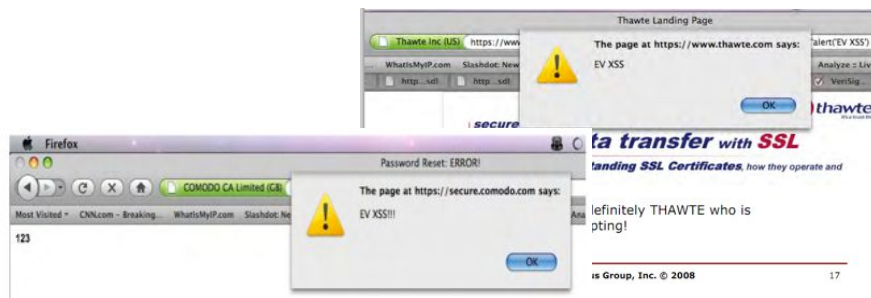
## A common suggested Solution – PKI & Client Certs (Chip&Pin)

- PKI Authentication Combines:
  - *Something you Have* (Smartcard / Token)
  - *Something you Know* (PIN)
- Authentication requires the physical device to be plugged in (Private key stored on device)
- The combination of smart card, PIN, and the strength of RSA, is why many consider PKI authentication as hack proof.
- The “Hack Proof” fallacy, urges organizations to switch to PKI based authentication at high costs



71

## Cross-site scripting for fun & profit



\* Note the green bar. It is definitely COMODO who is vulnerable to cross site scripting!

Intrepidus Group, Inc. © 2008

10

\* Criminal charges are not pursued: Hacking PKI, Mike Zusman Defcon 2008, [http://www.defcon.org/images/defcon-17/dc-17-presentations/defcon-17-zusman-hacking\\_pki.pdf](http://www.defcon.org/images/defcon-17/dc-17-presentations/defcon-17-zusman-hacking_pki.pdf)

Securics®: The science of security™

© 2011

UCCS

# PKI and private keys

## Real CA Attacks

Google search results for "filetype:key \"BEGIN RSA PRIVATE KEY\"".

Results 31 - 40 of about 28,300 results (0.09 seconds).

---BEGIN RSA PRIVATE KEY--- MIICXgIBAAKBgQDXMN9raW0xpTjwMryd0B0fApE2ebN4FDf8Xryb0nPqTze1dg ...

---BEGIN RSA PRIVATE KEY--- MIICXgIBAAKBgQDXMN9raW0xpTjwMryd0B0fApE2ebN4FDf8Xryb0nPqTze1dg ...

---BEGIN RSA PRIVATE KEY--- MIICXgIBAAKBgQDXMN9raW0xpTjwMryd0B0fApE2ebN4FDf8Xryb0nPqTze1dg ...

Securics®: The science of security™

© 2011

UCCS

# Active Man in the Middle Attack

- The attacker actively directs the victim to an "interesting" site
- The IFrame could be invisible; can assess keychain!

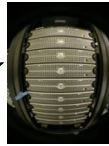
## Man-In-Browser “protection”

- Only known protection from MIB attacks are out-of band per -transaction challenge-response authentication from server
- Can we do that with biometric-based technology?

## Some network security issues

- Key exchange is hard, especially between unknown users.
- Man-in-the-middle effects many protocols., even RSA SecurID is still subject to MIM
- Key management is harder, even with online PKI systems.
- Offline key management (e.g. for storage) is even harder still.
- Unsupervised validation of user not just ID/Token.
- Cross-domain/federated authentication with little trust in end-point or network.

## Biometrics for Verified Web-Identity?



Biometrics provide identity assurance, convenient & low cost but

- Cannot revoke a fingerprint like a password or credit card!
- Like symmetric encryption both sides need the “secret”
- Only matching party can really trust match happened, other party must trust the matcher with their data!

The TRUSTED identity on the web needs  
a radically different and asymmetric  
identity approach.

## Outline

- Introduction/Background
- Privacy Issues for biometrics
- Biometrics Dilemma
- Security Models/Issues
- Limits of standard protection
- Multi-factor solutions
- Revocable biometric templates
- Kerckhoffs' principles
- Asymmetric Information

## “Three factor” security

1. Something you know (e.g. password)
2. Something you have (e.g. card)
3. Something you “are” (e.g. biometric)

*A biometric is really just have (e.g. fingerprint) or know (e.g. dynamic signature) that is harder to forget and maybe cheaper to give out.*

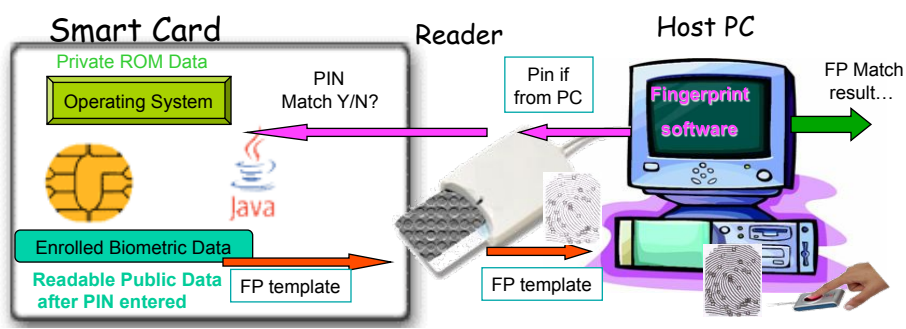
## Biometrics on Smartcards

- + No Central DB, store biometric in card.
  - + What type of system must it be?
- + Inherent multi-factor approach generally improve security.
- + Smartcard protects biometric if card is lost
- Card costs & maintenance
- Must have card to use.
- Must deal with physical reissue
- Card verification/hacking.
- Card usage is identifiable, linkable, generally observable

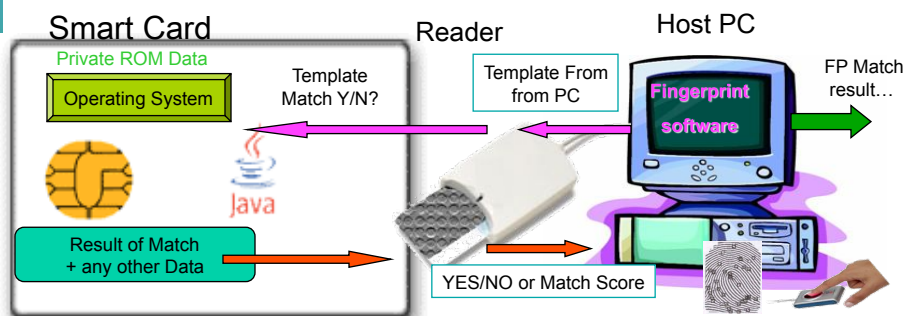


## The Problem of Adding Biometrics to Smartcards

- Traditionally, biometric data released after PIN.
- No way to add stronger security than PIN (especially if PIN is entered through host)
- Fingerprint (FP) data not really kept private, but is better than a central DB



## Match on Card: Claims more private?



- Smart-card with match on card (MOC) claims privacy enhancement as print never leaves card.
- But PC/reader collects print so no privacy advantage over “store” on card: User must trust PC/Reader. (And central DB for enrollment)
- But MOC can improve security, card only fully active after biometric matching
- System owner must still trust card’s “Yes/No”

## Everything on card/device

- Only true “smart card” solution for protecting biometric data privacy as Fingerprint may never leave the device.

Besides being expensive what are other the problems with EOC?

Duplicate Detection?

Must trust device!



<http://fidelica.com>



[www.mydigitaldefense.com](http://www.mydigitaldefense.com)



[Privaris.com](http://Privaris.com)

## Outline


- Introduction/Background
- Privacy Issues for biometrics
- Biometrics Dilemma
- Security Models/Issues
- Limits of standard protection
- Multi-factor solutions
- *Revocable biometric templates*
- *id-privacy*
- Conclusion to Part 1

Securics®: The science of security™  
© 2011  
UCCS


## "Cancelable biometrics: Non-invertible Transforms"

- Very early work in face template protection by IBM\*


Original Image 1




Intentional Distortion



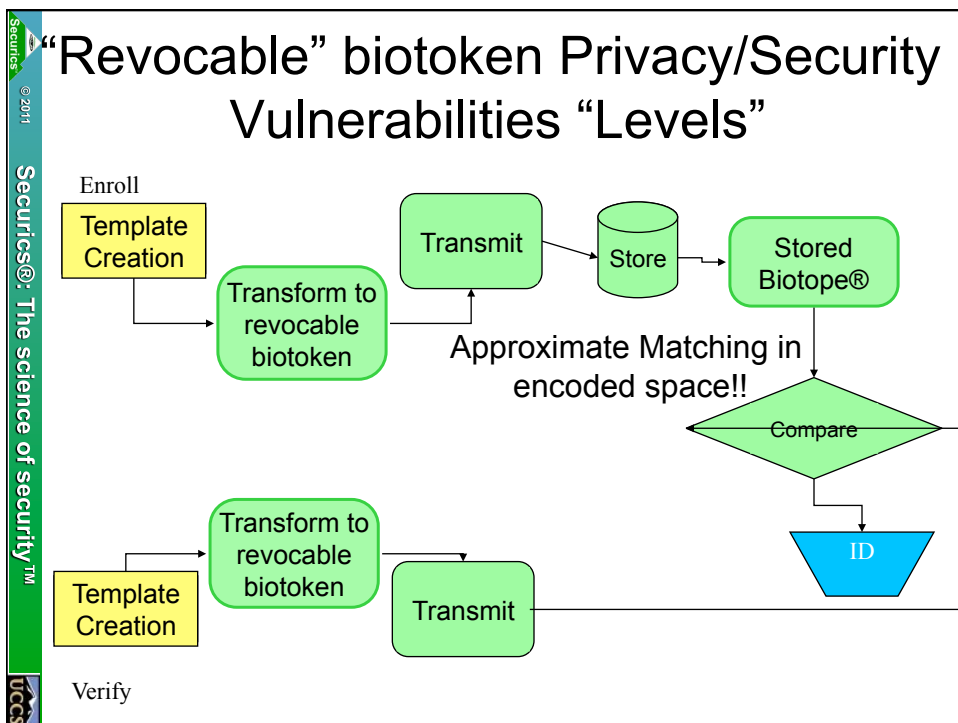
Original Image 2



Same Intentional Distortion



\*N. Ratha, J. Connell, and R. Bolle. Enhancing Security and Privacy in Biometrics-based Authentication Systems. IBM Systems Journal, 40(3):614-634, 2001.



## Basic revocability requirements

**Match while Encoded:** Tokens Are matched in their secure encoded form, without decoding/decrypting.

**Cryptographically secure:** Provides computationally intractable and cryptographically strong protection from revealing the individual identity or recovering data that matches against another of the users tokens.

## Why non-invertible is neither necessary nor sufficient.

- Let  $Z = \text{RSA}(X;N)$ ; The RSA transform is fully “invertible” (given the private key), but without the key is computationally intractable to recover  $X$  from  $Z$ .
- $Y = X^2$  is non-invertible, but has only 2 point ambiguity.
  - If we know  $x$  is positive it has none. If we shift  $x > 0$  but know or can compute the shifts, it still has none.
- Ever do a cryptogram or other puzzle?
  - Significant levels of “ambiguity” can be overcome with knowledge and the use of constraints. Biometric matchers may not even care.
- Privacy/security requires “cryptographically” secure transformations, not non-invertible ones.
- If “Non-invertible”, then when compromised must bring in customers to re-enroll. Will almost never happen.

## Basic revocability requirements

### **Partial Non-linkable revocability:**

Transform biometrics data, such that an individual's biotokens made with different keys do not match and are not linkable. The number of distinct non-matching forms must be extremely large, e.g. number of allowed integers.

**True non-linkable revocability:** each use is distinct and two uses of the same token cannot be linked. Each transaction must have unique token!

## Basic revocability requirements

- How to “revoke” a template? Work in this area must address what it means and what is process to revoke and reissue.
- Reissue must be simple/easy/cost effective.
- If reissue means people must reenroll, no company will “revoke”.
- Ideally, should support per-transaction tokens that are revoked after 1 use.

## Outline

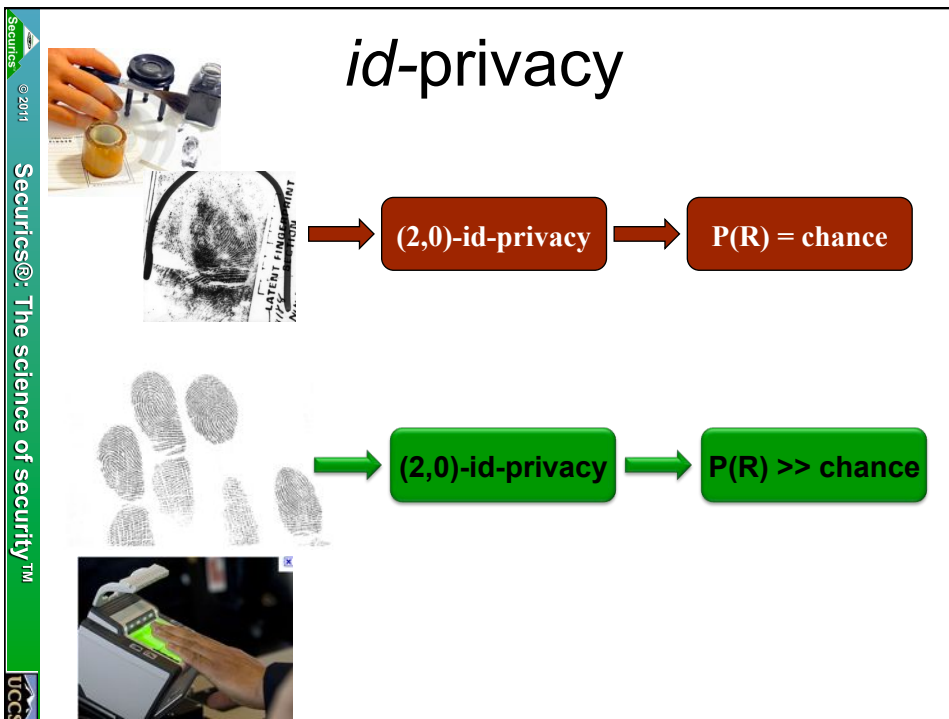
- Introduction/Background
- Privacy Issues for biometrics
- Biometrics Dilemma
- Security Models/Issues
- Limits of standard protection
- Multi-factor solutions
- Revocable biometric templates
- *id-privacy*
- Conclusion to Part 1

## Deduplication

- Any large scale/government application focused on fraud-prevention MUST support a means of detecting attempted multiple enrollments. So privacy enhanced technologies must still support deduplicaiton.
  - Does De-Duplication require search?
  - Can we do de-duplication and still limit function creap and use for other than deduplication?

## *id*-Privacy Goals

- Goals:
  - Develop a privacy preserving fingerprint recognition system that supports de-duplication
  - Specific case of multi-fingerprint
- We formally define the problem of *id*-Privacy
- Forest-Fingers for providing *id*-Privacy
- Experimentally demonstrate on largest publicly available dataset that recognition/de-duplication can be achieved while supporting *id*-privacy

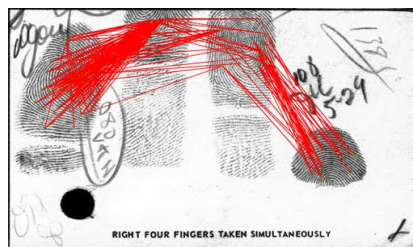


## id-privacy

*A recognition representation is said to have id-privacy when using only  $i-1$  items for the search input, the stored data cannot identify subjects with probability  $d$  greater than random chance, yet when  $i$  or more distinct items are present, the subject can be recognized at substantially above chance.*

- *This is statement about representation i.e.  $d = 0$ , no algorithm can do recognition with less than  $i$  inputs.*
- *For  $d > 0$ , algorithms/experiments can provide approximate estimate/bound on  $d$ .*
- *Broader and more precise definition than  $k$ -anonymity*
- *Defines a new class of problems/representations*

## Inter-item features for id-privacy

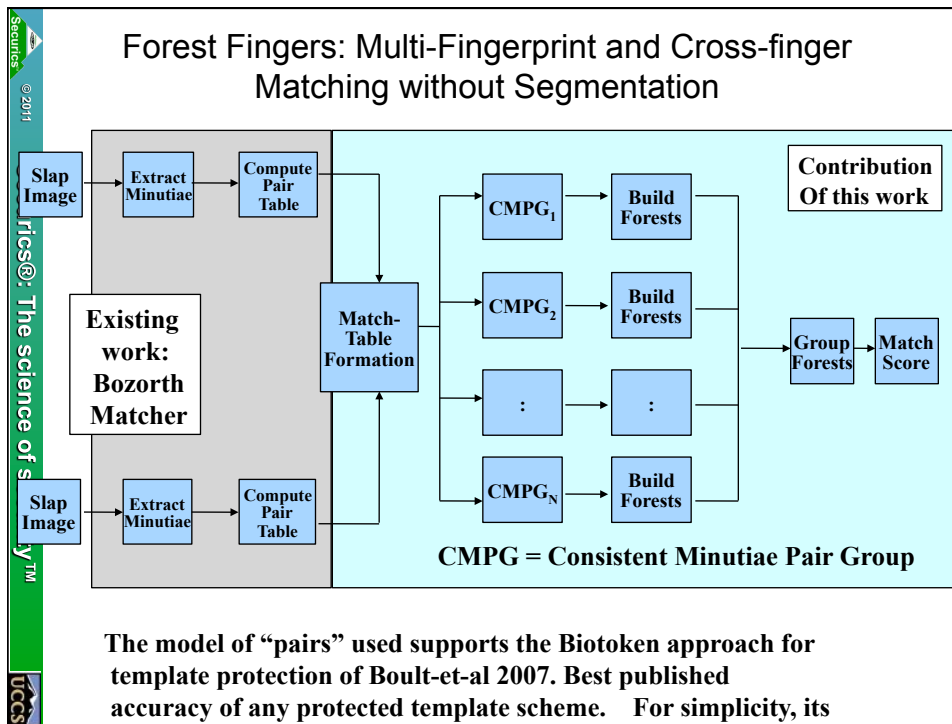


One way is to use only/predominantly inter-item features.

E.g. for fingerprints/slaps we use cross-finger representation

- Shown here is a version for (2,0)-id privacy
- Inter-item (cross-finger) mixes data from different fingers
- Since only uses features between fingers, single latent prints cannot possibly match (no edges are allowed to be formed within finger). Multiple latent would require ordering and alignment.
- Note: if individual features in pairs are unique enough, then  $d > 0$ .
- There was no “matching” algorithm for this type of representation





## Back to *id*-privacy

- Need intra-finger features. Forest algorithm directly applies, just limit choice of data in pairs.
- Can also allow some local feature pairing, resulting in  $d > 0$ .

## Proof of 2-0 id-privacy

### Assumptions:

- Let items in input = single fingers (e.g. latents !!)
- Store the data in cross-finger representation in database
- Individual features per finger are not-distinguishing, e.g. a generic minutiae.

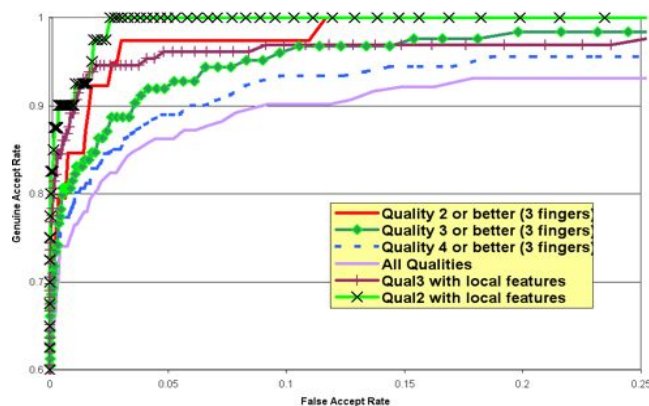
### Property 1: No recognition from single finger input

- Impossible to generate significant fraction of matching pairs
- Adversary could generate random pairs but probability of matching would be chance

### Property 2: 2 or more input fingerprints, matches above random chance

- If input is from slap image with more than 2 fingers, then valid cross-finger features will be formed. Because there is data overlap, the pair matching will be better than random resulting in  $P(R)$  better than random chance.

Inter-item matching can be easily extended to  $i > 2$  id-privacy



### Dependence on quality

- Recognition rate increases with better quality images (image quality measured with NISTQ algorithm)

### Reducing False Rejects

- Adding local features improves accuracy but increases the probability of matching with latents, yielding (2,.04)-privacy

False rejects can be improved with higher quality prints

## Conclusions

- Definition of id-privacy on which other can build
- Introduced inter-item matching as a solution and Forest Finger algorithm which applies to any inter-item matching problem, not just finger slaps.
- First solution to one of the most pressing privacy problem in large scale biometrics systems: How to perform duplicate detection while ensuring it cannot be abused for search with latents.
- Accuracy below the best methods, but is a start. performance can be improved with discriminative features like ridge-lines, PCA, DCT descriptors, or company proprietary features.

## Outline

- Introduction/Background
- Privacy Issues for biometrics
- Biometrics Dilemma
- Security Models/Issues
- Limits of standard protection
- Multi-factor solutions
- Revocable biometric templates
- *id-privacy*
- Conclusion to Part 1

## Some Opportunities

- It's not all doom and gloom.. Actual biometrics/security market size is still growing fast. Some good products are there, but lower-quality is there too. Real “breaches” are too few for users to assess actual security quality. So
  - Spend some time on PET development.
  - Compare your new work with leading commercial system(s).
  - Recruit teams of students to try to defeat your system, and/or defeat commercial systems.

### “TOP 10 Biometrics PET Requirements”

6. Helper data/keys cannot be used to compromise biometric data
7. The unit and the central authority mutually authenticate on both the unit level and the biometric-matching level.
8. It should not be possible for two users to authenticate against the same token with frequency higher than the FAR
9. Data transmitted outside the system, except during enrollment, should not be suitable for cross-matching/linking
10. *Follow a “Defense in Depth” approach*

## “TOP 10 Biometrics PET Requirements”

1. Algorithms must be openly described, and subjected to 3rd party review
2. The biotoken should be revocable and different on each transmission!
3. The user should control the usage of their templates.
4. Should allow only 1-1 or 1-few except for duplicate enrollment detection.
5. Multiple enrollments cannot be combined to recover effective biometric data