Why Biometrics and RFID are not a Panacea

(A Comedy of Errors, in Three Parts)

Peter Gutmann

University of Auckland

Introduction to Biometrics

A wide range of biometric traits can be employed

- Fingerprints, the most common mechanism
- Iris
- Retina
- Voiceprint
- Hand geometry
- Palm prints (vein structure analysed via IR light)
- …

Introduction to Biometrics (ctd)

Extract features of the presented trait and match the result against a stored template

- Process is lossy, matches are approximate

This is extremely hard for people to deal with, they expect 1:1 matches

- Weird things happen when everything comes with an associated error probability
- Example: Two biometrics are less accurate than one, see later slides

Introduction to Biometrics (ctd)

To appreciate the nature of the biometric matching process, replace all occurrences of “recognition” or “identification” with “guessing”

- (The CSI effect isn’t helping here — you never see footage of multiple experts spending hours arguing over the details of minutiae on TV)

Two Usage Modes for Biometrics

Mode 1: Access control:

- Only this exact person is allowed in
- Primary identifier uniquely identifies someone
  - Personal ID (public value)
  - PIN/password (private value)
- Biometric backs up the primary ID
  - Approximate match to a single biometric template weeds out the majority of impersonators
    - Match type is often referred to as “verification”
  - Match only this one identified person and no-one else

Two Usage Modes for Biometrics

Mode 2: Identification

- Inexact match used to find… uhh… things
  - Find one of 3 million people (DHS terrorist list) from a population of 6 billion
    - Match type is often referred to as “identification”
    - “Random guessing” is a better term, see later slides
- Real-life analogy: “Was this the person who robbed you” vs. “Find the person who robbed you in these 25 shelves of books of mugshots”
- The answer to all your terrorism problems

Introduction to RFID

Intended for for inventory control/product tracking

- Replacement for barcodes

Bar codes are per item-type

- Is this a new block of cheese, or a re-read of the previous one?

EPC tags are unique for each item

- Can track each individual item in the supply chain
- (Assuming that your back-end systems support this level of detail)

Introduction to RFID (ctd)

Bar codes need to be manually scanned

- Labour-intensive, limits throughput and/or whether the item is scanned at all

> The ability to read without line-of-sight is a principal advantage of RFID systems over bar-code systems […] scanning an item is cumbersome and expensive, and bar-codes are therefore read infrequently in the supply chain
>
> — "Integrating RFID"

EPC tag reading can be fully automated (at least in theory)

- Allows full supply-chain management

> RFID readers can sense items even when their tags are hidden […] this enables automation
>
> — "Integrating RFID"

Introduction to RFID (ctd)

Requirements for RFID

- Cheap
- Remotely readable (c.f. barcodes)
- Cheap
- Unobtrusive
- Cheap

Deployed in vast numbers

- Readers and tags are readily available at low cost
- (Vendors can sell a 5-cent tag for passport use for $*x*0)

Introduction to RFID (ctd)

RFID used for inventory control has two salient features

- Universally available technology
  - Anyone can get their hands on it
- Made to be as cheap as possible
  - Little to no security features

RFID when mis-used for other than inventory control adds a third item to the list

- Controls access to desirable items

Can you spot the problem?

Introduction to RFID (ctd)

> RFID tags have been likened to barcodes that broadcast their information, and the comparison is apt in the sense that the tiny devices have been used mainly for identifying parts and inventory, including cattle, as they make their way through supply chains […] But people are not products
>
> — Scientific American

Act 1: Politics

Biometrics and Politics

Biometrics will solve our political/ liquidity^H^H^H^Hterrorist problems

- Biometrics vendor Visionics spammed reporters on the afternoon of September 11 on the importance of their products in fighting terrorism
- Their stock rose 143 points as soon as trading reopened

Biometrics firms stock prices tripled overall in a few years after 9/11

- US Government planned to spend $8B on biometrics in the short term

Biometrics and Politics

Separate from that, the US-VISIT program alone is worth $10B over a 10-year period

- US Government Accounting Office report in 2003 said the cost would most likely end up “in the tens of billions”
- US-VISIT was a “financially very risky endeavour”

Other countries’ programs are no cheaper

- UK national ID card/passport estimated by government to cost US$5.5 billion
- Independent assessment by LSE puts it at US$15 billion

> If past experiences of IT project contracting is any guide, the actual costs will exceed even the most pessimistic estimates
>
> — The dotCrime Manifesto

Biometrics and Politics (ctd)

Biometrics had been trialled in a piecemeal manner in airports before 9/11

> An INS spokesperson says unexpected cuts in the agency’s technology budget are slowing rollouts
> — “Biometrics Takes Flight”, ID World

Then came 9/11, and all the budget problems magically cleared away…

A Short History of Biometric Pork…

US-VISIT contract was awarded to Accenture

- Formerly an Arthur Anderson LLP (of Enron fame) offshoot, reincorporated in Bermuda as a tax dodge

Accenture partnered with Datatrac Information Services Inc

- Set up by House Appropriations Homeland Security Subcommittee chairman Harold Rogers in his own congressional district
- Hired a former US government chief of procurement policy for outsourcing government work to act on their behalf

Drafted a document giving contractors great latitude and limiting the competitors to 2 or 3 “to speed the process”

A Short History of Biometric Pork… (ctd)

Four months before the contract was awarded, the Accenture team relocated into offices just below the US-VISIT official offices

The [Federal Register] Proposed Rule failed to both provide data to support its technology decisions and make the testing methods and data publicly available […]

The Proposed Rule provided no information about the threats (threat model) and risks considered relevant by the Department of State in their decision process […]

According to released documents, no independent analysis of the proposed technology was ever requested or conducted.

— "A Case Study of the Security and Privacy Risks of the US e-Passport"

A Short History of Biometric Pork… (ctd)

Accenture is overseen via phonecalls from an oversight office in Florida

- cough *Enron* cough

Documents and interviews with people familiar with the program, called US-VISIT, show that government officials are betting on speculative technology while neglecting basic procedures to ensure that taxpayers get full value from government contractors

— Washington Post

Researchers and the public were left to wonder for themselves what information and testing the Department of State was relying upon in making its technical assessments about risks and threats

— "A Case Study of the Security and Privacy Risks of the US e-Passport"

A Short History of Biometric Pork… (ctd)

The contractor and the government are working together without a clear idea of how the final virtual-border system will work or when it will be completed over the next decade. Such an arrangement is known as an “indefinite delivery-indefinite quantity contract”. The government can cancel the project at any point. The contractor is paid for specific tasks along the way, even if the overall system ultimately does not work.

For all those reasons, no one is certain of the final cost

— Washington Post

There’s no question we could end up spending billions of dollars and end up with nothing. It creates an illusion of security that doesn’t exist

— Steven Camarota, Director of Research at the
Center for Immigration Studies

A Short History of Biometric Pork… (ctd)

Quis custodiet ipsos custodes?

Weaknesses existed in all control areas and computing device types reviewed. These weaknesses collectively increase the risk that unauthorized individuals could read, copy, delete, add, and modify sensitive information

— US Government Accountability Office

DHS is spending $1.7 billion of taxpayer money on a program to detect potential terrorists crossing our borders, yet it isn’t taking the most basic precautions to keep them from hacking into and changing or deleting sensitive information

— Sen.Joseph Lieberman, chairman of the
Senate Homeland Security Committee

A Short History of Biometric Pork… (ctd)

With a little help from my friends…

UK

- Finally an excuse to introduce a de-facto national ID card
- (Government has been trying to do this for years)

Germany

- This is a great marketing opportunity for “Germany GmbH”
- (Germany already has a national ID card)

A Short History of Biometric Pork… (ctd)

Smaller countries…

(a) Variations on the UK theme

> * Why a Contactless chip?
>
> ** Ease of use both for travellers and border control staff
>
> ** High storage capacity
>
> — “New Zealand Passport Office: Securing the New Zealand Passport”

- Note no mention of “security” in the above

A Short History of Biometric Pork… (ctd)

Smaller countries…

(b) We have to do this in order to allow our citizens to travel to the US

- * New Zealand’s continued visa waiver access to the US is dependant on our ability to introduce a chip enhanced passport by 26 October 2005
- * NZ$80M impact/cost to New Zealand travellers annually if we do not maintain our visa waiver status

— “New Zealand Passport Office: Securing the New Zealand Passport”

A Short History of Biometric Pork… (ctd)

Global passport legislation as passed by US Congress

303(b)(2)The Attorney General [...] shall install at all ports of entry of the United States equipment and software to allow biometric comparison and authentication of all United States visas and other travel and entry documents issued to aliens, and passports issued pursuant to subsection 303(c)(1).

303(c)(1)The government of each country that is designated to participate in the visa waiver program [...] shall certify, as a condition for designation or continuation of that designation, that it has a program to issue to its nationals machine-readable passports that incorporate biometric and document authentication identifiers.

— Enhanced Border Security and Visa Entry Reform Act of 2002

A Short History of Biometric Pork… (ctd)

> Of the 25 countries that have been most adversely affected by terrorism since 1986, eighty percent have national identity cards, one third of which incorporate biometrics. This research was unable to uncover any instance where the presence of an identity card system in those countries was seen as a significant deterrent to terrorist activity
>
> — Privacy International study, 2004

> It is almost exclusively the paranoia of the US that is driving the use of e-passports to contribute to the Homeland Security of their country
>
> — Dr.Thomas Petermann, Bureau for Technology Assessment, German Parliament (translated)

Biometrics as a Dragnet

Can only compare traits against a database of trait characteristics

- Terrorists would have to register with the DHS in advance

Typical terrorist photo is a grainy 10-year-old B&W shot at 150m distance

- c.f. problems with authenticating bin Laden videos/broadcasts
- Requires a panel of experts to authenticate even when he announces his identity and provides a long stream of video/audio

Biometrics as a Dragnet (ctd)

Terrorism works because no-one knows who the grunts are

- Biometrics can never catch disposable terrorists

  Terrorist organisations will use operatives who are neither known to, nor suspected by, the targeted countries. Identifying individuals who are not identifiable as threats can't enhance security; worse yet, relying on such measures actually undermines security because it lulls us into a false sense of security

  — "The Assault on Logic", Michael Caloyannides

Biometrics as a Dragnet (ctd)

Stanford University researcher Lawrence Wein found that US-VISIT had only a 53% chance of catching a terrorist who was already listed on a watch list

- Chances of catching a non-listed terrorist are 0%

Example: Blacklist-based border security in action:

> On April 25, Gregory Despres arrived at the U.S.-Canadian border crossing at Calais, Maine, carrying a homemade sword, a hatchet, a knife, brass knuckles and a chain saw stained with what appeared to be blood. U.S. customs agents confiscated the weapons and fingerprinted Despres. Then they let him into the United States
>
> — Associated Press

- ("You're not on the list, welcome to the US!")

Biometrics as a Dragnet (ctd)

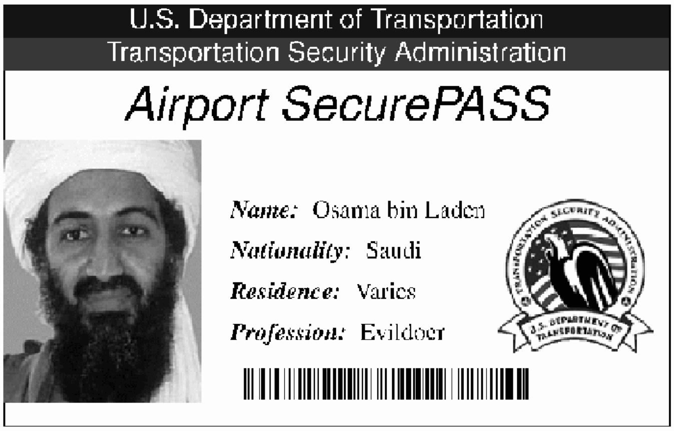
No biometric system has ever caught a terrorist or serious criminal

- The laws of chance mean that they’ll eventually get one somewhere
- (We’ll never hear the end of it when they do)

Biometrics as a Dragnet (ctd)

> When a highway patrolman is sent to his duty, he has to be given the authority to cite traffic violators. This cannot be done explicitly for each violator because at the time that the patrolman is sent to his duty, the traffic violator does not exist, and the identity of the future violators is not known, so that it is impossible to construct individual access rights for the violators at that time. The point is that the patrolman’s authority has to do with the behavior of motorists, not their identity
>
> — Naftaly Minsky, International Journal of Computer and Information Sciences, June 1978.

The only Effective ID for catching Terrorists



U.S. Department of Transportation
Transportation Security Administration

Airport SecurePASS

Name: Osama bin Laden

Nationality: Saudi

Residence: Varies

Profession: Evildoer

Image courtesy Steve Bellovin

How to apply this ID: Stop everyone who has given their occupation as “Evildoer”

But at Least It’s Doing Something…

The Politician’s Fallacy

1. Something must be done
2. This is something
3. Therefore this must be done

Q: How many cases of forged German identity documents in any conceivable way connected with terrorism is the government aware of?
A: None

— German parliamentary question, 29 May 2007 (translation)

What *real* safety measures could have been taken for the $10-20B that’s being thrown at biometrics?

- You could employ an awful lot of extra policemen for $10B

But at Least It’s Doing Something… (ctd)

Genuine (but false) DMV-issued ID in the US costs $2,000-$4,000

- Costs determined by auditors, private investigations, journalists, …

In one case Virginia asked 250 licensees to return fraudulently-issued licenses

- 13 drivers complied

In California, an investigation found DMV employees selling genuinely fake ID right after an anti-corruption operation to stop this practice had been concluded

But at Least It’s Doing Something… (ctd)

CDT study found corruption and security lapses “rampant” in DMVs

Even non-corrupt DMVs have problems

- Connecticut Auditor of Public Accounts found that the DMV couldn’t detect the use of fraudulent documents used to obtain new credentials

Search YouTube for “drivers license prank” for many examples of how outrageous you can make this

Other countries are no better

- UK requires two forms of ID like a household bill and a bank statement when applying for a passport

But at Least It’s Doing Something… (ctd)

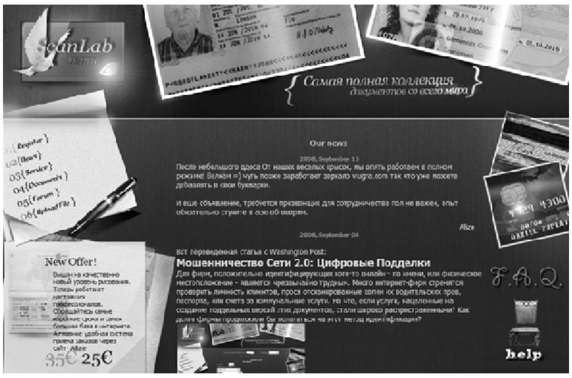
This makes it easy to bootstrap stronger and stronger forms of ID from easily-forged weaker ones

> Many of the documents accepted as proof of identity can be forged well enough to fool bored and indifferent DMV workers. The documents they then issue incorporate the weaknesses of the identifiers used to substantiate them
>
> — James Harper, “Identity Crisis”

> There is no identity check on the person signing for the passport when it arrives. In multi-occupancy flats they can be handed to anyone at the address. Thousands have already gone missing
>
> — Daily Mail, “‘Safest ever’ passport not fit for purpose”

But at Least It’s Doing Something… (ctd)

Large-scale commercial operations exist to manage identity document fraud



Our news

2008, September 15

После небольшого дэса От наших веселых крысок, мы опять работаем в полном режиме! Велкам =) чуть позже заработает зеркало vugra.com так что уже можете добавлять в свои букмарки.

И еще объявление, требуется прозвонщик для сотрудничества пол не важен, опыт обязательно стучите в асю обговорим.

Alize

2008, September 04

Вот переведенная статья с Washington Post:

Мошенничество Сети 2.0: Цифровые Подделки

Для фирм, положительно идентифицирующих кого-то онлайн - по имени, или физическое местоположение - является чрезвычайно трудным. Много интернет-фирм стремятся проверить личность клиентов, прося отсканированные копии их водительских прав, паспорта, или счета за коммунальные услуги. Но что, если услуги, нацеленные на создание поддельных версий этих документов, стали широко распространенными? Как долго фирмы продолжили бы полагаться на этот метод идентификации?

New Offer!

Вышли на качественно новый уровень рисования. Теперь работает настоящих профессионалов. Обращайтесь самые короткие сроки и самая большая база в интернете. Активная удобная система приема заказов через сайт. Alize

~~35€~~ 25€

- Will create proof-of-ID fax/photocopy of any document you want in any name you want

But at Least It’s Doing Something… (ctd)

The checking with passports is only slightly better than with drivers’ licenses

> Getting one of these supersecure passports under false pretenses isn’t particularly difficult for anyone with even basic forgery skills
>
> — Foreign Policy Magazine

US Government Accounting Office (GAO) had no problems obtaining multiple passports using fake names and fraudulent documents

- One for a dead person, one for a fictitious five-year-old pretending to be 53, one for …

But at Least It’s Doing Something… (ctd)

GAO investigators then used these genuine false passports to buy a plane ticket…

- … obtain a boarding pass …
- … and get past airport security

This is exactly what the introduction of these passports was supposed to prevent!

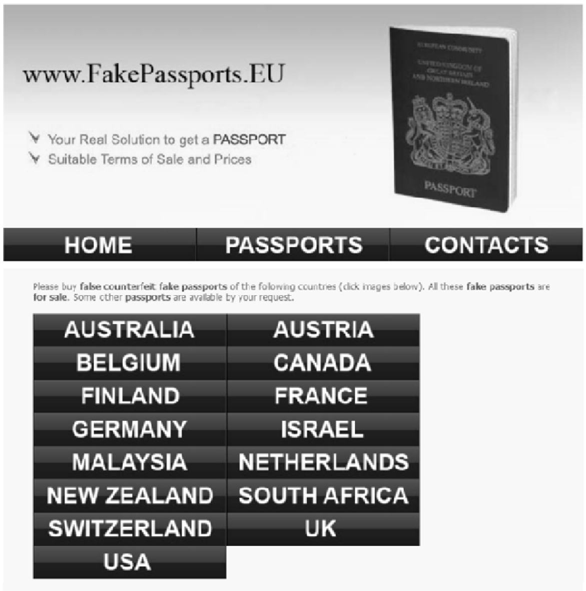
> The State Department agreed that there was a “major vulnerability” in the passport issuance process and agreed to study the matter
>
> — “Dead Man Gets Passport”

But at Least It’s Doing Something… (ctd)

Or you can just cut out the middleman…

- Netherlands: €800
- UK: €1000
- USA: €1100

Rule of thumb: passports cost about 1000 of any major currency



www.FakePassports.EU

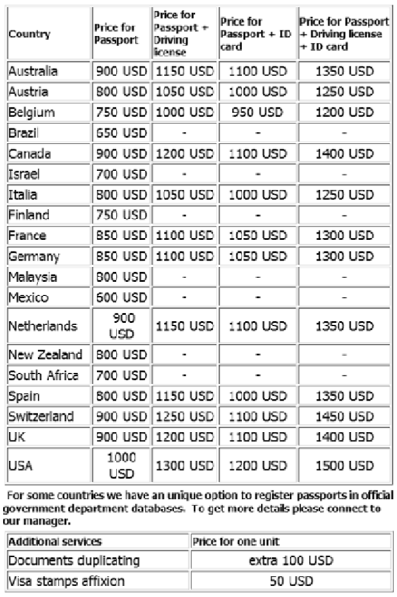
Your Real Solution to get a PASSPORT

Suitable Terms of Sale and Prices

Please buy **false counterfeit fake passports** of the folowing countries (click images below). All these **fake passports** are **for sale**. Some other **passports** are available by your request.

But at Least It’s Doing Something… (ctd)

Passports and associated documents are actively sold online by multiple vendors



Country	Price for Passport	Price for Passport + Driving license	Price for Passport + ID card	Price for Passport + Driving license + ID card
Australia	900 USD	1150 USD	1100 USD	1350 USD
Austria	800 USD	1050 USD	1000 USD	1250 USD
Belgium	750 USD	1000 USD	950 USD	1200 USD
Brazil	650 USD	-	-	-
Canada	900 USD	1200 USD	1100 USD	1400 USD
Israel	700 USD	-	-	-
Italia	800 USD	1050 USD	1000 USD	1250 USD
Finland	750 USD	-	-	-
France	850 USD	1100 USD	1050 USD	1300 USD
Germany	850 USD	1100 USD	1050 USD	1300 USD
Malaysia	800 USD	-	-	-
Mexico	600 USD	-	-	-
Netherlands	900 USD	1150 USD	1100 USD	1350 USD
New Zealand	800 USD	-	-	-
South Africa	700 USD	-	-	-
Spain	800 USD	1150 USD	1000 USD	1350 USD
Switzerland	900 USD	1250 USD	1100 USD	1450 USD
UK	900 USD	1200 USD	1100 USD	1400 USD
USA	1000 USD	1300 USD	1200 USD	1500 USD

For some countries we have an unique option to register passports in official government department databases. To get more details please connect to our manager.

Additional services	Price for one unit
Documents duplicating	extra 100 USD
Visa stamps affixion	50 USD

But at Least It’s Doing Something… (ctd)

Fake passports were tested by a BBC journalist

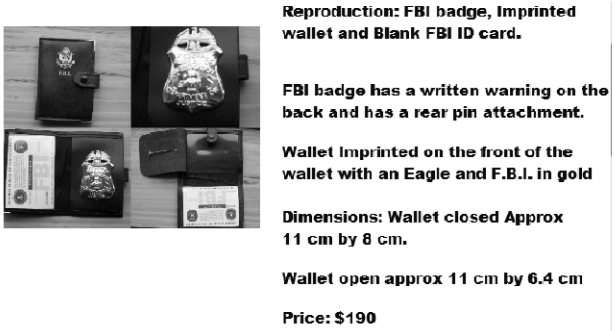
> Getting fake passports is neither very difficult nor very expensive […] Among the dealers I met, most were confident that their passports would get me into Britain. One was so sure he said I did not have to pay until I had crossed into Britain. And another one offered me an insurance policy on his passport
>
> — “Panorama: My Fake Passports and Me”

- Journalist had no problems entering the UK with fake passports at two different points of entry

> I met many immigrants in the UK on fake identities and passports. If I can get in so easily to Britain on not one, but two fake passports, just think who else could get in?
>
> — “Panorama: My Fake Passports and Me”

But at Least It’s Doing Something… (ctd)

Other types of fraudulent ID are also readily available



Reproduction: FBI badge, Imprinted wallet and Blank FBI ID card.

FBI badge has a written warning on the back and has a rear pin attachment.

Wallet Imprinted on the front of the wallet with an Eagle and F.B.I. in gold

Dimensions: Wallet closed Approx 11 cm by 8 cm.

Wallet open approx 11 cm by 6.4 cm

Price: $190

- Law enforcement officers couldn’t tell the difference between the fake badges and real ones

But at Least It’s Doing Something… (ctd)

Undercover investigators were able to purchase nearly perfect counterfeit badges for all of the Department of Defense’s military criminal investigative organizations to include the Army Criminal Investigation Command (Army CID), Naval Criminal Investigative Service (NCIS), Air Force Office of Special Investigations (AFOSI), and the Marine Corps Criminal Investigation Division (USMC CID). Also available for purchase were counterfeit badges of 42 other federal law enforcement agencies including the Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA), Alcohol, Tobacco and Firearms (ATF), Secret Service, and the US Marshals Service

— “Security Threat: Fraudulent Law Enforcement Credentials and Badges”

But at Least It’s Doing Something… (ctd)

The investigators found exact reproductions of the badges issued to Federal Air Marshals, Transportation Security Administration (TSA) Screeners, TSA Inspectors, and Special Agents of the TSA Office of Inspector General

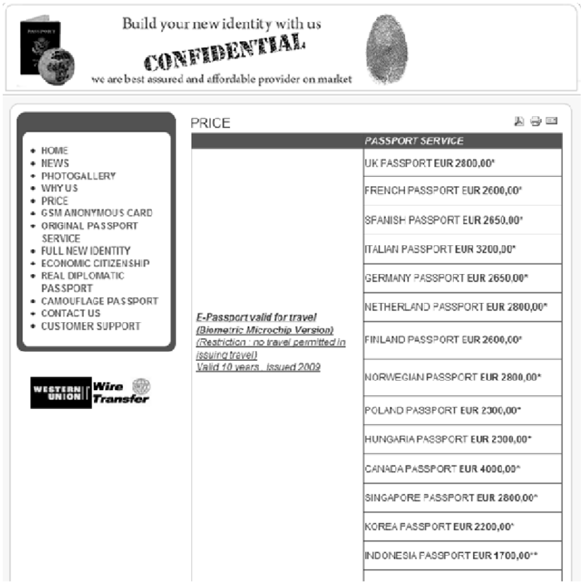
— “Security Threat: Fraudulent Law Enforcement Credentials and Badges”

- Investigators were able to enter 19 federal sites, 2 commercial airports, 6 military installations, 2 federal courthouses, and 3 state buildings (every one they tried) using the fake ID
- They were unchecked by security and “could have carried weapons, listening devices, explosives, and other such materials”

But at Least It’s Doing Something… (ctd)

So what about high-security biometric passports?

- This is one vendor, of many…



Build your new identity with us

CONFIDENTIAL

we are best assured and affordable provider on market

- HOME
- NEWS
- PHOTOGALLERY
- WHY US
- PRICE
- GSM ANONYMOUS CARD
- ORIGINAL PASSPORT SERVICE
- FULL NEW IDENTITY
- ECONOMIC CITIZENSHIP
- REAL DIPLOMATIC PASSPORT
- CAMOUFLAGE PASSPORT
- CONTACT US
- CUSTOMER SUPPORT

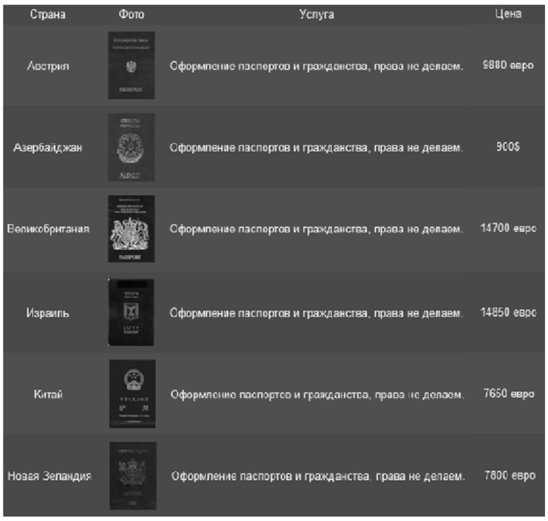
WESTERN UNION Wire Transfer

PRICE

	PASSPORT SERVICE
E-Passport valid for travel (Biometric Microchip Version) (Restriction : no travel permitted in issuing travel) Valid 10 years , issued 2009	UK PASSPORT **EUR 2800,00***
	FRENCH PASSPORT EUR 2600,00*
	SPANISH PASSPORT **EUR 2650,00***
	ITALIAN PASSPORT **EUR 3200,00***
	GERMANY PASSPORT **EUR 2650,00***
	NETHERLAND PASSPORT **EUR 2800,00***
	FINLAND PASSPORT EUR 2600,00*
	NORWEGIAN PASSPORT **EUR 2800,00***
	POLAND PASSPORT EUR 2300,00*
	HUNGARIA PASSPORT **EUR 2300,00***
	CANADA PASSPORT **EUR 4000,00***
	SINGAPORE PASSPORT **EUR 2800,00***
	KOREA PASSPORT **EUR 2200,00***
	INDONESIA PASSPORT **EUR 1700,00****

But at Least It’s Doing Something… (ctd)

Guess where most of them are based…



Страна	Фото	Услуга	Цена
Австрия		Оформление паспортов и гражданства, права не делаем.	9880 евро
Азербайджан		Оформление паспортов и гражданства, права не делаем.	900$
Великобритания		Оформление паспортов и гражданства, права не делаем.	14700 евро
Израиль		Оформление паспортов и гражданства, права не делаем.	14850 евро
Китай		Оформление паспортов и гражданства, права не делаем.	7650 евро
Новая Зеландия		Оформление паспортов и гражданства, права не делаем.	7800 евро

But at Least It’s Doing Something… (ctd)

In some cases it’s now cheaper to get a fake passport than a real one

- Holders of foreign passports used to be able to get them issued/renewed via the local consulate
- Because of the “enhanced security” of e-passports, consulates can no longer do this
- Only a small number of locations can issue them…
- …possibly in another country…
- …several thousand kilometres away
- One such passport renewal required two round trips (air fares, hotel stays), several days taken off work, …

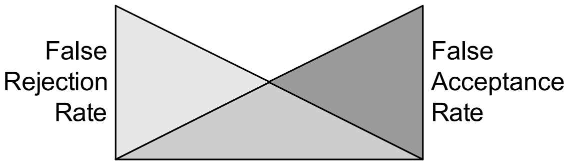
Once the cost was added up, it would have been cheaper to get it from the Russians

Biometrics 101

Biometrics is not a precise science

- All matching is approximate

Biometric use is a tradeoff between false acceptance rate (FAR) and false rejection rate (FRR) (think IDS)



- Good security = high FRR
- Good acceptability = high FAR

Biometrics 101 (ctd)

Medical research has standard terminology for these measures

- Sensitivity = $\dfrac{\text{true positives}}{\text{true positives + false negatives}}$
- Selectivity = $\dfrac{\text{true negatives}}{\text{true negatives + false positives}}$
- FAR/FRR is also called the “fraud rate” and “insult rate” in banking circles

Biometrics 101 (ctd)

Public claims about biometrics are mostly still at the 19th-century patented cure-all medicine stage

- There *is* serious research being done, but it rarely comes through when the biometric technology is being sold to the public

Some areas simply aren’t understood at all

- Like phrenology, it’s just assumed that they work a certain way

> The scientific basis of biometrics — from understanding the distributions of biometric traits within given populations to how humans interact with biometric systems — needs strengthening
>
> — US National Research Council

Biometrics 101 (ctd)

Example: London City Airport

- Fingerprint scans for access control
- 1,600 employees
- 90,000 prints/day
- FAR = 1.5%, FRR = 0.001%
  - Vendor figures, these are always *exceedingly* optimistic (see later slides)
- Result: 1,500 false alarms per day
  - That's more than *one false alarm a minute* nonstop, 24 hours a day

Statistical term for this is the base rate fallacy

The Base Rate Fallacy

Bob likes to show off, is married to a performer, has several tattoos, and will do almost anything on a dare.

Is Bob a librarian, farmer, trapeze artist, lawyer, or teacher?

The Base Rate Fallacy (ctd)

Bob likes to show off, is married to a performer, has several tattoos, and will do almost anything on a dare.

Is Bob a librarian, farmer, trapeze artist, lawyer, or teacher?

Most people will say “trapeze artist”

- Matches the stereotype

What’s the base rate for trapeze artists?

- Farmers, lawyers, teachers outnumber them 100,000 to 1 or more

Bob is likely to be a almost anything but a trapeze artist

- (This is a famous problem from psychology, “Linda scenario”)

Theoretical Background

Analysing false positives using the base-rate fallacy

- Apply a test for infection with the dreaded lurgy
- Test is 99% accurate
  - 99 of 100 ill patients will be detected
  - 99 of 100 healthy patients will be cleared
- Only 1 in 10,000 people have the disease
- Your doctor tells you that you’ve tested positive

What’s the chance that you actually have this disease?

Theoretical Background (ctd)

From Bayesian statistics we have that

$$p(\mathrm{S}|\mathrm{P}) = \frac{p(\mathrm{S}) \times p(\mathrm{P}|\mathrm{S})}{p(\mathrm{S}) \times p(\mathrm{P}|\mathrm{S}) + p(\sim\mathrm{S}) \times p(\mathrm{P}|\sim\mathrm{S})}$$

where

- S = probability of being ill
- ~S = probability of not being ill
- P = probability of a positive test result
- ~P = probability of a negative test result

Theoretical Background (ctd)

Plugging in the numbers

$$p(\mathrm{S}|\mathrm{P}) = \frac{{}^{1}/_{10000} \times 0.99}{{}^{1}/_{10000} \times 0.99 + (1 - {}^{1}/_{10000}) \times 0.01}$$

$$= 0.00980$$

$$= \sim 1\%$$

Even though the test is 99% certain, the fact that the population of healthy people is much larger than the population with the disease means that your chance of really having lurgy is only 1%

Theoretical Background (ctd)

Expressed as natural frequencies this is far more obvious

- 10 in 100,000 people have the disease (1 in 10,000)
- Of these 10 people, 9.9 will have a positive result
- Of the remaining 99,990 people, 999 will also have a positive result
- 100 times more likely to be a false positive than a true positive!
  - See “How to Improve Bayesian Reasoning without Instruction: Frequency Formats” for more

Theoretical Background (ctd)

Even though the test is 99% certain, the fact that the population of ordinary people is much larger than the population of terrorists means that your chance of really finding a terrorist is only 1%

- This has been ably demonstrated by US government travel watchlists: Nothing but false positives

Theoretical Background (ctd)

Real-world example of the base-rate fallacy in effect: Visionix/Identix trial at Palm Beach International Airport

- Database was seeded with picture-perfect voluteer “terrorist” photos
- 1 in 100 non-terrorists were identified as terrorists
  - (Oh, and over half the “terrorists” were missed)
- Real-terrorist base rate estimated at 1 in 10,000,000 (at best)

10,000 false alarms for every real terrorist identified...

- ... or at least guessed at, < 50/50 chance of actually catching them

Theoretical Background (ctd)

OK, so we get a few false alarms...

- Imagine a full terrorist alert (airport locked down, SWAT teams, ...)
- Now multiply that by ten thousand
- Now consider that you still have less than coin-toss odds of actually catching someone

The base-rate fallacy has been the death of IDSes

- “The Base-rate Fallacy and the Difficulty of Intrusion Detection” predicted why IDSes would fail years before the market determined this empirically

Biometrics and 9/11

Why didn’t the US government use biometrics before 9/11?

> The government didn’t have this stuff in place, precisely because it had been working on it and knew its limitations and didn’t find any value for the costs involved. The government has been on top of this; the government’s position hasn’t changed
>
> — Jim Wayman, former director, US Government Biometrics Center

Biometric Data Protection

Biometric data is often sent around unprotected

- c.f. Plaintext passwords

Example biometric system: Sensor outputs a binary yes/no signal on an external signal wire

- Capture biometric data with USB Snoop (software), USB Agent (hardware)

Biometric Data Protection (ctd)

Once one biometric becomes the standard, everyone will know it

- Most biometric systems use open view traits

  > I object to leaving my password on every glass I touch
  >
  > — Anon

  > A fingerprint is hardly personal data because you leave it on glasses and silverware and articles all over the world, they're like footprints. They're not particularly private
  >
  > — Michael Chertoff, Secretary of Homeland Security

Biometric Data Protection (ctd)

German CCC members obtained Interior Minister Wolfgang Schäuble's prints from a wine glass he'd touched

- (Schäuble is a strong advocate of control technology)
- Published the prints in their monthly magazine "Datenschleuder"

Included a thin film to place over your fingers and fool fingerprint readers

> We recommend that you use the film whenever your fingerprint is taken, such as when you enter the US, stop over at Heathrow, or even when you touch bottles at your local supermarket – just to be on the safe side
>
> — "CCC Publishes Fingerprints of German Home Secretary"

Biometric Data Protection (ctd)

CCC is creating a "biometric photo album" of biometric credentials of German politicians

> German Chancellor Angela Merkel and Bavaria's Minister President Günther Beckstein are on the list
>
> — "CCC Publishes Fingerprints of German Home Secretary"

Gattaca has arrived, but not the way that the politicians wished

> Biometrics rely on the secrecy of something that isn't very secret
>
> — Phillip Hallam-Baker, Verisign chief scientist

Biometric Data Protection (ctd)

Fingerprints can even be read remotely

- State-of-the-art in 2010 could read prints from 2m away using a portable, concealable device smaller than a tissue box
- Print is scanned in 0.1s

All-five-fingers device was due to be released the following year

> As with all new technology, the hope is further advancements will follow and increase the standoff distance
>
> — "Fingerprints Go the Distance"

By 2012, this had increased to 6m

> There's no need for a subject to touch a scanner to get a reading
>
> — "IDair's new fingerprint reader captures prints from 6m"

Biometric Data Protection (ctd)

US DoD is sponsoring work at CMU to read iris prints from 13m away

- “It’s so convenient, you can remotely read anyone’s biometrics without their knowledge… oh, wait…”

Biometric Data Protection (ctd)

ICAO biometric passport design leaks data everywhere

- Passport-processing systems in general leak data everywhere

May 2007: British visa processing leaks details of 50,000 applications

> It was a potential treasure trove for identity thieves and terrorists
>
> — Channel 4 News, UK

- The same organisation had problems with applications from Russia and Nigeria
  - (These two countries are probably the worlds two largest sources of online fraud activity)

Biometric Data Protection (ctd)

December 2007: Passport Canada allows anyone to access anyone else’s passport application info

> Boom, there was somebody else’s name and somebody else’s data
>
> — Jamie Laning, Globe and Mail

August 2008: Verified Identity Pass loses laptop containing personal information for 33,000 TSA-vetted travellers

- Allows them to bypass security lines at airports

Even something as (apparently) non-passport related as UK Tax and Customs’ loss of 25 million personal records would provide all the data needed to defeat the passport’s access control mechanism (BAC)

Biometric Data Protection (ctd)

Every country you visit ends up with a copy of your biometric ID

- Russia, Romania, Ukraine, China, Iran, Burma/Myanmar, …
- Many of these countries hold your passport for you for varying amounts of time
  - (See later slides on decoupled passport authorisation)

Prices for a CD or DVD of stolen data in Gorbushka market, Moscow

- Cash transfer records from Russia’s central bank: $1,500
- Tax records, including home addresses and incomes: $215
- Name, birthday, passport number, address, phone number, vehicle description, and VIN for every driver in Moscow: $100

Biometric Data Protection (ctd)

US Government: “These passports are a great justification for us getting our hands on everyone’s biometric traits”

Russian mafia: “Works for us too :-)”

> This enormous potential for organised crime and foreign governments creates a nightmare for citizens and law enforcement, since it’s the exact opposite of what was intended and what government propaganda lead us to believe
>
> — Andreas Pfitzmann, iX magazine 10/2007

Biometric Data Protection (ctd)

Mind you, it’s not just the Russian mafia that wants to steal your biometric data…

```
Thursday, 16 April 2009, 14:11
S E C R E T STATE 037561 NOFORN
SUBJECT: (S) REPORTING AND COLLECTION NEEDS: AFRICAN
  GREAT LAKES (DROC, BURUNDI, RWANDA)
REF: A. 08 KIGALI 00830--05/DEC/2008 B. 08 STATE
  122706--19/NOV/2008 C. 04 STATE 101403--
  06/MAY/2004
Classified By: SUZANNE MCCORMICK, DIRECTOR, INR/OPS,
  REASON: 1.4(C).

Biographic and biometric data, including [...]
  fingerprints, facial images, DNA, and iris scans.
CLINTON
```

Biometric Data Protection (ctd)

> Whilst still susceptible to traditional ID document abuse scenarios, new Machine Readable Travel Documents (MRTDs) offer numerous additional threats [...] The combination of these threats and weaknesses puts the security and privacy of European citizens at significant risk
>
> — Budapest Declaration on Machine Readable Travel Documents (MRTDs)

Biometric Data Protection (ctd)

As with SSNs, mission creep will mean that eventually *everyone* (not just governments) will have your biometric credentials

California Senate Bill 504, 18 February 2005

> No [car] dealer issued a license pursuant to this article [California Vehicle Code] shall sell a vehicle without first obtaining the right thumbprint of the purchaser and a photocopy of his or her valid form of identification

- This was piggybacked through buried inside an unrelated bill (in this case covering real estate transactions), a trojan horse trick often used in the US for unpopular measures
- Clause was removed before the bill became law

Biometric Data Protection (ctd)

Individual car dealers have already begun asking customers for biometric credentials

- Southbay BMW in California required all customers to deposit their biometric credentials “to prevent identity theft”
- Credentials are stored for seven years
  - (Imagine how secure the typical car dealer’s file server is going to be)

Biometric is never checked or matched against anything, it’s simply recorded and filed for seven years

- Practice continued until someone complained (loudly) and it got widespread media attention

Biometric Data Protection (ctd)

Federal Housing Finance Regulatory Reform Act of 2008

- Fingerprint registry requirements sneaked into the bill as a “manager’s amendment”

  > The fingerprinting requirements are not mentioned in bill summaries and press releases, or even in the table of contents of the Senate bill. Queries to the Senate Banking Committee and various senators haven’t been answered
  >
  > — Wall Street Journal

  - Another trojan horse measure, as with the CA bill
- Individual’s are required to “furnish […] information concerning the applicant’s identity, including fingerprints”

Biometric Data Protection (ctd)

This is already happening in some countries where biometrics are used for non-border-control/access control purposes

Example: Australia uses it for patrons of bars and clubs

> Pubs and clubs are signing up in droves to national and state biometrics databases that capture patron fingerprints, photos and scanned driver licences

- Security for the biometric data is… optional

> The databases are virtually free from government regulation as biometrics are not covered by privacy laws, meaning that the handling of details are left to the discretion of technology vendors
>
> — "National biometric pub list use 'explodes'"

Biometric Data Protection (ctd)

Example of credentials everywhere: Canon's iris watermarking (US patent application 2008/0025574)

- For copyright control purposes, your camera can embed a copy of your iris data in every photo you take
- Patent text is intentionally vague, but it appears that information will be attached as metadata
  - Not a watermark on the image itself but standalone biometric credentials alongside the image
  - One paragraph even suggests storing a raw iris image
  - No indication of who does the matching in case of a dispute
- (Additional problem: If you want to photograph child porn, steal or buy a used camera and use the stored credentials of the previous owner)

Biometric Data Protection (ctd)

Afghan girl’s identity was verified using IrisCodes extracted from her photo in National Geographic

Source: www.cl.cam.ac.uk/~jgd1000/afghan.html

- (Iriscodes are biometric identification traits from Iridian Technologies)

If I have your photo, I have your iris-scan ID

Biometrics and RFID

After September 11, biometrics vendors teamed up with RFID vendors to push the combined system to the US government

- No clear threat model, just “you need this to be secure”

  No coherent, integrated security concept for MRTDs [machine-readable travel documents] has been disclosed either to the general public or to interested experts

  — Budapest Declaration on Machine Readable Travel Documents

Biometrics and RFID

Publication of the US e-Passport Proposed Rule in the Federal Register resulted in 2,335 comments being submitted

- A total of 1% supported the move

  Overall, approximately 1% of the comments were positive, 98.5% were negative, and .5% were neither negative nor positive

  — US Department of State, Public Notice 5208

  Americans aren't that concerned about the RFID, particularly in this day and age when there are a lot of other ways to access personal information on people

  — Gigi Zenk, Washington State Department of Licensing

Biometrics and RFID (ctd)

Original (pre-9/11) ICAO plan was to use a 2D bar code containing a digitised form of the photo

- Standard ID counterfeiting technique swaps one photo for another

  [Photo] tampering represents about two-thirds of all passport fraud

  — John Mercer, US State Department Passport Office

- Just the right measure to solve a particular problem

Then business and politics got involved in what had been a state department administrative matter…

Biometrics and RFID (ctd)

RFIDs in passports are a disaster waiting to happen

- Do you want to broadcast your identity to everyone near you?

  > I suggested at an ISO/ICAO meeting last July in London to add a small metal shield to the front cover page of the passport, such that the RFID coil antenna in the back cover page can work effectively only while the passport booklet is open. This idea was quickly rejected by those driving the project as a privacy concern and therefore “of little interest here”
  >
  > — Markus Kuhn, Cambridge University

Biometrics and RFID (ctd)

Privacy issues never seem to come up in these projects…

In 2001 the European Central Bank proposed putting RFID into higher-denomination banknotes

- Idea was abandoned due to tag cost and problems with physical protection of chip and antenna in thin flexible notes

No (published) discussion even mentioned the security concerns

- Allows muggers to more easily identify worthwhile targets

The most stupid use of RFID ever proposed (well, so far)

- If the only tool you have is a hammer, everything looks like a thumb

Biometrics and RFID (ctd)

Industry lobbyists have managed to get RFID excluded from ever being subject to standard privacy controls

> In response to these concerns, dozens of U.S. states have introduced RFID consumer-protection bills — which have all been either killed or gutted by heavy opposition from lobbyists for the RFID industry. On the federal level, no high-profile consumer-protection bills related to RFID have been passed. Instead, in 2005, the Senate Republican High Tech Task Force praised RFID applications as “exciting new technologies” with “tremendous promise for our economy” and vowed to protect RFID from regulation or legislation
>
> — Scientific American

Biometrics and RFID (ctd)

Europe is little better

> E.U. commissioner for information society and media Viviane Reding announced that the commission would not regulate RFID but instead would allow businesses to regulate themselves. “I am here to tell you that on RFIDs, there is not going to be a regulation”, she said. “My view is that we should underregulate rather than overregulate so that this sector can take off”
>
> — Scientific American

Biometrics and RFID (ctd)

Although concerns about the US e-Passport's vulnerability to skimming were first raised in January 2003, tests to examine the vulnerability weren't started until February 2005

- The original deployment date was supposed to be December 2004

Biometrics and RFID (ctd)

FOIA'd documents established that US officials simply ignored the skimming issue

> Maybe I am grasping at straws, but it would be great it we could say that [RFID] really doesn't involve any additional risk
>
> — Frank Moss, Deputy Assistant Secretary of State for Passport Services, FOIA'd documents, April 2005

> Cloning Threats: Compared to paper based MRTDs copying the signed data stored on the RF-Chip is easily possible in general
>
> — PKI for MRTDs, Annex G: PKI and Security Threats

If you're familiar with RFID technology then US Department of State Public Notice 5208 is worth reading for its sheer entertainment value

Biometrics and RFID (ctd)

US e-Government Act of 2002 requires a privacy impact assessment (PIA) for IT projects

- Department of State PIA is a cursory two-page document that lacks any discussion of RFID and doesn't identify or address any RFID risks
- DHS PIAs for RFID in contrast are 14 and 34 pages long

> A comparison of the PIAs, without background knowledge of the projects, would lead to the erroneous understanding that the two agencies were undertaking wildly different projects
>
> — "A Case Study of the Security and Privacy Risks of the US e-Passport"

Do as I Say, Not as I Do

The US government has its own biometric ID standard, FIPS PUB 201-1, "Personal Identity Verification (PIV) of Federal Employees and Contractors"

- Differs wildly from the e-passport requirements

In some cases FIPS 201 mandates the exact opposite of what's done in the e-passport

- e-passport: Biometric data is stored in the passport and sent via the contactless interface to the reader
- US govt: Biometric data shall not be sent over the contactless interface for security and privacy reasons

Do as I Say, Not as I Do (ctd)

Rest of the talk will illustrate these contradictions with samples from FIPS 201

Example: Applicability

- e-passport: One size fits all
- FIPS 201: Carefully-considered list of usage scenarios with requirements, pros and cons of each scenario and usage type
    - E-passport type usage is explicitly disallowed, see previous slide

Do as I Say, Not as I Do (ctd)

Example: Data protection

- e-passport: “Maybe I am grasping at straws, but it would be great it we could say that [RFID] really doesn’t involve any additional risk”
- FIPS 201: “To ensure the privacy of applicants, departments and agencies shall do the following: […] employ an electromagnetically opaque sleeve or other technology to protect against any unauthorized contactless access to information stored on a PIV credential. Use of risk-mitigation techniques [like] high-assurance on-off switches for the wireless capability […] are permitted and encouraged

Do as I Say, Not as I Do (ctd)

Example: Impact assessment

- e-passport: Department of State PIA is a cursory two-page document that lacks any discussion of RFID and doesn't identify or address any RFID risks
- FIPS 201: Departments and agencies shall […] write, publish, and maintain a clear and comprehensive document listing the types of information that will be collected (e.g, transactional information, personal information in identifiable form [IIF]), the purpose of collection, what information may be disclosed to whom during the life of the credential, how the information will be protected, and the complete set of uses of the credential and related information at the department or agency. PIV applicants shall be provided full disclosure of the intended uses of the PIV credential and the related privacy implications

Do as I Say, Not as I Do (ctd)

At Defcon 17 in 2009, US government employees were horrified to learn that the RFID tags might have been scanned

- "It's supposed to be used by us, not by them!"

  This is why we're so adamant about making people aware [RFID in identity documents] is very dangerous. If you don't protect yourself, you're potentially exposing your entire [company or agency] to all sorts of risk

  — Brian Markus, Aries Security
- Agencies potentially exposed were FBI, Secret Service, National Security Agency, Department of Homeland Security, Defense Department, Treasury Department, U.S. Postal Inspection, and possibly further agencies who were there undercover

Act 2: Technology

RFID Passport Cloning

German passport tags were cloned shortly after they were released

- Lukas Grunwald simply implemented the comments in the ICAO passport specification

> Cloning Threats: Compared to paper based MRTDs copying the signed data stored on the RF-Chip is easily possible in general
>
> — "PKI for Machine Readable Travel Documents
> offering ICC Read-Only Access, Annex G:
> PKI and Security Threats, ICAO"

> Passive authentication […] does not prevent exact copying of the chip or chip substitution
>
> — ICAO Doc 9303

RFID Passport Cloning (ctd)

Belgian RFID passports had no security whatsoever for the first two years of issue

- Maybe they believed the US State Department when they said it wasn't necessary

  The passport data on the chip does not require encryption in order to be secure and protected

  — US Department of State, Public Notice 5208

- The attackers probably didn't read this notice though

  They demonstrated that it is possible to read the content of a first generation passport at a distance and in a few seconds without the owner's notice

  — "Belgian Biometric Passport does not get a pass…"

RFID Passport Cloning (ctd)

Later, basic security was added, but it proved little more than a speedbump

> Belgian passport, recipient of Interpol "World's most secure passport" award in 2003, provides the worst key entropy one has ever seen [...] two thirds of Belgian ePassports do not implement any data protection mechanism

— "ePassport: Securing International Contacts with Contactless Chips"

RFID Passport Cloning (ctd)

Even worse, the Belgian passport included additional unnecessary information like digitised owner signatures

- Nowhere in the ICAO specification does it require this
  - (Although they do define a data format for it… hmm)

Users have no way to tell what ends up in these things

> Before modifying the definition of 'electronic passport' to add a new or additional biometric identifier other than a digitized photograph, we will seek public comment through a new rule making process
>
> — US Department of State, Public Notice 5208

- ... and as before totally ignore any comments we receive

RFID Passport Cloning (ctd)

UK passport tags were cloned not long afterwards

> The most secure passport ever
>
> — UK Home Office before the cloning
>
> Being able to copy this does not mean that the passport can be forged
>
> — UK Home Office after the cloning
>
> This doesn't matter. By the time you have accessed the information on the chip, you have already seen it on the passport
>
> — Another UK Home Office spokesperson

If the presence of the tag is irrelevant anyway then why the enormous push to put them in there in the first place?

RFID Passport Cloning (ctd)

> The security around the UK passport chip prevents anyone changing or deleting any of the data or information on the chip, which is what is required to successfully forge a passport
>
> — UK Home Office spokesman

- Making an infinite number of absolutely perfect copies isn't a problem, as long as you can't replace the queen's portrait with a picture of Ozzy Osbourne

RFID Passport Remote Reading

Passport can be read and cloned as it goes through the mail

- Attack was demonstrated on a (volunteer) "victim" by the UK Daily Mail newspaper

> A shocking security gap allows the personal details and photograph in any electronic passport to be copied from the outside of the envelope in which it is delivered to homes. The passport holder is none the wiser when it arrives because the white envelope has not been tampered with or opened
>
> — Daily Mail

> All we can do is keep changing the design. We are going to change [the technology] more frequently than every 10 years. Our plan is to keep ahead of the forgers with a faster rate
>
> — Bernard Heridan, head of UK Passport Service

RFID Passport Remote Reading (ctd)

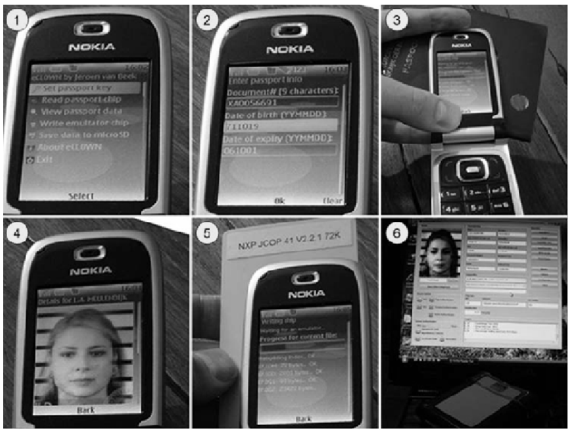
Electronically-read information is sufficient for identity theft in the UK

- Many UK banks, including the Post Office, no longer require an original passport but only a copy of the passport information

> By the end of the afternoon we had stolen enough information from the passport's electronic chip to be able to clone an identical document if we had wished. We had the details which would allow a fraudster or illegal immigrant to set up a new life in Britain. The criminal could open a bank account, claim state benefits and undertake a myriad financial and legal transactions in someone else's name
>
> — Daily Mail

RFID Passport Remote Reading (ctd)

The ePassport can even be cloned using a nothing more than a cellphone (!!)



Source: http://www.dexlab.nl

RFID Passport Remote Reading (ctd)

There doesn't seem to be any mechanism for revoking compromised passports…

19 January 2010: Hamas official Mahmoud al-Mabhouh is assassinated in Debai

- Assassins use fraudulently-obtained European and Australian passports
  - (Those would be the high-security ones for which this sort of thing can't ever happen)
- Shock, horror!
- News media publish the gory details

RFID Passport Remote Reading (ctd)

26 February 2010:

- Journalists have no problems opening bank accounts using the published information on the passports for authentication

> ITNews is waiting for comment from the Department of Foreign Affairs and Trade [Australian passport-issuing agency]
>
> — "Banks accept Dubai assassins' stolen IDs"

When you market a system as "the most secure ever":

- You need to invest in more than just marketing
- People will believe the hype and start relying on it
  - To the detriment of other security measures

RFID Passport Remote Reading (ctd)

Nasty catch-22 situation

- “Secure” = “has a chip in it”
- This says nothing about the infrastructure around it, which is what attackers will be targeting

But…

- People see “most secure” and assume that they can rely on it
- See “automation bias”

RFID Passport Remote Reading (ctd)

Problem isn’t limited to passports…

No-swipe credit cards can also be read remotely

- Through the mailer when it’s delivered
- From the wallet in your pocket

  Mr. Heydt-Benjamin was able to purchase electronic equipment online using a number skimmed from a card he ordered for himself and which was sealed in an envelope

  — New York Times

RFID Passport Remote Reading (ctd)

Card skimming using cell phones was demonstrated live at KiwiCon 2011

- Also independently done by a group at Royal Holloway in London

Using a cellphone in a MITM isn't even suspicious

- NFC phones are meant to be used as RFID cards

RFID Passport Remote Reading (ctd)

Cards appear to have no actual security

> American Express said its cards incorporate "128-bit encryption" and J. P. Morgan Chase said its cards use "the highest level of encryption allowed by the U.S. government". But tests on 20 cards from Visa, MasterCard and American Express found the cardholder's name and other data was being transmitted without encryption and in plain text
>
> — New York Times

> Personally-identifying information (PII) is broadcast in cleartext by every RFID-enabled credit card we have examined
>
> — "Vulnerabilities in First-generation RFID-enabled Credit Cards"

UK Chip-and-Pin cards are just as bad in terms of remote readability of credit card details

RFID Passport Remote Reading (ctd)

The same problems have been found in a range of other RFID tokens

- German airport security-zone access cards could be easily cloned

  We were shocked to discover that there were no security measures in place to prevent cloning
  — Der Spiegel (translated)

- Cloning an access card could be done while standing next to an airport employee on an escalator

  Upgrading 15,000 access cards and 500 readers was ruled out due to cost issues
  — Der Spiegel (translated)

RFID Passport Remote Reading (ctd)

Vendors claiming security measures that don’t actually exist is very common with RFID and biometrics technology

> Although RFID-enabled credit cards are widely reported to use sophisticated cryptography […] all the cards are susceptible to live relay attacks, all the cards are susceptible to disclosure of personal information, and all the cards are susceptible to various types of replay attacks
> — “Vulnerabilities in First-generation RFID-enabled Credit Cards”

RFID Passport Remote Reading (ctd)

Problem appears because the vendors took the easy way out in making the compatible with mag stripe cards

- Send ISO 7813 track 1+2 data to the reader as if it was a mag stripe read

  > The full cardholder name and card expiration date were present in cleartext in all transactions
  >
  > — "Vulnerabilities in First-generation RFID-enabled Credit Cards"

  - "It's the same info that's in the mag stripe, what's the problem?"
  - The exact same flawed reasoning was used with e-passports

RFID Passport Remote Reading (ctd)

Skimming was done with a standard commercial reader

> All of the RFID cards responded to our emulator exactly as they respond to a commercial RFID credit card reader
>
> — "Vulnerabilities in First-generation RFID-enabled Credit Cards"

RFID Passport Remote Reading (ctd)

Mythbusters were planning to devote an episode to RFID credit-card security flaws

> Linda and Tory get on the phone and Texas Instruments [RFID manufacturers] comes on along with chief legal counsel for American Express, Visa, Discover, and everybody else. And I get chills just as I describe it.… They […] absolutely made it really clear to Discovery that they were not going to air this episode talking about how hackable this stuff was, and Discovery backed way down. Tory still gets a little white when he describes that phone conversation
>
> — Adam Savage, Mythbusters

- Details of the story were later amended (only one legal counsel present, rest were managers; company was Mythbusters' own 'Beyond Productions' and not Discovery)

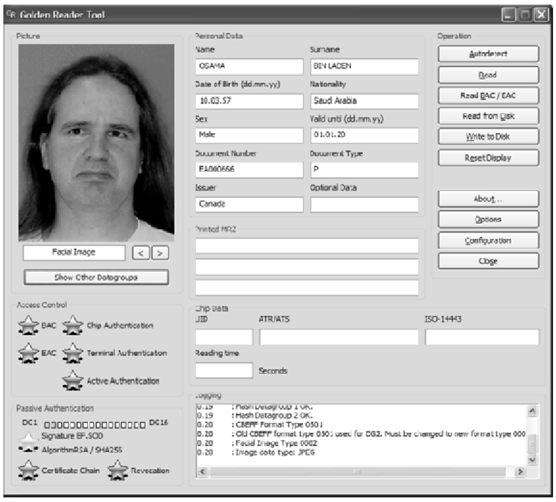
RFID Passport Remote Reading (ctd)

Issuers insist that this isn't a security problem

> Would you be comfortable wearing your name, your credit card number, and your card expiration date on your T-shirt?
>
> — New York Times

RFID Passport Remote Reading (ctd)

OK, so they can copy it but at least they can't forge it…



Personal Data

Name: OSAMA

Surname: BIN LADEN

Date of Birth (dd.mm.yy): 10.03.57

Nationality: Saudi Arabia

Sex: Male

Valid until (dd.mm.yy): 01.01.20

Document Number: EA000666

Document Type: P

Issuer: Canada

Optional Data:

Printed MRZ

Chip Data

UID

ATR/ATS

ISO-14443

Reading time

Seconds

AlgorithmRSA / SHA256

Logging

```
0.19     : Hash Datagroup 1 OK.
0.19     : Hash Datagroup 2 OK.
0.20     : CBEFF Format Type 0501
0.20     : Old CBEFF format type 0501 used for DG2. Must be changed to new format type 000
0.20     : Facial Image Type 0002
0.20     : Image data type: JPEG
```

Phew, that's a relief!

RFID Passport Remote Reading (ctd)

July 2008: Thieves steal 3,000 blank UK passports worth £2.5 million on the black market

- The RFID tags in the passports were unprogrammed and unlocked (!!)

August 2008: Dutch researcher Jeroen van Beek demonstrates "Elvis bin Laden" passport at Black Hat '08

- Bogus "passport" is accepted as genuine by the reference Golden Reader Tool, which doesn't check the PKD

RFID Passport Remote Reading (ctd)

In fact almost nothing checks the PKD

- Of 183 ICAO members only nine are PKD members and a grand total of five actually use it

Some countries (e.g. Germany) explicitly refuse to participate in the PKD

> Notably absent is at least one major passport issuer, Germany, where officials said they have concerns about how the directory service will distribute the certificates. They also have expressed some worries about its security. Some other countries also have balked at taking part, leading to questions of how many nations ultimately will join the database
>
> — "Germany Balks At Joining E-passport Key Directory"
> CardTechology

RFID Passport Remote Reading (ctd)

> You have to store a huge number of preverified (certificates) securely in your inspection systems. Imagine what happens if someone manages to add his own (certificate). Even worse, there's the idea that all information taken from the directory already is preverified, and, therefore, receiving states do not have to verify the (certificates). That's a real security nightmare
>
> — Dennis Kügler, BSI

RFID Passport Remote Reading (ctd)

The PKD also has an offline mode

> It is RECOMMENDED that the Signer Certificate required to validate the Document Security Object be also included in the Document Security Object itself. Receiving States SHOULD make use of a provided Signer Certificate
>
> — ICAO Doc 9303

- In the security field this is known as the “asking the drunk if he’s drunk” problem

RFID Passport Remote Reading (ctd)

UK home office reaction to the blank passport theft was almost comical

> The passport services said the stolen documents could not be used because of their hi-tech embedded chip security features
>
> — BBC News

> The Foreign Office […] said that the passports could not be used by the robbers because each contained a chip security system
>
> — Daily Telegraph

> The online information security discussion groups burst into laughter at yet another minister making statements of certainty about the impossibility of cracking a government system
>
> — UK Times

RFID Passport Remote Reading (ctd)

Of course the UK didn't actually check the RFID chip in the passport!

- It does make for a great red herring for the papers though
- Much discussion in news reports of various security issues… for a device that UK immigration neglected to check at the time

UK immigation did start checking the chips not long afterwards…

- … but your fake UK passport is still perfectly valid in almost every other country, which won't check the chips

RFID Passport Remote Reading (ctd)

Given the carefully-planned nature of the theft, it's fairly likely the crooks know exactly what "security" measures they were up against

- An "unusable" stolen document (UK Foreign Office) isn't worth £2.5 million

RFID Passport Remote Reading (ctd)

Some of the US responses to the passport manipulation were a lot more interesting than the UK reactions

Another LOSS in the war on terror. If this [pointing out that the “security” technology isn’t secure] isn’t a capital crime it should be. When we find out who these people are, just kill them. Done. Finito, end of problem. Just like a f***ing cockroach

– (Thankyou, Fox news)

Let me guess - The software was written by an INDIAN computer programmer!!!! America corporations have been laying off American engineers and replacing them with dirt cheap Indian and Chinese workers who, in turn, program in back doors and otherwise sell the technology to anyone with the money

... continues...

RFID Passport Remote Reading (ctd)

... continued...

ARE WE THAT BLIND THAT WE CANT SEE WHAT IS ENGAGING HERE. A SO CALLED ONE WORLD NATION. IF ANYONE READS THEIR BIBLE, IT IS ALL SUPPOSE TO HAPPEN. THE IDENTITY MARK, THE COLLAPSE OF ECONOMYS,ETC. ETC. PEOPLE PLEASE WAKEUP AND WHILE THERE IS STILL TIME. REPENT AND DO WHAT GOD SAYS

— Reader responses to a Washington Post article

Although others were more realistic

Look, you idiots, you can’t throw a perfectly good security system away just because it doesn’t work!! Think of all the investment in it! Think of the job losses!

RFID Passport Remote Reading (ctd)

UK national ID card, using the same technology as passports, is just as (in-)secure as the passport

> It is the same technology. We’re not running two different systems. It is just the facade that is different
> — UK Home Office spokesman

As with the passport security checks, the ID card checks seemed to be nonexistent in practice

- Journalist posed as a businessman wanting to verify an ID card
- Was told to call the UK Border Agency Card Verification Helpline
- After 19 minutes on hold was told to ask for ‘a second proof of identity’ from the card holder

RFID Passport Remote Reading (ctd)

Adam Laurie copied information from a UK foreign ID card (as proxy for the not-yet-issued national ID card) using his cellphone

- Changed the details read from the ID and wrote them to a new, blank ID
- Added a message “I am a terrorist – shoot on sight”

> And all of this has been done in such a way as to fool the electronic readers intended to check the ID card’s authenticity. It is, quite simply, a terrifying achievement
> — Daily Mail

RFID Passport Remote Reading (ctd)

UK Home Office reaction was the usual one

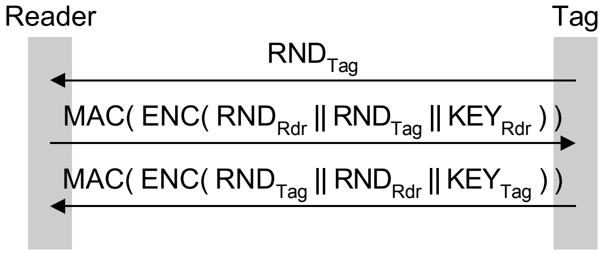
> We are satisfied the personal data on the chip cannot be changed or modified and there is no evidence this has happened

- Of course the original data wasn't changed, why would you want to when you can create an infinite number of perfect forgeries?
- Pay no attention to the perfect forgery behind the curtain

> My real concern is that if someone falls victim to an identity theft of the type we have demonstrated it is going to be very hard for them to prove their innocence if that forged card is subsequently used to commit a crime. After all, the Government claims that the technology is foolproof
>
> — Ian Angell, London School of Economics

RFID Passport Security Problems

After complaints about security issues, the passport standard added a basic access control (BAC) mechanism


Reader
Tag
RND_{Tag}
$MAC(ENC(RND_{Rdr} || RND_{Tag} || KEY_{Rdr}))$
$MAC(ENC(RND_{Tag} || RND_{Rdr} || KEY_{Tag}))$

$3DES\_shared\_key = KEY_{Rdr} \wedge KEY_{Tag}$

RFID Passport Security Problems

Straightforward challenge-response auth using a shared key

> As if we were still in the 1980s […] BAC is a poor key agreement protocol because it isn't even immune to passive adversaries
>
> — "E-Passport Threats"

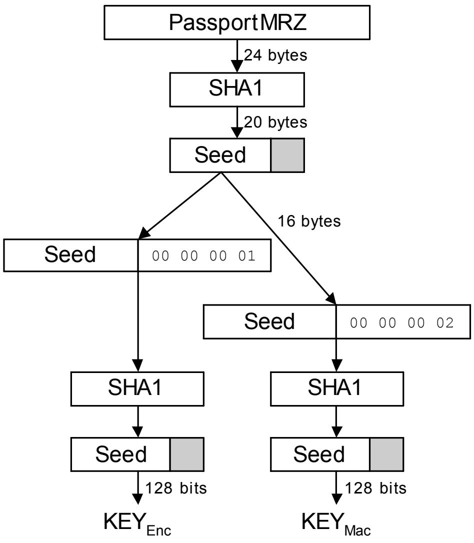
- You're allowed as many guesses as you like

> The PIV card shall include mechanisms to limit the number of guesses ad adversary can attempt if a card is lost or stolen
>
> — FIPS PUB 201-1

RFID Passport Security Problems (ctd)

Shared key is derived from the passport's machine-readable zone (MRZ)

- Obtained by the reader through reading the text on the passport cover page
- Pre-generated keys are stored in the tag



RFID Passport Security Problems (ctd)

In one stroke this has completely defeated the whole point of using RFID

> Claims of increased efficiency at Points of Entry disappeared as security improvements necessitated visual scans of the passport's data page in order to implement BAC
>
> — "A Case Study of the Security and Privacy Risks of the US e-Passport"

> The new type of passport has added to the checking delays
>
> — Bernard Herdan, UK Identity and Passport Service executive director

RFID Passport Security Problems (ctd)

"Never share your banking PIN with anyone. Never write it down"

- Passports do the equivalent of pre-printing the owner's PIN on their bank card

> RFID chips can be read at a short distance and tracked without their owner's knowledge, while the key to unlocking the passport's chip consists of details actually printed on the passport itself. It is almost like writing your pin number on the back of your cashpoint card
>
> — BBC

RFID Passport Security Problems (ctd)

MRZ is a non-secret "secret"

- Date of birth, date of expiry, passport number

Effective keyspace is *at most* 35 bits

That's the best-case…

- Germany: Keyspace 33.3 bits
- Netherlands: Keyspace 32.2 bits

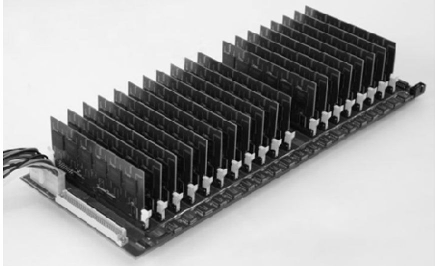
This is 200+ times weaker than the US's "exportable" encryption from the 1990s

- It's ~15 million times weaker than the DES keys that were ruled by European courts to be insecure… in 1998

RFID Passport Security Problems (ctd)

COPACOBANA project looked at time to break BAC security using their low-cost FPGA crypto breaker

- German passport: 22 seconds
- Dutch passport: 10.3 seconds
- The commercial RIVYERA S3-5000 version is around ten times faster than the original COPACOBANA



Source: www.copacobana.org

Many countries don't use even this basic level of access control

RFID Passport Security Problems (ctd)

> The proximity chip technology utilized in the electronic passport is designed to be read with chip readers at ports of entry only when the document is placed within inches of such readers
>
> — US Department of State, Public Notice 5208

Attack demonstration at Cards Asia conference in Singapore (“ePassport Privacy Attack”, Harko Robroch)

- Intercepted passport ↔ reader communications from 5m away
  - Eavesdropping on terminal was possible from 25m away
- Brute-forced the key to recover Dutch passport data

RFID Passport Security Problems (ctd)

Attack demonstration at BlackHat 2005 conference (“Long Range RFID and its Security Implications” Kevin Mahaffey)

- Read RFID tags from 50 feet away via a high-gain antenna
- Even longer distances are possible, but their demo was limited by the room size

Gerhard Hancke intercepted tag communication over 4m distance using standard off-the-shelf gear (Philips MF RC530 reader combined with Dynamic Sciences R-1250 receiver)

Another researcher read a tag from 25m away using a 4W reader

RFID Passport Security Problems (ctd)

It’s a good thing the long-range readers don’t know that they’re not permitted to do this!

> The ISO 14443 RFID specification permits chips to be read when the electronic passport is placed within approximately ten centimeters of the reader
>
> — US Department of State, Public Notice 5208

These attacks also work for other “range-limited” wireless technology

- In August 2004 the trifinite team performed a Bluetooth snarfing attack over 1.8km
- Supposed maximum range of Bluetooth is 10m

RFID Passport Security Problems (ctd)

The US Government’s own ID standard specifically forbids this mode of operation

> The two electronic fingerprints stored on the card shall be accessible only over the contact interface and after the presentation of a valid PIN. No contactless access is permitted for the biometric data specified to be stored on the PIV Card under this standard
>
> — FIPS PUB 201-1

Even the biometric vendors requested that RFID access not be allowed

> For privacy reasons contactless transmission of PINs and biometrics is not supported
>
> — Requested change to FIPS 201 from Biometric Associates Inc

RFID Passport Security Problems (ctd)

Passport RFID uses a 32-bit anti-collision value as part of its initial handshake

- Publicly broadcast before any access control is applied
- Needed at the RFID boot stage (c.f. ARP) it so can’t be secured

RFID Passport Security Problems (ctd)

ISO 14443 specifies that for privacy protection this should be a random value starting with the byte `08`

- Some countries (e.g. Italy, NZ) use a constant value for each tag → trivial passport tracking that bypasses any security measures
- Some countries (e.g. Australia) argue that the `08` byte identifies a passport RFID tag, so use a totally random value → identifies an Australian passport holder

> It will not permit ‘tracking’ of individuals
>
> — US Department of State, Public Notice 5208

– See “Background on Biometric Passports”, Privacy International, for background info on this

RFID Passport Security Problems (ctd)

Even with a random UID, citizen tracking by governments is still possible

> We present a distributed hardware architecture that can continuously read and record RF based communication at public places [...] one is able to trace any individual similar to tracing packages sent using postal services such as UPS
>
> — “E-Passport: The Global Traceability Or
> How to Feel Like a UPS Package”

- Should be tracked by TNT, then no-one would know where you are
  - (TNT were the company that lost the UK taxpayer records)

RFID Passport Security Problems (ctd)

Countries also identify the passport origin in the ATR

- ISO 7816 historic bytes contain ID strings
- NZ passport contains the manufacturer ID in the ATR

All countries’ passports can be uniquely fingerprinted using variations in the protocol implementation

> This turns out to be surprisingly easy to do. We were able to distinguish all passports that we tested
>
> — “Fingerprinting Passports”

Even below this level, fingerprinting at the physical layer is possible (demonstrated in controlled environments)

- Works independent of all higher-layer protocols and security mechanisms

RFID Passport Security Problems (ctd)

Only the US uses a metallic shield for its passports

- Hastily added after a public outcry

To distinguish US vs. non-US passports

```
if( good signal response )
  non-US passport holder;
elseif( weak signal response )
  US passport holder;
```

RFID Passport Security Problems (ctd)

Chris Paget demonstrated reading 125kHz prox tags right through several types of shielding at Black Hat'07

- All you need to do is increase the power

> Holders [should] keep their MRTD in a metal jacket when not in use. This will completely prevent unauthorized reading
>
> — Use of Contactless Integrated Circuits In
> Machine Readable Travel Documents

RFID Passport Security Problems (ctd)

HF tags can also be read through shielding

- Typical passport shielding bags provide about 7-8dB of attenuation
  - (Some vendors claim 80dB or more of attenuation; they're confusing a cloth bag using metallised threads with a faraday cage)
- Increasing reader power or providing extra antenna gain easily overcomes this

RFID Passport Security Problems (ctd)

Riddle: What do you get when you place a metallic reflector behind an active element?

RFID Passport Security Problems (ctd)

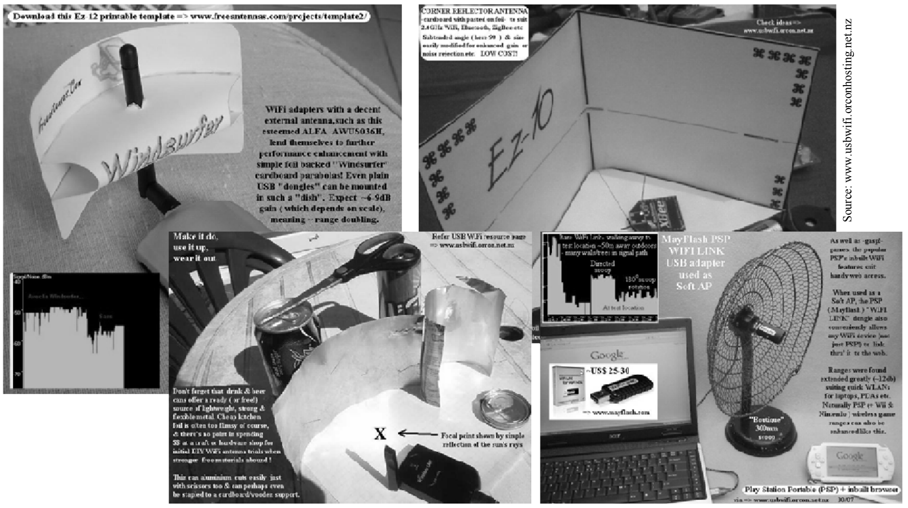
Riddle: What do you get when you place a metallic reflector (the shield) behind an active element (the tag)?

Answer: That’s right, you get a *dish antenna*

- Opening the passport even a tiny amount can make things worse than with no shield at all

RFID Passport Security Problems (ctd)

This is a standard trick used with cheap wireless gear to extend the range



Download this Ez-12 printable template => www.freeantennas.com/projects/template2/

WiFi adapters with a decent external antenna,such as this esteemed ALFA AWUS036H, lend themselves to further performance enhancement with simple foil backed "Windsurfer" cardboard parabolas! Even plain USB "dongles" can be mounted in such a "dish". Expect ~6-9dB gain (which depends on scale), meaning ~ range doubling.

CORNER REFLECTOR ANTENNA -cardboard with pasted on foil- to suit 2.4GHz WiFi, Bluetooth, ZigBee etc Subtended angle (here 90) & size easily modified for enhanced gain or noise rejection etc. LOW COST!

Check ideas=> www.usbwifi.orcon.net.nz

Make it do, use it up, wear it out

Refer USB WiFi resource page => www.usbwifi.orcon.net.nz

Don't forget that drink & beer cans offer a ready (or free!) source of lightweight, strong & flexible metal. Cheap kitchen foil is often too flimsy of course, & there's no point in spending $$ at a craft or hardware shop for initial DIY WiFi antenna trials when stronger Eco materials abound !

This can aluminium cuts easily just with scissors too & can perhaps even be stapled to a cardboard/wooden support.

X ← Focal point shown by simple reflection of the sun's rays

Bare WiFi Link walking away to test location ~50m away outdoors - many walls/trees in signal path

MayFlash PSP WIFI LINK USB adapter used as Soft AP

As well as -gasp- games, the popular PSP's inbuilt WiFi features suit handy web access.

When used as a Soft AP, the PSP (Mayflash) "WIFI LINK" dongle also conveniently allows any WiFi device (not just PSP) to link thru' it to the web.

Ranges were found extended greatly (~12db) suiting quick WLANs for laptops, PDAs etc. Naturally PSP (+ Wii & Nintendo) wireless game ranges can also be enhanced like this.

Play Station Portable (PSP) + inbuilt browser

via => www.usbwifi.orcon.net.nz 30/07

Source: www.usbwifi.orconhosting.net.nz

RFID Passport Security Problems (ctd)

Use the tag to attack the reader

- Use SQL injection from the RFID tag to open any door

Attack demonstrated by Joshua Perrymon, PacketFocus Security Solution

> It doesn't really matter who the vendor is… In any building you go with this, bang, you gain access

Use the tag to crash the access control system

> Grunwald found that by manipulating data on the RFID chip he could crash the system, opening the way for a thief to break into the building
>
> — "Fingerprinting Passports"

Use a blocking tag to DoS all readers in range

RFID Passport Security Problems (ctd)

Use the tag contents to attack the reader

- Modify the tag data to exploit flaws in readers

Lukas Grunwald modified the passport's JPEG2000 image to exploit buffer overflows in passport readers

> They could be vulnerable to a code-injection exploit that might reprogram a reader to approve expired or forged passports
>
> — Wired

RFID Passport Security Problems (ctd)

A fake chip doesn’t have to be inside the passport (Hlavác and Rosa)

- Disable the chip in the passport through standard means, e.g. EMP

Response comes from a second chip in the vicinity of the passport, e.g. in the user’s pocket, wallet, or handbag

RFID Passport Security Problems (ctd)

Reader broadcasts a request for a passport

- Whatever replies first is treated as the passport

The problem with multiple RFID devices was known long before the e-passport was introduced

> Radio signal and data confusion would occur when a passport holder held multiple visas stored in RFID chips, which would create insurmountable problems for the reader
>
> — “EU-Pläne zu Biometrie-Visas stecken in Sackgasse” (translated)

RFID Passport Security Problems (ctd)

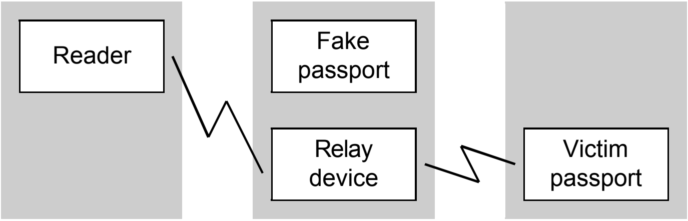
RFID decouples the passport from the authentication channel

> The Department of State did not adequately consider how adding an RF transponder to the passport transformed it from an inert identification document to a remotely readable technological artifact
>
> — “A Case Study of the Security and Privacy Risks of the US e-Passport”

> When reviewing the [FOIA’d] documents one notable omission is the lack of analysis of the security and privacy aspects of e-Passport project from the perspective of its intended users
>
> — “A Case Study of the Security and Privacy Risks of the US e-Passport”

RFID Passport Security Problems (ctd)

Use of this disconnected authentication channel greatly eases fake passport use



- To the customs officer, they’re seeing a real passport belonging to the victim

RFID Passport Security Problems (ctd)

Attack was demonstrated by student using homebrew gear

To demonstrate that it is not difficult to build the system locally to carry out the Mafia fraud attack on RFID

— "RFID Insecurity for Entity Authentication"

– ("mafia fraud" is the cryptographers term for this type of attack)

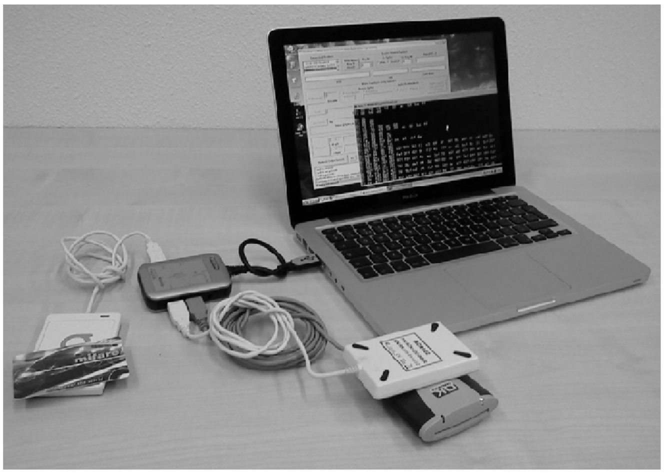
– (Attack was on an ISO 14443 crypto card using BAC-type authentication as the passport card does)

Other attacks are also enabled through this decoupling

- Gerhard Hancke demonstrated a MITM attack on the Mifare card with on-the-fly modification of data using a reprogrammed commercial reader

RFID Passport Security Problems (ctd)

Other groups have also done this using basic off-the-shelf gear



Source: www.libnfc.org

RFID Passport Security Problems (ctd)

Totally unnecessary use of RFID actually *enables* relay attacks

> It is, therefore, a bit surprising to meet an implementation that actually encourages rather than eliminates these attacks
>
> — "A Note on the Relay Attacks on e-passports:
> The Case of Czech e-passports"

> Our attack is only possible because the e-passports contain an RFID tag. If e-passports used a contact based smart card then such attacks would not be possible
>
> — "A Tracebility Attack against e-Passports"

This is the worst of both worlds

- BAC still requires physical scanning of the passport
  - Nothing has changed from pre-RFID passports
- RFID allows easy forgery/relay attacks

RFID Passport Security Problems (ctd)

The only thing that the RFID adds is security vulnerabilities!

> "Nearly every country issuing this passport has a few security experts who are yelling at the top of their lungs and trying to shout out: 'This is not secure. This is not a good idea to use this technology'"
>
> — BBC

> Comparing a MRTD that is equipped with a contactless chip with a traditional MRTD shows two differences
>
> – The data stored in the chip can be electronically read without opening the document (skimming)
>
> – The unencrypted communication between a chip and a reader can be eavesdropped within a distance of several metres
>
> — ICAO Doc 9303

RFID Passport Security Problems (ctd)

Protecting yourself: Countries

- Apply ICAO Doc 9303 section 7.1.1 paragraph 3

Protecting yourself: Individuals

- `https://events.ccc.de/congress/2005/static/r/f/i/RFID-Zapper(EN)_77f3.html`

RFID Cloning

Cloning of RFID tags is a geek sport…

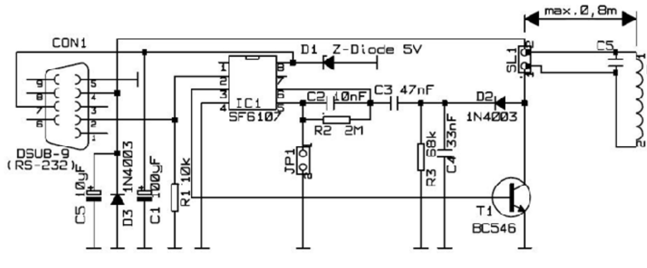
Remote-read and clone a key card for business premises (Jonathan Westhues)

Source: www.cq.cx/prox.pl

- Scratch-built the reader/cloner/tag emulator circuitry (!!)
  I always thought this might be a lousy security system
  — RFID access card test "victim" Van Bokkelen

RFID Cloning (ctd)

You don’t really need to scratch-build your own cloner though



Source: sfchip.de

- SF6107 RFID datalogger
  - Probably a custom-programmed AVR ATTiny
- Logs tags until its internal memory is full and plays them back over a serial/USB link

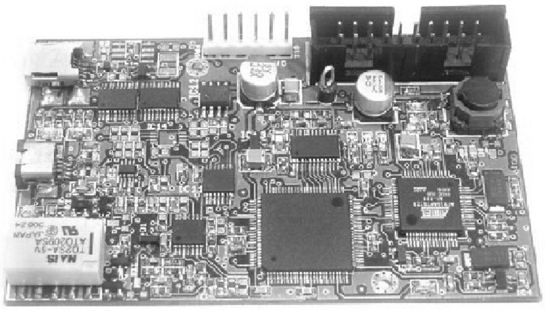
RFID Cloning (ctd)

Or you can just buy them commercially…

Source: xp2.ru

RFID Cloning (ctd)

Jonathan Westhues' proxmark3, the Rolls Royce of RFID tools



Source: cq.cx/proxmark3.pl

- DSP-based LF/HF universal RFID device with FPGA assist

RFID Cloning (ctd)

Implemented as software-defined radio (SDR) so goes beyond the capabilities of any standard reader to allow things like side-channel analysis/attack

- Sample config can read a TI 'glass transponder', read and clone a VeriChip, read and clone a Motorola FlexPass, read an ISO15693 tag, ...
- Nijmegen Mifare attacks were done using a proxmark3

Available in open-source form (Verilog, schematics, Gerbers, software, docs)

RFID Cloning (ctd)

Clone the ExxonMobil SpeedPass (Avi Rubin et al)

Clone the FasTrak road toll pass (Nate Lawson)

> It's trivial to clone a device. I have several clones with my own ID already
>
> — Nate Lawson

Clone a Trovan 'Unique' tag and use it to access a locked laptop (Adam Laurie)

Clone the tag for a cheap product into an expensive product to get it at the cheap-product price (Lukas Grunwald)

Clone a hotel-room door key into a tagged cream cheese packet, use the cheese to unlock doors (Lukas Grunwald)

RFID Cloning (ctd)

Clone VeriChip's human-implantable ID (Jonathan Westhues)

> This 'always-there' identification can't be lost, stolen, or duplicated
>
> — VeriChip

- Security = "the reader protocol is undocumented"

> The Verichip is a repurposed dog tag
>
> — "Demo: Cloning a Verichip"

- Specifically, it's a Trovan EM 4x05 / FDX-B
  - Off-the-shelf Q5 or Hitag2 smart tags can be programmed to emulate a EM 4x02's, EM 4x05's, and a number of other tags

RFID Cloning (ctd)

VeriChip's human-implantable tags have the same decoupling-from-the-physical-artefact problems as passports

> You could strap [the cloner] to your leg and somebody passing the VeriChip reader over your arm would pick up the ID. They'd never know they hadn't read it from your arm
> — Jonathan Westhues

RFID Cloning (ctd)

DHS is using this type of tag for border control security (!!)

- People Access Security Service (PASS) uses EPC Class 1 warehouse inventory-tracking tags for border security

  > Privacy and security experts are concerned that those who sign up for the cards are unaware of the risk: anyone with a readily available reader device — unscrupulous marketers, government agents, stalkers, thieves and just plain snoops — can also access the data on the licenses to remotely track people without their knowledge or consent
  > — Scientific American

  > The only information contained in the tag is a number that would be meaningless except to Homeland Security agents
  > — Ken Brown, DMV

  – A cloned tag could care less what its number means

RFID Cloning (ctd)

The publicly readable data in [Passport Cards and Electronic Drivers Licenses] can be straightforwardly cloned despite the implication of protection mechanisms in [DHS documents]

— “EPC RFID Tag Security Weakenesses and Defences”

Spoofing EPC tags is relatively straightforward

The device was able to successfully deceive the EPC reader and further to replace actual tag responses with a spoofed response

— “A Spoofing Attack Against an EPC Class One RFID System”

RFID Cloning (ctd)

As with many other RFID technologies (see the discussion of contactless credit cards, road toll passes, …), claimed security measures don’t appear to exist

In its Privacy Impart Assessment, the DHS highlights tag-specific IDs as a powerful tool for anti-counterfeiting [...] The Passport Cards and Electronic Drivers Licenses do not carry tag-specific IDs [...] but instead bear generic manufacturer codes

— “EPC RFID Tag Security Weakenesses and Defences”

RFID Cloning (ctd)

Even while it was still in the planning stages a trade association of ID-card manufacturers recommended that it be withdrawn

> NIST has, for the first time, endorsed a technology without exploring its use in the context of the government mission and presenting the pros and cons of that technology offering for that mission
>
> — Randy Vanderhof, Smard Card Alliance
> executive director

RFID Cloning (ctd)

Slide left blank for the “PASS security broken”
news stories that will appear presently
Please stay tuned

RFID Cloning (ctd)

More room for news stories about the
failure of the PASS system as soon
as it’s deployed

RFID Cloning (ctd)

First widely-publicised attack on PASS was by Chris Paget

- Drove past victims at 30 mph (50 kmh) cloning their IDs as he went
- Cards can be tracked and cloned up to a mile (1.5 km) away

> This is just simply the wrong technology
> — Chris Paget

Paget later made a video of himself wardriving, stealing identities from PASS card holders

http://www.youtube.com/watch?v=9isKnDiJNPk

RFID Cloning (ctd)

Germany was no better…

> Germany to roll out ID cards with embedded RFID
>
> The production of the RFID chips, an integral element of the new generation of German identity cards, has started [...] The new ID card will contain all personal data on the security chip that can be accessed over a wireless connection
>
> — International Business Times, 21 August 2010
>
> New government ID cards easily hacked
>
> […] They used the home scanning machines that will go along with the cards, and found that scammers would have few problems extracting personal information.
>
> Interior Minister Thomas de Maizière said he saw no immediate reason to act on the alleged security issue
>
> — The Local (Berlin English news), 24 August 2010

RFID Cloning (ctd)

Privacy concerns about the PASS IDs

- Act as electronic license plates
- Police can record who attends political rallies, protests, …
- Clone a political opponent's tag and leave it in a car parked outside a strip club

> Officials with the US Customs and Border Protection Department say they have no plans to overhaul the technology
>
> — The Register

RFID Cloning (ctd)

Chris Paget channels the Chaser

- Adopt a kitten from a homeless animal shelter
- Clone an entry card into the kitten's RFID tag
- "Break into the California Senate Building with a kitten. I'd like to see the DHS advisory that goes out for this"

Beware of Geeks bearing Kittens

RFID Cloning (ctd)

A real-world demo was carried out at the request of California Senator Joe Simitian

- Student wandered the corridors with a reader in a briefcase
- Cloned tags for nine senators

  The reader could send out any of those [senators'] numbers, getting him past any locked door a state senator would have access to. And he would appear as the senator in the electronic records

  — "California could become third state to ban forced microchip tag implants"

RFID Cloning (ctd)

Chris Paget, IOActive, was planning to demonstrate a single-chip RFID cloner at Black Hat 2007

- Built around a PIC16F628A
- Parts cost about $20 from any electronics store

Legal threads from RFID vendor HID blocked the talk

- (Frivolous) $10M lawsuit to prevent him from speaking
- HID spokesperson Kathleen Carroll said they knew that their products were insecure, but had no plans to fix them

> Carroll acknowledged that HID is aware that its RFID proximity cards are vulnerable to hacking attacks […] She did not say why the company has not fixed these well-known vulnerabilities
>
> — ZDNet Interview with HID

RFID Cloning (ctd)

In 2006 two of David Beckham’s BMW X5 SUVs were stolen by defeating the RFID keyless entry systems

$2 billion Dutch RFID transit card system was broken before it was even deployed (!!)

- OV-chipkaart system is based on Philips Mifare Classic (for reusable cards) or Mifare Ultralight (for disposable cards)

University of Amsterdam students demonstrated a card-reset attack in July 2007

- Mifare Ultralight doesn’t use any cryptography
- Attack resets the card to allow repeated re-use

RFID Cloning (ctd)

German CCC hackers recovered the homebrew crypto algorithm used in the Mifare Classic

Radboud University student demonstrated Mifare cloning on Dutch national television

Source: Blackbag, toool.nl

- (Ultralight was cloned, but either card is cloneable)
- Ghost device costs about €40 to build

RFID Cloning (ctd)

Full Mifare Classic (not Lite) key can be recovered in 3 minutes on a laptop given a single captured message (known IV)

> The security of this cipher is close to zero. This is particularly shocking, given the fact that, according to the Dutch press, 1 billion of MiFare Classic chips are used worldwide, including in many governmental security system
>
> — "Algebraic Attacks on the Crypto-1 Stream Cipher in MiFare Classic and Oyster Cards"

Some Mifare Lites can be cloned in as little as seconds

- (Older version of these slides said: Research on Mifare security is ongoing)

RFID Cloning (ctd)

Vendor recommended that people upgrade to Mifare DESFire's

- Uses 112/128-bit triple DES encryption

These lasted another three years, until 2011

- German researchers figured out how to extract the keys from the cards

Vendor recommended that people upgrade to Mifare DESFire EV1's

- Just use ~~Mifare Lite~~ ~~Mifare Classic~~ ~~Mifare DESFire~~ Mifare DESFire EV1… whatever!

RFID Cloning (ctd)

Used in London's Oyster Card, Netherlands OV-Chipcard, Boston CharlieCard, Christchurch MetroCard, …

> When an attacker eavesdrops communications [...] enable us to recover all keys used. We have successfully executed these attacks against real-world systems including the London Oyster Card and the Dutch OV-Chipkaart
>
> — "Dismantling MIFARE Classic"

> We need to understand how much our economy is vulnerable to sophisticated forms of electronic subversion where potentially one smart card developer can intentionally (or not), but quite easily in fact, compromise the security of governments, businesses and financial institutions worldwide
>
> — "The Dark Side of Security by Obscurity and Cloning
> MiFare Classic Rail and Building Passes
> Anywhere, Anytime"

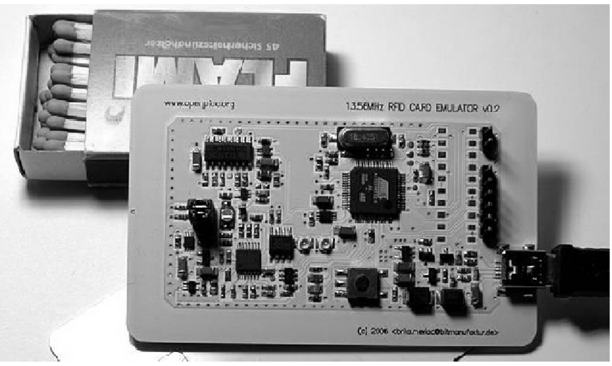
RFID Cloning (ctd)

As with passports, the travel cards also allow citizen tracking

- RFID-based transport in China (Shanghai Metro) and Singapore (SMRT) provide travel anonymity
- RFID-based transport in the UK (Oyster) provides complete travel trackability

RFID Cloning (ctd)

Tag emulators are freely available


www.openpicc.org
13.56MHz RFID CARD EMULATOR v0.2
(c) 2006 <brita.meriac@bitmanufaktur.de>

Source: openpcd.org

- Open-source circuit details, PCB layout, Gerber files
- Can also buy pre-built

RFID Cloning (ctd)

Existing technology can easily be repurposed

- Passport RFID technology is widely used in any number of other products

> The world of RFID is like the Internet in its early stages. Nobody thought about building security features into the Internet in advance, and now we're paying for it in viruses and other attacks. We're likely to see the same thing with RFIDs
>
> — Ari Juels, Research Manager, RSA Labs

> The company was an early adopter of RFID badges for employees. [The attacker] bought an RFID reader and went to a TGI Friday's favoured as an after-work hangout, where he surreptitiously swiped [remotely scanned] employee's badges. Then he bought blank RFID cards […] and made his own corporate ID
>
> — "Fatal System Error", Joseph Menn

RFID Cloning (ctd)

Related example: Street criminals were being arrested carrying a cornucopia of hotel room key cards, loyalty cards, gift cards, membership cards, …

- These were all skimmed credit cards
- Skimmers cost ~US$500, about the size of a USB thumb drive, store thousands of cards in a USB flash drive
- Skimming typically done at restaurants via the US practice of staff walking off with your card
- (Card scanners never checked for HiCo vs. standard cards)

Not-so-secret Secrets

Many (most) vendors never change the default keys set for RFID cards by the manufacturer

- Researchers built a dictionary of default keys collected from manufacturer web sites, manuals, data sheets, …

  I was really surprised we were able to open about 75 percent of all the cards we collected

  — Wired

Not-so-secret Secrets (ctd)

Library RFID tags are left unlocked (world-writeable) by default

> That's the recommended implementation of our tags. It makes it easier for libraries to change the data
>
> — Frank Mussche, Libramation

> Libramation has sold 5 million RFID tags in a "convenient" unlocked state
>
> — Wired

RFID Power Analysis

All power for RFID tags is provided wirelessly

> [RFID chip] cannot broadcast personal information because it does not have its own source of power
>
> — US Department of State, Public Notice 5208

- Side-channel attack information is broadcast to everyone within range!

RFID Power Analysis (ctd)

With standard side-channel attacks you at least need physical access to the device

- RFID power analysis attacks can be done remotely and purely passively

> As a proof of concept, we use power analysis to extract the [32-bit] kill passwords from Class 1 EPC tags. Tags from several major vendors were successfully attacked
>
> — "Remote Power Analysis of RFID Tags"

RFID Power Analysis (ctd)

We’ve barely scratched the surface of all the attacks that this makes possible

- e-passport active authentication in particular will open up a veritable cornucopia of attacks on card private keys
- These things use power consumption (load modulation) as their communications mechanism… ugh

ICAO spec requires that country signing keys (which are only ever used in highly secure environments) be protected from side-channel attacks

- Passport keys (which broadcast their operations in public) don’t have to be protected

RFID Passports as Terrorism Enablers

Worst-case RFID-enabled passport scenario: Targeted remote assassination

- Scatter RFID-triggered explosive charges around popular tourist destinations

  Mines and booby-traps will soon also be able to read out remotely the victim's name, age, height, sex and nationality right before triggering

  — Markus Kuhn, Cambridge University

  Smart bombs: The device only goes off it a person of sufficient rank is in range

  — Adam Laurie

RFID Passports as Terrorism Enablers (ctd)

Triggered by sensing e.g. a US passport

> The majority of the comments [about introduction of e-passports in the US] were concerned that terrorists could identify and target them as U.S. citizens
>
> — US Department of State, Public Notice 5208

- One study on remote RFID sensing actually used a (small, non-lethal) explosive charge concealed in a rubbish bin to demonstrate this

> The current [US passport] design caused the charge to detonate
>
> — "RFID Passport Shield Failure Demonstration: Video Security Brief"

`http://www.youtube.com/watch?v=-XXaqraF7pI`

RFID Passports as Terrorism Enablers (ctd)

Even those passports with an attempt at shielding are vulnerable

- Opening the passport as little as 5mm makes the shield useless
  - Quite likely to happen in a bag or pocket
  - Slip your boarding pass and travel documents into your passport and the shielding effect is gone

Near field/far field effect means that the tag can probably be read even if the shielded passport cover is completely closed

- Need to pass through a loop antenna in a door frame

Increase reader power/antenna gain to sidestep shielding

RFID Passports as Terrorism Enablers (ctd)

Even if it doesn’t work (the attacker has to use a human to manually detonate it), finding RFID reader components among the debris will be enough

Counterargument: There are easier ways to detonate a bomb

- This isn’t about detonating bombs, it’s about a worldwide denial of service on all passports, travel, tourism, and immigration/customs checks

RFID Passports as Terrorism Enablers (ctd)

After a few explosions, no-one will want to carry a US passport any more

No-one will want to associate with US passport holders

- Target particular individuals
  - Government officials
  - Military personnel
  - …

You can never be sure that you’ve found all of the devices

RFID Passports as Terrorism Enablers (ctd)

> Governments have forced their citizens to adopt new international MRTDs which dramatically decrease security and privacy and increase the risk of identity theft. Put simply, the current implementation of the [ICAO] passport system uses technologies and standards that are poorly conceived for its purpose.
>
> A complete re-evaluation and re-design of the technical solutions currently adopted for MRTDs, especially RFID and biometrics, should be performed. It should be considered whether these technologies are actually necessary
>
> — Budapest Declaration on Machine Readable Travel Documents (MRTDs)

Act 3: Practice

Practical Problems with Biometrics

Biometric systems have never had to withstand serious attack

- Smart cards took 15 years of criminals walking all over them before vendors started taking security seriously

Practical Problems with Biometrics (ctd)

Fingerprint scanners work poorly with the elderly, manual workers, children

- Children haven’t developed strong fingerprints yet
- Manual workers and the elderly don’t have strong fingerprints left
- German passport enrolment system ran into problems with people as “old” as 40 or 50
  - 10% of senior citizens can’t be reliably enrolled

> No one seems to be doing fundamental research on whether the physical or behavioural characteristics such technologies seek to measure are truly reliable, and how they change with age, disease, stress and other factors
>
> — The Economist

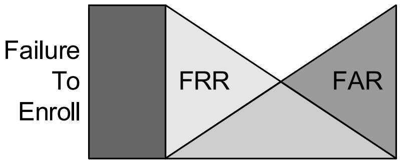
Practical Problems with Biometrics (ctd)

Children are particularly problematic

> It is virtually impossible to obtain fingerprints from children aged under 4 years [...] children who suck their thumbs a lot the skin of the finger is very soft, and it is often impossible to take a good print [...] children are crying or fidgety, so it is impossible to get them to look straight into the camera [for facial scans] for long enough [...] is unlikely that facial recognition software will be able to compensate for the effects on growth in children's faces [...] young children may be unwilling or unable to cooperate with a facial scan, causing delays
>
> — Evaluation Report, Biometrics Trial 2b or not 2b,
> Dutch Ministry of the Interior

Practical Problems with Biometrics (ctd)

Established wisdom: 3-4% of the population (goats) have unstable biometric traits that can't be identified by sensors



In practice FTE rate is often much, much higher

- Up to 50% reject rate, see later slides
- (Several other Fxyz's, too many to cover here)

Practical Problems with Biometrics (ctd)

Attack: Train the system to accept less and less reliable images

- Has happened (inadvertently) in real-world deployments as sensors were subject to wear and tear
- System would accept anything (elbow, nose) as a valid print

People forget which finger they enrolled with and try each one in turn

- Alternatively, a failure to verify the chosen print would lead to them trying all other fingers just in case
- (Happens to a lesser extent with passwords as well)

Fingerprint readers have problems with outdoor use, e.g. in winter cold

Practical Problems with Biometrics (ctd)

FARs for mass-market fingerprint readers are already wound sky-high to avoid consumer acceptance problems

- Need to wind the FAR up to the point where FRR = 0

> The readers will have a fairly broad tolerance on the basis that products that stop people using their own cars, computers or whatever because their fingers are a bit sweaty won’t turn out to be very popular
>
> — John Lettice, The Register

Practical Problems with Biometrics (ctd)

Example: Government ID card initiative found excessively high FTE/FRR

- At the rate that people were being processed it would have taken years to deal with everyone
- Wound the threshold down to a point at which things were acceptable
- Later found that an enrolment carried out during that period would match any other enrolment
  - Threshold had been set so low that now everyone matched

Practical Problems with Biometrics (ctd)

In a stack of forty-six biometrics vendor brochures, a total of two actually mention security performance

- Both from German vendors, give figures for FAR and FRR
- Pages and pages of information on things like power draw, operating temperature range, MTBF, …, but absolutely nothing about how secure the security device actually is
- ICAO passport spec (Doc 9303) defines FAR/FRR/FTE/FTAcquire and many others but then never mentions them again

Compare this with standard security products with endless claims about security features, key sizes, algorithms, packet filters, SPI, …

Practical Problems with Biometrics (ctd)

UK passport service required a biometric-compatible photo instead of the standard one

- 80,000 of the first set of photos (600K) were rejected for not meeting the requirements
- Computer-based systems are vastly easier to confuse than humans

Practical Problems with Biometrics (ctd)

UK Passport Service Enrolment Trial

- Enrolled 9,000 travellers to evaluate the enrolment experience

10% of users couldn’t enrol using the iris-recognition system

- (Maybe they should have got National Geographic to handle this for them)

30% of able bodied users couldn’t have their facial biometrics verified

- (c.f. conventional wisdom of 3-4% goats)

Practical Problems with Biometrics (ctd)

50% of disabled users couldn’t have their facial biometrics verified (!!)

- Particularly problematic due to laws like ADA that forbid discrimination against the disabled

“Fix” was probably to wind the sensitivity down so that almost anything would pass

- This is the universal solution for any failures in systems that employ approximate matching

Practical Problems with Biometrics (ctd)

German passport enrolment requirements stipulate the use of the least unreliable trait sample if no reliable one can be obtained

> There doesn’t seem to be any minimum acceptable quality measure for trait sampling
>
> — ‘starbug’, Chaos Computer Club

> In cases where there is difficulty in collecting even a single fingerprint of acceptable quality, the department or agency shall perform authentication using asymmetric cryptography
>
> — FIPS PUB 201-1

Practical Problems with Biometrics (ctd)

The e-passport solution is rather different

- If all else fails, click the “No Hand” button on the fingerprint software

  If the fingerprint isn’t readable, which isn’t uncommon, the passport records “No Hand” [“Keine Hand”]. There is no provision for “Fingerprint not readable”
  — Norddeutscher Rundfunk (NDR) Ratgeber

  This is an unfortunate ‘solution’
  — ‘starbug’, Chaos Computer Club

Cannot cope with a situation where a FTE (or any other Fxyz) occurs

- System is assumed to be perfect and failure-proof

Practical Problems with Biometrics (ctd)

Verification time was a full minute across a variety of systems

- Current verification time for intra-EU travel is < 5s
- Order-of-magnitude slowdown for traveller verification

Enrolment has similar problems

- German biometric enrolment system was advertised as taking 2½ minutes, in practice takes > 10 minutes

One of the reasons why pre-biometric passports had a 10-year life was that that was about the maximum throughput of the processing system

- Now, vastly more complex passports have to be rolled over in half the time

Practical Problems with Biometrics (ctd)

Failure rates were significantly higher for people with darker skin and/or eyes

- Dark skin/dark eyes absorb more light
- Features don’t stand out as much

These are all features of the ethnic group that these systems are targetting

- The targets are the ones least likely to be correctly processed!

Fingerprint Security

Faking prints (pre-biometrics)

- Photograph a latent print using high-contrast film
- Develop the film using a process that leaves ridges of loops and whorls raised in relief
- Use sebum (oil from skin, in this case hair grease) to create the “print”

Fingerprint Security (ctd)

Faking prints (today)

- Bring out the print using cyanoacrylate glue fumes
- Photograph the prints using a digital camera
- Print onto plastic foil, toner provides 3D structure
- Coat with wood glue to fix the 3D image

> The CCC hobbyists didn't need more than a plastic container [with the victim's prints on it], a digital camera, and three different types of glue
>
> — "Chaos Computer Club überlistet biometrische Pässe"

Fingerprint Security (ctd)

Time to copy a print with the owner's co-operation

- 15 years ago: 2-3 hours
- 5 years ago: 15 minutes, $10
- Today: A few minutes, < $1

Time to copy a latent print

- 15 years ago: Several days
- 5 years ago: 30 minutes, $20
- Today: A few minutes, < $1

The use of automated fingerprint recognition systems has made the forgery task vastly easier

> Current systems can all be fooled by a typical teenager
>
> — "Chaos Computer Club überlistet biometrische Pässe"

Fingerprint Sensors put to the Test

Network Computing review, 1998

- Only two of six fingerprint readers could reject a plastic finger

Japanese researchers produced a 100% failure rate in fingerprint readers using $10 worth of raw materials

- “Gummy fingers” (gelatin) can be created from latent prints
- You leave a copy of your PIN on everything you touch
- Gummy finger use is almost impossible to detect

DansData did the same with Silly Putty

Fingerprint Sensors put to the Test (ctd)

Inspired by the Japanese, the Germans had a go too…

- Six capacitive fingerprint scanners (the most common type)
- Two optical fingerprint scanners
- One thermal fingerprint scanners
- Two face-recognition systems
- One iris scanner

Fingerprint Sensors put to the Test (ctd)

All of them failed

- Some capacitive scanners could be fooled by breathing on the latent print (!!)

  > The products in the versions made available to us were more of the nature of toys than serious security measures
  >
  > — c't Magazine

- This technique was shown in action in the movie "Get Smart"
- Unlike many outrageous Hollywood James Bond tricks, this one was based on actual fact

Fingerprint Sensors put to the Test (ctd)

Swedish student tested the latest products at the 2004 CeBIT trade show

- All 9 failed

Clarkson University did it with "digits from cadavers and fake fingers molded from plastic, or even something as simple as Play-Doh or gelatin"

> The machines could not distinguish between a live sample and a fake one
>
> — Stephanie Schuckers, Associate Professor of Electrical and Computer Engineering

Fingerprint Sensors put to the Test (ctd)

German consumer affairs program Plusminus used fingerprint copies on plastic foil to buy goods on other people’s accounts at Edeka (large supermarket chain)

> Proving that the purchase was fraudulent will be difficult because fingerprints are regarded as being very secure
> — Heisen Online News (translation)

> The full set of fingerprints shall be collected from all PIV Card applicants who can provide them. [...] The requirement for ten fingerprints is based on matching accuracy data obtained by NIST in large-scale trials and reported in NISTIR 7123
> — FIPS PUB 201-1

Fingerprint Sensors put to the Test (ctd)

Mythbusters also had a go (Season 4, Episode 59)

- Tried to fool an enhanced biometric door lock that included liveness-detection technology to check for a pulse, body heat, and sweat
- Manufacturer claimed that it had never been defeated

As with previous experiments, the reader exhibited a 100% failure rate

- Could be fooled using anything from a cast of a latent print (lifted from a CD) to a simple photocopy of someone’s finger
- Licking the fakes (to simulate sweat) was enough to fool the scanner’s liveness detection

(I guess no-one had ever tried to defeat it before)

Fingerprint Sensors put to the Test (ctd)

CCC member ‘starbug’ defeated all fingerprint sensor liveness-detection mechanisms using relatively simple measures

- Blood flow, pulse, deformation of the print when pressure is applied, …

> I’ve never found a sensor I couldn’t defeat. It’s just a case of finding the right materials...
>
> — starbug

- Cyanoacrylate glue, amino-acid indicators (for prints on paper), wood glue, laser-cut plastic foil (for swipe sensors), graphite spray (for conductivity-based sensors), sellotape (to lift prints from glass),

Fingerprint Sensors put to the Test (ctd)

A Scottish prison used fingerprint sensors for its security (!!)

> Prison officers have been forced to abandon a new security system and return to the use of keys [...] problems arose after a prisoner demonstrated to wardens that he could get through the system at will. Other prisoners had been doing the same for some time
>
> — The Scotsman

The Daily WTF has a lengthy run-down of the biometrics comedy-of-errors that ensued from installing fingerprint readers in a gym, `http://thedailywtf.com/Articles/Cracking-your-Fingers.aspx`

Fingerprint Sensors put to the Test (ctd)

In Brazil, public employees sign in for work using fingerprint scanners

- Present a fingerprint, get paid
- (See if you can guess where this is heading...)

> Doctor ‘used silicone fingers’ to sign in for colleagues
> — BBC

Fraud extended to around 300 people in one town alone

Other Problems with Fingerprint Sensors

Security systems that encourage attackers to steal parts of your body may have user acceptance problems

> Police in Malaysia are hunting for members of a violent gang who chopped off a car owner’s finger to get round the vehicle’s hi-tech security system
> — BBC News

Other Problems with Fingerprint Sensors (ctd)

Fingerprint sensors represent *severe* hygiene problems

- Look at the US-VISIT sensor next time you land
- These sensors contain more bacteria than a toilet seat (!!)
  - (Consider the cleaning policy and usage of toilet seats vs. fingerprint sensors)

No-one seems to have brought this to the public's attention yet so we don't know what the reaction will be

Face recognition put to the Test

Palm Beach Airport (Florida) facial recognition system was "less accurate than a coin toss"

- 10,000 face captures/day
- Worked only 47% of the time, under ideal testing conditions
- Eyeglasses or turning your head slightly would fool it

NIST found a 43% FAR for face recognition *under perfect conditions*

Face recognition put to the Test (ctd)

Tampa, Florida two-year pilot yielded zero results

Large numbers of false positives

- Confused male and female subjects, different ages, weights
  - These systems have almost comical problems with gender recognition, something that evolution has made humans very good at
- Woman was identified as a male sex offender

Initially, officers increased the threshold to try and reduce the false alarms

- Result: No-one was matched any more

Face recognition put to the Test (ctd)

Eventually, police just stopped using it

- Logs show that it was still active, but no-one paid any attention to it

  When a system generates a fair number of false positives relative to the remote possibility of a true positive, operators will inevitably become lax. When that happens, it defeats the whole objective of having a screening process in the first place

  — The Economist

Number of extra police that could have been employed for the projected cost: About 20

- c.f. US-VISIT costs

It was of no benefit to us. It served no real purpose

— Tampa Police Captain Bob Guidana

Face recognition put to the Test (ctd)

In 1998 Newham borough in London ran a major PR campaign about their CCTV cameras scanning faces in the street for criminals

- The criminals moved elsewhere
  - (This is an established effect of crime relocation cameras, no net decrease in crime)

Face recognition put to the Test (ctd)

The Guardian newspaper put the system to the test

- No matter how suspiciously the reporter acted, he wasn't picked up

  From the point of view of the security cameras, I might as well have been wearing a sandwich board with the words "Villain - sample only" on it

  — "Robo Cop", UK Guardian

  The computer never knew I had been there. Sandra, the always cheerful Newham press officer, didn't sound surprised when she reported the failure of the Visionics system, and by this time, neither was I

  — "Robo Cop", UK Guardian

Face recognition put to the Test (ctd)

Police later revealed that the system had never recognised anyone

> Not once, as far as the police know, has Newham's automatic facial recognition system spotted a live target
>
> — "Robo Cop", UK Guardian

> [CCTV Enforcement Officer] Tisshaw hinted that the true value of FaceIt was in deterrence, regardless of whether it worked or not, like a fake burglar alarm on the outside of a house
>
> — "Robo Cop", UK Guardian

- (Security by placebo effect)

Face recognition put to the Test (ctd)

The evasiveness of the Newham council to questions from the Guardian about the system's effectiveness is straight from "Yes Minister"

> "The reason we don't publish these figures is because it's just contrary to the way we run this scheme. What we're saying to criminals is: this is the system we've got, and we don't want you doing your wrongdoing, because we know you're around"

> "The figures, if released, would never be viewed in the right way"

> I asked about a press release Visionics put out on January 10, saying that "the FaceIt surveillance system, running in a UK town centre, successfully identified a subject wanted by law enforcement authorities". Could she say where this happened and what kind of suspect was involved? She couldn't

Face recognition put to the Test (ctd)

2001 Super Bowl (“Snooper Bowl”) scanned 70,000 participants for terrorists/criminals

- Zero matches
- Did match a ticket scalper, but he vanished before police got there

INS stopped using face recognition at the Mexico/US border because it didn’t work

Sydney Airport SmartGate system couldn’t detect when two Japanese tourists swapped passports

Face recognition put to the Test (ctd)

DARPA face recognition test, under perfect conditions, yielded

- FRR = 33%
- FAR = 10%

> To detect 90% of terrorists we’d need to raise the alarm for one in every three people… it’s absolutely inconceivable that any security system could be built around this kind of performance
>
> — Image Metrics COO Gareth Edwards

Face recognition put to the Test (ctd)

Boston Logan Airport trial

- 10 of the 19 September 11 hijackers boarded at Logan
- Evaluation only detected 37% of “volunteer” terrorists
  - This was under artificially good conditions: Only 40 participants going through 2 checkpoints
- FaceIt spokesperson said that their figures showed an 85.7% success rate
  - 53 out of 153 “terrorist” entries = 37%

> Logan Airport results will not affect plans to use face recognition to enhance passport security
>
> — Kelly Shannon, US State Department

Face recognition put to the Test (ctd)

Fresno Airport trial

- US Army Research Lab test showed that the Visionics FaceIt system correctly identifies individuals only 51% of the time

> True matches (picking criminals out of a crowd) appear to be a crapshoot
>
> — Thomas Claburn, “Smart Business”

2001 evaluation by the UK National Physical Laboratory found that face recognition was almost the worst biometric technology there is

- Only vein patterns fared worse

Face recognition put to the Test (ctd)

Any kind of plastic surgery confounds face-recognition

- Nose job: 60% failure rate
- Facelift: 98% failure rate

  For a face-lift, the results were dismal: a match rate of just 2 percent

  — "Plastic Surgery 1, Face Recognition 0"

Under ideal conditions with perfect lighting, the best available algorithms had a 60% failure rate

- (Face-recognition works, as long as you don't try and defeat it)

Face recognition put to the Test (ctd)

Surgery also defeats other biometrics

- Illegal immigrants from China enter Japan by having their fingerprints surgically altered

  She was only discovered when she was arrested on separate charges […] The apparent ability of illegal migration networks to break through hi-tech controls suggests that other countries who fingerprint visitors could be equally vulnerable […] Police believe the practice may be widespread

  — BBC News

Face recognition put to the Test (ctd)

Face-matching of celebrities on MyHeritage.com

- Bill Clinton matches Bill Clinton
  - And Billy Graham
  - And Eric Clapton
- George Bush matches George Bush
  - And James Coburn, and Joseph Stalin (!!)
- A teletubby matches Yoko Ono and Tori Amos
- Gollum matches Minnie Driver and Michael Dukakis
- Shrek matches Barbara Streisand and Kelsey Grammar
- A smiley matches Cameron Diaz and Ozzy Osbourne

Face recognition put to the Test (ctd)

Vietnamese Internetwork Security Centre demonstrated bypassing facial biometric logon software on Lenovo, Asus, and Toshiba laptops

Source: news.cnet.com/8301-17938_105-10110987-1.html

- Grabbed a photo from a Skype call
- Printed out a barely-recognisable likeness on an inkjet printer
- All of the laptops accepted it as a real person

Face recognition put to the Test (ctd)

Galaxy Nexus face recognition was easily defeated in a similar manner, despite Google's denials

> It was soon discovered that its face unlock feature could be defeated with a photograph, despite Google's Tim Bray stating on Twitter that it was not possible
>
> — "Samsung Galaxy S3 Face Unlock Tricked by Photograph"

Samsung updated the face recognition for the latest S3 model

> We found that the Galaxy S3 cannot distinguish between a photograph and a real person
>
> — "Samsung Galaxy S3 Face Unlock Tricked by Photograph"

Face recognition put to the Test (ctd)

All of these face-detection evasion mechanisms are poke-and-hope

- What if you specifically targeted the face-recognition algorithm?

Algorithms are precisely-defined mathematical transformations

- Take the algorithm target data and work backwards to the source to figure out what you need to change there

Face recognition put to the Test (ctd)

Biometric algorithms work by feature extraction

- Isolate the few features that the algorithm needs in order to work
- Make just those minimal changes

Even appropriately-applied makeup can now defeat the face recognition

> Images without [algorithm-tuned makeup applied] tested negative, no face was found
>
> — "CV Dazzle Makeup"

Face recognition put to the Test (ctd)

Face-recognition trial of three systems run by the German Bundeskriminalamt (Federal Criminal Police Office)

- Tested under slightly more normal conditions, not a special optimal test environment
- Even then, the test user base was only 200 people
  - Normal daily traffic volume is 23,000 people from a pool of tens of millions
- In addition, tests were carried out on escalators to ensure distinct facial shots
  - Smooth, continuous movement, people looking straight ahead
- (Assume a perfectly spherical elephant of negligible mass and volume)

Face recognition put to the Test (ctd)

Achieved an average accuracy rate of around 30%

- In a poll before the trial, manufacturers expected to see 60-80% accuracy

Even under artificially good conditions, none of the three systems ever achieved a peak success value over 60%

- Under less-than-ideal conditions, it went as low as 0%

  I will recommend to the Minister of the Interior that this tool not be used for fighting terrorism

  — Jörg Ziercke, President of the Bundeskriminalamt

  It’s rare to see privacy advocates and security authorities agree on something in the fight against terrorism

  — Der Spiegel

Face recognition put to the Test (ctd)

Face recognition couldn’t find the suspects in the Boston bombings

The technology came up empty even though both Tsarnaevs’ images exist in official databases

— The Washington Post

They were eventually tracked down through human analysis

The work was painstaking and mind-numbing: One agent watched the same segment of video 400 times

— The Washington Post

Iris Scans put to the Test

Iris codes are advertised as being highly secure

> [Iris-code biometric templates] cannot be reconstructed, decrypted, reverse-engineered or otherwise manipulated to reveal a person's identity. In short, biometrics can be thought of as a very secure key
>
> — Biometric vendor B12 Technologies' web page

Can in fact be faked 80% of the time

- Use genetic algorithm to mutate a synthetic iris image until it passes a check for the real thing
- Takes 100-200 iterations to produce an iris code identical to the original
- Done from an image, doesn't require access to an iris scanner

Iris Scans put to the Test (ctd)

Tested against the VeriEye system

- Among to top algorithms tested in a NIST evaluation

Fooled it 80% of the time

- Even untrained humans scored better than this

> Once you have the image you can actually print it and show it to the recognition system and it will say 'okay, this is the [right] guy'
>
> — "Reverse-Engineered Irises Look So Real, They Fool Eye-Scanners"

Iris Scans put to the Test (ctd)

Under benign conditions, Iridian iris scans “only” failed 6% of the time (Iridian owns the patents on iris scanning)

- For 1M daily air travellers that’s *forty thousand* false alarms a day
- (And anyone who wants to defeat the system can just lift your Iriscode from a photo)

Biometrics in the Real World

Performance figures for biometrics are almost always given under carefully-controlled conditions

When tested in real-world situations, they can drop drastically

- Fingerprint error rate went up tenfold when real-world (rather than ideal lab) conditions were applied
- Iris recognition went from 90% success rate to 75% failure rate under real-world conditions

> Biometric quality measurement has become an important concern after biometric systems’ poor performance on pathological samples
>
> — “Quality Measures in Biometric Systems”

Use of Multiple Biometrics

Some countries have proposed the use of multiple biometrics to reduce problems with individual biometrics

- We can sell them twice as much biometrics!
  - (D’oh, we should have gone for four or give)

This makes things *less* secure, not more

- Huh?

Combining two measures makes them stronger

- However, dual biometrics have four measures (2 × FAR and FRR), not two

Use of Multiple Biometrics (ctd)

When combining error rates

- One becomes stronger than the better of the two
- One becomes weaker than the worse of the two

This problem is a known issue among biometrics technologists

- No vendor will ever admit to it
- No customer even knows about it

Use of Multiple Biometrics (ctd)

Example (analogy): Device designed to prevent you from falling off a cliff

- Two are better than one, right?
- Not necessarily…

Use the first device

- It works! I didn’t plunge to my death

Now let’s see if the second device works as well…

Result: The combination of two is less secure than one on its own

- (The statistical maths explanation isn’t nearly as easy to understand)

Use of Multiple Biometrics (ctd)

Unless the FAR/FRR are perfectly matched, two biometrics are significantly worse than one

- The chances of two biometrics being perfectly matched is slim
- Little chance of a match when the underlying technologies are fundamentally different

Even if (somehow) there are two well-matched technologies, their working environment will cause a mismatch

- Poor lighting will affect facial recognition but not fingerprints
- Sweat/dirt/airline food remnants will affect fingerprints but not facial recognition

Protection of Biometric Data

Support systems for biometrics are uniformly awful

- Companies are often created by academics with extensive knowledge of the science of biometrics and little knowledge of security technology

The back-end systems are full of security holes

> Weaknesses existed in all control areas and computing device types reviewed. These weaknesses collectively increase the risk that unauthorized individuals could read, copy, delete, add, and modify sensitive information
>
> — US Government Accountability Office

> I'm not surprised that the system is so insecure; I'm surprised that anyone is surprised
>
> — Bruce Schneier

Protection of Biometric Data (ctd)

None of the support systems are anywhere near as secure as a standard Windows PC

These are SCADA systems with SCADA security

- "SCADA security" = "the protocol is undocumented" + "we use an unroutable network protocol"

> Vulnerabilities that are near-dead in the PC realm, are abundant
>
> — "Exploiting Embedded Systems: The Sequel"

Protection of Biometric Data (ctd)

A few selected examples of different products…

- Reader physically protected with 1.2mm of ABS plastic
- Reader runs embedded Linux with a fixed root password and SSH, Samba, …
- Reader verifies the biometric by requesting a copy of the credentials from a remote server
  - The attacker can request credentials for every user in the system
- Biometric data server is a standard Windows PC with credentials stored in plaintext in an Access database

...continues...

Protection of Biometric Data (ctd)

...continued...

- Biometric is verified by submitting it to a server and waiting for a yes/no response
  - Replay a yes response for any request
- Communicates data over 802.11
  - You don't even need to physically penetrate the network to get in
- Data communicated in plaintext or poorly-obfuscated form

> It is clear that the data transfer between the device and management server is in plaintext
>
> — Biologger — A Biometric Keylogger

...continues...

Protection of Biometric Data (ctd)

...continued...

- Use of proprietary, homebrew protocols for all communications
- Ability to remotely reprogram security aspects of the system

  It was possible to add new users to access control devices within the network

  — Biologger — A Biometric Keylogger

  – This included administrators

  [We] successfully added a user “Hacker” […] with a PIN of “1234” and administrator privileges

  — Biologger — A Biometric Keylogger
- Other messages included door unlock commands

(Pretty standard for SCADA systems, but it shouldn’t be this bad for something intended to provide security)

Protection of Biometric Data (ctd)

Original biometrics can be recovered from stored templates

- For a long time this was regarded as impossible, without anyone actually ever trying it
- “We don’t need to secure the templates since no-one can do anything with them”

  The reconstructed images have a very good quality and may be used to attack existing fingerprint recognition systems

  — “Can Fingerprints be Reconstructed from ISO Templates?”

Protection of Biometric Data (ctd)

Attack was tested against nine state-of-the-art fingerprint readers

> The reconstructed images are very realistic and, although it is unlikely they can fool a human expert, there is a high chance to deceive state-of-the-art commercial fingerprint recognition systems
>
> — "Fingerprint Image Reconstruction from Standard Templates"

Intercept a template message to/from the reader and you can impersonate the subject

- Capture the template database and you can impersonate *anyone* on it!

Protection of Biometric Data (ctd)

Biometric systems can render the system they're used with unsafe

UPEK fingerprint-reader software on laptops from Acer, Amoi, Asus, Clevo, Compal, Dell, Gateway, IBM/Lenovo, Itronix, MPC, MSI, NEC, Sager, Samsung, Sony and Toshiba stored credentials for account logon, Windows EFS, and other sensitive services in near-plaintext

> UPEK's implementation is nothing but a big, glowing security hole compromising (and effectively destroying) the entire security model of Windows accounts"
>
> — "Laptop fingerprint reader destroys 'entire security model of Windows accounts'"

Protection of Biometric Data (ctd)

Ignore the applications and target the underlying ICCs and IFDs (cards and readers)

> The use of a product that conforms to this standard does not guarantee the security of the overall system in which the product is used
>
> — FIPS PUB 201-1

- Once you 0wn the low-level protocol stack, it's game over

> Security flaws are abundant on embedded devices
>
> — "Exploiting Embedded Systems: The Sequel"

Protection of Biometric Data (ctd)

Several attacks on wireless device stacks have already been demonstrated

- Example: Trifinite's BlueSmack attack on Toshiba's Bluetooth stack caused an instant BSOD on the host

Codenomicon's Bluetooth testing found even worse problems

> Most of the Bluetooth-enabled devices simply crashed when tested with any level of robustness testing. Sometimes the result from the testing was that the device ended up totally corrupt, requiring re-programming of its flash memory to become operable
>
> — "Wireless Security: Past, Present, and Future"

Protection of Biometric Data (ctd)

Other devices were no better

> All the [802.11] access points failed with some of the protocol tests, but more alarmingly there were access points that failed with almost everything that was run against them
>
> — "Wireless Security: Past, Present, and Future"

Overall result of wireless device testing was abysmal

> Testing found problems in 90 percent of the devices tested
>
> — "Wireless Security: Past, Present, and Future"

This was straight fuzzing, not even a targeted, device-specific attack!

Protection of Biometric Data (ctd)

IFDs/ICCs make SCADA systems look good in comparison

- Writing an IFD/ICC driver isn't so much implementing a spec as finding (by trial and error) the appropriate silly-walk to induce a given device and firmware combination to provide the intended result

> Conformance to this standard does not assure that a particular implementation is secure
>
> — FIPS PUB 201-1

Protection of Biometric Data (ctd)

Readers/devices will…

Hang (requiring a soft reset)

Lock up (requring a power cycle)

Return invalid data lengths (too much/too little)

- The ICAO has already run into some of these bugs during interop testing

  We have found that some cards expect 4-byte and some 5-byte APDU when Le = 00

  — ICAO 9303 supplement 2005-4

... continues ...

Protection of Biometric Data (ctd)

... continued ...

Return invalid data (tags, field lengths, element counts, field entries, ...)

Three different implementations were found at read binary of Odd_INS Byte when reading data greater than 32k byte

1) The Le byte contains V only.
2) The Le byte contains TL and V.
3) The Le byte contains extended TL and V

— ICAO 9303 supplement 2005-4

- Extensive bug lists in amendments to ICAO 9303 provide a roadmap of attack vectors to try

... continues ...

Protection of Biometric Data (ctd)

... continued ...

Require invalid data (reject correctly-formatted data)

- This one is especially entertaining to figure out

React to commands in unexpected/undefined ways

> From our Singapore InterFest experience, we know some card vendors expect Le = 28 and some expect Le = 00 or will only respond correctly if Le = 00
>
> — ICAO 9303 supplement 2005-4

- This includes doing things that shouldn't be permitted

... continues ...

Protection of Biometric Data (ctd)

... continued ...

Implement undocumented commands or command extensions

- This is very common
- Some are bugs, some are just vendor-specific supplementary functionality
  - ISO 7816-4 defines different classes of command, CLA '0x' = standard, CLA '8x' / '9x' = vendor-specific
  - Vendors implement the bare minimum of CLA '0x'
  - As much functionality as possible is implemented in CLA '8x' / '9x' to prevent interoperability

... continues ...

Protection of Biometric Data (ctd)

... continued ...

You have no idea of knowing what capabilities lurk inside these devices

- California FasTrak road toll passes were supposed to be read-only
- Nate Lawson (see earlier slides) found that they were writeable

> FasTrak is probably not aware of this
>
> — Nate Lawson

... continues ...

Protection of Biometric Data (ctd)

... continued ...

You also have no idea what capabilities don't lurk inside these devices

> In the past, authorities have insisted that the FasTrak system uses encryption to secure data [...] But when Lawson opened up a transponder, he found that there was no security protecting these IDs
>
> — MIT Technology Review

- c.f. the missing encryption in contactless credit cards
- Another device used an XOR-based stream cipher with a CRC for "integrity protection"
  - Allows undetectable data manipulation

... continues ...

Protection of Biometric Data (ctd)

... continued ...

Even industry insiders were unaware of what their own technology did

> That sentence [pointing out problems] makes us think this guy Lawson is an amateur. The only “research” needed to establish whether anything could be planted on the FasTrak transponder is a visit to the website of the manufacturer, Sirit. This makes clear what everyone in the toll business knows, namely that the FasTrak transponder is a read-only device which cannot have anything written to it at all
>
> — TOLLROADSnews commentary

- “That sentence makes us think this guy Columbus is an amateur. Everyone knows that if you sail too far into the Atlantic, you fall off the edge of the world”

Protection of Biometric Data (ctd)

... continued ...

> If Lawson has not even established that FasTrak transponders are a read-only device rather than read-write, then he’s totally unqualified to be talking about potential misuse
>
> — TOLLROADSnews commentary

- This is scary: Industry experts are clueless about what their own products do
  - Insert joke about “a used car salesman knows when he’s lying”

... continues ...

Protection of Biometric Data (ctd)

... continued ...

And you have no idea where these things end up

> I often ask people if they have an RFID card and half the people emphatically say no I do not. And then they pull out the cards to prove it and … there has been an RFID in their wallet. This stuff is being deployed without people knowing it
> — Chris Paget

... continues ...

Protection of Biometric Data (ctd)

... continued ...

To ease privacy concerns, RFID tags can be killed

> Interrogators and Tags shall implement the Kill command [...] render itself silent and shall not respond to an Interrogator thereafter [...] Killed Tags shall remain in the killed state under all circumstances, and shall immediately enter killed upon subsequent power-ups. A kill operation is not reversible
> — EPC Class 1 standard

- This doesn’t actually kill the tag
- All it does is zero some ID fields
- The tag is still fully functional and responds to read requests

... continues ...

Protection of Biometric Data (ctd)

... continued ...

To revive a “killed” tag, write a new ID to it

> The method for tag resurrection is very simple [...] the inventory application was then able to read, verify and modify the resurrected tag
>
> — “The Lazarus Effect: Resurrecting Killed RFID Tags”

Protection of Biometric Data (ctd)

ICC/IFDs are at the Internet Explorer 3.02 level of data handling

- The hard thing about attacking them isn’t the attack itself but making sure that you don’t simply crash the IFD or ICC with the data that you send it

RFID/Biometric Product Redux

Anyone who’s ever been to any hacker con will have seen demos of endless examples of “The vendor claims/thinks their product does X, it actually does Y, here’s the exploit”

- RFID/biometrics is no exception
- Possibly even worse than the general software world, since there’s very little darwinian evolutionary pressure

This is a classic lemon market

- See “The Market for Lemons: Quality Uncertainty and the Market Mechanism”
- No way to tell what you’re really getting

So what is it good for?

Attended biometric usage: Access control

- Primary identifier uniquely identifies someone
- Biometric backs up the primary ID
  - Match only this one identified person and no-one else

So what is it good for? (ctd)

Unattended biometric usage: Prevent people from sharing credentials

- This is a serious problem, e.g. over-18s selling/lending licenses to drink to siblings
  - They never consider the fact that they're selling their identity

This is solving a social problem rather than a security problem

- Any basic biometric measure will do the job, even a 100%-false-positive fingerprint reader

Even just adding photos and names to security tokens has been found to be effective

So what is it good for? (ctd)

RFID tags

- Barcode replacement/inventory control

  > While it may not matter if RFID tags on pallets of carrots are vulnerable to counterfeiting, it will most certainly matter when RFID is used to secure the world's supply of pharmaceuticals
  >
  > — Ari Juels, RSA Security

Closing thoughts

The industry has set up [a] negative perception, because it has claimed biometrics are foolproof in terms of identification for security purposes. That's the wrong approach. Number one, it's not foolproof. And number two, it really isn't for security — it's for convenience

— Jim Wayman, former director,
US Government Biometrics Center

For applications related to human beings, RFID appears to offer little benefit when compared to the consequences it brings for privacy and data integrity. Instead, it increases risks to personal privacy and security with no commensurate benefit for performance or national security

— "The Use of RFID for Human Identification",
DHS Emerging Applications and Technology Subcommittee

Closing thoughts (ctd)

Computers are fast at computation but not very good at judgment. People can fool speed cameras by taping a fake license plate over the real one, fingerprint readers with a piece of tape, or automatic face scanners with — and I'm not making this up — a photograph of a face held in front of their own. Even the most bored policeman wouldn't fall for any of those tricks

— Bruce Schneier

Thanks to movies and spy thrillers, people have come to think of […] biometric means of identifying evildoers as being completely foolproof. In reality, they are not and never have been, and few engineers who design such tools have ever claimed them to be so. [This has lead] to a great deal of public money being squandered and the fostering of a sense of security that is largely misplaced

— The Economist

Closing thoughts (ctd)

Users frequently forget passwords, but they rarely forget fingers

> People like biometrics because they believe in them
>
> — Tom Rowley, Veridicom CEO

> The biometric (fingerprint reader) feature in this device is not a security feature and is intended to be used for convenience only. It should not be used to access corporate networks or protect sensitive data, such as financial information
>
> — Microsoft fingerprint reader setup dialog

> What's scary is that [some people] don't even care if biometrics are actually safe since using biometrics is just so cool
>
> — "The Trouble with Biometrics", Christopher Calabrese