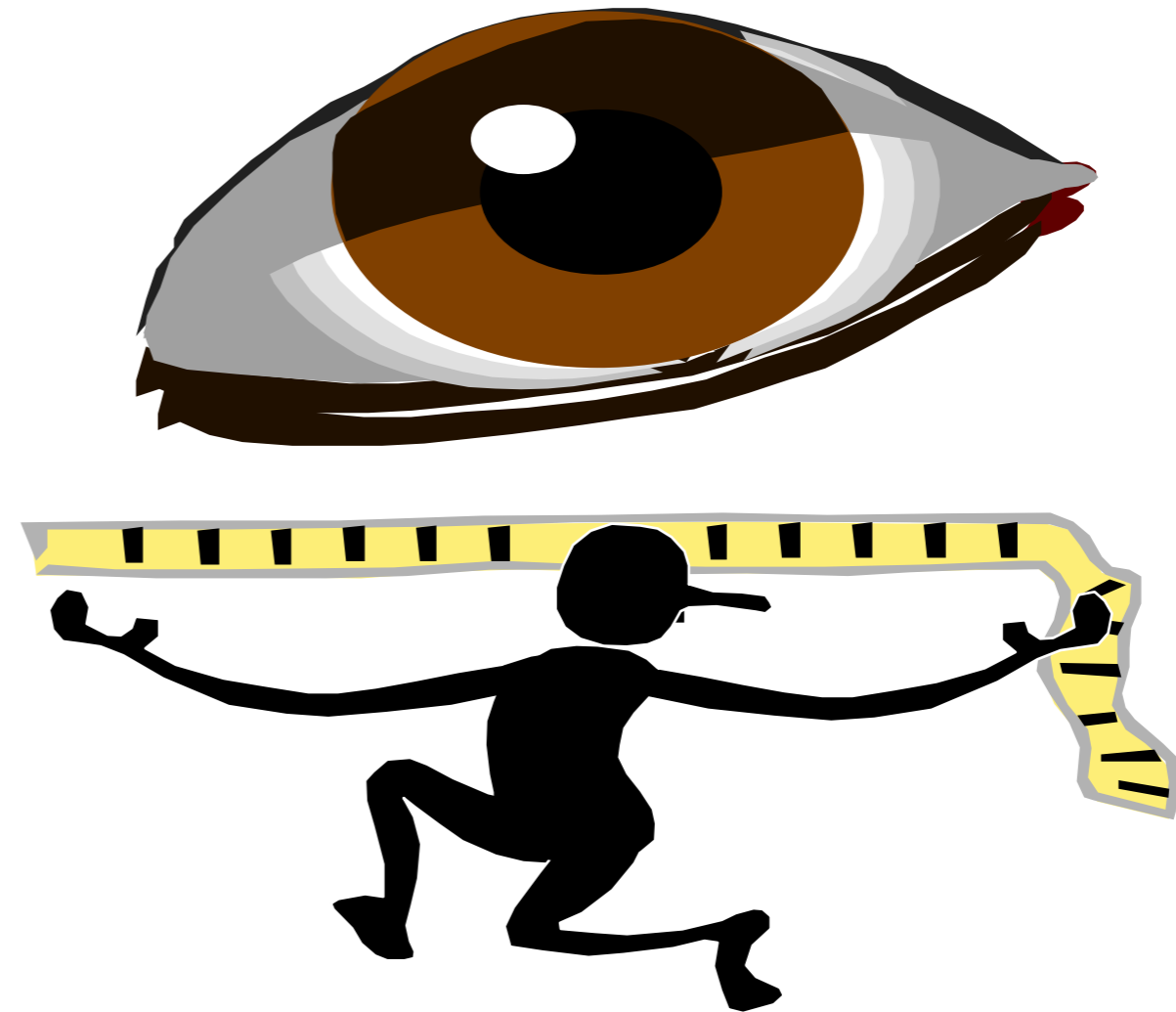


Biometrics + Authentication Tokens

Thanks to [Ari Juels](#) for most of this deck!

Biometrics

- Measurement of some biological characteristic
- “Something-you-are” authentication factor
- Essentially how people authenticate one another



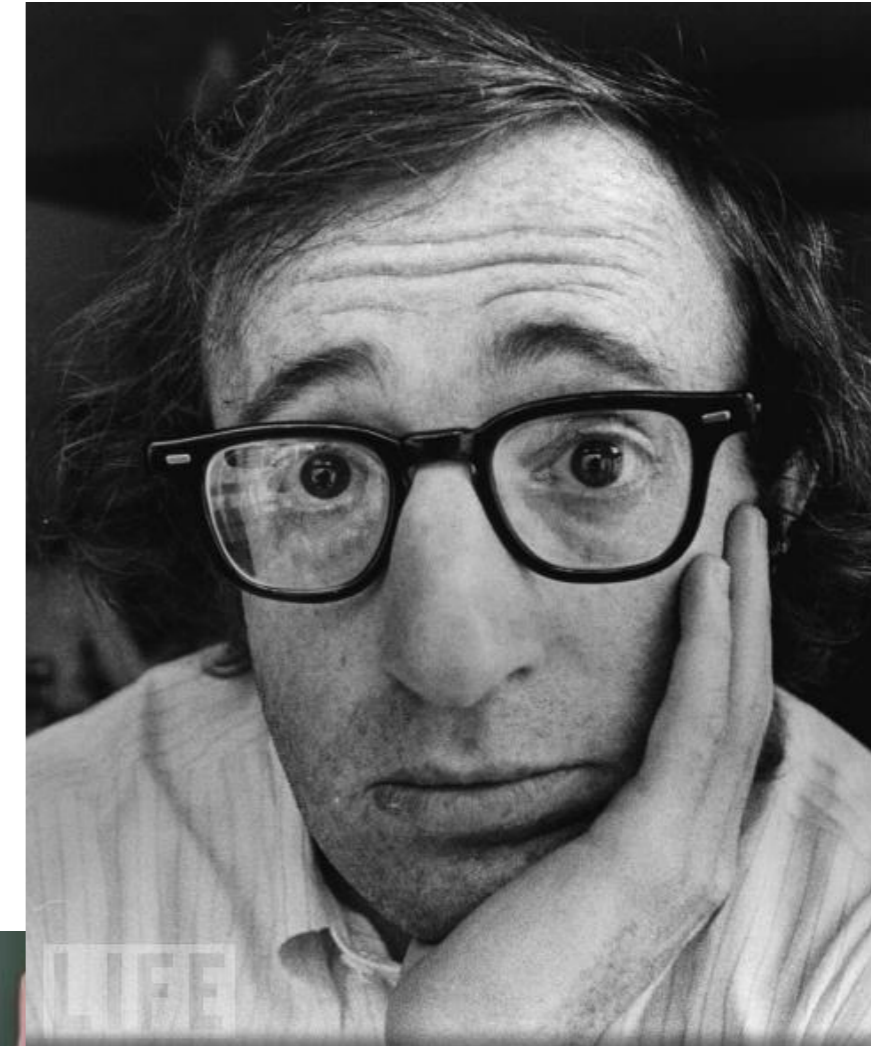
Biometrics

- Some attractive features
 - Minimal user effort
 - Nothing extra to carry or remember
 - Hard to lose!
 - Can't be shared (usually)
- Some drawbacks
 - Not always accurate
 - Work poorly for some people
 - Security challenges (to be discussed)

Here are some examples...

Face recognition

- Pros:
 - Very intuitive
 - Can use ordinary camera
 - Or one on mobile device
- Cons:
 - Poor accuracy
 - (Purported improving rapidly)
 - Not terribly secret



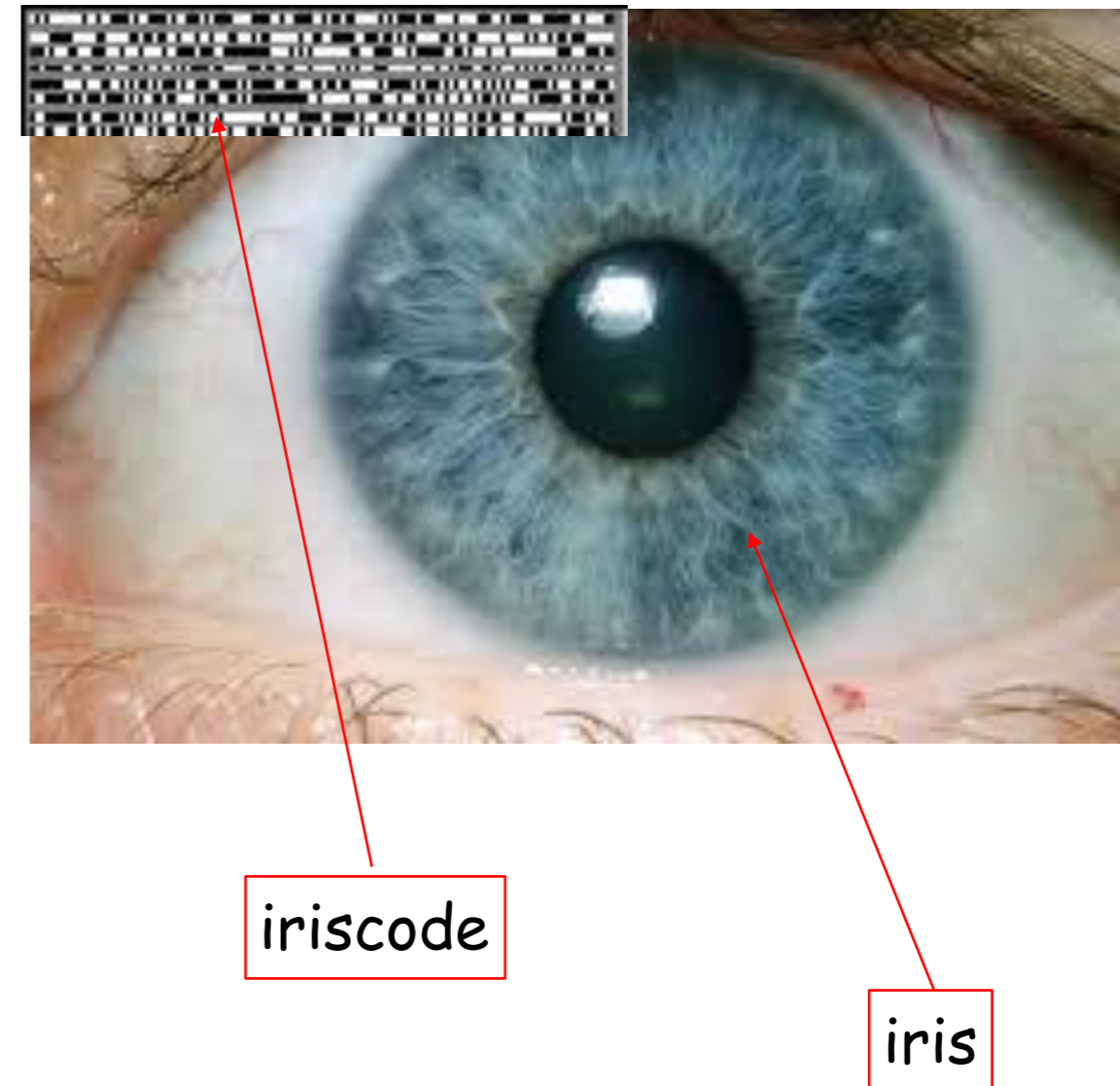
Fingerprint

- Pros:
 - Lots of experience in law enforcement
 - Belief in uniqueness
 - (We'll talk about this...)
- Cons:
 - Social stigma
 - Spoofable



Iris

- Pros:
 - Extremely accurate
 - Estimated 250 bits of entropy in iriscodes!
 - Can in principle yield a cryptographic-strength "key" (but is it really a key?)
 - Non-invasive
 - Note: not retina!
- Cons:
 - Requires special camera
 - Very sensitive to lighting conditions
 - People confused about difference between the iris and retina...



Other types

- Some less common ones:

- Hand geometry
- Retina
- Keystroke dynamics
- Gait
- Pulse

...We won't discuss these to

- Even less common:

- Ear recognition
- Body odor

...We won't discuss and will try to forget...



Featured Research

from universities, journals, and other organizations

Identity verification: Body odor as a biometric identifier

Date: February 4, 2014

Source: Universidad Politécnica de Madrid

Summary: Researchers are making progress on the development of a new biometric technique that would allow us to identify people through their personal odor.

Share This

> Email to a friend

> Facebook

> Twitter

> LinkedIn

> Google+

And also...

January 18, 2012, 1:00 PM ET

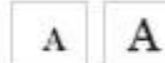
Forget Fingerprints: Car Seat IDs Driver's Rear End

Wall Street Journal

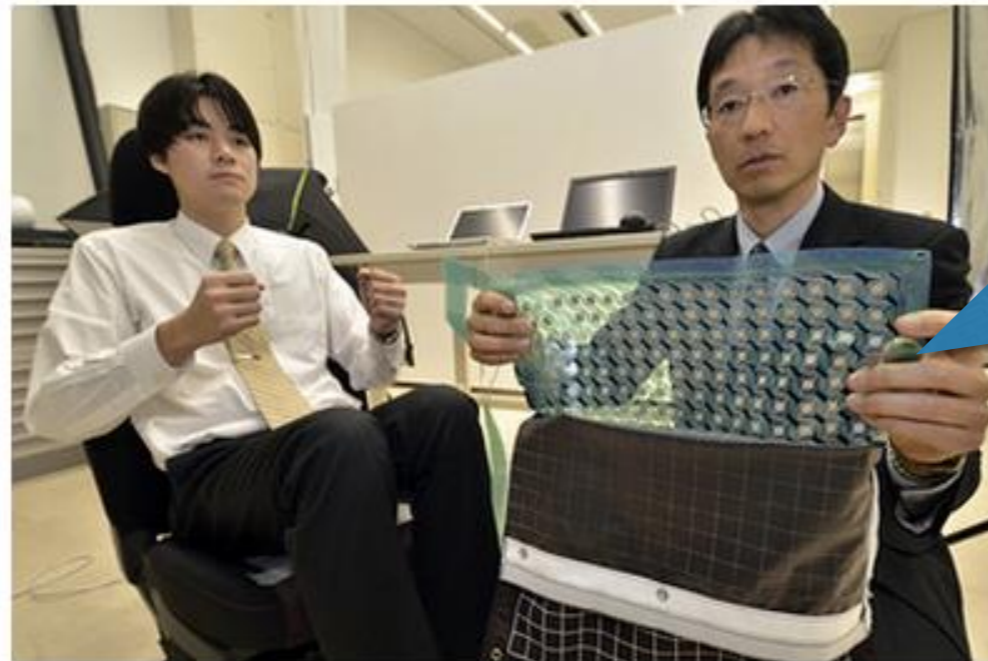
Article

Comments (1)

Email Print



By YOREE KOH [CONNECT](#)



Getty Images

Shigeomi Koshimizu shows his seat sensor.

If Shigeomi Koshimizu has his way, sometime in the not too distant future car owners may control their vehicles by the seat of their pants.

Literally.

Mr. Koshimizu, a mechanical engineering associate professor at the Advanced Institute of Industrial Technology in

Tokyo, has developed an ultra-sensitive sheet that sometime down the line could make the contours of a driver's rear end an integral part of a car's security system.

360 pressure-sensing disks

Unfortunately:

- \$900 each
- 2% false rejection rate

Many current uses of biometrics

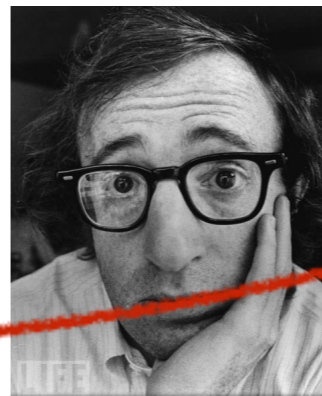
- Law enforcement
 - E.g., FBI database of fingerprints
- Government services
 - E.g., delivery of welfare / social services
- Traveler authentication
 - E.g., passports, Global Entry
- Unlocking your mobile phone
 - E.g., iPhone
- Securing national treasures
 - E.g...



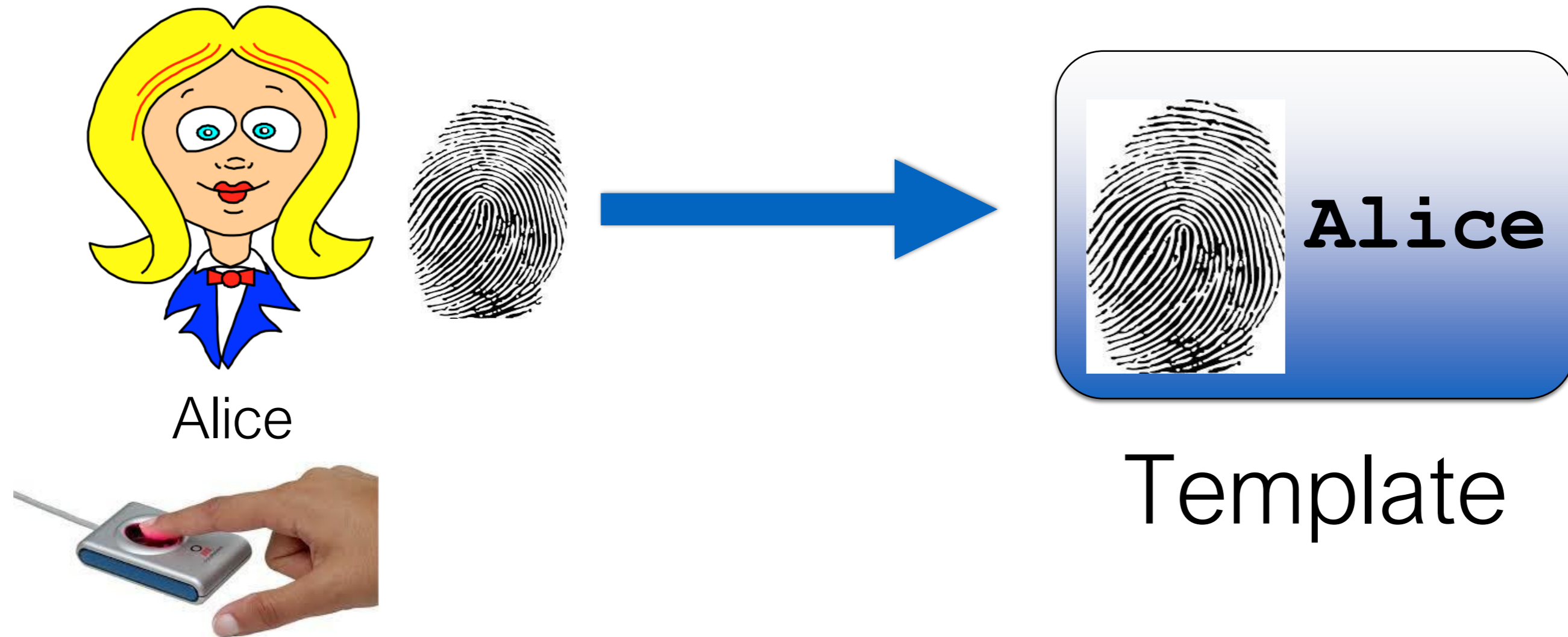
How does biometric authentication work?

Two goals for biometrics

- Identification
 - Goal: Learn a person's identity
 - E.g., identify criminal from fingerprint or DNA at crime scene
- Authentication
 - Goal: Determine whether claimed identity is correct
 - E.g., this is really Woody



Registration

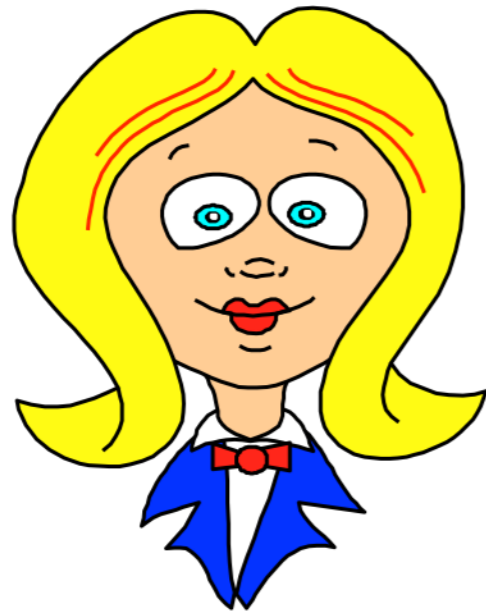


Template is stored



- Stored in, e.g.,
- mobile device
 - database
 - smartcard

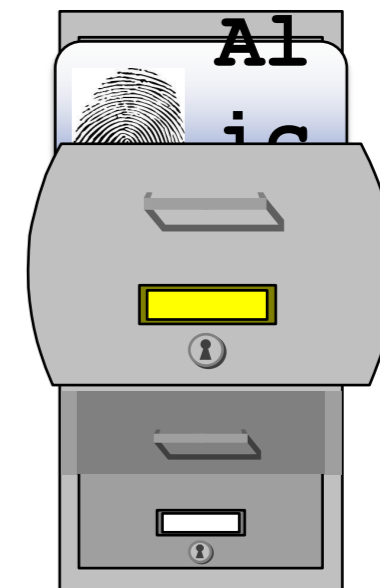
Authentication



Alice



It's Alice!!!



Match is “fuzzy”

- Every time a biometric is presented, it looks slightly different
- E.g., fingerprint:
 - Rotation
 - Pressure
 - Angle of presentation
 - Chapping (NYC winters)
- And it may not work for everyone
 - E.g., people with small fingers, bricklayers

Key concepts

- **False acceptance rate (FAR)**

...or “fraud rate”

- Probability that wrong biometric or forgery (e.g., fingerprint) is accepted

- **False rejection rate (FRR)**

...or “insult rate”

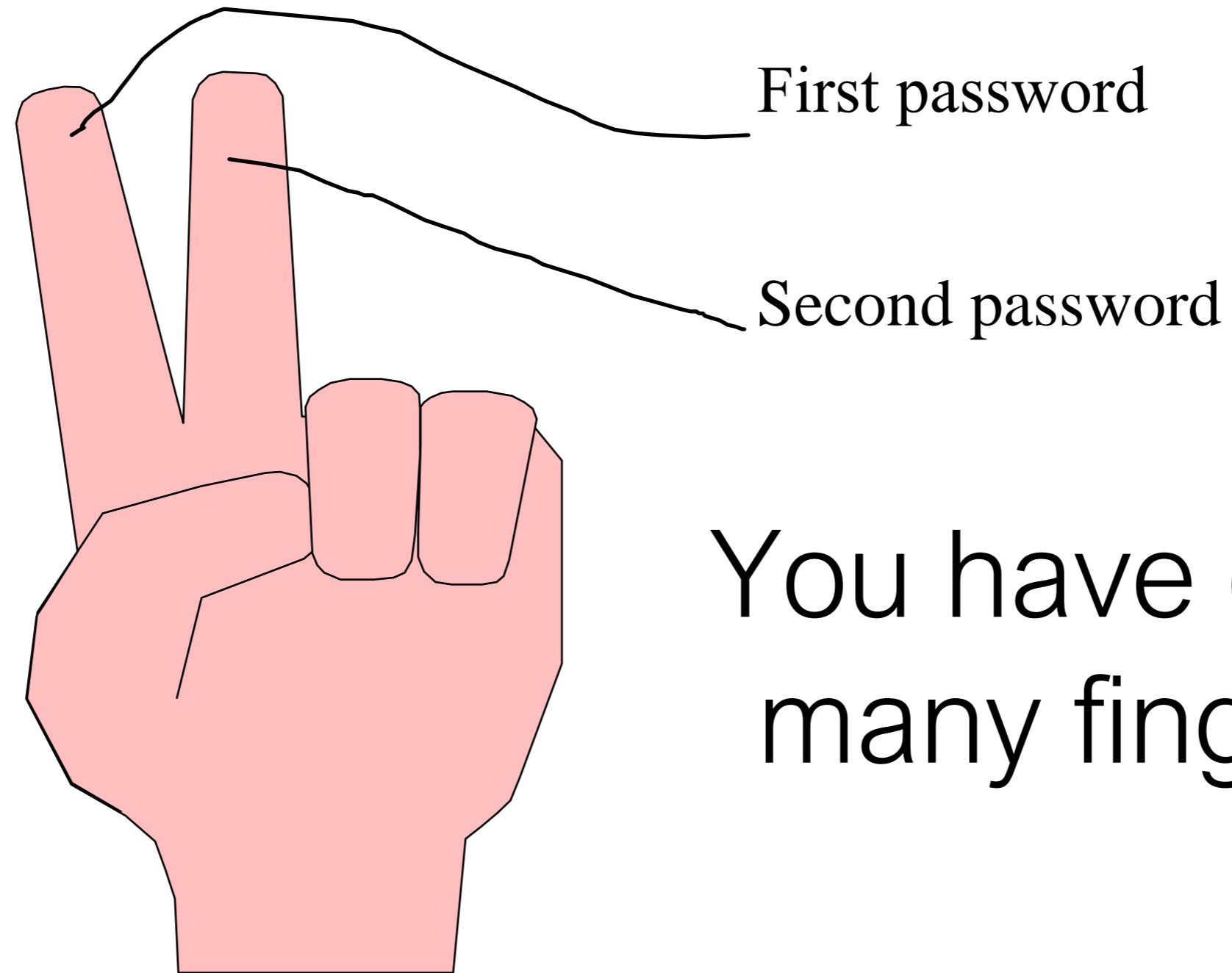
- Probability that valid user is rejected
- U.K. banks set an FAR of 1%, insult rate of 0.01% [R. Anderson, *Security Engineering*]
 - ...showing the emphasis on **convenience over security**
- iPhone TouchID has claimed (2013) an FAR of 0.002%
 - So in this setting, fingerprint is far from *unique*

Big security architecture questions

- Where is the template stored?
- How is the template protected?
- Where is the match performed?

Security is important because...

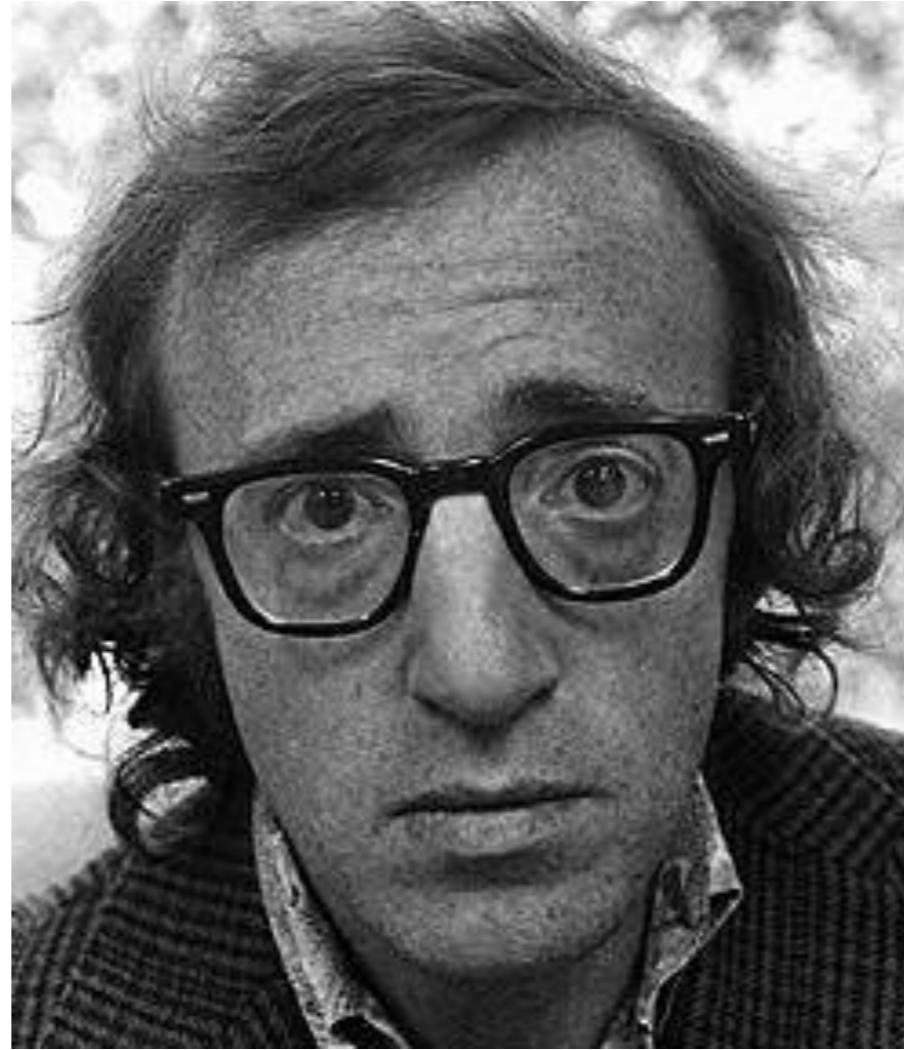
Revocation of biometrics is hard



You have only so many fingers...

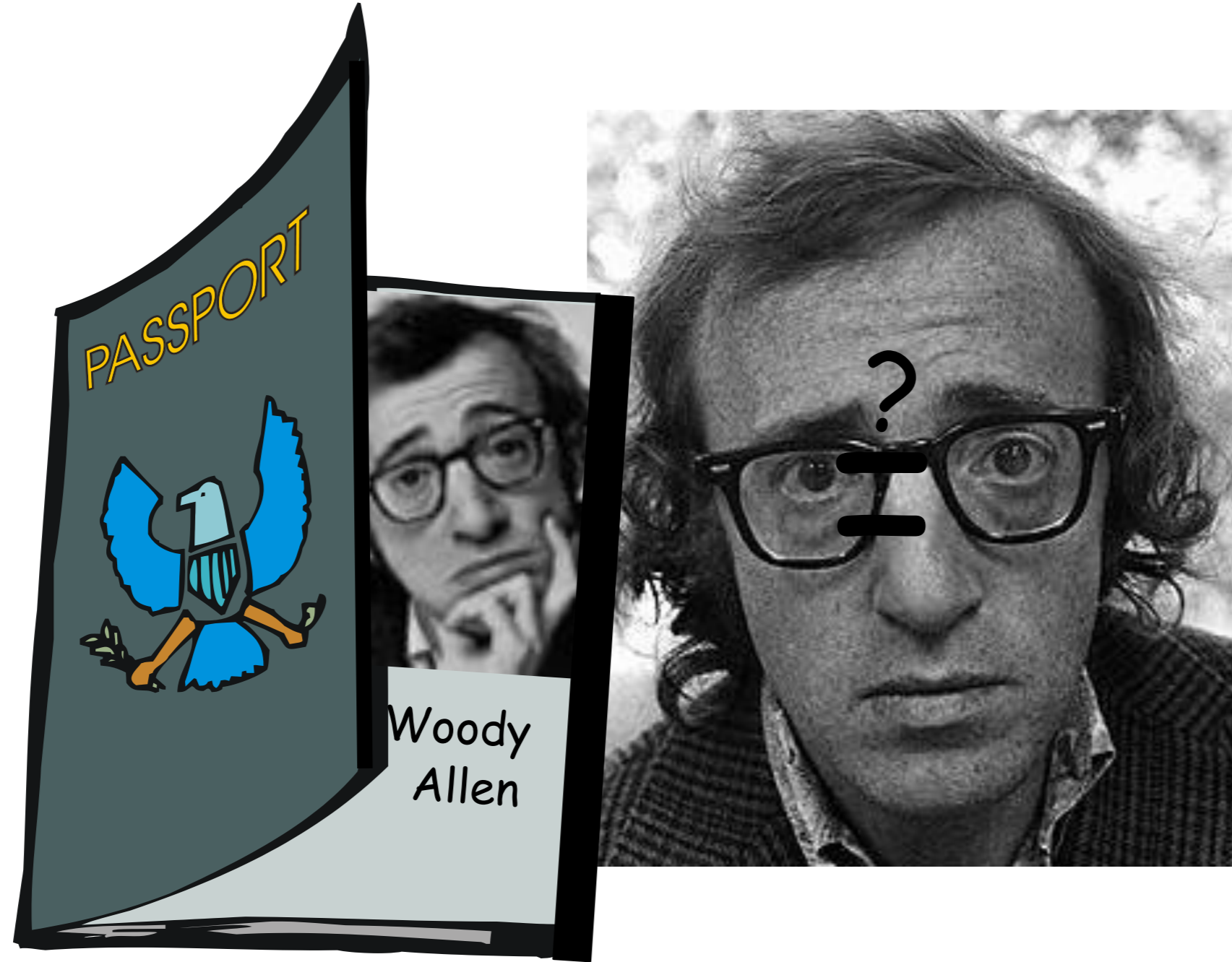
Biometric secrecy

Classical biometric authentication



Is it Woody? Yes, it's Woody!

Classical biometric authentication



Is it Woody? Yes, it's Woody!

Classical biometric authentication



|| ?



Hello,
Mr. Woody Allen



In these scenarios, biometric data need not
be kept secret

- Spoofing is difficult with human oversight
- Indeed, your face is public anyway
- (Assuming, of course, that passport is not a forgery)

But what happens when...

A human-guided process



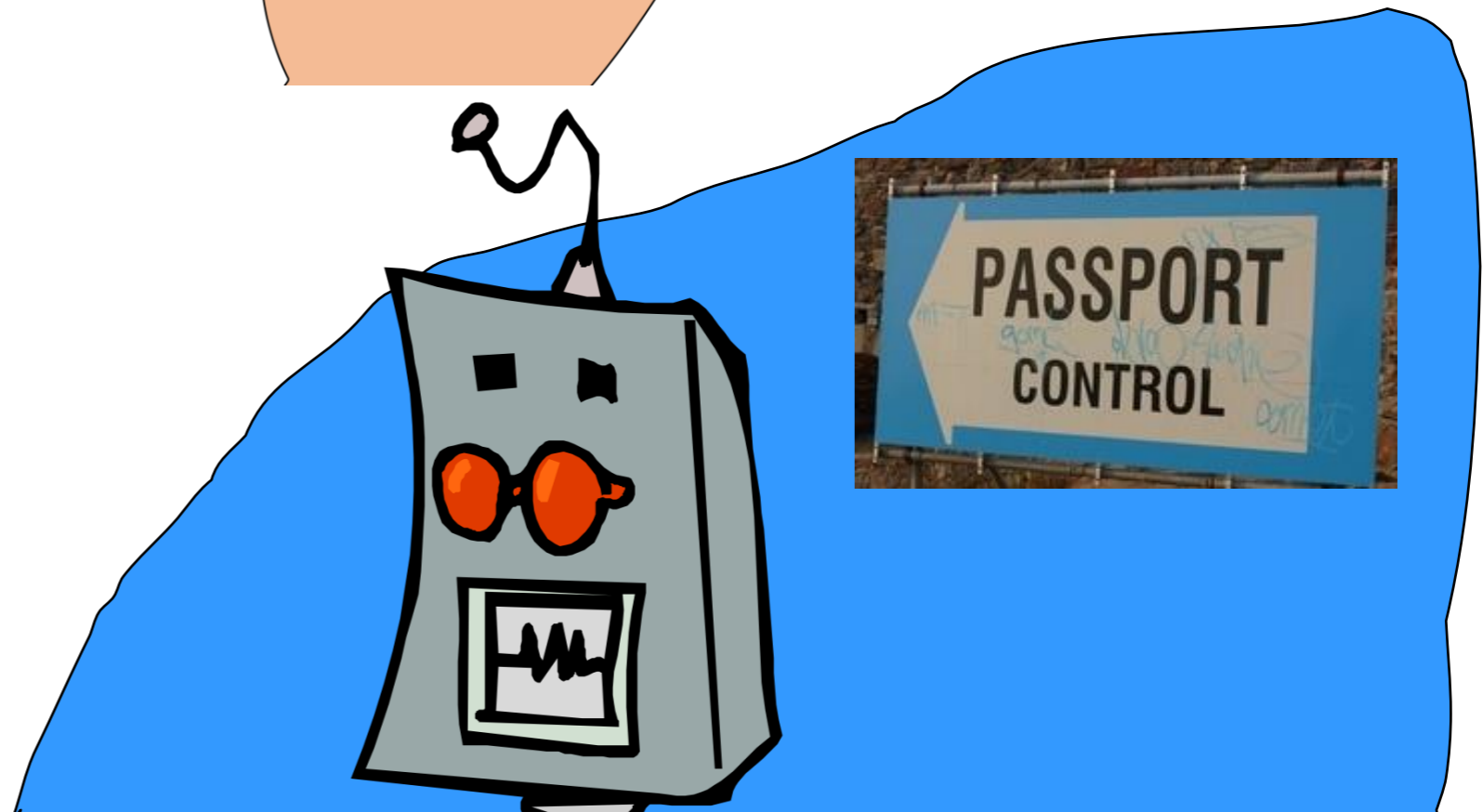
|| ?



Becomes automated?



|| ?



Secrecy of biometric data is now more important to security

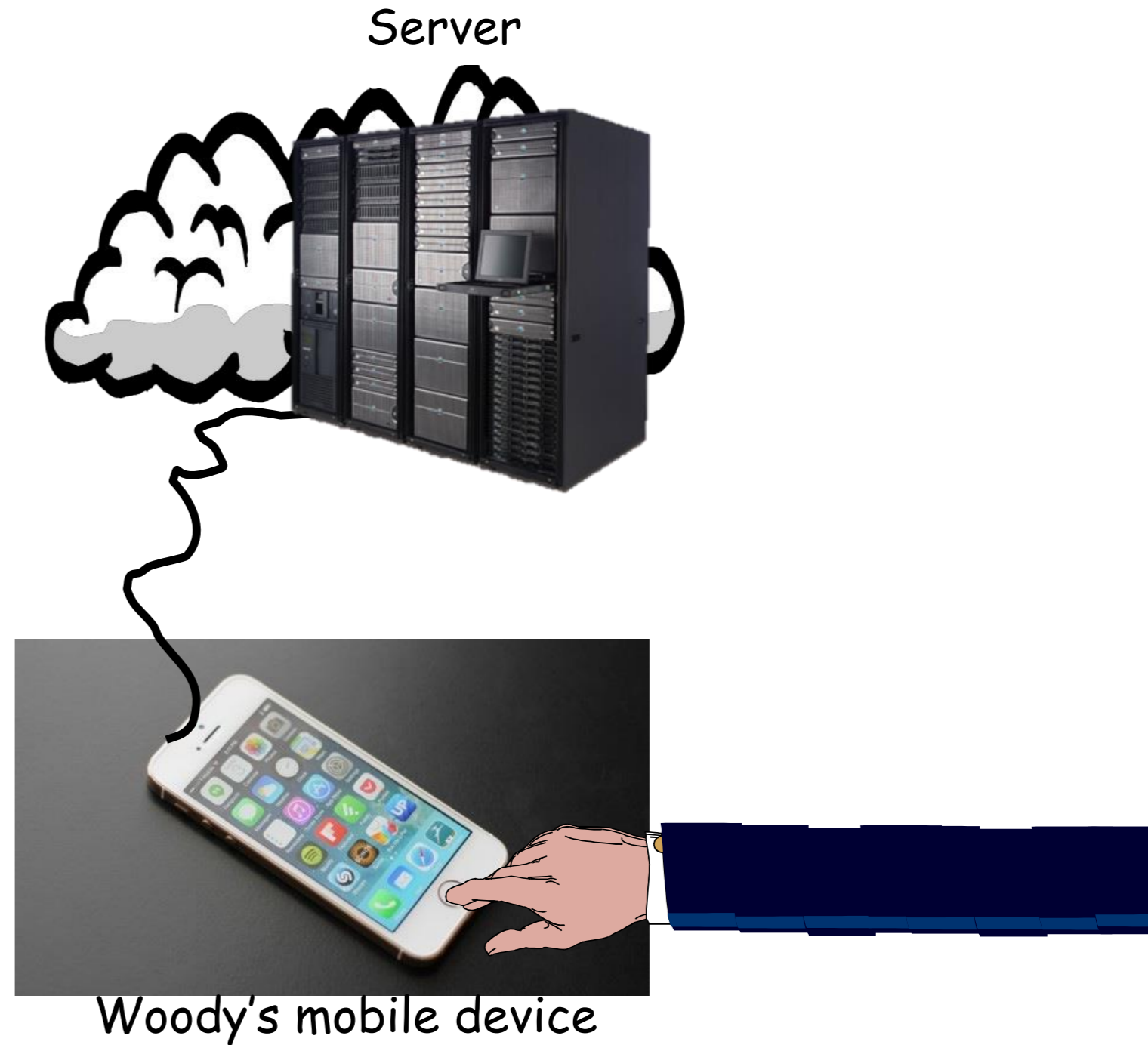
- **Reason 1:** Automation will mean relaxation of human oversight
 - More opportunity for spoofing
 - Holding up photos instead of presenting faces, fake fingerprints, etc.



Schiphol airport: Iris scanning

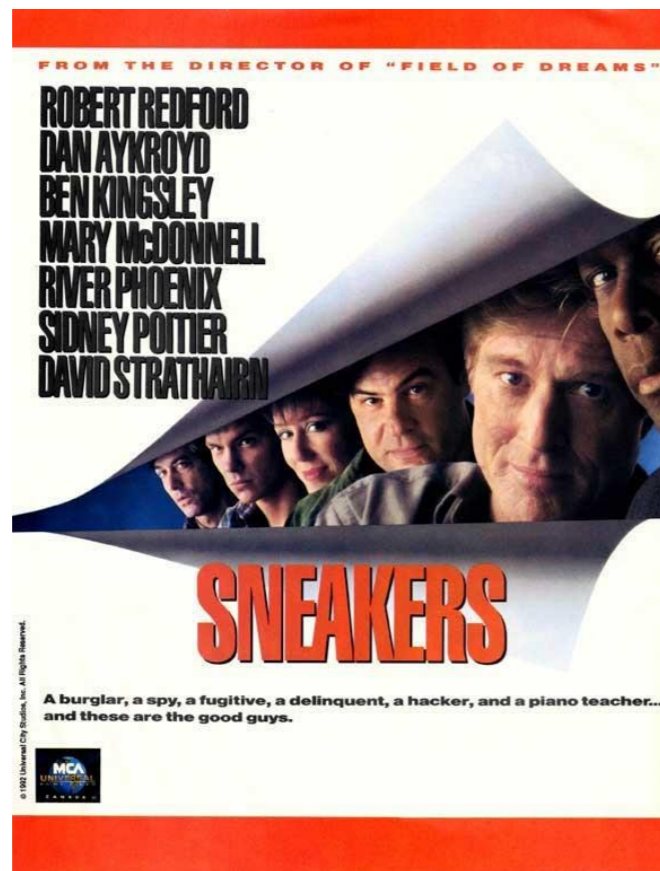
Secrecy of biometric data is now more important to security

- Reason 2: On-device and remote authentication

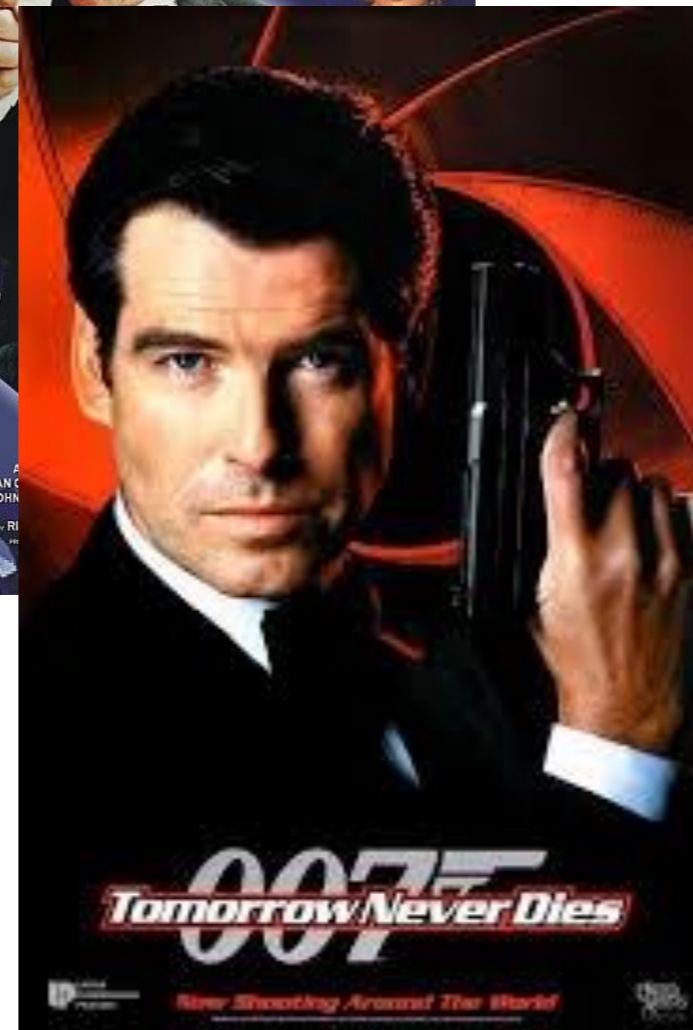


Attacks

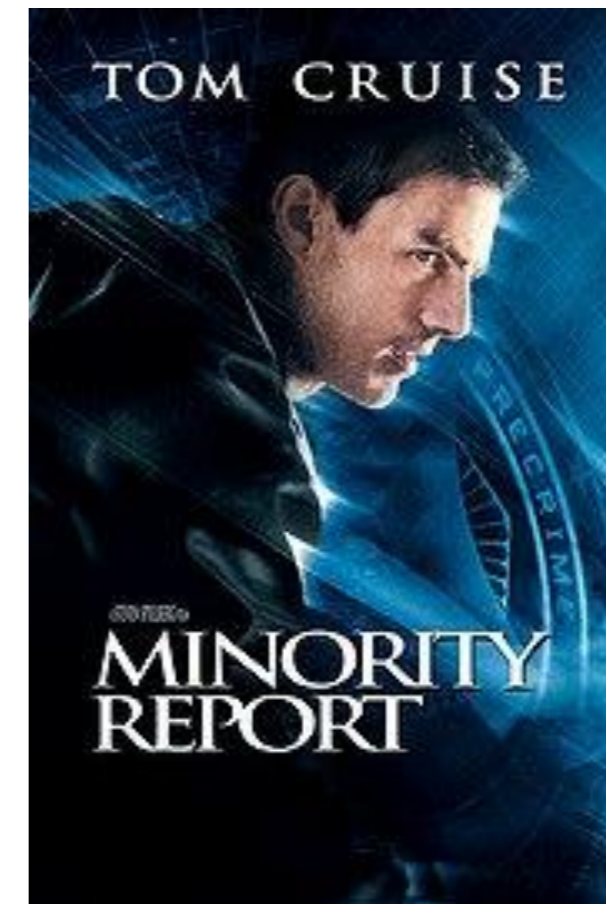
Some attacks



“My voice is my passport”



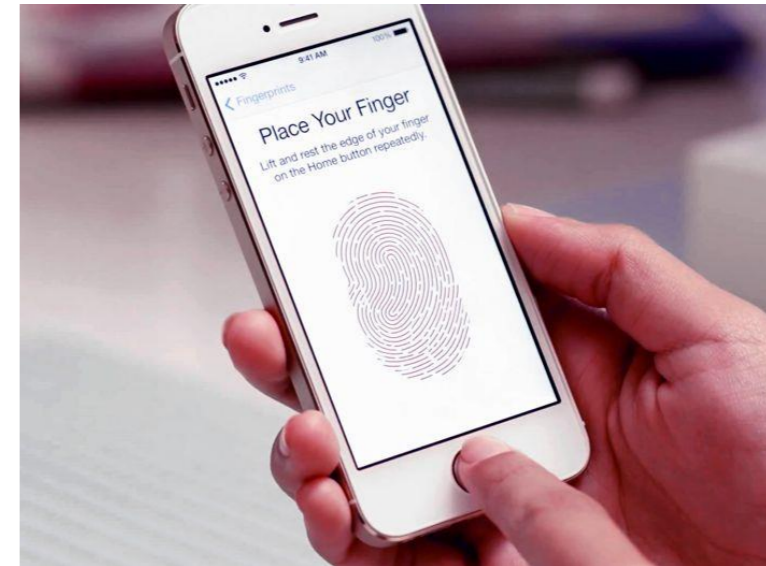
Fake fingerprints



Eyeballs in a bag

Spoofing / cloning

- Apple TouchID
- Chaos Computer Club hack (Starbug)
 - A week or two after TouchID release
 - Moderately sophisticated attack converts fingerprint photo to wood glue prosthetic
 - [Video](#)



Spoofing: Gummy fingers

Making an Artificial Finger from Residual Fingerprint

Materials

A photosensitive coated Printed Circuit Board (PCB)
"10K" by Sanhayato Co., Ltd.



320JPY/sheet

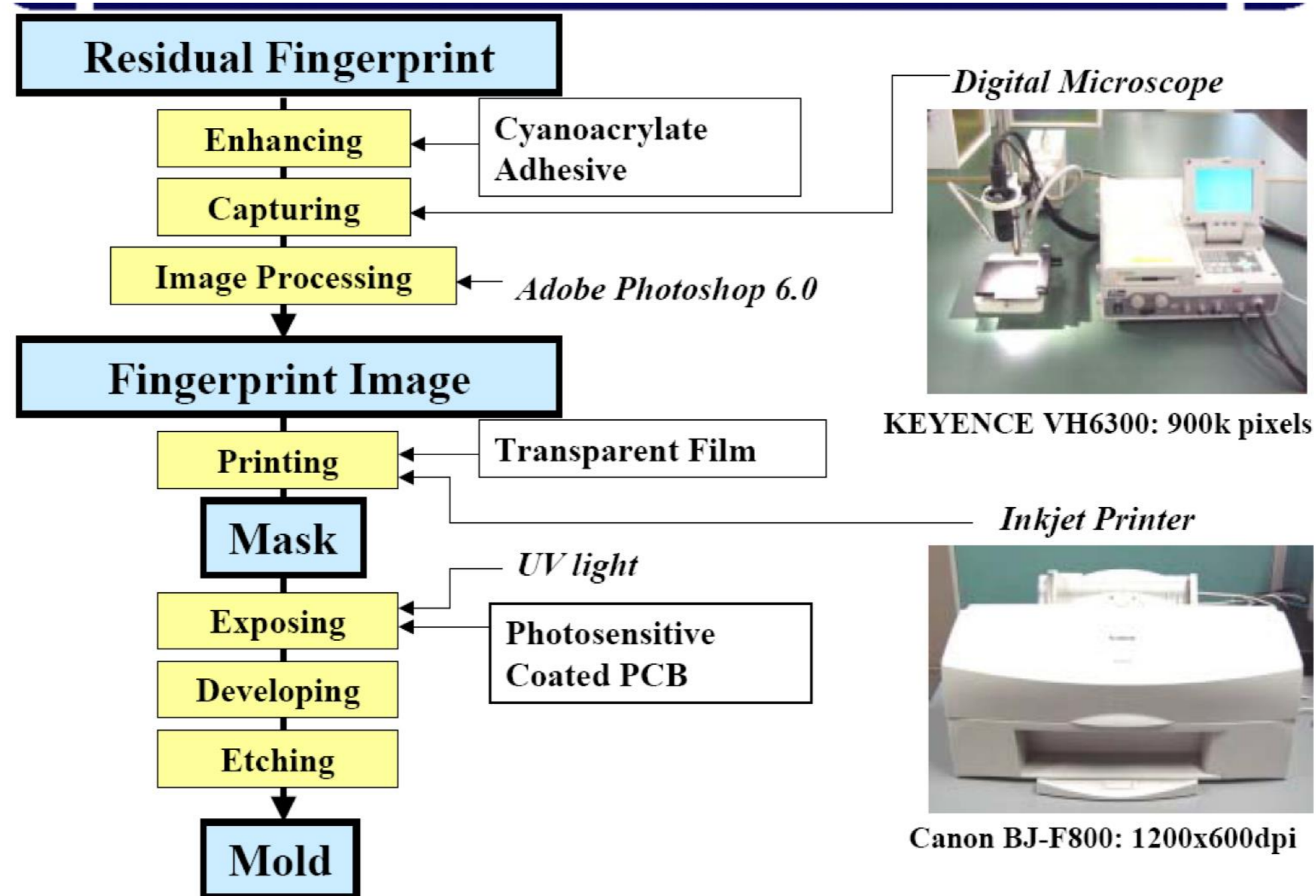
Solid gelatin sheet
"GELATINE LEAF"
by MARUHA CORP



200JPY/30grams

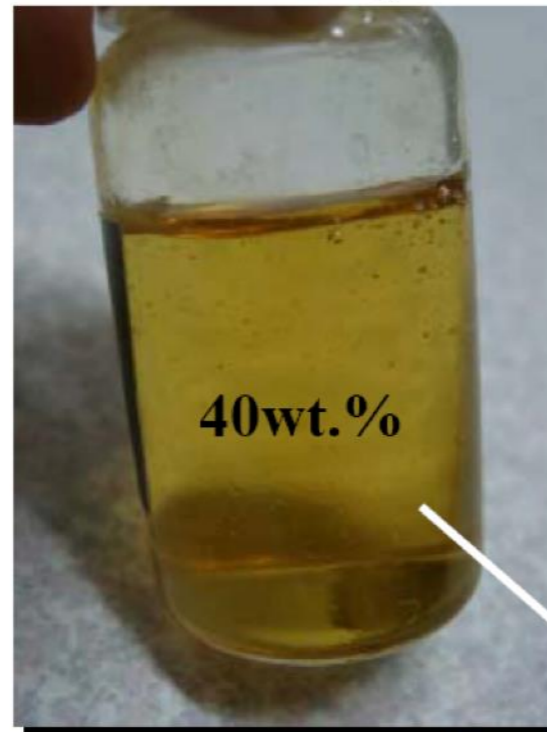
Yokohama Nat. Univ. Matsumoto Laboratory

Spoofing: Gummy fingers

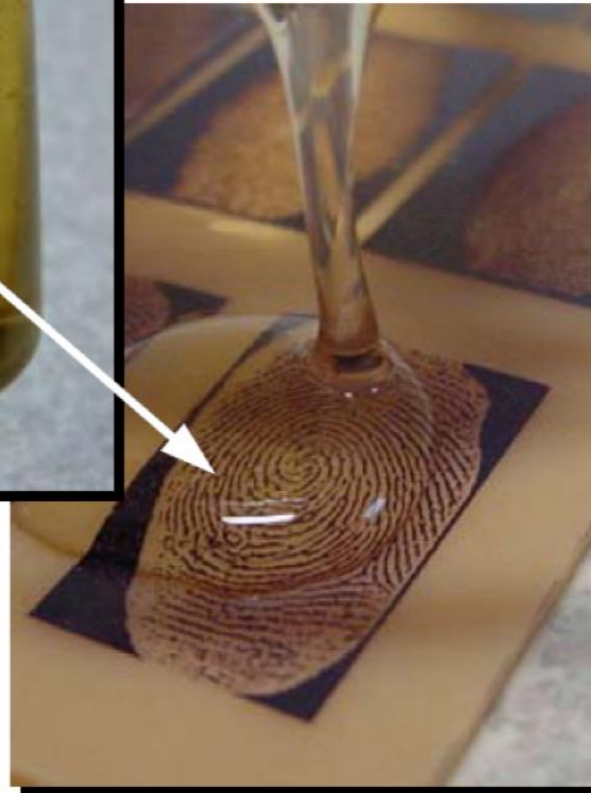


Spoofting: Gummy fingers

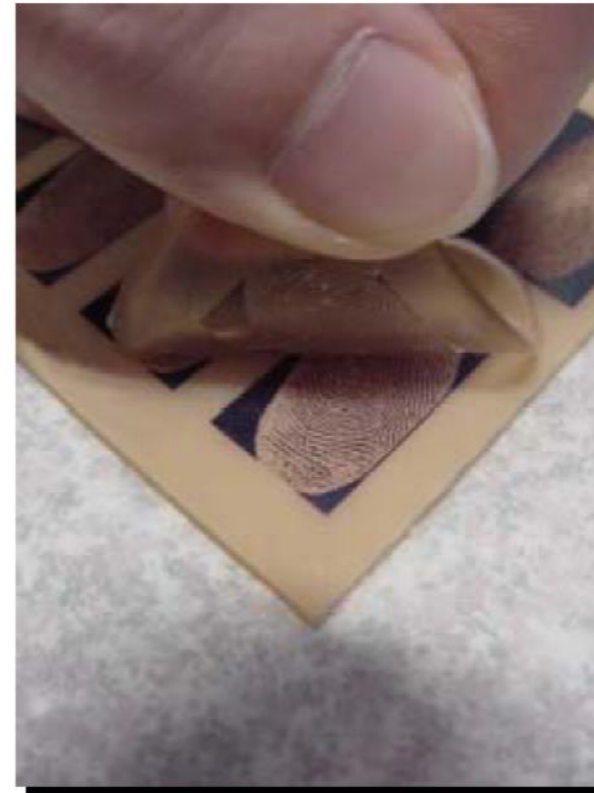
Gelatin Liquid



Drip the liquid onto the mold.



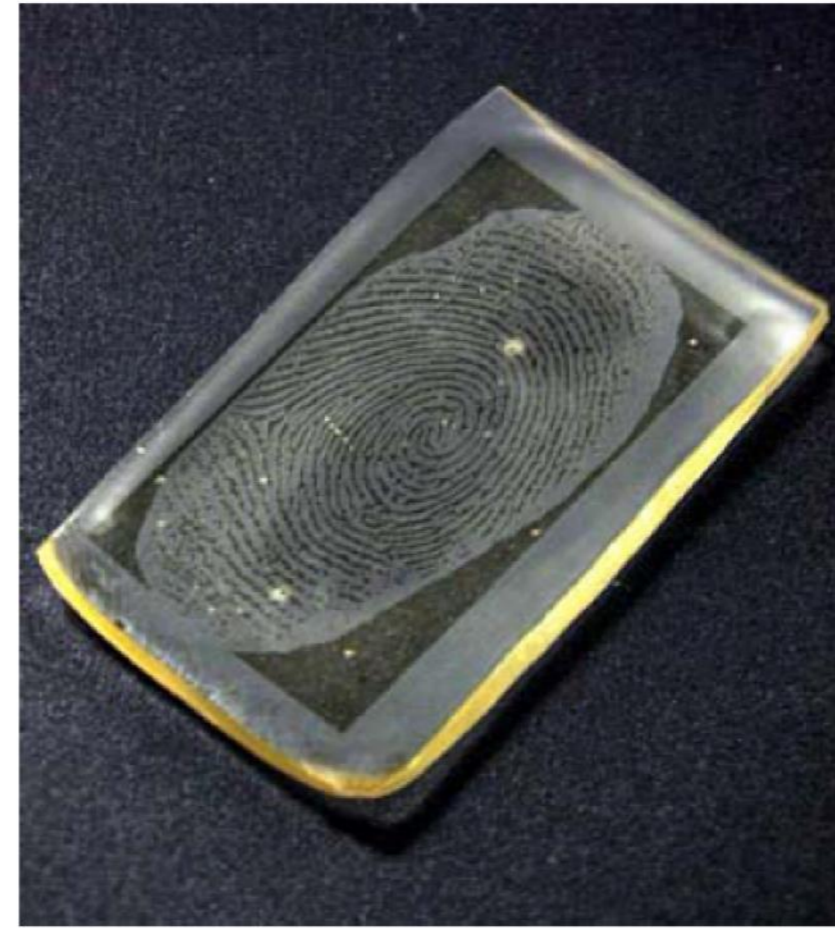
Put this mold into a refrigerator to cool, and then peel carefully.



Spoofing: Gummy fingers



Mold: 70JPY/piece
(Ten molds can be obtained
in the PCB.)



Gummy Finger: 50JPY/piece

Maybe we want weak security...



The Register

Data Center Software Networks Security Business Hardware Science Bootnotes Video Forums We
Financial News Small Biz CIO Media Policy Jobs

BUSINESS > MEDIA

Carjackers swipe biometric Merc, plus owner's finger

Sometimes you might not want such great security...

By John Lettice, 4 Apr 2005

[Secure remote control for conventional and virtual desktops](#)

A Malaysian businessman has lost a finger to car thieves impatient to get around his Mercedes' fingerprint security system. Accountant K Kumaran, [the BBC reports](#), had at first been forced to start the S-class Merc, but when the carjackers wanted to start it again without having him along, they chopped off the end of his index finger with a machete.

Although security systems of this sort are typically fitted to high end cars (because of import duties, Kumaran's car is reported to have been worth \$75,000 "second-hand" - under the circumstances, we think we'd have said 'at resale'), they're not in essence

Track

Share 10

Tweet 4

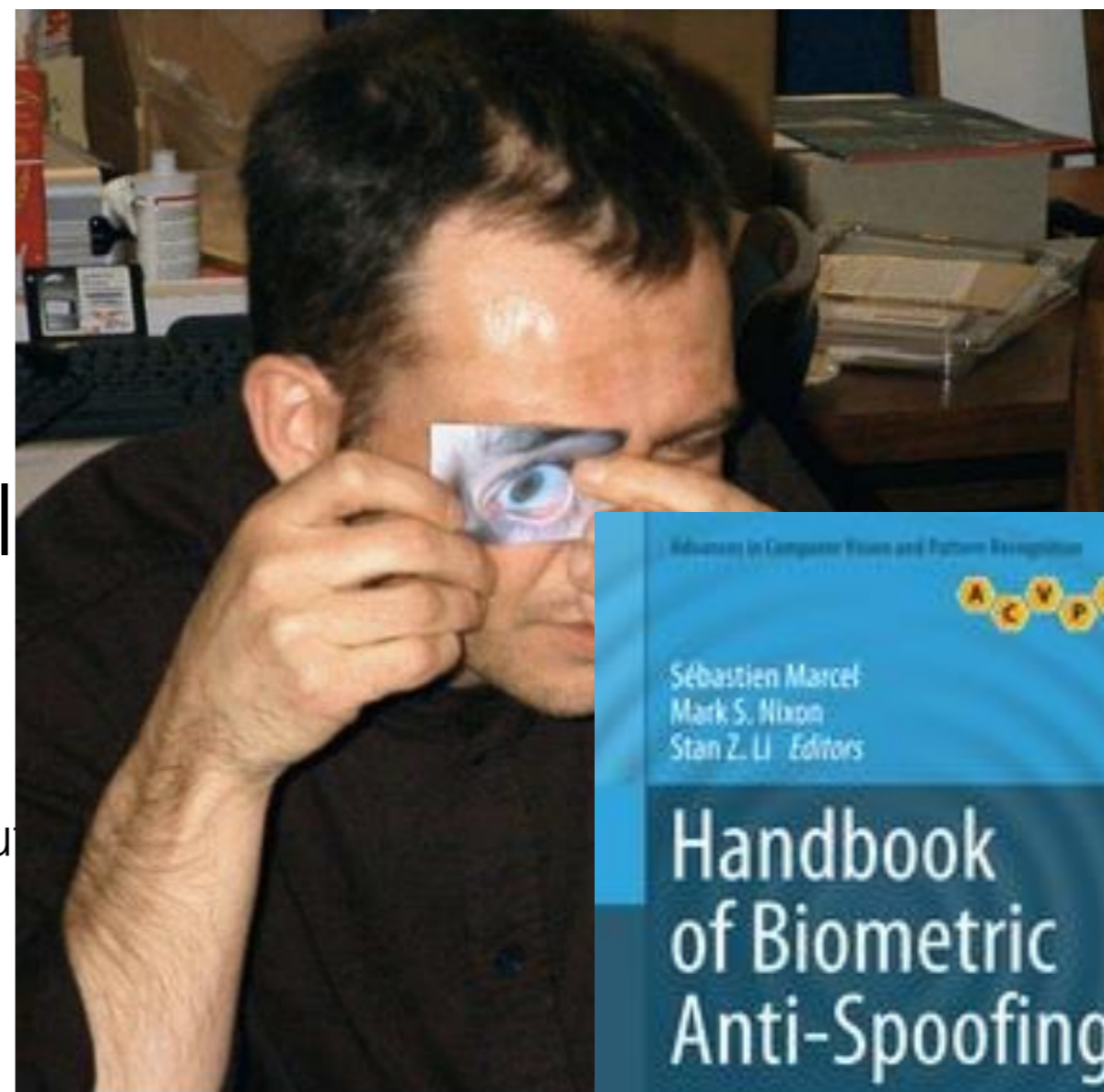
Share 0

Or perhaps we want liveness detection

- In fingerprint readers
 - Capacitance
 - Color changes
 - Perspiration
- For iris scanning
 - Pupil dilation

But that doesn't always work either

- Gummy fingers are transparent and thus expose color
- For iris you can check pupil dilation, but...
- L. Thalheim, J. Krissler, "Body Check: Biometric Access Protection Devices and their Programs Put to the Test", c't magazine, November 2002.
- Thankfully, there's a handbook...



Things can get grotesque

“...in countries like South Africa where fingerprints are used to pay pensions, there are persistent tales of ‘Granny’s finger in the pickle jar’ being the most valuable property she bequeathed to her family.”

[R. Anderson, *Security Engineering*, Chap. 15]

GIZMODO

Chinese Woman Fools Scanners By Surgically Switching Her Fingerprints

Sean Fallon
Filed to: CRIME 12/08/09 8:00pm



Yup...

CREATING ANOTHER SMART
DEVICE ON WHEELS.
IT'S AWESOME



Business Impact

Iris scanner can distinguish dead eyeballs from living ones

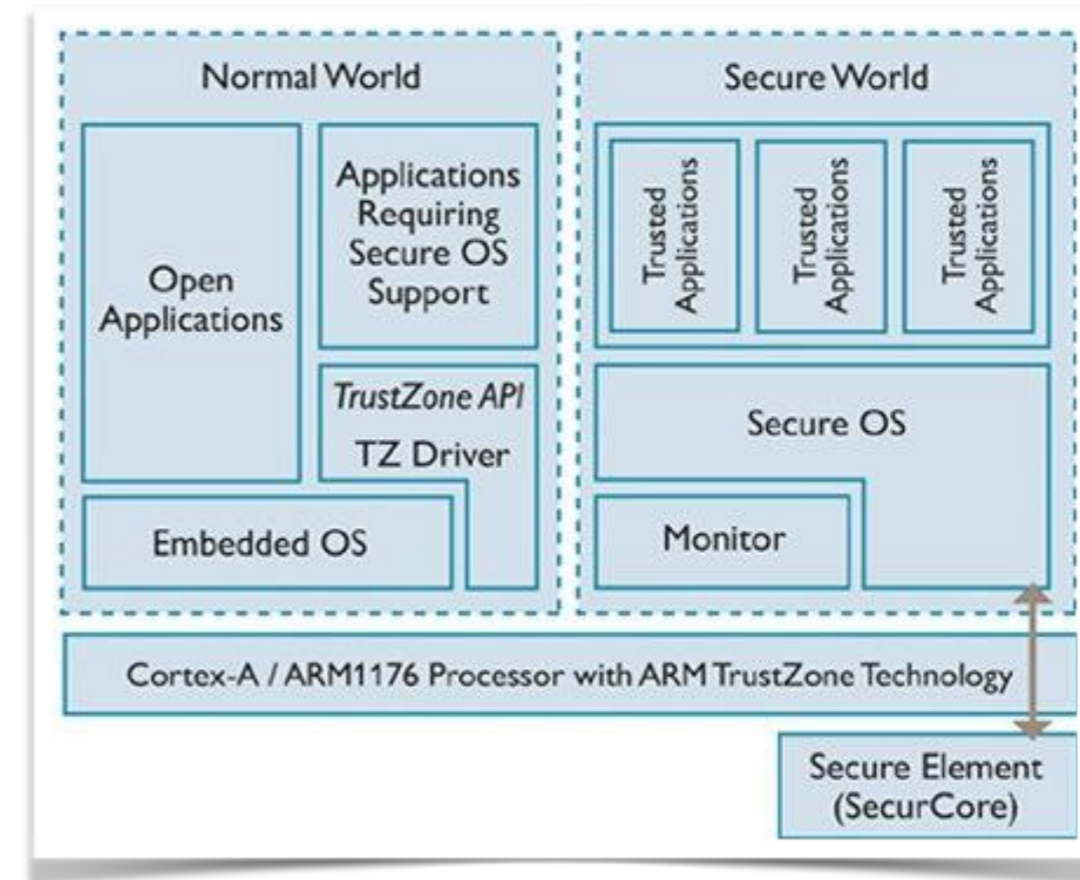
In theory, an iris scanner can be hacked using an eyeball plucked from the victim. Now researchers have trained a machine-vision system to tell the difference between dead irises and live ones.

by Emerging Technology from the arXiv July 24, 2018

Deployments and deployment challenges

Touch ID

- Uses secure hardware
- Introduced with ARM A7 with “Secure Enclave”
- Coupled with NFC in Apple Pay



Arm TrustZone

HTC caught storing fingerprints AS WORLD-READABLE CLEARTEXT

Android biometric banks more Fort Nope than Fort Knox.



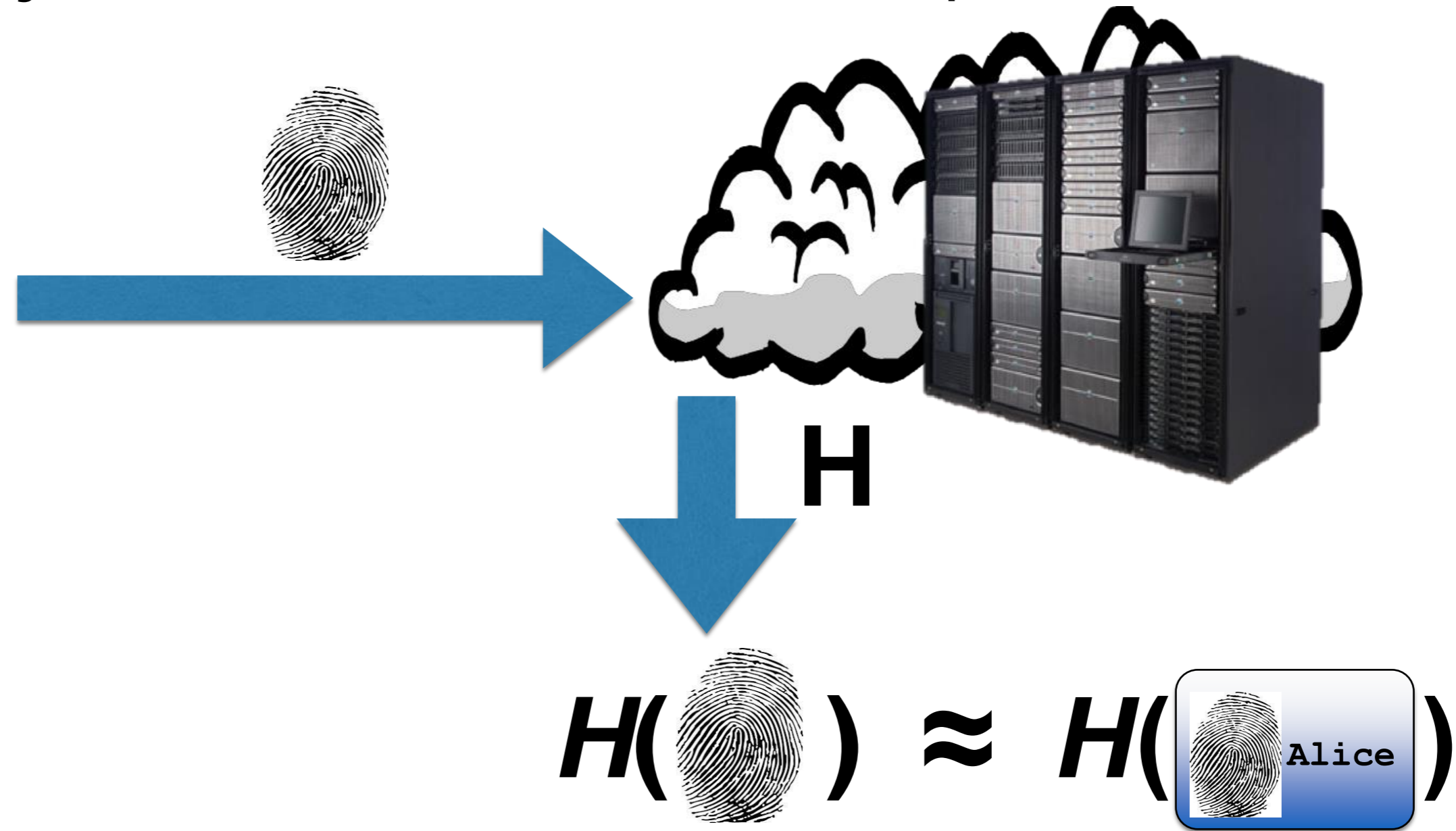
10 Aug 2015 at 04:26, [Darren Pauli](#)

India's AADHAAR system

- Holds fingerprints, iris scans, and facial scans of 600+ million people
- Used to deliver subsidies, deliver wages to bank accounts, control fraud, etc.
- Very different security problem than iPhone
 - iPhone generally holds one user's template
 - AADHAAR holds entire country's templates!
- Compromise endangers security of entire country!
- How to protect templates?

Protecting big databases of biometric templates?

Ideally, we would *hash* templates



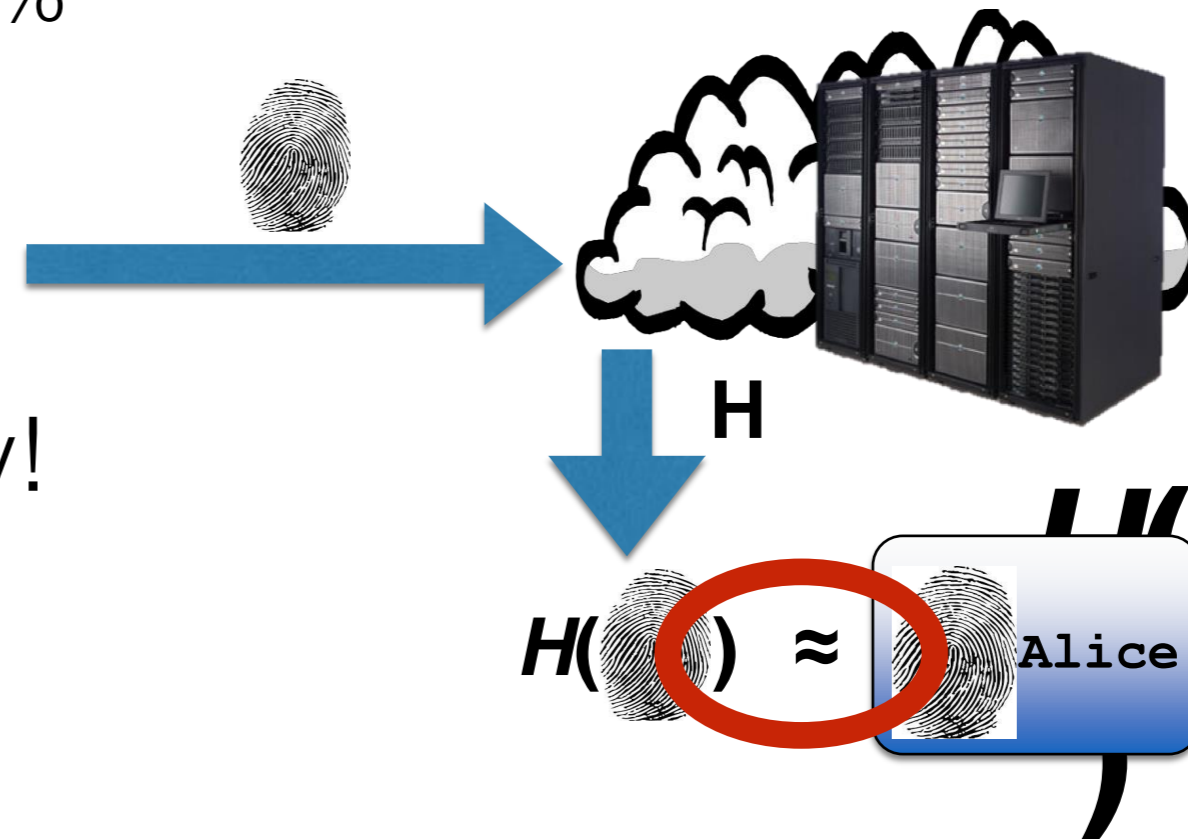
Two problems

1. Hash easily cracked

- FAR → Guessing probability 0.002%
- Weaker than three-character password!
- $\{a\dots z\} + \{A\dots Z\} + \{0\dots 9\}$

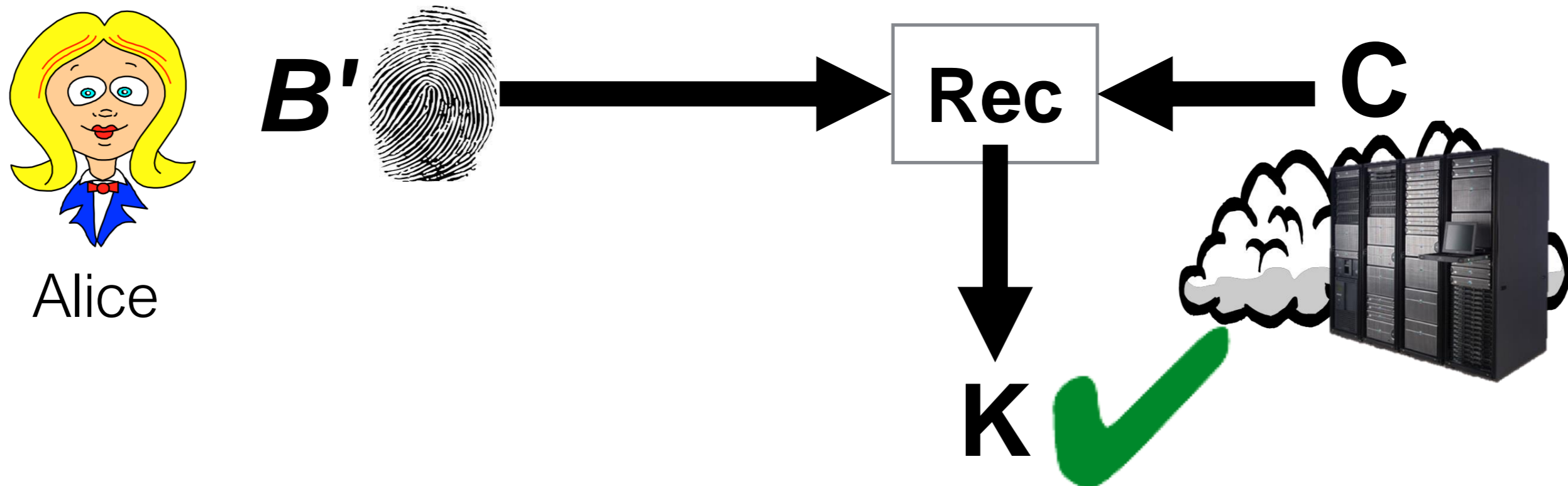
2. Hashing won't work anyway!

- Hash comparisons must be exact
- Same value in ROM cell?
- Remember: Biometrics are "noisy"
- Small reading errors / variations



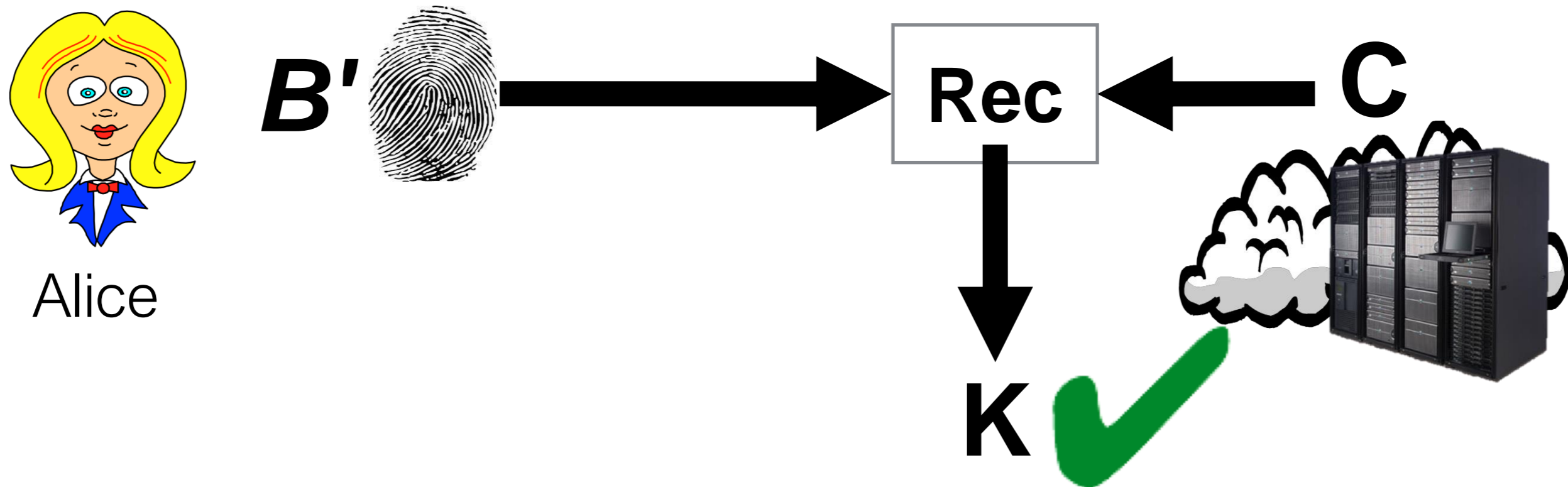
"Fuzzy" cryptography

- Combines error-correcting codes with cryptography
- Server stores only error-correcting information C for each user
 - *Doesn't store biometric template*
- Function Rec (recover) derives consistent key K from noisy biometric B' and C



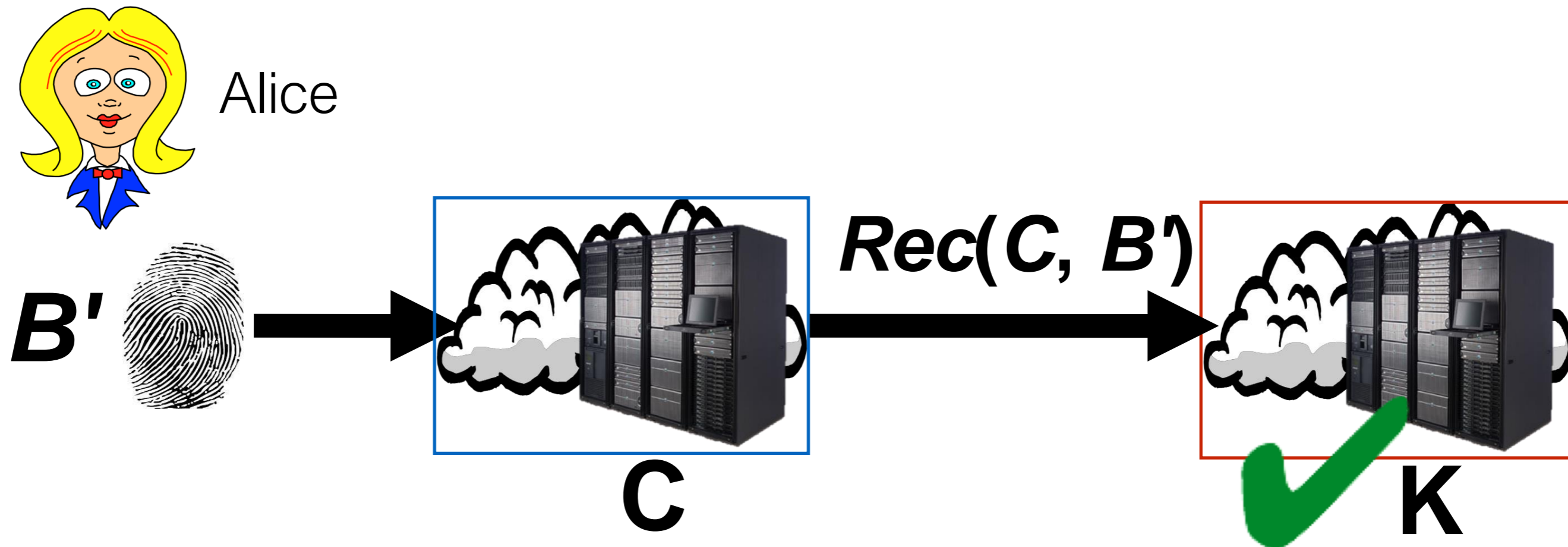
"Fuzzy" cryptography

- But where is K stored?
- Remember: low entropy!
- K on server \rightarrow brute-force attack
 - Attacker tries B' until $B' = \text{Rec}(B', C) = K$



Split-server approach

- Idea: Distribute authentication across two servers
 - Red stores C
 - Blue stores K
- Compromise of Red *or* Blue doesn't break system

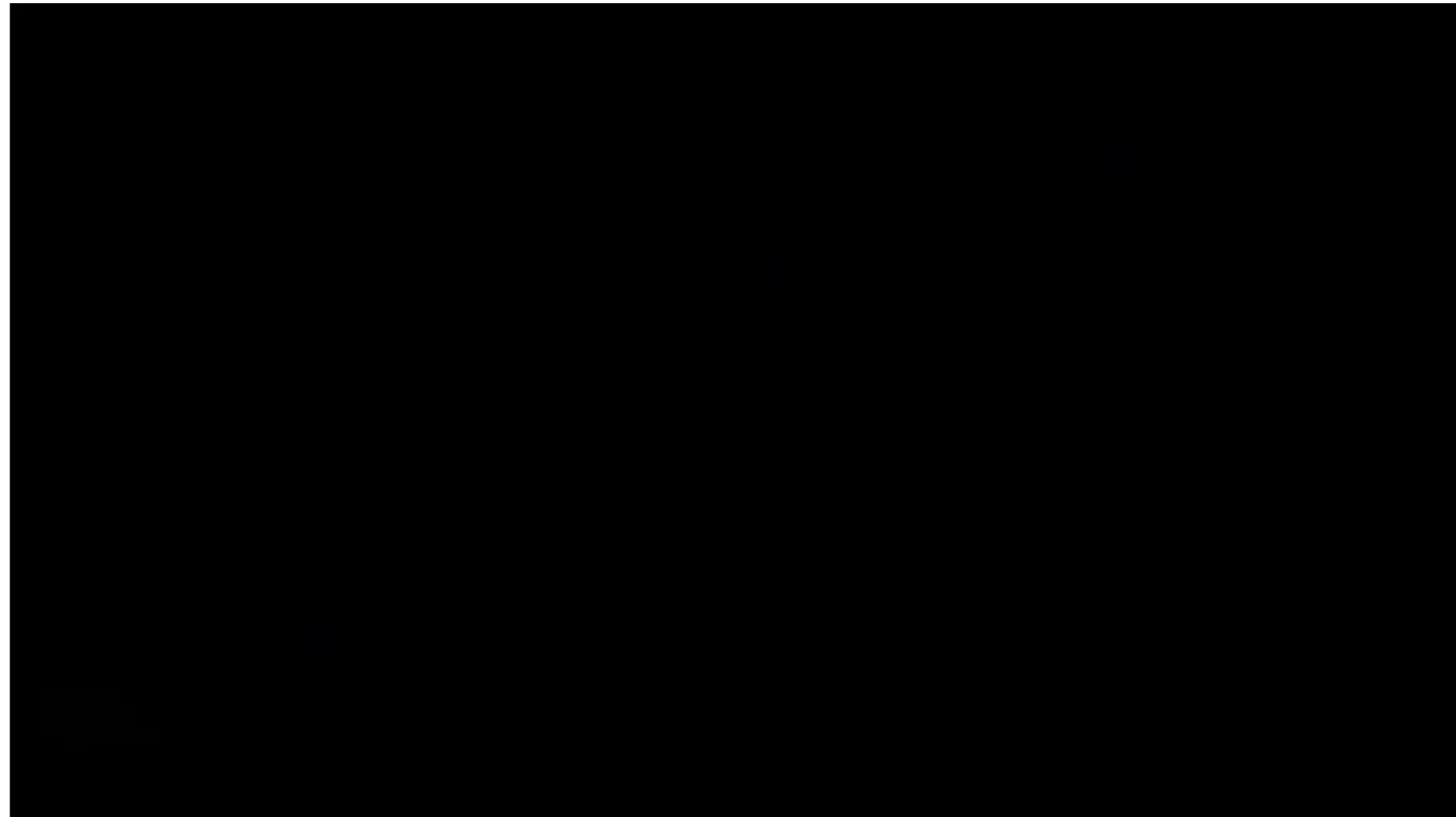


Smartwatches as "prosthetic biometrics"?

- No biometric (yet) in Apple watch
- But heart-rate monitor and other sensors could enable one
- Could smartwatch become "killer authenticator"?
 1. Watch biometrical authenticates user at beginning of day
 2. Watch monitors for detachment
 - If none, user remains authenticated
 3. *Watch authenticates for the user* via NFC, Bluetooth, etc.



Smartwatches as "prosthetic biometrics"?

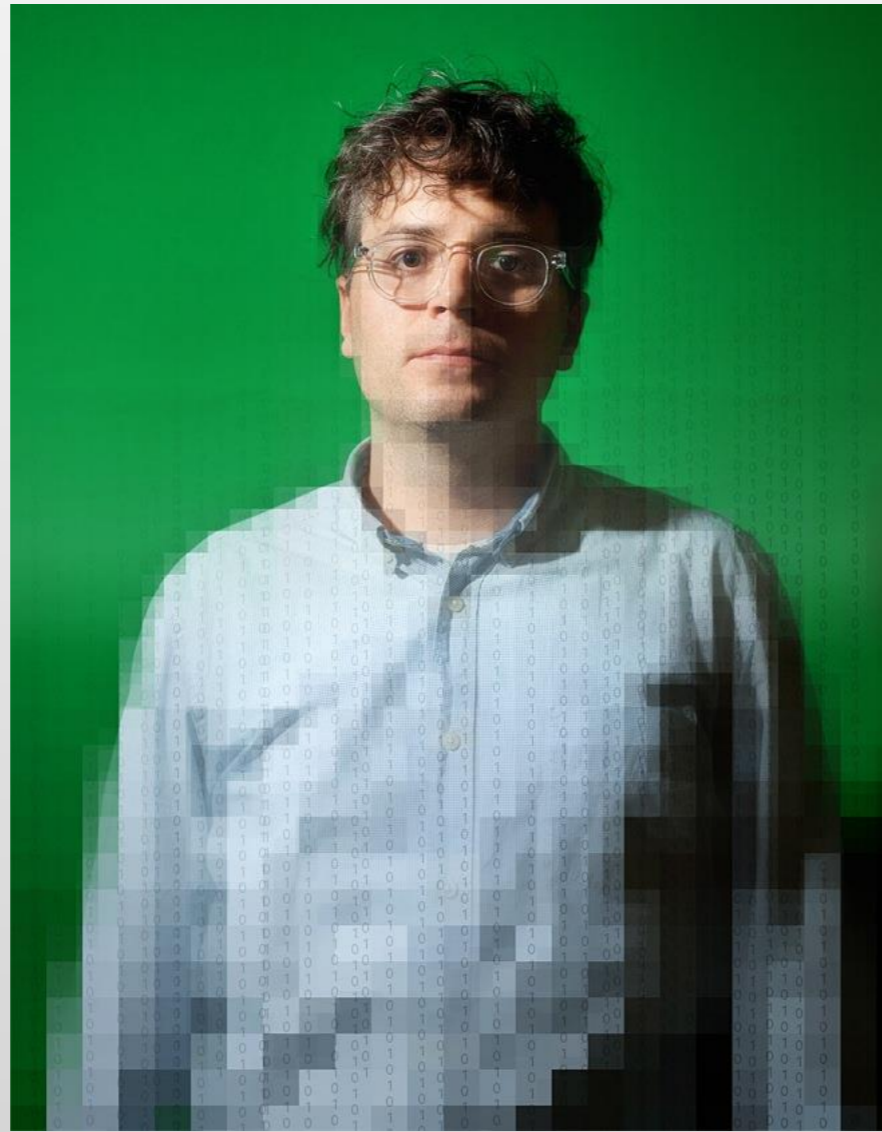


Biometrics takeaways

- Biometric authentication measures biological feature to confirm identity
- Many flavors: fingerprint, iris, face, etc.
- Convenient
 - Hard to forget at home
 - Easy to use
- Some drawbacks
 - Spoofing
 - Theft can hurt
 - Accuracy far from ideal (FAR / FRR)
 - Hashing not viable protection
- TouchID bringing biometrics into mainstream...

Authentication Tokens

Mat Honan's recommended solution

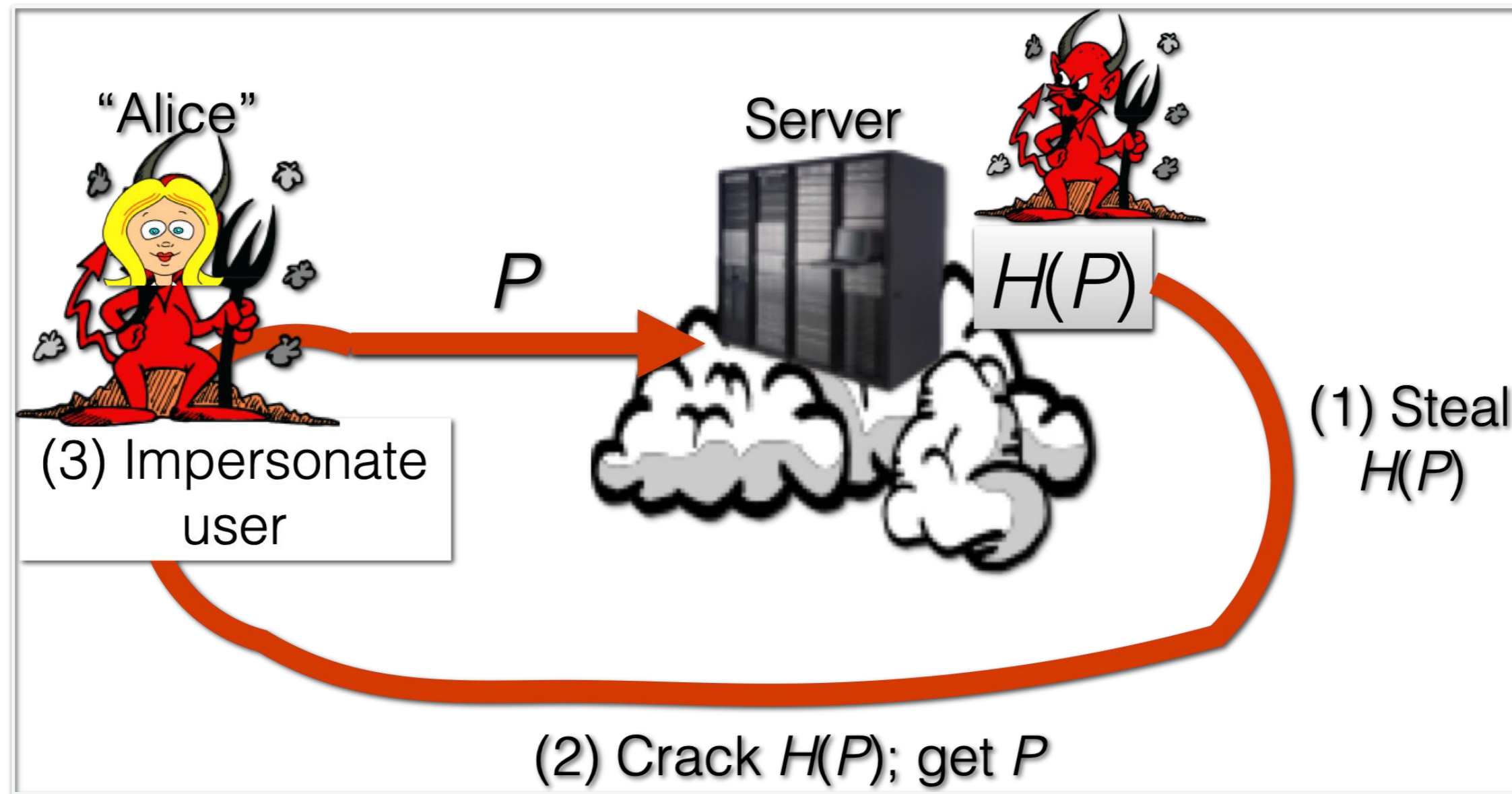


Google Authenticator

In the beginning was
the password
(and it's still here)


“Something you know” authentication factor

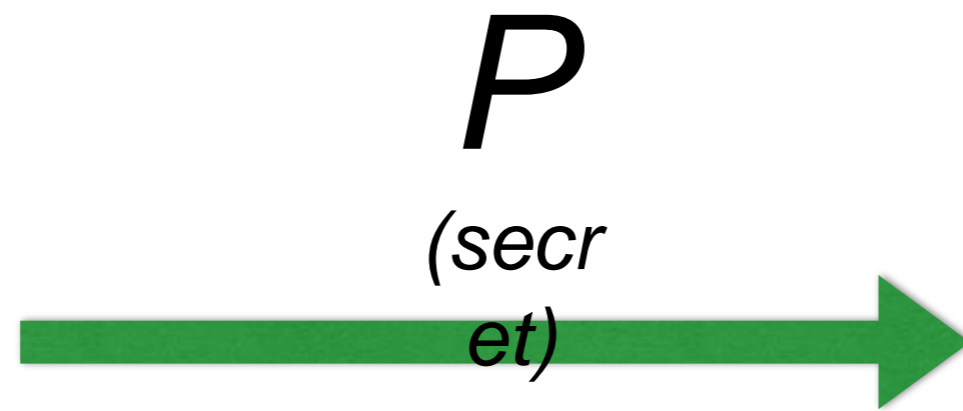
Remember the password cracking problem



But even if the server is well protected, passwords can still be stolen from *the user*.

Eavesdropping

Alice

 P
(secret)

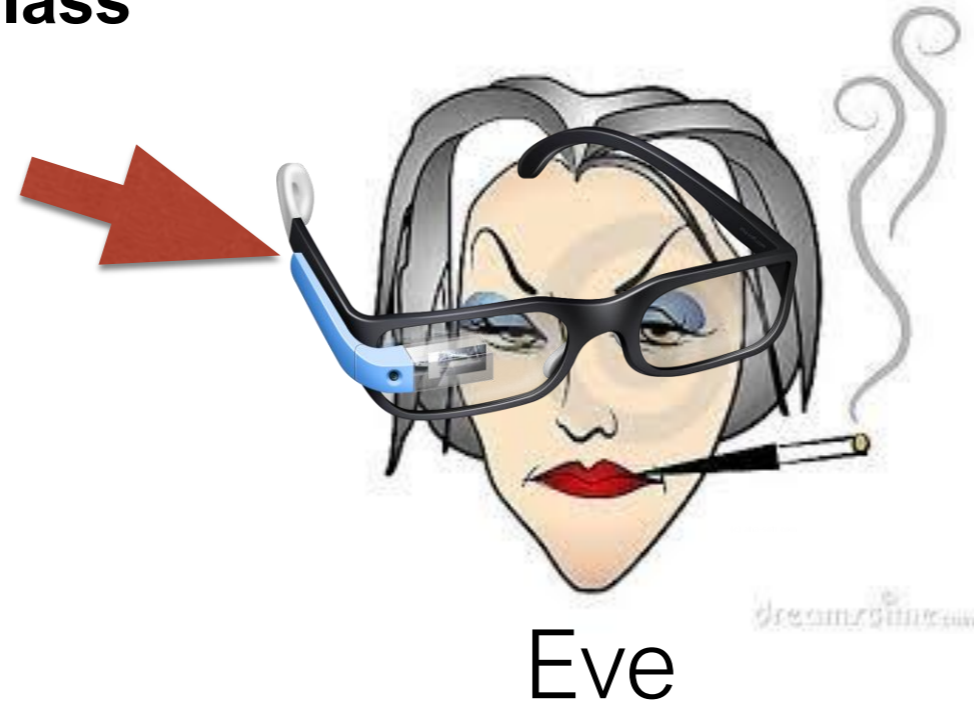


Eve




Sticky notes

Google Glass



Alice

Visual capture

Malware



Alice



P
(secret)



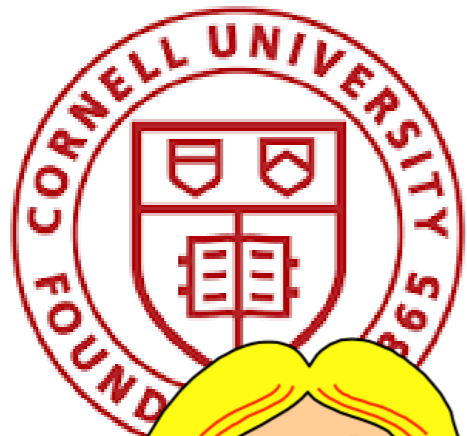
Eve

E.g., keystroke logger

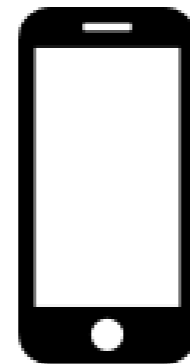
Phishing



Social engineering



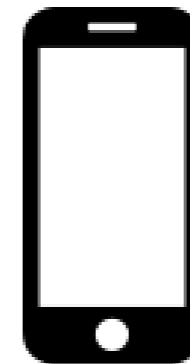
Alice



"Hi, Eve. This is Cornell IT. (Go Big Red!!) A hacker has broken into your account, and we need to change your password..."



Eve



Idea 1: User-driven password changes

- Common interval: 90 days
- May help sometimes, but...
 - 90 days is a long time!
 - Helps users forget passwords
 - Estimated \$150 cost per user per year
 - META group estimate: 1.75 help desk calls a month; Gartner group: 30% of calls are for password resets; Forester research: \$25 / call
 - Password-reset questions, social engineering, etc., come into play...

Idea 1: User-driven password changes

- How do users change their passwords?

Password1

Password2

Password3

Pa\$word1

- Y. Zhang, F. Monrose, M. K. Reiter: The security of modern password expiration: an algorithmic framework and empirical analysis. ACM CCS, pp. 176-186, 2010.

Idea 2: One-time passcodes

Alice



789128



~~789128~~

001025

330236

919511

668336

...

~~789128~~

001025

330236

919511

668336

...

A scratch-off variant



- **Pros:**
 - Fits in wallet
 - Recyclable
 - You feel as though you have a chance of winning the lottery
- **Cons:**
 - Winning the lottery just means you can log into your bank account
 - Messy, inconvenient
 - Limited-use

Another idea:
One-time
passcode tokens

One-time passcode tokens

“Something you have” authentication factor



Many types

(Proof that security can be stylish)



How a time-based token works

secret
key

K

Alice



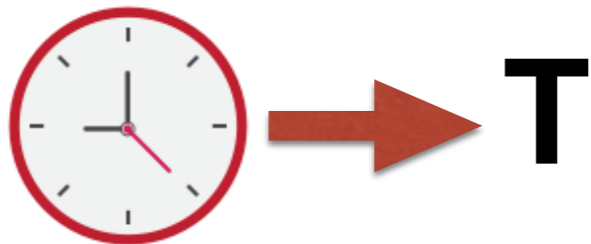
P_T (e.g., 790062)



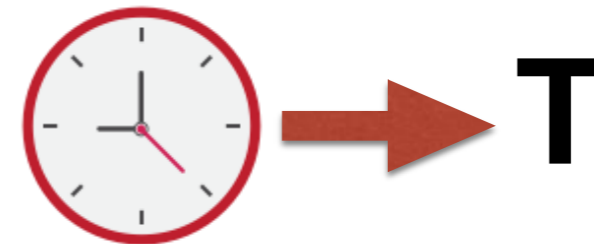
K



$$P_T = F(K, T)$$



$$P_T = F(K, T)$$



Similar for counter-based token

secret
key

K

Alice



P_C (e.g., 878883)




K



$$P_C = F(K, C)$$



 **$C \leftarrow C+1$**

$$P_C = F(K, C)$$

$C \leftarrow C+1$



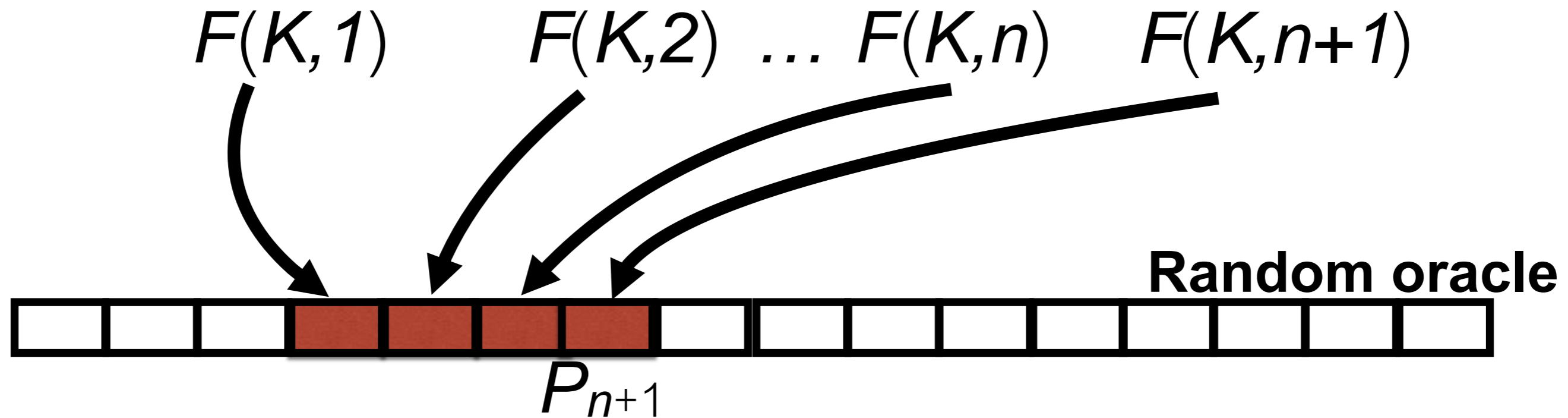
What's the function F ?

- Should be hard to create passcodes without knowledge of K ; some (simplified) variants used in practice:
 - $F(K, C) = \text{AES}_K(C)$
 - $F(K, C) = H(C \parallel K)$
 - $F(K, C) = \text{HMAC}(K, T)$ [OATH, RFC 6238 TOTP]
- Note: Output needs to be truncated for passcode display
 - E.g., $P_C = F(K, C) = H(C \parallel K) \bmod 1,000,000$ (for 6 digits)

Adversarial model and security goal?

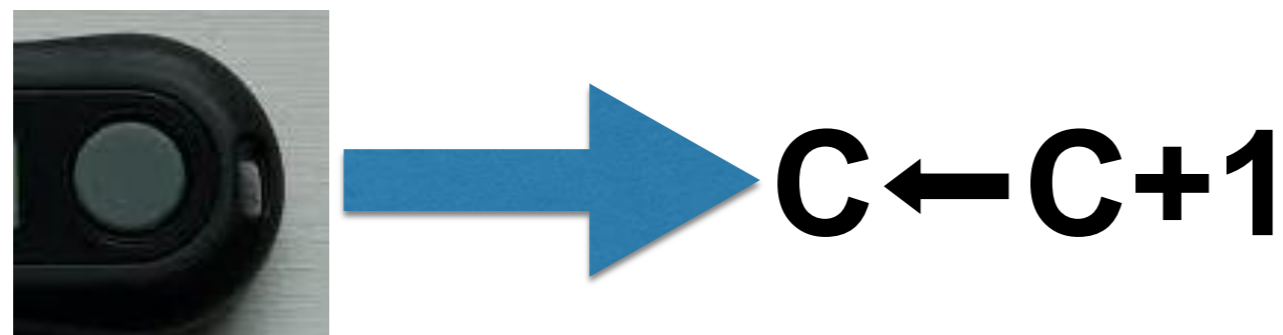
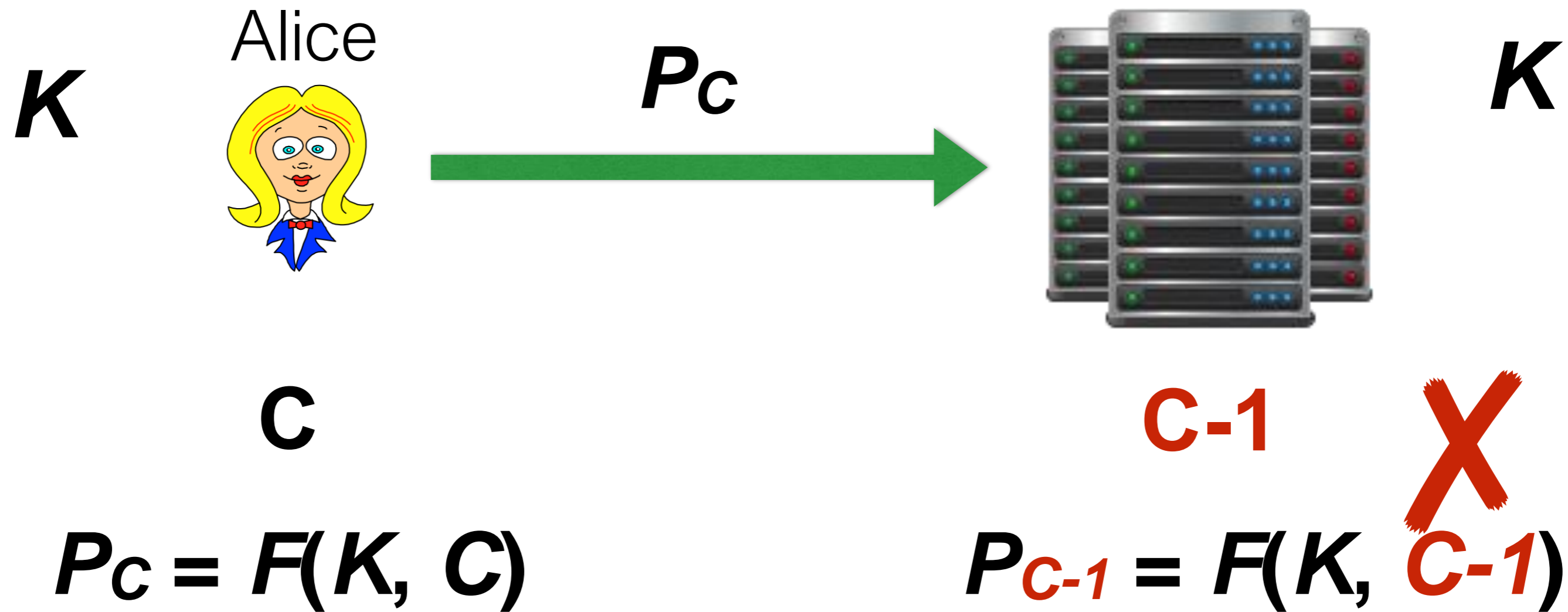
- Adversarial model:
 - Worst case assuming eavesdropping adversary?
 - Assume that the adversary learns a long sequence of passcodes $P_1, P_2, \dots P_n$.
- Security goal:
 - We want adversary not to be able to guess P_{n+1} .
 - What does this mean?
 - Ideally, adversary can do no better than random guess at P_{n+1} .
 - Consider $F(K, C)$ in ROM (e.g., F implemented using a hash function), and for simplicity, assume no truncation

In the ROM



- Only way for adversary to find red region is to guess K
- But if K is long (e.g., 128 bits), this is infeasible.
- So adversary has no way of finding cell containing $F(K,n+1)$
- Thus $P_{n+1} = F(K,n+1)$ is **perfectly random** in view of adversary—exactly what we wanted!

What happens if Alice pushes the button but doesn't authenticate?



The fix: accept a *window* of W passcodes

Alice



P_{C+1}

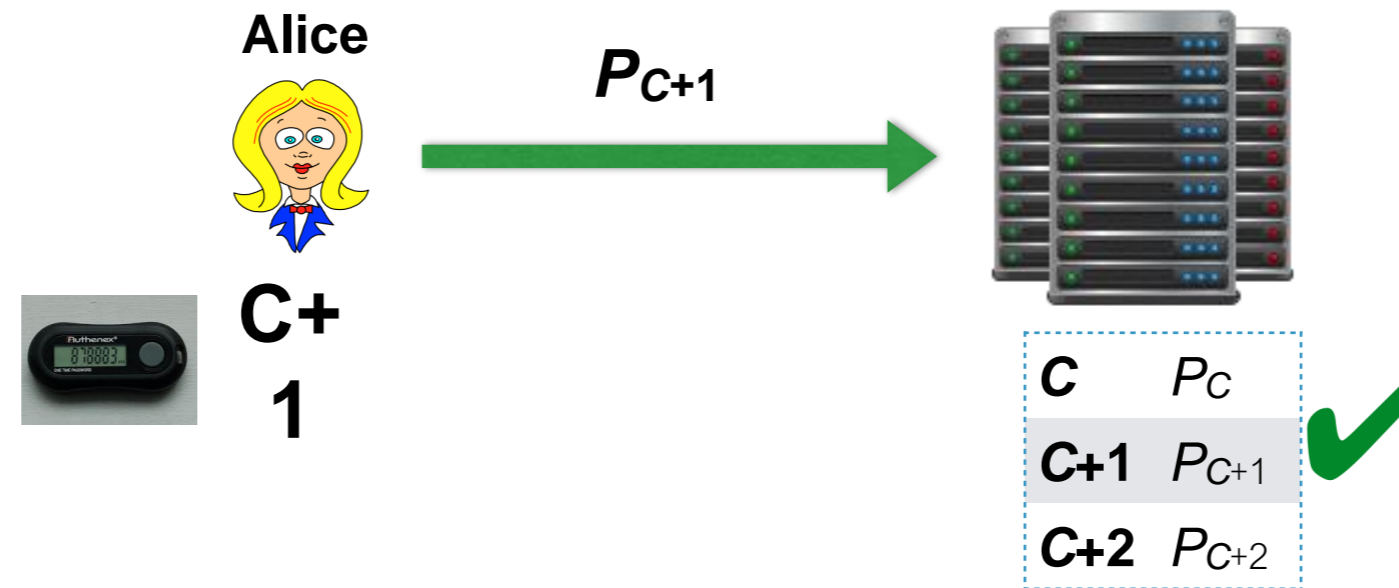


$C+1$

C	P_C
$C+1$	P_{C+1}
$C+2$	P_{C+2}



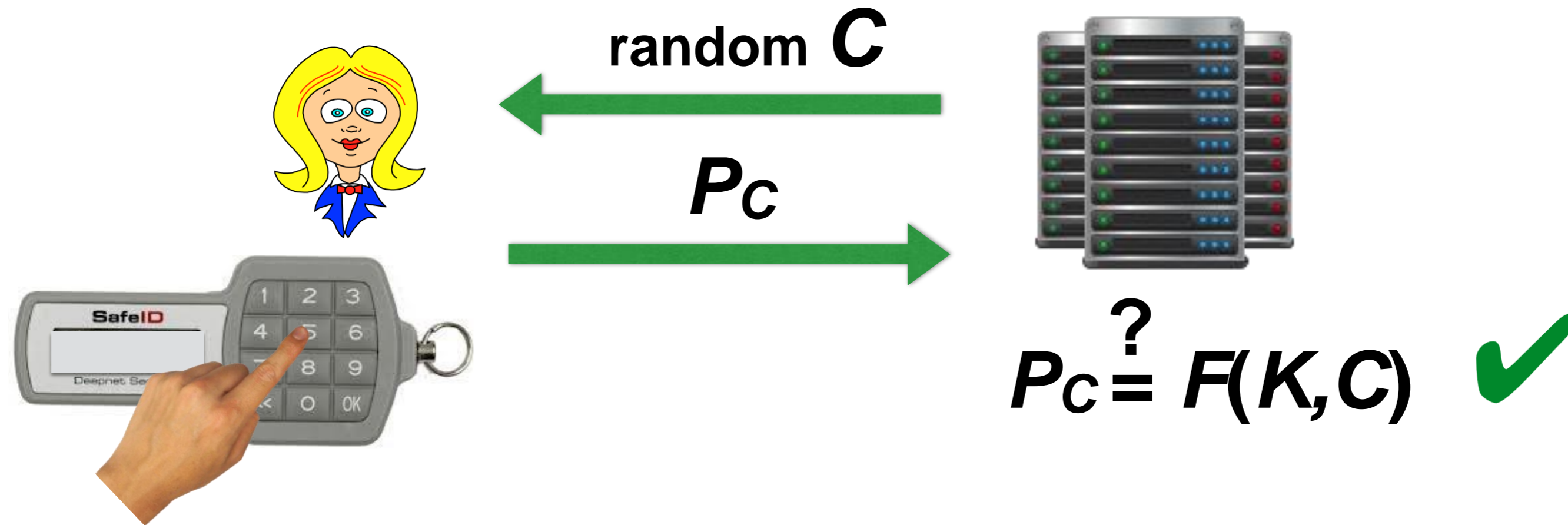
The fix: accept a *window* of W passcodes



Drawback?

- Now adversary can guess any of W passcodes to impersonate Alice
- I.e., window size W gives increases adversary's success probability by factor of W !
- And you'll still get desynchronized if your six-year-old daughter discovers how fun it is to press the button...

How about challenge-response?



- Desynchronization problems gone!
- Royal pain to use!

Protection against physical attacks

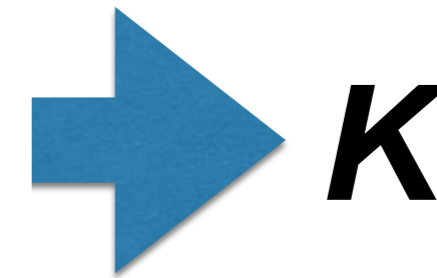


Mallory

What happens if there's a lunchtime attack on your token?



Mallory



- You leave your token on your desk during lunch.
- Mallory steals into your office, breaks open your token and extracts secret.
- Mallory replaces token so you don't know about attack.
- Mallory uses your passcodes and impersonates you...

Funkspiel schemes



- Huub Lauwers was a Dutch agent with the Special Operations Executive (British intelligence) during WWII.
- He made radio transmissions to SOE.
- He was captured by the Germans in 1942, along with his radio.
- The Germans had also intercepted three messages.
- Germans sought to mount a “Funkspiel”, i.e., pass false messages to SOE by impersonating Lauwers.

Funkspiel schemes



- To detect the capture of agents, the SOE used a secret “message authentication code.”
 - Agents intentionally inserted special, pre-agreed errors into their messages
- The Germans knew this.
- They confronted Lauwers with his messages and demanded his code...

Authentication code

- Lauwers's "authentication code" was "corrupt the 16th letter of every message"

Message 1: stop ...

16th letter

Message 2: stop ...

Message 3:

Authentication code

- Lauwers's "authentication code" was "corrupt the 16th letter of every message"
- Happily, Lauwers made a clever observation about his messages.
- He figured out how to fool Germans and alert SOE to his capture. How?
- He gave the Germans the wrong authentication code... "corrupt 'o' in the word 'stop'"

Message 1: stop ...

16th letter

Message 2: stop ...

Message 3:

The result in WWII

What happened?

- The Germans were fooled!
- The British were fooled!
- The Germans captured many SOE agents...

Message 1: stup ...

16th letter

Message 2: step ...

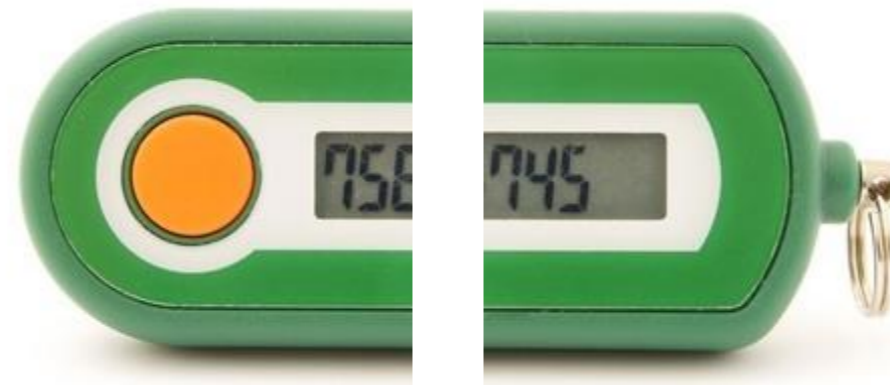
Message 3:

Result in 21st century



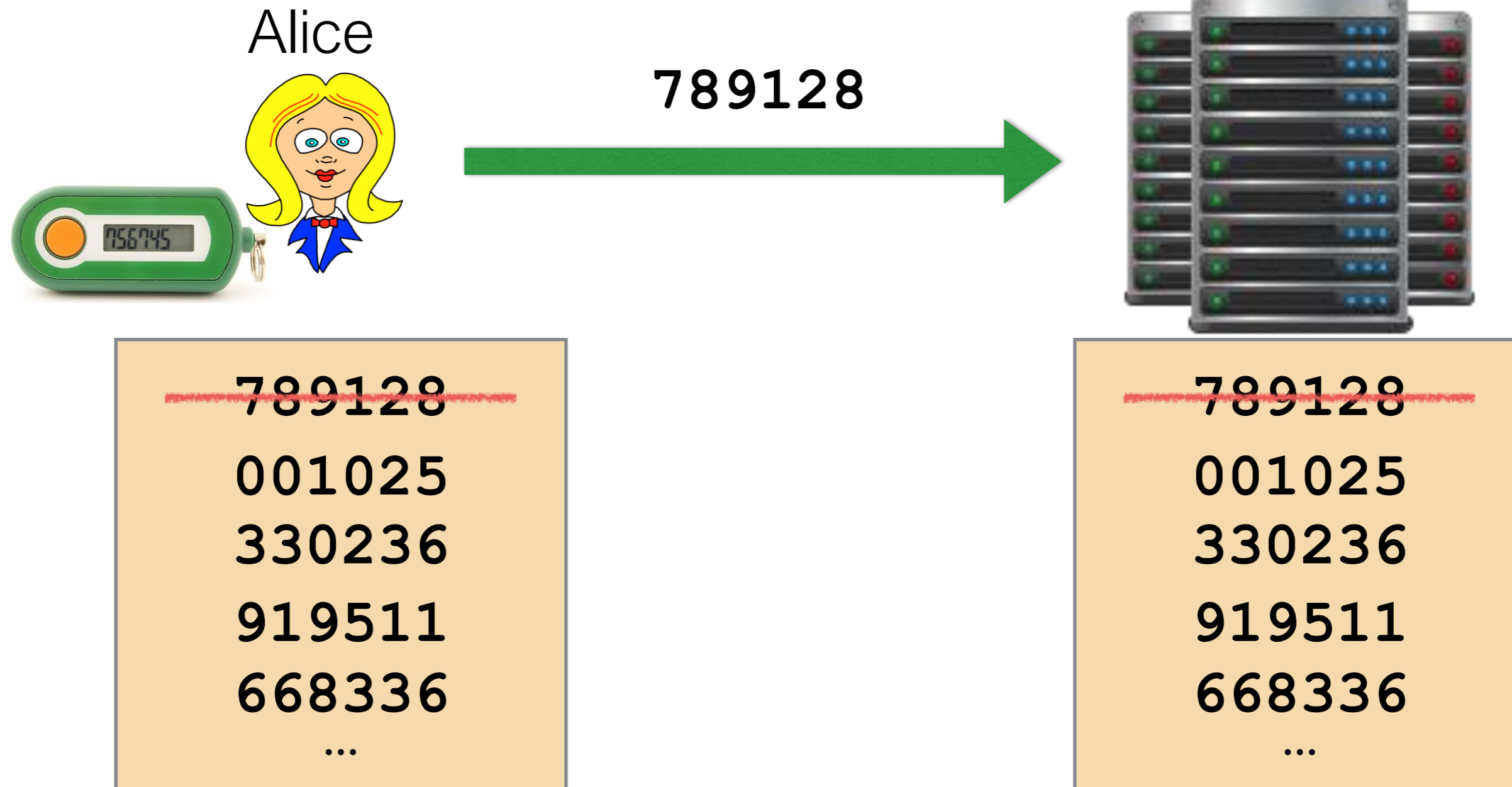
Lauwers' cleverness became a product idea.

Idea: Funkspiel scheme for tamper detection

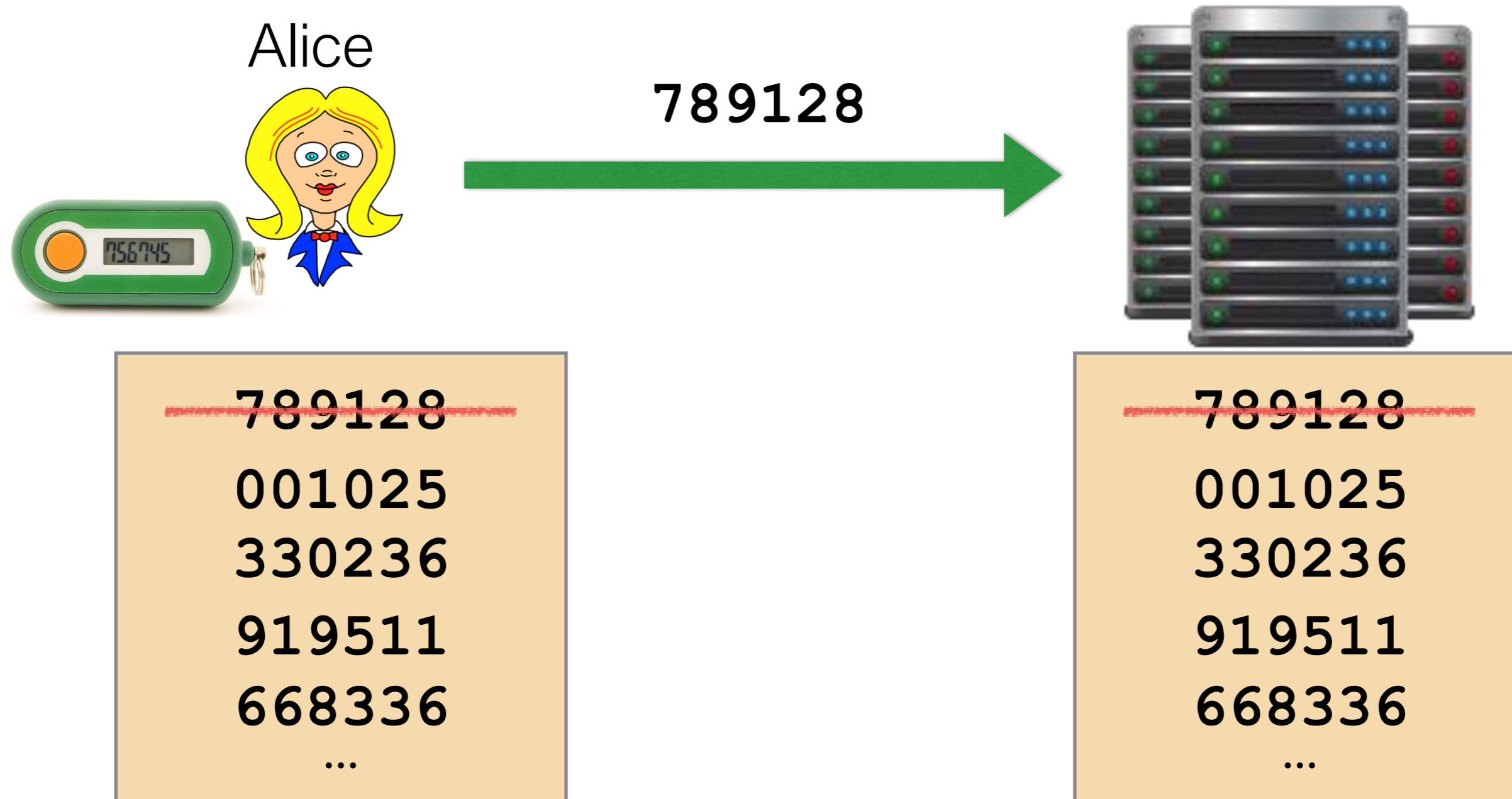


- Lunchtime attack involves tampering.
 - Funkspiel idea: If tampering is detected, token embeds secret alert for server in passcodes.
 - Even if adversary Mallory
 - Sees previous messages / passcodes (like Germans)
 - Breaks open token and gets future passcodes
- ...Mallory can't tell if secret alert was activated!

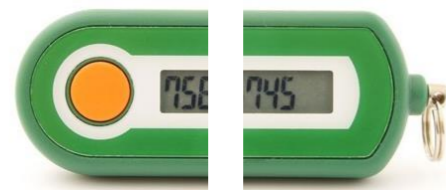
Remember simplified token model



(Simplified) secret alert: $+1 \pmod{10}$
for all digits in unused passcodes



Secret alert: $+1 \pmod{10}$ for all digits in unused passcodes

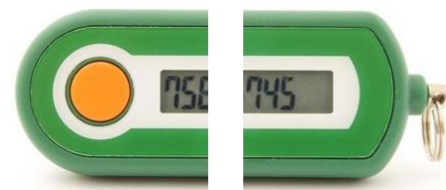


~~789128~~
001025
330236
919511
668336
...



~~789128~~
001025
330236
919511
668336
...

Secret alert: $+1 \pmod{10}$ for all digits in unused passcodes



~~789128~~
112136
441347
020622
779447
...



~~789128~~
001025
330236
919511
668336
...

Secret alert: $+1 \pmod{10}$ for all digits in unused passcodes



Looks random to me...



Mallory



~~789128~~

112136

441347

020622

779447

...

~~789128~~

001025

330236

919511

668336

...



$$112136 - 001025 = 111111 !!!$$



112136



~~789128~~
112136
441347
020622
779447
...

~~789128~~
001025
330236
919511
668336
...

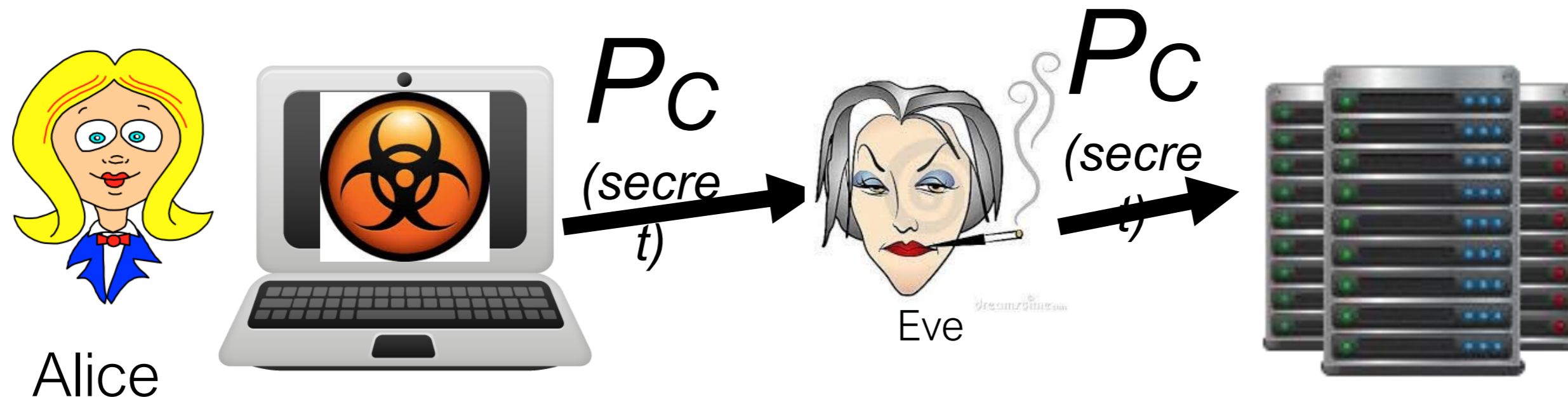
Notes

- This is a *simplified* scheme with some problems, e.g.,
 - If Mallory thinks silent alarm sounded, she can *subtract* 11111 to get valid passcode.
 - Mallory can also simulate tampering by intercepting Alice's passcode and adding 11111 to it.

Building better authentication tokens

Authentication tokens are still problematic

- Man-in-the-middle attacks
 - Phishing, malware, social engineering can all capture at least one passcode
 - So Eve can impersonate Alice at least once



Authentication tokens are still problematic



- Useability
 - Things people don't like:
 - Wearing authentication tokens as necklaces, carrying them everywhere, etc.
 - Transcribing passcodes + PINs
 - Users dislike use of tokens for authentication...

Authentication tokens are *still* problematic

- Lost, forgotten, or broken tokens
 - Credential recovery problem
 - Back to the name of your favorite pet...



Authentication tokens still have problems

- Cost
 - Tokens can cost \$50-60 a piece
 - Some lower-cost options available...
 - E.g., Deepnet GridID



RSA

RSA SecurID Authenticator SID700 5 Pack Key Fob, 3 Years

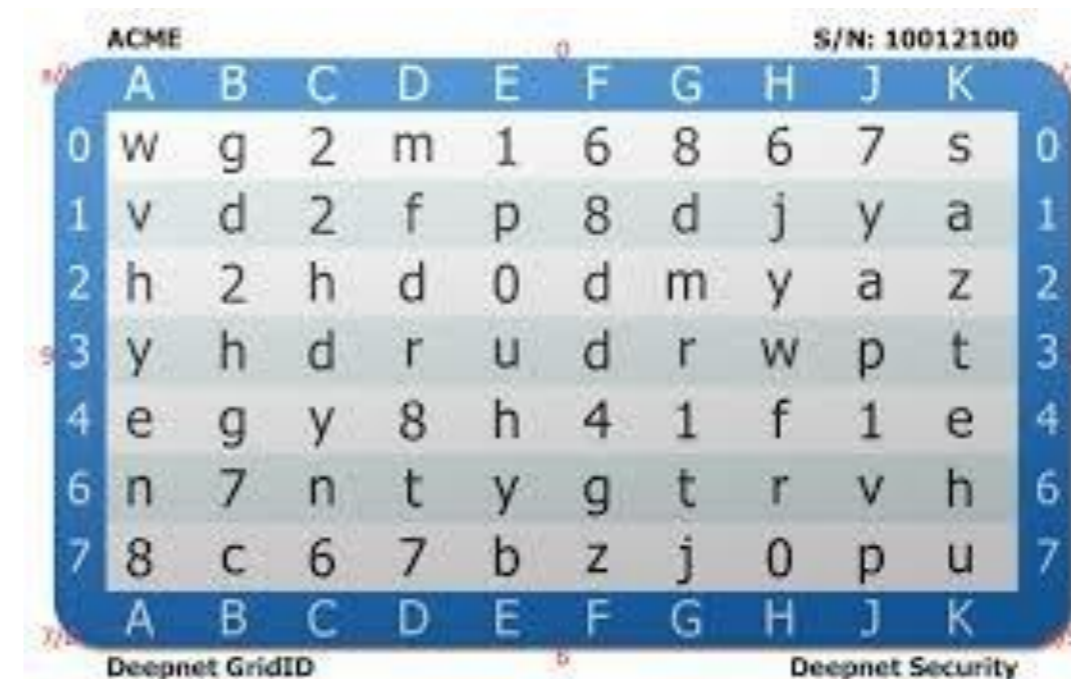
MSRP: \$310.00
Save: -\$51.00
\$259.00

FedEx Ground
FREE SHIPPING
\$100 Minimum Order
US Shipments Only

Qty: 1 **Add to Cart** VeriSign® Secured

Model: SID700-6-60-36-5

Overview: RSA SecurID Authenticator SID700 5 Pack Key Fob, 3 Years



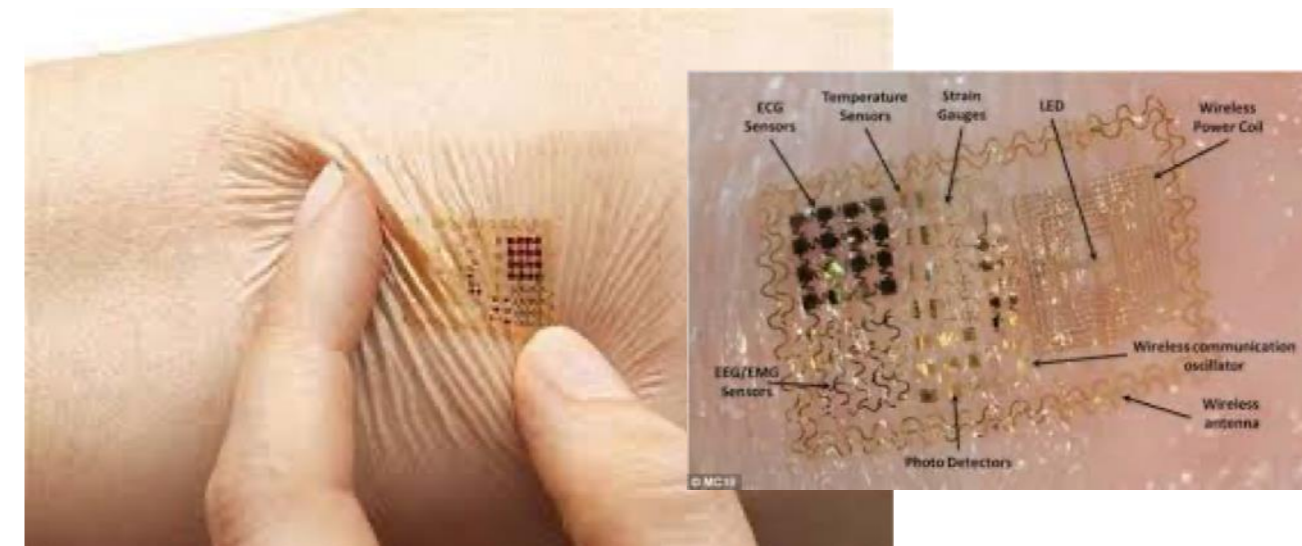
Authentication tokens still have problems

- Passcodes on mobile devices
 - Mobile devices are vulnerable to malware
 - SMS sometimes used; can be compromised in other ways
 - Consumers often don't activate when it's optional

The future of authentication tokens

The authentication situation is desperate.
But Motorola has an answer (two, actually).

Good for teenagers: "... you can be sure that they'll be far more interested in wearing an electronic tattoo, if only to piss off their parents..."



"The pill features a small chip with one switch that uses your stomach acids to activate an 18-bit ECG-like signal inside your body."

Already FDA approved.

Yubikey



- Offered as a FIDO U2F token
- Pros:
 - No typing
 - Plugs into USB; touch activation
 - (Some models) activate via NFC with mobile devices
 - Public-key cryptography supported (some models)
 - Resists man-in-the middle attacks



Yubikey



- Cons:
 - Lost / broken token → backup authentication problem
 - Bootstrapping: Who's going to distribute / pay for these things?
 - \$15+
 - Who wants to carry yet another device?



Is authentication the killer app for smartwatches?



Remember from last lecture:

- Biometrics
- Wireless communication
 - (No passcode typing)
 - Can eliminate attacks such as man-in-the-middle
 - NFC interface for payments
- Always with you

Is authentication the killer app for smartwatches?

SALON



WEDNESDAY, SEP 10, 2014 01:43 PM EDT

A killer app for the Apple Watch: Gun control

Authentication Tokens takeaways

Authentication tokens furnish one-time passcodes

- Stronger than passwords
- Still many problems:
 - Poor usability
 - Backup authentication problem
 - Man-in-the-middle attacks
 - Etc., etc.
- Changing in interesting ways...