

CSc 466/566

Computer Security

27 : Authentication II

Version: 2019/12/04 10:28:08

Department of Computer Science
University of Arizona

collberg@gmail.com
Copyright © 2019 Christian Collberg

Christian Collberg

1/49

Outline

- 1 Introduction
- 2 SIM Cards
- 3 RFIDs
- 4 Biometrics
- 5 Summary

Introduction

2/49

Means of Authentication

We identify someone by a combination of

- 1 something they have — smart card, key fob
- 2 something they know — password, mother's maiden name, first pet's name
- 3 something they are — fingerprint, retina scan



- Here we'll look at: something physical you possess, or something you are (biometrics).

Introduction

3/49

Outline

- 1 Introduction
- 2 SIM Cards
- 3 RFIDs
- 4 Biometrics
- 5 Summary

SIM Cards

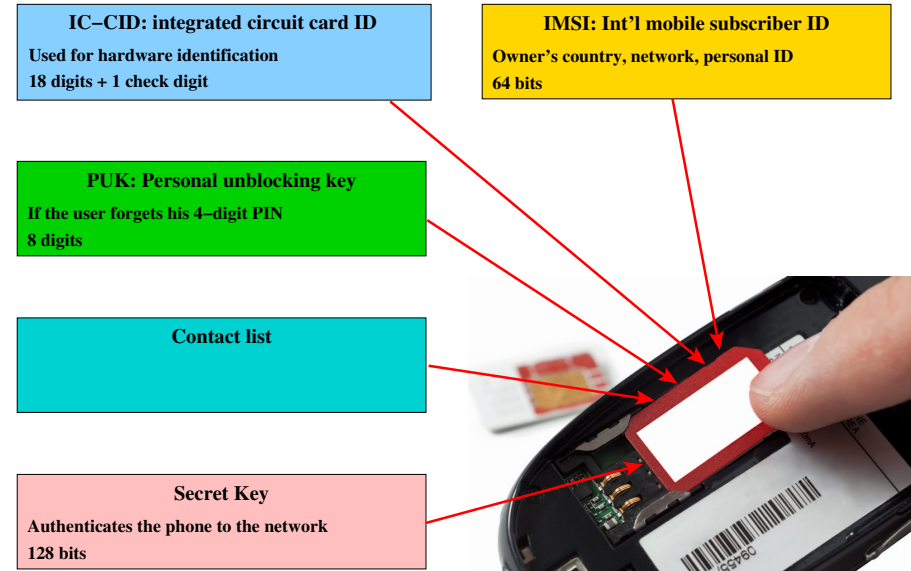
4/49

SIM Cards



- **Subscriber Identity Module Card**.
- Issued by the **network provider**.
- Contains personal information allowing the user to authenticate themselves to the network.

SIM Cards



SIM Cards: ICC-ID Example

89	91	10	1200	00	320451	0
Telecom ID	country code	network code	MM/YY of manufacturing	switch config. code	SIM number	check digit

- The check digit is calculated using the Luhn Sum algorithm.

SIM Cards: IMSI Example

310	150	123456789
USA Mobile Country Code (MCC)	AT&T Mobile Network Code (MNC)	Mobile Subscription Identification Number (MSIN)

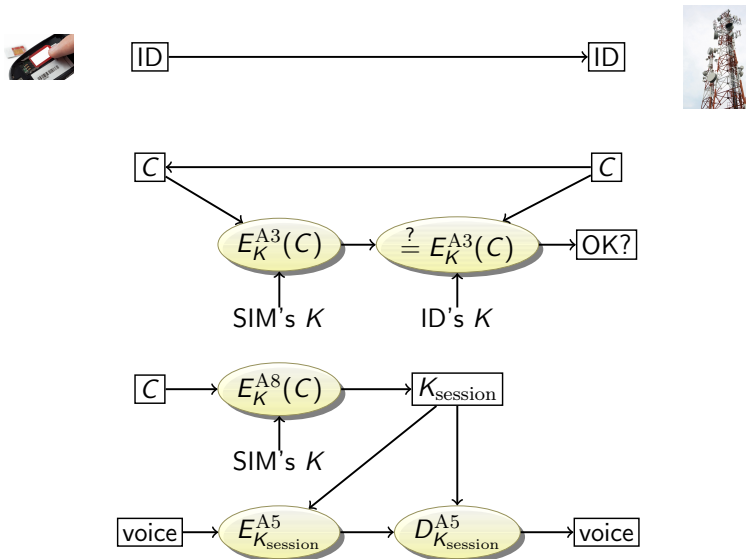
- There are some differences between different countries.

GSM Challenge-Response Protocol

- ID = IMSI (the phone's ID)
- K = The phone's 128-bit secret key
- C = 128-bit random challenge generated by cell tower
- A3, A5, A8 = secret encryption algorithms

GSM Challenge-Response Protocol...

- 1 The phone sends ID to the base station;
- 2 The base station generates and sends C to the phone;
- 3 The phone sends $V = E_K^{A3}(C)$ to the base station;
- 4 The base station looks up ID's key K in its database;
- 5 The base station compares $V \stackrel{?}{=} E_K^{A3}(C)$. If they are the same, the phone is authenticated;
- 6 The phone and base station both compute a session key $K_{\text{session}} = E_K^{A8}(C)$;
- 7 The phone uses A5 to encrypt data.



GSM Vulnerabilities

- A3, A5, A8 were chosen over standard cryptographic algorithms for efficiency reasons.
- The A3/A8 were reverse engineered and found to be insecure:
 - Given certain input (over the air!) the attacker can discover the card's key.
 - Given the key, a new SIM card can be cloned.
- A5 implementations have also had flaws, allowing eavesdropping on conversations.

Exercises I

- 1 What does SIM stand for?



- 2 What information is stored on a SIM card?



- 3 What does IMSI stand for?



Exercises II

- 4 Describe the GSM Challenge-Response Protocol!



Exercises III

- 5 How was GSM attacked?



Greatest Moments In Hacking History

- <https://www.youtube.com/watch?v=UBaVek2oTtc>
- Kevin Mitnick is a fugitive hiding out in Colorado. In an attempt to avoid detection from the authorities, Mitnick decides he wants to hack a cellphone so he can hide his location while using the device. To do this, the hacker sets up a social engineering attack against Motorola.

Outline

- 1 Introduction
- 2 SIM Cards
- 3 **RFIDs**
- 4 Biometrics
- 5 Summary

RFIDs



- RFID = **Radio Frequency IDentification**.
- IC for storing information + coiled antenna.
- Many RFIDs are passive (no battery).
- Range: a few centimeters to a few meters.
- Harder to clone than barcodes.

Uses of RFIDs



- track products, theft detection, track animals.
- In 2004 night clubs in Barcelona implanted RFID chips under the skin of their VIP customers, to identify them and allow them to pay for drinks. <http://news.bbc.co.uk/2/hi/technology/3697940.stm>.

RFID Vulnerabilities

- **Privacy issues**: RFID tags can be read from a distance.
- Important to protect against unauthorized readers.

Remote Automobile Entry



- The RFID and the car lock have the same pseudo-random number generator (PRNG).
- Both generate the same sequence of random numbers.
- What happens if the devices become desynchronized?

Desynchronization

PRNG = $\langle 42, 99, 27, 63, 82, 32, 66, 87, 11, 24, \dots \rangle$



42 → 42
99 → 99
27 → 27
63
82 → 63

Hopping (Rolling) Codes

- The car lock keeps track of the next 256 random numbers, and skips to the next one that matches.
- If the key-fob is pressed more the 256 times without connecting to the car: factory reset!

PRNG = $\langle 42, 99, 27, 63, 82, 32, 66, 87, 11, 24, \dots \rangle$



42 → 42 next=42,99,27,63,82
99 → 99 next=99,27,63,82,32
27 → 27 next=27,63,82,32,66
63
82 → 82 next=~~63~~,82,32,66,87

Replay Attack



42 → next=42



99 → next=42,99

27 → next=42,99,27 →



- **Replay attack**: jam the radio signal, collect the PRNG sequence, play it back to the car.

Remote Automobile Entry: KeeLoq

- **KeeLoq** is a proprietary code hopping algorithm using a 32-bit key.
- Reduced key-space attack:
 - 1 Note: some car models share common key bits;
 - 2 collect many transmissions;
 - 3 calculate for days.
- Side channel attack:
 - 1 Use power analysis to extract the manufacturer's (e.g. Chrysler's) "master key" from an encoder;
 - 2 intercept two messages from any encoder (up to 100 meters);
 - 3 clone the encoder!
- Newer designs use longer keys.

Remote Automobile Entry: RollJam

- DEF CON 23 - Samy Kamkar - Drive it like you Hacked it: New Attacks and Tools to Wireles
- <https://www.youtube.com/watch?v=UNgvShN4USU>
- Start watching at 8:40.

Remote Automobile Entry: RollJam...

RollJam ... is meant to be hidden on or near a target vehicle or garage, where it lies in wait for an unsuspecting victim to use his or her key fob within radio range. The victim will notice only that his or her key fob doesn't work on the first try. But after a second, successful button press locks or unlocks a car or garage door, the RollJam attacker can return at any time to retrieve the device, press a small button on it, and replay an intercepted code from the victim's fob to open that car or garage again at will.

<https://www.wired.com/2015/08/hackers-tiny-device-unlocks-cars-opens-garages>

RFID Passports (E-Passports)






- Since 2006, US passport have RFID tags, containing personal information + a digital picture.
- **Skimming**: With special equipment you can read the the passport from 10m.
- Countermeasures to skimming:
 - 1 A thin metal lining.
 - 2 To read the RFID, a PIN (printed on the passport data page) has to be entered into the reader.
 - 3 The communication is encrypted.

Uses of RFIDs



In Sweden, some workers are . . . electing to have a chip . . . implanted in their bodies to help them unlock doors, operate printers, open storage lockers and even buy smoothies with the wave of their hand. . . . Epicenter . . . has made the implanted chip available to its workers and to member organizations It's a biohacking experiment in simplicity that's been embraced by some early adopters associated with the center but represents a technological frontier sure to make others shudder.

<https://www.washingtonpost.com/news/on-leadership/wp/2017/04/04/some-swedish-workers-are-getting-microchips-i>

Exercises I

- 1 What does RFID stand for?

- 2 Do RFIDs send out information?

- 3 How are RFIDs powered?


Exercises II

- 4 Give 3 examples of applications of RFIDs!

- 5 What's a Hopping/Rolling Code?


Exercises III

- 1 Describe the Replay Attack on Rolling Codes!



- 2 Give examples of RFID privacy issues!



Exercises IV

- 1 How can you prevent passport skimming?



- 2 Is passport skimming a real problem these days?



Outline

- 1 Introduction
- 2 SIM Cards
- 3 RFIDs
- 4 **Biometrics**
- 5 Summary

Biometrics

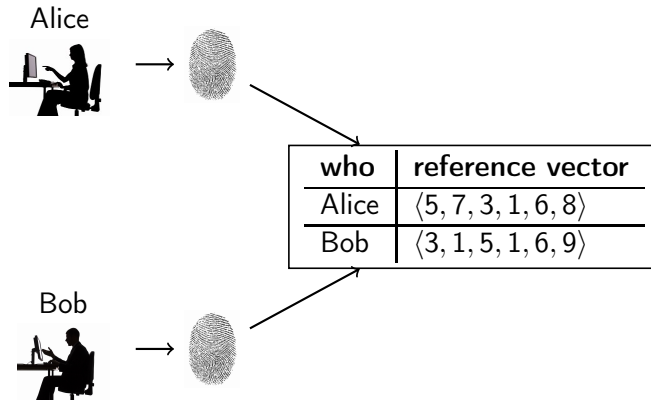


Definition (biometric)

Any measure used to uniquely identify a person based on biological or physiological traits.

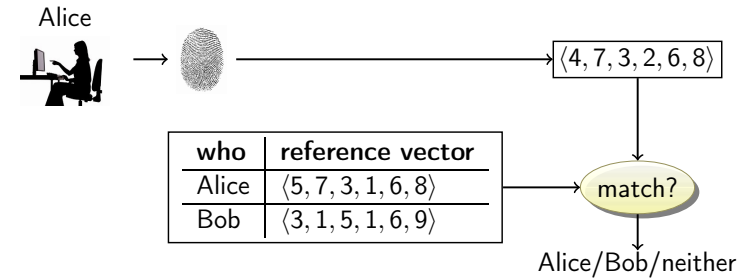
- **Biometric verification** — biometrics supplement other means of identification (smartcard, etc.).
- **Biometric identification** — biometrics is the only means of identification.

Biometrics: Collecting Reference Vectors



- For every user, extract a *reference vector* from their biometric measurement.

Biometrics: Matching Feature Vectors



- Extract a *feature vector* from the biometric measurement and do a fuzzy match against stored reference vectors.

Biometrics: Which Features?

- **Fingerprints:**
 - features: ridges, line splits, ...
 - collectability: easy
 - distinctiveness: high
 - permanence: change slightly over time
 - spoofability: gummy bears!
- **Voice recognition:**
 - collectability: easy
 - distinctiveness: low
 - permanence: changes from year to year
 - spoofability: tape recorders!

Biometrics: Which Features?...

- **Face recognition:**
 - features: ridge of eyebrows, edges of mouth, tip of nose, ...
 - collectability: easy
 - permanence: facial hair, ...
- **Eye scanning:**
 - Retinal scan: uncomfortable lighting of retina
 - Iris scan: photograph of the surface

Biometrics: Privacy Concerns

- Biometric data is the same over a lifetime.
- Must not be compromised!
- Just store and compare cryptographic hashes!

$$h(\text{feature vector}) \stackrel{?}{=} h(\text{reference vector})$$

Uh, no. We need to do approximate matching.

- AMAC — Approximate Message Authentication Codes:
 - Can easily determine similarity between two AMACs;
 - Given $\text{AMAC}(M)$ it's hard to find a message M' such that $\text{AMAC}(M') \approx \text{AMAC}(M)$.

Exercises I

- 1 What is biometric identification?



- 2 What is biometric verification?



Exercises II

- 3 What is a reference vector?



- 4 What is a feature vector?



Exercises III

- 5 To handle privacy concerns, can you just store a SHA-1 hash of the reference vector? If not, why?



Outline

- 1 Introduction
- 2 SIM Cards
- 3 RFIDs
- 4 Biometrics
- 5 Summary

Summary Question

- 13 Explain the GSM challenge-response protocol.
- 14 What is **desynchronization** for remote automobile entry?
- 15 What is a **hopping** code for remote automobile entry?

Summary Questions...

- 19 Explain the replay attack for remote automobile entry?
- 20 Give three countermeasures to skimming E-passports.

Readings and References

- **Chapter 2** in *Introduction to Computer Security*, by Goodrich and Tamassia.

Acknowledgments

Material and exercises have also been collected from these sources:

- 1 Christian Collberg, Jasvir Nagra, *Surreptitious Software, Obfuscation, Watermarking, and Tamperproofing for Software Protection*,

<http://www.amazon.com/Surreptitious-Software-Obfuscation-Watermarking-Tamperproofing/dp/0321549252>.

- 2 Tom Olzak, *Protect your network against fiber hacks*,

<http://www.techrepublic.com/blog/security/protect-your-network-against-fiber-hacks/222>

- 3 Bruce Schneier,

http://www.schneier.com/blog/archives/2007/09/eavesdropping_o_1.html

- 4 Erik Poll, *Embedded Software Security, ISSISP 2015*,

http://www.cs.ru.nl/~erikpoll/talks/ISSIPS_erik_poll.pdf