SECURITY (COMP0141): WHAT YOU HAVE

AUTHENTICATION

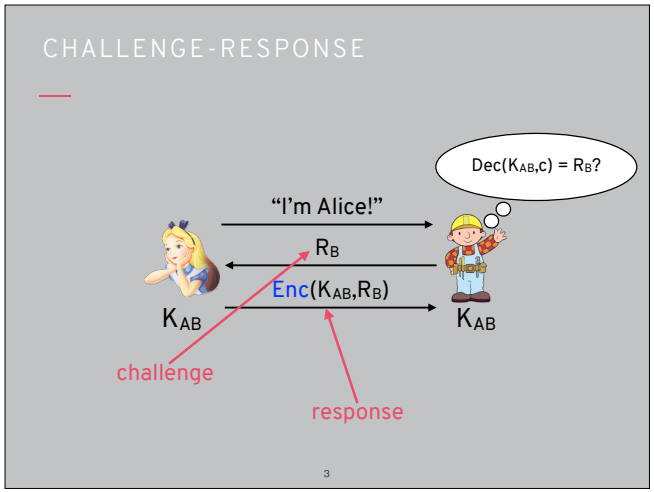
Authentication is:

What you know

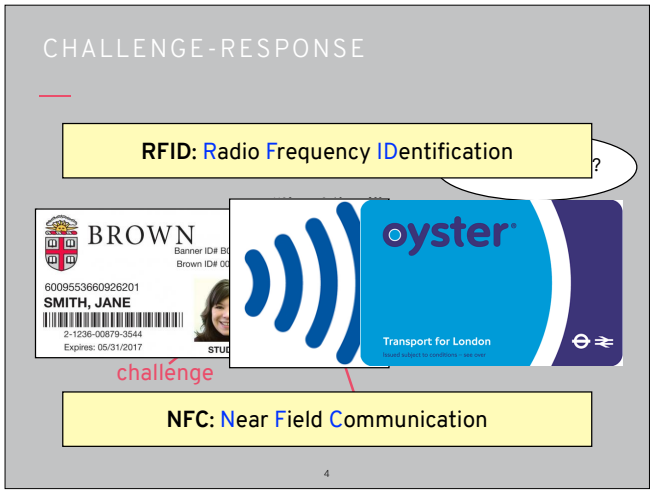
text passwords graphical passwords personal details

What you have

What you are

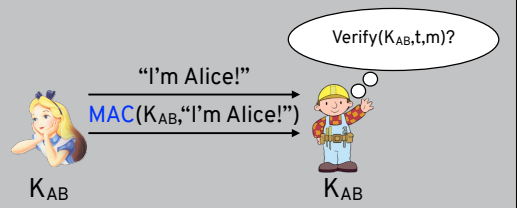


Classic challenge-response: If Alice can encrypt Bob's random value using their shared key, then it must be her! Random value is the challenge ('I dare you to encrypt this properly') and valid encryption is the response



You all use challenge-response many times a day, any time you use your student card, make a contactless payment, etc. These protocols are carried out via RFID or NFC

WHY NOT DO THIS?

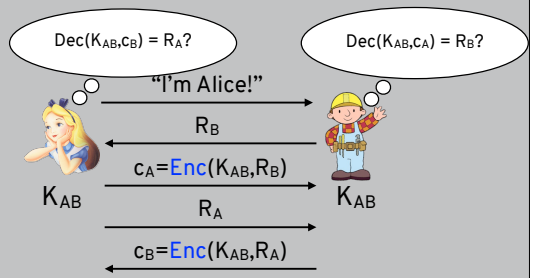


this doesn't work in really constrained environments!

5

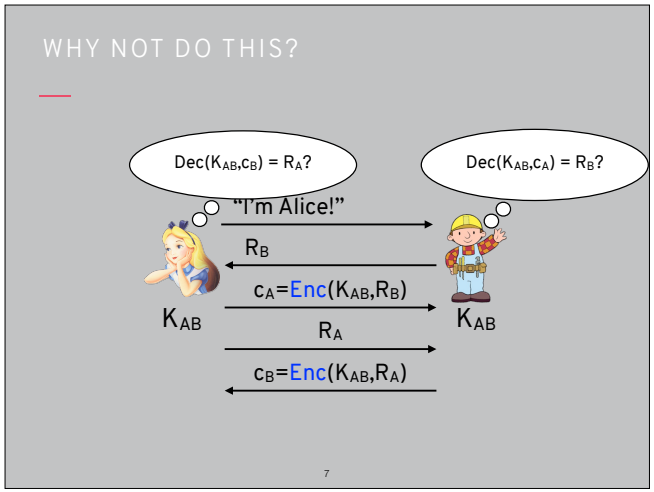
Could think of other ways to do this, but they don't always work in constrained environments (all computation has to be done on tiny chip on card, communication with very low bandwidth)

TWO-WAY CHALLENGE-RESPONSE

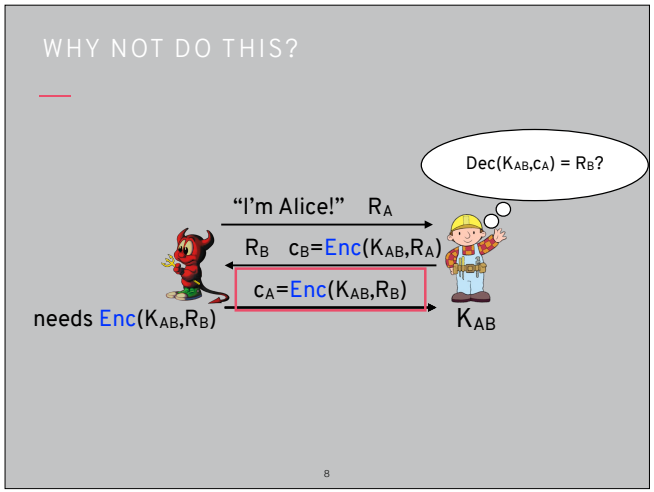


6

One way to do two-way authentication is to just repeat challenge and response

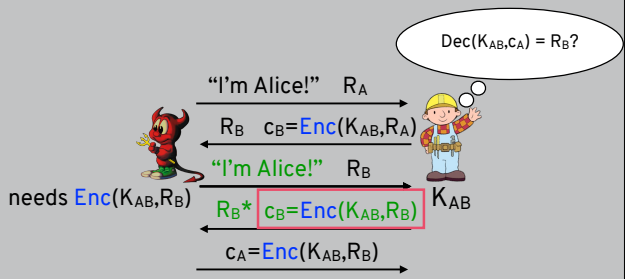


Might be tempted to optimise and have challenges and responses happen concurrently…



…but this is subject to an attack. First the attacker starts one session, he doesn't have key so won't be able to produce valid encryption

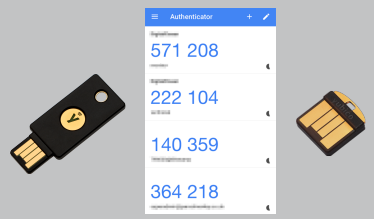
WHY NOT DO THIS?



don't design your own crypto!
need to consider **all** possible attackers

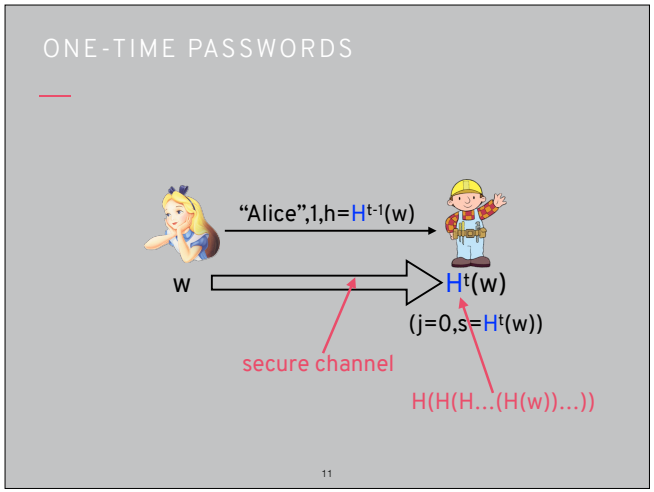
But if he starts a second session and reuses the same challenge that Bob gave him, can get as a response the exact value he needed, successfully authenticates as Alice. Same warning as always: don't design your own crypto!

ONE-TIME PASSWORDS

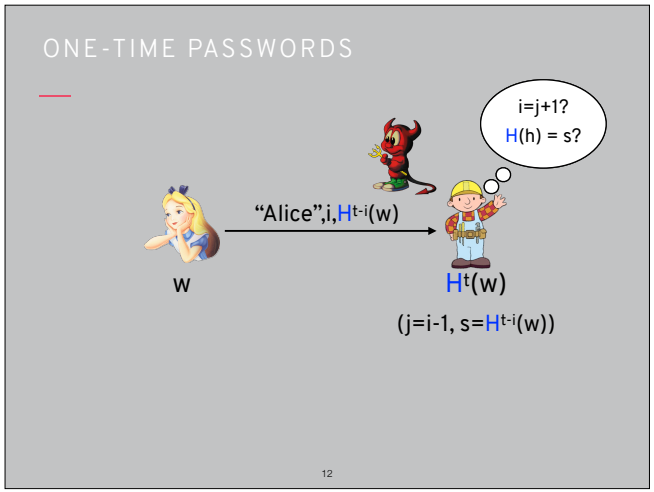


could be based on time (requires sync) or **math**

Tokens containing one-time passwords are used at many big companies

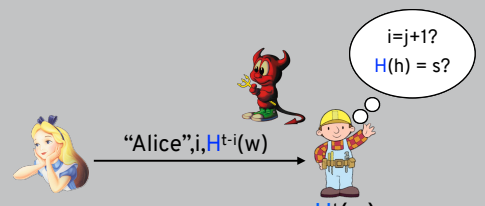


Here Alice computes a hash of a hash of a value w, many times over. This is called a hash chain (https://en.wikipedia.org/wiki/Hash_chain), which you may remember seeing a variant on back in Week 4. Every time she wants to sign in, she "peels off one layer" of the hashing and sends this pre-image to Bob, who can check that it's the right pre-image for the time she's logging in and increment his counter of how many times she has logged in.



Even if an adversary sees the pre-image when she sends it, because Bob increments his counter this same pre-image won't work ever again

ONE-TIME PASSWORDS



pre-image resistance: given h, hard to find m such that H(m) = h

13

So, the adversary would need to break pre-image resistance to log in as Alice

---

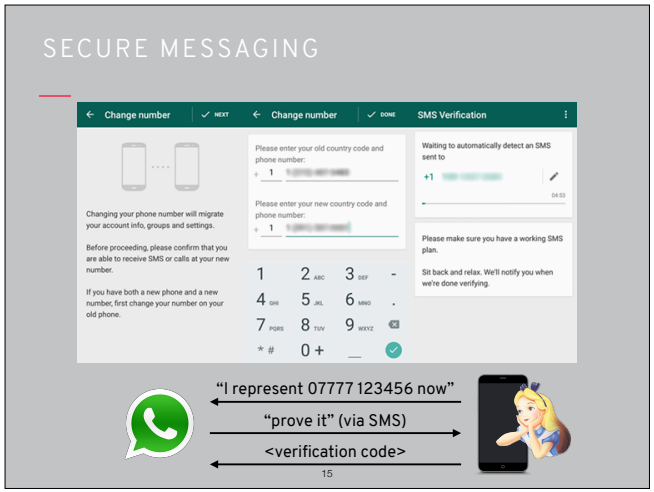
SECURE MESSAGING

	Encrypted in transit?	Encrypted so the provider can't read it?	Can you verify contacts' identities?	Are past comms secure if your keys are stolen?
FACEBOOK	yes	no		
IMESSAGE	yes	yes		
SIGNAL	yes	yes		
TELEGRAM	yes	no		
WHATSAPP	yes	yes		

what enables encryption is keys stored on your device

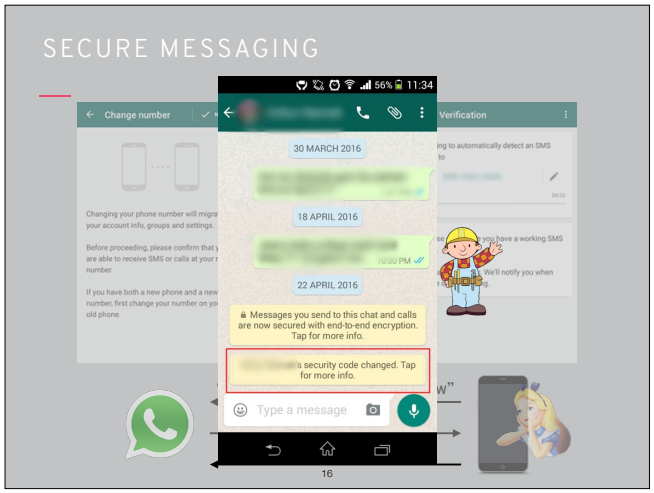
14

We saw secure messaging last week, and actually what allows your conversations to be encrypted is security tokens (keys) stored on your phone



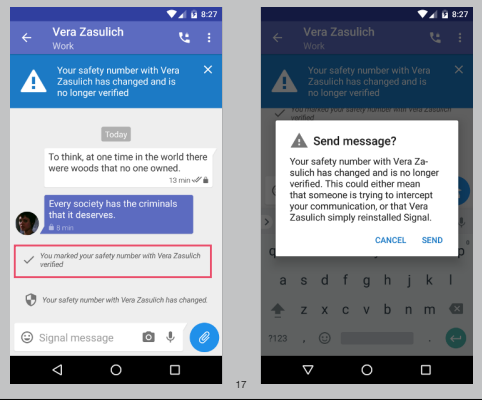
Those keys are generated only after you verify your number using SMS, to prevent impersonation

---



But how do Alice's contacts know that she really initiated this change? In some apps Bob would see a notification like this one saying her security code has changed

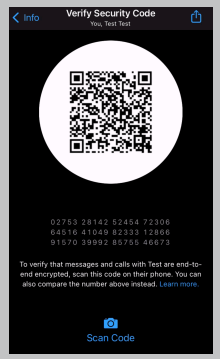
SECURE MESSAGING



17

In Signal you see a stronger warning if you've previously marked someone as verified. But how do you do that in the first place?

KEY VERIFICATION DEMO



18

This relies on being in the same physical place as your contact, which is a quite heavy burden on users

SECURE MESSAGING

	Encrypted in transit?	Encrypted so the provider can't read it?	Can you verify contacts' identities?	Are past comms secure if your keys are stolen?
FACEBOOK	yes	no	no	
IMESSAGE	yes	yes	no	
SIGNAL	yes	yes	yes	
TELEGRAM	yes	no	no	
WHATSAPP	yes	yes	yes	

19

This feature is not as well supported (and probably used even less!)

AUTHENTICATION

Authentication is:

What you know

text passwords graphical passwords personal details

What you have

RFID card cryptographic tokens

What you are

20