Second week tutorial

Ross Anderson

Q 1

- Why would the US NIST deliberately limit key lengths to 56-bits on financial cryptography? What other implications might that choice have?

Q 1

- Why would the US NIST deliberately limit key lengths to 56-bits on financial cryptography? What other implications might that choice have?
- Chapter on crypto, surveillance: IBM proposed 128 bits, the NSA demanded 48, and they settled on 56
- It was predictable that DES would break in the 90s
- NSA didn't want foreign governments to adopt DES as many were using kit from Crypto AG, which the US and German agencies secretly owned

Q 2

- What do Offset calculation, VSM and XOR-to-null-key collectively tell us about pitfalls in designing secure protocols? What lessons might we learn for Open Banking, and what trouble might we see ahead?

Q 2

- What do Offset calculation, VSM and XOR-to-null-key collectively tell us about pitfalls in designing secure protocols? What lessons might we learn for Open Banking, and what trouble might we see ahead?
- Complexity is the enemy of security
- Open Banking is getting extremely complex, with variations between countries (e.g. UK and German versions have different protocols)
- Add features till it breaks ...

Q 3

- What is the difference between an Acquirer and an Issuer? Why might the issuer have stronger incentives to fix the No-Pin attack, and how could each fix the bug?

Q 3

- What is the difference between an Acquirer and an Issuer? Why might the issuer have stronger incentives to fix the No-Pin attack, and how could each fix the bug?
- The costs of fraud fall on the issuer or on their cardholder, depending on local law
- The acquirer can check return-code consistency locally, at their gateway or even in the PED
- The issuer has to do it across the network, which can be flaky, especially across national borders

Q 4

- Why is SMS insecure as a two-factor authentication mechanism? Is it entirely useless, and are there better alternatives?

Q 4

- Why is SMS insecure as a two-factor authentication mechanism? Is it entirely useless, and are there better alternatives?
- Targeted attackers use SIM swapping to take over the mobiles of high-value account holders
- Other possibilities include SS7 hacking (seen since 2018) and Android malware
- It still blocks simple attacks involving passwords
- Authenticator apps are better, but RASP?

Q 5

- How might the large-scale move from chip-and-pin to contactless payments affect the security of banking payments?

Q 5

- How might the large-scale move from chip-and-pin to contactless payments affect the security of banking payments?
- Some implementation errors, e.g. limits not always checked on foreign currency transactions
- Apart from that, stolen cards have some value even if the PIN isn't known or guessable
- The pandemic turbocharged the move away from cash, with multiple likely second-order effects

Q 6

- Dual-controls in banking can be used to mitigate the risk of an employee "going bad" – the insider threat. To what extent do they also benefit employees, and against what forms of attack and adversary?

Q 6

- Dual-controls in banking can be used to mitigate the risk of an employee "going bad" – the insider threat. To what extent do they also benefit employees, and against what forms of attack and adversary?
- They make it much less likely that your family will be taken hostage by gangsters who demand you give them access to the vault, or make a large wire transfer!