Security Engineering Question Sheet 2: Lectures 3 and 4

Ross Anderson & Yuvraj Patel*

Here are a set of questions to help you think through the topics covered in lectures 3 and 4, on Banking Security. We will consider these in the tutorials, so be prepared to discuss them.

1. Why would the US NIST deliberately limit key lengths to 56-bits on financial cryptography? What other implications might that choice have?
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?
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?
4. Why is SMS insecure as a two-factor authentication mechanism? Is it entirely useless, and are there better alternatives?
5. How might the large-scale move from chip-and-pin to contactless payments affect the security of banking payments?
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?

*Material adopted from the class taught by Prof. Ross Anderson & Dr. Sam Ainsworth in 2022.