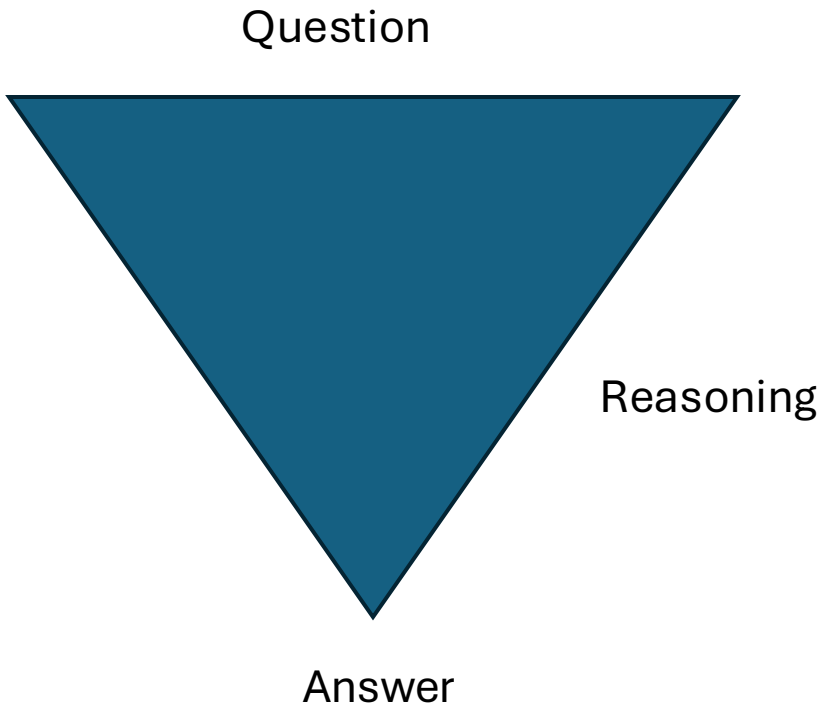
Answers in security engineering vs other courses





Security Engineering Problem Class 2

20/10/2026

Q1

Why is the optimal amount of card not present fraud non-zero? Who benefits from the current liability regime for card not present fraud, and who shoulders the cost?

Q1

- Economic reasons
  - Diminishing Returns on Prevention: Achieving zero fraud would require security measures so draconian (e.g., constant identity verification, frequent transaction blocks) that they would "kill" the user experience.
  - Cost of false positives: If a bank or merchant sets fraud detection filters too high, they begin rejecting legitimate customers. The lost revenue and damaged brand loyalty from these "false declines" are often more expensive than occasionally absorbing a fraudulent transaction.
- Fairness reasons
  - Liability Beneficiaries: Consumers benefit most from the current regime. Card holders don't usually have to pay for fraud, even when they were sloppy with details
- Cost Bearers: Merchants shoulder the primary burden. In CNP transactions, if a fraudster uses a stolen card, the merchant typically loses both the product and the revenue via a "chargeback," while also paying administrative fees to the bank.
- Banks earn billions (£50bn+) in credit card fees, they can afford a bit of fraud

READ IT: https://www.bitsaboutmoney.com/archive/optimal-amount-of-fraud/

Q2

Many banking apps now use on-device biometrics (like finger prints) to authenticate users. How could a criminal log into the victim's account using the only using the criminal's finger print? (There are at least 2 examples, with varying digress of likelihood)

Q2

1. Unlikely but physical kidnap could be a way, evidence of this in Colombia and even in London
2. Another unlikely option is finding a "collision". Some people have the same finger print reading as you
3. Hardware attack that undermines finger print reader
4. Much more likely is registering the app on a new phone, which will attest the finger print is valid
    - Mitigations are to force an approval on the old device to register on a new one

Q3

Historically, joint bank accounts required a signature from both account owners on both cheques and bank transfer requests. What are the barriers to adopting a similar separation of duties in online banking? Which cybercrimes would this help prevent?

Q3

- Friction to get approvals from both sides for a transaction
  - Could lead to bad situations for customers who need to move money in a pinch
  - Password sharing might undermine this in pratice
- However, it would reduce incidence of all kinds of push payment fraud as it forces a second party to intervene
  - Investment fraud if the 2nd person is more risk averse/sensible, very effective with romance fraud

Q4

How committed is the banking industry to customer security?

In what ways does the banking industry show a lack of commitment to customer security?

Q4

Uncommitted

- Downgrade attacks --- allow old payment devices to use legacy, insecure payment methods (e.g. offline, no chip and pin)
- Banking authentication ---
  - used just password for ages
  - Had a great solution in CAP readers but prioritised usability
  - Many still use SMS despite known attacks
  - Many weak points around account reset (registering new phone)

Committed

- Pioneered many infosec innovations
- Financial industry largely avoided ransomware and data breaches
- Colossal security budgets globally

Q5

What is the tension between backwards compatibility and card fraud?

Q5

- Why backwards compatibility is always supported
  - Credit cards are a 2 sided network
  - Valuable because you can use in any shop
  - Forcing merchants to buy new devices at short notice causes bad will and has delays
- Why it undermines security
  - Legacy versions are "unpatched"
  - EMV cards have magnetic strip for old terminals
    - Chip fall back attacks --> destroy chip and use mag stripe + signature
    - Skimmed



Q6

Microsoft issued patches for 1,246 Common Vulnerabilities and Exposures (CVEs) across its products in 2025. What economic ideas help explain why individuals and businesses continue to use Microsoft products?

Q6

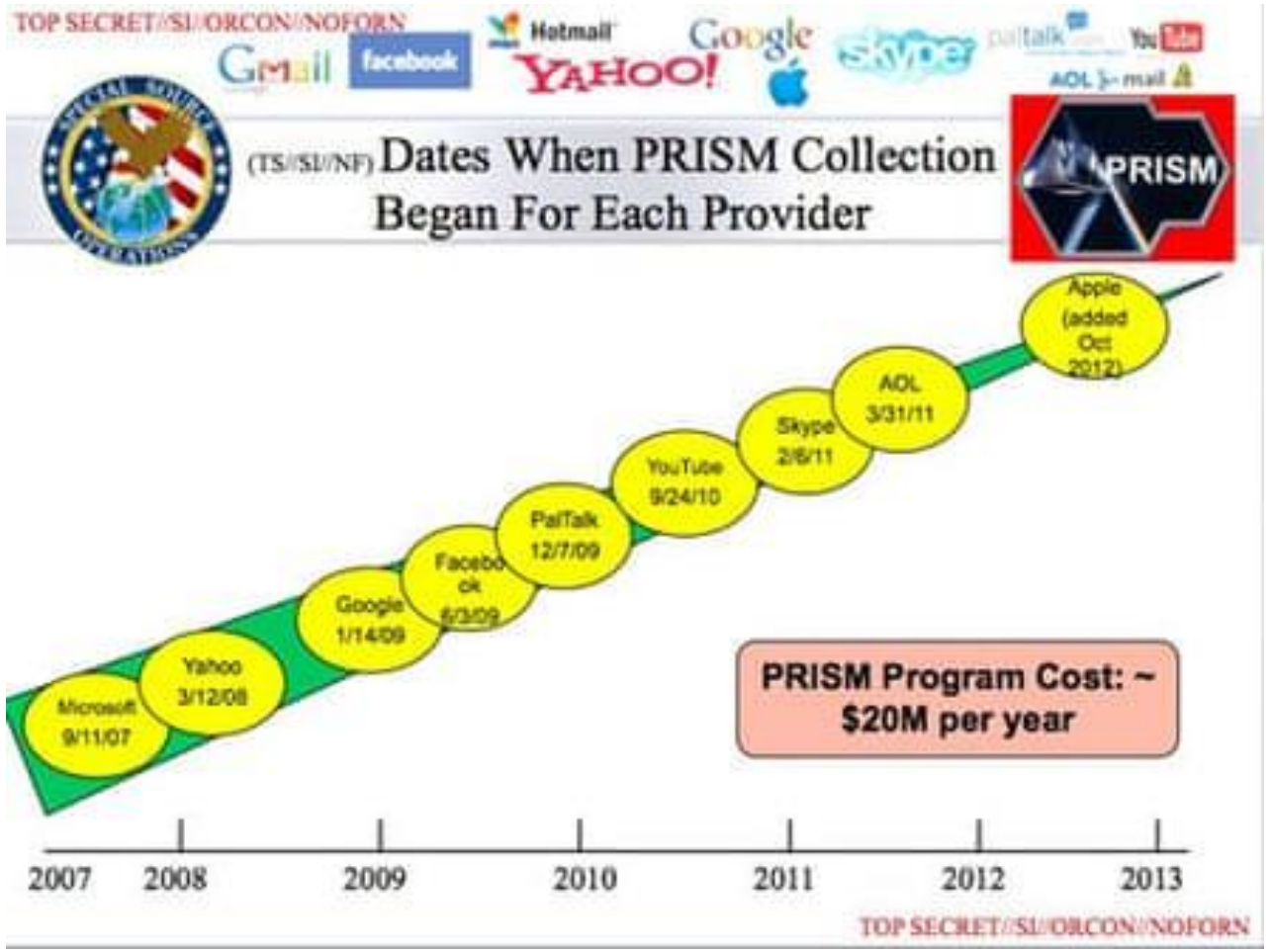
LOCK IN

- Windows was first to market and quickly established dominance, especially in corporate
- Companies find it hard to migrate many accounts at once, especially as there are interdependencies between diff solutions
  - Mostly new tech companies who use Apple, Gsuite etc
- Users like the excel shortcuts, the Windows layout etc

Q7

To what extent does market concentration help intelligence communities? How does this explain attempts to ban foreign social media networks?

Q7



Telegram's Pavel Durov announces new crackdown on illegal content after arrest

Platform with millions of subscribers discloses a more proactive approach to reporting infringers to authorities



Telegram founder and CEO Pavel Durov delivers a speech in Barcelona, Spain, on 23 February 2016. Photograph: Albert Gea/Reuters

Q8

- Which of the following is the biggest driver of security failures:
  - Principal agent problems
  - Negative externalities
  - Information asymmetry
  - Market concentration

Q8

Nit picky answer

- Principal agent problems is the core concept, and the others are variations
  - Info asymmetry is about the principal's ability to assess the agent
  - Negative externalities when one agent impacting many, many principals
  - Market concentration only matters if agent is dominant in the market

Better answer

- Dominant tech firms provide some of the best security/privacy
  - Apple/Google. Microsoft's lack of investment is perhaps just culture
- Negative externalities more of a 2000s problem with DDoS
- Supply chain issues most important (both info asymmetry + principal-agent)
  - Huge % of security incidents and fraud caused by business partners not investing

Q9

Antivirus software is sometimes considered a “market for lemons”. To what extent is this true, and is it down to hidden information, hidden action, or both?

Q9

Hidden info

- Hard to evaluate the quality of software that detects malicious software, unless you have a big sample
  - But even then, maybe they're good at detecting known malware samples, what about new samples/techniques
  - See MITRE EVALUATIONS

Hidden action

- To a lesser extent, you don't know how good they'll be at investing in the product moving forward

Q10

To what extent is blaming the user a valid explanation for why security failures happen?

Q10

Blaming user less justified

Insider threat

Knowledge based processing exploited

Skilled based processing exploited

Clicking phishing links

Florida Man Working as a Ransomware Negotiator Pleads Guilty to Conspiracy to Deploy Ransomware and Extort U.S. Victims

Monday, April 20, 2026

Former bank employee found guilty in $2 million fraud scheme targeting elderly customers

By Ashley Pomplas

Published: Feb. 10, 2026 at 7:08 PM GMT+0

Share | Add Us On Google

CLEVELAND, Ohio (WOIO) - After a five day trial, a federal jury has convicted a man who used his role as a bank employee in a scheme to steal money from elderly customers.

'You get sucked in': crypto scam victims on how they lost up to £162,000

Retired NHS doctor and others conned into investing – only to sink larger sums in trying to get cash back

Haunted by shame: victims of bank transfer scams tell of lasting trauma

Fraud can have devastating consequences on victims, and not only financially



Modern scams are sophisticated, often involving spoof telephone numbers and texts mimicking banks' security protocols. Photograph: Panther Media GmbH/Alamy

Q11

- Provide an example of a cyber attack technique that exploits each of: (1) skill-based behaviour; (2) rule-based behaviour; and (3) knowledge based-behaviour.
- Can you think of an example that exploits multiple?

Q11

1. Skills: Get user to click on a link with a malicious URL that looks benign
2. Rules: Get malware listed as top result in Google and impersonate as legitimate software. User searches google, finds app, installs your malware..
    - Following habituated rule for installing new software
    - I've heard of this with malicious Teams and Bloomberg apps
3. Knowledge: Contact user and convince them you're part of the IT teams and need access to their machine to do some checks, getting them to install a remote access tool.

3 could be combined with 1 if you make first contact via a spoofed email.

Q12

Which aspects of psychology would you have expected to be covered in these course, but were not?

Q12

Insider fraud: has the cost-of-living crisis increased the risk to your business?

Our fraud awareness specialists give their insights on how you can protect your business against the growing threat of insider fraud.

https://www.rbs.co.uk/business/insights/technology/fraud/insider-fraud-has-cost-of-living-crisis-increased-business-risk.html

Florida Man Working as a Ransomware Negotiator Pleads Guilty to Conspiracy to Deploy Ransomware and Extort U.S. Victims

Monday, April 20, 2026

Former bank employee found guilty in $2 million fraud scheme targeting elderly customers

By Ashley Pomplas

Published: Feb. 10, 2026 at 7:08 PM GMT+0

Share

Add Us On Google

CLEVELAND, Ohio (WOIO) - After a five day trial, a federal jury has convicted a man who used his role as a bank employee in a scheme to steal money from elderly customers.

Q13

Imagine that you are designing a spear-phishing attack designed to scam Edinburgh students out of money. How would you do it, who (or what) would you impersonate, how would you extract the money, and could you use Prospect Theory to increase your chances? Are there any other social-psychology tricks that might help?

Next steps

- Friday (23 October): lecture on Network Security
- Next Tuesday (27 October): NO LECTURE. I will set mock exam
- Friday (30 October): Lecture
- Tuesday (3 November): Guest Lecture from CISO of UoE
  - Lecture is in business school for some reason!!