Problem Class 4

Security Engineering

Q1: Why do military and safety critical software buyers maintain requirements for high-assurance, where as other software buyers have dropped this requirement? What is lost as a result?

Q1

- Higher cost of failures is the obvious answer
  - Even then, it's not clear this "kind of assurance" helps
  - User failure can be just as costly in medicine
- Easier for leaders to defend
  - No-one gets fired for buying IBM
- Arguably other industries face higher pressures
  - If I build a bad consumer SaaS product, I get no business

Q2: Can traditional approaches to assurance be reconciled with a focus on user testing?

Q2

- Obvious answer is no. It's hard to build a formal specification of users and test the properties of it
- More subtle answer is you can build light-weight formal methods into development process
- An even deeper answer is that we can formalise some aspects, but not others
  - TLS protocol was formally tested, but browsers can play around with how it's visualised to users

Q3: What is the relationship between prices in a bug bounty program and assurance over software security?

Q3

- General intuition is that higher prices = more assurance
  - Increases cost of compromise
  - Researchers sell to vendor instead of criminal
- Economic PoV is more complex
  - High prices could just be a sign there's lots of demand
  - There's many reasons supply curve is steeper, not just quality of software

Q4: Discuss the defensibility of the four patch strategies introduced in the lecture for a CISO facing allegations they were negligent.

1. **PCI DSS:** Update high and critical vulnerabilities (according to CVSS) within one month of release
2. **EPSS:** Patch what ML says is most likely to be exploited.
3. **KEV:** Patch what has already been exploited.
4. **Cloud infra:** Rely on professionals.

Q4: Discuss the defensibility of the four patch strategies introduced in the lecture for a CISO facing allegations they were negligent.

1. **PCI DSS:** Update high and critical vulnerabilities (according to CVSS) within one month of release
   - This is industry standard, baked into many standards. You have a clear defence
2. **EPSS:** Patch what ML says is most likely to be exploited.
   - This is new and untested, you don't get credit for the proactive vulns you avoided. But you will be blamed if you didn't patch a critical vuln or one that's been actively exploited
3. **KEV:** Patch what has already been exploited.
   - Reasonably defensible. You might be blamed if a "critical" vuln has been left unpatched for months because it hadn't been exploited
4. **Cloud infra:** Rely on professionals.
   - Highly defensible

Q5: If a vendor goes bankrupt, what are the security benefits and risks associated with "open-sourcing" their code bases?

Q5

- Benefits
  - In theory, customers or a 3rd party could fork the code and release a patch if a vulnerability is discovered
  - OSS is a good thing, maybe a community actively supports the project
- Risks
  - Source code helps attackers find vulnerabilities
  - "Patched" forked codebase might include a backdoor
  - Is the eventual vendor less likely to maintain if it's OSS?

Q6: Name three traditional security assumptions that are no longer true due to advances in AI systems.

Q6

- Fraudulent emails tend to have lots of errors
- Hearing a voice/seeing a video of a person is a form of authentication
- Traditional CAPTCHAs block bots
- Attackers don't have time/capacity for reconnaisance to understand procedures
- ...

Q7: How can a defender avoid forum shopping when it comes to assessing their vendors' security posture?

Q7

You have to do it via:

- Choose a security scanning rating yourself
- Direct verification via integrations
- Ask your own questions

E1: You are the student security officer at a University. You are tasked with protecting student data. What external threats should you anticipate, and what are the most reliable mitigations?

E1 Guidance

- List 3-6 threats and harms but provide enough explanation for each risk, try to choose a range
  - Don't go so narrow you become repetitive: 6 different forms of social engineering
  - Be specific "data breach" bad, "leak of database of student records" better. Remember to mention **why**
- Mention mitigations that are relevant to the threats and also reflect on "reliable"

E2: Password phishing involves tricking users into revealing their password. Using the SRK model, explain why phishing is one of the most common tactics deployed by attackers, and discuss how a system might be engineered to limit the efficacy of phishing and other social engineering techniques.

E2 Guidance

- Explain SRK as a theory, and explain how it relates to cyber attacks
- Try to explain what an attacker does next, e.g. not just how the password is revealed
- You don't need to invent the wheel. Pick MFA or principle of least privilege. But get specific. Which attacks can it prevent, and which can't it prevent
  - E.g. phishing resistance and MFA

E3: How can economics explain the continued prevalence of botnets that enable Denial of Service Attacks?

E3 Guidance

- Focus on the economics!
- Mention theories/concepts if you can, but describe them if you can't
  - Info asymmetry (hard to identify secure devices)
  - Negative externalities (device owner doesn't always suffer consequences)

E4: A policy maker recommends that all social networking mobile apps are formally verified by a 3rd-party to protect their privacy. Analyze the costs and success likelihood of this policy from an economic perspective.

E4

- Costs range from direct costs of verification through to slower product cycles lead to a worse product
- Success
  - Forum shopping – pick the least onerous reviewer
  - Is privacy really a formal assurance problem?

E5: What existing legal obligations might shape the security of a mobile app offered in the UK, EU or US?

E5 Guidance

- Pick 1--2 laws and try to explain why they apply and what obligation they place
  - GDPR (or UK GDPR) – personal data of user. May need to collect consent, need to apply appropriate technical and organizational measures
  - UK Product Security and Telecommunications Infrastructure – applies to connectable devices, prevents default passwords etc.
  - …