Assurance & Compliance

1. Why do military and safety critical software buyers maintain requirements for high-assurance, whereas other software buyers have dropped this requirement? What is lost as a result?
2. Can traditional approaches to assurance be reconciled with a focus on user testing?
3. What is the relationship between prices in a bug bounty program and assurance over software security?
4. Discuss the defensibility of the four patch management strategies introduced in the lecture for a CISO facing allegations they were negligent.
5. If a vendor goes bankrupt, what are the security benefits and risks associated with "open-sourcing" their code bases?
6. Name three traditional security assumptions that are no longer true due to advances in AI systems.
7. How can a defender avoid forum shopping when it comes to assessing their vendors' security posture?

Exam-Style Questions

1. 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?
2. 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.
3. How can economics explain the continued prevalence of botnets that enable Denial of Service Attacks?
4. 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.
5. What existing legal obligations might shape the security of a mobile app offered in the UK, EU or US?