

Problem Class 1 (Security Engineering 26/27)

Risks, Threat Actors & Policy

1. To what extent do the findings in the FBI's IC3 report align with the cyber insurance claims from Lecture 1?
2. Lecture 1 suggests individuals should primarily worry about online fraud. What is an argument against this?
3. All large software has bugs in it, and the most powerful nation-state actors will have a collection of zero-day attacks for all of the most popular systems. So why is installing the latest software updates still good security advice for most people despite this?
4. What kind of actors should worry more about their machines being infected and used for botnets vs data theft/extortion?
5. Why did ransomware evolve from automated software targeting individuals with fixed demands to targeting companies and opening up negotiations?
6. Recall Ross Anderson's 4-way classification of the threat actor ecosystem (crooks, spooks, geeks and the swamp). Are there actors who fall into multiple categories? Any threat actors who don't fall into any of these?
7. Modern infostealer malware groups sell a live data dump from infected machines. What other business models are possible and why do they go for this approach?
8. Let's say crooks are 1, spooks are 2, geeks are 3 and the swamp is 4. Come up with a profile of a defender who'd rank them the following from high to low:
 - a. Crooks then equal 2, 3 and 4
 - b. Swamp then 2 then equal 3 and 4
 - c. 3 highest
 - d. Spooks highest
9. What is a reasonable "safety" policy for a firm offering a frontier LLM?
10. Was the IC's move to multi-level security for intelligence stored in computer systems more successful in protecting information than the equivalent physical system? What kind of security violations are possible despite MAC?
11. Why is the concept of "trusted computing" particularly important in power metering situations? How are the associated security assumptions supported by periodic physical inspections of the meter?