Questions on Overshadow

What problem is being solved?
- Is it a real problem?
- What are the presumptions that must hold for it to be worth solving?

Describe the threat model
- What is realistic about it?
- What isn't?

Multi-shadowed Cloaking
- What are GVPNs and GPPNs and MPNs?
  (what did we used to call them?)
- Where have we seen examples of many-to-one GPPN->MPN mappings?
- What is multi-shadowing? What kind of mapping does it provide?
- What is cloaking?
- What are the overheads (time, space) of cloaking?
- Why is a secure hash stored?
- What could an "integrity only" mode be used for?
- What happens during the basic cloaking protocol?
  What is the IV for?
  Why does the system differentiate the "Plaintext Saved (IV,H)" state
  and the "Plaintext R/W" state?

OS Integration
- Why does Overshadow have to get involved on sys calls, traps, interrupts, etc.?
- Describe the flow of control during an interrupt that takes place
  when an app is running cloaked - when do page table switches take place?
- Where in the interrupt/fault handler must overshadow be careful not to leak info?
  (i.e., what would happen if only page table switches were used)
- Why are system calls more complicated?
- What types of system calls are easiest to handle?
- Which ones are hard? Why?
- Why does mmap() work better than read()/write() ?
- Overall, how much knowledge of the OS is required by the VMM?

Metadata
- What types of metadata are in the system?
- Where does it reside?
- How is it protected?
- What is most interesting about metadata management?

Performance
- What do you get out of the evaluation?