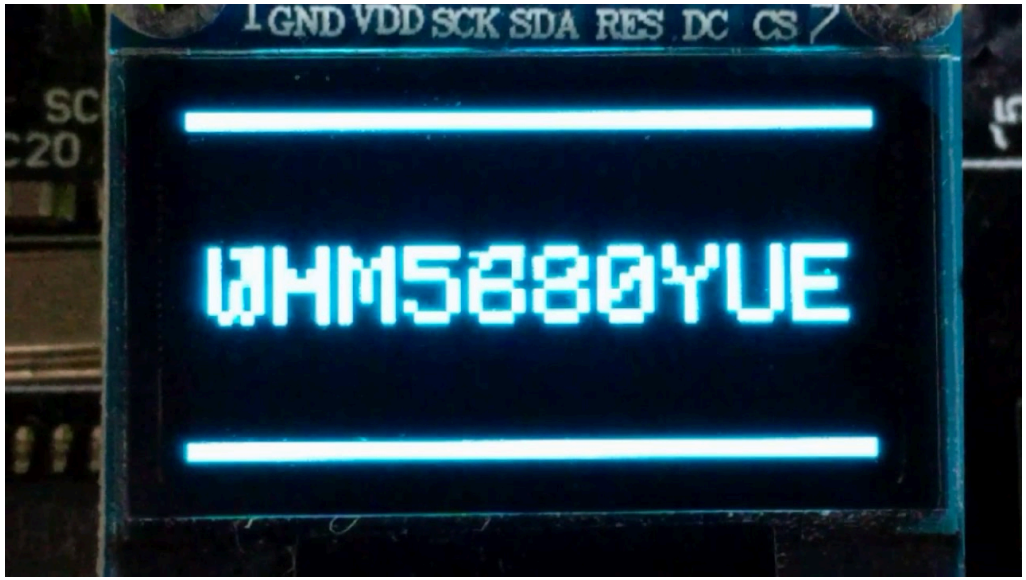
More Midterm 2 Review

CS642:
Computer Security

Wargames

- **https://www.hulu.com/watch/90c62d64-9b2d-4ddb-b55f-012d82445622**
  - Time 1:39



Sample Questions

- The source code for an electronic voting machine contains the following definition. #define DESKEY ((des_key*)"F2654hD4") Explain why this indicates a security problem.
- Can a stateless firewall block TCP connection initiation requests from an external location to any local host, but at the same time allow returning traffic from connections initiated by local hosts? Why or why not?
- Can the TPM be used to prevent a virus from modifying the machine's Master Boot Record (MBR), used for bootstrapping the OS, without being detected? If so, explain why. If not, explain why not.

Sample Questions 2

- Can a firewall be used to block all incoming email containing the phrase “low mortgage rates”?
- Can a firewall be used to block all incoming email from Nigeria?
- Can a firewall installed at a web site protect the web site from a DDoS SYN flood attack?

Sample questions 3

Media players enforcing content protection rules need to ensure that their executable image on disk has not been modified by the user (otherwise, one could bypass content protection by disabling the content protection component). These mechanisms are intended to defend against attackers who modify the executable instructions.

- A simple method for a program to detect tampering with its executable is follows: at startup the program hashes (using SHA-1) the executable image loaded in memory and compares the result with a pre-computed hash value (say, stored in the executable header). The program exits in case of mismatch. Explain how an attacker could defeat this mechanism with a single word change to the executable image.

Sample questions 4

- Suppose an operating system uses a TCP implementation that generates predictable TCP initial sequence numbers. Can this be used to defeat the confidentiality and integrity properties of the HTTPS protocol?
- In class we mentioned that when fragments with overlapping segments are re-assembled at the destination, the results can vary from OS to OS. Give an example where this can cause a problem for a network-based packet filtering engine (an engine that blocks packets containing certain keywords). How should a filtering engine handle overlapping fragments to ensure that its filtering policy is not violated?

Sample questions 5

PwdHash is a web browser extension that that transparently produces a different password for each site. When a user types in a plaintext password like rover, destined for a site like wellsfargo.com, the browser sends a series of characters determined by h(rover, wellsfargo.com), where h is a cryptographic hash function. Assume that the hash function is publicly known, since anyone can download PwdHash and run it. However, it is not feasible to compute x from h(x), or find collisions. When a customer uses PwdHash, the bank server sees the hashed password as the user's password.

- Suppose a phisher sets up a site that looks like Citibank, at a domain different from the real Citibank login site. How will PwdHash protect a customer entering a password to the phishing site?