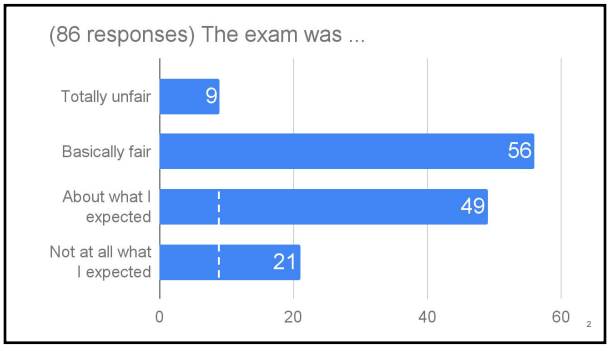
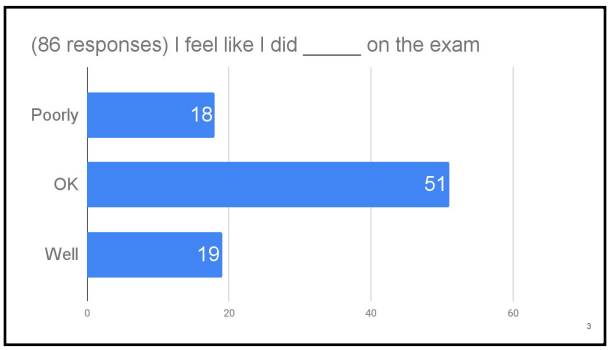
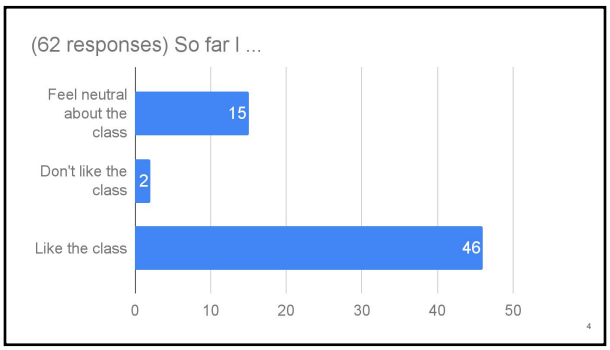
Malicious Software

COMP 435
Fall 2017
Prof. Cynthia Sturton







From the comments

- Exam: base 2 to base 10 conversion ??
- Lectures: like the concepts, want more exercises
- Laptops: evenly split
- Topics: want to cover current events

Quick Review

Reference Monitor

- Complete mediation
- Tamperproof
- Verifiable

Malware: malicious software

Attacker's Means and Motivation

- Fame
- Financial Gain
- Espionage

Malware Classification

- Targeted vs general
- Needs host code vs stand alone
- Self replicating vs not
- Propagation vs payload

Targeted Malware: Advanced Persistent Threat

- Targeted
- Long-lived
- Well funded
- Stealthy

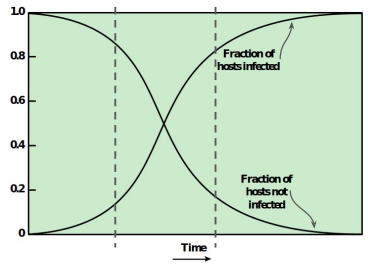
Virus

- Payload
- Infection mechanism
- Trigger

Worm

- Replicates across a network
- Payload

Worm Propagation



Computer Security: Principles and Practice, 3rd Ed. Stallings and Brown

Trojan Horse

- Hides inside useful code
- Opens a backdoor

Countermeasures

Countermeasures

- Effective
- Usable
- Feasible

User Vigilance

- Use known vendors
- Test in isolation
- Open only safe attachments
- Install only safe SW
- Know the potential harm of websites
- Maintain backups

User's Burden

"Apply all patches promptly except when doing so would cause more harm than good…"

Anti-virus Software

Compare executables against a database of known viruses

Anti-virus SW

- Easy to deploy
- Catches 45% of malware

Anti-virus SW

- High overhead
- Reactive, not proactive
- Risk of false positives
- Inflexible

Risk of False Positives

- Cost of false positives
- Base rate fallacy

Pattern Matching is Inflexible

```
add eax, ebx  ;eax = eax+ebx
mov ebx, 0    ;ebx = 0
```

Vs

```
add eax, ebx  ;eax = eax+ebx
xor ebx, ebx  ;??
```

Anti-virus Software

Generating the database of malware signatures

Virus Analysis

- Honeypots
- Disassembly
- Contained analysis

Writing Secure Code: Modularity

- Single-purpose
- Small, simple, testable
- Independent
- Well defined interfaces

Writing Secure Code: Testing

- Unit testing
- Function testing
- Regression testing
- Black-box testing
- Clear-box testing

“Testing can be used to show the presence of bugs, but never to show their absence”

--E.W.Dijkstra