Midterm Review

Chengyu Song
Administrivia

• Midterm
  • In class on Wednesday (Nov 1)
  • Covers malware and software security
  • Based on lecture and supplementary materials
    • Indicated as Preparation on the class schedule
  • Closed book. No additional sheets of notes
Types of questions

- Multiple choice
- Short answers
Malware

- You can get infected by malware by
  - Opening an email attachment
  - Receiving a multimedia message
  - Installing a software/app from unknown source
  - Browsing a USB stack
Malware

You can get infected by malware by

- Opening an email attachment
- Receiving a multimedia message
- Installing a software/app from unknown source
- Browsing a USB stack
Malware

• What of the following is true about worm
  • Worm can infects other computers through files
  • Worm can infects other computers through network
  • Worm mainly targets servers
  • Worm can be used to build botnet
Malware

• Which of the following is true about worm

  • Worm can infects other computers through files
  • Worm can infects other computers through network
  • Worm mainly targets servers
  • Not anymore
  • Worm can be used to build botnet
Malware

• Botnet can be used to
  • Send spam
  • Demand ramsome
  • Launch Distributed Denial-of-Service (DDoS) attack
  • Mine bitcoin
Malware

• Botnet can be used to
  • Send spam
  • Demand ransom
  • Bot master aims to use the infected machine as a generic computation platform (similar to cloud) for as long as possible; so they prefer stealthy instead of letting you know you're infected
  • Launch Distributed Denial-of-Service (DDoS) attack
  • Mine bitcoin
Malware

• Which of the following is true about AV software
  • It can only detect known malware
  • It can prevent malware infection
  • It cannot detect polymorphic malware
  • AV can remotely scan your computer and warn you
Malware

Which of the following is true about AV software

- It can only detect known malware
  - Behavior signatures can detect unknown malware
- **It can prevent malware infection** (Yes, but not all infection)
- It cannot detect polymorphic malware
  - Modern AV can detect polymorphic malware
- AV can remotely scan your computer and warn you
  - NO! It's FAKE AV!
Software security

- Which of the following is true about vulnerability
  - Only software contains vulnerability
  - All bugs are vulnerabilities
  - All vulnerabilities can be exploited
  - Malware exploits vulnerabilities
Software security

• Which of the following is true about vulnerability
  • Only software contains vulnerability
    • No, vulnerability include any weakness, including hardware and configurations
  • All bugs are vulnerabilities
    • No, not exploitable bugs are not vulnerabilities
  • All vulnerabilities can be exploited
  • Malware exploits vulnerabilities
Software security

Which of the following is true about memory corruption

- It is one of the most popular vulnerabilities
- It can be exploited to execute arbitrary code
- It can be exploited to leak secret
- It can be exploited to escalate privilege
Software security

• Which of the following is true about memory corruption
  • It is one of the most popular vulnerabilities
  • It can be exploited to execute arbitrary code
  • It can be exploited to leak secret
  • It can be exploited to escalate privilege
Software security

- Which of the following techniques belong to dynamic analysis
  - Regression test
  - Fuzzing
  - Symbolic execution
  - Abstraction interpretation
Software security

• Which of the following techniques belong to dynamic analysis
  • Regression test
  • Fuzzing
  • Symbolic execution
  • Abstraction interpretation
    • Semantic analysis
Software security

Which of the following is true about automated program analysis

- Analysis can be both sound and complete
- Dynamic analysis is complete but not sound
- Static analysis is sound but not complete
- Static analysis is neither sound nor complete
Software security

Which of the following is true about automated program analysis

- Analysis can be both sound and complete
  - NO, this is undecidable
- Dynamic analysis is complete but not sound
- Static analysis is sound but not complete
  - Not all, syntactic analysis is not
- Static analysis is neither sound nor complete
  - Not all, semantic analysis can be sound
Short answers

- Similar to homework