CSE 127 final review

Chris Kanich
6/3/2011

What did we learn this quarter???
• Projects
• Homeworks
• Lectures

Projects
• Project 1
  – What is the threat model?
  – Where else/how else can these attacks be launched?
  – What can be done to prevent them?
  – Where else did these experiences reemerge?

Projects
• Project 2
  – What is the threat model?
  – What were the bugs that allowed you to perform your exploits?
  – How would you fix these problems?

Homework 1
• Problem 1: suggested solution to buffer overflows
  – What was it trying to prevent?
  – Why didn’t it work?
  – What other ‘solutions’ might you suggest?
• Problem 2: Thompson backdoor
  – Where else might the concepts from this problem be relevant?
• Problem 3: Secure Document Disposal
  – There *will* be a non-computer security question
  – Keep your head about you; get a good night’s rest

Homework 2
• IPv6 worms
  – Analyze hypotheticals using fundamentals
    • What changed? What does the attacker want? Does this change make it harder to achieve?
  – Don’t be afraid to ask questions about networking concepts if you don’t understand certain attacks
• Brute force attacks on access control
  – What about an analogy to Computer Security?
Main topics

- Necessary but NOT sufficient
  - this is NOT a complete study guide
  - your notes should be better than this

Assembly-level vulnerabilities

- Low-level programming
  - What assumptions were early computer programmers operating under?
  - Why did this cause problems?
- What defenses have been developed?
  - What breaks them?
  - What (if anything) do they achieve nowadays?

Writing secure code

- DJB
  - Why does Hovav love qmail?
  - What are the design decisions that have made qmail secure?
- Syscall interposition/control flow integrity
  - What do these technologies provide?
  - How do they make an attacker’s life harder?

Network Security

- Review the basics of how Internet communication works
  - What are the assumptions, capabilities, threat models, etc when there is a network attacker
  - My slides & Stefan’s slides are good for this
- Can you explain NAT traversal?
  - What is it used for? What “security” mechanism is it thwarting?
  - How could this be used for evil?

Browser Security

- What’s the threat model????
  - What can attackers do?
  - What extra stuff can attackers do?
- Same Origin Policy
- Heap Spraying
- Cross site (request forgery/scripting)
  - Let your project be your guide

Browser Security Cont’d

- HTTPS
  - What are the major differences?
  - How can they be circumvented by an attacker?
- Phishing
- Other “layer seven attacks”
  - Aka PEBKAC
Chris’s axegrinding corner

• Consider the attacker’s motivations
  – What can you do with information about the economics of a given scam?
• Where will you get your most bang for your buck when deploying defenses?
• Spam filtering: false POSITIVES are bad, false NEGATIVES are a nuisance

Final Suggestions

• Study hard
• Sleep early
• Think slowly