CSci 4271W
Development of Secure Software Systems
Day 7: More Threat Modeling

Stephen McCamant
University of Minnesota, Computer Science & Engineering

Outline

Starting synchronous lecture recording

More perspectives on threat modeling

Threat modeling: printer manager

Logistics update, incl. project 1

Attacks and shellcode followup

Recording from today

- By multiple requests, I will record my synchronous lectures starting today
- No recording of break-outs and discussions
- For best privacy, ask questions by chat

Outline

Starting synchronous lecture recording

More perspectives on threat modeling

Threat modeling: printer manager

Logistics update, incl. project 1

Attacks and shellcode followup

Software-oriented modeling

- This is what we've concentrated on until now
  - And it will still be the biggest focus
- Think about attacks based on where they show up in the software
- Benefit: easy to connect to software-level mitigations and fixes

Asset-oriented modeling

- Think about threats based on what assets are targeted / must be protected
- Useful from two perspectives:
  - Predict attacker behavior based on goals
  - Prioritize defense based on potential losses
- Can put other modeling in context, but doesn't directly give you threats

Kinds of assets

- Three overlapping categories:
  - Things attackers want for themselves
  - Things you want to protect
  - Stepping stones to the above

Attacker-oriented modeling

- Think about threats based on the attacker carrying them out
  - Predict attacker behavior based on characteristics
  - Prioritize defense based on likelihood of attack
- Limitation: it can be hard to understand attacker motivations and strategies
  - Be careful about negative claims

Kinds of attackers (Intel TARA)

- Competitor
- Data miner
- Radical activist
- Cyber vandal
- Sensationalist
- Civil activist
- Terrorist
- Anarchist
- Irrational individual
- Gov't cyber warrior
- Corrupt gov't official
- Legal adversary

Kinds of attackers (cont'd)

- Internal spy
- Government spy
- Thief
- Vendor
- Reckless employee
- Information partner
- Disgruntled employee

Outline

Starting synchronous lecture recording

More perspectives on threat modeling

Threat modeling: printer manager

Logistics update, incl. project 1

Attacks and shellcode followup

Setting: shared lab with printer

- Imagine a scenario similar to CSE Labs
  - Computer labs used by many people, with administrators
- Target for modeling: software system used to manage printing
  - Similar to real system, but use your imagination for unknown details

Example functionality

- Queue of jobs waiting to print
  - Can cancel own jobs, admins can cancel any
- Automatically converting documents to format needed by printer
- Quota of how much you can print

Things to model

- Draw architecture with data flows and trust boundaries
- List assets and attackers
- What are the threats a system must block?

Outline

Starting synchronous lecture recording

More perspectives on threat modeling

Threat modeling: printer manager

Logistics update, incl. project 1

Attacks and shellcode followup

Project 1 code now available

- BCImgView source code and binary to attack are now posted
  - On the public course web site, Assignments page
- About 1000 lines of code, including comments
  - Remember, not all equally relevant to security
- Also available: sample normal images

About project 1 vulnerabilities

- The code has at least four intentional vulnerabilities that are known to be exploitable
- For full credit in auditing and attack, you will need to get at least three of these
- Coincidentally, BCImgView supports three image formats

Complete instructions coming soon

- Coming soon: more details on format and logistics of your submission
- In upcoming lectures: advice about technical writing in security
- First due date still Friday, October 9th (week from Friday)
  - Recommend starting right away

In lab: return of BCLPR

- Tomorrow's lab will again use the buggy BCLPR program
- Move on from auditing to attacking
- Instructions posted by late tonight
  - And you can already review the auditing code example

Preferred followup venue: Piazza

- Best place for discussing and asking questions about labs and lecture exercises after the fact in Piazza
- Suggestion: 24 hour delay before public spoilers
- Most effective if both students and staff are in the discussion

Outline

Starting synchronous lecture recording

More perspectives on threat modeling

Threat modeling: printer manager

Logistics update, incl. project 1

Attacks and shellcode followup

Reminder: what is shellcode

- Machine code that does the attacker's desired behavior
- Just a few instructions, not a complete program
- Usually represented as sequence of bytes in hex

Reminder: basic attack sequence

- Make the program do an unsafe memory operation
- Use control to manipulate contol-flow choice
  - E.g.: return address, function pointer
- Make the target of control be shellcode

Overflow example hands-on

- Steps of overflow-from-file example

Side-effects example

- A second example with a new wrinkle