CSci 4271W
Development of Secure Software Systems
Day 9: More Threat Modeling

Stephen McCamant
University of Minnesota, Computer Science & Engineering

Outline

Threat modeling: printer manager

Announcements intermission

Attacks and shellcode lab 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

Assets and attackers

- What assets is the system protecting?
  - What negative consequences do we want to avoid?
- Who are the relevant attackers?
  - What goals motivate those attackers?
- Take 5 minutes to brainstorm with your neighbors

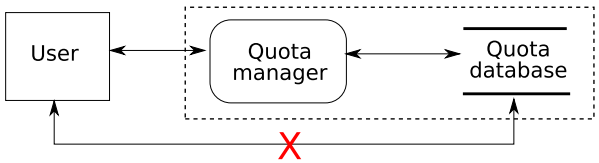
Assets and attackers

- Administrators:
  - Want to let students do printing needed for classes
  - While minimizing spending on paper, toner, and admins responding to problems
- Attackers:
  - Non-students might try to print
  - Students might try to print too much
  - Students might interfere with each other

Data flow diagram

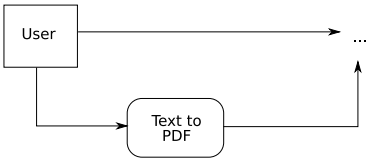
- Show structure of users, software/hardware components, data flows, and trust boundaries
- For this exercise, can mix software, OS, and network perspectives
- Include details relevant to security design decisions
- Take 15 minutes to draw with your neighbors

DFD #1: access control



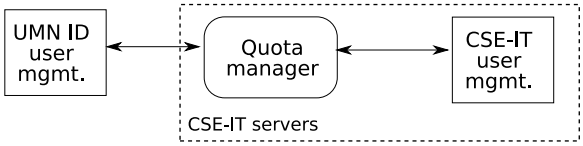
- The absence of data flow will need an implementation

DFD #2: optional processing



- Text-to-PDF can't add much risk here

DFD #3: a trust boundary



- Different risks from where authentication lies

STRIDE threat brainstorming

- Think about possible threats using the STRIDE classification
- Are all six types applicable in this example?
- Take 10 minutes to brainstorm with your neighbors

STRIDE examples

S: make your jobs look like a different student's
T: insert mistakes in another student's homework
R: claim you don't know why your quota is used up
I: read another student's homework
D: break printing before an assignment deadline
E: student performs administrator actions

Outline

Threat modeling: printer manager

Announcements intermission

Attacks and shellcode lab followup

Brief announcements

- Problem set 1 is available on the public web page now
  - Due a week from Friday, 2/25
- The first midterm exam will be a week from today in class
  - Open book, open notes
  - You will have the whole class period
  - Topics will be memory safety bugs and attacks, and threat modeling
  - Similar concepts, but less depth, than labs and p-set

Outline

Threat modeling: printer manager

Announcements intermission

Attacks and shellcode lab 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