388 Discussion 4/16

Final Exam Review

Short Answer

- MITM vs Eavesdropper
  - Active vs passive attacker
  - MITM attacks against non-authenticated protocols like Diffie-Hellman
  - Passive eavesdroppers are hard to detect
- Principle of Least Privilege
  - Every entity only has the permissions necessary to complete its task
  - Reduced damage if a user account or program is compromised

Short Answer

- DEP (Data execution prevention)
  - Cannot execute code on the stack
  - Prevents an attacker from executing instructions placed on the stack

- Salting Passwords
  - Identical passwords will have different salted hashes
  - A rainbow table attack would need to take the salt into account

Cross-site request forgery

- What is it?
  - Sending unauthorized commands on behalf of a user
- What can it do?
  - Could be used to transfer funds out of a bank account
- What can we do?
  - Include a randomly generated token with each request
  - Properly defend against cross-site scripting

ARP Spoofing

- What is it?
  - An attacker sends an ARP reply to associate his MAC address with another resource
- What can it do?
  - An attacker could man-in-the-middle your connection
- What can we do?
  - Static ARP entries

Hash Collisions

- What is it?
  - When two different pieces of data have the same hash value
- What can it do?
  - Remember part 2 of project 1?
- What can we do?
  - Use better hash functions like SHA-256 or SHA-3

Cold-boot Attack

- What is it?
  - Resetting a computer and immediately dumping the contents of memory
- What can it do?
  - Steal encryption keys that were stored in memory
- What can we do?
  - Limit the amount of time keys are stored as plaintext in memory

Picture-in-Picture Attack

- What is it?
  - Displaying a fake browser window in a real window
- What can it do?
  - Steal a user’s password
- What can we do?
  - Include a unique icon or image in your browser

Control Hijacking

```
/* Break me please */
int funky(char *str) {
    char buf[100];
    unsigned short len = strlen(str);
    if (len >= 100) {
        return -1;
    }
    strncpy(buf, str, strlen(str);
    return 0;
}
```

Exploit?

SQL Injection

```
$username = $_POST[user];
$password = $_POST[pass];
$sql = "SELECT * FROM users WHERE name = '$username' AND password = '$password'";
$rs = mysql_query($sql);
if (mysql_num_rows($rs) > 0) {
        // Success
}
```

- Can an input cause the (AND…) to be ignored?
- add \ before characters (‘,”,\,null) what can be done?
- Prepared statements prevent data from becoming part of the SQL query

```
INSERT INTO PRODUCT (name, price) VALUES (?, ?)
```

Electronic Voting

- Goals of Electronic Voting
  - Confidentiality
  - Authentication
  - Integrity

- Scenario 1
  - How can the voter's identity be leaked?
  - Who verifies the voter's identity?

- Scenario 2
  - Is confidentiality preserved?
  - Authenticity of votes?

Questions?