a1 documentation
Boris Kravchenko
bkravche
20332359

sploit3.c

Vulnerability: The vulnerability exploited is incomplete mediation *(submit.c 150).* It's possible to replace the bash echo command that the submit command calls with an arbitrary executable called echo, which will be run as root.

Exploit: My program outputs and compiles a C executable named echo which appends a new user (hacker::0:0:hacker::/bin/bash) to /etc/passwd. This C executable is placed in present working directory. Then submit is called, and submit uses the echo inside present working directory, instead of the bash echo command. Once submit finishes, my exploit spawns a new shell with the hacker account.

Repair: This exploit could be repaired by using a different, safer method to write to a log file, without using echo redirection.

sploit4.c

Vulnerability: The vulnerability exploited is the format string vulnerability *(submit.c 198)*. It's possible to set src to contain a format string which overwrites the return address of the main method to any arbitrary value.

Exploit: My program calls submit with a specially crafted format string as the src parameter, and shellcode as the message parameter. The beginning of the string hardcodes the location of the return address, and uses %x to move up the stack to the src buffer, and %n to write to the location that's at the front of the string buffer - which is the location of the return address. It does two unaligned writes to overwrite the address. The value written into the return address is the address of the message string, which contains shellcode.

Repair: This can be fixed by replacing printf(src) *(submit.c 198)* with printf("%s", src).

Written Questions

1. Traditional voting, as described in the question, is susceptible to all four attacks. For interception, the adversary can wiretap the phone line of the polling station to get the results of the vote before it's made public, the adversary doesn't have authorization to the results in this case. For interruption, the adversary can phone in a bomb threat for the polling station, which will cause it to temporarily close, which would delay the vote. For modification, the adversary can do a man-in-the-middle attack on the phone call and the signed report. The adversary would intercept the phone call, get the result of the vote, and call the headquarters himself to submit the result. For the signed report, he would intercept the mail, change the value in the report, and forward it to the headquarters. This attack assumes there's no authentication in place for the phone call, or for the report. For fabrication, the adversary, with the aid of a corrupt official, can perform ballot stuffing by submitting multiple ballots into the ballot box while the official watching the box looks the other way.

Internet voting, as described in the question, is also susceptible to all four attacks. For interception, the adversary installs a keylogger on the voter's phone/computer and records who the voter voted for. For interruption, the adversary launches a DDOS attack on the centralized server, which takes it down and prevents voters from voting, which delays the vote. For modification, the adversary installs malware on the voter's phone/computer, which steals the authorization code by displaying a fake voting website. The user proceeds to vote on the fake website, without realizing that they didn't actually vote. The attacker then goes on the real voting website and uses the authorization codes he collected. For fabrication, it's possible that the centralized server itself is compromised (by a rogue developer writing a back door for example), and the adversary can generate extra keys and use them to vote, which is the online equivalent of ballot stuffing in this example. This assumes there are no additional audits and checks in place.

In conclusion, I don't think either system, as described in this example, is more secure than the other, because they're both susceptible to all 4 attacks.

2. The cashier is expected to both identify and authenticate Alice through her signature. The authentication happens during the act of comparing the signature Alice gives to the signature on the card. If they match, then the person using Alice's card is authenticated as Alice. The identification is similar, because no two people can have the same signature, therefore the person that has the same signature as Alice must be Alice, therefore can be identified as Alice.

This model breaks down for online transactions because an adversary can simply take a photo of Alice's signature, as it appears on the card and submit it with the purchase.