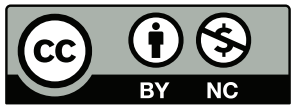
Searching Securely: Technical Issues with Warrants for Remote Search



The Fourth Amendment to the U.S. Constitution

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Note well: “unreasonable”, “probable cause”, “particularly describing”.

Remote Search, AKA Lawful Hacking

- Done today—but the FBI has said very little about how it's done
- Goes back to at least 2001
- A 2007 search warrant describes the "Computer IP Address Verifier" (CIPAV)—collects IP and MAC addresses, open ports, browser, OS version, username
- Requires two court orders: a search warrant for the hacking, and a "pen/trap" order to operate
- (For legal reasons, pen/trap orders do not require probable cause.)
- Hacking foreign computers generally does *not* require a warrant

Rule 41 of the *Rules of Criminal Procedure*

- Governs issuance and execution of search warrants
- Specifies that magistrates can only issue warrants for searches in their district
- Proposed change: a single warrant will suffice to search—"hack"—many computers if (a) their location has been "concealed through technological means" or (b) the warrant is for computers in five or more districts
- There are problems. . .

Searching Victims

- The proposed change legalizes mass searches of *victims*' computers
- The supporting documentation suggests using a "common scheme" to infect them
- A common scheme might fail on some computers, and in failing cause damage
- Common software can't be narrowly targeted, which means it could be reverse-engineered and repurposed, especially if it spreads too far
- Testing is *never* completely sufficient
- These are *victims* of the crime

Location

- Is a VPN a “technological means” to conceal location? Or is it a normal and rational protective measure?
- If you don’t know a target’s location, how do you know what country it is in?
- Would that country consent to a remote search? To any search that doesn’t use the mutual legal assistance treaty (MLAT) procedures?

Search Techniques

- The FBI won't discuss their remote search tools—but then, how can defense attorneys assess its reliability?
- In the last few months, serious problems have been found in FBI lab techniques for hair analysis and DNA similarity reporting
- Courts do not have a deep understanding of the technology, either

Authenticity and Integrity

- Normal forensic examination of computers relies on read-only copies, verified by a cryptographic hash of the disk
- You can't do that remotely—the disk will change while the search program is running
- Many search techniques will change the "last accessed time" field of files' metadata
- Hard to search the free block list on an active system

Specificity

- How is a search of *many* computers “particular”?
- What parts of the computer may be searched, and for what?
- That’s a contentious issue in general—and is far more important when searching victims’ computers

Notice

- How are search warrant targets to be notified?
- Email? Spammers and hackers are already sending email purporting to be from the FBI.
- Pop-ups? They'll be ignored.
- Physical mail? Tracing computers is expensive and difficult

The Rule Change Process

- We, Google, and many organizations (e.g., the EFF and the ACLU) file statements opposing the rule change
- The Advisory Committee approved it anyway
- Next steps: the Standing Committee, the Judicial Conference, the Supreme Court, and Congress
- It may go into effect December 2016

Our Recommendations

- Don't issue multi-computer warrants
- Specify exactly what area of the computer can be searched
- Try hard to get international cooperation when searching overseas computers
- Work with the technical community on better notice mechanisms