Forced Guard Node Rotation

Problems and Possible Solutions

DCAPS Winter 2015

This talk was given by Griffin Boyce

Senior Censorship Researcher at OpenITP
and Fellow at The X-Lab

https://github.com/glamrock

Guard Exhaustion

Because the adversary's goal is to exhaust options for guards they do not control, I call this phenomenon “guard exhaustion.”

What

- Guard nodes are critical, but can be blocked by network operators at local and regional levels.
- Adversarial position
  - Operator or adversary between the user and the guard node
  - ISPs can be forced to block IPs for various reasons
  - Local network ops can block IPs to prevent abuse
  - Blacklists can be added to routers or local firewall by choice, through trickery, or due to vulnerability.

The Danger

- Guard exhaustion reduces complexity of the circuit – and if the adversary runs multiple relays, it becomes much more likely that the adversary controls the entire circuit.
- Only highly technically-advanced users will ever notice that this is happening.
- Because only very advanced users will notice it *when* it happens, effective mitigation relies on the user knowing that they are at risk. Few do.

The Danger

- It's not currently possible to detect adversarial guard nodes.
  - There's no injected ads or malware.
  - It's easy to simply set up a relay and wait for it to be awarded guard status.
  - The difficult part is determining the user's initial guard.
  - To eliminate access, simply DDoS that guard (and the fallback guard). Repeat the process for all new guards.
- But, it's difficult to conduct this attack.
  - 6849 total Tor nodes; 1591 Guard nodes (23%)

Who would do this?

- Governments
  - Political control
  - Economic advantage
- This might make sense for extremely high-level political targets (eg, journalists in Belarus, Muslim activists in Rohingya) and for economic espionage where state interests are involved.
- The Belarus Problem.

Who would do this?

- ISPs
  - Forced by government
  - Personal vendetta of employee
  - Economic espionage
- Individuals (unlikely)
  - Hacking routers is easy
  - The market for technical “solutions” offered to stalkers and paranoid parents is large
  - Some researchers only publish at hacker conferences

Wait, are people actually doing this?

Yep.

Incidents have been reported in UK and Germany.

(but it still seems incredibly rare)

Technical Mitigations *Now*

- Using a bridge means that this bridge becomes your guard node by default, and changes the circuit from a 3-node to 4-node.
  - To change guards, just change the bridge.
  - Doesn't avoid service restriction, but does provide protection against using a bad guard.
  - Side note: the adversary could attempt to flood the bridge and flashproxy pools, but no one's tried.
- Using flashproxy allows users to have ephemeral bridges, and therefore ephemeral guards.

Issues with usability

- As most users have average technical understanding, how can we convey this information in a way they can understand?
  - Currently Tor Browser automatically chooses new guards, which is ideal for usability, but has some pitfalls with security.
- How to avoid false positives?
  - 'In the lab, the false positive rate is close to zero.' (A. Johnson, 2015).

Issues with usability

- False positives:
  - If Belarus blocks all 6800 nodes suddenly, how can we distinguish this blocking event from a targeted attack?
    - But, if Belarus took a smarter tactic, they'd block the 1591 good guard nodes and leave only ones they set up.
  - The network naturally expands and contracts with time, and it's not unrealistic to expect some users to have to change guards more than every 90 days.

User Interface Options

1) Select a new set of guards automatically
2) Select new guards, but alert the user that it happened
3) Convey to users that they have run out of guards, and present a variety of options.
4) Initially fall back to flashproxy, while offering subtle alert with dropdown options.

#2 User Experience Considerations

- Users may not know what to do with the information
  - “Am I being targeted? What do I do?”
  - One solution may be better served by knowing how many times this has happened to them.
- Users may not notice if it is subtle.
- Users may disregard it if the alert is not phrased in a way they understand. (Nesmith 2014)

#3 User Experience Considerations

- Users will likely click a simple “Continue” without knowing what is going on.
- Proposed alert options:

  [Try Connection Again]

  [More Information]

  [Automatically find new guards]

  [Use a bridge]

#4 User Experience Considerations

- Users have slower service speed, which increases the likelihood that they will notice the guard exhaustion notification.
- Because a browser notification can be persistent, it offers users a way to change their preference or see new status updates without interrupting their current session.

Open Questions

- What's the false-positive rate with real users?
- Do the group of affected users represent more than 0.0000025% of Tor's overall userbase?
- Will adjustments to the guard rotation parameters eliminate this problem?

Thanks! ^_^