

Hacker Conference CFP Field Guide

Practical guidance for making the real work visible to a conference review committee.

What makes it a hacker talk

A hacker conference proposal should show what was broken, built, reversed, abused, measured, or learned through unusual first-hand access. It should make a technically curious reader want to see the mechanism, not merely agree that the topic is important.

The essential question is practical: what can this speaker show this audience that they could not get from a policy panel, product briefing, management conference, or blog post?

This guide is independent and unofficial. It is informed by public DEF CON guidance and historical outcome patterns from the CFP Doctor project. It does not reproduce private submissions or individual reviews, and it does not speak for DEF CON or any other review board.

Put the break on the page

The strongest evidence is a working exploit, demonstrated bypass, new vulnerability, tool, code release, original dataset, or a first-hand incident account with access no outside commentator could have. These artifacts do not replace judgment, but they let the reviewer see that the work exists.

Name the target. Name the version when it changes the result. Explain the preconditions honestly. A local foothold before post-exploitation is not automatically a fatal limitation; a precondition that already grants the claimed impact may be.

If there is no exploit, demo, tool, or new finding, say what the audience receives instead. A historical account, culture talk, legal analysis, or war story needs irreplaceable access and a clear lesson. "There is a lane for this" does not itself make the session compelling.

Write to the practitioner

Read the abstract and ask who "you" means. If it means a buyer, executive, organization, compliance leader, or security program, the pitch may be aimed at the wrong room.

Practitioner framing uses verbs: dump, trace, intercept, reverse, exploit, bypass, fuzz, recover, instrument, build, test. These words only help when they describe real work. Sprinkling them into a management talk will not survive a human read.

Weak: "Organizations must prepare for the emerging threat landscape."

Stronger: "We trace the parser state that makes the bypass possible, reproduce it against three current builds, and release a harness for testing other implementations."

Make the outline contain the attack

Reviewers need more than a table of contents. "Introduction, background, methodology, demo, conclusion" does not reveal whether the proposed session has forty-five minutes of substance.

Inside the outline, name the operations, targets, versions, failure modes, and results. A reader should be able to follow the movement from access to observation to exploit or lesson. Detailed section timings may help with pacing; they do not make an empty section substantive.

A useful outline might include:

- Target and access: exact devices, builds, protocols, samples, or incident role.
- Reconnaissance or reversing: what was inspected and what changed the hypothesis.
- The break: primitive, chain, preconditions, and impact.
- Proof: measurement, exploit, demonstration, affected versions, or first-hand records.
- Generalization: the transferable method or broader target class.
- Release and disclosure status.
- What attendees can attempt themselves.

Explain novelty without pretending everything is new

Prior art is common. Combining known primitives into a new capability can still be worthwhile when the combination and result are clear. Name what exists and what you add.

Prior presentation is not automatically disqualifying. Disclose it and explain what changed. Reviewers care about getting a worthwhile session, not about forcing every idea to appear from nowhere. Re-presenting an unchanged talk is a different problem.

Do not let a fashionable target stand in for a contribution. A routine bug against a surprising device may create audience draw, but the technique and impact should be described separately.

Know when the project is the talk

A great tool can produce a thin talk. If the proposal mostly demonstrates features, installation, and usage, consider a demo lab, village, or tool-focused program. If the talk explains a research question, technique, or class of failures and the tool makes that work reproducible, say so directly.

A redirect is advice about format, not a declaration that the work is weak.

Use specificity as credibility

Concrete targets beat categories. "Three BMC firmware families" tells the reviewer more than "critical infrastructure." A current version, sample size, exploit condition, or measured time makes the scope testable.

Avoid absolute impact statements unless the evidence supports them. Explain what did not work, what remains untested, and where the result stops. Technical reviewers often trust a bounded claim more than a sweeping one.

Establish first-hand access

A useful bio answers why these speakers could do this work. It might name the system they built, incident they handled, project they maintain, disclosure they led, dataset they collected, or research area they have practiced.

First-time speakers belong at hacker conferences. Do not manufacture conference experience. Link verifiable work when the CFP permits it and let the proposal demonstrate command of the material.

Before you submit

- The title names a target, mechanism, or result.
- The abstract makes the break or first-hand access explicit.
- The pitch speaks to practitioners rather than buyers.
- Preconditions and limitations are honest.
- The outline contains the technical actions and evidence.
- Prior work and prior presentations are disclosed and differentiated.
- A tool supports a research story, or the proposal targets the right tool program.
- The bio establishes access without inflated credentials.
- Disclosure and release promises are realistic by the event date.
- Every technical claim, number, CVE, and link has been checked.
- The proposal answers the current event's actual form and rules.

A draft can have the right shape and still miss because the work is too narrow, the program is full, or experts disagree about its importance. A score cannot resolve those judgments. The purpose of the pre-check is to force the important questions onto the page while the author can still answer them.

Sources and currency

This edition was checked on October 2, 2026. The current event call is published at <https://defcon.org/html/defcon-34/dc-34-cfp.html>, and official call announcements are posted at <https://forum.defcon.org/>. The event's current form and terms control when they differ from this guide.