Gmail **Carlos Denner <carlosdenner@gmail.com>**

Fit check: “Prompt Injection, Demystified”: a Practice-section playbook for engineers

10 messages

Carlos Denner <carlosdenner@gmail.com> Mon, Oct 27, 2025 at 2:51 PM
To: eic@cacm.acm.org

Dear Editor-in-Chief,

I would like to sanity-check a short paper possibility with you, please.

Working title
Prompt Injection, Demystified: Market Landscape, Engineering Practice, and Research Roadmap for Safer LLM Systems

Fit for CACM Practice
The Practice section’s mission is to enhance practitioners’ understanding and improve job performance; CACM is elevating Practice to stand co-equal with Research. Our article is written for working engineers and tech leads deploying LLMs, with clear patterns, measurement rubrics, and an MVP-ready reference architecture.

Prompt injection remains the most visible, fast-moving risk in LLM applications; CACM welcomes unsolicited submissions that provide broad, practical value to a diverse technical readership. This survey distills what works in production today and what’s next.

Practitioner takeaways
1) A reference gateway architecture (policy engine + guardrails + classifier + tool mediation) with options for sub-10 ms, ≤100 ms, and offline workflows.
2) A defense matrix comparing effectiveness vs. implementation complexity vs. runtime cost (signatures, classifiers, guardrails, multi-LLM/agent, tokenizer-level).
3) A repeatable evaluation kit aligned to current industry practice (red-team prompts, CI/CD gates, success metrics) that teams can drop into pipelines immediately.

Abstract
Prompt injection subverts guardrails, exfiltrates data, and hijacks tool use. We synthesize the state of practice (deployed patterns and pitfalls), the market (commercial tools and open-source guardrails), and the research corpus (benchmarks, detectors, mitigations). Building on a cleaned study of 24 unique patents plus a curated survey of academic papers and repos, we present a practitioner’s playbook: threat models, a deployable gateway architecture, and a comparative defense matrix covering effectiveness, cost, and latency. We close with engineering checklists and an agenda for session-level and multimodal defenses. Artifacts (datasets, search protocol, code to reproduce figures) will be released with the article for reproducibility. CACM’s practitioner audience and renewed emphasis on Practice make it the ideal venue for this piece.

Would this angle be a good fit for CACM Practice? Any guidance on emphasis or scope is welcome.

Thank you,
Carlos Denner dos Santos, PhD

CACM Editor in Chief <cacm.editor.in.chief@gmail.com> Wed, Oct 29, 2025 at 11:14 AM
To: Carlos Denner <carlosdenner@gmail.com>
Cc: eic@cacm.acm.org, Terence Kelley <tpkelly@eecs.umich.edu>

Forwarding to co-chair of Practice section.

Jim

James Larus

Editor-in-Chief, Communications of the ACM (CACM)
http://cacm.acm.org/
Professor Emeritus, EPFL, Lausanne Switzerland

[Quoted text hidden]

Terence Kelly <tpkelly@eecs.umich.edu> Wed, Oct 29, 2025 at 8:56 PM
Reply-To: Terence Kelly <tpkelly@eecs.umich.edu>
To: Carlos Denner <carlosdenner@gmail.com>
Cc: CACM Editor in Chief <cacm.editor.in.chief@gmail.com>

Hi Carlos,

Thanks for reaching out to CACM Practice.

I'll try to find an editor with an appropriate background to work with you to refine your ideas.

You may ping at weekly intervals until you hear back from us.

Thanks.

-- Terence Kelly, Practice Co-Chair

On Wed, 29 Oct 2025, CACM Editor in Chief wrote:

> Forwarding to co-chair of Practice section.
>
> Jim
>
> James Larus
>
> Editor-in-Chief, Communications of the ACM (CACM)http://cacm.acm.org/
> [Quoted text hidden]

Carlos Denner <carlosdenner@gmail.com> Thu, Oct 30, 2025 at 10:39 AM
To: Terence Kelly <tpkelly@eecs.umich.edu>
Cc: CACM Editor in Chief <cacm.editor.in.chief@gmail.com>

Thanks, James and Terence! This is great news. I am looking forward to it.

Regards,
Carlos Denner dos Santos, PhD

[Quoted text hidden]

Carlos Denner <carlosdenner@gmail.com> Tue, Nov 4, 2025 at 11:33 AM
To: Terence Kelly <tpkelly@eecs.umich.edu>
Cc: CACM Editor in Chief <cacm.editor.in.chief@gmail.com>
Bcc: Kelsen Andrade <hkelsen@gmail.com>, charley spektor <cspektor@onthebrinkb2b.com>

Dear Terence and James,

As you guys demonstrated interest, I took the liberty to prepare a manuscript following CACM guidelines.

Would you please take a look at it and confirm whether my manuscript fits and is timely? If so, I am going to anonymize it, and submit it through the system for peer review.

Please let me know,

Carlos Denner dos Santos, PhD

On Wed, Oct 29, 2025 at 8:56 PM Terence Kelly <tpkelly@eecs.umich.edu> wrote:
[Quoted text hidden]

prompt_injection_cacm.pdf
1342K

Terence Kelly <tpkelly@eecs.umich.edu> Tue, Nov 4, 2025 at 8:59 PM
Reply-To: Terence Kelly <tpkelly@eecs.umich.edu>
To: Carlos Denner <carlosdenner@gmail.com>

Hi Carlos,

Will get back to you in a few days.

Note that CACM submissions are not anonymous.

Thanks for thinking of CACM.

-- Terence
[Quoted text hidden]

Carlos Denner <carlosdenner@gmail.com> Fri, Nov 21, 2025 at 3:46 PM
To: Terence Kelly <tpkelly@eecs.umich.edu>

Hi Terence,

Did you have a chance to look into the manuscript?

Thanks a lot,
Carlos Denner dos Santos, PhD

[Quoted text hidden]

Terence Kelly <tpkelly@eecs.umich.edu> Fri, Nov 21, 2025 at 8:50 PM
Reply-To: Terence Kelly <tpkelly@eecs.umich.edu>
To: Carlos Denner <carlosdenner@gmail.com>

Hi Carlos,

I tried to find an editor to give more detailed guidance but the most qualified people are busy. Thanks for your patience.

Since you have a paper written, go ahead and submit to CACM Practice.

Your chances of acceptance might increase if you adjust the presentation style prior to submission. Generally we discourage the overuse of PowerPoint-like bullet lists, boldface, big loud graphics.

Our preferred modus operandi is to work with authors from the concept stage thru the outline stage, so next time please approach us sooner.

Thanks.

-- Terence
[Quoted text hidden]

Carlos Denner <carlosdenner@gmail.com> Sat, Nov 22, 2025 at 1:25 PM

To: Terence Kelly <tpkelly@eecs.umich.edu>

Thanks for your feedback. I will try to adjust the presentation style and submit. Please dont be shy to give me a big major review. I worked hard on the experiment, thus I am willing to work equally hard to get it published.

I didn't know about this modus operandi, and will follow it next time.

Best,
Carlos Denner dos Santos, PhD

[Quoted text hidden]

Terence Kelly <tpkelly@eecs.umich.edu> Sat, Nov 22, 2025 at 2:34 PM
Reply-To: Terence Kelly <tpkelly@eecs.umich.edu>
To: Carlos Denner <carlosdenner@gmail.com>

Good luck.

Attached is my personal list of desirable characteristics in a Practice article. A good paper need not have all of them, nor even most of them, but a paper with none of them probably has a slim chance of acceptance.
[Quoted text hidden]

---

checklist_2025.05may.05.txt
4K