

IETF Hackathon

OpenNHP

IETF 126

18-19 July 2026

Vienna, Austria

AI attacks are outpacing defenders

Problem: AI models such as [Claude Mythos](#) can automate cyberattacks at machine speed, leaving defenders less time to detect, respond, and patch.

The connect-first model is broken for the AI era:

- Services are exposed before users are authenticated
- Visibility enables scanning, probing, and attack
- The Internet becomes a “dark forest,” where visibility creates vulnerability (*The Three-Body Problem*)

A new model: authenticate before connect

- **NHP:** Network-infrastructure Hiding Protocol
- *OSI Layer 5* cryptography verifies and authorizes the requester before connection
- Protected resources stay hidden until access is approved

Hackathon goal: Test whether NHP reduces the pre-authentication attack surface.

What we are testing

OpenNHP is the open-source reference implementation of the NHP protocol.

Project links: [OpenNHP website](#) · [GitHub](#) · [IETF 126 Hackathon wiki](#) · [NHP Internet-Draft](#)

Default-deny visibility

- An unauthenticated scan should not discover the protected service
- A malformed or forged knock should not create an access path

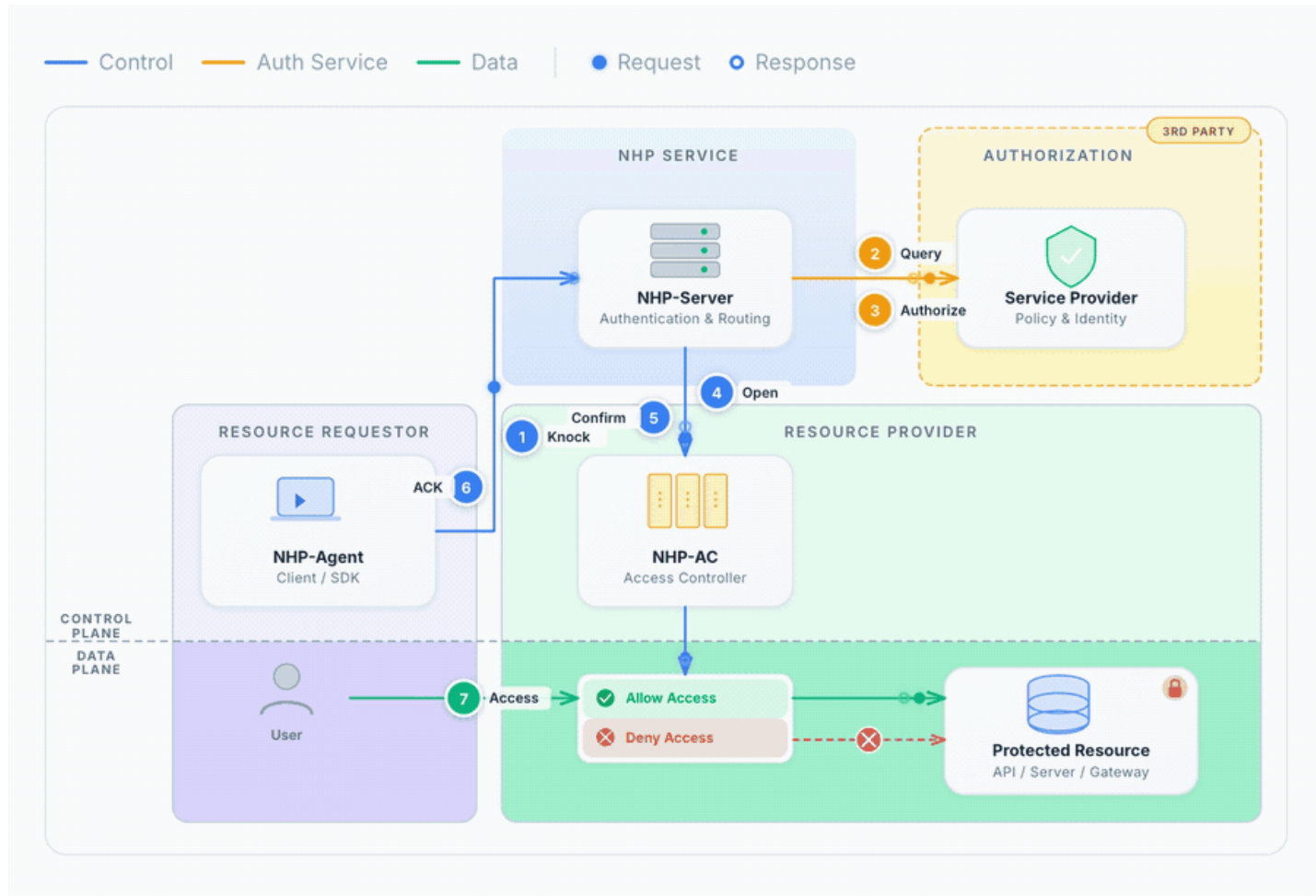
Authentication and freshness

- Replayed or stale requests should be rejected
- A valid requester should reach only the authorized resource

Access lifecycle

- The temporary path should close after its configured TTL
- Revocation should restore the deny-all state predictably

How OpenNHP grants access



What got done

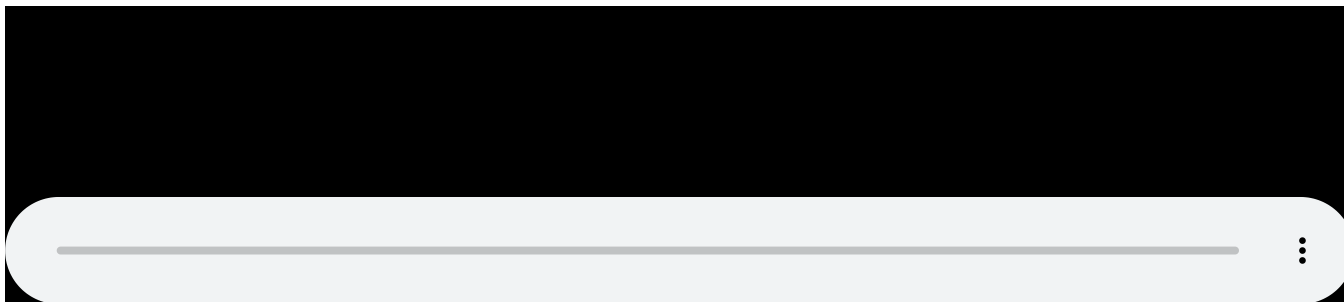
A live OpenNHP demo is now available: <https://opennhp.org/demo/>

- Experience the effect of NHP's authenticate-before-connect model
- Compare access before and after authentication
- Test the protected service—and try to break it

A complete workflow video is available on the same page.

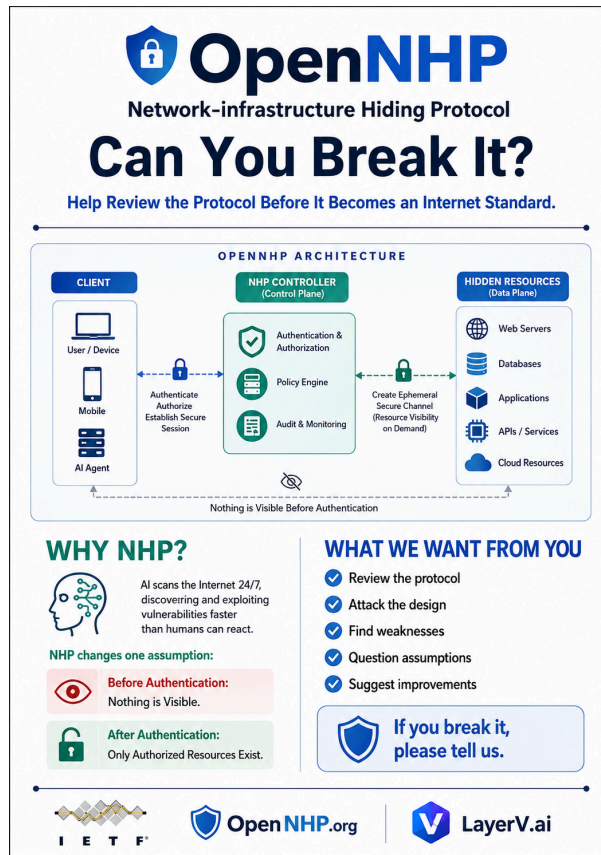
The recording shows the full journey: the protected service is invisible by default, then becomes accessible only after successful authentication.

See OpenNHP in action



Video available at: <https://opennhp.org/demo/>

What we learned



Results

- **Before authentication:** no service exposure
- **After authentication:** temporary access for authorized users only
- **Security testing:** no successful protocol break so far

Conclusion: OpenNHP worked as expected.

Wrap up

Team members:

- Benfeng Chen — Champion
- OpenNHP community

Sponsors:



Project links:

- [Website and demo](#)
- [Source code](#)
- [Internet-Draft](#)

Notes and contacts:

- support@opennhp.org