ERNW
providing security.



KEYNOTE · SCAPYCON 2026

Adventures with IPv6 and Scapy

or — The Human Element in Protocol Design and Research

IPv6 → Hop-by-Hop → Routing → Fragment → Dest-Opt → **Payload**

Enno Rey

ERNW · ERNW Research · TROOPERS

providing security.

Good morning and welcome to ScapyCon 2026. It's an honor to speak to you today. At TROOPERS, the conference that I started a while ago, we always expect that keynote speakers provide some food for thought — hence I'm grateful that Nils invited me, since this forced me to think hard about some lines which I hope will meet that bar.

Networking guy in the 90s. Founded, in 2001, one of the coolest and longest-existing vendor-independent security companies in Europe (ERNW), plus another one in 2015 (ERNW Research), and a conference in 2008 (TROOPERS). Did some research, gave a couple of talks, sat on the review board of a few conferences, contributed to some books.

Being an early Internet person, and having a background in networking, I had a strong interest in IPv6 — an interest that eventually took me to Apple.

Let me now speak about my personal journey with Scapy. It played a huge role in research I performed back in 2014 together with two other fine folks: my friend Antonios Atlasis, and Rafael Schaefer, whom I had the pleasure to work with for nearly a decade at ERNW. In that research, which we presented at Black Hat US and Europe, we looked at the unfortunate role that IPv6 extension headers played for security controls like network intrusion detection devices. In a nutshell: one could fly under the radar of major commercial IDPS solutions by adding unusual combinations of extension headers to the packet streams of otherwise easily detectable attacks.

To be able to craft various types of IPv6 packets with different combinations of extension headers, we used Chiron — a kind-of command line interface that Antonios had coded on the basis of Scapy. So at the end of the day it was Scapy which built the packets before they were sent to the wire.

When I managed a research group of interns at Apple in 2020 who were learning about IPv6, Scapy was the first OSS tool I longed to get approval for.

At this point you may wonder why there seems to be such a strong relationship between Scapy and IPv6 — just look at the workshops Guillaume Valadon regularly provides, or the demos Éric Vyncke from Cisco performs during his talks on IPv6 security. To understand why this might not be a coincidence, let's look at the history of IPv6.

In the early 90s some people realized that IPv4 might run out of address space at some future point, and initiated discussions on a new ('next generation') Internet Protocol. At the same time, in many networks IP(v4) was not the prevalent protocol, and quite some of the others — e.g. CLNP — had been developed by the ISO, the International Organization for Standardization, headquartered in Geneva. It wasn't clear which organization — the IETF, only formed a couple of years earlier, or the ISO — should be in charge of specifying such a future protocol, and there were heavy debates. That's why the term *Protocol Wars* is sometimes used for that era.

Some consensus could be established about technical requirements for IPng, but the discussion on the standardization body lasted for years — with strong proponents leaning towards the ISO — until a group of passionate people pushed towards the IETF by heavily engaging in mailing lists and showing up in large numbers at the IETF meeting in Toronto in 1994, eventually resulting in RFC 1883, considered the initial specification of IPv6.

However, the outcome was a heavily over-engineered protocol — and I'm saying this as one of the main protagonists of Apple's IPv6 efforts a couple of years ago — and some design elements might be attributed to the desire to reconcile with the ISO folks. So political factors probably influenced the technical design of IPv6.

Allow me to divert from my little history discourse for a thought experiment. What if AI had been available at the time?

What if Claude had been asked to develop a new protocol? Fair chance it would have come up with a better outcome than IPv6 in its current form.

What if Claude had been asked to provide guidance on the IETF-vs-ISO governance debate? Fair chance it would have recommended installing the ISO as the governing body for the future Internet protocol. As a consequence the course of history, and Internet development, might have been quite different — and, this is my personal evaluation, not in a good way.

History took a certain turn because a bunch of humans fought a passionate fight for the right thing.

Not many people deployed the new protocol outside experimental and research networks in the following years, so few noticed the significant security shortcomings it had. One of the main issues was — and is — the role of so-called router advertisements. These are packets, presumably sent out by routers, meant to control the core parameters and hence the networking behavior of adjacent nodes. They are unauthenticated, unencrypted, and there's no integrity protection around them.

To understand why this is a problem, look at this cute guy. The audience of *Jim Knopf und Lukas der Lokomotivführer* — primarily 6–10-year-old kids — intuitively understand the ruse that little Jim uses here, and the inherent trust issue that leads to it. It's even mentioned explicitly in the pirates' song:

Wir folgen ihm durch Tag und Nacht, denn der Stern gibt ihm Macht.

Not sure why the IPv6 designers could let such a thing slip through — but, fully seriously, there might have been good reasons for that.

One of the first security researchers to note this was Marc 'van Hauser' Heuse, in his presentation at 22C3, where he also released the THC-IPv6 Toolkit with a dedicated tool to exploit this vulnerability. That was in 2005. Fast forward to 2011, where the IETF came up with an idea to mitigate it: a switch-based feature called RA Guard.

In theory a good idea (also as in: efficient, operations-wise). But security researchers had meanwhile spotted the other main weakness of IPv6: extension headers. Marc himself had implemented adding specific headers and fragmentation to his toolkit, and independently Antonios Atlasis had started working on tooling and finding related vulnerabilities in the Linux kernel. These streams led to the research Antonios, Rafael and I started in 2013 — research that at least I myself, who never was a great coder, could only perform with the help of Scapy.

Our setting could be described as follows: we had a hypothesis — *“there have to be trade-offs which will influence security decisions”* — which led to a research question; we performed experiments to observe the behavior of network devices and to gather data; on the basis of this data we validated, refined or dismissed our hypothesis; and, of course, we documented and shared the results, which should be part of research anyway.

We essentially followed a line of thinking which, since the early modern period, is coined *the scientific method*.

Now another thought experiment. What if we'd asked Claude to come up with interesting ideas for security research in the space of IPv6? It might have suggested looking at the negative impact of extension headers on the effectiveness of network security controls — or not. (Actually I recently did, and the response was a crude mix of things.)

My thesis is that human intuition, experience as security researchers, and plain curiosity played a huge role here. Or — since Newton, presumably in 1666 under an apple tree, experienced the moment that inspired his theory of gravitation — we can phrase it differently:

Would an LLM be able to have such a moment of ingenuity that changes the understanding of the world?

Let's pursue that Gedankenexperiment further, and assume Claude would have been able to come up with the proper research question and perform the proper experiments — even with more comprehensive results than we produced, in shorter time. Then the question remains: what would have changed in the space of actual code running on actual devices, in real-life networks?

It took the IPv6 working groups at the IETF a while to realize — let alone acknowledge — that a structural problem existed. Change, in the form of an RFC (6980) that described the

problem and included recommendations, needed one guy: Fernando 'Maradona ;-)' Gont, pushing for it in the relevant circles.

So what do we take from this? It was human curiosity — and security-researcher experience stitching together the trust issues of RAs and the inherent parsing problems of extension headers — that led to specific research, and one man's doggedness to get at least a partial cure into actual implementations. While the tooling part performed by Scapy, Marc's, or Fernando's toolkits might be much easier these days, those other factors — curiosity, experience and passion — might not be replaceable by an AI.

Science cannot tell us how to live, nor which values are worth pursuing. — Max Weber, paraphrased by Hartmut Rosa

Let me slightly rephrase this, and come to the end of my talk. In the near future we, humans, may no longer be the ones who do the smartest packet analysis or write the best packet-analysis tools. However, we will still be the ones to ask the right questions, to create meaningful innovation, and to pursue what matters — the ones that use Scapy for interesting research, and as a tool to make the world a safer place.

With that I wish you all a great ScapyCon 2026, and thanks again for having me here on stage.

Links & References

Everything I pointed to on stage — the companies, the conference, and the tools and sources behind the research.

ERNW

Specialist security assessments — one of the coolest and longest-existing vendor-independent security companies in Europe.

ernw.de

ERNW Research

Incident response and research — founded 2015.

ernw-research.de

TROOPERS — the conference I mentioned

Pure, practical IT security since 2007. Make the world a safer place.

troopers.de

ADDITIONAL TOOLS & SOURCES

- github.com/aatlasis/Chiron
- github.com/vanhauser-thc/thc-ipv6
- si6networks.com/research/tools/ipv6toolkit
- Enno Rey — Structural Deficits in IPv6 (RIPE74)
- insinuator.net — A brief history of the IPv4 address space
- Black Hat EU-14 — Evasion of High-End IDPS Devices in the IPv6 Era

ERNW providing security. · ernw.de