About Fissure Security

Fissure Security is an independent security research organization. We identify foundational gaps in the industry's assumptions, prove them with working research, and propose the models that close them. Whenever possible, we publish the test files used in our research so anyone with a lab environment can reproduce the results against their own tooling. Research files that could enable malicious use are documented in the paper but not released.

We are not bound to any industry or domain. The deciding factor for what we build is always the gap, where existing tooling fails people, not the market segment.

Subtext

Subtext inspects a file the way the AI will read it, before the AI reads it.

In the AI era, every file is text. A model reads an image, a sound, a video frame, and a barcode the same way it reads a paragraph, as tokens it will act on. That collapses the line between a file and plaintext. A file's real attack surface is everything a model will extract from it, not what a human sees on screen.

Most file controls do not inspect the file. They inspect what a parser handed them. That parser was written for human consumption. It has no threat model and no security role, and it has already decided which of the file's possible readings counts as the content and which parts to drop as presentation. By the time there is text to inspect, the scope of the inspection was set by a component that was never asked to set it.

For a model there is no single canonical reading to extract. Which readings exist depends on what the model can consume, and that changes every generation. Extracted text is one projection among many, and a projection cannot be fixed by labelling it.

Subtext reduces a file to every reading a model would take from it and interrogates each one, then returns a verdict on the content rather than a rule about a folder, a sender, or a device. It runs self contained, at the boundary the file is crossing, and it holds no inventory of what sits on either side.

Content has no direction. The payload a model would ingest and the secret leaving in a container that declares something else are the same operation, caught the same way, at the same point.

Contact

Matt Boksa
Fissure Security
fissuresecurity.com