Avoiding impossibilities in well-defined systems using regulations

Saar Tochner

Many aspects of our life go from real-life/complexed/"chaotic" environments toward well-defined/schematic systems.

A key example is the known problem of regulating an automated car that needs to *choose* between hitting an old lady or a baby.

The regulator's work has been changed to define the desired behavior of systems in scenarios that are now evaluated with metrics, instead of verbal situation.

During this process, the "law" is starting to be written as equations.

We slowly uncover fundamental contradictions (that has always been there), and we need to re-adjust the existing conception of the systems' goals.

In this talk, we will dive into an example from my recent work, regarding an attacker that monopolizes the routes in the lightning network.

The lightning network is a distributed paying system, in which payments are executed along paths in the network's graph (vertexes and edges).

Anyone can open a "channel" (edge in the graph) and ask for a fee in order to participate in payment. The paying node can choose a route according to his own preferences.

The work shows that, as expected, people prefer routes with lower fees. Therefore an attacker can "hijack" routes by offering lower fees (and monopolize the market).

In addition to the above, we can show that every node's strategy that somehow prefers lower fees - will be always vulnerable to such an attack.

This idea is a very simple example of a market in which every regulation that is enforced on the routing nodes - will not be effective.

In fact, if we want to keep the network an open market (in the sense that everyone can open any channel), then the only effective policy to avoid this hijack is to route without considering the fees, which is practically useless