All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

So-called secure provenance

Once more we see the various claims surrounding the use of digital signature technology to assure the authenticity or content, and once more they ignore the obvious.

To get around almost all such technologies, I merely edit graphical content on my computer and take a picture of it.

Then I have clean provenance from my original picture of the modified picture I found.

This is nothing new. It has always been true. And it has been widely published before. And instead of taking a new photograph, I can also do a screen capture, etc.

As old as … the 1980s at least

Having said that, there are emerging methods that improve the situation a bit for those trying to provide authentic content and assure its provenance. They all involve the same fundamental concept as they did long ago. Starting with a cryptography checksum of content, adding a chain of such checksums of content plus previous provenance information, and presenting such for integrity verification. This existed long before blockchain was introduced.

Then came blockchain, combining cryptographic checksums with distributed ledgers so that there is a distributed copy of the checksum reflecting the current and all previous checksums of all of the ledger entries. Of course the problem with a long chain is that it's only as strong as the weakest link, and there are lots of weak links in the blockchain technology related to performance, the majority rules approach, and computational/environmental/energy expense.

But they are getting better at it

The newer versions of this technology are allowing for the attachment of provenance information at inception and throughout the lifecycle of content. This is done by creating a signed image, document, or other similar content component using one or more cryptographic checksums for signature; and provenance information typically used such as time, location, identifier of the user and/or owner, publisher, device, and so forth. Each modification adds additional content and signatures, and so forth. As long as the participants participate, it works reasonably well, and by embedding it in the software used for every step of the process, it creates a built-in audit trail with versioning, at the expense of time, space, and so forth. As long as everybody participates, this can work… until they don't participate any more.

Conclusions

Provenance embedding is increasingly used for content, as it is starting to be used for software bills of materials, as it has been used for inventory before that. It is a worthwhile thing to do, but for clarity, it adds little or nothing to some "security" properties like availability, use control, and confidentiality, but it is good for transparency, integrity, and accountability.

