AUTHENTICATION IN ART

AiA Art News-service

HELPNETSECURITY

Vermeer’s Camera: Uncovering the link between art criticism and cybersecurity

The 9th annual HITB Security Conference (Amsterdam, 9-13 April) features six 3-day technical training courses followed by a 2-day triple track conference.

My mother is a lacemaker; thus, her attachment to the Vermeer painting of that name. It's in the Louvre. If you only know it from reproductions, it's smaller than you may expect – just 24.5cm by 21cm. Vermeer led me into the art of the past. Whatever first attracted me to his work – perhaps a sense of quiet mystery – is not dispelled by Philip Steadman's book Vermeer's Camera.

Over the last century, there has been acceptance that artists of this period used optical aids. Steadman went further. He reconstructed the room layouts from some of Vermeer's pictures (one reconstruction including Carol Vorderman at the virginals). By perspective geometry, he deduced that five of them were painted in the same room using a booth-sized camera obscura projected onto the rear wall.

Tantalisingly, the painting Allegory of the Faith may actually show a tiny image of this booth, reflected in a mirrored sphere. Scientific studies in art history, however, raise as many questions as settling answers. This is not the conclusive detective work of early crime novels.

Cybersecurity and art forgery

With the startling price rises in the art market, the current interest in forgery is unsurprising. For more details on the forensics, consider developments in the case of the Cranach 'Venus'. Art crime, in all its guises, is now big business. Forgers (always 'sophisticated' – just as hoaxes are always 'ingenious') are, in our terms, active adversaries. They know how art historians think. They subvert art historians' aesthetic judgements. Yet scientific analysis and due diligence can help defeat them.

Recently, there has also been a convergence between the language of information security and art criticism: we now talk of 'provenance', 'curation', 'authentication' and 'attribution'. In our world, this is the language of governance and regulation.

Forensics provides evidence of who, what, and how. Today, the business need for computer forensics extends beyond litigation support into compliance. These techniques are now needed in incident response for root cause analysis. The General Data Protection Regulation (GDPR) requires this type of analysis, so that incidents are not repeated.

Tracing provenance

In information security, provenance is now a crucial aspect of governance. The GDPR requires you to keep track of where personal data came from (and where it goes).

Similarly, for software developers, it is vital to know where any open source code came from. Open source needs be kept up to date to patch security vulnerabilities, and it must be removed when it is no longer being maintained. Again, end-users downloading software rely implicitly on provenance. A public app store is no more reliable a provenance than a dodgy art dealer; organisations need their own corporate app store which contain only curated apps, verified for security.

Extending authentication

When we talk about authentication, we mainly think of users. The art world reminds us to focus on the authentication of objects. For us, this means devices and programs; usually this is achieved with digital signatures. However, most systems do not enforce authentication of devices and programs as thoroughly as authentication for users. Mission-critical systems should authenticate everything, as well as everyone.

Security practitioners therefore need to extend business processes to cover:

- Root cause analysis for security incidents, including keeping appropriate records
- Provenance of data and code. Do you know where it all came from?
- Comprehensive curated content. Does your app store contain all the apps your users may reasonably need?
- Authentication of devices and programs – not just users

Attack attribution

Finally, attribution. It is more common nowadays to see public attribution, as governments try to hold hostile organisations accountable for attacks like WannaCry. Will these public attribution statements change anyone's point of view, or are they sabre-rattling? Governments aren't going to produce their evidence for who did attack; and unsympathetic people would dismiss those facts as “fake news” even if they did. Provenance can at least help to detect fake news though.

A last note on the question of attribution. In Alan Bennett's play Single Spies, Anthony Blunt (already known by the authorities to be a Soviet spy) unexpectedly encounters the Queen. They discuss van Meegeren, the Vermeer forger. Blunt demurs:

– I still think the word “fake” inappropriate, Ma'am.
– If something is not what it claims to be, what it is?
– An enigma?
– That is, I think, the sophisticated answer.

After she leaves, a shaken Blunt remarks:

– I was talking about art. I'm not sure she was.