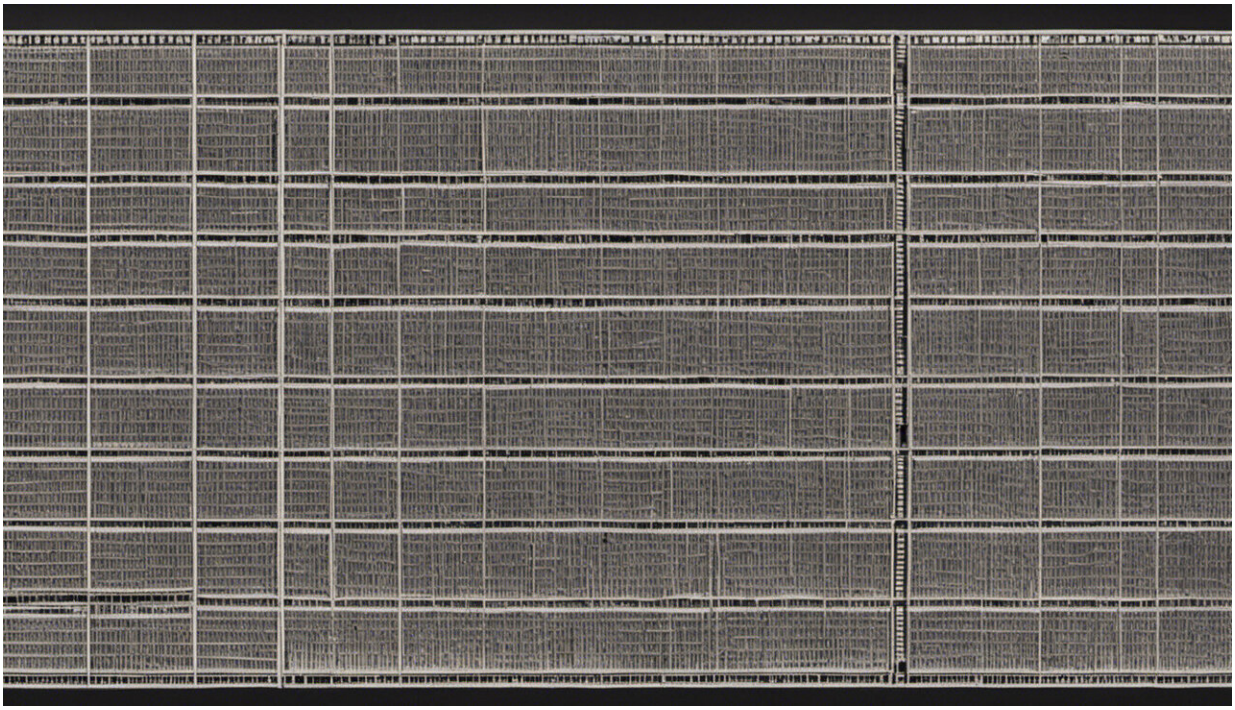
What Hollywood gets right and wrong about hacking

July 20 2018, by Catherine Flick



Credit: AI-generated image (disclaimer)

Spoiler warnings for Mr. Robot, Arrow and Blackhat

Technology is everywhere we look, so it's no surprise that the films and TV we enjoy are similarly obsessed. That's not to say they manage to get it right when it comes to portraying tech accurately however – and one

of their worst areas is computer hacking.

I've been a Linux system administrator in and out of industry for 20 years. That means I ensure all kinds of internet services such as email, websites and news systems run smoothly, and preferably don't get hacked. My current job is to research the ethics and social impact of technology, so I love seeing anything tech-related come up in pop culture.

The operating system that only seems to exist in movies (let's call it "MovieOS") is fascinating – the constant beeping, the clicking with every key pressed, the impossibly long progress bars, the helpful warning alerts, not to mention the ability to zoom in forever on digital images without losing clarity.

But it's the hacking scenes that get me. Every single time.

Expectations versus reality

Hacking is most often portrayed as a frantic exercise, with fast-paced music to raise the tension while boxes flash up on screen. In one episode of the fantasy series Arrow however, the protagonists are able to continue "hacking" despite not being able to see their screens, and eventually this ridiculous hack-war turns into a tennis match with both hackers sending power surges back and forth until the antagonist's computer is blown up.

It's pretty far-fetched but hacking as a means of destruction isn't fictional and it has been portrayed better in the tech drama series Mr. Robot. In one episode, the protagonist Elliot uses a planted device to upload software onto back-up energy storage devices owned by the shadowy corporation, ECorp. This software is then used to trigger explosions – entirely reasonable as these gadgets usually use lead acid

batteries which can emit explosive hydrogen gas when overcharged.

Most of the time though, MovieOS capabilities don't accurately reflect the abilities or uses of real-life operating systems. Being able to draw a line between fantasy and reality is useful in film, but it can also cause problems when dealing with people's expectations of computers and their understanding of how hacking works, particularly common hacks that non-technical people are vulnerable to.

Making hacking look realistic

Aside from MovieOS, which is usually custom designed as a series of screenshots or animations, Linux is one of the most beloved operating systems of set designers. There's loads of typing involved, the software prints obscure-looking outputs and it's frequently used by "real" hackers.

One of the more popular programs to show for hacking purposes in film is Nmap, a scanner which can detect who is using a computer network. Nmap is popular because it produces reams of text which scroll past in the way we've become used to seeing any complicated computer wizardry, and it can theoretically be used for a wide range of hacking activity, such as looking for open ports that might be exploitable, so it actually has some legitimate "geek cred" too.

Mr. Robot offers the most accurate depictions of hacking because it recognises that humans are frequently the weakest links in security. E-mail phishing scams, impersonation of staff or other manipulations of social norms and expectations are often more successful than technical efforts and, with the costs of phishing attacks often significant, it's no wonder they are used so frequently.

In a reasonable effort at realism, the film Blackhat (2015) attempted to show how email phishing could be used to get someone's password, but

it's unlikely someone working at the National Security Agency (NSA) would fall for such a scam.

Still, when this kind of social engineering is shown accurately in films or TV it can raise awareness of common methods and help people recognise attempts before it's too late.

The perils of being too accurate

Accurate representations can cause problems as well however. After Wargames came out in 1983, the US brought in the Computer Fraud and Abuse Act (1984) out of fear that hackers might attempt to replicate attacks made in the film . When The Matrix Reloaded featured realistic use of Nmap in 2003, the Scotland Yard Computer Crime Unit in the UK released a press release warning would-be hackers away from emulating the film.

The depictions of hackers up against "The Man" or a large company with dubious moral values sets up a romanticised view of hacking, which remains illegal and, generally speaking, unethical. A recently updated set of ethical guidelines for computing professionals states that people should "access computing and communication resources only when authorised or when compelled by the public good", noting that if the latter reason is used as justification that "extraordinary precautions must be taken to avoid harm to others".

Hackers like Elliot in Mr. Robot may indeed have some moral high ground to take on big corporations, but as we've seen throughout the show, his methods can also have disastrous impacts on innocent people.

So while it's good to have realistic depictions of hacking, it's sometimes better to just laugh off how terrible they are. Personally, I'd like to see more complete pictures of what hacking is like – and have realistic

consequences depicted as well. Mr. Robot is definitely the frontrunner here, but there is room in TV and film for more realistic and critical views of technology and society.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation