GRESHAM COLLEGE
EST. 1597

Do Computers Get Sick?

Professor Robin May and Professor Victoria Baines

7 May 2025

For this year's lecture series, I am trying a different format of transcript. Rather than a long-form written document, which has been largely rendered obsolete by the ability to transcribe from the YouTube recording, this handout is a brief summary of the key topics in the lecture, together with some more extensive suggestions for extra reading. As ever, we would be delighted to hear your thoughts on this new approach!

*This lecture was a joint venture between **Professors Robin May & Victoria Baines.** We enjoyed working on it together and we hope it will stimulate some suitably 'cross-disciplinary' thinking amongst our wonderful audience too!*

Our world relies on computers. They run our offices, our transport network and our healthcare systems. And when they go wrong, the consequences can be disastrous: lost time, lost business and sometimes even lost lives.

In recent decades, a whole anti-industry has grown up in producing 'malware' that is designed to damage or destroy computers. As a result, most businesses and individuals invest regularly in antivirus software to try and prevent such damage occurring. But how similar are these viruses to their biological namesakes? Can we learn from human immunity to help protect our computer hardware? And might vaccinations of the future owe more to antivirus software development than we can currently imagine?

Viruses and Other Nasties

Biological viruses come in multiple flavours. At their heart, though, they all function in a similar way. Too small and simple to be able to produce their own machinery for replication, instead they hijack proteins produced by the host cell and use them to copy their own genome and produce a new coat or 'capsid' for it. Their efficiency in achieving this is remarkable – a single infecting virus particle can produce hundreds or even thousands of new copies within a day or two. In the meantime, the lack of available machinery for daily 'maintenance' within the host cell means that it accumulates damage and eventually dies – that is, assuming that the virus hasn't already ruptured it in order to escape.

When it comes to computers, we tend to use the word 'virus' to describe lots of nasties that don't always behave like biological viruses, and we regularly talk about computers being 'infected'. Coding errors, often called 'bugs' after a moth that caused a malfunction in a computer at Harvard University in the 1940s, can be really damaging. Vulnerabilities in programs and networks can be exploited by criminals and other bad actors. 'Zero-day' vulnerabilities can be particularly harmful: as the name suggests, these are newly discovered deficiencies for which there isn't a patch. Worms are perhaps the closest thing we have in computing to biological viruses. These are pieces of malicious software (malware) that self-replicate across networks without the need for human intervention. In the WannaCry cyber-attack that disrupted the NHS in 2017, a worm encrypted data and issued ransom demands on more than 300,000 computers across 150 countries.

How to Spot a Virus…

Fortunately, despite the fact that the world is teeming with viruses, life-threatening viral infections remain relatively rare, primarily because our immune system is exceptionally good and finding and destroying viruses before they become established. Broadly speaking, it achieves this in one of three ways. Firstly, it deploys an army of receptors that are designed to recognise molecules that humans do not make themselves but are often found within viruses. So, for instance, long double-stranded molecules of RNA (dsRNA) are often produced as part of a viral replication cycle, but never by mammalian cells. Consequently, a molecule called Toll-Like Receptor 3 (TLR3) is on permanent lookout for dsRNA – if it spots any, then it activates a potent inflammatory cascade designed to hunt down the virus and destroy it.

Secondly, almost all cells within your body operate a 24/7 'inventory' system. By regularly sampling proteins and displaying fragments of them on the cell surface within a special 'holder' called the Major Histocompatibility Complex (MHC), each cell provides a visible menu of proteins currently being produced within it. If the immune system spots something on the menu which doesn't belong there, such as viral protein, then it delivers a lethal cocktail of toxins that kill the infected cell, taking its viral hijacker along with it.

Finally, but most famously, there are antibodies. Produced by an army of B-cells, each antibody can recognise a different foreign molecule, and the huge number of B-cells within the body means that each of us is capable of recognising millions of different targets – including a wide range of the proteins found in viral particles. Although this response is rarely vigorous enough upon a first encounter to completely block infection, if we reencounter a virus we have seen previously (or one for which we have been vaccinated) then the plethora of highly specific antibodies in the circulation can bind to that virus, preventing it from entering host cells and earmarking it for destruction by white blood cells.

Computer immunity looks to strengthen network defences, spot anomalies, and profile and remove malicious software. The biggest difference between how we fight biological and computer viruses is the scale: according to one estimate, 560,000 new pieces of malware are detected every day! This means that preventing infection is paramount. As well as looking for and closing the technical vulnerabilities, humans need to be trained not to fall for scams designed to give hackers access to networks and programs. Those dodgy emails asking you to click on a link or attachment can contain malware; the request for your login details is not always as legitimate as it looks.

In cybersecurity we also look for users and programs that shouldn't be there. Controlling access to networks and systems is one of the best ways to stop the baddies getting in. But it also makes the credentials of authorised users valuable to criminals, hence all those phishing emails. Malicious programs can hide in plain sight, waiting to be activated remotely by a criminal or even by an insider (whether they mean to or not). So, verifying that programs are legitimate and quarantining or blocking what looks suspicious is an important part of cyber defence. With hundreds of millions of attempted cyber-attacks every single day, this task has become automated. You could say that to some extent we now rely on computers to look after themselves.

Specific variants of malicious software are analysed, profiled, and given unique signatures. Antivirus software contains a database of these signatures, comparing these to files on the computer system being scanned. It conducts analysis of suspicious files in a virtual 'sandbox' to prevent any damage to the system itself. Because hundreds of thousands of new threats appear every day, there's a race against time to profile these, and antivirus software now continuously updates itself. Many antivirus tools also conduct heuristic analysis, looking for common characteristics and attributes – in fact, this is one of the ways new malware variants are detected.

The Future of Antivirals

Despite the remarkable power of the human immune system, viruses still make us sick and sometimes threaten our lives – something that was all-too-evident during the Covid-19 pandemic. Viruses, by definition, rely on our own cellular machinery for their lifecycle, which presents a major challenge when it comes to designing drugs to interfere with viral replication whilst leaving human physiology untouched. For that reason, we currently have a relatively limited repertoire of antiviral drugs and instead the primary strategy for tackling viral infection is vaccination.

But there are some exciting discoveries around the corner that might improve our ability to fight back. One recent surprise that has upended the world of virology is the discovery of 'viruses of viruses' – tiny satellite viruses that hijack the hijacker, diverting the machinery of a co-infecting virus to instead replicate the satellite. We still know very little about these enigmatic organisms, but in the future perhaps we may be able to use them to help augment our own antiviral defences.

In parallel, we are living through a revolution in genetics, driven by the development of the 'CRISPR' gene-editing system. Thus far, the focus on CRISPR has been either for laboratory studies or to help create gene-edited animals or plants for health or agricultural reasons. But some of the most difficult viruses to treat are those like HIV or Herpes viruses that become dormant within our own cells, sometimes embedding themselves within our own DNA. What if we could use CRISPR to specifically mutate such dormant viruses, preventing them from ever reactivating.

Finally, with the recent explosion in 'plug and play' vaccine technology, such as the mRNA vaccines that proved to be such a gamechanger during the pandemic, might the future of antiviral immunity in humans show more than a passing similarity to that of our computers, with annual 'updates' being delivered in the mail, or the rollout of predictive vaccines, designed to protect from viruses that don't even exist yet..?

In the computing world, as in medicine, we're already starting to see the impact of Artificial Intelligence, and Machine Learning in particular. As well as automating defence against and response to cyber-attacks, antivirus software increasingly incorporates threat intelligence on the bad guys. Next generation antivirus (NGAV) promises to proactively monitor, identify and neutralise even previously unseen threats with minimal human intervention. The expectation is that software that continuously learns will be more adaptive. It is also hoped that AI will spot patterns that humans haven't yet noticed: for example, attack vectors that *don't* rely on malicious software.

Last but not least, there's some truly groundbreaking research and innovation happening right now that is aimed at reducing the risk of infection in the first place. AI is helping to develop new ways of authenticating authorised users on a network that are harder to spoof or steal. Think that proving your identity using your brain waves is a thing of science fiction? Think again…

Key topic in the lecture	Further reading
How do viruses work?	What Are Viruses and How Do They Work? | Tufts Now
The different types of biological virus	Baltimore classification - Wikipedia
The different types of computer virus	National Cyber Security Centre Glossary
History of computer viruses	Computer virus - Wikipedia
Antiviral immunity – pattern recognition receptors	Detection of Viral Infections by Innate Immunity - ScienceDirect
Antiviral immunity – antigen presentation & T-cell killing	Antigen Processing and Presentation | British Society for Immunology
	Function of Cytotoxic T Cells in the Immune Response
Antiviral immunity – antibodies	Antibody basics | Abcam
Current antivirals	A review: Mechanism of action of antiviral drugs - Shamaila Kausar, Fahad Said Khan, Muhammad Ishaq Mujeeb Ur Rehman, Muhammad Akram, Muhammad Riaz, Ghulam Rasool, Abdul Hamid Khan, Iqra Saleem, Saba Shamim, Arif Malik, 2021
'Viruses of viruses'	Virophage - Wikipedia
CRISPR gene editing	What are genome editing and CRISPR-Cas9?: MedlinePlus Genetics
mRNA vaccines	The Long History of mRNA Vaccines | Johns Hopkins | Bloomberg School of Public Health
Vaccine design and predicting the future	How are vaccines developed?
Current cyber threat ecosystem	Microsoft Digital Defense Report 2024
WannaCry ransomware attack	NHS England case study on WannaCry's impact
Brainwaves for cybersecurity	Unlocking the Future of Cybersecurity: Harnessing Brainwave Detection for Encryption and ID Verification