Making the Internet a safer place

Back in May 2017, a huge cyberattack crippled several of the largest digital networks in the UK and US, paralysing over two hundred thousand computers. To combat such threats ***Dimitrios Pezaros****, Senior Lecturer at the University of Glasgow, and* ***David Hutchison****, Distinguished Professor of Computing at Lancaster University, launched SAI² (A Situation-Aware Information Infrastructure), a research project aimed at developing new technologies to fight against cyber threats.*

Cyber attacks are becoming more and more common, finding their way into the headlines every couple of months. The incident in May 2017 was a fairly typical but high impact ransomware attack. Software called WannaCry infected several organisations' internal computer networks, using the EternalBlue tool, or 'exploit', to install rogue software on unpatched and vulnerable computers. The vulnerability was also used to spread the WannaCry code from one computer to another. On each infected computer a ransom was demanded for putting the rightful users back in control.Another widely publicised cyberattack hit Dyn, a Domain Name System (DNS) provider, in 2016. A 'botnet' was formed by infecting large numbers of easily-hacked networked IoT (Internet of Things) devices such as IP cameras, printers and other everyday gadgets which were used to launch a Distributed Denial-of-Service (DDoS) attack on the Dyn servers. This led to many major Internet platforms that are dependent on Dyn becoming unavailable to huge numbers of their users.

Situation Awareness added to our resilience framework can help the fight against damaging cyberattacks

According to the Situation-Aware Information Infrastructure (SAI²) investigators, such incidents could be better controlled if resilience management were in future deployed in networks, acting more intelligently to detect the onset of attacks, assisted by situation awareness information.

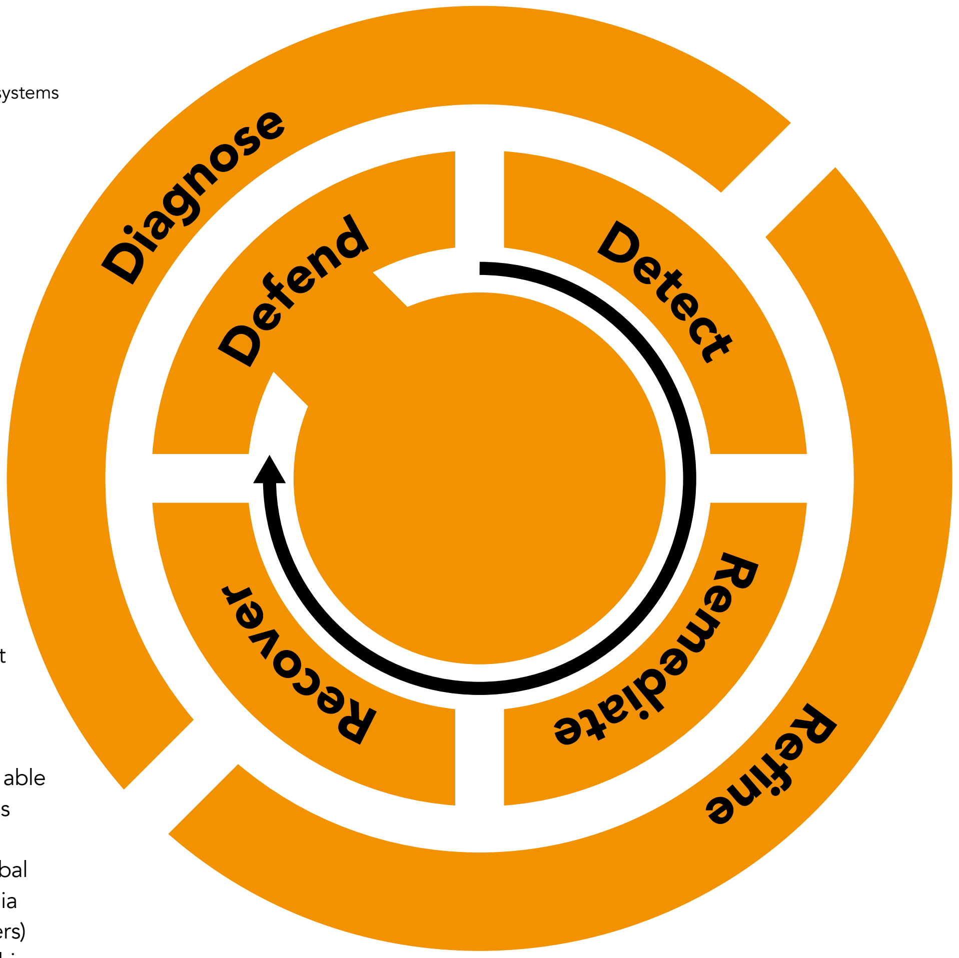
UNITED WE STAND; DIVIDED WE FALL

The SAI² researchers were concerned that cyber security was too reliant on the static defence of individual end devices. The focus should be on protecting the whole networked system, and constantly checking for intrusions.

Think about the setup in a typical household – a desktop, a laptop, a tablet and a smartphone. All these devices can be fitted with protective technology like antivirus software. But in case of a threat, each will mind its own digital business. If a hacker fails to get past the security running on a desktop, it doesn't mean he or she will be just as unlucky when attacking a laptop. One way around this is to use a home gateway equipped with a firewall that is supposed to protect the whole network. But the firewall's rules – what it does and does not recognise as a threat – are usually static and thus can't adapt intelligently to break-ins on the network or attacks it has not encountered before. When we multiply this by thousands of computers connected into one of the largest networks of the world, the problem gets significantly worse.

That's why the SAI² team focused on building a security system that integrates different sources of information like operators' warnings about cyber threats, social media news feeds, or indeed any relevant contextual information, as well as conventional network traffic packet traces.

A computer network is frequently referred to as the information highway,



A framework for resilience in networked systems

carrying bits of data travelling in both directions between connected devices at extremely high speeds, and as with a real highway there's much that can be inferred by measuring the traffic. What the SAI^2 team proposed was algorithms and tools for detecting anomalies in the measured traffic, and then reacting to such anomalies in short timescales. It sounds simple, but the real challenge lies in deciding how to respond to anomalies. The SAI^2 researchers have been better able to spot when something suspicious is going on by analysing network data traffic patterns alongside global information feeds from social media (e.g., Twitter) and news (e.g., Reuters) sources. However, to accomplish this and at the same time feed any alerts back to the network infrastructure in short timescales, they decided to revisit the fundamental packet switching mechanisms of the network. Doing so for large networks that transmit data at rates of hundreds of Gigabits per second and multiplex traffic for millions of users over large, geo-distributed data centres poses significant technical challenges. So, the SAI^2 team developed a novel, programmable switching architecture that can natively incorporate monitoring and adaptive control intelligence as part of the main packet forwarding operation of the network infrastructure. This way, Hutchison, Pezaros and their colleagues designed a cyber security system that is aware of what's going on in the entirety of the network it protects, and can react according to the temporal operational conditions and incidents as and when they unfold. But knowing what's going on inside the network was only the first step in building a situation-aware infrastructure. The next logical step was to equip the network with the ability to understand, to an appropriate extent, the outside world as well.

Resilience management can use Situation Awareness to help make better remediation and recovery decisions

LOOKING OUTSIDE

While the term 'cloud computing' sounds intangible, the reality is our photos, emails, videos or medical records have to be physically stored on servers located somewhere. Clouds and any critical infrastructure will be subjected to challenges including natural disasters and a variety of operational failures as well as cyber attacks. The SAI^2 investigators apply a resilience management framework to protect such networked systems, assisted by situational awareness information from external sources including social media.

Of all social media platforms, Twitter is certainly one of the most accommodating to researchers – its data is easily obtainable: how many people tweeted a particular message; how many used a given hashtag; when and where those people did so, etc. This is all invaluable information when it comes to dealing with and assessing crises. Suspicious activity will appear in Twitter data patterns like ripples in the water. So, the SAI^2 team went on to build algorithms that model such news feeds into their cyber security systems. In this way, computer networks of the future will know what's happening around them as well as inside the network and can react accordingly. Does this mean they will become self-aware? No, they won't. But the idea is that future networks will exhibit other properties like self-management and self-adaptation which ultimately will make them more resilient and reliable: properties which will benefit us all.

Behind the Bench

Professor David Hutchison

Dr Dimitrios Pezaros

E: d.hutchison@lancaster.ac.uk **T:** +44 (0)1524 510331 **W:** https://www.gla.ac.uk/schools/computing/staff/dimitriospezaros/
W: www.research.lancs.ac.uk/portal/en/people/david-hutchison

Research Objectives
Prof Hutchison and Dr Pezaros work on improving cybersecurity. In particular, their research aims to give networks better abilities to detect and respond to cyberattacks and other challenges.

Funding
- UK Engineering and Physical Sciences Research Council (EPSRC) TI3 Project EP/L026015/1: Situation Awareness.
- European Cooperation in Science and Technology (COST) Action CA15127: RECODIS on Resilient Communication Services.

Collaborators
Lancaster University: Andreas Mauthe, Angelos Marnerides, Noor Shirazi, & Steven Simpson. University of Glasgow: Joemon Jose, Long Chen, & Simon Jouet

Bio
Dimitrios Pezaros, CEng, SMIEEE, SMACM, is Senior Lecturer (Associate Professor) at the School of Computing Science, University of Glasgow. His research focuses on the resilient and efficient operation of virtualised and software-defined networked infrastructures. He holds BSc and PhD degrees in Computer Science from Lancaster University, UK.

David Hutchison is Distinguished Professor of Computing at Lancaster University and has been doing computer network research for more than 25 years. He now focuses largely on resilient and secure networking, with interests in the Future Internet and also the protection of critical infrastructures including utilities and industrial control systems.

Contact
Prof David Hutchison
Lancaster University, InfoLab21
Lancaster, LA1 4WA
UK

Q&A

What first got you interested in cyber security and resilience?
The realisation that computer networks increasingly become part of the national critical infrastructures, and are therefore too important to fail. We have been working in the areas of network and service management for years, and we are bringing this know-how into an emerging area requiring holistic solutions to enable emergent properties such as reliability and resilience of large-scale networked systems. Actually, what we work on is the resilience of networked systems, which includes cybersecurity but goes beyond it to respond to cyberattacks (and other disruptive challenges such as natural disasters) and rapidly attempt to remediate and recover the normal operation of the system.

How can the Situation-Aware information infrastructure benefit us, the end users?
A Situation-Aware information infrastructure should aim at making the underlying interconnection medium even more transparent to the end-user by minimising down-time and through rapid re-engineering of its operation at the onset of adversarial events, while offering uninterrupted services to its end users.

How does your Situation-Aware network architecture work?
Situation Awareness is facilitated through a novel network architecture that makes the network's main data-forwarding plane programmable. This is achieved through each switch in the network supporting a minimal, performance-bound instruction set. Based on this, centrally-controlled, minimal programs can be installed on the switches along the data path to enable high-speed, adaptive functionality alongside packet switching. Using this novel architecture, we have demonstrated several use-cases of monitoring and control functionality such as exponential weighted mean average computation on every switch along the data path for normal behaviour profiling (a prerequisite for enabling anomaly detection), as well as collaborative pushback for distributed, denial of service attack remediation.

How can a cyberattack affect a regular person?
Cyberattacks can deprive users from accessing their data on a physical machine or over the cloud, and from always-on connectivity which is increasingly considered vital. Cyber incidents where attackers encrypt the victim's data and subsequently ask for ransom in order to decrypt it are becoming increasingly popular. At the same time, attacks on the networked infrastructure can have wider and more costly effects. Volume-based amplification attacks can take significant parts of the infrastructure offline for long periods of time, preventing users from accessing online services but also from running their own businesses over the cloud.

What, in your opinion, will perpetrators do to defeat future cybersecurity systems like those you're working on?
Over the years, there has been the typical cat-and-mouse game between perpetrators and defence systems where the latter have been developed or amended in response to a new attack, and new attacks are being developed to exploit previously unknown vulnerabilities. The work in this project strives to break this endless cycle of events by making the infrastructure adaptive, able to learn from its own past behaviour, and to harness as much information as possible to try and predict the onset of adversarial events. This way, defence against cyber-attacks does not depend on static knowledge that can only protect against a certain set of vulnerabilities but rather it evolves together with the operation of the networked infrastructure.