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 dependant on Dyn becoming unavailable to huge numbers of their users.

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.

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.
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 SAFI 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 easy to 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 likeripples in the water. So, the SAFI 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 exploit other properties like self-management and self-adaptation which ultimately will make them more resilient and reliable properties which will benefit us all.

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 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.

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 your research projects? Over the years, there has been the typical cat-and-mouse game between perpetrators and defense 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 net 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, resilience 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.