PETRAS

LANDSCAPE BRIEFING

11 NOVEMBER 2020

COVID-19: The Internet of Things and Infrastructure

Prepared by Dr Monica Racovita
with input from Caroline Wijnbladh

The COVID-19 pandemic has inspired a range of Internet of Things (IoT) and AI innovations to help stop the spread of the virus. This is an Infrastructure sector-specific edition of COVID-19: IoT and Cybersecurity looking at the intersection between IoT, critical infrastructure and cybersecurity in the age of the COVID-19 pandemic.

Past editions are found on the PETRAS website.

The COVID-19 pandemic is accelerating the adoption of IoT devices, to keep businesses and infrastructure operating. It is also moving much of the economy online. These two trends are increasing the number of attack surfaces and diversity of attack vectors. Combined with existing cybersecurity challenges, like the lack of commonly adopted standards, and low awareness for the need of stronger cybersecurity measures from IoT manufacturers, these factors increase the risk of catastrophic attacks on critical infrastructure at a time when countries are already heavily burdened with the fight against the pandemic.

Use of IoT in critical infrastructure during COVID-19

IoT-powered vaccine cold chain monitoring

The UNDP and the Indian government developed an IoT-enabled mobile-based technology which tracks the temperature, location and stock levels of vaccines to strengthen the vaccine supply chain[1].

Overview

- Critical infrastructure benefited from the use of IoT in all sectors during the pandemic with examples provided here from health, energy and finance.
- The pandemic saw the emergence of a new generation of critical infrastructure, including vaccine research labs, clinical trial administrators, manufacturers of components for ventilators or food retailers.
- Cybersecurity is a major issue as COVID-19 saw an increase in cyberattacks on critical infrastructure facilities.
- The purpose of these attacks can be to gather intelligence on COVID-19, scientific information, treatment or government response strategies (cyberespionage), money (cybercrime), or to threaten national security.
- IoT devices can be vulnerable to attacks through internal vulnerabilities such as ‘Ripple20’, or wider ecosystem vulnerabilities, such as counterfeit hardware and vulnerable local networks.
- Cybersecurity recommendations include a decentralisation approach to security, like isolating the IoT devices on a separate network segment, security by design, but also strengthening local networks.

IoT detecting virus outbreaks by analysing wastewater

The Israeli-based company Kando has developed an IoT solution for large-scale real-time monitoring of COVID-19 outbreak and intensity in wastewater[2]. When the conditions are met (e.g., the presence of viral genetic material), the electrochemical and optical sensors trigger an auto-sampler which collects wastewater and lets operators know that it is ready for analysis. The sample will then be

analysed using machine learning capabilities to identify the population infection level in an area as small as a single street.

IoT helping deliver reliable energy during the pandemic

When stay-at-home orders are engaged, the energy industry must maintain operations while preserving the health of its employees. IoT devices can play a positive role by monitoring the health of on-site workers (thermal imaging) or by remote monitoring of equipment. There is also an increasing interest in predictive maintenance where IoT are coupled with robotics and data fed into AI models to increase the predictability and reliability of the energy grid[3].

Point of Sale (PoS) payments have increased during the pandemic

MarketsandMarkets reported in April 2020 that the IoT market in Banking Financial Services is to grow, driven by an increase in digital payments with mobile paying devices ranging from small wearables to parking meters, fitting room mirrors, and vending machines[4].

IoT cybersecurity in critical infrastructure

COVID-19 pandemic brings a new generation of critical infrastructure

A recent Deloitte report identifies the emergence of a new generation of critical infrastructure, which needs to consider expanded cybersecurity challenges and new regulatory compliance and resilience protocols[5]. Thus, organisations like vaccine research labs, clinical trial administrators, manufacturers of components for ventilators or food retailers became part of critical infrastructure. For many, due to their time-sensitive work they are a target for ransomware attacks, like the Netwalker criminal gang attack on the University of California San Francisco (UCSF) on 1st of June[6]. The targeted medical research institution within UCSF, which was working on a COVID-19 cure, ended paying hackers 1.14m USD (£875k).

In addition, state-sponsored threat actors will try to access data related to COVID-19 and national measures to mitigate it. The Deloitte report advises newly critical organisations to not confuse compliance with security, understand third party risks and strengthen incident response.

'Ripple20' vulnerabilities in IoT devices

The Israeli cybersecurity consultancy JSOF identified 19 bugs, called 'Ripple20' vulnerabilities, in a TCP/IP software library used to connect IoT devices to the Internet via TCP/IP connections[7]. This affects millions of older IoT devices used in transportation, aviation, oil and gas, medical devices, power grids, or home products. JSOF together with Trek, the software company which built the software library, developed a security patch by March 2020. Companies affected include Baxter, Cisco, Dell, Intel, Samsung, or Xerox[8].

Yet experts fear that the vulnerabilities will continue to affect many more IoT devices because many companies are unaware that they use this code, as the library was integrated into other software[9].

IoT ecosystem vulnerabilities: counterfeit hardware and local networks

IoT devices or networks to which they are connected can become compromised through faulty hardware. One example is the discovery of counterfeit Cisco router switches, which allows networked devices and multiple users to access the Internet. F-Secure Consulting analysed the counterfeit switches in July 2020 after a software upgrade caused them to fail after seemingly working fine for a long time[10]. The switches were shown to pose network security risks.

IoT devices can be compromised by gaining access to the local network first. A cyberattack on Halloween night this year, called NAT Slipstreaming, targeted local networks. According to security researcher Samy Kamkar, NAT Slipstreaming can bypass Network Address Translation (NAT) and firewalls just by the victim visiting a website, containing malicious JavaScript, and be behind a vulnerable Application Level/Layer Gateway (ALG)[11].

Cyberespionage, cybercrime and national security threats

COVID-19 saw an increase in cyberattacks on critical infrastructure facilities. The purpose of these attacks can be to gather intelligence on COVID-19, scientific information, treatment or government response strategies (cyberespionage), money (cybercrime), or to threaten national security.

PETRAS is funded by the UKRI via the Security of Digital Technologies at the Periphery (SDTaP) programme.

Advanced persistent threats are reported to be increasing, linked to attempts to gather intelligence on the virus[12]. They can gain unauthorised access to networks and devices and remain undetected for a long time. These threats are conducted by nation state or state-sponsored groups. Examples include Iran or North Korea backed groups, which targeted the World Health Organisation (WHO), a Vietnamese-backed APT32 group targeting China[13], Russian based groups targeting Ukrainian targets, or groups aligned with the Chinese government targeting Vietnam, the Philippines, Taiwan, and Mongolia[14].

Monetary reasons were behind ransomware attacks on a US natural gas facility in February 2020[15], and Taiwan's state-owned energy company, CPC Corp in May 2020[16].

Japan saw a string of internal network breaches at defence-related companies such as the largest telecommunications company, NTT, in May 2020[17], Kobe Steel Ltd and satellite data provider Pasco Corp in February 2020[18], and Mitsubishi Electric and NEC in January 2020[19].

Cyberattacks can also result in the loss of human life, as the September 2020 attack on University Hospital Düsseldorf (UKD) in Germany shows[20]. The police found that the ransomware attack, which exploited the Citrix ADC vulnerability, was actually intended for Heinrich Heine University rather than the hospital. When hackers were contacted and made aware of the error, they withdrew the ransom demand and provided a decryption key. Unfortunately, as a result of the attack, a patient in a life-threatening condition died during the time UKD was unable to offer emergency services and was sent to another hospital.

Cybersecurity recommendations for IoT devices

In 'COVID-19 pandemic cybersecurity issues', researchers recommend isolating IoT devices on a separate network segment, to prevent the compromise of primary devices like main computers in the eventuality of an attack[21].

Yet, GlobalData argue in a recent report, that a decentralised approach to security, while necessary especially for big networks such as utility infrastructures, will place a heavier burden on edge elements, to maintain the resilience of the utilities system and the resilience of the devices in case of attacks[22]. Edge elements, like IoT, could even enhance the security of the system by providing a better monitoring of unusual patterns. GlobalData also point towards a lack of awareness for stronger cybersecurity measures from utilities companies. Many comply with cybersecurity standards only when they are mandatory, thus lacking comprehensive security measures. The industry also has an inadequate reporting mechanism for cyberattacks when information sharing could help prevent further attacks.

After some light reading?

A recent book describes a scenario where attackers do not merely hijack the control systems of grid operators to cause short-term blackouts, but instead reprogram the automated elements of the grid to cause physical damage. The idea, used by the infamous Russian-backed hacker group Sandworm, was known and tested by the United State government years earlier[27].

Experts recommend security by design but that can incur higher product costs. With consumer IoT manufacturing companies already operating with thin margins, often reducing security costs is employed to increase profits[23].

The Australian government passed new security regulations for critical infrastructure in August 2020 imposing "obligations on companies to employ encrypted cyber defences under a three-tiered ranking system of commercial assets and systems"[24]. Yet on IoT consumer devices only a voluntary code of practice will be implemented.

These recommendations focus on security at the IoT device level when the devices are seen as a gateway entry to entire networks. Yet as the NAT Slipstreaming cyberattack on Halloween proved, attacks can breach local networks of which IoT devices are a part. This could potentially mean attackers could have access to IoT home devices like smart thermostats and could turn off the heating in the middle of winter for millions of households at once. To protect against such attacks, security researcher Samy Kamkar recommends "disabling ALG on their router/firewall (assuming they don't need it for something like a VoIP phone!) and I'm sure browser and router vendors will implement additional safeguards to protect against this"[25].

A Critical National Infrastructure (CNI)-specific look at NCSC guidance on remote access architecture design was published on 9 November[26].

Endnotes

1 https://www.in.undp.org/content/india/en/home/projects/gavi1.html
2 https://www.kando.eco/copy-of-covid-19
3 https://www.iotworldtoday.com/2020/08/14/iot-in-utilities-market-brings-resilience-in-wake-of-covid-19-pressure/
4 https://www.prnewswire.co.uk/news-releases/covid-19-impact-on-internet-of-things-iot-market-exclusive-report-by-marketsandmarkets-tm--870475171.html
5 https://www2.deloitte.com/bg/en/pages/risk/articles/covid-19-the-impact-of-cyber-on-critical-infrastructure-in-the-next-normal.html
6 https://www.bbc.co.uk/news/technology-53214783
7 https://www.darkreading.com/iot/ripple20-bugs-plague-enterprise-industrial-and-medical-iot-devices/d/d-id/1338106
8 https://unit42.paloaltonetworks.com/iot-supply-chain/
9 https://www.zdnet.com/article/ripple20-vulnerabilities-will-haunt-the-iot-landscape-for-years-to-come/
10 https://labs.f-secure.com/assets/BlogFiles/2020-07-the-fake-cisco.pdf
11 https://github.com/samyk/slipstream
12 https://www.enterprisetimes.co.uk/2020/07/09/apt-activity-is-targeting-covid-19-research/
13 https://www.enterprisetimes.co.uk/2020/07/09/apt-activity-is-targeting-covid-19-research/
14 https://www.technologyreview.com/2020/03/12/916670/chinese-hackers-and-others-are-exploiting-coronavirus-fears-for-cyberespionage/
15 https://www.bbc.co.uk/news/technology-51564905
16 https://www.cyberscoop.com/cpc-corp-ransomware-attack-taiwan-trend-micro/
17 https://www.zdnet.com/article/fortune-500-company-ntt-discloses-security-breach/
18 http://www.asahi.com/ajw/articles/13108916
19 https://www.zdnet.com/article/trend-micro-antivirus-zero-day-used-in-mitsubishi-electric-hack/
20 https://www.bleepingcomputer.com/news/security/ransomware-attack-at-german-hospital-leads-to-death-of-patient/
21 https://onlinelibrary.wiley.com/doi/full/10.1002/itl2.247
22 https://www.power-technology.com/comment/cybersecurity-power-utilities-agenda-covid-19-globaldata/
23 https://www.iotworldtoday.com/2020/07/27/common-internet-of-things-security-pitfalls/
24 https://www.lexology.com/library/detail.aspx?g=0cedcf95-8b22-469b-a83c-0fb84d39fce6
25 https://www.theregister.com/2020/11/02/application_level_gateway_flaw/
26 https://www.wired.com/story/how-30-lines-of-code-blew-up-27-ton-generator/
27 https://www.wired.com/story/how-30-lines-of-code-blew-up-27-ton-generator/
https://www.ncsc.gov.uk/blog-post/cni-system-design-secure-remote-access