# Chapter 7
# Security for Science: How One Thing Leads to Another

**Hannah Short**

## 7.1 Introduction

I have a vivid memory as a child of a particularly austere English teacher berating me for overuse of the word “Thing”. Imagine my relief as we entered the 2010s, “Thing” found its way into the spotlight and I was able to freely and legitimately reinsert it into my vocabulary! In my childhood, “Thing” was criticised for being imprecise. I enjoyed many conversations with friends and colleagues whilst researching this chapter, and ventured to ask for their own definition of a “Thing” from the Internet of Things (IoT). The answers I received have led me to believe that my English teacher was, in fact, ahead of her time; outside a small circle of experts the concept of “Thing” is indeed imprecise. This chapter will exploit this imprecision as we discuss the overlap between the IoT and Science. We will touch on the experiments, laboratories and scientists impacted, plus the “Things” themselves.

As a member of the Computer Security team at the European Council for Nuclear Research (CERN), the content here has a declared bias towards High Energy Physics. Many of the ideas, however, are relevant further afield.

### *7.1.1 The Coolest, Largest, and Fastest Things on Earth*

Scientific experiments are designed to push the limits. Some of the most interesting hypotheses currently being tested focus on questions that require powerful, specialised and often complex machines to be constructed. The Square Kilometre Array will be the largest observatory ever built; with a total collecting area of well

H. Short (✉)
Ferney Voltaire, France
e-mail: Hannah.short@cern.ch

F. D. Hudson (ed.), *Women Securing the Future with TIPPSS for IoT*, Women in Engineering and Science, https://doi.org/10.1007/978-3-030-15705-0_7

over one square kilometre (or one million square metres) spread over two continents [1]. Researchers at the National Institute of Standards and Technology (NIST) are using lasers to create temperatures colder than the coldest regions of the universe [2]. There was great excitement when it seemed plausible that particles had travelled faster than the speed of light between CERN and Gran Sasso in Italy, a distance of over 700 km through the crust of the earth [3]. This turned out to be a false alarm but the principle is the same. We know how the rules of science work in our environment, to make discoveries we need to probe the extremes.

Experiments can span countries, continents and occasionally planets. They rely on physical networks (and sometimes more inventive solutions involving satellites, etc.) to transfer data. Attached to these networks are the actors involved in our workflows; the experiments that produce the data, the machines that process and store the outputs, the researchers that perform their analyses. Each actor introduces risks into scientific workflows.

There are several concrete ways in which IoT devices have been recognised to play a part in scientific workflows and experiments today:

- IoT devices integrated with the control systems of experiments, such as sensors.
- Connected scientific apparatus in the laboratory, such as thermometers and oscilloscopes.
- “Custom” IoT devices developed by researchers.

The experiment control systems, the software and hardware that configure the machinery and electronics at the heart of an experiment, will typically not be connected to the internet directly but separated on a dedicated network. At CERN, this is called the Technical Network, shown in Fig. 7.1, and offers near complete isolation from the outside world. Devices may be connected at any point in the chain, both on the Technical Network and General Purpose network that is connected to the Internet. IoT devices on a Technical Network, whilst not necessarily conforming to the “internet” condition of being an “Internet of Things” device, equally pose security concerns for science and this chapter includes all networked IoT-like devices.

It is essential that a defence-in-depth approach is taken towards IoT security for science, with best practices incorporated in network hygiene, security awareness campaigns and procurement practices, to name but a few relevant aspects. This chapter takes a closer look at security for distributed science, IoT in a laboratory setting, and focuses on an example taken from CERN’s recent campaign to identify and secure connected devices.

### *7.1.2 Science as a Target*

Research, as any other sector, has its own particular threats. Two key risks, as highlighted in SURF’s Cyber Threat Assessment 2017, are that of “obtaining and publicizing data” and “espionage” [5]. It may seem perverse that research, particularly

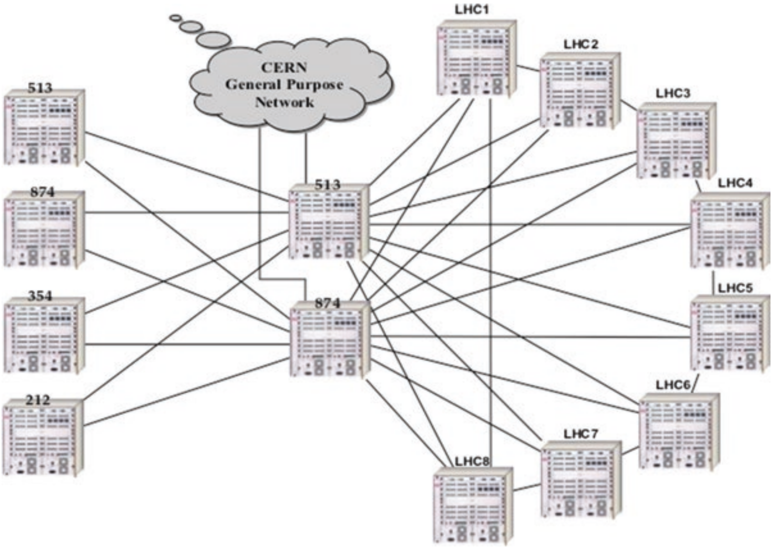

**Fig. 7.1** Technical Network schematic, from the Large Hadron Collider (LHC) Design Report, 2004. The LHC is CERN's particle accelerator that sits 100 m below the ground and measures approximately 27 km in circumference. End node security and updates are paramount; "It must be noted that because the technical network infrastructure is interconnected with the general purpose network, security break-ins can be attempted on the devices connected to this infrastructure. End nodes security survey and updates must not be forgotten" [4]

open research initiatives, should be the target of espionage. The science will be publicly available, so why steal it? Until the point that science is published, there is usually a need to ensure confidentiality of data. Two key reasons for this are firstly that those paying for time on an experiment may be entitled to exclusive access during a certain period, and secondly that a level of separation of information between research groups is often necessary to avoid bias and ensure scientific integrity. The target audience (potential customers!) of stolen scientific data is small, meaning that organisational data that provides insights into new technologies, planned financial decisions of institutes or personal information of individuals may be a more interesting target for espionage.

Certain Research fields, particularly those dealing with topics in the popular domain such as nuclear research or genomics, are swathed in conspiracy theories that make them interesting targets for "hacktivists" (activist hackers) and others wishing to cause damage to reputation. For example, defacing a single research website may provoke a media storm culminating in a headline stating that a multimillion euro experiment was "almost hacked".

An additional target for online attackers is the abuse of computing power. The potential to exploit computing capabilities for disruption (e.g. denial of service attacks) or financial purposes (e.g. digital currency mining) can be an attractive incentive and Research organisations play home to powerful resources.

The threat landscape for Research Institutes is complex and includes threats typical to both Industry and the Education sectors. The inclusion of IoT devices into this landscape may both alter the existing attack vectors and introduce new opportunities that focus on Science as a target.

## 7.2 No Scientist Is an Island

### *7.2.1 Connected Communities, Data and People*

The individuals working on an experiment are mobile and highly interconnected. Typically, laboratories will welcome visiting scientists who will bring with them their own devices (laptops, phones) and contribute under the affiliation to their home organisation. A scientist may spend 40 years working on an experiment but change university ten times in the process. Many research communities not only encourage researchers to work on their own devices but also to continue to use credentials (username and password, certificates, authorisation tokens, etc.) from their home organisation. For example, someone may contribute to the Laser Interferometer Gravitational Wave Observatory (LIGO) using a digital identity from the University of Edinburgh [6]. This identity could be used to allow the researcher to access one of LIGO's underlying computing centres based anywhere in the world and shared by other Research Communities. Security vulnerabilities can be introduced at the home organisation, by LIGO themselves, or at the underlying infrastructure, and can propagate throughout the stack. The mobility of researchers means that attack vectors exist to link organisations and institutes, which, at first glance, seem unrelated.

To cope with the connectedness of actors in scientific workflows, a strong layer of policy and trust frameworks is necessary to ensure that each organisation operates in line with a common baseline of acceptable operational security. This baseline may need to be updated as previous assumptions become invalid in the era of IoT. Whereas before we were dealing with PCs and portable devices that were well understood, homogeneous, and largely inaccessible from the outside, all bets are now off with the variety of devices available.

### *7.2.2 Joint Incident Response and Trust*

There is no such thing as 100% security. Since you are reading this book, I assume this is a concept that you have already accepted so will not spend long trying to convince you. Security professionals are in a constant battle against attackers, with new vulnerabilities periodically emerging; as proactive as your security measures may be there will be a gap between a vulnerability's disclosure and your mitigating actions. Sometimes you will fall victim to an attack. Once we accept the inevitability of security incidents it becomes clear that a fundamental component of a robust security programme is Incident Response. Incident Response encompasses many phases, principally; preparation, containment, investigation, resolution and post-incident review of procedures and practices. Responsive collaboration of service and network operators, forensics experts, public communications and policy makers is critical.

Large-scale science tends to rely on distributed computing infrastructures, where resources are incorporated into a computing pool. Computing power may come from member organisations, supercomputing centres, and increasingly commercial infrastructure providers. In this model, an efficient response to a security incident becomes a problem of coordination and trust. Distributed Computing requires the collaboration of each participant that contributes to the computing needs of an experiment. Shared policies, procedures and the fostering of trusting relationships between participants are critical to ensuring that an incident can be successfully resolved [7]. Failure to build the required level of coordination will result in a suboptimal response. There are myriad ways in which the Incident Response process can be disrupted; some examples are loss of evidence (a contributing data centre reinstalls a system rather than gathers forensic evidence), inability to deploy defensive measures (a site fails to patch systems due to a poorly understood dependency) or a leak of confidential information to the media (without pre-established disclosure agreements or identification of a designated communication manager an individual may respond to journalists and cause damage to reputation). As with operational security, there are existing frameworks that identify the correct behaviour between computing providers [7] during Incident Response. It remains to be seen exactly how consideration of IoT might have an impact.

## 7.3 IoT in the Laboratory

### *7.3.1 Mitigating Curiosity*

It is widely held that “curiosity killed the cat”, but for a scientist curiosity is an essential ingredient of research. As a defining characteristic of many researchers, curiosity has the potential to introduce significant risks when it comes to security. Scientists and engineers tend to have both the technical knowledge and drive to be among the first to test out new technologies. Walk into a physicist’s garage and you may well find an arduino geared up to measure the humidity and report back to its owner in case of excess moisture, step onto their balcony and their herbs may be watered autonomously by a similar setup. When we talk about IoT and Scientists, we are not only talking off-the-shelf IoT. Such homemade devices may be set up once (with a thought to secure configuration if we are lucky) and possibly never touched again.

This curiosity for technology is what has driven many students to research in the first place but applied to connected devices it has the potential to introduce unanticipated risks. A certain level of security education should be given to any scientist dealing with computing topics or infrastructure and, wherever possible, secure solutions and tools should be offered and maintained by laboratories and institutes. Security education, of course, stretches far beyond IoT security. Training in secure software development, access control, privacy fundamentals, to name a few areas, should be made available to scientists in the interest of the wider community.

### *7.3.2 Abundance of IoT*

In 2016, CERN began a wide scale scan of its network to identify IoT devices [8]. You might ask yourself why a scan was required; surely it should be clear which devices are connected to a network? The principal reason is the following: bring-your-own device is standard at many Research Institutes. Granting network access to an abundance of visiting scientists, often in the thousands and increasingly with multiple devices, brings a certain overhead that, at scale, must be delegated to the scientists themselves who are trusted to register devices. Scientists are able to request access for their own devices and specify characteristics (operating system, vendor, etc.) manually. Since having total control over the devices connected to the network is unachievable, instead, effort is invested in policy, monitoring, incident response and network security. The introduction of IoT devices into society has been a slowly evolving process, with the result that CERN—like other laboratories and institutes—has devices connected to the network alongside desktop PCs, phones and laptops. It has become commonly acknowledged that good cyber hygiene recommends that IoT devices be connected to a network with tighter controls than those appropriate for laptops and desktop PCs. To be able to move such devices to a secure network architecture, the first step is to identify them.

A preliminary scan of the CERN network led to the identification of approximately 3000 devices distributed across the General Purpose Network and the Technical Network [9]. These devices were split into categories based on information gathered either through CERN's database of device information or through additional network analysis. The breakdown of devices can be seen in Fig. 7.2, with Routers and Switches, Webcams, Virtual Network Computing Viewers and Printers being the most abundant. In addition to these general-purpose devices, a number of scientific instruments were found. Notably thermometers.

Thermometers are used around CERN, sometimes as stand-alone apparatus and sometimes attached to experiments and integrated into their configuration systems. The ability to override a thermometer could directly impact the operation of a scientific experiment. I will let you use your imagination as to how, precisely, but to give one possibility—safeguards against overheating could be triggered by increasing the measured temperature leading to system shutdown, unavailability and loss of data taking. There are opportunities for holding devices to ransom, and direct financial consequences from the missed data capture. A more subtle concern

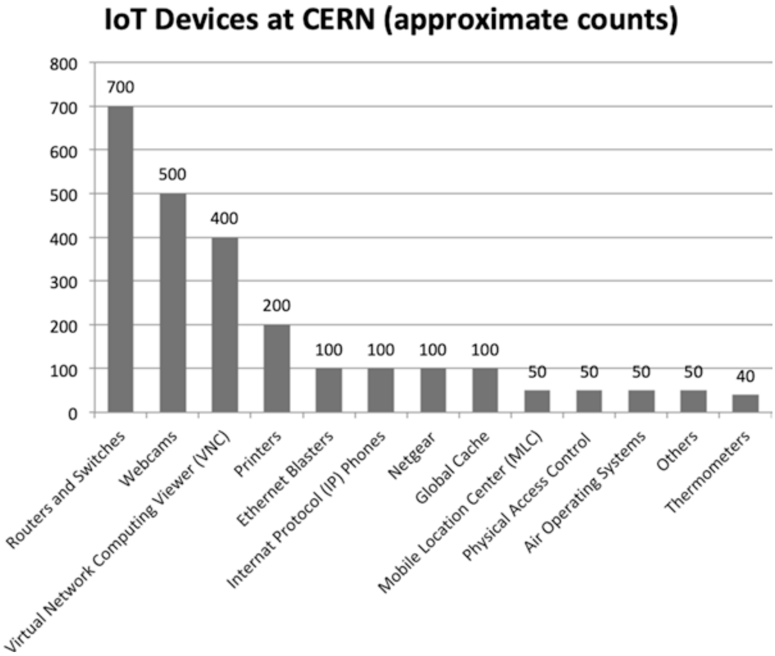

**Fig. 7.2** Approximate numbers of IoT devices found at CERN, on both the General Purpose and Technical Networks [9]

is the potential for the integrity of data to be compromised and lead to invalid scientific results.

Whilst investigating the security vulnerabilities of Papouch TME Thermometers, commonly used in laboratories, a number of concerns were highlighted [9]:

- There was no authentication required for access to the Web User Interface or Telnet port.
- The Web User Interface allowed a range of actions, including changing the firmware and device configuration.
- A superadmin account was enabled by default, whose username and password cannot be overwritten.

All three of these aspects have the potential to cause significant disruption. In particular, the ability to arbitrarily change the code running on a device connected to a large-scale physics experiment should give cause for concern. In the case of CERN these vulnerabilities were either quickly addressed with the collaboration of the device owner, or the device was disconnected from the network. However, a one off scanning activity is not enough. IoT devices should be securely configured, facilitated by training for scientists and specific security audits, and their maintenance folded in to ongoing security processes. The impact of a compromised IoT device should be mitigated as an absolute priority. Trusting a single IoT device as part of a scientific workflow presents a particularly inviting vector of attack; the likelihood of undetected compromise can be significantly reduced by deploying multiple devices, and by calibrating against “un-connected” devices.

In a domain like physics the consequences can be great, but typically the experiments can be repaired and the data retaken. When research domains deal with living samples, the consequences can be more grave. Connected fridges and freezers that alert the researcher to unexpected temperature changes offer the opportunity to avert potential thawing but at the same time may introduce the possibility for a malicious actor to do just the opposite [10].

## 7.4 Where Are We Heading?

IoT devices are set to play a major role in scientific workflows. In the future they may offer considerable benefit to data taking and experiment configuration, with scientists already expressing interest in their potential. It is perhaps early days to make concrete predictions; the full impact of IoT is yet to be understood for the laboratories, the computing infrastructures and the individual researchers. However, there is no denying that IoT devices are already present and proactive measures should be taken to mitigate the risks that have been introduced:

- Network hygiene practices for Research Institutes must evolve to mitigate IoT risks. Appropriate network configuration should be the default and checks for known vulnerabilities should be made on a periodic basis. The message from the Large Hadron Collider Design Report, 2004, in Fig. 7.1 is still valid, and particularly pertinent for IoT: “End nodes security survey and updates must not be forgotten”.
- Measures should be put in place to minimize the impact of an exploited device. IoT devices for scientific measurements should not be used without calibration against “un-connected” devices. Any deviation should be investigated. An additional safeguard may be to deploy multiple IoT devices and calibrate between them.
- Policies and procedures should evolve to include specific measures for IoT. This may include the augmentation of policies that span the multiple organisations and infrastructures that contribute to global science.
- Security training for scientists is required to highlight the risks of connected devices and the need to undertake certain security measures such as upgrading firmware and changing default passwords.

As, I am sure, will be mentioned in other chapters of this book, there is a strong hope that IoT vendors will step up and improve the security of their products. This is particularly important in scientific equipment such as cooling, heating and measurement devices where it is possible that compromise could lead to experiment malfunction and ultimately financial or physical risk.

**Acknowledgments** Pascal Oser (CERN) and Sharad Agarwal (CERN), for their work on scanning CERN's network for IoT devices. Stefan Lueders (CERN) and Romain Wartel (CERN) for insight into attack vectors against laboratories. A particular thank you to Clement Onime from The Abdus Salam International Centre for Theoretical Physics for the insightful discussion.

## References

1. How The SKA Telescope Will Be Spread Out Across Two Continents, https://www.skatelescope.org/layout/; 2018. Available from: https://www.skatelescope.org/layout/
2. Clark JB, Lecocq F, Simmonds RW, Aumentado J, Teufel JD (2017) Sideband cooling beyond the quantum back action limit with squeezed light. Nature 541:191 EP. https://doi.org/10.1038/nature20604
3. ICARUS Collaboration, Antonello M, Aprili P, Baiboussinov B, Baldo Ceolin M, Benetti P et al (2012) Measurement of the neutrino velocity with the ICARUS detector at the CNGS beam. Phys Lett B 713:17–22
4. Brüning OS, Collier P, Lebrun P, Myers S, Ostojic R, Poole J et al (2004) LHC design report. CERN yellow reports: Monographs. CERN, Geneva. Available from: https://cds.cern.ch/record/782076
5. SURF Cyber Threat Assessment 2017, Education and Research Sectors (2018) Available from: https://www.surf.nl/binaries/content/assets/surf/en/knowledgebase/2017/surfcyberthreatassessment.pdf
6. Atherton CJ, Barton T, Basney J, Broeder D, Costa A, van Daalen M, et al (2018) Federated identity management for research collaborations. Available from: https://doi.org/10.5281/zenodo.1307551
7. Short H, Wartel R (2016) Building security and trust in inter-federation. Proc Sci. https://doi.org/10.22323/1.270.0030
8. Lueders S (2017) Computer security: IoTs: the treasure trove of CERN. Available from: https://home.cern/cern-people/updates/2017/01/computer-security-iots-treasure-trove-cern
9. Agarwal S, Oser P, Short H, Lueders S (2017) Internet of Things security. Available from: https://doi.org/10.5281/zenodo.1035034
10. Perkel JM (2017) The Internet of Things comes to the lab. Nature 542(7639):125–126