

Saal: Project 21:15 01:00 Day: 4 Track: Security & Hacking nA
2501

Title: **How to Destroy a Laptop with Top Secrets**

Subtitle: How did GCHQ do it to the Guardian's copy of Snowden's files?

Speaker: **Mustafa Al-Bassam, Richard Tynan**

Short: *In the summer of 2013, Guardian employees destroyed computers storing top secret documents from Snowden, on instruction and supervision from GCHQ. With access to the destroyed pieces, we investigated what GCHQ's instructions were and what we can learn from it about securely eradicating data on a machine.*

Long: While the initial disclosures by Edward Snowden revealed how US authorities are conducting mass surveillance on the world's communications, further reporting by the Guardian newspaper uncovered that UK intelligence services were just as involved in this global spying apparatus. Faced with the prospect of further public scrutiny and accountability, the UK Government gave the Guardian newspaper an ultimatum: hand over the classified documents or destroy them. The Guardian decided that having the documents destroyed was the best option. By getting rid of only the documents stored on computers in the UK, it would allow Guardian journalists to continue their work from other locations while acquiescing to the Government's demand. However, rather than trust that the Guardian would destroy the information on their computers to the Government's satisfaction, GCHQ sent two representatives to supervise the operation. Typically, reliable destruction of such hardware in the circumstances would be to shred or melt all electronic components using a much larger version of the common paper shredder and leaving only the dust of the original devices. Indeed, some devices such as external USB sticks were turned to dust. Alternatively, it might have been expected that GCHQ would solely target the hard drives of the devices in question. The hard drives, after all, are one of the few components of a computer where user data is supposed to be retained after the power to the device is removed. Surprisingly, however, GCHQ were not just interested in hard drives nor did they destroy whole devices. An examination of the targeted hardware by Privacy International, with cooperation from the Guardian, has found the whole episode to be more troubling and puzzling than previously believed. During our investigation, we were surprised to learn that a few very specific components on devices, such as the keyboard, trackpad and monitor, were targeted along with apparently trivial chips on the main boards of laptops and desktops. Initial consultation with members of the technology community supported our identification of the components and that the actions of GCHQ were worth analysing further. In light of GCHQ's actions, we have asked hardware manufacturers to explain what these elements actually do: what information can be stored on a device, how much information it can retain, and for how long.