

Appendix: Photographs of IoT Failures

In my travels, it disturbs me to find so many everyday devices as well as safety-critical devices without adequate cybersecurity controls.

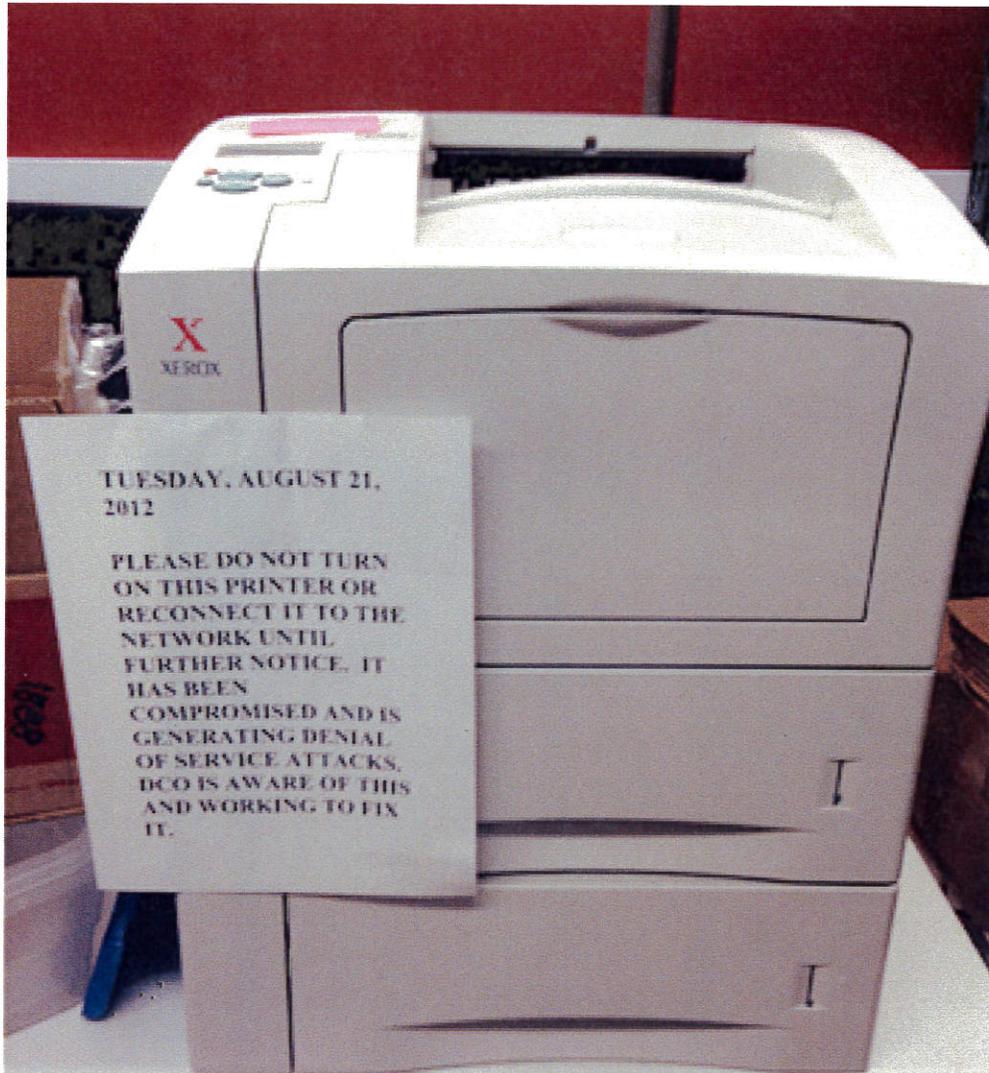


Figure 2: A smaller scale precursor to the Dyn DDoS attack, this printer at the University of Michigan was infected by network-based malware and began to generate denial of service attacks against other institutions.



Figure 3: This water treatment facility in Michigan depends on insecure Windows XP for its water pump controls. In my photograph, you can see the Windows XP logo. Note that Windows XP ended security patch maintenance several years ago, and customers were advised of the expiration date before making purchases of the software. Windows XP machines are trivially compromised because there are no security fixes available and perimeter-based security provides little assurance.

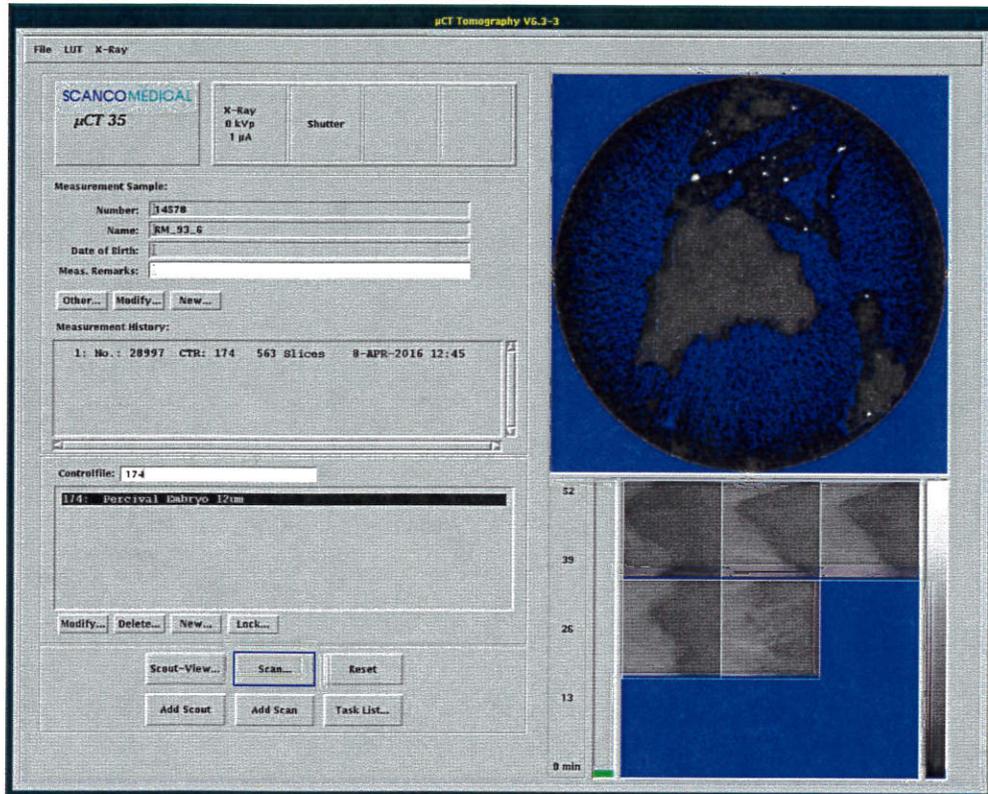


Figure 4: A researcher on Twitter claims to have discovered a tomography machine on the Internet by using the Shodan IoT vulnerability search engine. I have insufficient information to verify, however, but it is quite plausible. IoT medical devices can be both victims and sources of DDoS attacks.



Figure 5: I found this gas pump had crashed, and was unable to pay at the pump. Imagine if a virus knocked out every gas pump simultaneously in the nation, or if a chorus of infected gas pumps began to unwittingly mount DDoS attacks on critical infrastructure.



Figure 6: This airplane entertainment system running Linux crashed on my plane. While entertainment is not safety critical, imagine if flight control systems accidentally had a pathway to the entertainment software. Automobiles used to separate entertainment systems from engine control. However, a programmer eventually mixed the two systems unwittingly, enabling hackers to take control of an automobile by infecting the entertainment system.



Figure 7: Crashed flight display consoles are a common occurrence in airports. Imagine if every smart TV in the world were simultaneously infected with a virus, sourcing a massive DDoS attack against a victim like Dyn.



Figure 8: When checking in for a flight, I had difficulty because the boarding pass kiosk gave me a Windows GUI. Computing is everywhere, and we often forget how much we depend on hard-to-maintain software.



Figure 9: This is a pharmaceutical compounder from my lab at the University of Michigan. Hospitals use this device to mix custom, liquid drugs for IV delivery. FDA received a complaint that this model of compounder was infected with a virus. We found the machine to be running Windows XP, an insecure operating system. It was trivial to infect. A former employee of the company further explained that when the compounder was brought in for repair, the malware was accidentally spread to other compounders under repair.



Figure 10: Even taxi cabs run on Windows. For the moment, the payments systems are separate from the engine control unit. But history shows that engineering mistakes happen, and one could imagine a vulnerability in an IoT payment system that causes massive disruption of transportation.