STATEMENT OF PROF. KEVIN FU, PH.D.

DEPARTMENT OF
ELECTRICAL ENGINEERING & COMPUTER SCIENCE
UNIVERSITY OF MICHIGAN
ANN ARBOR, MI

CEO, VIRTA LABORATORIES, INC
ANN ARBOR, MI

INFRASTRUCTURE DISRUPTION:
INTERNET OF THINGS SECURITY

SUBMITTED TO THE
U.S. HOUSE ENERGY AND COMMERCE COMMITTEE

SUBCOMMITTEE ON COMMUNICATIONS AND
TECHNOLOGY & SUBCOMMITTEE ON COMMERCE,
MANUFACTURING, AND TRADE
JOINT HEARING ON

UNDERSTANDING THE ROLE OF CONNECTED DEVICES
IN RECENT CYBER ATTACKS

WEDNESDAY, NOVEMBER 16, 2016

1 Introduction

Good morning, Chairman Walden, Chairman Burgess, Ranking Member Eshoo, Ranking Member Schakowsky, and distinguished members of the Committee. I am testifying before you today on the insecurity of the Internet of Things (IoT) as related the recent attacks on Dyn. I will provide a perspective on the evolving cybersecurity risks and frame the issues in broader societal context. In the appendix of my written testimony, you can also find photographs and stories of problematic IoT devices where I invite your questions. In short, IoT security remains woefully inadequate, and the Dyn attack is a sign of worse pains to come. None of these attacks are new, but the sophistication, scale of disruption, and impact on infrastructure is unprecedented[1]. Cybersecurity needs to be built into IoT devices, not bolted on after the fact. I will close with a summary and recommendations on what can be done to improve IoT security and innovation.

Credentials and experience. My name is Dr. Kevin Fu. I represent the academic cybersecurity research community. I am Associate Professor of Electrical Engineering & Computer Science at the University of Michigan where I conduct research on embedded security, the discipline of protecting computers built into every day objects ranging from mobile phones and smart thermostats to pacemakers and automotive airbags. My educational qualifications include a Ph.D., master's degree, and bachelor's degree from M.I.T.'s Department of Electrical Engineering and Computer Science. Michigan teaches programming to over 1,300 undergraduates each year, and we teach a rigorous course in computer security to 440 undergraduates each year. I am speaking today as an individual. All opinions, findings, and conclusions are my own and do not necessarily reflect the views of any of my past or present sponsors or employers.

[1] The earliest prediction of IoT problems I have found is from 1995 on page 22 of the MIT Voodoo Humor Magazine on Internet-enabled lightbulbs. `http://web.mit.edu/voodoo/www/archive/pdfs/1995-Fall.pdf`

2 Observations and Recommendations

In this testimony, I'd like to make the following observations and recommendations.

1. Security needs to be built into IoT devices, not bolted on. If cybersecurity is not part of the early design of an IoT device, it's too late for effective risk control.

2. Good security and bad security look the same at the surface. Default passwords are pervasive and harmful. Testing is an essential part of security, but a complete security development lifecycle is necessary to effectively defend against increasingly sophisticated threats.

3. Focus on *exposure* to cybersecurity risks rather than merely "connectedness."

4. For IoT devices already deployed, take joy that the millions of insecure IoT devices are just a small fraction of what the IoT market will resemble in 2020.

5. Unlike inconvenient security problems for your tablet or notebook computer, IoT insecurity puts human safety at risk. Innovative systems will not be safe if they are not secure. Human factors may impact IoT security more so than the technology. For instance, poor user interfaces may encourage consumers to make unwise security decisions.

6. Security is a solution, not a problem. Better cybersecurity will enable new markets, promote innovation, and give consumers confidence to use new technologies that improve the quality of life. Poor security will likely cause the IoT market to eventually collapse on itself as consumers begin to lose trust in technology from compilations of horror stories.

7. There are tens of thousands of unfilled cybersecurity jobs in the USA. Existing approaches are insufficient to train a large enough work force to counter growing cybersecurity threats against IoT devices, our economy, and infrastructure.

8. The nation lacks independent, FFRDC-scale testing facilities akin to the NTSB (postmarket), automotive crash safety testing (premarket), or NNSS (destruction and survivability testing) to provide a proving ground for embedded cybersecurity defenses needed by IoT.

My recommendations aim to ensure that insecure IoT technology does not put our national infrastructure, hospitals, and homes at risk.

1. Incentivize built-in, basic cybersecurity hygiene for IoT devices by establishing meaningful security milestones and encouraging use of strong cryptography.

2. Support agencies such as NIST and NSF to advance our understanding of how to protect IoT devices and to establish a cybersecurity workforce that meets industry needs.

3. Study the feasibility of standing up an independent, national embedded cybersecurity testing facility modeled after the NTSB, automotive crash safety testing, or the Nevada National Security Site.

4. Leverage the existing cybersecurity expertise within NIST's National Cybersecurity Center of Excellence (CCoE) and Information Security and Privacy Advisory Board (ISPAB).

5. To meet national cybersecurity workforce shortfalls and protect our national infrastructure, universities, industry, and government must find the strength and resolve to invest in embedded cybersecurity with interdisciplinary science and engineering, industrial partnerships for research and education, and service to the nation.

3 Why All the Fuss about Internet of Things Security?

None of these risks are new. Researchers have known about these flaws for decades. What's new is the scale and ease of attack because of the quantity of insecure IoT devices operated by a highly distributed set of unwitting consumers.

To put the Dyn attack in perspective, think back to the 1980s when a person might dial the operator to ask, “Please connect me to Alice.” The operator looks in a directory, finds the phone number, then connects the caller to Alice. If only a few people call the operator in a period of time, there is no problem. If 100,000 compromised IoT devices make this simple query simultaneously, the operator will be overwhelmed. Legitimate callers will likely receive a busy tone. That is essentially what happened to Dyn. An overwhelming number of insecure IoT devices were tricked into making directory queries to Dyn.

Think exposure, not connectedness. The term “networked” and “connected” are red herrings in the long term because both terms hint at a perimeter-based security model. There are no effective network perimeters because IoT devices are notorious for piercing perimeters. Moreover, a device can be partially connected. The healthcare community does not issue different guidance for flu transmitted by cough versus flu transmitted by sneeze. Therefore, the cybersecurity community should not limit its thinking to just networks and connectivity. A network is not necessary for a cybersecurity exploit; malware gets in just fine by unhygienic USB drives carried by unwitting personnel. Hackers continue to use social engineering by telephone to trick personnel into giving out unauthorized remote access. Rather than focus on *connected* devices, a more comprehensive approach would examine *exposed* devices. Focus on outcomes, not modalities. I recommend using language such as “exposed to cybersecurity risk” instead of “networked” or “connected” when discussing overall objectives because cybersecurity threats are constantly evolving.

Complexity breads insecurity. In my role as a member of the Computing Community Consortium (CCC) Council, I recognize the painful challenges of IoT security. One of the core problems with the increasing number of IoT devices is the increased complexity that is required to operate them safely and securely. This increased complexity creates new safety, security, privacy, and usability challenges far beyond the difficult challenges individuals face just securing a single device.

4 Examples of IoT Security Problems

Many of the security problems in IoT devices are attributable to lack of proper security engineering during early design, but IoT devices also pose risks quite different in nature from traditional computing. While both traditional computing and IoT devices suffer from poor cyberhygiene such as the use of factory-set default passwords, IoT devices tend to have safety consequences or involve physical manipulation of the world that could more easily lead to harm.

National Vulnerability Database. The NVD now includes a category for IoT devices. NIST quantifies risks of IoT vulnerabilities, and some of the results appear in the Common Vulnerabilities and Exposures (CVE) database. Relevant to the Dyn attack, a DDoS vulnerability was scored in 2009 for a connected coffee pot (CVE-2008-7174), vehicle vulnerabilities, (CVE-2015-5611, Jeep Chrysler vehicle) and medical devices (CVE-2011-3386, Medtronic insulin pump).

Internet-connected home security cameras. The irony is not lost on me that security cameras have created an unwitting army of network bandwidth weaponry. I built my own home security system and implanted home-made wirelessly powered sensors in the concrete foundation of my house because I found that most security cameras have unverified or weak security. For instance, one foreign manufacturer is a common OEM that supplies software to a number of popular security camera products sold in the USA. This particular software was vulnerable to a remote root exploit, which means an attacker can take total control of the system via the Internet. When the software manufacturer issued a patch to fix the security problem, the software malfunctioned and consumers were forced to undo the patch. The manufacturer has since removed the patch, and provides no mitigating security solution. Consumers are stuck with insecure security cameras.

Hospitals and healthcare delivery. The number one cybersecurity problem for hospitals is how to ensure continuity of clinical operations to deliver safe and timely patient care. Note that security is a means to an end: delivery of care. The healthcare community dodged the bullet on the Dyn attack. Hospitals survived not by design, but by luck. The adversary did not target healthcare. This time. Dyn represents a single point of failure for resolving Internet names, but hospitals have other kinds of single points of failure. For instance, heating and ventilation now resembles IoT with unpatched computers controlling negative pressure in units with highly infectious diseases. Elevators systems run on embedded computers, where there is little understanding of defensive technology. A number of hospitals expressed concern about IoT devices, and no one has been able to provide assurance that a future Dyn-like attack will not cause a massive, nation-wide healthcare outage.

The best known approach is to maintain a more accurate, risk-based inventory of devices, software, and cyberexposure such that when a new vulnerability is discovered, hospitals can more quickly identify affected devices to triage and remediate. However, hospitals simply do not have accurate inventories of software in actual use. In my experience, we usually find “shadow IT” on hospital networks. That is, contraband computing enters hospital infrastructure in unusual ways.

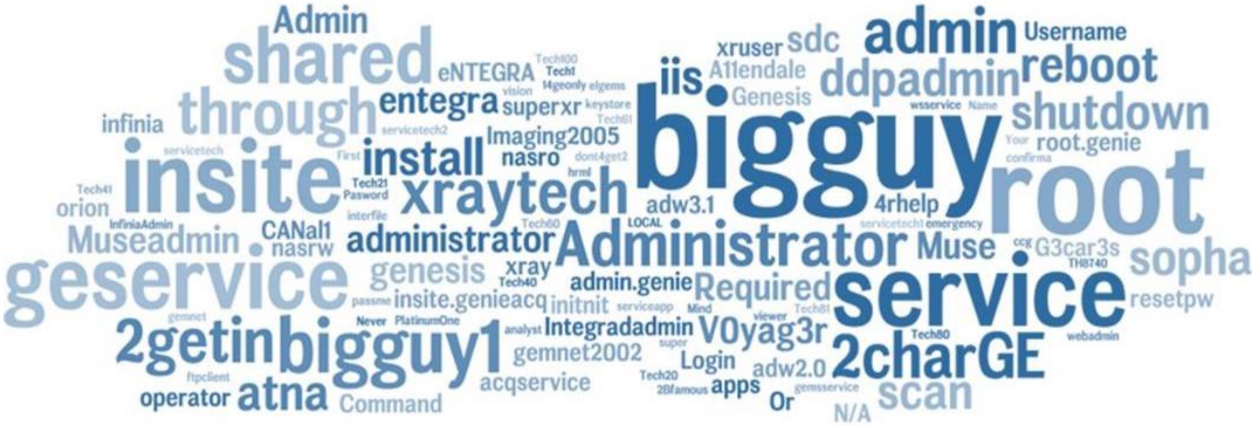


Figure 1: One medical device manufacturer had 35 CVEs and 125+ sets of exposed credentials. This word cloud, courtesy of Scott Erven, describes common default passwords from a single medical device manufacturer. Default passwords on cameras and other IoT devices enabled attackers to direct a tsunami of network traffic at Dyn. Similar default password risks exist for medical devices.

Medical device security. Default passwords and the inability to tolerate intrinsically hostile networks are two common problems in medical IoT devices. Another unusual problem with medical devices is that traditional cryptography does not work as easily on battery-powered, implantable devices because of the risks of cryptographic computations draining the battery. When an implant’s battery runs low, it requires surgical replacement. For this reason, NIST’s effort on lightweight cryptography is especially important. More information about medical device security appears at `medicalsecurity101.org` and `secure-medicine.org`.

No Fire and Forget. There is no fire and forget for IoT security. Threats and vulnerabilities constantly change. Therefore, any solution based solely on manufacturing is doomed to failure. Software effectively ages because of shifting threats, and there will always be a need for vigilance and updates/maintenance. NIST produced a cybersecurity framework for industrial control systems that may apply well to IoT security. NIST recommends to first (1) assess cybersecurity risks of inventory, (2) deploy compensating controls that address specific risks, and (3) continuously monitor the effectiveness of the controls as threats change.

5 Why IoT Needs Embedded Cybersecurity

Embedded cybersecurity represents a rapidly growing area in terms of educational opportunities, research questions, talent demand, and federal policy for science and engineering. Safety critical systems such as automobiles, airplanes, and medical devices depend on embedded cybersecurity. The market size for securing the Internet of Things is predicted to reach $37B by 2021. While there are pockets of cybersecurity research and education programs across the country, the nation lacks an independent testing facility that can begin to model complex behavior of interoperable devices in homes, hospitals, transportation, etc. Moreover, industries will require a highly skilled workforce for embedded security as they discover that security solutions are needed before consumers will gain confidence in innovative new technologies like self-driving cars and sensors that wirelessly command medical devices to delivery therapy.

Assessing medical IoT security. The Mayo Clinic reportedly spends roughly $300K per medical device to perform security assessment, and they have thousands of models of devices. It makes little economic sense to have individual hospitals testing the security of devices that ought to remain secure for all 6,000 hospitals in the USA. Cybersecurity ought to be a public good much like automobile safety. Imagine if every car dealer were individually responsible for crash testing automobiles: costs would skyrocket and the public would have little confidence. A facility for embedded cybersecurity at the scale of a hospital could provide testing to both government and industry, while allowing students to conduct innovative research during surplus time.

National embedded cybersecurity testing facility. Neither industry nor government have the capability to safely conduct thorough security testing and assessment on IoT devices spanning healthcare to transportation. The cost to establish a realistic test facility for healthcare IoT cybersecurity, for instance, is likely to exceed $1.1 billion because of the sheer complexity and specialized equipment. But that is much cheaper and more effective than having 6,000 hospitals across 50 states each attempting to establish tiny facilities.

6 National Activities on IoT Security

Federal agencies such as NIST and NSF have a number of initiatives aimed at improving IoT security. The Computing Research Association's CCC Council has also produced a number of IoT security recommendations on behalf of the computing community. Below I provide references to such documents at various stages of maturity to improve IoT security.

- The Computing Research Association primer on IoT policy and its role in innovation. `http://cra.org/govaffairs/wp-content/uploads/sites/6/2016/02/IoT-Policy-Document.pdf`

- *Systems Computing Challenges in the Internet of Things* by the CCC Council explains that existing best practices in building robust and secure systems are insufficient to address the new security challenges that IoT systems will present.
  `http://cra.org/ccc/wp-content/uploads/sites/2/2015/09/IoTSystemsChallenges.pdf`

- NIST published a widely cited document on cybersecurity for industrial control systems, and one of the draft standards on lightweight cryptography is designed for the especially constrained environment of IoT devices.
  `http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf`
  `http://csrc.nist.gov/publications/drafts/nistir-8114/nistir_8114_draft.pdf`

- NIST published *Special Publication 800-183: Networks of "Things"'* as a framework to guide engineers responsible for securing IoT technology.
  `http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-183.pdf`

- NIST has created a small number of projects to solve security problems in certain high priority IoT technologies such as smart home devices, medical infusion pumps, and manufacturing industrial control systems. http://tinyurl.com/zlhl653

https://nccoe.nist.gov/projects/use_cases/medical_devices

https://nccoe.nist.gov/projects/use_cases/manufacturing

- NSF highlighted a number of projects related to IoT security with application to cars, medical devices, and voting machines.

  https://www.nsf.gov/discoveries/disc_summ.jsp?cntn_id=136601

Thank you. I would be happy to respond to any questions you may have, especially on how IoT security impacts hospitals and medical devices.

Biography

Dr. Kevin Fu, Ph.D., is Associate Professor of Electrical Engineering and Computer Science at the University of Michigan and CEO and co-founder of healthcare cybersecurity startup Virta Laboratories, Inc. His research investigates how to achieve trustworthy computing on embedded devices with application to health care, commerce, and communication. He teaches computer science courses in security and privacy. Virta Labs provides hospitals a managed cybersecurity service called BlueFlow to assure continuity of clinical operations despite medical device security risks.

Fu received his Ph.D. in EECS from MIT where his research pertained to secure storage and how web authentication fails. His participation in the provocative 2008 research paper [12] analyzing the security of a pacemaker/defibrillator led to a wake-up call for cybersecurity in medical device manufacturing.

Fu has given nearly 100 invited talks on medical device security to industry, government, and academia—including Senate and House hearings, the Institute of Medicine, and National Academy of Engineering events. He directs the Archimedes Center for Medical Device Security at the University of Michigan. He co-chaired the AAMI Working Group on Medical Device Security, which led to the the AAMI TIR57 document that advises medical device manufacturers on how to incorporate security engineering into medical device product development. Fu co-authored the NIST Information Security and Privacy Advisory Board recommendations [16] to HHS on how the federal government must adapt to risks of medical device security. His medical device security efforts were recognized with a Fed100 Award, Sloan Research Fellowship, NSF CAREER Award, MIT TR35 Innovator of the Year award, and best paper awards on medical device security by organizations such as IEEE and ACM [2, 13, 10, 6, 7, 3, 15, 14, 5, 4, 11, 1, 9, 17, 8].

Fu served as a visiting scientist on cybersecurity research at the U.S. Food & Drug Administration, the Beth Israel Deaconess Medical Center of Harvard Medical School, Microsoft Research, and MIT CSAIL. He was a member the NIST Information Security and Privacy Advisory Board. ISPAB is a Federal Advisory Committee that identifies emerging managerial, technical, administrative, and physical safeguard issues relative to information security and privacy in Federal Government information systems.

References

[1] W. P. Burleson, S. S. Clark, B. Ransford, and K. Fu. Design challenges for secure implantable medical devices. In *Proceedings of the 49th Design Automation Conference*, DAC '12, June 2012. Invited paper https://spqr.eecs.umich.edu/papers/49SS2-3_burleson.pdf.

[2] S. S. Clark and K. Fu. Recent results in computer security for medical devices. In *International ICST Conference on Wireless Mobile Communication and Healthcare (MobiHealth), Special Session on Advances in Wireless Implanted Devices*, Oct. 2011. https://spqr.eecs.umich.edu/papers/clark-mobihealth11.pdf.

[3] B. Defend, M. Salajegheh, K. Fu, and S. Inoue. Protecting global medical telemetry infrastructure. Technical report, Institute of Information Infrastructure Protection (I3P), Jan. 2008. https://web.eecs.umich.edu/~kevinfu/papers/whitepaper-protecting_global_medical.pdf.

[4] T. Denning, K. Fu, and T. Kohno. Absence makes the heart grow fonder: New directions for implantable medical device security. In *Proceedings of USENIX Workshop on Hot Topics in Security (HotSec)*, July 2008. https://spqr.eecs.umich.edu/papers/watchdog-hotsec08.pdf.

[5] K. Fu. Inside risks, reducing the risks of implantable medical devices: A prescription to improve security and privacy of pervasive health care. *Communications of the ACM*, 52(6):25–27, June 2009. http://www.csl.sri.com/users/neumann/insiderisks08.html#218.

[6] K. Fu. Software issues for the medical device approval process, Apr. 2011. Statement to the Special Committee on Aging, United States Senate, Hearing on a delicate balance: FDA and the reform of the medical device approval process, Wednesday, April 13, 2011 https://spqr.eecs.umich.edu/papers/fu-senate-comm-aging-med-dev-sw-apr-2011.pdf.

[7] K. Fu. Trustworthy medical device software. In *Public Health Effectiveness of the FDA 510(k) Clearance Process: Measuring Postmarket Performance and Other Select Topics: Workshop Report*, Washington, DC, July 2011. IOM (Institute of Medicine), National Academies Press https://spqr.eecs.umich.edu/papers/fu-trustworthy-medical-device-software-IOM11.pdf.

[8] K. Fu. On the technical debt of medical device security. Technical report, National Academy of Engineering FOE, Sept. 2015. http://www.naefrontiers.org/File.aspx?id=50750. A version appeared in the National Academy of Engineering's *The Bridge*, Winter 2016.

[9] K. Fu and J. Blum. Inside risks: Controlling for cybersecurity risks of medical device software. *Communications of the ACM*, 56(10):21–23, Oct. 2013. http://www.csl.sri.com/users/neumann/cacm231.pdf.

[10] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu. They can hear your heartbeats: Non-invasive security for implanted medical devices. In *Proceedings of ACM SIGCOMM*, Aug. 2011. https://spqr.eecs.umich.edu/papers/gollakota-SIGCOMM11-IMD.pdf.

[11] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel. Security and privacy for implantable medical devices. *IEEE Pervasive Computing, Special Issue on Implantable Electronics*, 7(1):30–39, Jan. 2008. https://spqr.eecs.umich.edu/papers/b1kohFINAL2.pdf.

[12] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In *Proceedings of the 29th Annual IEEE Symposium on Security and Privacy*, pages 129–142, May 2008. https://www.secure-medicine.org/public/publications/icd-study.pdf.

[13] S. Hanna, R. Rolles, A. Molina-Markham, P. Poosankam, K. Fu, and D. Song. Take two software updates and see me in the morning: The case for software security evaluations of medical devices. In *Proceedings of 2nd USENIX Workshop on Health Security and Privacy (HealthSec)*, Aug. 2011. https://spqr.eecs.umich.edu/papers/hanna-aed-healthsec11.pdf.

[14] S. Lee, K. Fu, T. Kohno, B. Ransford, and W. H. Maisel. Clinically significant magnetic interference of implanted cardiac devices by portable headphones. *Heart Rhythm Journal*, 6(10):1432–1436, Oct. 2009. http://bit.ly/1NEk3dR or http://download.journals.elsevierhealth.com/pdfs/journals/1547-5271/PIIS1547527109007401.pdf.

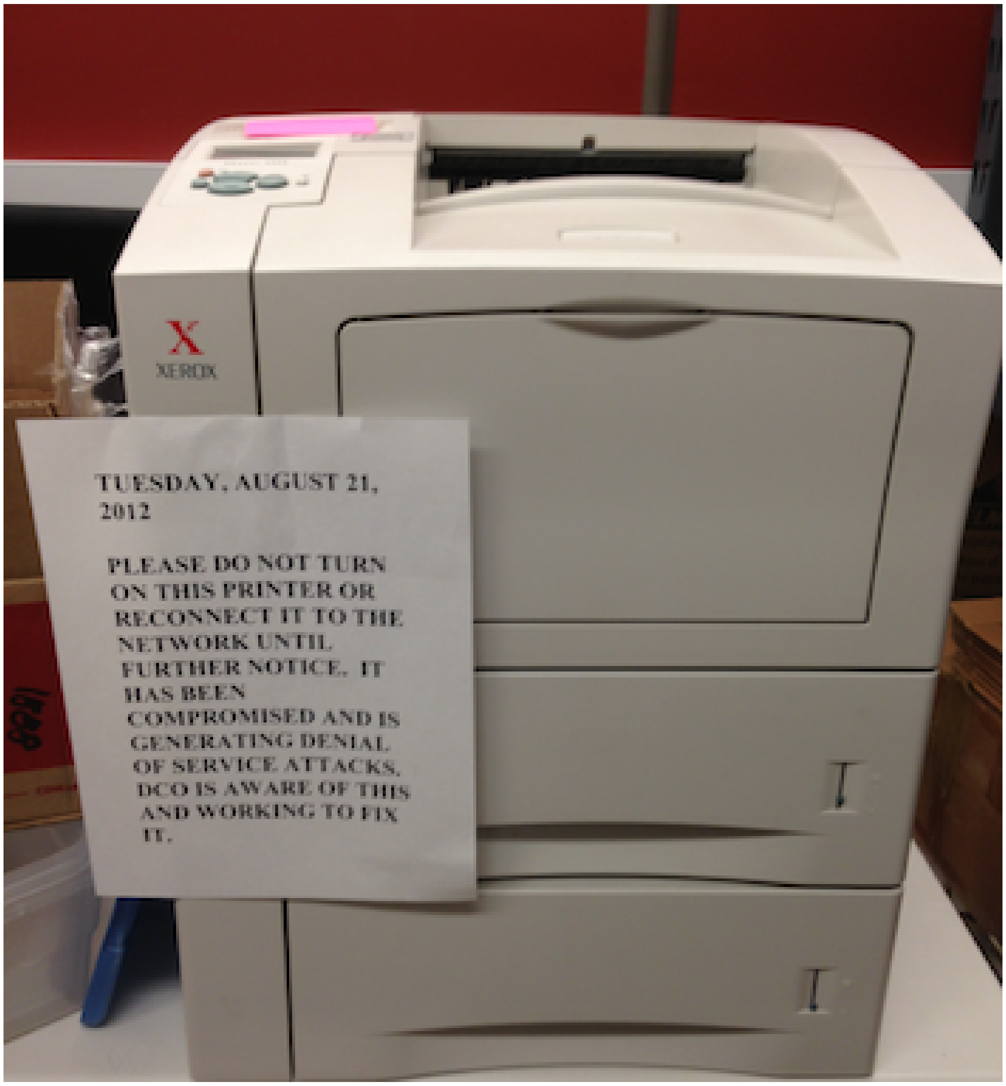
[15] A. D. Molina, M. Salajegheh, and K. Fu. HICCUPS: Health information collaborative collection using privacy and security. In *Proceedings of the Workshop on Security and Privacy in Medical and Home-Care Systems (SPIMACS)*, pages 21–30. ACM Press, Nov. 2009.

[16] NIST ISPAB federal advisory commmittee recommendations on improving medical device cybersecurity, 2012. Sent to OMB Director, HHS Secretary, NSC, DHS, NIST, March 30, 2012 http://1.usa.gov/1qlnh0X or http://csrc.nist.gov/groups/SMA/ispab/documents/correspondence/ispab-ltr-to-omb_med_device.pdf.

[17] M. Salajegheh, A. Molina, and K. Fu. Privacy of home telemedicine: Encryption is not enough. *Journal of Medical Devices*, 3(2), Apr. 2009. Design of Medical Devices Conference Abstracts `https://spqr.eecs.umich.edu/papers/salajegheh-DMD09-abstract.pdf`.

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.



TUESDAY, AUGUST 21, 2012

PLEASE DO NOT TURN ON THIS PRINTER OR RECONNECT IT TO THE NETWORK UNTIL FURTHER NOTICE. IT HAS BEEN COMPROMISED AND IS GENERATING DENIAL OF SERVICE ATTACKS. DCO IS AWARE OF THIS AND WORKING TO FIX IT.

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.

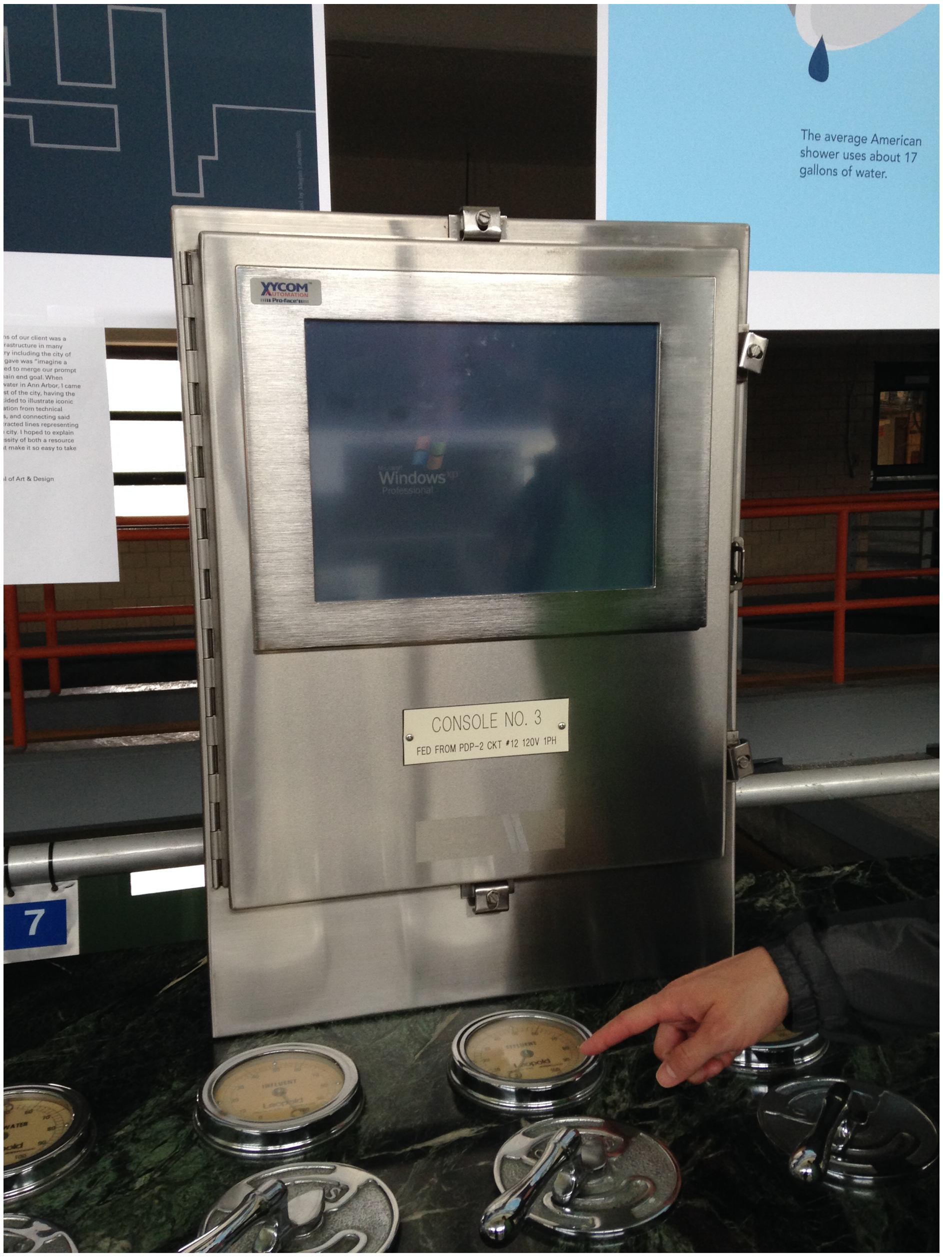
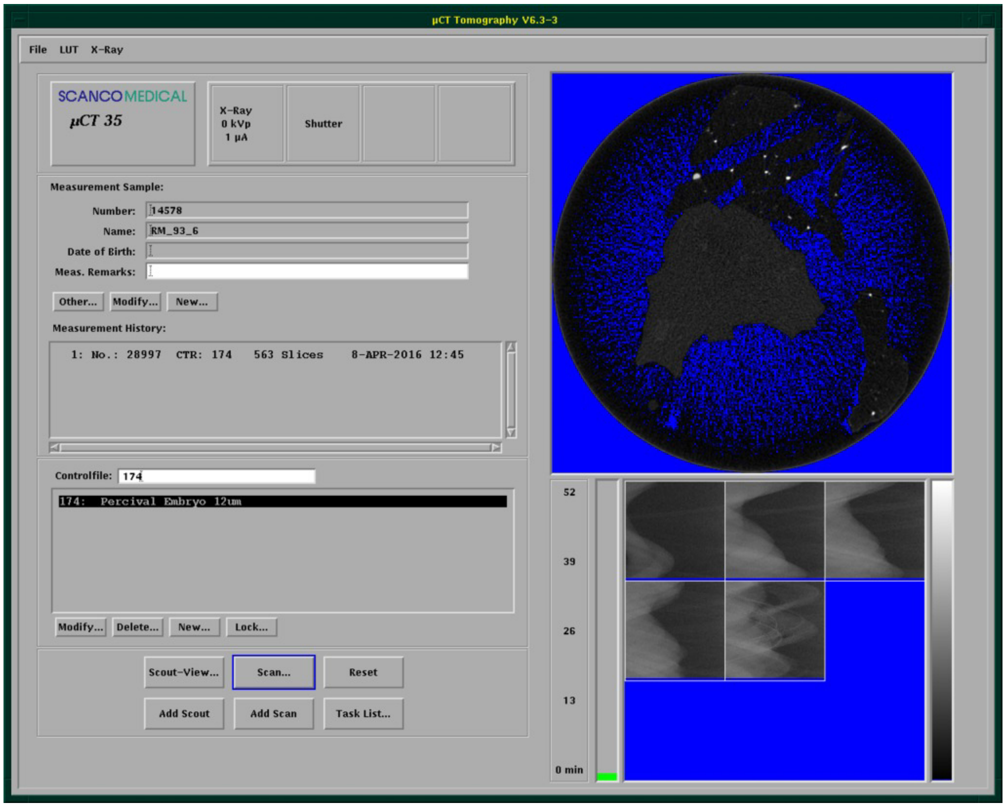

The average American shower uses about 17 gallons of water.
XYCOM AUTOMATION
Windows XP Professional
CONSOLE NO. 3
FED FROM PDP-2 CKT #12 120V 1PH
7

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.



X-Ray
0 kVp
1 µA

Measurement Sample:

Number: 14578
Name: RM_93_6
Date of Birth:
Meas. Remarks:

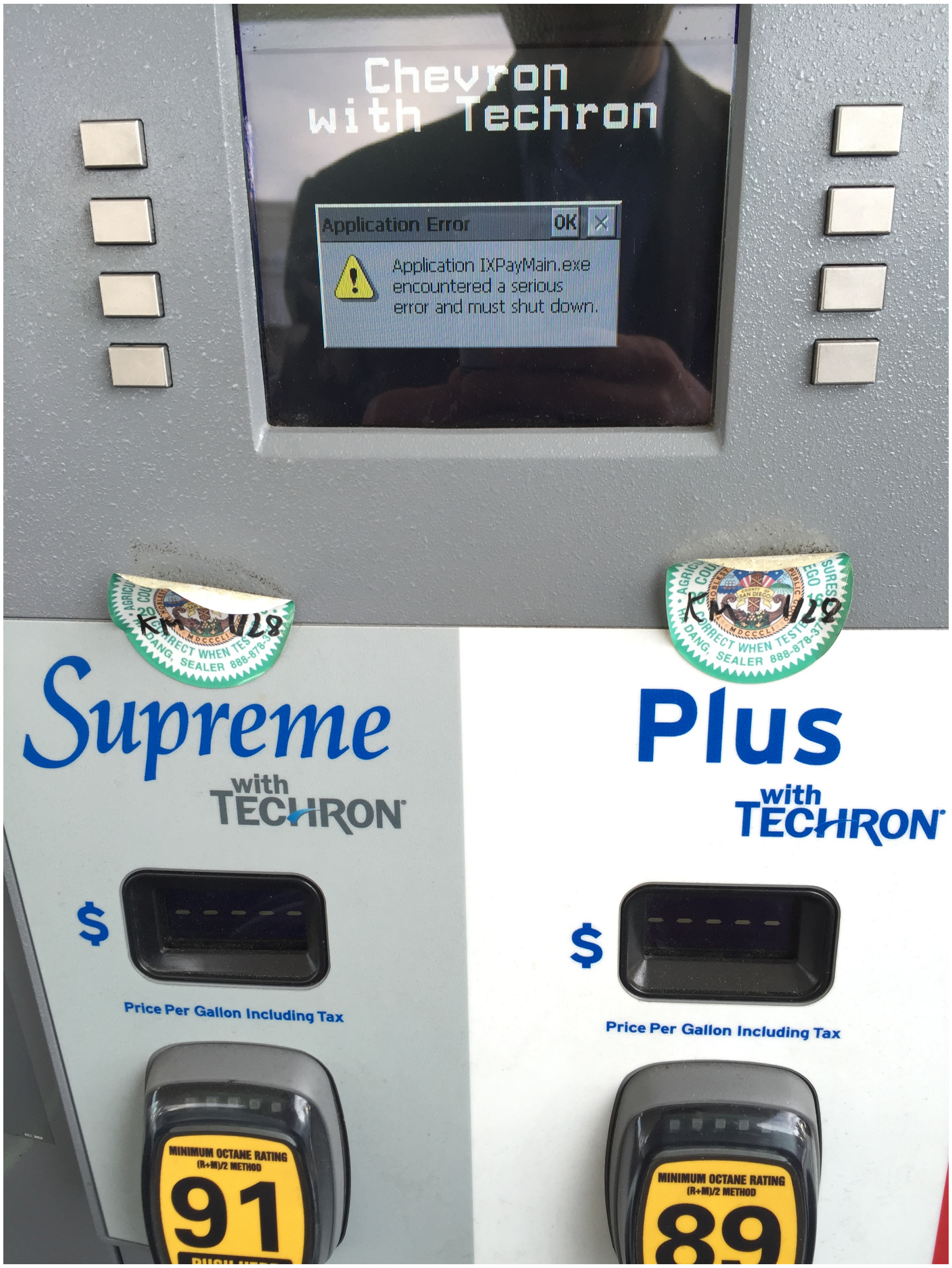
Measurement History:

```
1: No.: 28997   CTR: 174   563 Slices   8-APR-2016 12:45
```

Controlfile: 174

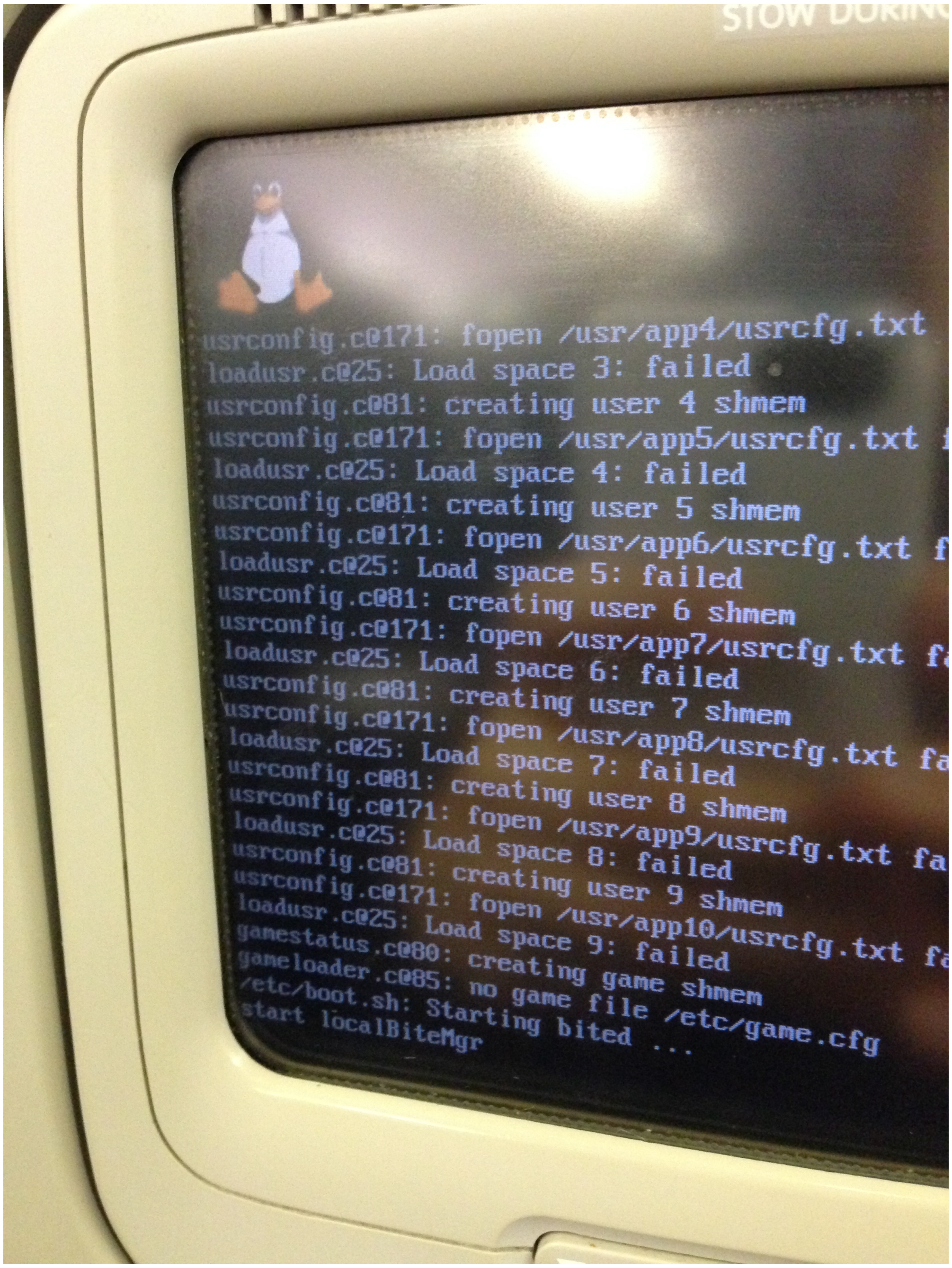
```
174:  Percival Embryo 12um
```

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.



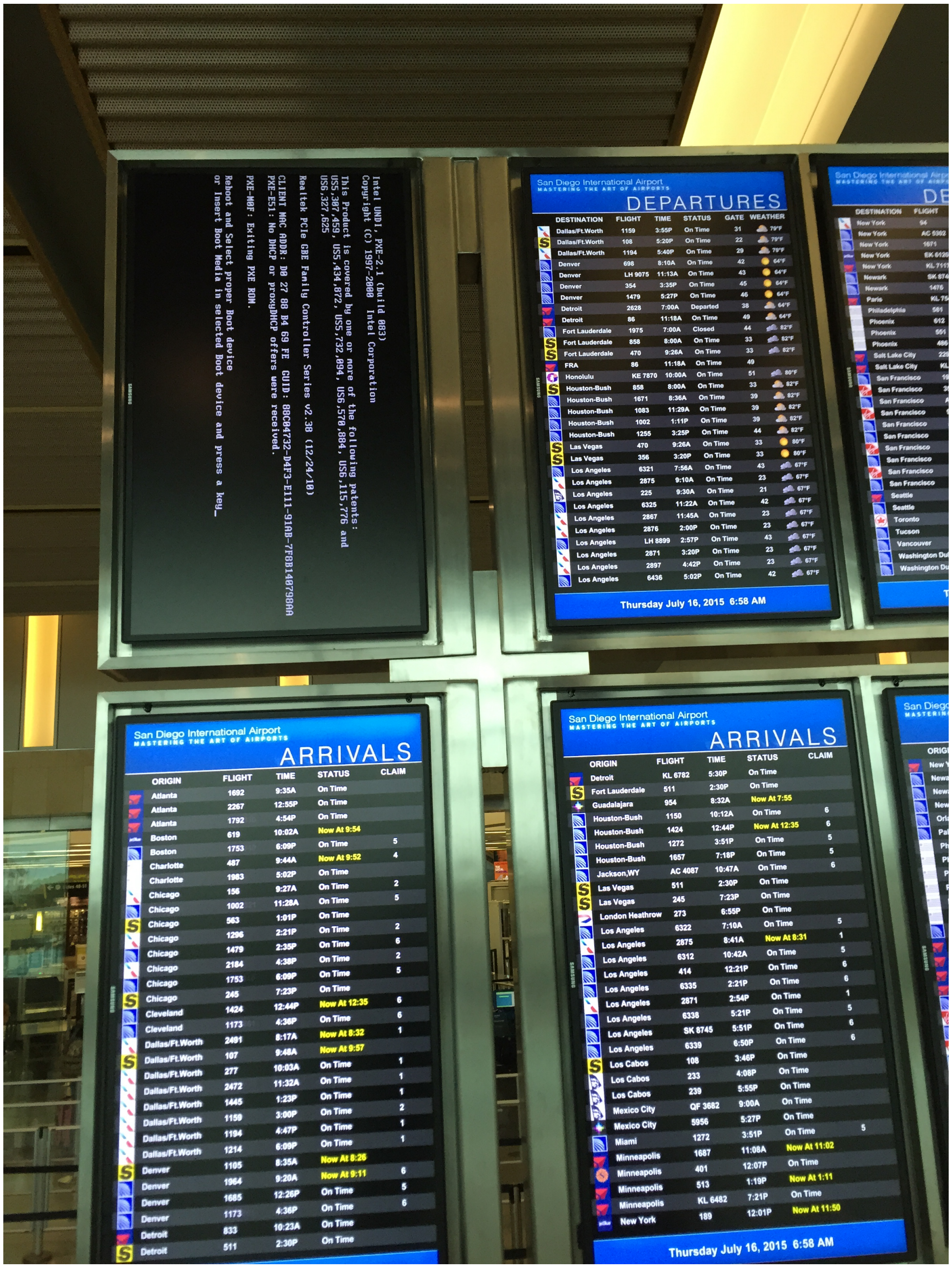
Application IXPayMain.exe encountered a serious error and must shut down.

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.



```
usrconfig.c@171: fopen /usr/app4/usrcfg.txt
loadusr.c@25: Load space 3: failed
usrconfig.c@81: creating user 4 shmem
usrconfig.c@171: fopen /usr/app5/usrcfg.txt f
loadusr.c@25: Load space 4: failed
usrconfig.c@81: creating user 5 shmem
usrconfig.c@171: fopen /usr/app6/usrcfg.txt f
loadusr.c@25: Load space 5: failed
usrconfig.c@81: creating user 6 shmem
usrconfig.c@171: fopen /usr/app7/usrcfg.txt fa
loadusr.c@25: Load space 6: failed
usrconfig.c@81: creating user 7 shmem
usrconfig.c@171: fopen /usr/app8/usrcfg.txt fa
loadusr.c@25: Load space 7: failed
usrconfig.c@81: creating user 8 shmem
usrconfig.c@171: fopen /usr/app9/usrcfg.txt fa
loadusr.c@25: Load space 8: failed
usrconfig.c@81: creating user 9 shmem
usrconfig.c@171: fopen /usr/app10/usrcfg.txt fa
loadusr.c@25: Load space 9: failed
gamestatus.c@80: creating game shmem
gameloader.c@85: no game file /etc/game.cfg
/etc/boot.sh: Starting bited ...
start localBiteMgr
```

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.



```
Intel UNDI, PXE-2.1 (build 083)
Copyright (C) 1997-2000  Intel Corporation

This Product is covered by one or more of the following patents:
US5,307,459, US5,434,872, US5,732,094, US6,570,884, US6,115,776 and
US6,327,625

Realtek PCIe GBE Family Controller Series v2.38 (12/24/10)

CLIENT MAC ADDR: D0 27 88 B4 69 FE  GUID: 88C04732-D4F3-E111-91AB-7F8B140798AA
PXE-E51: No DHCP or proxyDHCP offers were received.

PXE-M0F: Exiting PXE ROM.

Reboot and Select proper Boot device
or Insert Boot Media in selected Boot device and press a key_
```

San Diego International Airport
MASTERING THE ART OF AIRPORTS
DEPARTURES
Thursday July 16, 2015 6:58 AM
San Diego International Airport
MASTERING THE ART OF AIRPORTS
ARRIVALS
San Diego International Airport
MASTERING THE ART OF AIRPORTS
ARRIVALS
Thursday July 16, 2015 6:58 AM

Figure 7: Crashed flight display consoles are a common occurence 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.

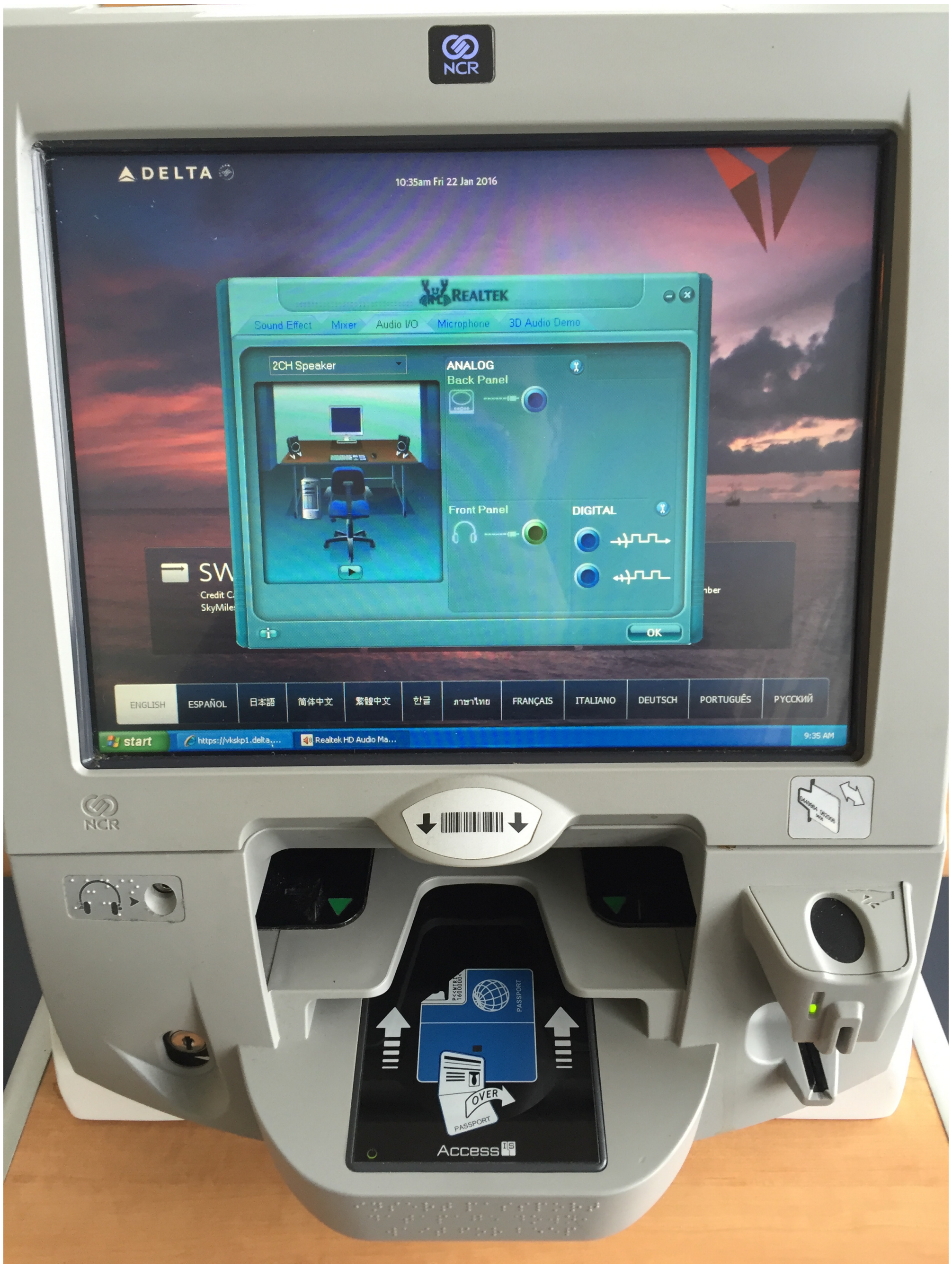


Figure 8: When checking in for a flight, I had difficulty because the boarding pass kiosk gave me a Windows GUI. Computing is everywhere, and we often forget how much we depend on hard-to-maintain software.

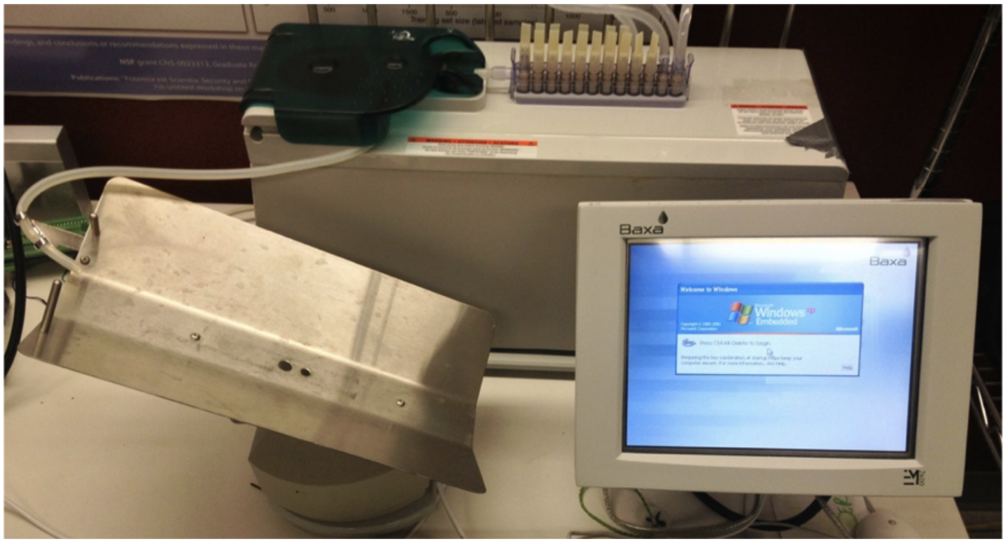
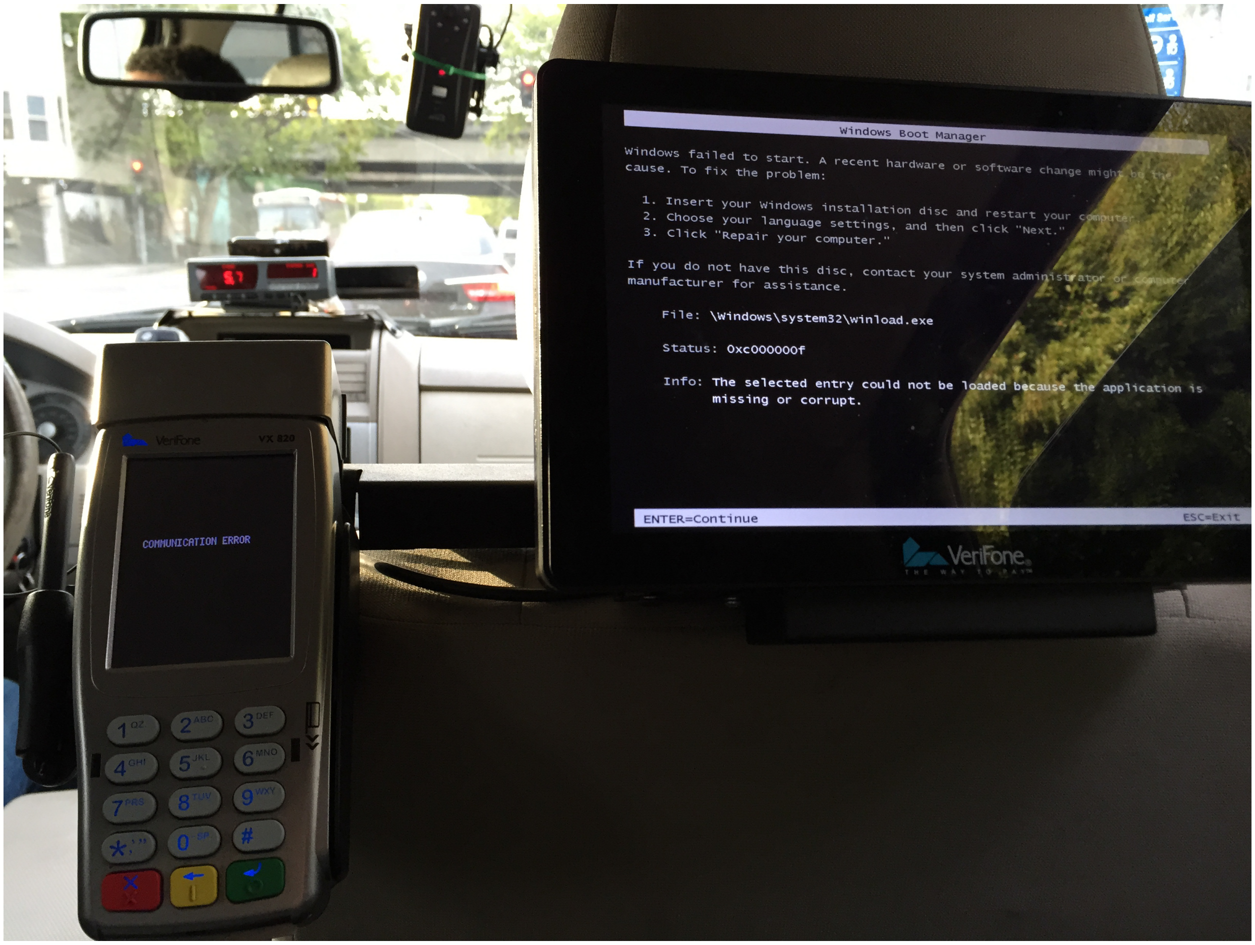


Figure 9: This is a pharmaceutical compounder from my lab at the University of Michigan. Hospitals use this device to mix custom, liquid drugs for IV delivery. FDA received a complaint that this model of compounder was infected with a virus. We found the machine to be running Windows XP, an insecure 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.



```
                         Windows Boot Manager
Windows failed to start. A recent hardware or software change might be the
cause. To fix the problem:

  1. Insert your Windows installation disc and restart your computer
  2. Choose your language settings, and then click "Next."
  3. Click "Repair your computer."

If you do not have this disc, contact your system administrator or computer
manufacturer for assistance.

    File: \Windows\system32\winload.exe

    Status: 0xc000000f

    Info: The selected entry could not be loaded because the application is
          missing or corrupt.

ENTER=Continue                                                      ESC=Exit
```

```
COMMUNICATION ERROR
```

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.