BLOG@UBIQUITY

IOT, POLICY, PRIVACY AND SECURITY, TECHNOLOGY

Dealing with Infrastructure Disruption: IoT Security

DECEMBER 28, 2016 | KEVIN FU | 0 COMMENTS

Editor's intro: *The Internet of Things (IoT) has become a hot topic because of unprecedented cybersecurity problems that have caused massive outages of key Internet services. IoT devices can help improve the lives of individuals, but lack of market incentives has led to huge cybersecurity vulnerabilities that threaten to undermine national infrastructure and public trust. Prof. Kevin Fu was invited to a U.S. House Hearing by Chairman Greg Walden of the Subcommittee of Communication and Technology and Chairman Michael Burgess of the Subcommittee on Commerce, Manufacturing, and Trade to discuss IoT vulnerabilities and what might be done about them. We are pleased to present a copy of his testimony.*

Last month, I had the opportunity to testify in U.S. Congress on how to improve the security of the Internet of Things (IoT) in the wake of the crippling attack on Dyn, a DNS service provider and single point of failure for popular Internet services.

The hearing was a joint project between the Commerce, Manufacturing, and Trade Subcommittee (CMT) and the Communications and Technology Subcommittee within the U.S. House Energy & Commerce Committee. The CMT subcommittee held an IoT specific hearing in March 2015 along with a showcase of multiple IoT devices for Congressional members. Congress called upon my advice because of my expertise across a variety of these issues in the broader societal context, especially healthcare and medical device security.

I reminded our U.S. Representatives that we've been slowly boiling a frog, and the problem is more broadly how to protect computers built into everyday objects ranging from mobile phones and smart thermostats to pacemakers and automotive airbags. In short, security must be built into IoT devices, rather than bolted on after deployment.

I provided a perspective on the evolving cybersecurity risks framed in a broader societal context. 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. (The earliest prediction of IoT problems I have found is from 1995 on page 22 of MIT's humor magazine, *Voo Doo*, on Internet-enabled light

bulbs.)

We are in this sorry and deteriorating state because there is almost no cost to a manufacturer for deploying products with poor cybersecurity to consumers. Has a consensus body or federal agency issued a meaningful IoT security standard? Not yet. Is there a national testing lab to verify and assess the premarket security of IoT devices? No. Is there a tangible cost to any company that puts an insecure IoT device into the market? No.

I'd like to highlight eight observations about IoT security.

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. The healthcare community does not issue different advice for flu transmitted by cough versus flu transmitted by sneeze. Similarly, both connected and disconnected IoT devices carry significant cybersecurity risks. A USB drive can spread malware quite effectively.
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. It will get worse if security problems remain unchecked.
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 more than 209,000 unfilled cybersecurity jobs in the USA, and more than 1 million unfilled positions globally. Existing approaches are inadequate to train a large enough workforce to counter growing cybersecurity threats against IoT devices, our economy, and infrastructure.
8. The nation lacks an independent testing facility at the scale of a federally funded research and development center (FFRDC) as a proving ground for testing premarket IoT cyber-

crashworthiness and for testing embedded cybersecurity defenses.

I shared five recommendations to protect our national infrastructure, hospitals, and homes from IoT security risks.

1. Incentivize built-in, basic cybersecurity hygiene for IoT devices by establishing meaningful milestones and encouraging use of strong cryptography.
2. Support agencies such as the National Institute for Standards & Technology (NIST) and the National Science Foundation (NSF) to advance our understanding of IoT security, and to train hundreds of thousands of students necessary for a robust cybersecurity workforce.
3. Study the feasibility of setting up an independent, national embedded cybersecurity testing facility modeled after post-incident initiatives such as the National Transportation Safety Board, incident-prevention initiatives such as the National Highway Traffic Safety Administration, and survivability and destruction testing at the Nevada National Security Site.
4. Leverage the existing cybersecurity expertise within NIST, NSF, DHS, and DARPA. NIST also provides expertise via the National Cybersecurity Center of Excellence (NCCoE) and Information Security and Privacy Advisory Board (ISPAB).
5. Universities, industry, and government must find the strength and resolve to partner to meet national cybersecurity workforce shortfalls and for protecting our national infrastructure. Investments in embedded cybersecurity will pay great dividends to our society and economy with interdisciplinary science and engineering, industrial partnerships for research and education, and service to the nation.

DHS released an IOT security document on the day before my testimony (Strategic Principles for Securing the Internet of Things). I find the document consistent with my thinking, but without an action plan or Congressional remit with teeth. This is already a marketplace failure, and it's time for government to intervene with appropriate regulations for the public good. A software bill of materials is an excellent idea to enable more informed, risk-based decision making by industry and consumers.

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 have dialed the operator to ask, “Please connect me to Alice.” The operator looked in a directory, found the phone number, then connected the caller to Alice. If only a few people call the operator within a period of time, there is no problem. If 100,000 compromised IoT devices make this simple query simultaneously, the operator would be overwhelmed. Legitimate callers would 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 distinguish a flu transmitted by cough versus a 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 breeds 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.

Examples of IoT Security Problems

Many of the security problems in IoT devices are attributable to a 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 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 U.S. This particular software was vulnerable to a remote root exploit, which means an attacker could 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, but provided 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 pro-

vide 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-plus 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 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 cy-

bersecurity risks of inventory, (2) deploy compensating controls that address specific risks, and (3) continuously monitor the effectiveness of the controls as threats change.

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 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 deliver 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 U.S. 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. Moreover, partnerships across industry, government, and academia can amortize this cost.

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.

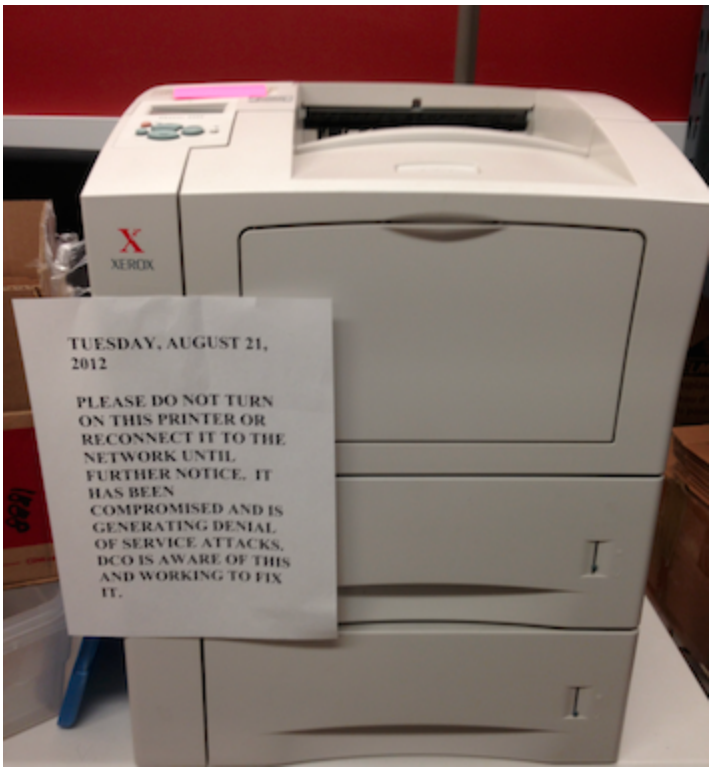
1. The Computing Research Association primer on IoT policy and its role in innovation.
2. *Systems Challenges in the Internet of Things* by the CCC Council explains existing best practices in building robust and secure systems are insufficient to address the new security challenges that IoT systems will present.
3. 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.
4. NIST published *Special Publication 800-183: Networks of "Things"* as a framework to guide engineers responsible for securing IoT technology.
5. 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.
6. NSF highlighted a number of projects related to IoT security with application to cars, medical devices, and voting machines.

This research is supported in part by the National Science Foundation (CNS-1330142). The views and conclusions contained in this paper are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of NSF or our sponsors.

Appendix

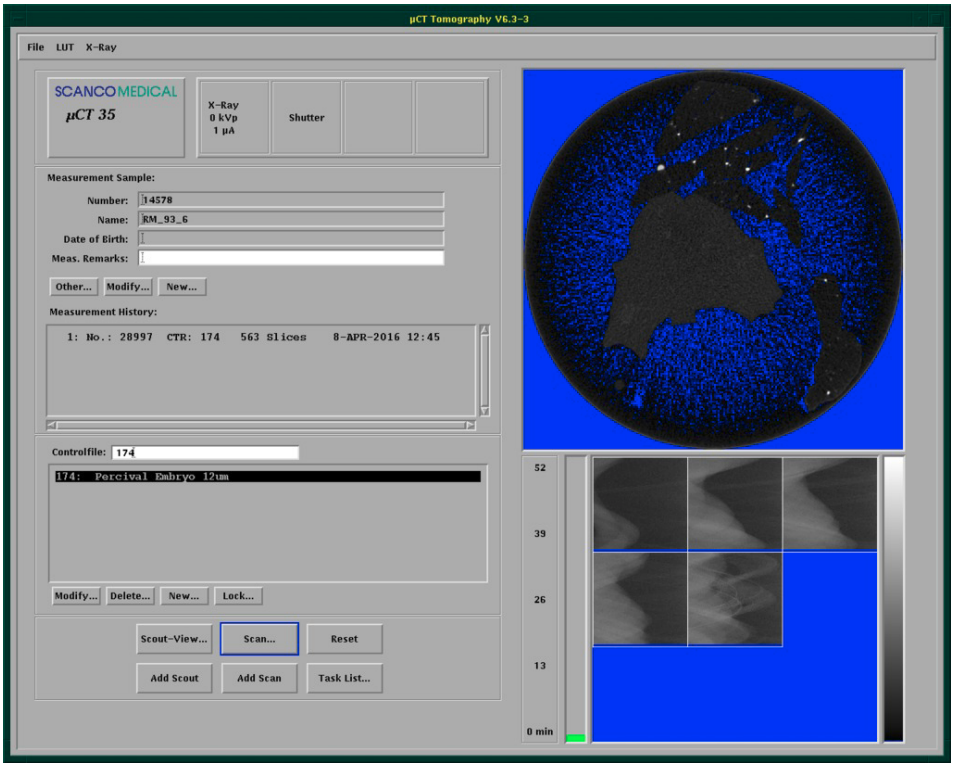
Photographs of IoT Failures

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

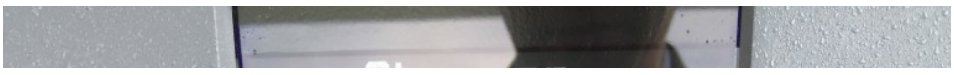


A smaller scale precursor to the Dyn DDoS attack, this printer at the University of Michigan was infected by network-based malware and began to generate denial of service attacks against other institutions.

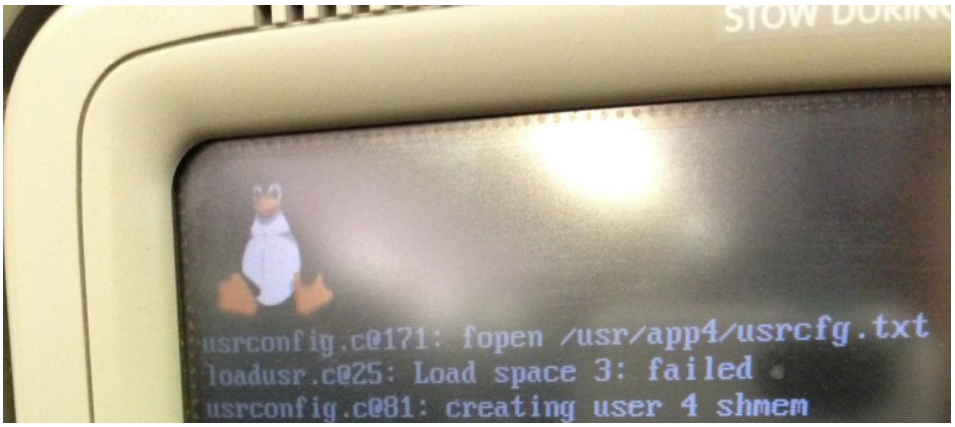
This water treatment facility in Michigan depends on insecure Windows XP for its water pump controls. In my photograph, you can see the Windows XP logo. Note that Windows XP ended security patch maintenance several years ago, and customers were advised of the expiration date before making purchases of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



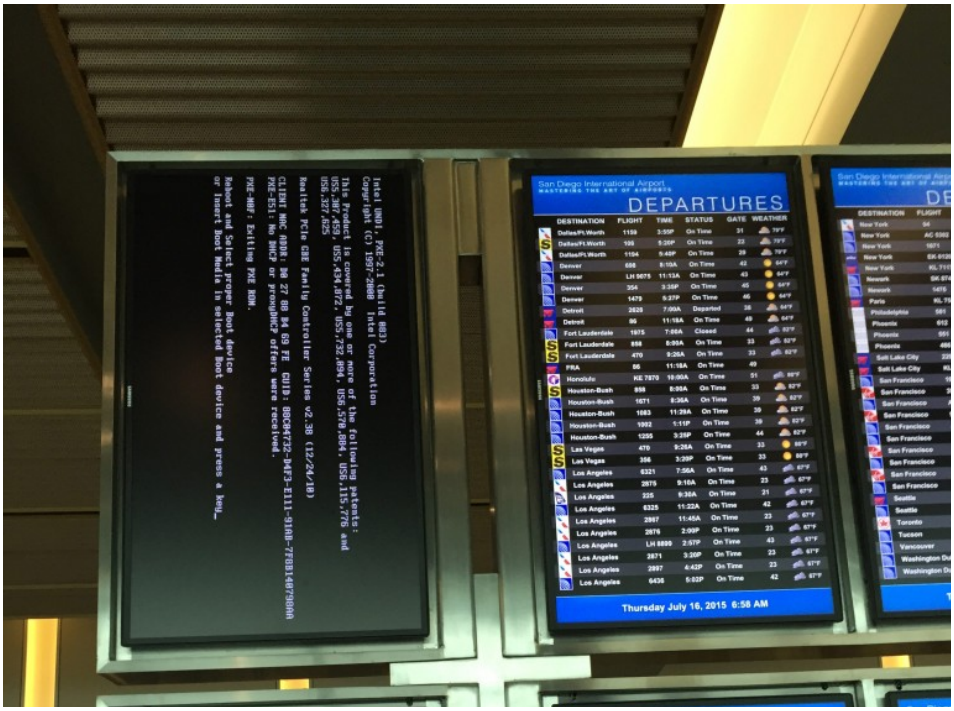
A researcher on Twitter claims to have discovered a tomography machine on the Internet by using the Shodan IoT vulnerability search engine. I have insufficient information to verify, however, but it is quite plausible. IoT medical devices can be both victims and sources of DDoS attacks.



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.

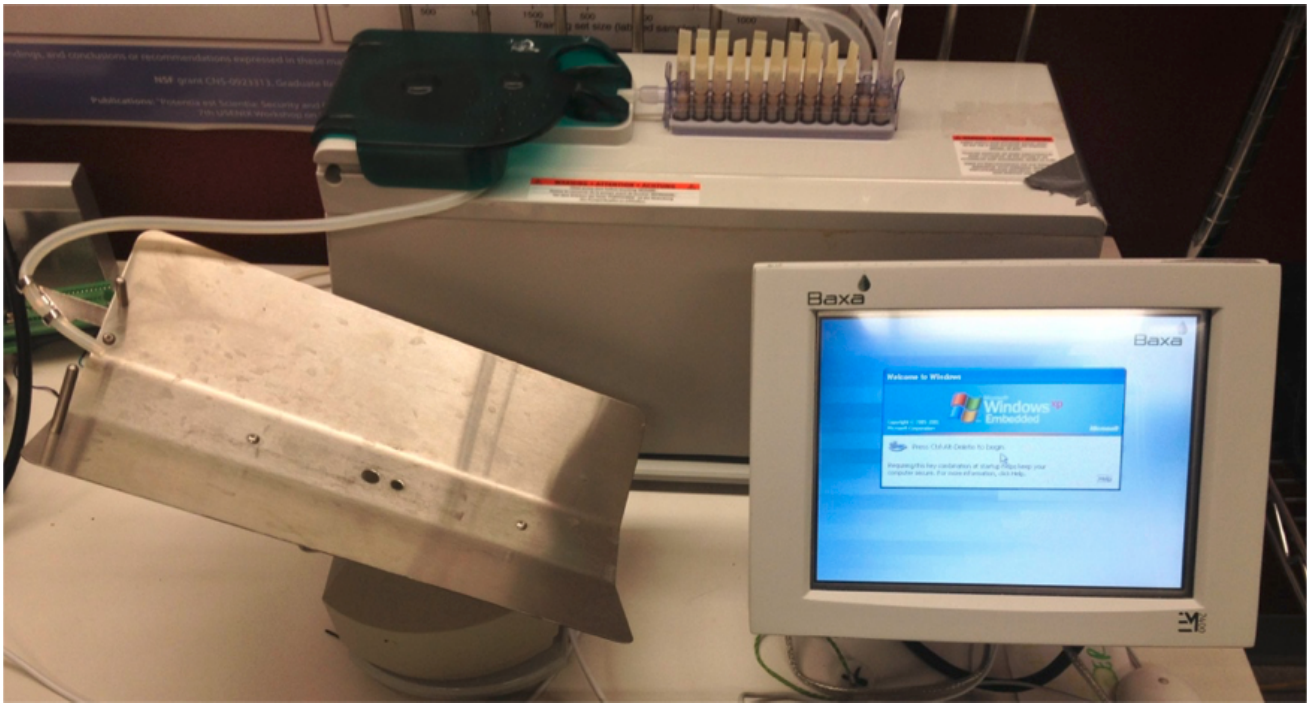


This airplane entertainment system running Linux crashed during my flight. While entertainment is not safety critical, imagine if flight control systems accidentally had a pathway to the entertainment software. Automobiles used to separate entertainment systems from engine control. However, a programmer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

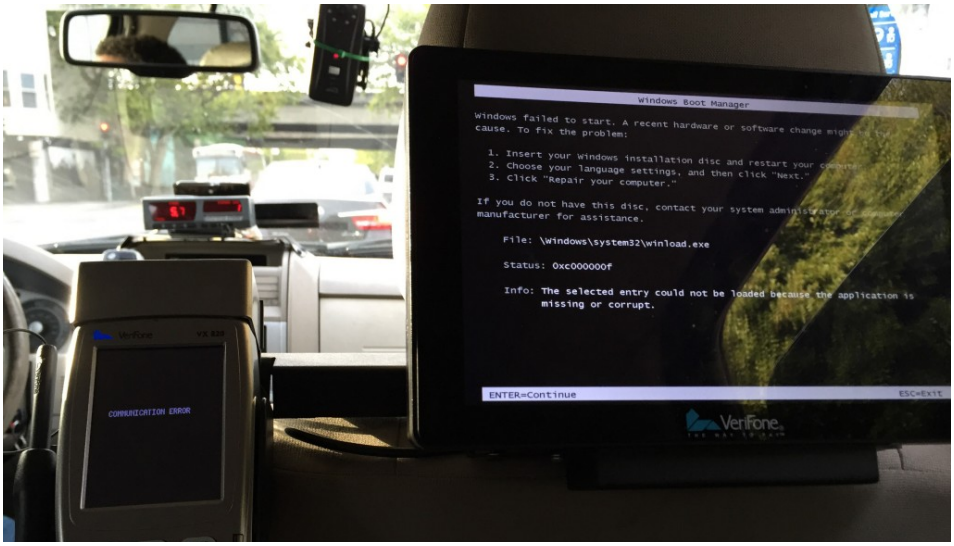


Crashed flight display consoles are a common occurrence in airports. Imagine if every smart TV in the world were simultaneously infected with a virus, sourcing a massive DDoS attack against a victim like Dyn.

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.



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. The FDA received a complaint that this model 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.



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

+2 0

GOVERNMENT IOT SECURITY

ALSO ON **UBIQUITY**

Are Google and Apple About to Pivot?

2 comments • 4 years ago

Avatar **coldsnout** — Talking about these two behemoths is an undertaking in itself! I was doing Software

The Future of Tech is Regulation

2 comments • 4 years ago

Avatar **Ted Lewis** — Gil, no question about it -- but, we don't know how Topsy.com computes "sentiment".