Vermont Right to Repair Task Force
November 19, 2018

Breaking Integrity

Testimony from Dr. Earl Crane, PhD, CISSP
Security Advisor for the Security Innovation Center

About Dr. Earl Crane

I am a cybersecurity executive and advisor to public and private sector organizations, helping them to manage their strategy, risk and cybersecurity programs. I have worked at early security startups, the White House National Security Council serving under President Obama, the financial sector and other Fortune 100s. I have been an adjunct professor at Carnegie Mellon since 2002 teaching cybersecurity to graduate students and executives, and I am a Cybersecurity Fellow at the University of Texas at Austin Strauss Center. I currently serve on the board of directors for ISC2, the global cybersecurity professional credentialing organization.

Cybersecurity Concerns in Repair

I want to share with you today, as someone whose entire professional career has been in the field of cybersecurity, that pushing insecure repair breaks the device integrity model and can make security worse for all of us.

Lessons learned from my experience in Homeland Security, The White House, the financial sector and enterprise cybersecurity all make me concerned how this legislation promotes insecure repair.

I am concerned because we have made significant progress in improving cybersecurity over the years, and that uninformed policy changes could unintentionally unwind the progress made that may lead us to a less secure ecosystem.

There are three main ways that insecure repair breaks integrity:

1. By removing accountability for security
2. By countering efforts to build security by design, from the ground up, including secure repair options
3. By not acknowledging importance of safety in a connected ecosystem

Trust

At the root of all security is trust. Trust is based on system integrity and assurances of accountability. Let's take these one at a time.

System Integrity

Integrity is one component of the security model triad of Confidentiality, Integrity and Availability. Integrity doesn’t get the same public attention as data breaches and system outages, but it is equally important and directly applicable to the conversation we are having here today.

Integrity is at the root of modern security. We call this the “trusted root” or a “trusted system”. By establishing an initial foundation of trust, we can then build a trust chain to extend trust to more things beyond the root.

The holy grail of any root of trust is physical access. It is always easier to manipulate something when you can get your hands on it.

If a device is physically manipulated and its trusted root is compromised, the extended chain of trust is shattered. Said another way, if we can't trust the device running our software, we can't trust any of the software running on our device, nor can we trust any other device connected to our now untrusted device. This becomes a problem when our friends, family and employers trust our devices with sensitive information.

We have all seen the alerts about a friend with a possible compromised account. The concern here arises when a user does not know their device is compromised and untrustworthy.

How important is integrity? In 2011 the Dutch Certificate Authority DigiNotar was compromised allegedly by Iranian hackers. DigiNotar held what is called a “root certificate” which was used to issue additional certificates, and was trusted by companies like Google, Yahoo, and others. Iranian hackers were able to use the compromised root certificate to spy on about 300,000 Iranian gmail users.

Why should we care? Because the compromised certificates affected all users globally, requiring everyone to update their browsers. The compromised certificate was also made public, possibly exposing others. As a result, the company DigiNotar filed for bankruptcy later that same year.

Repair without trust breaks the physical integrity of the device.

Accountability

Consumers have an expectation of privacy and security. They believe that technology products and services should perform as designed. Without accountability we have nothing to trust, and without trust we lose integrity. In the issue of repair, we are removing the manufacturer’s accountability because an unauthorized repair breaks the chain of trust. Without trust or accountability, we lose the integrity of our systems.

For repair to have security it must have accountability, and we must work together to build security into a more secure digital ecosystem. Any repair legislation without consideration for security and the preservation of trust is a risk and danger to the consumer.

Security by Design

The second thing I want to share with you today is the concept of “security by design” and how to enable a “secure repair”, where devices are built with security from the ground-up.

The cybersecurity industry has been working for years to improve security in our hardware and software systems. For example, at Homeland Security we sponsored the “Build Security In” program to help develop best practices and guidance to build security into every phase of software and hardware design. This has led to new efforts in security engineering by government, industry and academia.

Thankfully, industry has increasingly embraced secure development principles, leading to a safer and more secure cybersecurity ecosystem.

I am concerned that repair legislation uncoordinated with the security efforts of industry will be taking a step backwards.

Manufacturers make conscious decisions about what they release publicly, what they share with only partner networks, and what they keep confidential to their trusted partners. For example, many companies already publish their documentation and APIs publicly so organizations and individuals can build interfaces.

Forcing manufacturers to share complete code and schematics may push beyond what is appropriate for intellectual property protection. It may also result in the information sharing environment of partner networks to clamp down, inhibiting innovation, growth and the sharing of security information.

Today, authorized shops and dealers that provide repair have an obligation that a repair is performed to manufacturer standards, addressing safety and security issues. The safety issues may be obvious when dealing with cars and tractors, but safety issues also apply to the Internet of Things (IoT) and connected consumer electronics, as part of a broader need for privacy and security.

As we increase the power and pervasiveness of connected devices, an insecure repair can introduce new risks to the rest of our shared ecosystem. An insecure repair harms everyone else in the connected ecosystem -- which leads me to my third point.

A Secure Ecosystem

We live in a connected world. Our connected products are more powerful with increased speed, storage and bandwidth, and insecure devices may unknowingly impact our friends, family, community and coworkers.

According to Forbes, internet connected devices will continue to grow at a Compound Annual Growth Rate (CAGR) of 7.3% annually, with Industrial IoT projected to be $123B in sales by 2021. These are not small numbers, and IoT is increasingly becoming embedded as part of our lives.

As we continue to welcome more networked systems into our physical life, like locks, cameras, smoke detectors, safety alarms and more, we trust them in our home and with our lives.

We are discussing health, life, and safety issues here. Think of the security implications for connected fire alarms, smart cities applications, industrial IoT, and infrastructure management systems that ensure our drinking water is clean and our power grid is functional.

I bring this up because of the growing risk of IoT Botnets. When I was at the White House, the Botnet Working Group was stood up to try to address the challenge that people's personal devices may be infected with malicious software, called a "bot", that used their device to launch attacks on other computers. That problem was easier, because at least the home PC had an owner. The IoT botnet challenge has the potential to be much worse, because many of these devices are unmanaged. Recent botnet attacks, like Mirai from 2016 and Torii discovered in September of 2018 are recent examples.

IoT devices frequently do not have a single owner who can be held accountable for secure repair. A compromised device can no longer be trusted, and has the potential to affect other devices as well.

Just recently, the Department of Commerce's National Telecommunications and Information Administration, the NTIA, highlighted this issue in a report earlier this year, titled "Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats". In this report, some of the key challenges to botnet mitigation included that products need to be secured at all stages of the lifecycle, from shipment through to end-of-life.

This would include any repair to extend a products' life.

A product that has been insecurely repaired -- by mistake or by malice -- has the risk of being compromised and puts consumers at risk. Taking away the ability for manufacturers to protect their products, their customers and their brands erodes much of the IoT security work that has been done to mitigate future attacks.

Thank You

I thank you for your time and allowing me to provide my perspective on why insecure repair can break the integrity of our devices.

This is a complex issue with no easy solutions, but I would like to offer a few guiding points:

1. Continue to enable and empower those who want to get their devices repaired to do so in a secure manner
2. Provide the ability to perform secure repairs while protecting the intellectual property of the manufacturer
3. Provide consumers with choices to get repair, based on their level of informed risk acceptance and their need for accountability
4. Improve the overall level of security in connected devices, by shining a spotlight on security and enabling paths for secure repair

The model legislation that I have seen misses the mark on these critical security issues.

Given what I have learned over nearly two decades of cybersecurity practice, I am concerned that repair legislation uncoordinated with security could take us a step backwards. Additionally, a blanket repair legislative push without considering the risks and balancing their needs with cybersecurity and privacy risks runs counter to the current policy objectives here in Vermont, and in many other states, to increase people's privacy and reduce their cyber risk.

Security often loses as a trade-off against cost and ease-of-use. However, smart policy decisions made now can help prevent future risks that expose us to numerous vulnerabilities, wasting countless hours, dollars, and other potential harms.

It is precisely for this reason that I hope the task force will consider accountability, security by design, and building a secure ecosystem in their final report. Also, I caution the task force against endorsing a broad-based, one-size-fits all repair legislation that could break the integrity of our secure devices.

Again, thank you for your time.