10 At-Risk Emerging Technologies

featuring Bill Thomas reading a blog post by Christopher King

Bill Thomas: Welcome to the SEI Podcast Series, a production of the Carnegie Mellon University Software Engineering Institute. The SEI is a federally funded research and development center sponsored by the U.S. Department of Defense. A transcript of today's podcast is posted on the SEI website at sei.cmu.edu/podcasts.

My name is Bill Thomas. The text of this podcast originally appeared on the SEI Blog.

In today's podcast, we will highlight 10 At-Risk Emerging Technologies from a blog post by Christopher King. This post provides a snapshot of our current understanding of the risks involved with future technologies.

And now,

10 At Risk Emerging Technologies
By Christopher King
Vulnerability Analyst
CERT Division

> In today's increasingly interconnected world, the information security community must be prepared to address vulnerabilities that may arise from new technologies. Understanding trends in emerging technologies can help information security professionals, leaders of organizations, and others interested in information security identify areas for further study. Researchers in the SEI's CERT Division recently examined the security of a large swath of technology domains being developed in industry and maturing over the next five years. Our team of analysts—Dan Klinedinst, Todd Lewellen, Garret Wassermann, and myself—focused on identifying domains that not only impacted cybersecurity, but finance, personal health, and safety, as well. This blog post highlights the findings of our report prepared for the Department of Homeland Security United States Computer Emergency Readiness Team (US-CERT) and provides a snapshot of our current understanding of future technologies.

Methodology

Our work in this area began in 2013, just as Internet-of-Things (IoT) devices were beginning to gain attention. US-CERT and our team of researchers wanted to focus our efforts on getting ahead of the vulnerability discovery cycle. Our first report for US-CERT in 2014 provided a snapshot of the current understanding of future technologies. The report helped US-CERT make an informed decision about the best areas to focus resources for identifying new vulnerabilities, promoting good security practices, and increasing understanding of systemic vulnerability risk.

CERT researchers initially focused on technology domains that would likely have an impact on global information security. It is important to note that we did not consider domains that were already widely deployed (e.g., mobile computing, cloud computing, supervisory control and data acquisition [SCADA]), or domains that were simply not applicable.

For this newest report, we implemented an approach adapted from ISO 26262 and the SAE paper *Threat Analysis and Risk Assessment in Automotive Cyber Security*. Our new approach evaluated each technology domain based on the disruption that a cybersecurity event would have on the following four factors:

- safety - impact to human health or life
- privacy - amount of personally identifiable information that may be released
- finance - amount of losses for an individual or organization
- operation - impact on performance of the technology

10 At-Risk Emerging Technology Domains

As outlined in our technical report, *2016 Emerging Technology Domains Risk Survey*, we identified 10 emerging domains, including information such as expected timelines for major worldwide adoption, the impact on cybersecurity, supporting standards, and underlying technologies of these domains.

- **Augmented reality.** Augmented Reality (AR) uses technology to add context to a user's surrounding environment. Using real-time imagery and other sensor-provided input, an AR system aims to enhance or otherwise alter how people perceive physical reality. For example, some flight navigation systems overlay recommended flight paths and visual indicators for runways, buildings, and other hazards onto the aircraft's forward-facing video feed.

  Our team of researchers recommends further research of this domain in 2016 due to the growth of AR systems in military, medical and infrastructure applications.

One risk is that some AR technologies are relied upon as a primary source for mission-critical information. For example, a navigator using a navigation system may rely heavily upon the accuracy of the system's output to safely pilot a vehicle. Similarly, medical professionals must be able to trust the output of AR systems when using them to perform medical procedures.

- **Connected home.** The connected home involves automation of home devices, appliances, and computers that integrate with a centralized service for consumer use and control. The devices are diverse, from sensors (temperature, motion, movement, humidity) to controllers (smart thermostats, refrigerators, light bulbs) and are able to interact with the environment and each other. Online service such as If This Then That (IFTT) and ThingSpeak provide a common platform to trigger actions to environmental stimuli on certain devices.

  Our team of researchers recommends continuing to focus on improving the quality of home routers, the first line of defense for the IoT home. A risk of the connected home is that it is vulnerable to attacks because it relies on a single defense—the home router. For most consumers, the security of the home network depends on the router's default security. Many home routers deployed today have outdated firmware, insecure configurations, and aren't supported by the vendor.

- **Enterprise 3D printing (additive manufacturing).** 3D printing is an additive technique used to create three-dimensional objects by applying physical materials iteratively via an automated system. While there has been little evidence to suggest security problems with 3D printing, this situation may change as 3D printing evolves to use more complex and durable materials. Today, a variety of 3D printers are already available with rapid growth to 5.6 million units expected by 2019.

  Additive manufacturing is not an area of explicit security concern. These devices contain ethernet or Wi-Fi connectivity, a programmable logic controller, and various servomechanisms to control the heating units and distribution nozzles. While a security compromise could result in damage to the device or the surrounding area (due to heated material produced) these risks are not fundamentally different from those posed by existing industrial machinery.

- **Networked telematics.** Telematics encompasses all functions of the vehicle electronics that are designed to be accessible to users, including the dashboard, controls, and navigation system. Many vehicle manufacturers have recently added cellular connectivity to their vehicle to provide richer, more interactive services to the consumer. Developers of smartphone operating systems have also begun to integrate their products more closely with telematics systems.

  The upcoming mass deployment of this domain will increase the risk of new vulnerabilities, especially those of a systemic nature. The emerging smartphone-telematics integration technologies (e.g., Apple CarPlay, Google's Open Automotive Alliance, Blackberry QNX) are of particular concern. Telematics should therefore be considered a high-risk domain for systemic vulnerabilities. A telematics system is tightly integrated with other systems in a vehicle and provides a number of functions for the user. The recent additions of wireless connectivity such as Bluetooth, Wi-Fi, and LTE increase the risk of compromise. An Internet-connected vehicle is vulnerable to a wide range of attacks, both from determined attackers and traditional threats such as malicious code and phishing.

- **Smart medical devices.** These biomechanical machines interact with the human body in an inpatient or outpatient context. The medical industry has moved to more connected devices, in part, due to the benefits the data from such devices provide to hospital systems. Given the risk to human lives, our team recommends prioritizing this domain. The regulatory structure of this domain has shown that the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) and the FDA will be the primary champions of good security practices. In addition, the National Health Information Sharing and Analysis Center has begun developing best practices to improve the security of medical devices.

  As more devices are connected to hospital and clinical networks, patient data and information will be increasingly vulnerable. Even more concerning is the risk of remote compromise of a device directly connected to a patient. An attacker could theoretically increase or decrease dosages, send electrical signals to a patient, or disable vital sign monitoring.

- **Autonomous machines.** Smart robots or autonomous machines are independent, self-correcting, and learning machines. Unlike robots of the past few decades, modern *smart robots* are increasingly user-friendly and integrated with the human worker. These autonomous systems are used to automate warehouse retrieval and storage, automate some part of a human task, mix and dose drugs, and transport items from one area to another.

  Although autonomous machines are 5 to 10 years away from mainstream adoption, the devices could be compromised through networked back-end servers that provide some of the automation, or through the robot itself, which is networked and communicates across the Internet to the manufacturer for diagnostic information and software updates.

- **Smart sensors.** Smart sensors are one of the key technologies of ubiquitous computing (i.e., IoT). Sensor technologies provide information about or control of a physical environment in response to certain stimuli. Two major types of sensors are being deployed by manufacturers: non-actuated and actuated sensors. Non-actuated sensors send information about the environment to a processing engine. Examples of non-actuated sensors include temperature sensors, vibration sensors, and soil moisture sensors. Actuated sensors send information about the environment but also receive commands or react to the environment in a particular way, usually by flipping an electronic switch or through mechanical manipulation. Examples of actuated sensors include wirelessly controllable smart lights, switches, and door locks. Both non-actuated and actuated sensors use wireless technologies to communicate. (While this domain is similar to SCADA, it differs in that smart sensors use a greater number of standard network protocols and the

Internet to facilitate communication.)

Based on our analysis, our team of researchers recommends a continued focus on this domain in the year to come with particular emphasis on commercial applications. The smart sensor domain is likely to be successful. Sales of the Nestsmart thermostat, smart lights, smart electrical plugs, and intelligent smoke alarm products have increased. Yet, in 2014, researchers found that devices were also susceptible to attack.

- **Commercial unmanned aerial vehicles.** Colloquially known as drones, these vehicles are remotely operated and controlled by an operator with full control (via joystick) or semi-autonomously (via map waypoints, for example). UAVs were initially developed for military applications to provide warfighters with remote strike capability. In recent years however, the open source and commercial communities have developed UAVs for traffic monitoring, surveillance, agriculture, filming, and shipping.

  Based on our analysis, our team of researchers recommends conducting background research and outreach to the FAA and other standards bodies in 2016. There is a clear potential for risk as drones become ubiquitous. Some of these risks might include invasion of privacy (overflights with sophisticated cameras/microphones), physical damage/harm (drones carrying explosives or using itself as a projectile), or aviation interference, among others.

- **Vehicle autonomy (driverless cars).** Autonomous vehicles have the ability to move without direct commands from an operator. They can navigate to a destination using an autopilot-like capability, relying on onboard sensors, including GPS, cameras, lasers, and radar. The onboard sensors also enable autonomous vehicles to avoid potential obstacles.

  This domain is being actively researched and tested by every major automobile manufacturer and by major technology companies such as Google, Apple, and Uber. Building an understanding and analysis capability in this field will allow for better outreach to manufacturers and researchers in the community. Beyond safety concerns that are tied to basic flaws in implementation, there is the threat of active exploit. At Black Hat 2015, researchers demonstrated remote access and exploitation of a passenger vehicle.

- **Vehicular communication systems.** Vehicular communication systems combine wired and wireless technologies to enable intelligent transport systems for future cars, roads, and cities. Vehicular communication can be broken into two fields: vehicle-to-vehicle (V2V) communication and vehicle-to-infrastructure (V2I) communication. V2V provides vehicles with the ability to communicate their speed, position, and other status information to nearby vehicles. V2I allows for vehicles to receive and send information to smart roads, tollbooths, and other infrastructure components.

  Given the millions of vehicles expected to use this technology—and the potentially fatal consequences of failure—our team recommends that this domain be a high priority for further vulnerability analysis. For example, Department of Transportation (DoT) officials have suggested that this technology may be mandatory for new vehicles in 2017. DoT and the National Highway Traffic Safety Administration (NHTSA) have stated that in the initial rollout of the technology in vehicles and infrastructure, V2V and V2I will only communicate safety warnings to the driver, not control functionality.

While the DoT and NHTSA insist that vehicular communication systems have many safeguards to protect privacy and automobiles, the simple act of providing an open communication path to a vehicle introduces risk. Recent vehicular automotive vulnerability research has demonstrated that the introduction of a new technology into a vehicle can create behavior that the manufacturer did not intend.

Future Research

In addition to identifying at-risk emerging technologies, we also identified five of these domains that should be prioritized for further study based on a number of factors including the factors cited above: safety, privacy, finance, and operation.

These five domains are as follows:

- networked telematics
- smart medical devices
- autonomous machines
- autonomous vehicles
- commercial UAVs

While this research was developed for U.S. CERT, it also informs our own research agenda. Based on our previous emerging technologies report, CERT researchers recently focused on connected vehicles. (Read our white paper on this research, *On Board Diagnostics: Risks and Vulnerabilities of the Connected Vehicle.*)

We welcome your feedback on this research.

Bill: Thank you for joining us today. This blog post, 10 At-Risk Emerging Technologies, is available at insights.sei.cmu.edu. Click on the authors tab and find Christopher King's name.

Additional resources include the technical report on which the blog post featured in this blog post is based, 2016 Emerging Technology Domains Risk Survey.

Links to additional resources are provided in the transcript.

This podcast is available on the SEI website at

s e i dot

c m u dot

e d u, forward slash

podcasts.

and on Carnegie Mellon University's iTunesU site. As always, if you have any questions, please don't hesitate to email us at info@sei.cmu.edu. Thank you.