Software Engineering Institute
Carnegie Mellon University

2017 Emerging Technology Domains Risk Survey

Daniel Klinedinst
Joel Land
Kyle O'Meara

October 2017

TECHNICAL REPORT
CMU/SEI-2017-TR-008

CERT Division

http://www.sei.cmu.edu

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

This report was prepared for the SEI Administrative Agent AFLCMC/AZS 5 Eglin Street Hanscom AFB, MA 01731-2100

DM17-0275

Table of Contents

Executive Summary **iv**

Abstract **vi**

1 Introduction **1**
1.1 Report Format 1
1.2 Methodology 2

2 Blockchain **6**
2.1 Overview 6
2.2 Recommendation 6
2.3 Time Frame 6
2.4 Impact 6
2.5 Exploitation Examples 7

3 Intelligent Transportation Systems **8**
3.1 Introduction 8
3.2 Recommendation 8
3.3 Time Frame 8
3.4 Impact 8
3.5 Exploitation Examples 8

4 Internet of Things Mesh Networks **9**
4.1 Introduction 9
4.2 Recommendation 9
4.3 Time Frame 9
4.4 Impact 9
4.5 Exploitation Examples 9

5 Machine Learning **10**
5.1 Introduction 10
5.2 Recommendation 10
5.3 Time Frame 10
5.4 Impact 10
5.5 Exploitation Examples 10

6 Robotic Surgery **11**
6.1 Introduction 11
6.2 Recommendation 11
6.3 Time Frame 11
6.4 Impact 11
6.5 Exploitation Examples 11

7 Smart Buildings **12**
7.1 Introduction 12
7.2 Recommendation 12
7.3 Time Frame 12
7.4 Impact 12
7.5 Exploitation Examples 12

8 Smart Robots 13
8.1 Introduction 13
8.2 Recommendation 13
8.3 Time Frame 13
8.4 Impact 13
8.5 Exploitation Examples 13

9 Virtual Personal Assistants 14
9.1 Introduction 14
9.2 Recommendation 14
9.3 Time Frame 14
9.4 Impact 14
9.5 Exploitation Examples 14

10 Conclusion 15

References/Bibliography 16

List of Tables

Table 1:	New and Emerging Technologies	2
Table 2:	Security Impact of New and Emerging Technologies	4
Table 3:	Severity Classifications and Impact Scores	5

Executive Summary

> *The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it.*
>
> *—Mark Weiser [Weiser 1991]*

Mark Weiser first coined the term *ubiquitous computing*, describing it as "invisible, everywhere computing that does not live on a personal device of any sort, but is in the woodwork everywhere" [Weiser 1988]. With advancements in miniaturization and in the economies of scale for systems-on-a-chip, Weiser's vision is finally becoming a reality.

Weiser's vision of the future also included the difficult challenge of securing the near-infinite amounts of data generated, processed, and stored by ubiquitous devices (or in today's parlance, the "Internet of Things" [IoT]). This increasing prevalence of new devices—and the extent to which Americans have come to rely upon them in daily life—presents new challenges for the vulnerability coordination community. Can the Common Vulnerability Enumeration (CVE) methodology support this myriad of devices? Can the Common Vulnerability Scoring System (CVSS) provide effective and meaningful vulnerability information as increasingly complex and interrelated vulnerabilities surface?

The Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT) "strives for a safer, stronger Internet for all Americans by responding to major incidents, analyzing threats, and exchanging critical cybersecurity information with trusted partners around the world" [DHS 2017]. To carry out its mission, US-CERT must be proactive, focusing on future threats and vulnerabilities amid fear and uncertainty that often result from highly publicized cybersecurity attacks.

To support the US-CERT mission of proactivity, the CERT Coordination Center (CERT/CC) located at Carnegie Mellon University's Software Engineering Institute was tasked with studying emerging systemic vulnerabilities, defined as exposures or weaknesses in a system that arise due to complex or unexpected interactions between subcomponents. The CERT/CC researched the emerging technology trends through 2025 to assess the technology domains[1] that will become successful and transformative, as well as the potential cybersecurity impact of each domain. This report is intended to provide a brief background of each emerging technology domain along with a discussion of potential vulnerabilities and the risks of compromise or failure within each domain.

This report covers new or changed domains compared to the CERT/CC *2016 Emerging Technology Domains Risk Survey* [King 2016]. This list does not supersede previous reports. Many of the previously reviewed domains remain important. This report can be considered an addendum to that report.

[1] In this report, the term *domain* is used to describe a particular field of technology.

This report also identifies the domains that should be prioritized for further study based on a number of factors. Three domains must be considered high priority for outreach and analysis in 2017:

1. Intelligent Transportation Systems
2. Machine Learning
3. Smart Robots

This report does not imply that every domain requires detailed analysis. Each domain is nuanced. Some domains may require further study earlier in their technology development lifecycle than others. Approaches to improving security should be adjusted depending on the specific nature of each domain. In some cases, outreach is the best approach for improving the security of a technology; in other cases, technical vulnerability discovery may be the best way to provide better information to the government and public. This report includes a specific approach recommended by the CERT/CC for improving security in each domain.

Abstract

In today's increasingly interconnected world, the information security community must be prepared to address emerging vulnerabilities that may arise from new technology domains. Understanding trends and emerging technologies can help information security professionals, leaders of organizations, and others interested in information security to anticipate and prepare for such vulnerabilities. This report, originally prepared in 2015 for the Department of Homeland Security United States Computer Emergency Readiness Team (US-CERT), provides a snapshot in time of the current understanding of future technologies. This report also helps 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.

1 Introduction

As the world becomes increasingly interconnected through technology, information security vulnerabilities emerge from the deepening complexity. Unexpected interactions between hardware and software subcomponents can magnify the impact of a vulnerability. As technology continues its shift away from the PC-centric environment of the past to a cloud-based, perpetually connected world, it exposes sensitive systems and networks in ways that were never before imagined.

The information security community must be prepared to address emerging systemic vulnerabilities—exposures or weaknesses in a system that are introduced due to complex or unexpected interactions between subcomponents. To help identify these vulnerabilities, the CERT Coordination Center (CERT/CC) located at Carnegie Mellon University's Software Engineering Institute developed this report, which breaks down the major technology trends expected over the next 10 years. This report provides the background for further analysis work by the CERT/CC and aids the Department of Homeland Security (DHS) United States Computer Emergency Readiness Team (US-CERT) in its work towards vulnerability triage, outreach, and analysis.

The goal of this report is to provide a snapshot in time of the current understanding of future technologies. This report also enables US-CERT to make an informed decision about areas where it should focus resources to identify new vulnerabilities, promote good security practices, and increase understanding of systemic vulnerability risk.

1.1 Report Format

This report presents information on eight emerging domains and aims to provide the reader with

- an understanding of the major emerging technology domains
- the expected timeline for major worldwide adoption
- ways the domain may affect cybersecurity
- supporting standards and underlying technologies used by these domains
- likelihood of the domain becoming a success
- examples of exploitation in the domain or similar domains

The format of this report allows readers to quickly jump to a section and familiarize themselves with a domain. Each domain section contains the following subsections:

1. Introduction serves as a background on the application domain.
2. Recommendation includes the CERT/CC's recommendation for US-CERT on addressing this domain.
3. Time Frame addresses the time and likelihood in which broad adoption is likely.
4. Impact provides a discussion of the potential impact of security vulnerabilities in the domain.
5. Exploitation Examples details concepts or existing research demonstrating exploits of this domain.

1.2 Methodology

A measured approach to analysis is required when undertaking the difficult task of reviewing all new and emerging technology domains, their likelihood of success, and any potential vulnerabilities. The CERT/CC used Gartner's long-term assessment of emerging technologies as a filter to form the initial list of domains [Gartner 2014]. Gartner subscribers can access a list of "hype cycles" that describe each technology, its current maturity in the market, and when Gartner believes it will reach mainstream adoption in its industry [Fenn 2017]. This list tracks over 2,000 different technologies from inception to full adoption. From this list, the CERT/CC team identified domains likely to have an impact on global information security. Domains that were not included (e.g., mobile, cloud computing, and supervisory control and data acquisition [SCADA]) were either already widely deployed or simply not applicable.

For the 2017 report, the team triaged each identified domain according to the safety, privacy, financial, and operational impact that a cybersecurity incident could cause. The team used an approach adapted from ISO 26262 [ISO 2011] and the Society of Automotive Engineers paper *Threat Analysis and Risk Assessment in Automotive Cyber Security* [Ward 2013] (Table 2 and Table 3). If the impact score reached a total of four or higher on the SAE criteria in Table 2 (reflecting either serious risk in one or two domains, or low in all four) and was less than 5-10 years away from adoption, the domain was considered for inclusion in the report. Of those domains under consideration, the team decided which to include based on whether they had novel risks or security considerations. Some domains were renamed, combined, or modified with respect to the Gartner hype cycle lists. The team then assessed each chosen domain individually to determine its likelihood of success, potential impact if compromised, exploitation examples, and adoption timeline. In Table 1, domains in **bold** were included in this year's report. Those that are ~~crossed out~~ were reviewed in our *2016 Emerging Technology Domains Risk Survey* [King 2016].

Table 1: New and Emerging Technologies

Gartner's 2015 List of New Technology	CERT's List of Emerging Domains	Trust Boundary Breached?	Consumer, Enterprise, or Both?	Predicted Adoption Timeline
Smart Dust		Yes	Enterprise	10+
Virtual Personal Assistants	Virtual Personal Assistants	Yes	Both	5-10
Digital Security		Yes	Both	5-10
Quantum Computing		Yes	Enterprise	10+
Brain-Computer Interface		Yes	Both	10+
Human Augmentation		Yes	Both	10+
Volumetric Displays		No	Both	10+
Smart Robots	same	Yes	Both	5-10
Affective Computing		Yes	Consumer	5-10
~~**Connected Home**~~		Yes	Consumer	5-10
IoT Platform		Yes	Both	5-10
Biochips		No	Consumer	5-10
Software-Defined Security	Software-Defined Anything	Yes	Both	5-10

Gartner's 2015 List of New Technology	CERT's List of Emerging Domains	Trust Boundary Breached?	Consumer, Enterprise, or Both?	Predicted Adoption Timeline
Micro Data Centers		No	Both	5-10
Smart Advisors	Virtual Personal Assistants	No	Both	5-10
~~**Autonomous Vehicles**~~	Intelligent Transportation Systems	Yes	Both	5-10
Machine Learning	Machine Learning/Big Data	Yes	Both	2-5
Natural-Language Question Answering	Virtual Personal Assistants	Yes	Both	5-10
~~**Augmented Reality**~~		Yes	Both	5-10
~~**Autonomous Field Vehicles**~~	Intelligent Transportation Systems	Yes	Enterprise	2-5
Virtual Reality		Yes	Both	5-10
Gesture Control Devices		No	Both	2-5
Blockchain		No	Both	5-10
Cognitive Expert Advisors	Virtual Personal Assistants	No	Both	5-10
~~**Commercial UAVs**~~	Intelligent Transportation Systems	Yes	Enterprise	5-10
Context Brokering		Yes	Enterprise	5-10
Conversational User Interfaces	Virtual Personal Assistants	Yes	Enterprise	5-10
Data Broker PaaS		Yes	Enterprise	5-10
Enterprise Taxonomy and Ontology Management		No	Enterprise	10+
General Purpose Machine Intelligence		Yes	Enterprise	10+
Nanotube Electronics		No	Enterprise	5-10
Neuromorphic Hardware		No	Enterprise	10+
Personal Analytics		Yes	Both	5-10
Smart Data Discovery		Yes	Enterprise	5-10
Smart Workspace		No	Both	5-10
Software-Defined Anything (SDx)		Yes	Enterprise	2-5
Intelligent Transportation Systems		Yes	Both	2-5
Smart Buildings		Yes	Enterprise	5-10
Robotic Surgery		No	Enterprise	5-10
IoT Mesh Networks		Yes	Both	5-10

Table 2: Security Impact of New and Emerging Technologies

Gartner's 2015 List of New Technology	Safety (S0, S1, S2, S3, S4)	Privacy (S0, S1, S2, S3, S4)	Financial (S0, S1, S2, S3, S4)	Operational (S0, S1, S2, S3, S4)
Smart Dust	2	2	0	3
Virtual Personal Assistants	0	4	4	1
Digital Security	0	0	0	3
Quantum Computing	0	4	4	0
Brain-Computer Interface	2	2	0	0
Human Augmentation	4	2	0	1
Volumetric Displays	0	0	0	0
Smart Robots	4	3	1	4
Affective Computing	0	2	0	0
~~**Connected Home**~~	2	3	0	3
IoT Platform	2	3	0	3
Biochips	0	4	0	0
Software-Defined Security	0	1	1	1
Micro Data Centers	0	2	2	2
Smart Advisors	0	3	1	0
~~**Autonomous Vehicles**~~	4	2	0	3
Machine Learning	3	3	4	2
Natural-Language Question Answering	0	2	0	0
~~**Augmented Reality**~~	3	2	0	2
~~**Autonomous Field Vehicles**~~	4	0	0	3
Virtual Reality	1	2	0	0
Gesture Control Devices	0	0	0	0
Blockchain	0	4	4	3
Cognitive Expert Advisors	0	3	1	0
~~**Commercial UAVs**~~	4	0	0	4
Context Brokering	0	4	0	0
Conversational User Interfaces	0	2	2	0
Data Broker PaaS	0	4	0	0
Enterprise Taxonomy and Ontology Management	0	2	0	2
General Purpose Machine Intelligence	0	1	1	4
Nanotube Electronics	0	0	0	0
Neuromorphic Hardware	2	3	4	4
Personal Analytics	3	4	3	2
Smart Data Discovery	0	4	3	3

Gartner's 2015 List of New Technology	Safety (S0, S1, S2, S3, S4)	Privacy (S0, S1, S2, S3, S4)	Financial (S0, S1, S2, S3, S4)	Operational (S0, S1, S2, S3, S4)
Smart Workspace	0	2	0	3
Software-Defined Anything (SDx)	2	2	0	3
Intelligent Transportation Systems	4	4	1	3
Smart Buildings	4	3	1	5
Robotic Surgery	4	4	0	3
IoT Mesh Networks	2	3	0	3

Table 3: Severity Classifications and Impact Scores

Class	Safety-Related Severity	Class	Privacy-Related Severity
S0	No Injuries	**S0**	No unauthorized access to data
S1	Light or moderate injuries	**S1**	Anonymous data only
S2	Severe and life-threatening injuries (survival probable) *Light or moderate injuries for multiple people*	**S2**	Identification of person (personally identifiable information) or technology *Anonymous data for multiple people*
S3	Life threatening (survival uncertain) or fatal injuries *Severe injuries for multiple people*	**S3**	Tracking of individual or technology *Identification of multiple people or technologies*
S4	Life threatening or fatal injuries for multiple people	**S4**	Tracking of multiple people or technologies
Class	**Financial-Related Severity**	**Class**	**Operational-Related Severity**
S0	No financial loss	**S0**	No impact on operational performance
S1	Low-level loss (~$10)	**S1**	Impact not discernible to user
S2	Moderate loss (~$100) *Low losses for multiple people*	**S2**	User aware of performance degradation *Indiscernible impacts for multiple users*
S3	Heavy loss (~$1,000) *Moderate losses for multiple people*	**S3**	Significant impact on performance *Noticeable impact for multiple users*
S4	Heavy losses for multiple people	**S4**	Significant impact for multiple users

2 Blockchain

2.1 Overview

A blockchain is a highly distributed data structure that underlies such technologies as the Bitcoin digital currency. It can provide a high level of data integrity without the need for centralized management. This approach allows participants to securely perform transactions without an existing trust relationship. Blockchain technology is being investigated for its potential to decrease overhead costs in finance, real estate, insurance, contracts, intellectual property, and other transaction-based industries.

Blockchains are sometimes divided into permissionless and permissioned (or private) blockchains. The former allows anyone to participate; trust is assured by the underlying protocols and algorithms. The latter only allows approved users to participate, thus reinstating a centralized control. It is still uncertain whether a permissioned blockchain provides its owners with any advantages over existing ledger systems [Hampton 2016].

Blockchain technology has unique security challenges. Since it is a tool for securing data, any programming bugs or security vulnerabilities in the blockchain technology itself would undermine its usability. It also retains the risks of any digital information system; for example, the private keys used to access Bitcoin funds must be kept private.

2.2 Recommendation

The CERT/CC recommends performing background research and developing a list of companies for future research. This technology is still developing and has only one proven business model to date, which is Bitcoin itself. However, with the amount of research being done in multiple industries, it is likely that blockchain-related technologies will become more widespread in the near future.

2.3 Time Frame

Gartner considers blockchain as being 5-10 years away from mainstream adoption. CERT/CC believes mainstream adoption will happen toward the end of that range, when distributed, computable trust becomes crucial to autonomous systems and systems-of-systems.

2.4 Impact

The potential impact for security vulnerabilities in the blockchain ecosystem depends on the value of the information it is protecting. Since the primary use to date is for financial or finance-related transactions, the impact can be severe for companies whose business is based on the technology. As blockchain technology becomes embedded in transactions for physical property (real estate, manufacturing supply lines), ownership of property will be based on the security assumptions of the underlying blockchain.

Other suggested uses for blockchain technology take advantage of its distributed trust model to

prove the integrity of data without relying on a centralized or proprietary system-of-record. Some examples include health records, education transcripts, peer-to-peer commerce, and widely distributed Internet of Things systems [Asharaf 2017]. Trust in these records and transactions will only be as strong as the trust in the blockchain technology used to manage them.

2.5 Exploitation Examples

There have been numerous unauthorized transfers ("thefts") of Bitcoins already [BitcoinTalk 2014]. The largest of these was the collapse of the Mt. Gox Bitcoin exchange, in which 850,000 Bitcoins (with a current value of approximately $1.4 billion U.S. dollars) were lost and presumed stolen [Adelstein 2016].

3 Intelligent Transportation Systems

3.1 Introduction

The CERT 2016 Emerging Technology Domains Risk Survey identified several emerging domains related to connected and autonomous vehicles. While those domains are still highly relevant, they are increasingly commingling in what are called "Intelligent Transportation Systems" (ITS) [DOT 2017a]. Future ITSs will provide communications and data between connected and autonomous cars and trucks, road infrastructure, other types of vehicles, and even pedestrians and bicyclists.

The goal of these systems is not only to provide individual vehicles and users with information they need, but also to provide central authorities with the ability to better manage traffic at the macro level. For example, if an accident caused traffic delays, the autonomous cars could automatically be rerouted. Traffic lights on the alternate route could automatically have their timing changed to accommodate the influx of traffic. Additional buses or subway trains could be dispatched. These tasks will require a high degree of automation and internetworking.

3.2 Recommendation

The CERT/CC recommends continuing to do outreach as well as technical research in all areas of transportation security.

3.3 Time Frame

There are already pilot programs of ITS running in multiple U.S. cities, but they will not be widely deployed for 5–10 years. CERT/CC believes there will be a gradual adoption of ITS components. GPS and traffic apps already have a degree of "intelligence," but substantial policy, economic, and safety concerns will likely delay implementation of fully integrated systems for at least 10 years.

3.4 Impact

The impact of security compromises is similar to the impact for individual autonomous or connected vehicles, but on a larger scale. A miscommunication in the system, whether accidental or intentional, could lead to numerous traffic accidents, causing property damage, injury, and possibly death. Privacy is a concern due to the ability to track every vehicle's location in real time [DOT 2017b]. A compromise of a city-wide system could lead to a massive traffic jam or other major event.

3.5 Exploitation Examples

Although vulnerabilities have been demonstrated in individual components, from self-driving cars to traffic lights, CERT/CC is not aware of any exploitations of the systems currently being tested or deployed in public.

4 Internet of Things Mesh Networks

4.1 Introduction

A mesh network is a decentralized network topology where many or all of the networked devices double as nodes through which data may propagate. Mesh networks are not uniquely the providence of the Internet of things (IoT), but IoT stands to become a significant driver of their use as it continues to be commercially successful.

There are a few characteristics of IoT mesh networks that set them apart from general mesh networks: the devices or nodes typically have low power and bandwidth requirements, communicate wirelessly, and do not remain in fixed locations. A number of competing low power communications protocols that support wireless mesh networking have emerged to support these IoT characteristics, including ZigBee, Z-Wave, 6LowPAN, and Thread [Components 2015].

4.2 Recommendation

By interfacing with traditional network technologies to obtain Internet connectivity, IoT mesh networks will extend the perimeter both as access points and as additional targets for exploitation. As such, the CERT/CC recommends engagement with the standards bodies and device vendors towards establishing and reinforcing good security practices and awareness.

4.3 Time Frame

Due to the reliance upon market penetration of IoT as a whole, and further on the emergence and implementation of standard protocols, the CERT/CC expects IoT mesh networking to overlap with general IoT adoption. Estimates suggest that as many as 40 billion wireless connected IoT devices will be in use by 2020 [ABIResearch 2014].

4.4 Impact

IoT mesh networks generally carry similar risks as traditional wireless networking devices or access points (e.g., spoofing, man-in-the-middle attacks, and reconnaissance) in addition to risks based on device designs and their implementations of protocol-specific security features. A single compromised device may become a staging point for attacks on every other node in the mesh as well as on home or business networks that act as Internet gateways.

4.5 Exploitation Examples

ZigBee implementation flaws were abused to take control of smart light bulbs and unlock smart locks as discussed at Black Hat 2015 [Zillner 2015]. In an IoT hacking contest at DEF CON in 2016, 47 new vulnerabilities were identified across devices from 21 product vendors [Constantin 2016]. IoT devices have also been implicated in a number of distributed denial of service (DDoS) attacks [ENISA 2016].

5 Machine Learning

5.1 Introduction

Machine learning broadly refers to the processes by which a program can be trained on a body of data to make inferences about new or related information. Real-world applications of machine learning range from big data analytics and data mining to image processing, spam filtering, intrusion detection systems, and self-driving cars. Generally, machine learning enables the automation of inductive reasoning about data, including pattern recognition and anomaly detection tasks. Machine learning is a fundamental component of other emerging domains, and particularly of artificial intelligence.

5.2 Recommendation

As a component technology, machine learning does not easily fit into a general strategy of observation. The CERT/CC suggests monitoring individual emerging technologies on a case-by-case basis for characteristic uses of machine learning to identify the gravity of potential abuses. Characteristics of interest likely include big data applications dealing with sensitive information, security products whose efficacy depends on effective anomaly detection, and learning sensors that inform actions in physical reality (such as in self-driving vehicles).

5.3 Time Frame

While already in production in a number of contexts, Gartner considers machine learning to be within 2–5 years of mainstream adoption. The CERT/CC expects this to be one of the most aggressive and quickly adopted technology trends over the next several years.

5.4 Impact

The actual security impact of vulnerabilities in machine learning technologies will largely depend on specific implementations. Where sensitive information is aggregated, for example, there is the potential for theft or leakage. The ability of an adversary to introduce malicious or specially crafted data for use by a machine learning algorithm may lead to inaccurate conclusions or incorrect behavior. Fooling the sensors of a self-driving car may lead to accident, injury, or death [Harris 2015]. Theoretical attacks posit that an attacker with the ability to provide input may be able to manipulate the behavior of machine learning algorithms and, for instance, bypass spam filters or neutralize IDS protections [Barreno 2006].

5.5 Exploitation Examples

At the time of this publication, no in-the-wild exploits of machine learning technology are known to us. While misuse of information derived from machine learning systems may be likely, it is not in scope for this work. As noted above, theoretical attacks have been documented and may be used as a useful data point in monitoring decisions.

6 Robotic Surgery

6.1 Introduction

Robotic surgery in current practice typically refers to robot-assisted surgery in which a surgeon performs an operation via a computer console that controls a robotic arm, but may also refer to fully autonomous procedures. While the former is fairly well established, albeit with some growing pains—a recent 14-year study found that in-the-field results of 1.75 million procedures had non-negligible difficulties [Alemzadeh 2016]—full autonomy is still a nascent technology being honed on lab animals [Strickland 2016].

Robotic surgery has the demonstrated potential to facilitate the performance of complex procedures with greater precision and fewer complications than conventional techniques. According to numbers from Intuitive Surgical, over 3 million patients have been operated on using their da Vinci Surgery devices [da Vinci 2017].

6.2 Recommendation

The CERT/CC recommends researching existing and emerging robotic surgery technologies. Due to cost, individual product testing may be prohibitive, however reviewing independent studies and component datasheets may help to isolate areas to focus interest. The biggest area of concentration should be devices with networked communications, as these may be at risk for remote attacks.

6.3 Time Frame

Robotic-assisted surgery is already seeing limited use on human subjects for minimally invasive operations and is within 5–10 years of mainstream adoption. The CERT/CC does not expect to see autonomous robotic surgery on human subjects in this time frame.

6.4 Impact

The potential safety impact of security vulnerabilities in surgical robots is critical for the patient being operated on, but low in terms of numbers of people given the likelihood of chilling effects from a publicized security event. Where surgical robots are networked, attacks—even inadvertent ones—on these machines may lead to unavailability, which can have downstream effects on patient scheduling and the availability of hospital staff.

6.5 Exploitation Examples

University research in 2015 uncovered numerous vulnerabilities in surgical robots that could be exploited to create denial of service conditions or manipulate controls [Storm 2015]. The high occurrence of hospital network compromise—90 percent of healthcare organizations suffered a breach between 2014 and 2016 [Ponemon 2016]—combined with the increasing connectivity of medical devices has set the stage for the recent global WannaCry ransomware attack that broadly affected British National Health Service organizations [NHS 2017].

7 Smart Buildings

7.1 Introduction

The concept of smart buildings currently refers to using Internet of Things sensors and data analytics to make commercial buildings more efficient, comfortable, and safe. Typically this approach involves monitoring sensors to make real-time adjustments to lighting, HVAC, security, and maintenance parameters. For example, a conference room could start heating up when it knows it will be occupied soon; or it could cool down depending on the number of people in it. Sensors could report electrical or plumbing problems before they get bad enough to affect people in the building. Elevators could prioritize taking people up in the morning and down at the end of the day.

More smart building technologies might be introduced in the future. One such technology is reconfigurable interiors. The mixture of office space vs. meeting space could ebb and flow based on occupancy, or an event planner could specify the square footage desired for an event, and the building would rearrange interior walls to accommodate it [Gross 2012]. Another technology being touted is "self-awareness;" that is, the ability of a building to detect potential maintenance issues and take some sort of action to fix the issue without the need for human analysis [Gurgen 2013].

7.2 Recommendation

The CERT/CC recommends doing outreach as well as technical research in smart building technologies, particularly safety- and security- related technologies.

7.3 Time Frame

Gartner does not specifically discuss smart buildings, but the CERT/CC expects these technologies to spread rapidly in the next 2–5 years, especially in new construction.

7.4 Impact

The security risks of smart building technologies will vary according to the specific technologies. The highest risks will involve safety- and security- related technologies, such as fire suppression, alarms, cameras, and access control. Security compromises in other systems may lead to business disruption or nothing more than mild discomfort. There are privacy implications both for businesses and individuals.

7.5 Exploitation Examples

There have been published vulnerabilities in specific systems, such as cameras [Costin 2016]. The Mirai botnet used a large number of surveillance cameras and DVRs to attack other systems [Newman 2016]. As these system become more interconnected and ubiquitous, the CERT/CC expects to see more compromises.

8 Smart Robots

8.1 Introduction

Smart robots are autonomous machines that work alongside or in the place of human workers. As the machine learning and artificial intelligence domains come into prominence, smart robots will emerge that can learn from their environments, adapt, and make informed decisions, or 'behave like MacGyver' [Georgia 2012]. As capabilities continue to advance, it is reasonable to expect that we will find smart robots, humanoid or otherwise, affecting all facets of our lives.

8.2 Recommendation

As another broad domain of interest that includes everything from drones to industrial controls to robotic surgery, it is difficult to make general recommendations about smart robots as an emerging domain. The CERT/CC encourages vigilance and proactive engagement with industry, academia, and standards bodies.

8.3 Time Frame

Gartner considers smart robots to be 5–10 years from mainstream adoption. The CERT/CC expects to see commercial and industrial robots for specific purposes in 2–5 years, with more general purpose smart robots emerging in 5–10 years.

8.4 Impact

There are many components in the smart robot ecosystem, not limited to hardware, operating system, and interconnectivity with other networked devices. Well-known classes of software and network vulnerabilities are likely to be discovered. It is not difficult to imagine the financial, operational, and safety impact of shutting down or modifying the behavior of manufacturing robots, delivery drones; service-oriented or military humanoid robots; industrial controllers; or, as previously discussed, robotic surgeons.

8.5 Exploitation Examples

There is active research on the security of existing robot products that has resulted in the discovery of numerous specific vulnerabilities [Cerrudo 2017]. Examples of the potential impact of exploitation can be seen in tangential or overlapping domains, including robotic surgery, IoT, autonomous vehicles, and others.

9 Virtual Personal Assistants

9.1 Introduction

A virtual personal assistant (VPA) is a data-crunching application that mimics the skills and functions of a human assistant. By seamlessly applying machine learning analytics to constantly evolving user data, VPAs are uniquely positioned to streamline and improve task management and performance. As VPA technology and the intrinsically related domains of machine learning and artificial intelligence continue to mature, its functionality will continue to expand, shaping how users interact with their Internet-connected ecosystems.

9.2 Recommendation

The CERT/CC recommends obtaining and maintaining awareness of the presence and data curation practices of emerging and established VPAs, such as Apple's Siri, Google Now, Amazon's Alexa, and Microsoft's Cortana.

9.3 Time Frame

Gartner considers VPAs as being 5–10 years away from mainstream adoption. The CERT/CC believes adoption will be sooner than that since most of the necessary technologies already exist and are being integrated in current and near-term products.

9.4 Impact

The efficacy of VPAs is almost wholly dependent on access to data, making privacy the chief concern from a security perspective. VPAs will potentially access users' social network accounts, messaging and phone apps, bank accounts, and even homes. In business settings, they may have access to knowledge bases and a great deal of corporate data.

9.5 Exploitation Examples

There are many articles addressing privacy concerns since VPAs will have access to large amounts of data, but how consumers' information will be shared with outside firms has yet to be fully defined [Economist 2015]. The other privacy concern is the trail of information a user could leave with having everything accessed and shared by a VPA [Waddell 2016].

10 Conclusion

In preparing this report, the CERT/CC analyzed emerging technologies that are expected to become mature before 2025. This analysis resulted in a list of 8 technology domains of cybersecurity interest. For each domain, the team developed a brief background, recommendations for research, an expected time frame of adoption, impacts of vulnerabilities, likelihood of success, and exploitation examples.

This report provides an understanding of cybersecurity issues that may result as part of each domain's adoption in the future. It also identifies the domains that should be prioritized for further study based on a number of factors. The three domains that CERT/CC considers high-priority for outreach and analysis in 2017 are:

1. Intelligent Transportation Systems
2. Machine Learning
3. Smart Robots

These three domains are being actively deployed and have the potential to have widespread impacts on society. Intelligent Transportation Systems affect one of the fundamental components of a society: transportation, which nearly every person in a technological society depends on. Societies and their economies rely on cars, buses, mass transit, boats, and planes to function. They also have a large potential safety impact since ITSs will eventually control many large vehicles that move very fast.

ITS is dependent on the other two high-priority domains, Machine Learning and Smart Robots since autonomous vehicles are themselves a type of smart robot. However, the impact of these latter two domains goes beyond transportation. Machine Learning will be applied to finance, public policy, engineering, and military purposes. Smart Robots will be used in construction, logistics, manufacturing, and many other industries. Machine Learning and Smart Robots are also heavily dependent on each other.

The other domains are less widely applicable, at least in the near future. They may appeal only to early adopters (Blockchain, Virtual Personal Assistants) or be specific to one industry (Smart Buildings, Robotic Surgery.) The CERT/CC does not expect them to be adopted as widely in the next 12–18 months.

References/Bibliography

URLs are valid as of the publication date of this document.

[ABIResearch 2014]
ABIResearch. The Internet of Things Will Drive Wireless Connected Devices to 40.9 Billion in 2020. *ABIResearch Website*. August 20, 2014. https://www.abiresearch.com/press/the-internet-of-things-will-drive-wireless-connect/

[Adelstein 2016]
Adelstein, Jake; & Stucky, Nathalie-Kyoko. Behind the Biggest Bitcoin Heist in History: Inside the Implosion of My. Gox. *The Daily Beast Website.* May 19, 2016. http://www.thedailybeast.com/articles/2016/05/19/behind-the-biggest-bitcoin-heist-in-history-inside-the-implosion-of-mt-gox

[Alemzadeh 2016]
Alemzadeh, Homa; Raman, Jaishankar; Leveson, Nancy; Kalbarczyk, Zbigniew; & Iyer, Ravishankar. Adverse Events in Robotic Surgery: A Retrospective Study of 14 Years of FDA Data. *National Center for Biotechnology Information—PLoS One Website.* April 20, 2016. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4838256/

[Asharaf 2017]
Asharaf, S. & Adarsh, S. Decentralized Computing Using Blockchain Technologies and Smart Contracts: Emerging Research and Opportunities. Information Science Reference, Hershey, PA. 2017.

[Barreno 2006]
Barreno, Marco; Nelson, Blaine; Sears, Russell; Joseph, Anthony D.; & Tygar, J.D. Can machine learning be secure? Pages 16-25. In *Proceedings of the 2006 ACM Symposium on Information, computer and communications security* (ASIACCS). New York, NY, USA. 2006

[Bigelow 2015]
Bigelow, Pete. Combine a self-driving car with V2V, and here's what happens. *Autoblog Website*. December 12, 2015. http://www.autoblog.com/2015/12/12/autonomous-car-delphi-v2v-vehicle-ces/

[BitcoinTalk 2014]
Dree12 [user ID] List of Bitcoin Heists. *Bitcoin Talk Forum*. November 16, 2014. https://bitcointalk.org/index.php?topic=576337

[Cerrudo 2017]
Cerrudo, Cesar & Apa, Lucas. Hacking Robots Before Skynet. *IOActive Website.* 2017. https://ioactive.com/pdfs/Hacking-Robots-Before-Skynet.pdf

[Components 2015]
RS Components. 11 Internet of Things (IoT) Protocols You Need to Know About. *Designspark Website.* April 20, 2015. https://www.rs-online.com/designspark/eleven-internet-of-things-iot-protocols-you-need-to-know-about

[Constantin 2016]
Constantin, Lucian. Hackers found 47 new vulnerabilities in 23 IoT devices at DEF CON. *CSO Website.* September 13, 2016. http://www.csoonline.com/article/3119765/security/hackers-found-47-new-vulnerabilities-in-23-iot-devices-at-def-con.html

[Costin 2016]
Costin, A. Security of CCTV and Video Surveillance Systems: Threats, Vulnerabilities, Attacks, and Mitigations. Pages 45-54. *Proceedings of the 6th International Workshop on Trustworthy Embedded Devices* (TrustED '16). ACM, New York, NY, USA. 2016

[da Vinci 2017]
Minimally Invasive Surgery. *da Vinci Surgery Website.* 2017. http://www.davincisurgery.com/

[DHS 2017]
U.S. Department of Homeland Security. *US-CERT Website.* 2017. https://www.us-cert.gov

[DOT 2017a]
U.S. Department of Transportation. *Intelligent Transportation Systems Joint Program Office Website.* 2017. https://www.its.dot.gov/research_archive.htm

[DOT 2017b]
U.S. Department of Transportation. Connected Vehicles and Your Privacy. https://www.its.dot.gov/factsheets/pdf/Privacy_factsheet.pdf

[Economist 2015]
The Economist. The software secretaries. *The Economist Website.* September 12, 2015. http://www.economist.com/news/business-and-finance/21664071-technology-firms-are-competing-become-consumers-personal-secretaries-big-implications

[ENISA 2016]
European Union Agency for Network and Information Security (ENISA). Major DDoS Attacks Involving IoT Devices. *ENISA Website.* November 3, 2016. https://www.enisa.europa.eu/publications/info-notes/major-ddos-attacks-involving-iot-devices

[Fenn 2017]
Fenn, Jackie; Raskino, Mark; & Burton, Betsy. Understanding Gartner's Hype Cycles. *Gartner, Inc. Website.* January 4, 2017. https://www.gartner.com/doc/2538815/understanding-gartners-hype-cycles

[Gartner 2014]
Gartner's 2015 Hype Cycle for Emerging Technologies Identifies the Computing Innovations That Organizations Should Monitor. *Gartner, Inc. Website.* October 8, 2014. http://www.gartner.com/newsroom/id/3114217

[Georgia 2012]
Robots Using Tools: With New Grant, Researchers Aim to Create 'MacGyver' Robot. *Georgia Institute of Technology Website.* October 9, 2012. http://www.news.gatech.edu/2012/10/09/robots-using-tools-new-grant-researchers-aim-create-'macgyver'-robot

[Gross 2012]
Gross, Mark D. & Green, Keith Evan. Architectural Robots, Inevitably. *Interactions*. Issue 19. Number 1. January 2012.

[Gurgen 2013]
Gurgen, L.; Gunalp, O.; Benazzouz, Y.; & Gallissot, M. Self-aware cyber-physical systems and applications in smart buildings and cities. Pages 1149-1154. *2013 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Grenoble, France. 2013,

[Hampton 2016]
Hampton, Nikolai. Understanding the blockchain hype: Why much of it is nothing more than snake oil and spin. Computerworld Website. September 5, 2016. https://www.computerworld.com.au/article/606253/understanding-blockchain-hype-why-much-it-nothing-more-than-snake-oil-spin/ (

[Harris 2015]
Harris, Mark. Researcher Hacks Self-driving Car Sensors. *IEEE Spectrum Website.* September 4, 2015. http://spectrum.ieee.org/cars-that-think/transportation/self-driving/researcher-hacks-selfdriving-car-sensors

[ISO 2011]
International Organization for Standardization. *ISO 26262-1:2011: Road vehicles—Functional safety—Part 1: Vocabulary.* https://www.iso.org/standard/43464.html

[King 2016]
King, Christopher; Klinedinst, Dan; Lewellen, Todd; & Wassermann, Garret. *2016 Emerging Technology Domains Risk Survey.* Software Engineering Institute, Carnegie Mellon University. 2016. http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=453809

[Newman 2016]
Newman, Lily Hay. The Botnet That Broke The Internet Isn't Going Away. *Wired Website.* December 9, 2016. https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-away/

[NHS 2017]
Statement on reported NHS cyber attack. *NHS Digital Website.* May 2017. https://digital.nhs.uk/article/1491/Statement-on-reported-NHS-cyber-attack

[Panetta 2016]
Panetta, Kasey. Gartner's Top 10 Strategic Technology Trends for 2017. *Gartner, Inc. Website.* October 18, 2016. http://www.gartner.com/smarterwithgartner/gartners-top-10-technology-trends-2017/

[Ponemon 2016]
Ponemon, Larry. Nearly 90 Percent of Healthcare Organizations Suffer Data Breaches, New Ponemon Study Shows. *Ponemon Institute Website.* May 12, 2016. http://www.ponemon.org/blog/sixth-annual-benchmark-study-on-privacy-security-of-healthcare-data

[Press 2014]
Press, Gil. Internet of Things By The Numbers: Market Estimates And Forecasts. *Forbes Website*. August 22, 2014. http://www.forbes.com/sites/gilpress/2014/08/22/internet-of-things-by-the-numbers-market- estimates-and-forecasts/

[Storm 2015]
Storm, Darlene. Researchers hijack teleoperated surgical robot: Remote surgery hacking threats. *Computerworld Website.* April 27, 2015. http://www.computerworld.com/article/2914741/cybercrime-hacking/researchers-hijack-teleoperated-surgical-robot-remote-surgery-hacking-threats.html

[Strickland 2016]
Strickland, Eliza. Autonomous Robot Surgeon Bests Humans in World First. IEEE Spectrum Website. May 4, 2016. http://spectrum.ieee.org/the-human-os/robotics/medical-robots/autonomous-robot-surgeon-bests-human-surgeons-in-world-first

[Waddell 2016]
Waddell, Kaveh. The Privacy Problem with Digital Assistants. *The Atlantic Website.* May 4, 2016. https://www.theatlantic.com/technology/archive/2016/05/the-privacy-problem-with-digital-assistants/483950/

[Ward 2013]
Ward, David; Ibarra, Ireri; & Ruddle, Alastair. Threat Analysis and Risk Assessment in Automotive Cyber Security. *SAE International Journal of Passenger Cars – Electronic and Electrical Systems.* Volume 122. Issue 7. Pages 507-513. 2013. https://doi.org/10.4271/2013-01-1415

[Weiser 1988]
Weiser, Mark. Ubiquitous Computing. http://www.ubiq.com/hypertext/weiser/UbiHome.html

[Weiser 1991]
Weiser, Mark. The Computer for the 21st Century. *Scientific American Special Issue on Communications, Computers, and Networks.* September, 1991

[Zillner 2015]

Zillner, Tobias. Zigbee Exploited: The good, the bad and the ugly. *Cognosec.* August 6, 2015. https://www.blackhat.com/docs/us-15/materials/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly-wp.pdf

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	September 2017	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
2017 Emerging Technology Domains Risk Survey	FA8721-05-C-0003

6. AUTHOR(S)

Daniel Klinedinst, Joel Land, and Kyle O'Meara

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2017-TR-008

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFLCMC/PZE/Hanscom Enterprise Acquisition Division 20 Schilling Circle Building 1305 Hanscom AFB, MA 01731-2116	n/a

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

In today's increasingly interconnected world, the information security community must be prepared to address emerging vulnerabilities that may arise from new technology domains. Understanding trends and emerging technologies can help information security professionals, leaders of organizations, and others interested in information security to anticipate and prepare for such vulnerabilities. This report, originally prepared in 2015 for the Department of Homeland Security United States Computer Emergency Readiness Team (US-CERT), provides a snapshot in time of the current understanding of future technologies. This report also helps 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.

14. SUBJECT TERMS	15. NUMBER OF PAGES
cybersecurity, emerging technologies	28

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. Z39-18
298-102