Security and Privacy Issues in Contemporary Consumer Electronics

By Dalton A. Hahn, Arslan Munir, and Saraju P. Mohanty

The technological advancements in consumer electronics (CE) in a variety of domains offer consumers with new systems aimed at providing assistance, efficiency, comfort, connectivity, entertainment, and safety. Although CE provides new capabilities, services, and conveniences to consumers, it also brings new challenges. In particular, security and privacy issues emerging from CE systems are critical. This article provide an overview of prevalent CE domains and provide a classification of security and privacy issues within these realms. Furthermore, the challenges in addressing security and privacy issues in CE and potential mitigation techniques are presented.

I. Introduction

The CE products, while offering various enchanting features and providing a range of new benefits and entertainment opportunities, have also raised new privacy and security concerns. From the collection of sensitive patient data in medical devices, to location privacy concerns in personal devices, the world of CE faces many challenges that need to be addressed.

The CE products are potential sources of many security and privacy vulnerabilities. Many of these CE products have wireless interfaces which increases their susceptibility to security and privacy attacks. Recently, many of these CE products are part of Internet of things (IoT) because of the products' ability to connect to the Internet and making various physical components smart [1]. The Internet connectivity further exacerbates the security and privacy challenges of these CE products and provides new ways for malicious actors to breach privacy and security. In late 2016 and early 2017, for example, the Mirai botnet infected and controlled more than 200,000 IoT and embedded devices [2].

Holistic discussions of security and privacy issues in CE are lacking in literature. This paper aims to fill this gap and presents an overview of contemporary CE from security and privacy perspective. We then provide a classification of security and privacy issues in CE devices. Furthermore, we discuss challenges in addressing security and privacy issues, and contemplate potential solutions to mitigate security and privacy issues in CE.

II. Security and Privacy Perspective of Contemporary Consumer Electronics

CE is a growing field with a range of applications and devices as depicted in Figure 1. This overview by no means is a comprehensive coverage of all CE products.

Medical Consumer Electronics: The medical CE, including pacemakers, heart-rate monitors, insulin pumps, are often connected to the Internet for firmware and software updates. This ability to provide online updates allows for greater flexibility and longevity of the devices and permits fewer invasive surgeries and procedures for the patients. However, the Internet connectivity of medical CE also opens new entry points for attackers and new vulnerabilities that can have grave consequences for the consumers of these devices.

Home Consumer Electronics: Home CE products, such as Amazon Alexa, Google Home, smart thermostats, and coffee makers, are becoming more and more ubiquitous in homes around the world. Often paired with a smartphone application or a personal assistant device, home CE are easily controlled and configured. However, with these benefits of remote controllability and configurability, these devices also introduce new ways for malicious actors to breach our privacy and security.

Personal Consumer Electronics: Personal CE products (e.g., smartphones, portable music players, tablets, and laptops) are the most ubiquitous amongst CE categories. Along with smartphones and mobile computers, personal CE products include devices that connect to smart phones and mobile computers, like headset.

Wearable Consumer Electronics: Wearable devices have emerged into the CE market in a variety of ways, such as smart watches, smart clothing, activity trackers and pedometers. Wearable CE also introduce security and privacy issues as these products expose consumer personal information to risk.

Business Consumer Electronics: From point-of-sale (POS) terminals to information kiosks and automated teller machines (ATMs), CE products are being incorporated into the business and financial world. New methods of payment such as cryptocurrency or smart payments

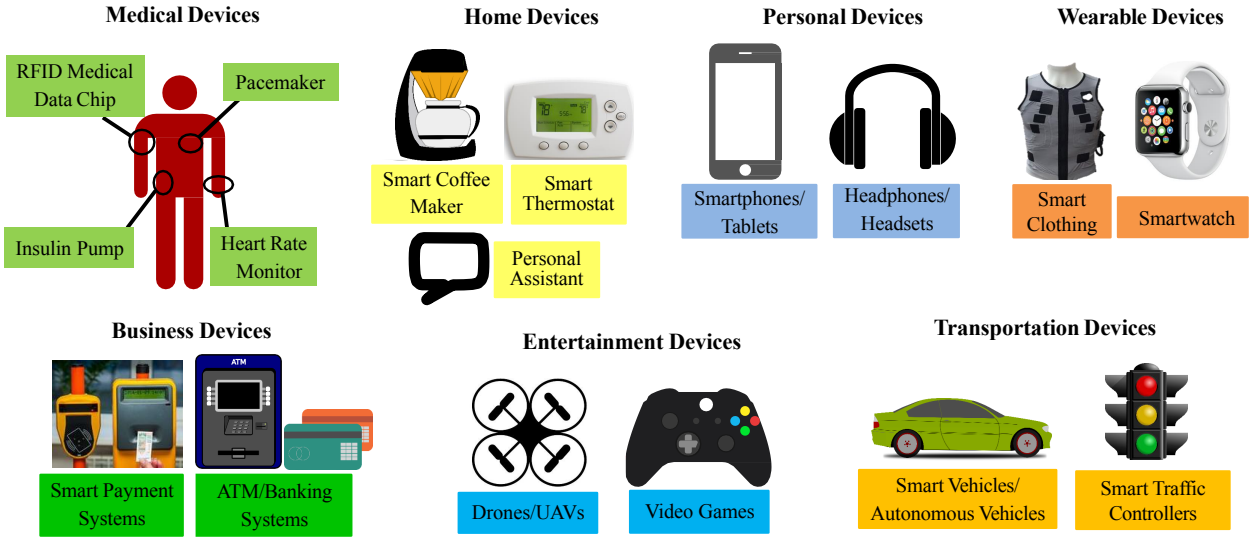

Fig. 1: A selection of consumer electronic systems classified according to their relationship with consumers.

through smartphones present additional security and privacy challenges for these CE products.

Entertainment Consumer Electronics: Entertainment-focused CE products, such as video games, virtual reality systems, or unmanned aerial vehicles (UAVs) are becoming increasingly popular. For example, UAVs have a range of consumer applications including multimedia (e.g., enabling users to capture moments and scenes not possible with traditional means) and business applications for package deliveries. However, UAVs present additional challenges as the UAVs can be used to infringe on the privacy of other individuals.

Transportation Consumer Electronics: The CE products relevant to transportation industry include UAVs and a variety of transportation electronics including, navigation system, in-car entertainment systems, and parking assistance system. The CE products, including smartphones, portable music players, and Bluetooth devices, are connected to vehicles, which while providing various benefits also creates security and privacy vulnerabilities.

III. Classification of Security and Privacy Issues

A. Security Issues in Consumer Electronics

A classification of security issues of CE has been discussed in terms of standard security dimensions such as confidentiality, integrity, availability, authentication and identification, and non-repudiation.

Confidentiality: Confidential communication between CE devices is vital to ensuring the security and privacy of consumers. In the UAV example, confidential communication between a UAV and the hand-held receiver of the UAV operator is crucial for proper control of the device [3]. Table I highlights attacks such as the man-in-the-middle (MITM) attack, where an adversary is positioned between the sender and the receiver of the communication. In the absence of confidentiality during the control interaction, an adversary listening on the proper channel could eavesdrop on the communication between the operator and the UAV [3].

Integrity: Common attacks on the integrity of a system, such as the MITM attack described earlier and the Sybil attack (the attack where an attacker creates a large number of pseudonymous identities to subvert the reputation system [4]), can create dangerous situations where a CE device may not react correctly or may take fallacious decisions/actions based on the incorrect or malicious data.

Availability: The availability for CE products is important for not only to communicate with one another and provide enjoyable experiences for users but also for consumer safety. For example, the availability of medical CE products is paramount for patients as these products' unavailability can create life-threatening situations.

Authentication and Identification: Authentication and identification of consumers as well as CE products are important for a variety of applications. For medical CE products, authentication and identification provide a framework for physicians and medical professionals to securely access the information and provide control commands to these devices.

Non-Repudiation: Non-repudiation provides the ability to prove that a party is responsible for an action observed, without deniability. Non-repudiation enables to unambiguously trace a message back to its originator, which can be useful for forensics and legal matters. For

TABLE I: **Case Study of UAV Security Issues**

Attack Example	Security Dimension	Attack Type
Denial of Service	Availability	Active
Sybil Attack	Integrity, Availability	Active
Man-in-the-Middle	Confidentiality, Integrity Availability, Authentication	Active/Passive
Spoofing	Integrity, Availability Authentication	Active
Eavesdropping	Confidentiality	Passive
Data Poisoning	Integrity, Availability	Active
Replay Attack	Integrity, Authentication	Active

example, if a UAV is observed in a "no-fly" zone, or is seen potentially spying on someone, non-repudiation would prevent the ability for the individual responsible for those actions to deny his/her actions. However, despite the security benefits of non-repudiation, its tradeoff with privacy presents an interesting challenge.

B. Privacy Issues in Consumer Electronics

The CE devices store a plethora of personal information of consumers and thus are a potential source of privacy violations and vulnerabilities. This section classifies privacy issues in CE such as identity privacy, information privacy, location privacy, and usage privacy.

Identity Privacy: Identity privacy in context of CE provides the basis of protecting consumers' identity when they interact with CE products. Many CE devices require an account to be created in order to access the services provided by the device. By registering an account, the identity of the owner is linked to the device. Research in autonomous vehicles, shown in Figure 1, has recently explored using *pseudonyms* (fictitious names) in order to mask the identity of individuals within ITS [5]. However, even this strategy of utilizing pseudonyms and changing them various times has been shown to be ineffective in preserving identity privacy within ITS as well as other CE [6]. Attribute-based credentials [7] have been proposed as an alternative to psuedonyms. Privacy-enhancing attribute-based credentials permit users to authenticate to verifiers in a data-minimizing way such that users are unlinkable between authentications and only divulge those attributes from their credentials that are pertinent to the verifier [8]. However, attributed-based credentials require establishment of shared secrets/attributes for all desired services. Nevertheless, identity privacy needs to be considered in CE products to protect consumer privacy.

Information Privacy: Within payment systems, mobile phones, and medical devices, a range of information about an individual (e.g., name, birthday, home address, social security number, driver's license number, credit card number, etc.) is utilized in order to provide efficient and enjoyable service. In the case of medical devices, information about a person's health may be stored and transmitted in order to provide life-saving services to the patient [9]. *Differential privacy* aims to preserve information privacy by providing means to maximize the accuracy of queries from statistical databases while minimizing the probability of identifying its records [10]. However, true user privacy is still challenging to attain via differential privacy as creation of ϵ-differentially private databases becomes difficult as $\epsilon \to 0$.

Location Privacy: Location privacy means the privacy of a consumer's location. Location information is often collected in CE devices to provide location-aware services. Location obfuscation or location cloaking [11] is a technique utilized in privacy-preserving location-based services, which protects the location of the users by slightly modifying, substituting, or generalizing their location in order to avert disclosing their real position.

Usage Privacy: Usage privacy refers to the privacy of behaviors and habits of a consumer. CE devices collect and store information about a user to create patterns of movement, activity, etc., of an individual. Many of the devices described as *home consumer electronics* depend on this usage data and activity patterns in order to provide their services. For example, smart thermostats turn on when a consumer is present in the home, and conserve energy when no body is at home [12]. While this information collection helps CE products to provide valuable services to the user, it also presents privacy vulnerabilities if the collected information is not properly protected.

C. Analysis of Security and Privacy Approaches

Table II depicts a comparative analysis of some of the contemporary approaches to security and privacy issues within CE. We mention the advantages and disadvantages of the proposed solutions. For example, a common solution for implementing authentication mechanisms in CE is to utilize message authentication codes (MACs), however, MACs require additional computation overhead in order to perform the symmetric cryptography verification process. Each of the proposed solutions benefits certain aspects of security and privacy in CE, but may also introduce additional challenges that must be taken into account.

IV. CHALLENGES

Balancing the need for new features and cost-effective solutions in CE while preserving consumer security and

TABLE II: **Comparative Analysis of Selected Current Approaches to Security and Privacy Issues in CE**

Category	Current Approaches	Advantages	Disadvantages
Confidentiality	Symmetric Key Cryptography	+ Low computation overhead	- Key distribution problem
	Asymmetric Key Cryptography	+ Good for key distribution	- High computation overhead
Integrity	Message Authentication Codes	+ Verification of message contents	- Additional computation overhead
Availability	Signature-based Authentication	+ Avoids unnecessary signature computations	- Requires additional infrastructure and rekeying scheme
Authentication	PUFs	+ High speed	- Additional implementation challenges
	Message Authentication Codes	+ Verification of sender	- Computation overhead
Non-Repudiation	Digital Signatures	+ Link message to sender	- Difficult in pseudonymous systems
Identity Privacy	Psuedonym	+ Disguise true identity	- Vulnerable to pattern analysis
	Attribute-based Credentials	+ Restrict access to information based on shared secrets	- Require shared secrets with all desired services
Information Privacy	Differential Privacy	+ Limit privacy exposure of any single data record	- True user-level privacy still challenging
	Public-Key Cryptography	+ Integratable with hardware	- Computationally intensive
Location Privacy	Location Cloaking	+ Personalized privacy	- Requires additional infrastructure
Usage Privacy	Differential Privacy	+ Limit privacy exposure of any single data record	- Recurrent/time-series data challenging to keep private

privacy is extremely challenging for CE producers. This section highlights the challenges involved in integrating security and privacy primitives in CE.

Resource Constraints of Consumer Electronics: Due to the design and cost constraints, many of the CE devices have limited storage, memory, computing power, and communication range. With these resource limitations and consumer demands for new features, designers face a tradeoffs in improving functionality and features versus information security and privacy. Additionally, due to computing power constraints in CE, attacks such as *denial of service (DoS)*, where a device is flooded with malicious requests to prevent legitimate requests from being processed, become easy to perform.

Real-Time Constraints of Consumer Electronics: Many CE applications, in particular cyber-physical systems (CPS) applications, require real-time responses to events occurring in the world, and many of the miniaturized CE products struggle to meet the strict timing requirements. The inability to meet real-time deadline of safety-critical CPS (e.g., medical and transportation systems) puts consumers' safety at risk.

Individual Privacy Preferences: Privacy preferences among consumers vary widely ranging from those who desire ultimate privacy and little to no exposure to those who voluntarily share their information and opt-in to new services. With the drastic difference in privacy preferences of consumers, managing the preferences of users in CE and striking a balance between these ends of the privacy spectrum is challenging for CE producers. By maintaining privacy measures in a transparent way, consumers are better informed as to what information is being collected about them and how this information is being utilized.

Secure Storage and Distribution of Secret Keys: Integration of security primitives, such as confidentiality, integrity, and authentication, in CE relies on secret keys. Not all the CE devices have the capability to securely store and manage secret keys, which puts the security and privacy of consumers at risk. Besides secure storage of secret keys, secure key distribution of secret keys between CE devices involved in a given application presents another challenge. Resource constraints of many CE devices makes it difficult to implement complex secret key exchange protocols with large key lengths required to provide adequate security.

V. Mitigation of Security and Privacy Vulnerabilities

Secure Storage and Generation of Secret Keys: Secret keys can be stored in a secure tamper-resistant memory to mitigate leakage and extraction of secret keys. Furthermore, hardware-based security techniques, such as physically unclonable functions (PUFs), provide a promising avenue for secret key generation without the need for storing the secret key in memory [13].

Intrusion Detection Systems: By providing a *first line of defense* against potential threats, intrusion detection

systems (IDS) can be utilized in CE to thwart common attacks against devices. The IDS used in CE can be made more effective by maintaining fresh signatures as well as leveraging machine learning-based techniques for intrusion detection.

Secure Processor Architecture: The resource constraints of many CE systems is one of the limiting factor that prevents implementation of stronger security protocols. A case study of automotive electronic control unit (ECU) shows that integration of security and dependability in the processor architecture itself can meet security and dependability needs of the device while ensuring that real-time constraints of the application are satisfied in an energy-efficient manner [14].

Privacy-Preserving Computing: Integration of CE in everyday life raises issues of privacy of data collection and analytics on this data while maintaining consumer privacy. Privacy-preserving computing, wherein the participating parties jointly compute a function over their inputs while keeping those inputs private, has emerged as one such solution to this issue [15]. Similarly, new strategies and methods are being developed to perform big data analytics while preserving consumer privacy [15].

VI. Conclusions

CE products bring interesting solutions to common issues in our daily lives, such as remotely monitoring our homes, improved health care and patient monitoring, and new forms of entertainment. However, with these benefits, proliferation of CE devices in our daily lives also brings new security and privacy concerns, which if not addressed, can be exploited by attackers to launch attacks against personal data, privacy, and safety. Hence, it is imperative that security and privacy be considered in the design of CE products

Acknowledgments

This work was supported by the National Science Foundation (NSF) (NSF-CNS-1743490). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the NSF.

About the Authors

Dalton Hahn (daltonhahn@ku.edu) is a graduate student in the Department of Computer Science at the University of Kansas.

Arslan Munir (amunir@ksu.edu) is currently an Assistant Professor in the Department of Computer Science at Kansas State University.

Saraju P. Mohanty (saraju.mohanty@unt.edu) is currently a Professor at the University of North Texas.

References

[1] S. P. Mohanty, U. Choppali, and E. Kougianos, "Everything You wanted to Know about Smart Cities," vol. 5, no. 3, pp. 60–70, July 2016.

[2] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, and Y. Zhou, "Understanding the Mirai Botnet," in *Proc. 26th USENIX Security Symposium*, 2017.

[3] G. Zhang, Q. Wu, M. Cui, and R. Zhang, "Securing UAV Communications via Trajectory Optimization," in *Proc. IEEE Global Communications Conference*, 2017, pp. 1–6.

[4] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET Security Challenges and Possible Cryptographic Solutions," *Vehicular Communications*, vol. 1, no. 2, pp. 53–66, April 2014.

[5] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 1, pp. 86–96, Jan 2012.

[6] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, "Privacy in Inter-Vehicular Networks: Why Simple Pseudonym Change is not Enough," in *Proc. International Conf. on Wireless On-demand Network Systems and Services*, 2010, pp. 176–183.

[7] G. Neven, G. Baldini, J. Camenisch, and R. Neisse, "Privacy-Preserving Attribute-Based Credentials in Cooperative Intelligent Transport Systems," in *Proc. IEEE Vehicular Networking Conference*, 2017, pp. 131–138.

[8] J. Camenisch, A. Lehmann, G. Neven, and A. Rial, "Privacy-Preserving Auditing for Attribute-Based Credentials," in *Proc. of European Symposium on Research in Computer Security*, M. Kutyłowski and J. Vaidya, Eds., 2014, pp. 109–127.

[9] Z. E. Ankarali, Q. H. Abbasi, A. F. Demir, E. Serpedin, K. Qaraqe, and H. Arslan, "A Comparative Review on the Wireless Implantable Medical Devices Privacy and Security," in *Proc. International Conference on Wireless Mobile Communication and Healthcare*, 2014, pp. 246–249.

[10] F. Kargl, A. Friedman, and R. Boreli, "Differential Privacy in Intelligent Transportation Systems," in *Proc. 6th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2013, pp. 107–112.

[11] E. Yigitoglu, M. L. Damiani, O. Abul, and C. Silvestri, "Privacy-Preserving Sharing of Sensitive Semantic Locations under Road-Network Constraints," in *Proc. IEEE 13th International Conference on Mobile Data Management*, 2012, pp. 186–195.

[12] B. Copos, K. Levitt, M. Bishop, and J. Rowe, "Is Anybody Home? Inferring Activity From Smart Home Network Traffic," in *Proc. IEEE Security and Privacy Workshops*, 2016, pp. 245–251.

[13] V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, "Making Use of Manufacturing Process Variations: A Dopingless Transistor Based-PUF for Hardware-Assisted Security," *IEEE Transactions on Semiconductor Manufacturing*, vol. 31, no. 2, pp. 285–294, May 2018.

[14] B. Poudel and A. Munir, "Design and Evaluation of a Novel ECU Architecture for Secure and Dependable Automotive CPS," in *Proc. IEEE Consumer Communications Networking Conference*, 2017, pp. 841–847.

[15] R. Lu, H. Zhu, X. Liu, J. K. Liu, and J. Shao, "Toward Efficient and Privacy-Preserving Computing in Big Data Era," *IEEE Network*, vol. 28, no. 4, pp. 46–50, July 2014.