Security and Privacy Issues in Contemporary Consumer Electronics

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

The advancements in consumer electronics (CE) in a variety of domains offer consumers 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 these systems—including collecting sensitive patient data through medical equipment to location privacy concerns in personal devices—are critical.

CE products are potentially rife with security and privacy vulnerabilities. Many of these electronic items have wireless interfaces, which increases their susceptibility to attack. Recently, a flood of CE contrivances have become part of the Internet of Things (IoT) because of their ability to connect to the Internet, making various physical components smart [1]. This Internet connectivity further exacerbates these products' security and privacy challenges and creates new ways for malicious intruders to succeed. 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 contemporary CE devices are lacking in the literature. This article aims to fill this gap. We provide a classification of the relevant issues, discuss the challenges in addressing them, and contemplate potential solutions to mitigate them.

Holistic discussions of security and privacy issues in contemporary CE devices are lacking in the literature.

Digital Object Identifier 10.1109/MCE.2018.2867979
Date of publication: 10 December 2018

SECURITY AND PRIVACY PERSPECTIVES ON CONTEMPORARY CE

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

- *Medical CE*: This area includes such equipment as pacemakers, heart-rate monitors, and insulin pumps, which 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 items also opens entry points for attackers and new vulnerabilities that can have grave consequences for consumers.
- *Home CE*: These products, such as Amazon Alexa, Google Home, smart thermostats, and intelligent coffee makers, are becoming more ubiquitous in homes around the world. Often paired with a smartphone application or a personal assistant device, home CE apparatuses are easily controlled and configured. However, along with these benefits of remote controllability and configurability comes the risk of malicious actors finding new ways to breach our privacy and security.
- *Personal CE*: Such gadgets include smartphones, portable music players, tablets, and laptops and are the most widespread among the CE categories. Along with smartphones and mobile computers, personal CE products include devices that connect to smartphones and mobile computers, like headsets.
- *Wearable CE*: Wearable devices have emerged in the CE market in a variety of forms, such as smartwatches, smart clothing, activity trackers, and pedometers. Wearable CE also introduces security and privacy issues, as these products expose consumers' personal information to the risk of attack.
- *Business CE*: From point-of-sale terminals to information kiosks and automated teller machines, CE products are being incorporated into the business and financial world. New methods of payment, such as cryptocurrency or smart payments through smartphones, present additional security and privacy challenges for these CE items.

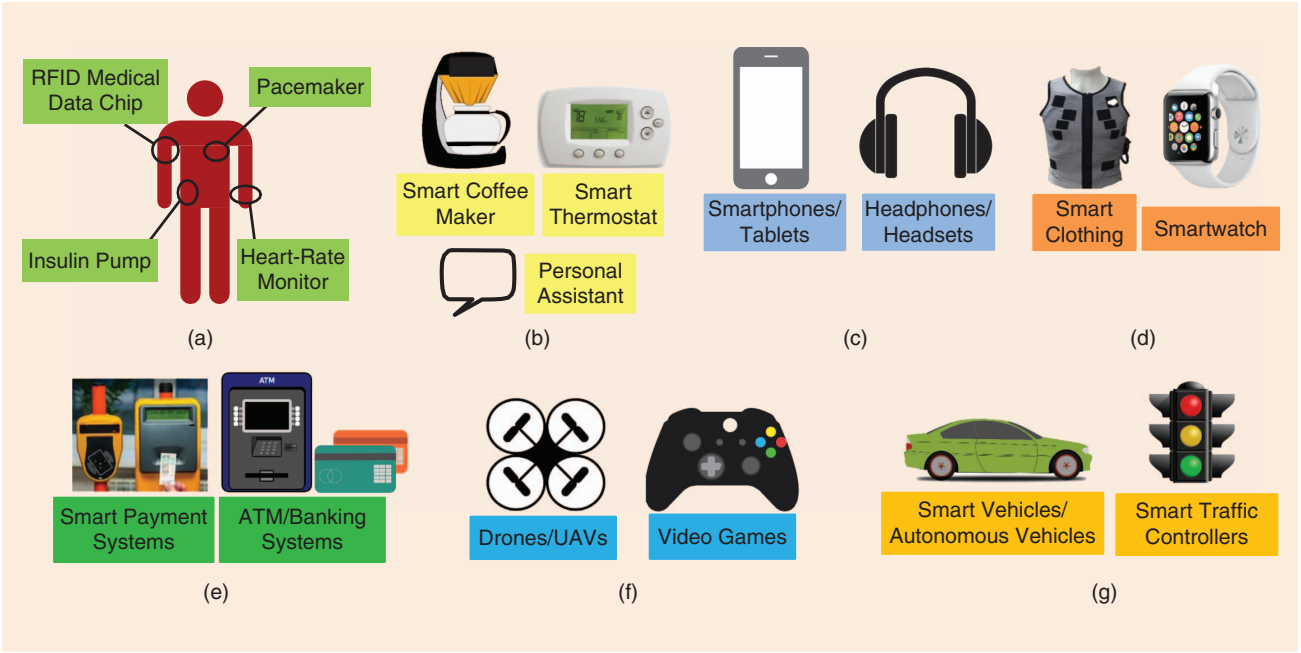

FIGURE 1. A selection of CE systems, classified according to their relationship with consumers: The devices are in various fields including (a) medical, (b) home, (c) personal, (d) wearables, (e) business, (f) entertainment, and (g) transportation.

- *Entertainment CE*: 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 by traditional means) and business applications for package deliveries. However, UAVs present additional challenges, as the they can be used to infringe on the privacy of other individuals.
- *Transportation CE*: Among the CE products relevant to the transportation industry are UAVs and a variety of transportation electronics, including systems for navigation, in-car entertainment, and parking assistance. Other CE devices like smartphones, portable music players, and Bluetooth devices are connected to vehicles, which, while providing various benefits, also create security and privacy vulnerabilities.

Table 1. A case study of UAV security issues.

Attack Example	Security Dimension	Attack Type
Denial of service	Availability	Active
Sybil attack	Integrity, availability	Active
MITM	Confidentiality, integrity, availability, authentication	Active/passive
Spoofing	Integrity, availability, authentication	Active
Eavesdropping	Confidentiality	Passive
Data poisoning	Integrity, availability	Active
Replay attack	Integrity, authentication	Active

CLASSIFICATION OF SECURITY AND PRIVACY ISSUES

SECURITY ISSUES IN CE

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

- *Confidentiality*: Confidential communication between CE devices is vital for ensuring the security and privacy of consumers. In the UAV example, confidential communication between a UAV and the operator's handheld receiver is crucial for proper control of the aircraft [3]. Table 1 highlights malicious actions, 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 just described and the Sybil

attack (where an assailant 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, make poor decisions, or engage in perilous actions based on incorrect or subversive data.

- *Availability*: The availability of CE products is important for interpersonal communication and to provide enjoyable experiences for users—and for consumer safety. For example, the availability of medical CE devices is crucial for patients, as these products' unavailability can threaten lives.
- *Authentication and identification*: For consumers and CE products alike to be properly authenticated and identified is important for a variety of applications. For medical CE apparatuses, authentication and identification provide a framework for physicians and medical professionals to securely access the information and provide control commands to these devices.
- *Nonrepudiation*: This dimension provides the ability to prove that a party is responsible for an action observed, without deniability. Nonrepudiation enables the unambiguous tracing of a message back to its originator, which can be useful in forensics and legal matters. For example, if a UAV is observed in a no-fly zone or seen potentially spying on someone, nonrepudiation would prevent the individual responsible for those actions from denying them. However, despite the security benefits of nonrepudiation, its tradeoff with privacy presents an interesting challenge.

PRIVACY ISSUES IN CE

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

- *Identity privacy*: Identity privacy in the context of CE provides the basis for protecting consumers' identity when they interact with electronic products. Many such devices require an account to be created to access the services they provide. By registering an account, the identity of the owner is linked to the device.

CE devices store a plethora of consumers' personal information and thus are a potential source of privacy violations and vulnerabilities.

Research on autonomous vehicles, shown in Figure 1, has recently explored using pseudonyms (fictitious names) to mask the identity of individuals in intelligent transportation systems (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 and other CE categories [6].

Attribute-based credentials [7] have been proposed as an alternative to pseudonyms. Privacy-enhancing attribute-based credentials permit users to authenticate to verifiers in a data-minimizing way such that users are unlinkable between authentications and divulge only those attributes from their credentials that are pertinent to the verifier [8]. However, attribute-based credentials require the 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*: In payment systems, mobile phones, and medical devices, a range of information about an individual (e.g., name; birthday; home address; Social Security, driver's license, and credit card numbers; and the like) is utilized to provide efficient and enjoyable service. In the case of medical devices, information about a person's health may be stored and transmitted to provide lifesaving services to the patient [9]. Differential privacy aims to preserve information privacy by providing the 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 the creation of ϵ-differentially private databases becomes difficult as $\epsilon \rightarrow 0$.
- *Location privacy*: This relates to the privacy of a consumer's whereabouts. Such 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 whereabouts of users by slightly modifying, substituting, or generalizing their location to avert disclosing their real position.
- *Usage privacy*: This refers to a consumer's privacy in terms of behaviors and habits. CE devices collect and store information about a user to create patterns of an individual's movements, activities, and so forth. Many of the devices described as *home CE* depend on these usage data and activity patterns to provide their services. For example, smart thermostats turn on when a consumer is present in the home and conserve energy when the resident is absent [12]. While this information helps CE products to provide valuable services to the user, it also presents privacy vulnerabilities if the collected information is not properly protected.

ANALYSIS OF SECURITY AND PRIVACY APPROACHES

Table 2 depicts a comparative analysis of some of the contemporary approaches to security and privacy issues in 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 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 considered.

CHALLENGES IN INCORPORATING SECURITY AND PRIVACY SOLUTIONS

Balancing the need for new features and cost-effective solutions in CE while preserving consumer security and privacy is extremely challenging for producers. This section highlights the challenges involved in integrating security and privacy primitives in electronic contrivances.

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

Hardware-based security techniques, such as physically unclonable functions, provide a promising avenue for secret key generation.

- *Real-time constraints of CE*: Many CE usages, in particular cyberphysical system (CPS) applications, require real-time responses to events occurring in the world, and many miniaturized CE products struggle to meet the strict timing requirements. The inability to meet real-time deadlines of safety-critical CPSs (e.g., medical and transportation systems) puts consumers' safety at risk.
- *Individual privacy preferences*: Privacy preferences among consumers vary widely, ranging from the desire for ultimate privacy and little to no exposure to the willingness to voluntarily share information and opt in to new services. With the drastic differences in consumers' privacy inclinations, 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 CE devices have the capability to securely store and manage secret keys, which endangers consumers' security and privacy. Besides the secure storage of secret keys, secure key distribution of secret keys between CE devices involved in a given application presents another challenge. The resource constraints of many CE devices make it difficult to implement complex secret key exchange protocols with the large key

Table 2. A 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	MACs	Verification of message contents	Additional computation overhead
Availability	Signature-based authentication	Avoids unnecessary signature computations	Requires additional infrastructure and rekeying scheme
Authentication	Physically unclonable functions	High speed	Additional implementation challenges
	MACs	Verification of sender	Computation overhead
Nonrepudiation	Digital signatures	Link message to sender	Difficult in pseudonymous systems
Identity privacy	Pseudonym	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

lengths required to provide adequate security.

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 their leakage and extraction. Furthermore, hardware-based security techniques, such as physically unclonable functions, 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 (IDSs) can be utilized in CE to thwart common attacks against devices. The IDSs can be made more effective by maintaining fresh signatures and by leveraging machine-learning-based techniques for intrusion detection.
- *Secure processor architecture*: The resource constraints of many CE systems is one of the limiting factors that prevents the implementation of stronger security protocols. A case study of the automotive electronic control unit shows that the integration of security and dependability in the processor architecture itself can meet the security and dependability needs of the device while ensuring that the real-time constraints of the application are satisfied in an energy-efficient manner [14].
- *Privacy-preserving computing*: The integration of CE in everyday life raises issues of the privacy of data collection and the 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].

CONCLUSION

CE products bring interesting solutions to common issues in our daily lives, such as remotely checking our homes, improved health-care and patient monitoring, and new forms of entertainment. However, with these benefits, the proliferation of CE devices in our daily lives opens up new security and privacy vulnerabilities, which, if not addressed, can be exploited by malefactors to launch attacks against personal data, privacy, and safety. As a result, 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 A. Hahn (daltonhahn@ku.edu) is a graduate student in the Department of Computer Science, University of Kansas, Lawrence.

Arslan Munir (amunir@ksu.edu) is an assistant professor in the Department of Computer Science, Kansas State University, Manhattan.

Saraju P. Mohanty (saraju.mohanty@unt.edu) is a professor at the University of North Texas, Denton.

REFERENCES

[1] S. P. Mohanty, U. Choppali, and E. Kougianos, "Everything you wanted to know about smart cities," *IEEE Consum. Electron. Mag.*, vol. 5, no. 3, pp. 60–70, 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 Symp.*, 2017, pp. 1093–1110.

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

[4] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," *Veh. Commun.*, vol. 1, no. 2, pp. 53–66, 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 Trans. Veh. Technol.*, vol. 61, no. 1, pp. 86–96, 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. Int. Conf. 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 Conf.*, 2017, pp. 131–138.

[8] J. Camenisch, A. Lehmann, G. Neven, and A. Rial, "Privacy-preserving auditing for attribute-based credentials," in *Proc. European Symp. Research Computer Security*, 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. Int. Conf. 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 Conf. Security and Privacy 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 Int. Conf. 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 Trans. Semicond. Manuf.*, vol. 31, no. 2, pp. 285–294, 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 Conf.*, 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 Netw.*, vol. 28, no. 4, pp. 46–50, 2014.