Proceedings of the Eleventh International Symposium on
Human Aspects of Information Security & Assurance (HAISA 2017)

The Socio-Technical Impact on Security of the Healthcare Internet of Things in the Use of Personal Monitoring Devices (PMDs)

H.P.A.I. Pathirana[1] and P.A.H. Williams[2]

[1]College of Science and Engineering, Flinders University, Adelaide, Australia
[2]Flinders Digital Health Research Centre, Flinders University, Adelaide, Australia
e-mail: path0037@flinders.edu.au; patricia.williams@flinders.edu.au

Abstract

New healthcare technologies facilitate additional care pathways and opportunities for patients beyond that of traditional care. Patient care using the Healthcare Internet of Things (HIoT) such as regular fitness and blood pressure monitoring and storing the data for detailed analysis are one of these new pathways. Chronic disorders such as respiratory illness, physiological disorders, cardiovascular diseases, stroke, and diabetes have benefitted from using Personal Monitoring Devices (PMDs). In addition, the aged care and child care sectors consider regular monitoring of people vital, and individuals are using PMDs to learn more about their calories burned, diet, exercise regime and vital signs. However, there is an increasing concern for privacy and security of personal health information generated by PMDs, and users themselves contribute to leakage of information. Therefore, it is essential to educate users to interact safely and securely with the HIoT environment without introducing additional vulnerabilities and unnecessary risks to personal information. At present, there is insufficient attention paid to the socio-technical perspectives specific to HIoT. Further, there is no guidance for consumers on the human factors influencing secure PMD usage. A case study method was used to devise a framework to map mitigation techniques that could be applied to improve the security and privacy of information based on the human security factors of HIoT. The research identified the level of involvement of users in their personal security posture when using HIoT PMDs. This research may assist in educating people in secure information usage, and explore mechanisms to improve a secure user experience with such devices. Such research is important given the sensitive nature of health information.

Keywords

Healthcare Internet of Things, personal monitoring devices, socio-technical security, human factors.

1. Introduction

The Internet of Things (IoT) introduces a new and exciting opportunity for creating a connected environment by linking smart objects, equipped with sensors and actuators, over the Internet. IoT is proving an exciting technological enhancement which is contributing the global economy whilst simultaneously advancing society by providing improved human experiences. Research predicts a massive growth in devices connected to the Internet in the coming five years, with more than 50 billion devices predicted to be connected by year 2018 in United States (Patel, Asch, &

Volpp, 2015), and Cisco suggesting that global IoT market will reach $14.4 trillion by 2022 (Andrea, Chrysostomou, & Hadjichristofi, 2015).

Aligning with this growth is the adoption of the Healthcare Internet of Things (HIoT) as a primary vertical of the technology because of the benefits the healthcare sector can expect with the evolution of IoT. Unlike other sectors, the indirect costs associated with health, such as longevity and quality of life, are important in the assessment of benefits despite being problematic to quantify financially. The healthcare requirements of individuals are broad, and using HIoT is one way to bring increased personalisation to healthcare using technology.

HIoT has drawn considerable attention from the research community as highlighted by the numerous and annually increasing in corresponding research and development efforts (Sungmee & Jayaraman, 2013). As healthcare costs are increasing and the world population is ageing (Hao & Foster, 2008), there is a need to monitor a patient's health status while a person is out of the hospital and in their home environment. Over recent years a variety of system prototypes and commercial products have been trialled to address the demand for real time feedback on personal health conditions. Undeniably, HIoT provides a practical approach for introducing real time care (Kodali, Swamy, & Lakshmi, 2015). Personal healthcare devices introduce a new way for monitoring an individual's health and potentially avoiding additional costs and lengthy hospital stays. It is the interconnectedness that HIoT can provide that will also provide longer term benefits of personalised coordinated care.

HIoT can be introduced as umbrella term for many technologies in healthcare. Whilst the technological improvements introduce advanced use of devices for enhancing healthcare, it also creates a vulnerable operating environment from a security perspective for both the user and device manufacturer. Data confidentiality and personal privacy can be impacted with poor security practices. Recent episodes have involved unauthorised access due to the complexity of the interconnection (Williams & McCauley, 2016) and the human element introducing vulnerabilities due to poor understanding of the way to ensure secure technological implementation (Andrea et al., 2015). Hence, the security in HIoT is crucial and significant when compared to the security of other types of IoT because of the sensitivity of healthcare information (Darshan & Anandakumar, 2015). The increasing number of devices in the HIoT infrastructure, each a potential entry point to a network, means the vulnerabilities should not be underestimated. This research focussed on preventing such situations by introducing a framework to preserve information protection for the user and to strengthen the secure use of PMDs.

The question posed by this research covers the risk of information security introduced by the threats and vulnerabilities in the use of PMDs. Whilst the threat landscape evolves, each threat has no opportunity to exploit once vulnerabilities do not exist. The objective of this research is to reduce the possibility of introducing vulnerabilities, by investigating if a socio-technical impact framework can be developed to assist users with the secure use of personal monitoring devices.

2. Background

The HIoT environment is complex due to the increasing use of devices and advances in technology, however it is essential to preserve information security over complex use to strengthen user trust. The user should be interested in securing their sensitive healthcare information, so they will not introduce vulnerabilities unintentionally, however their contribution to the problem can be significant. To better understand the issues in the use of PMDs it is important to pay attention to individual scenarios of use to propose mitigations across technologies and stakeholders.

A conceptual view of the use of PMDs in the HIoT environment is illustrated in Figure 1. People are the central focus, with the technology and use of the technology supporting the healthcare requirements for better quality of life. The process includes people interacting with devices (as the user), and the output of interest is the healthcare information produced by the devices about the user. The application software provides an interface and the data storage for the data captured by the sensors in the device. The server side of the application and device is the repository for the data. The device may store data on the device temporarily, and then the data is synchronised with other storage services for decision making.

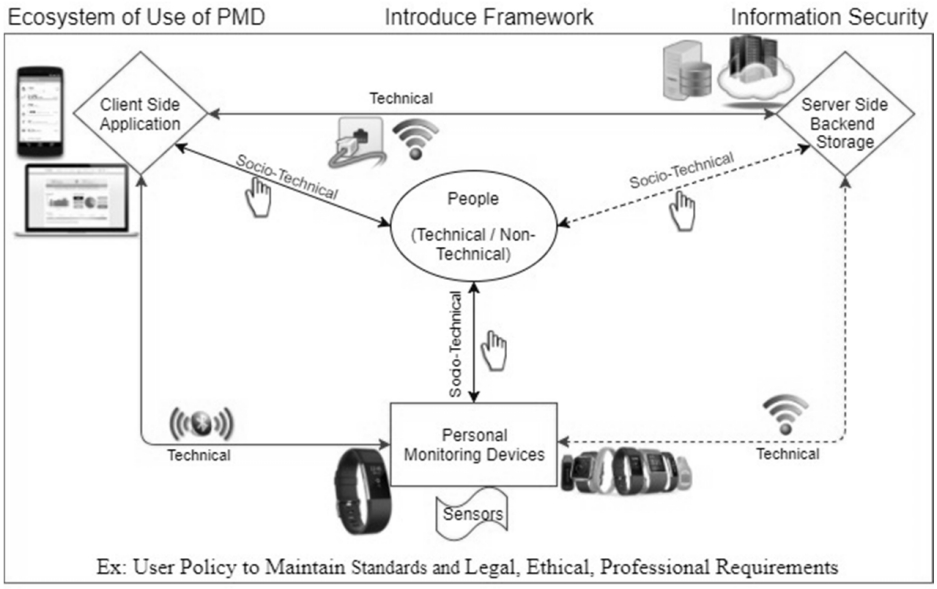

Figure 1: Conceptual view of the HIoT environment of use of PMD

2.1. The Internet of Things

The IoT technology or device can include a processing component without direct involvement of the user. The IoT related technologies are developed with near-field communication (NFC) and sensor networks as one example. Such configurations have been influenced by the evolution of the Internet into the Web 3.0 level, and as a result, the machine-to-machine communication is introduced over the Internet. The

ease and mode of communication is a key motivation for more devices to be online and to intercommunicate, and hence form the Internet of Things (IoT) paradigm.

To date there is no widely agreed or universal definition for the Internet of Things, however the concept is to equip devices with identifying, sensing, networking and processing capabilities allowing them to communicate each other devices over services utilising the Internet to accomplish some worthwhile objective. The hardware, software and architecture drive the technology of IoT, whereas the applications of IoT, supply chain, social applications, smart infrastructure and healthcare receive the benefit of this technological innovation (Andrea et al., 2015).

2.2. The Healthcare Internet of Things (HIoT)

HIoT includes healthcare applications with connection to electronic health records. As a result, HIoT has been introduced as a significant branch of IoT given the unique benefits it can offer personal healthcare. Alternative healthcare solutions, tele-health, m-health, and e-health are driving the healthcare sector towards redesigning modern healthcare infrastructure to include technological, social and economic advances.

Smart medical devices are unique source for generating data such as temperature, glucose level and heart rate, for decision making by healthcare professionals and patients in the management of chronic conditions, as well as future health conditions (Sungmee & Jayaraman, 2013). Similarly, PMDs include specific features such as monitoring sleep and exercise patterns, which implicitly monitor using non-intrusive sensors (Islam et al. 2015). Wearable devices form part of the environment as they co-exist and interoperate with the available HIoT architecture for intercommunication between devices and applications.

2.3. Use of Personal Monitoring Devices

PMDs used for monitoring personal health conditions are becoming a phenomenon to maintain quality of life and promote wellness over long periods of time. The present HIoT infrastructure facilitates PMDs to interact with other devices (such as smart phones) to store the personal healthcare data for evaluation for maintaining health, diagnosis of disease, and monitoring health conditions on a regular basis. Consumers measure their blood pressure, monitor their heart rate and other indices of health constantly, and synchronise the data electronically with centralised systems, and can allow health care providers to monitor this data remotely (Reilly et al., 2006). Device manufacturers and health care providers are confident that these technological advances can help to reduce the cost of care, and is confirmed by the significant growth in manufacturing of such devices (Sungmee & Jayaraman, 2013).

Alongside the technology there has been an increase in monitoring physical activity to maintain an individuals' health. There are guidelines for physical activity minimum levels: children and adolescents - 60 minutes/day; and adults 18 to 64 years old -150 to 300 minutes/week (Straker et al., 2016; Tremblay et al., 2011). Such guidelines motivate consumers to use PMDs to meet these objectives.

2.4. Security of Internet of Things

IoT is based on the Internet, sensor networks and mobile communication networks, so the security concerns of those areas are reflected in the fundamental IoT environment (Andrea et al., 2015). Further, given the potential of IoT, its wider deployment, the volumes of information generated, use of wireless technologies in public locations, the increasing number of cybersecurity attacks, device mobility and the dynamically changing environment, the security of IoT is an increasingly challenging factor (Xu, Wendt, & Potkonjak, 2014).

The conventional static security becomes obsolete when faced with increased complexity of communication systems and attacks (Xu et al., 2014), thus sustaining security measures using traditional approaches is difficult. The overhead cost increases dramatically and the security is automatically inefficient and inappropriate. Thus, new mechanisms are needed by addressing the nature of IoT to preserve security. The trade-off among security mechanisms and performance is also vitally important for investigating new protective techniques (El Maliki & Seigneur, 2010).

2.5. Security of Healthcare Internet of Things

Although HIoT facilitates a new environment of interoperability, each endpoint is a probable point of vulnerability for a complete network (Williams & McCauley, 2016). The security of HIoT is specific over security of IoT considerations, since the sensitivity and management of healthcare information is complex. The complexity in the security of HIoT increases due to many reasons including limited processing capabilities and power, storage capabilities, low power design, and a lack of standard interfaces (Williams & McCauley, 2016). As a result, the use of outdated hardware, older operating systems, and legacy application software contribute to vulnerable points for attack vectors. Further, there are regulatory issues inherent in the heterogeneous connectivity of the environment that impact security posture.

2.6. Secure of Use of PMDs

The sensors in PMDs capture healthcare information and synchronise with different applications using different NFC techniques such as Bluetooth, Bluetooth Low Energy (BLE), and Zigbee. The security of PMDs is more specific over security of HIoT considerations due to the very limited resource available with wearable devices. Further, the technology with weak security is a particular challenge for healthcare information security. Whilst PMD connections can use different communication protocols (e.g. Zigbee, Bluetooth, BLE), the security functionality across protocols is inconsistent. This makes such protocols problematic for the secure transfer of personal health information. The available literature specific for PMDs is not sufficient, so alternative research to identify the issues for IoT is needed to understand the possible vulnerabilities and associated security issues.

3. Methodology

This research considered the possibility of improving the socio-technical impact on security in the use of personal medical devices by introducing a framework for the users of PMDs. The research was undertaken in three phases.

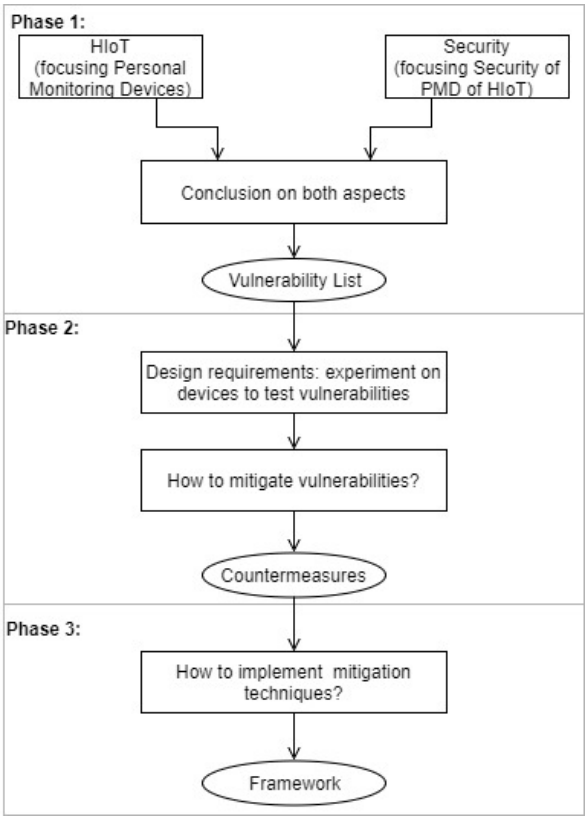

Figure 2: Research Design

The first phase reviewed the literature to ascertain the security considerations associated with HIoT. This phase ascertained a list of vulnerabilities and current mitigations using a case study qualitative approach. In the second phase, quantitative experimentation using the Fitbit and Garmin PMDs was undertaken, and potential countermeasures identified. The third phase introduced a framework of mitigation techniques to improve the security of information based on the human factor security in HIoT. This framework was designed to communicate the risks of use of PMDs in HIoT environment, so the likelihood of exploiting a vulnerability may be reduced by addressing the risks to information protection. The overall study can be introduced as interpretivism study as per a paper publish on making real research in medical information security (Williams, 2006).

4. Results

The outcomes of each phase are discussed in this section providing the list of vulnerabilities, list of countermeasures, and the mitigation framework. The vulnerabilities identified from evaluation of the literature are shown in Table 1.

Vulnerability	Description
Non-Technical Vulnerabilities	
Theft	Intentional and subsequent impact or damage may be high.
Lost	Unintentional but subsequent impact or damage may be high.
Unattended Device	The device information can be captured, and the stolen information used for intercepting device communication.
Enable Bluetooth Always	The third-party Bluetooth receiver may be listening to information to capture sensitive information.
Eavesdropping	The user's credentials for application access may be captured.
Human Error / Failure	User error may lead to information leakage.
Missing, Inadequate Policy	Insufficient policy implementation advising the user about the significance and sensitivity of their health information.
Social Engineering	Social communications with the potential impact of stealing sensitive information.
Social Networking	Sharing personal health information over social networks may violate and put at risk an individuals' privacy
Technical Vulnerabilities	
No Use of Encryption	Some devices do not use encryption due to the additional processing power.
No Use of Authentication	The authorisation is based on a 4-digit pin code in most cases, but no use of other authentication for the device.
Technological Obsolescence	People use devices over several years, and new technological evolution may make the devices and security measures obsolete.
Multiple Connectivity	The PMD uses NFC to communicate with applications, and the applications synchronise data with storage over IP network. Introducing standards is complex in such environments.
Inherent Latency of BLE	The inherent latency of BLE introduces an opportunity for an attacker to represent legitimate traffic.
Software Attack	Mobile applications and web communications can present risks due to software attacks focusing configuration change and capturing data.
Quality of Services	The endpoints are not capable of buffering traffic for the handshaking process to assure effective quality of service.
Man in the Middle	Third parties can intercept the communication media to listen passively. Brute force attack is also possible.
Communication Medias	Bluetooth and BLE are popular among PMD, whilst Zigbee, WiFi, and GSM are more secure alternatives.
Denial of Services	Legitimate traffic is interrupted by introducing false traffic into the communication pathway, creating a jamming effect.

Table 1: List of Vulnerabilities

The countermeasures are identified in Table 2 based on the data in Table 1.

Countermeasures	Description
Non-Technical Countermeasures	
User Policies	Human error and failures are identified using specific policy on sensitive information protection.
Monitoring and Maintaining	The evolving environment must be monitored for assuring secure use.
Social Awareness	Education and training sessions for increasing user awareness.
Technical Countermeasures	
Security policies	It is necessary to introduce technical implementation in the policy to identify and guide secure development.
Introducing Light Weight Encryption	The encryption avoids understanding captured data without the key. It discourages third party interception
Introduce Multiple MAC Addresses for a Device	In theory, a MAC address is unique for a device, however multiple MAC addresses can be introduced to reduce the possibility of device tracking.
Clear & Informative User Interfaces	The PMD device interface may be compact and no ability to disable Bluetooth.
Tools for Managing Data	The consumer is owner of the data, so it is essential to have user control of the data using data management tools.

Table 2: List of Countermeasures

Categorising and grouping the countermeasures is based on the similarity of the countermeasure, and resulted in the general framework as in Figure 3.

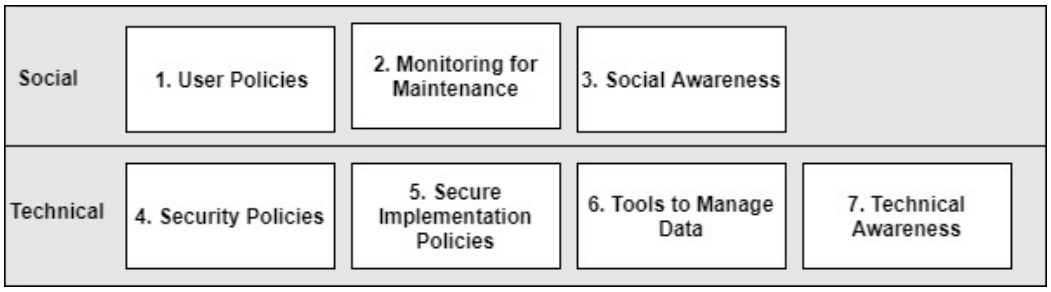

Figure 3: Framework

At the top level, the framework makes a distinction between the technical and social factors. The social layer is divided into: User Policies, Monitoring and Maintenance, and Social Awareness. The technical layer is divided into Security Policies, Secure Implementation Policies, Tools to Manage Data, and Technical Awareness. The policy implementation is one major consideration in any secure environment. Here, the identified vulnerabilities can be addressed by introducing environment specific Box 1. User Policies, Box 4. Security Policies and Box 5. Secure Implementation Policies in the framework. The technological evaluation and the consumer need, influence the security of the environment, and as a result monitoring the environment to maintain security is essential as shown in Box 2. Monitoring for Maintenance of the framework. The user must be advised about the importance of social behaviour through education and training, and this is represented by Box 3. Social Awareness component of the framework. Box 6. Tools to Manage Data focus on user's privilege to control data as owner of data using tools. Finally, Box 7. Technical Awareness focuses on acknowledging the importance of available security implementation by

conducting education and training. However, conserving the resources, such as power, constrains the PMDs, and therefore the social aspect should be considered as a priority over technical aspects for the user.

5. Discussion

Seven complementary and integrated approaches are introduced in the framework, and each approach consists of three levels, as shown in Table 3. Low Level is the least secure, with High Level the most secure practice.

Approach	Level	Description
Social Approaches		
User Policy	Low	No user policy for use of PMD.
	Medium	User policy inherent from general artefacts only.
	High	User policy specific to the use of PMDs.
Monitoring for Maintaining	Low	No monitoring or maintenance
	Medium	No pre-defined frequency for monitoring and maintenance
	High	Pre-defined frequency for monitoring and maintenance
Social Awareness	Low	No education and training.
	Medium	Informal and ad-hoc education and training only.
	High	Formalised education and training.
Technical Approaches		
Security Policy	Low	No user security policy for use of PMD.
	Medium	Security policy inherent from general artefacts only.
	High	Security policy specific to the use of PMDs.
Implementation Policy	Low	No implementation policy for use of PMD.
	Medium	Ad-hoc implementation policy.
	High	Formalised implementation policy.
Tools to Manage Data	Low	No tool to manage data.
	Medium	Constrained tools to manage data only.
	High	Comprehensive tools to manage data.
Technical Awareness	Low	No education and training.
	Medium	No official education and training.
	High	Official education and training.

Table 3: Framework Description

Clearly, there is overlap between the management of the socio-technical aspects of security and the cyber-physical systems inherent in IoT. The social and technical layers cannot be separated entirely and must be considered collectively for comprehensive security protection. The approaches in the framework also imply that data-driven decisions should be increasingly incorporated, particularly in boxes 2, 6 and 7. The construction of the social context, in which the information flow is dependent on the way the device and the data is used by an individual user, will further impact the potential diversity of levels of protection as shown in Figure 3. The convergence in using physical devices to communicate within the cyber (virtual) environment means that the associated information flows need to consider the multiple, sometimes competing, factors of the physical device security, human behaviour and socially constructed context of use.

6. Conclusion

The use of PMDs is becoming more prevalent due to the benefits for maintaining health and managing chronic health conditions, however the sensitive health information protection and secure practices have not yet matured due to the poor consideration of PMD specific environment. Further, the technical implementation of PMDs is not enough for assuring the security of sensitive health information, because of resource constraints, and the impact of social practices. As a result, the users of PMDs have significant responsibility for assuring the protection of their sensitive health information. This framework guides implementation of usable information security mechanisms for the users of PMDs and can be used to develop corresponding awareness and education programs. This research provides the fundamental understanding of the use of PMDs and the associated issues, and forms the basis for further investigation into the design of advice and education.

7. References

Andrea, I., Chrysostomou, C., & Hadjichristofi, G. (2015, 6-9 July 2015). *Internet of Things: Security vulnerabilities and challenges.* Paper presented at the 2015 IEEE Symposium on Computers and Communication (ISCC).

Darshan, K. R., & Anandakumar, K. R. (2015, 17-19 Dec. 2015). *A comprehensive review on usage of Internet of Things (IoT) in healthcare system.* Paper presented at the 2015 International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT).

El Maliki, T., & Seigneur, J.-M. (2010). *A security adaptation reference monitor (SARM) for highly dynamic wireless environments.* Paper presented at the Emerging Security Information Systems and Technologies (SECURWARE).

Hao, Y., & Foster, R. (2008). Wireless body sensor networks for health-monitoring applications. *Physiological measurement, 29*(11), R27.

Kodali, R. K., Swamy, G., & Lakshmi, B. (2015, 10-12 Dec. 2015). *An implementation of IoT for healthcare.* Paper presented at the 2015 IEEE Recent Advances in Intelligent Computational Systems (RAICS).

Patel, M. S., Asch, D. A., & Volpp, K. G. (2015). Wearable devices as facilitators, not drivers, of health behavior change. *Jama, 313*(5), 459-460.

Reilly, J. J., Kelly, L., Montgomery, C., Williamson, A., Fisher, A., McColl, J. H., Grant, S. (2006). Physical activity to prevent obesity in young children: cluster randomised controlled trial. *Bmj, 333*(7577), 1041.

Sungmee, P., & Jayaraman, S. (2013). Enhancing the quality of life through wearable technology. *IEEE Engineering in Medicine and Biology Magazine, 22*(3), 41-48. doi:10.1109/MEMB.2003.1213625

Williams, P. A. H. (2006). *Making Research Real: Is Action Research a Suitable Methodology for Medical Information Security Investigations?* Paper presented at the Australian Information Security Management Conference.

Williams, P. A. H., & McCauley, V. (2016, 12-14 Dec. 2016). *Always connected: The security challenges of the healthcare Internet of Things.* Paper presented at the 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT).

Xu, T., Wendt, J. B., & Potkonjak, M. (2014). *Security of IoT systems: design challenges and opportunities*. Paper presented at the Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design, San Jose, California.