12-11-2020

THaW publications

Carl Landwehr
George Washington University, carl.landwehr@gmail.com

David Kotz
David.F.Kotz@Dartmouth.EDU

THaW publications

The Trustworthy Health and Wellness (THaW) project
Carl Landwehr and David Kotz

Dartmouth Computer Science Technical Report TR2020-904

December 11, 2020

Abstract

In 2013, the National Science Foundation's Secure and Trustworthy Cyberspace program awarded a Frontier grant to a consortium of four institutions, led by Dartmouth College, to enable trustworthy cybersystems for health and wellness. As of this writing, the Trustworthy Health and Wellness (THaW) project's bibliography includes more than 130 significant publications produced with support from the THaW grant; these publications document the progress made on many fronts by the THaW research team. The collection includes dissertations, theses, journal papers, conference papers, workshop contributions and more. The bibliography is organized as a Zotero library, which provides ready access to citation materials and abstracts and associates each work with a URL where it may be found, cluster (category), several content tags, and a brief annotation summarizing the work's contribution. For more information about THaW, visit thaw.org.

Introduction

There are many ways one might organize the works in a collection such as this one. For simplicity, this bibliography assigns each work to one of eight loosely defined clusters or a catchall "other" cluster. Inevitably, many works do not fit precisely or only into one particular cluster; the content tags provide another way to organize the works and to help users find material relevant to their interests. Each work is labeled with up to four content tags drawn from a set of twenty, also loosely defined, categories. The collection can be filtered by cluster category or content tag to help locate entries of interest to the user. (In the Zotero version of the bibliography,[1] clusters and tags are both recorded in the Zotero "tags" field. However, the bibliography can still be grouped by cluster simply by filtering on the appropriately named tag.)

Each of the following sections provides a brief overview each cluster, ordered roughly by the size of cluster. Each cluster has its own 'References' section listing the publications in that cluster.

[1] https://www.zotero.org/groups/2647330/thaw/library

1 Devices

The usability, security, and privacy of medical devices and systems has been a primary focus for THaW researchers. The earliest THaW contribution in this category is a comprehensive Systematization of Knowledge (SoK) paper published at the IEEE Symposium on Security and Privacy in 2014 that provides a baseline for research in security and privacy for implantable and body area network devices. THaW research produced several innovative devices both to simplify authentication for medical systems and to provide continuous authentication. Papers and reports on the ZEBRA (later BRACE) system and the KBID system document some of this work, for which two patents were also issued. Vocal resonance as a biometric was also explored as a means to assure the identity of a microphone wearer. Research also investigated unexpected vulnerabilities in several devices, including interactions between acoustic and electromagnetic energy producers and sensors. Crafted acoustic signals were demonstrated to be able to damage hard drive availability and integrity. Vulnerabilities of implantable pacemakers, and communicating the consequent risks to patients were also the subject of THaW research and publication. Jointly with the IEEE, THaW supported the development of a draft "building code" for medical devices with security responsibilities. Additional device-related research can be found in the bibliography under this cluster.

References

[1] Connor Bolton, Kevin Fu, Josiah Hester, and Jun Han. How to curtail oversensing in the home. *Communications of the ACM*, 63(6) pages 20–24, June 2020. DOI 10.1145/3396261.

ACM Viewpoint notes the risks of promiscuous provision of sensor data to apps on IoT devices and endorses applying Principle of Least Privilege and establishing appropriate design patterns so that user privacy will not be accidentally compromised.
[architecture, cluster-devices, design, opinion, privacy]

[2] Connor Bolton, Sara Rampazzi, Chaohao Li, Andrew Kwong, Wenyuan Xu, and Kevin Fu. Blue Note: How Intentional Acoustic Interference Damages Availability and Integrity in Hard Disk Drives and Operating Systems. In *IEEE Symposium on Security and Privacy (SP)*, pages 1048–1062. IEEE, May 2018. DOI 10.1109/SP.2018.00050.

Paper documents mechanisms by which acoustic interference can disrupt hard drive performance, demonstrates the effects, and proposes protective measures to protect hard drives against such interference.
[architecture, cluster-devices, security, vulnerabilities]

[3] A. J. Burns, M .Eric Johnson, and Peter Honeyman. A brief chronology of medical device security. *Communications of the ACM*, 59(10) pages 66–72, October 2016. DOI 10.1145/2890488.

Short survey of medical device security history, organized into four overlapping periods, with comments on the future. Eric Johnson video segment available.
[cluster-devices, medical-devices, security, survey, vulnerabilities]

[4] Joe Carlson. 750,000 Medtronic Defibrillators Vulnerable to Hacking, March 2019. Online at http://m.startribune.com/750-000-medtronic-defibrillators-vulnerable-to-hacking/507470932/.

Newspaper report of security vulnerability in Medtronics implantable defibrillators.
[cluster-devices, medical-devices, security, vulnerabilities]

[5] Joseph Carrigan, David Kotz, and Aviel Rubin. STEM Outreach Activity with Fitbit Wearable Devices. Technical Report TR2018-839, Dartmouth College, February 2018. Online at https://digitalcommons.dartmouth.edu/cs_tr/376/.

Report is a template for a STEM classroom outreach activity involving student use of activity monitoring devices (e.g. FitBit).
[cluster-devices, medical-devices, privacy, security]

[6] Joseph Carrigan, Paul D. Martin, and Michael Rushanan. KBID: Kerberos Bracelet Identification (Short Paper). In Jens Grossklags and Bart Preneel, editors, *Financial Cryptography and Data Security (FC)*, volume 9603 of *Lecture Notes in Computer Science*, pages 544–551. Springer, February 2016. DOI 10.1007/978-3-662-54970-4_32.

Paper presents an authentication system that incorporates a user-worn bracelet that can in effect store strong authentication information (e.g. a lengthy password) and provide information based on it so that the user need not remember and recall the authentication information.
[cluster-devices, security]

[7] Kevin Fu, Peter Honeyman, Timothy Trippel, and Ofir Weisse. Protecting motion sensors from acoustic injection attack. US Patent Application PCT/US2017/033544, May 2017. Online at https://patents.google.com/patent/WO2017201409A1/en.

Application date 19 May 2017. This is a patent application for software techniques to mitigate the effects of acoustic injection attacks on sensors such as MEMS accelerometers. See also Trippel2017:WALNUT.
[cluster-devices, security, sensor]

[8] Kevin Fu and Wenyuan Xu. Inside risks: risks of trusting the physics of sensors. *Communications of the ACM*, 61(2) pages 20–23, February 2018. DOI 10.1145/3176402.

CACM Viewpoint argues that sensors need to be designed to be checkable in order to detect/defeat malicious attacks on them; also notes need to educate students about physical aspects of computing.
[cluster-devices, opinion, security]

[9] Sai Gouravajhala, Sree Vadrevu, Matthew Hicks, Jenna Wiens, and Kevin Fu. An LED Blink is Worth a Thousand Packets: Inferring a Networked Device's Activity from its LED Blinks. In *USENIX Summit on Information Technologies for Health (HealthTech)*, August 2015. Online at https://www.usenix.org/conference/healthtech15/poster-session.

Poster presented at HealthTech 2015. Evidently reports a scheme for inferring a medical device's network activity based on the blinking of its LEDs. Poster not available for download.
[cluster-devices]

[10] D.E. Holcomb and Kevin Fu. Physical unclonable function using augmented memory for challenge-response hashing. US Patent 9,787,481, October 2017. Online at https://patents.google.com/patent/US9787481B2/en.

Application filed 28 August 2015; Patent granted 10 October 2017. This is a patent for a method of using an array of SRAM cells to provide a physically unclonable function (PUF).
[cluster-devices, security]

[11] Daniel B. Kramer and Kevin Fu. Cybersecurity concerns and medical devices: lessons from a pacemaker advisory. *Journal of the American Medical Association (JAMA)*, 318(21) pages 2077–2078, December 2017. DOI 10.1001/jama.2017.15692.

Viewpoint discussing FDA's release of a safety communication concerning cybersecurity of pacemakers from St. Jude Medical.
[cluster-devices, opinion, security]

[12] Andrew Kwong, Wenyuan Xu, and Kevin Fu. Hard Drive of Hearing: Disks that Eavesdrop with a Synthesized Microphone. In *IEEE Symposium on Security and Privacy*, pages 125–139. IEEE, May 2019. DOI 10.1109/SP.2019.00008.

Documents how acoustic signals may be recovered from hard drives, whose read/write heads are sensitive to pressure changes and thus can provide as a side channel, a record of acoustic signals.
[cluster-devices, experiment, security, vulnerabilities]

[13] Carl Landwehr. We need a building code for building code. *Communications of the ACM*, 58(2) pages 24–26, February 2015. DOI 10.1145/2700341.

Article advocates the development of the analog of building codes for software with significant security responsibilities, and reports the development of a draft code for medical devices developed at a workshop convening researchers, developers, and government representatives.
[cluster-devices, design, opinion, security, testing]

[14] Carl Landwehr. Workshop to Develop a Building Code and Research Agenda For Medical Device Software Security (Final Report). Technical Report GW-CSPRI-2015-1, The George Washington University, January 2015. Online at http://www.landwehr.org/2015-01-landwehr-gw-cspri.pdf.

Report describes a workshop to develop an analog of a building code for medical device software security and provides a draft code developed by the workshop. Participants included medical device developers, researchers, and government representatives.
[cluster-devices, medical-systems, security]

[15] Xiaohui Liang and David Kotz. Securely Connecting Wearable Health Devices to External Displays. In *USENIX Safety, Security, Privacy, and Interoperability of Health Information Technologies (HealthTech)*. USENIX, August 2014. Online at https://www.usenix.org/conference/healthtech14/summit-program/presentation/liang.

Presentation describes approaches to projecting information from wristband monitor (eg FitBit) to nearby displays securely, with little user interaction, and without hardware modifications. Suggested approach involves a light-sensing monitor detecting light from screen. (No paper - workshop presentation only)
[cluster-devices, security]

[16] Xiaohui Liang, Ronald Peterson, and David Kotz. Securely connecting wearables to ambient displays with user intent. *IEEE Transactions on Dependable and Secure Computing*, page 1, May 2018. DOI 10.1109/TDSC.2018.2840979.

Paper describes the LightTouch system for displaying wristband information securely on nearby displays, coordinating by using an ambient light sensor on the wristband and light output by the display. Experiments demonstrate the feasibility, security, and reliability of the approach. See earlier version liang:lighttouch.
[cluster-devices, security]

[17] Xiaohui Liang, Ronald Peterson, and David Kotz. Securely Connecting Wearables to Ambient Displays with User Intent. *IEEE Transactions on Dependable and Secure Computing*, 17(4) pages 676–690, July 2020. DOI 10.1109/TDSC.2018.2840979.

This journal paper builds on and summarizes work reported in an earlier (2018) INFOCOM paper on a system for displaying wristband information securely on nearby displays, coordinating by using an ambient light sensor on the wristband and light output by the display. Experiments demonstrate the feasibility, security, and reliability of the approach.
[cluster-devices, security]

[18] Xiaohui Liang, Tianlong Yun, Ron Peterson, and David Kotz. Secure System For Coupling Wearable Devices To Computerized Devices with Displays. U.S. Patent 10,581,606, March 2020. Online at https://patents.google.com/patent/US20170279612A1/en.

Priority date 2014-08-18, Grant date 2020-03-03. Patent describes a system enabling information from mobile health sensors (eg Fitbit) to be displayed onto nearby screens without being affected by local security threats. The scheme uses visible light sensor on the mobile device. See papers liang:lighttouch and liang:jlighttouch.
[cluster-devices, security]

[19] Xiaohui Liang, Tianlong Yun, Ronald Peterson, and David Kotz. LightTouch: Securely Connecting Wearables to Ambient Displays with User Intent. In *IEEE International Conference on Computer Communications (INFOCOM)*. IEEE, May 2017. DOI 10.1109/INFOCOM.2017.8057210.

Paper describes a system enabling information from mobile health sensors (eg Fitbit) to be displayed onto nearby screens without being affected by local security threats. The scheme uses visible light sensor on the mobile device. Prototype system built and evaluated. See journal version liang:jlighttouch.
[cluster-devices, security]

[20] Rui Liu, Cory Cornelius, Reza Rawassizadeh, Ron Peterson, and David Kotz. Poster: Vocal Resonance as a Passive Biometric. In *International Conference on Mobile Systems, Applications, and Services (MobiSys)*, page 160. ACM, June 2017. DOI 10.1145/3081333.3089304.

Poster reports on a system to use a device with a contact microphone to receive acoustic (speech) signals transmitted through the body and to use these signals to authenticate the wearer of the device. The speaker must first have gone through an enrollment process. Reported accuracy of recognition is good.
[cluster-devices, experiment, implementation, security]

[21] Anthony Louie. *Information leakage in mobile health sensors and applications*. PhD thesis, University of Illinois at Urbana-Champaign, June 2014. Online at https://thawproject.files.wordpress.com/2014/07/anthony-louie-final-information-leakage-in-mobile-health-sensors-and-applications.pdf.

(Senior Honors Thesis) surveys characteristics of several specific mobile health sensing devices, considers potential security vulnerabilties in them, discusses the severity of threats against them and lists potential research topics.

[cluster-devices, security, vulnerabilities]

[22] Shrirang Mare. *Seamless authentication for ubiquitous devices*. PhD thesis, Dartmouth College, Hanover, NH, May 2016. Online at http://www.cs.dartmouth.edu/reports/TR2016-793.pdf.

Ph.D. Dissertation focuses on usable and continuous authentication, starting with user studies, developing the concept of bilateral authentication, and culminating in development of a seamless authentication method for desktops and smartphones that employs a wristband to detect motions of the user that can be correlated wtih inputs observed from the authenticated user's desktop or smartphone. Available as Dartmouth Computer Science Technical Report TR2016-793.

[cluster-devices, experiment, medical-systems, security]

[23] Shrirang Mare, Andrés Molina-Markham, Cory Cornelius, Ronald Peterson, and David Kotz. ZEBRA: Zero-Effort Bilateral Recurring Authentication. In *IEEE Symposium on Security and Privacy*, pages 705–720. IEEE, May 2014. DOI 10.1109/SP.2014.51.

Observing problems with current approaches to continuous authentication of users at keyboards, the paper proposes ZEBRA. In ZEBRA, a user wears a bracelet (with a built-in accelerometer, gyroscope, and radio) on her dominant wrist. When the user interacts with a computer terminal, the bracelet records the wrist movement, processes it, and sends it to the terminal. The terminal compares the wrist movement with the inputs it receives from the user (via keyboard and mouse), and confirms the continued presence of the user only if they correlate. This project has been renamed CSAW. Note: since the time this paper was published we have learned of a relevant trademark on the name 'Zebra'. Thus, we have renamed our approach 'CSAW' and will use that name in future publications.

[cluster-devices, security]

[24] Shrirang Mare, Andrés Molina-Markham, Cory Cornelius, Ronald Peterson, and David Kotz. ZEBRA: Zero-Effort Bilateral Recurring Authentication (Companion report). Technical Report TR2014-748, Dartmouth College, Computer Science, Hanover, NH, May 2014. Online at http://www.cs.dartmouth.edu/reports/abstracts/TR2014-748/.

Technical report providing additional details and depth on ZEBRA, a system for providing continuous authentication for users of keyboard input devices. This project has been renamed CSAW. Note: since the time this paper was published we have learned of a relevant trademark on the name 'Zebra'. Thus, we have renamed our approach 'CSAW and will use that name in future publications.

[cluster-devices, security]

[25] Shrirang Mare, Andrés Molina-Markham, Ronald Peterson, and David Kotz. System, Method and Authorization Device for Biometric Access Control to Digital Devices. U.S. Patent 9,832,206, November 2017. Online at http://www.cs.dartmouth.edu/~dfk/papers/mare-patent9832206.pdf.

Patent covers technology reported under 'SAW' project papers for continuous authentication of users of medical systems through motion-detecting wristbands.

[cluster-devices, medical-systems, security]

[26] Shrirang Mare, Reza Rawassizadeh, Ronald Peterson, and David Kotz. SAW: Wristband-based authentication for desktop computers. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT) (Ubicomp)*, 2(3), September 2018. DOI 10.1145/3264935.

Paper describes a wristband device that, by detecting motions of the wearer's wrist and conveying these to a monitor, permits those motions to be correlated (or not) with the motions of an authenticated user. In this way, if the authenticated wearer of the wristband is replaced by another user at the same workstation, for example, the new user's inputs will not correlate with the wristband of the authenticated user. In this way, the device provides a means for continuous authentication.

[cluster-devices, experiment, medical-systems, security]

[27] Shrirang Mare, Reza Rawassizadeh, Ronald Peterson, and David Kotz. Continuous Smartphone Authentication using Wristbands. In *Proceedings Workshop on Usable Security*. Internet Society, February 2019. DOI 10.14722/usec.2019.23013.

Building on prior work, the paper describes a method (CSAW) for proving continuous authentication between a user and a smartphone through use of a wristband worn by the same user. The method correlates motions detected by the wristband with those detected by the smartphone. In a study of CSAW with 11 participants, CSAW could verify the user with 96.5% accuracy every 2 seconds during continuous phone use.

[cluster-devices, design, experiment, implementation, validation]

[28] Paul D. Martin, David Russell, Aviel D. Rubin, Stephen Checkoway, and Malek Ben Salem. Sentinel: Secure Mode Profiling and Enforcement for Embedded Systems. In *IEEE/ACM International Conference on Internet-of-Things Design and Implementation (IoTDI)*. IEEE, April 2018. DOI 10.1109/IoTDI.2018.00020.

Paper reports on Sentinel, a secure mode profiler for embedded devices. Sentinel uses a bus-tapping interface to derive a partial control flow graph during device operation. The control flow graph can then be used to audit device execution and detect deviations, which may be attacks.

[cluster-devices, security]

[29] Andrés Molina-Markham, Shrirang Mare, Ronald Peterson, Jr., and David Kotz. Continuous Seamless Mobile Device Authentication Using a Separate Electronic Wearable Apparatus. U.S. Patent 9,961,547, May 2018. Online at https://www.cs.dartmouth.edu/~dfk/papers/molina-markham-patent9961547.pdf.

The invention is a wearable device whose motions can be correlated to inputs to a mobile device. The inventions supports continuous authentication for users wearing the device.

[cluster-devices, design, implementation]

[30] Timothy J Pierson, Xiaohui Liang, Ronald Peterson, and David Kotz. Demo: Wanda, Securely Introducing Mobile Devices. In *International Conference on Mobile Systems, Applications, and Services Companion (MobiSys Companion)*, page 113. ACM, June 2016. DOI 10.1145/2938559.2938581.

Demonstration of novel device that exploits the differences in signals received over two antennas separated by a half wavelength to associate a wi-fi enabled device with a wi-fi network.

[cluster-devices, experiment, security, validation]

[31] Timothy J Pierson, Xiaohui Liang, Ronald Peterson, and David Kotz. Apparatus for Securely Configuring A Target Device and Associated Methods. U.S. Patent 10,574,298, February 2020. Online at https://patents.google.com/patent/US20180191403A1/en.

This is a patent. Priority date 2015-06-23, Grant date 2020-02-25. Patent based on 'Wanda' device, described in other publications. Device implements a scheme for single antenna wi-fi device to determine its proximity to another wi-fi device with which it is communicating, in order to assure it is not unwittingly communicating with a distant adversary device rather than a nearby device. See paper pierson:wanda.

[cluster-devices, security]

[32] Timothy J Pierson, Travis Peters, Ronald Peterson, and David Kotz. Poster: Proximity Detection with Single-Antenna IoT Devices. In *International Conference on Mobile Computing and Networking (MobiCom)*, pages 663–665. ACM, October 2018. DOI 10.1145/3241539.3267751.

Poster describes scheme for single antenna wi-fi device to determine its proximity to another wi-fi device with which it is communicating, in order to assure it is not unwittingly communicating with a distant adversary device rather than a nearby device.

[cluster-devices, security]

[33] Timothy J. Pierson, Travis Peters, Ronald Peterson, and David Kotz. CloseTalker: Secure, Short-Range Ad Hoc Wireless Communication. In *ACM International Conference on Mobile Systems, Applications, and Services (MobiSys)*, pages 340–352. ACM Press, June 2019. DOI 10.1145/3307334.3326100.

Paper describes design, implementation, and evaluation of CloseTalker, a system that leverages multiple antennas and the physics of near-field radio to ensure wireless devices in close physical proximity can securely communicate while more distant devices cannot recover the information transmitted. CloseTalker works irrespective of device type or manufacturer and without additional hardware, out-of-band channels, complicated computation, or manual configuration.

[cluster-devices, design, implementation, testing]

[34] Timothy J. Pierson, Travis Peters, Ronald Peterson, and David Kotz. Proximity Detection with Single-Antenna IoT Devices. In *ACM International Conference on Mobile Computing and Networking (MobiCom)*, pages 1–15. ACM Press, October 2019. DOI 10.1145/3300061.3300120.

Paper describes scheme for single antenna wi-fi device to determine its proximity to another wi-fi device with which it is communicating, in order to assure it is not unwittingly communicating with a distant adversary device rather than a nearby device.

[cluster-devices, security]

[35] Timothy J Pierson, Reza Rawassizadeh, Ronald Peterson, and David Kotz. Secure Information Transfer Between Nearby Wireless Devices. In *ACM Workshop on Wireless of the Students, by the Students, and for the Students (S3)*, pages 11–13, October 2017. DOI 10.1145/3131348.3131355.

Paper proposes to facilitate secure transmission of data over short distances (less than 10 centimeters) by using one antenna of a wifi router to send the data while the other antenna transmits a jamming signal, blocking reception by devices not close by because of the inverse square law governing received power from a point source. Elsewhere referred to as JamFi.

[cluster-devices, medical-devices, security]

[36] Reza Rawassizadeh, Timothy Pierson, Ronald Peterson, and David Kotz. NoCloud: exploring network disconnection through on-device data analysis. *IEEE Pervasive Computing*, 17(1) pages 64–74, March 2018. DOI 10.1109/MPRV.2018.011591063.

Article advocates that device designers think twice about offloading mobile and wearable device storage and processing tasks to cloud services. Instead, consider a 'no-cloud' architecture for better privacy and trust, energy efficiency, network reliability, and response time.

[architecture, cluster-devices, opinion, privacy, security]

[37] Michael Rushanan, Aviel D Rubin, Denis F Kune, and Colleen M Swanson. SoK: Security and Privacy in Implantable Medical Devices and Body Area Networks. In *IEEE Symposium on Security and Privacy (S&P)*, pages 524–539. IEEE, May 2014. DOI 10.1109/sp.2014.40.

Comprehensive introduction and survey of security and privacy issues and state of knowledge in implantable medical devices and body area networks. Includes substantial graphic organizing research trends in the area.

[cluster-devices, privacy, security, survey]

[38] Sougata Sen and David Kotz. VibeRing: Using vibrations from a smart ring as an out-of-band channel for sharing secret keys. In *Proceedings of the International Conference on the Internet of Things (IoT)*, page Article#13 (8 pages). ACM, October 2020. DOI 10.1145/3410992.3410995.

Conference paper describes a scheme for assuring that an IoT device has an authenticated channel to another device, typically a smartphone the user trusts. The scheme employs a user-worn "Vibe-Ring", which generates vibrations to be received by the IoT device, which must include an accelerometer for sensing the vibrations. Design details are discussed; a prototype was built, and user studies (N=12) were conducted, demonstrating feasibilty.

[cluster-devices, design, implementation, security, testing]

[39] David J. Slotwiner, Thomas F. Deering, Kevin Fu, Andrea M. Russo, Mary N. Walsh, and George F. Van Hare. Cybersecurity vulnerabilities of cardiac implantable electronic devices: communication strategies for clinicians. *Heart Rhythm*, 15(7) page e61–e67, July 2018. DOI 10.1016/j.hrthm.2018.05.001.

Paper describes vulnerabilities/attacks on medical devices (cardiac implantable devices) and discusses whom to notify when vulnerabilities are discovered and appropriate communication methods to use. (Proceedings of the Heart Rhythm Society's Leadership Summit)

[cluster-devices, opinion, vulnerabilities]

[40] Takeshi Sugawara, Benjamin Cyr, Sara Rampazzi, Daniel Genkin, and Kevin Fu. Light Commands: Laser-Based Audio Injection Attacks on Voice-Controllable Systems. In *Proceedings of the USENIX Security Symposium (USENIX Security)*, pages 2631–2648. USENIX Association, August 2020. Online at https://www.usenix.org/conference/usenixsecurity20/presentation/sugawara.

USENIX 2020 paper and presentation describes using laser at a distance of 110 meters to stimulate audio sensors on smart speakers and thereby insert audio commands that are accepted as coming from a legitimate user. Techniques for dealing with this vulnerability are proposed.

[cluster-devices, security, vulnerabilities]

[41] Timothy Trippel, Ofir Weisse, Wenyuan Xu, Peter Honeyman, and Kevin Fu. WALNUT: Waging Doubt on the Integrity of MEMS Accelerometers with Acoustic Injection Attacks. In *IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, April 2017. DOI 10.1109/eurosp.2017.42.

Paper reports on attacks on MEMs accelerometers through acoustic signals, in detail.

[cluster-devices, security, vulnerabilities]

[42] Yazhou Tu, Sara Rampazzi, Bin Hao, Angel Rodriguez, Kevin Fu, and Xiali Hei. Trick or Heat?: Manipulating Critical Temperature-Based Control Systems Using Rectification Attacks. *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS)*, pages 2301–2315, November 2019. DOI 10.1145/3319535.3354195.

Conference paper demonstrates methods for attacking temperature sensors for control systems, leading to incorrect and possibly dangerous behavior of the temperature control mechanisms. A remote signal injection attack exploits the unintended rectification effect in operational and instrumentation amplifiers to generate a controllable DC component on the amplifier output that can be used to manipulate the sensor readings. Several methods to mitigate these attacks are explored, including a hardware anomaly detection system.

[attack, cluster-devices, experiment, sensor]

[43] Chen Yan, Hocheol Shin, Connor Bolton, Wenyuan Xu, Yongdae Kim, and Kevin Fu. SoK: A Minimalist Approach to Formalizing Analog Sensor Security. In *IEEE Symposium on Security and Privacy (SP)*, pages 233–248. IEEE, May 2020. DOI 10.1109/sp40000.2020.00026.

This IEEE S+P conference Systematization of Knowledge paper provides a framework for assessing the security of analog sensors. Contributions include a simple model for sensor security, formalisms to help predict new attack vectors, and defensive design patterns.

[cluster-devices, security, survey]

[44] Tuo Yu, Haiming Jin, and Klara Nahrstedt. WritingHacker: Audio-based Eavesdropping of Handwriting via Mobile Devices. In *ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp)*, pages 463–473. ACM, September 2016. DOI 10.1145/2971648.2971681.

Noting that the sounds from keyboards have been used to eavesdrop on content of the typed information, this paper presents WritingHacker, a prototype system which explores the possibility of audio-based eavesdropping on handwriting via mobile devices.

[cluster-devices, security, vulnerabilities]

[45] Tuo Yu and Klara Nahrstedt. ShoesHacker: Indoor Corridor Map and User Location Leakage through Force Sensors in Smart Shoes. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 3(3), September 2019. DOI 10.1145/3351278.

Paper documents a side channel attack on force detection sensors worn in shoes. The sensor data is analyzed to reconstruct building corridor maps and potentially the location of the individual in the building at the time the force data is collected. The attack takes a machine

learning approach and entails the development, also described in the paper, of an algorithm to identify when the wearer ascends or descends a typical staircase.

[cluster-devices, privacy, security]

2 Automated policy

Formulating security and privacy policies that provide both fine grained control and accountability and yet are easy to configure and use continues to be a challenging problem. THaW research reported in this cluster covers this topic and a wide range of others. All too often, apps violate policies intended by the platforms on which they run. Some early THaW work in this category revealed widespread use of unsecured internet communications by mHealth applications for Android and proposed mitigation strategies for them. Later work proposed augmenting SE-Android security controls with SEACAT, designed to support more fine-grained and flexible resource management. Genomic data security and privacy policies and enforcement are comprehensively reviewed in a THaW 2015 *ACM Computing Surveys* paper and subsequent ACM CCS tutorial paper. Concerns about disease propagation raise the question of whether two people have been in the same place at nearly the same time. Answering this question while preserving individual location privacy is the subject of THaW research on the SPICE system, which uses crowdsourcing to identify such "close encounters." The Internet of Things raises numerous privacy and security issues. Sensors in the home or elsewhere collect rich streams of data from which "recognizers" may extract sensitive information. THaW researchers proposed the development of a "decognizer" toolkit that could redact sensitive information from such a stream. Again, further work is reported in the bibliography under this cluster.

References

[1] Erman Ayday and Jean-Pierre Hubaux. Privacy and Security in the Genomic Era. In *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, pages 1863–1865. ACM, October 2016. DOI 10.1145/2976749.2976751.

Brief introduction to genomics and the security and privacy issues raised by storing and processing genomic data. This is the abstract for a tutorial at CCS based on ThaW survey paper https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4666540/.

[cluster-automated-policy, genomics, privacy, security, tutorial]

[2] Vincent Bindschaedler, Reza Shokri, and Carl A. Gunter. Plausible deniability for privacy-preserving data synthesis. *Proceedings of the VLDB Endowment*, 10(5) pages 481–492, January 2017. DOI 10.14778/3055540.3055542.

Paper proposes and analyzes an alternative criterion to differential privacy, called plausible deniability, to enable release of medical datasets without unduly compromising privacy or degrading potential analysis.

[cluster-automated-policy, privacy]

[3] Bo Chen and Klara Nahrstedt. FIS: Facial Information Segmentation for Video Redaction. In *IEEE Conference on Multimedia Information Processing and Retrieval (MIPR)*. IEEE, March 2019. DOI 10.1109/MIPR.2019.00071.

Paper proposes the Facial Information Segmentation algorithm (FIS), which combines the Harris Corner, the color information and an off-the-shelf face detection algorithm to identify

pixels revealing facial information. Evaluation is by comparison with the human trace tracking (HTT) and an off-the-shelf face detection algorithm (FD) proposed in earlier works. The result demonstrates that FD is unsuitable for video redaction. Further, compared with HTT, FIS achieves higher background preservation with negligible loss of video privacy in most cases.

[cluster-automated-policy, implementation, privacy, privacy protection technologies, validation]

[4] Bo Chen, Klara Nahrstedt, and Carl A. Gunter. ReSPonSe: Real-time, Secure, and Privacy-aware Video Redaction System. In *EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (MobiQuitous)*, pages 39–48. ACM Press, November 2018. DOI 10.1145/3286978.3286990.

Paper presents a real-time video redaction system (ReSPonSe), which aims to protect private information in personal videos according to permissions of people-in-video for other viewers to view them in the video. Video production has two stages: Encapsulation, which produces neutral videos in real-time, and Decapsulation, which provides privacy-aware video to the viewer, revealing private content of people-in-video who grants access rights to that viewer. Efficiency and accuracy of the system in protecting private information are evaluated.

[cluster-automated-policy, implementation, privacy, privacy protection technologies, validation]

[5] Soteris Demetriou, Nathaniel D. Kaufman, Jonah Baim, Adam J. Goldsher, and Carl A. Gunter. Toward an Extensible Framework for Redaction. In *Workshop on Security and Privacy for the Internet-of-Things (IoTSec)*, April 2018. Online at http://seclab.illinois.edu/wp-content/uploads/2018/06/demetriou2018toward.pdf.

The paper introduces the concept of a 'decognizer' toolkit which could be used to redact sensitive information in an image or text, complementing the function of a recognizer toolkit, which helps detect such information.

[cluster-automated-policy, medical-devices, privacy]

[6] Soteris Demetriou, Xiaoyong Zhou, Muhammad Naveed, Yeonjoon Lee, Kan Yuan, Xiaofeng Wang, and Carl A. Gunter. What's in Your Dongle and Bank Account? Mandatory and Discretionary Protection of Android External Resources. In *Network and Distributed Systems Security Symposium (NDSS)*. Internet Society, February 2015. DOI 10.14722/ndss.2015.23098.

Paper notes vulnerabilities introduced by customary use of Android privilege management for controlling external resources and introduces SEACAT to support more fine-grained and flexible resource management. SEACAT builds on the SE-Android base.

[cluster-automated-policy, design, implementation]

[7] Karan Ganju. *Inferring properties of neural networks with intelligent designs*. PhD thesis, University of Illinois at Urbana-Champaign, April 2018. Online at http://seclab.illinois.edu/wp-content/uploads/2018/06/ganju2018inferring.pdf.

M.S. Thesis reviews neural network techniques and the extent to which an attacker may infer properties of the data set used to train the network.

[cluster-automated-policy, privacy, vulnerabilities]

[8] Karan Ganju, Qi Wang, Wei Yang, Carl A. Gunter, and Nikita Borisov. Property Inference Attacks on Fully Connected Neural Networks using Permutation Invariant Representations. In *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, pages 619–633. ACM, October 2018. DOI 10.1145/3243734.3243834.

Paper studies fully-connected neural nets (FCNNs) and shows how adversarial machine learning techniques can reveal properties that the developer of the model did not intend to share.

[AI, cluster-automated-policy, machine-learning, security, vulnerabilities]

[9] Carl A. Gunter, Mike Berry, and Martin French. Decision Support for Data Segmentation (DS2): Application to Pull Architectures for HIE. In *USENIX Safety, Security, Privacy, and Interoperability of Health Information Technologies (HealthTech)*, August 2014. Online at https://www.usenix.org/conference/healthtech14/summit-program/gunter.

Short paper and video of talk describe a scheme for controlling the flow of information to physicians in accordance with a privacy policy. Paper records are physical and segmented and thereby provide some de facto privacy control. Digital records can flow more freely and transparently. The scheme introduced here involves predicates that determine whether a patient record implies a specified (potentially privacy-sensitive) condition, reducers that remove parts of a record so the condition cannot be inferred, and an inference analyzer that estimates the probability a condition can be inferred.

[cluster-automated-policy, privacy, security]

[10] Sayed H Hashemi, Faraz Faghri, Paul Rausch, and Roy H Campbell. World of Empowered IoT Users. In *IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI)*, pages 13–24. IEEE, April 2016. DOI 10.1109/iotdi.2015.39.

Noting the rise in the Internet of Things and consequent development of large aggregations of data, the paper describes a user-centric, multi-level, multiple granularity mechanism to share the data from these devices with people and organizations. Revisiting the fundamental mechanisms in security for providing protection, the proposed solution uses capabilities, access lists, and access rights following well-understood formal notions for reasoning about access. The contribution is to describe an auditable, transparent, distributed, decentralized, publication-subscription based robust mechanism and automation of these ideas in the IoT realm that is well-matched to the current generation of clouds

[architecture, cluster-automated-policy, privacy, security]

[11] Dongjing He. *Security threats to Android apps*. PhD thesis, University of Illinois at Urbana-Champaign, May 2014. Online at http://hdl.handle.net/2142/49659.

M.S. Thesis studies mHealth apps for Android, revealing widespread use of unsecured internet communications and widespread use of third party servers. The research also finds side channels in the Android platform that could be exploited by malicious users and proposes mitigation strategies.

[cluster-automated-policy, privacy, security, vulnerabilities]

[12] Shubhra Kanti Karmaker Santu, Vincent Bindschadler, ChengXiang Zhai, and Carl A. Gunter. NRF: A Naive Re-identification Framework. In *ACM Workshop on Privacy in the Electronic Society (WPES '18)*, pages 121–132, October 2018. DOI 10.1145/3267323.3268948.

De-identification of data is performed in order to enable data to be analyzed without revealing identities of study participants. But de-identification is done by rules derived from HIPAA that cannot guarantee participants are not later re-identified using outside data sources. This paper develops models that enable estimating the probability that individuals can be re-identified.

[cluster-automated-policy, experiment, privacy]

[13] Yunhui Long, Vincent Bindschaedler, and Carl A. Gunter. Towards Measuring Membership Privacy. In *arXiv*, volume 1712.09136. University of Illinois at Urbana-Champaign, December 2017. Online at http://seclab.illinois.edu/wp-content/uploads/2017/12/long2017towards.pdf.

Paper introduces the concept of Differential Training Privacy (DTP), intended to enable estimating the privacy risk to the training data of a machine-learning-based system that is posed by the release of a classifier of those data. It proposes that classifiers with DTP measures greater than 1 should not be published.

[AI, cluster-automated-policy, machine-learning, privacy]

[14] Muhammad Naveed, Erman Ayday, Ellen W Clayton, Jacques Fellay, Carl A. Gunter, Jean-Pierre Hubaux, Bradley A. Malin, and Xiaofeng Wang. Privacy in the genomic era. *ACM Computing Surveys (CSUR)*, 48(1), September 2015. DOI 10.1145/2767007.

Extensive introduction to genomic data, genomic data processing, and the privacy and security issues raised. Results of an opinion poll of an opportunistically assembled group of 61 experts are included.

[cluster-automated-policy, genomics, privacy, survey]

[15] Aarathi Prasad. *Privacy-preserving controls for sharing mHealth data*. PhD thesis, Dartmouth College, Hanover, NH, May 2016. Online at http://www.cs.dartmouth.edu/reports/TR2016-794.pdf.

Ph.D. Dissertation covers development of two systems, ENACT and SPICE, that enable mobile users to collect and share health information within the bounds of user privacy requirements. Focus groups are used to understand human sharing and privacy concerns. Available as Dartmouth Computer Science Technical Report TR2016-794.

[architecture, cluster-automated-policy, privacy, security]

[16] Aarathi Prasad, Xiaohui Liang, and David Kotz. Poster: Balancing Disclosure and Utility of Personal Information. In *International Conference on Mobile Systems, Applications, and Services (MobiSys)*, pages 380–381. ACM, June 2014. DOI 10.1145/2594368.2601448.

Poster proposes a web service, ShareBuddy, that is interposed between users (subjects) and data recipients so that users can understand the risks and benefits of sharing their data before they surrender it. In addition to the web service, ShareBuddy software resides on both the subject's and recipient's devices (smartphones).

[architecture, cluster-automated-policy, experiment, privacy]

[17] Aarathi Prasad, Xiaohui Liang, and David Kotz. SPICE: Secure Proximity-based Infrastructure for Close Encounters. In *ACM Workshop on Mobile Crowdsensing Systems and Applications (CrowdSenSys)*, pages 56–61. ACM, November 2017. DOI 10.1145/3139243.3139245.

Paper introduces SPICE, a system using crowdsourcing to identify 'close encounters' – events when system users are close to each other in space and/or time. The security model

calls for unlinkability, anonymity, and confidentiality of the information about close encounters. The system design therefore avoids the use of a trusted third party server.

[cluster-automated-policy, privacy, security]

[18] Güliz Seray Tuncay, Soteris Demetriou, Karan Ganju, and Carl A. Gunter. Resolving the Predicament of Android Custom Permissions. In *Network and Distributed System Security Symposium (NDSS)*. Internet Society, February 2018. DOI 10.14722/ndss.2018.23210.

Paper describes weakness in Android runtime permissions structure, which allows untrusted apps to set custom permissions, which are then treated the same as system permissions. A fix called Cusper, which allows custom permissions to be distinguished from system permissions, is proposed, implemented, and analyzed.

[cluster-automated-policy, security]

[19] Tuo Yu. *Two faces of Mobile Sensing*. PhD thesis, University of Illinois at Urbana-Champaign, May 2020. Online at http://hdl.handle.net/2142/107938.

Dissertation studies various vulnerabilities introduced by the incorporation of high resolution sensors in mobile devices and provides a framework for analysis. These sensors can improve device function but also ease the exploitation of side channels for information leakage. See Abstract.

[cluster-automated-policy, design, privacy, vulnerabilities]

[20] Bingyue Wang. Learning device usage in context: a continuous and hierarchical smartphone authentication scheme. Technical Report TR2016-790, Dartmouth College, Hanover, NH, March 2016. Online at http://www.cs.dartmouth.edu/reports/TR2016-790.pdf.

(Senior Honors Thesis) proposes that smartphone app access controls be based partly on user location.The idea is to combine behavioral and contextual information to support a hierarchical authentication scheme for continuous authentication. Machine learning techniques are used to learn contexts.

[cluster-automated-policy, security]

[21] Aston Zhang. *Analyzing intentions from big data traces of human activities*. PhD thesis, University of Illinois at Urbana-Champaign, May 2017. Online at http://seclab.illinois.edu/wp-content/uploads/2017/08/zhang2017analyzing.pdf.

Ph.D. Dissertation studies analysis of intentions from big data traces of human activities as a means to improve accuracy of computational models, for example in query auto-completion (QAC), both for static and mobile devices. Security and Privacy implications for some medical applications are considered.

[AI, cluster-automated-policy, machine-learning, privacy, security]

[22] Wen Zhang, You Chen, Thaddeus Cybulski, Daniel Fabbri, Carl A. Gunter, Patrick Lawlor, David Liebovitz, and Bradley Malin. Decide Now or Decide Later? In *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, pages 1182–1192. ACM, November 2014. DOI 10.1145/2660267.2660341.

Paper develops cost models for access control schemes that determine access a priori (prospective) or a posteriori (retrospective). Machine learning methods are used to classify the

correctness of the access control decisions, and a new method, termed bispective analysis, is developed to quantify the difference in cost between alternative access control schemes.

[AI, cluster-automated-policy, machine-Learning, medical-systems, security]

3 Human / Machine interaction

Many aspects of human machine interaction including the development of trust between people and machines have been explored by THaW researchers. Studies of workarounds that users employ to avoid security and privacy measures reveal that the theory of privacy as contextual integrity can help explain such behaviors. A patient who needs to provide sensor readings from home to the doctor's office must first figure out how to connect the sensor to the home network. To simplify this common problem, THaW researchers designed a clever device "Wanda" that the user need only point at or touch the device for it to be added to the network. Other work addressed the use of voice for authentication to a constrained computing environment presented by wearable health and fitness devices. Finally, the use of 3-D virtual headsets like Microsoft's HoloLens was investigated as a way to bring patient images from an emergency situation to a similarly equipped provider at a remote location.

References

[1] A J Burns, Jacob Young, Tom L Roberts, James F Courtney, and T Selwyn Ellis. Exploring the role of contextual integrity in electronic medical record (EMR) system workaround decisions: an information security and privacy perspective. *AIS Transactions on Human-Computer Interaction*, 7(3) pages 142–165, September 2015. Online at http://aisel.aisnet.org/thci/vol7/iss3/4/.

Study of how the theory of privacy as contextual integrity might explain work-arounds employed by healthcare workers with respect to security and privacy controls in Electronic Medical Record systems. Results indicate that contextual integrity provides a useful framework for understanding information transmission and workaround decisions in the health sector.

[cluster-HCI, experiment, privacy]

[2] Kevin R. Dufendach, Sabine Koch, Kim M. Unertl, and Christoph U. Lehmann. A randomized trial comparing classical participatory design to VandAID, an interactive crowdsourcing platform to facilitate user-centered design. *Methods of Information in Medicine*, April 2017. DOI 10.3414/ME16-01-0098.

Describes a software tool that enables users to customize visual interfaces to help in requirements definition. The system was used successfully by neonatal clinicians to help create a neonatal handoff tool.

[cluster-HCI, implementation, medical-systems]

[3] Tarek Elgamal, Bo Chen, and Klara Nahrstedt. Teleconsultant: Communication and Analysis of Wearable Videos in Emergency Medical Environments. In *ACM International Conference on Multimedia (MM)*, pages 1241–1242, October 2017. DOI 10.1145/3123266.3127920.

This short paper reports on a telemedicine demonstration in the context of emergency medicine. A person at the site of the emergency with a wearable camera (Microsoft HoloLens) surveys the victim and transmits images to a medical provider also wearing a

HoloLens at the remote site. Algrotithms for detecting facial droop were developed and employed to alert the provider to the state of the victim.

[architecture, cluster-HCI, medical-systems]

[4] Alexander G. Fiks, Nathalie DuRivage, Stephanie L. Mayne, Stacia Finch, Michelle E. Ross, Kelli Giacomini, Andrew Suh, Banita McCarn, Elias Brandt, Dean Karavite, Elizabeth W. Staton, Laura P. Shone, Valerie McGoldrick, Kathleen Noonan, Dorothy Miller, Christoph U. Lehmann, Wilson D. Pace, and Robert W. Grundmeier. Adoption of a portal for the primary care management of pediatric asthma: a mixed methods implementation study. *Journal of Medical Internet Research*, 18(6) page e172, June 2016. DOI 10.2196/jmir.5610.

Describes 'mixed-methods implementation study' in which patient portal was offered to pediatric asthma patients/families. Of 9133 patients invited to enroll, 237 (less than 3%) enrolled. 'Although use was associated with higher treatment engagement, our results suggest that achieving widespread portal adoption is unlikely in the short term. Implementation efforts should include workflow redesign and prioritize enrollment of symptomatic children.'

[cluster-HCI, experiment, medical-systems]

[5] James Brian Jones, Jonathan P Weiner, Nirav R Shah, and Walter F Stewart. The wired patient: patterns of electronic patient portal use among patients with cardiac disease or diabetes. *Journal of Medical Internet Research*, 17(2) page e42, February 2015. DOI 10.2196/jmir.3157.

Study reviewed weblogs of patient engagements with electronic health information portals. Specifically, logs of patients with cardiovascular disease and/or diabetes who had a Geisinger Clinic primary care provider and were registered 'MyGeisinger' Web portal users were studied. Hierarchical cluster analysis indicates that there are clusters of patients with different portal use characteristics.

[clinical-study, cluster-HCI, sampling]

[6] David Kotz and Travis Peters. Challenges to Ensuring Human Safety Throughout the Life-cycle of Smart Environments. In *ACM Workshop on the Internet of Safe Things (SafeThings)*, pages 1–7. ACM, November 2017. DOI 10.1145/3137003.3137012.

Paper lists challenges in the Internet of Things environment, and in particular what issues arise as people and 'things' move into and out of new (and old) environments. The context is challenges to safety, but many of these challenges could be posed as security challenges as well. The life cycle of 'things' – creation, deployment, configuration, renewal, disposal – provides a framework.

[architecture, cluster-HCI, opinion, security]

[7] Xiaohui Liang and David Kotz. AuthoRing: Wearable User-presence Authentication. In *ACM Workshop on Wearable Systems and Applications (WearSys)*, pages 5–10. ACM, June 2017. DOI 10.1145/3089351.3089357.

Paper introduces a device for continuous authentication – a ring with an embedded accelerometer. Software correlates user input actions with ring movements for authentication. An experimental prototype is built and evaluated.

[cluster-HCI, experiment, medical-devices, security]

[8] Rui Liu, Cory Cornelius, Reza Rawassizadeh, Ron Peterson, and David Kotz. Vocal resonance: using internal body voice for wearable authentication. *Proceedings of the ACM on Interactive, Mobile,*

Wearable and Ubiquitous Technologies (IMWUT) (UbiComp), 2(1) page Article No. 19, March 2018. DOI 10.1145/3191751.

Paper proposes that internal body voice (vocal resonance within the body, as measured by a contact microphone) can be used as a biometric. An objective is to assure the device is physically on the authenticated speaker's body, not merely nearby. Results indicate the method is a feasible authentication method.

[cluster-HCI, security]

[9] Timothy J Pierson. *Secure Short-range Communications*. PhD thesis, Dartmouth Computer Science, June 2018. Online at https://digitalcommons.dartmouth.edu/dissertations/54/.

Ph.D. Dissertation incorporates work on Wanda, SNAP, and CloseTalker (JamFi), generally addressing issues of radio communications over short distances and exploiting properties of antennas and electromagnetic waves to achieve authentication and secure communication without altering commercial products.

[cluster-HCI, medical-devices, security]

[10] Timothy J Pierson, Xiaohui Liang, Ronald Peterson, and David Kotz. Wanda: Securely Introducing Mobile Devices. In *IEEE International Conference on Computer Communications (IEEE INFOCOM)*. IEEE, April 2016. DOI 10.1109/INFOCOM.2016.7524366.

Paper introduces and describes Wanda, a device designed to simplify the introduction of target wireless devices, including blood pressure monitors and other home medical evices, into a wifi network. The device includes two antennas separated by a distance of a half wavelength. Information is transmitted by discriminating the received signal strength of packets sent over one antenna or the other. This discrimination is possible only when the device is physically close to its target. The idea is that the user merely touches or points Wanda to a nearby device and presses a button to introduce the device to the network.

[cluster-HCI, design, implementation, security]

[11] Timothy J Pierson, Xiaohui Liang, Ronald Peterson, and David Kotz. Wanda: Securely Introducing Mobile Devices – Extended Version. Technical Report TR2016-789, Dartmouth College, Hanover, NH, February 2016. Online at http://www.cs.dartmouth.edu/reports/abstracts/TR2016-789/.

Technical report providing additional details and depth on Wanda, a device to ease the introduction of wireless devices into wifi networks and in general to simplify the transmission of medical data from in-home patient monitors to remotely stored Electronic Health Records. (Expanded version of the INFOCOM 2016 paper by the same title)

[cluster-HCI, design, implementation, security]

[12] Aarathi Prasad and David Kotz. ENACT: Encounter-based Architecture for Contact Tracing. In *International Workshop on Physical Analytics (WPA)*, pages 37–42. ACM, June 2017. DOI 10.1145/3092305.3092310.

Paper proposes a problem, detecting 'close encounters' – instances where people were at the same place at slightly different times so that, if one carried a virus, the other might have been exposed to it. The idea is to be able to alert those exposed. The proposed scheme aims to protect users locational privacy and to prevent fake alerts.

[architecture, cluster-HCI, medical-systems]

[13] Reza Rawassizadeh, Chelsea Dobbins, Manouchehr Nourizadeh, Zahra Ghamchili, and Michael Pazzani. A Natural Language Query Interface for Searching Personal Information on Smartwatches. In *IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pages 679–684. IEEE, March 2017. DOI 10.1109/PERCOMW.2017.7917645.

Based on user observations, researchers develop a natural language (textual) interface to enable users to query mobile health devices (e.g. wristbands) for quantified health data (e.g. step count).

[cluster-HCI, design, implementation]

[14] Sougata Sen, Archan Misra, Vigneshwaran Subbaraju, Karan Grover, Meera Radhakrishnan, Rajesh K. Balan, and Youngki Lee. I4S: capturing shopper's in-store interactions. In *ACM International Symposium on Wearable Computers (ISWC)*, pages 156–159, October 2018. DOI 10.1145/3267242.3267259.

Paper describes a system for monitoring and recording shoppers' interactions with products on shelves in a retail environment, recording both items selected and items considered but not selected for purchase. The system incorporates information from Bluetooth Low Energy beacons, smartwatches, and smartphones. System details, implementation, evaluation covered very lightly.

[architecture, cluster-HCI, design]

[15] Lanier Watkins, Shreya Aggarwal, Omotola Akeredolu, William H Robinson, and Aviel Rubin. Tattle Tale Security: An Intrusion Detection System for Medical Body Area Networks (MBAN). In *Workshop on Decentralized IoT Systems and Security (DISS)*. Internet Society, February 2019. DOI 10.14722/diss.2019.23003.

Paper is about human machine interaction in the sense that it deals with a body area network and devices that may be sensing the state of the body. The idea is to detect intrusions into a body area network on the basis of anomalous power usage exhibited by devices in the network.

[cluster-HCI, security]

[16] Chen Yan, Kevin Fu, and Wenyuan Xu. On Cuba, diplomats, ultrasound, and intermodulation distortion. *Computers in Biology and Medicine*, v.104 pages 250–266, January 2019. DOI 10.1016/j.compbiomed.2018.11.012.

Paper proposes that disturbing sounds heard by US workers in Cuban embassy could have arison from intermodulation distortion coming from ultrasound-based sensing systems operating at different frequencies. Experiments are conducted to show that the released signals are not inconsistent with this hypothesis.

[cluster-HCI, vulnerabilities]

[17] Tuo Yu, Haiming Jin, and Klara Nahrstedt. Audio Based Handwriting Input for Tiny Mobile Devices. In *IEEE Conference on Multimedia Information Processing and Retrieval (MIPR)*. IEEE, April 2018. DOI 10.1109/MIPR.2018.00030.

Handwriting recognition system using audio signals and tabletop writing with fingers. Machine Learning and gesture tracking are used to train the system, and techniques to deal with audio multipath yield a claimed accuracy of 90-95% accuracy in laboratory environments.

[AI, cluster-HCI, experiment, machine-learning, medical-devices]

[18] Tuo Yu, Haiming Jin, and Klara Nahrstedt. ShoesLoc: In-shoe force sensor-based indoor walking path tracking. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 3(1), March 2019. DOI 10.1145/3314418.

Walking direction change and the stride length of each step made by the user are estimated based on insole sensors. A particle filter is applied to the data to improve the accuracy of the estimated walking path.

[cluster-HCI, design, implementation, validation]

[19] Tuo Yu, Haiming Jin, and Klara Nahrstedt. Mobile devices based eavesdropping of handwriting. *IEEE Transactions on Mobile Computing*, 19(7) page 1649–1663, July 2020. DOI 10.1109/TMC.2019.2912747.

Demonstrates how content of handwriting (as in patient information forms) may be deduced from audio signals generated by writing implements and recorded by nearby mobile devices in contacr with the writing surface.

[cluster-HCI, design, implementation, vulnerabilities]

[20] Tuo Yu, Haiming Jin, Wai-Tian Tan, and Klara Nahrstedt. SKEPRID: Pose and illumination change-resistant skeleton-based person re-identification. *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM) - Special Section on Deep Learning for Intelligent Multimedia Analytics*, 14(4), November 2018. DOI 10.1145/3243217.

Paper presents SKEPRID, a re-identification method that is resistant to strong pose and lighting changes. By incorporating skeleton information, the impact of changes in pose is reduced, and a set of skeleton-based illumination-independent features can be designed that significantly improves re-id accuracy. Experimental results show that SKEPRID outperforms other current approaches and confirms the benefit of handling complex poses and various illumination jointly.

[cluster-HCI, design, implementation, validation]

4 Management

The continuing evolution during the THaW grant of the CMS/ONC "Meaningful Use" criteria to encourage the adoption and use of electronic health records stimulated research to study the effects of these criteria on healthcare institutions. Results indicate that institutions satisfying stage 1 meaningful use criteria experienced a temporary reduction in external breaches but at the same time experienced an increase in internal breaches. In the longer term, such institutions do see reductions in all breaches. Reports on this work can be found in this cluster, along with several other studies relating cybersecurity and hospital management, including training of clinical IT personnel. Also included are studies of whether a data breach at a hospital leads to subsequent effects on the mortality rate at the hospital. For those hospitals that suffered data breaches, mortality rates were seen to decline less rapidly relative to other hospitals in the same geographic area.

References

[1] A. J. Burns and Eric Johnson. The evolving threat to privacy: analyzing breach data to understand the cyberthreat vector. *IT Professional*, 20(3) pages 64–72, May 2018. DOI 10.1109/MITP.2018.032501749.

Article reviews the distinct impact of data breaches involving PII, finding that these breaches are significantly larger compared to other breaches, and shows that past breaches are useful for predicting future breaches.

[cluster-management, sampling, vulnerabilities]

[2] A.J. Burns and M. Eric Johnson. Securing health information. *IT Professional*, 17(1) pages 23–29, January 2015. DOI 10.1109/MITP.2015.13.

The authors briefly describe the changing landscape of an IT-enabled healthcare ecosystem and discuss the emerging issues of mobility and security.

[cluster-management, security, survey]

[3] You Chen, Joydeep Ghosh, Cosmin A. Bejan, Carl A. Gunter, Siddharth Gupta, Abel Kho, David Liebovitz, Jimeng Sun, Joshua Denny, and Bradley Malin. Building bridges across electronic health record systems through inferred phenotypic topics. *Journal of Biomedical Informatics*, v.55 pages 82–93, June 2015. DOI 10.1016/j.jbi.2015.03.011.

The paper studies records of patient populations from two hospitals, aiming to see whether inferred phenotypes of patients provide a better match between the populations than do convenitonal billing codes. The inferred phenotypes are observed to perform better. Latent Dirichlet allocation is the basis for the generative topic modeling strategy used to infer phenotypes.

[AI, cluster-management, machine-learning, medical-systems]

[4] Sung Choi and M. Eric Johnson. Do Hospital Data Breaches Reduce Patient Care Quality? In *Workshop on the Economics of Information Security*, June 2017. Online at https://arxiv.org/pdf/1904.02058.pdf.

Paper studies hospital mortality figures, comparing those hospitals that suffered data breaches with those that didn't. Findings include that hospitals suffering breaches showed reduced declines in mortality relative to those that didn't, suggesting that the response to the breach had some negative effects on healthcare delivery.

[cluster-management, medical-systems, security]

[5] Sung J. Choi, M. Eric Johnson, and Christoph U. Lehmann. Data breach remediation efforts and their implications for hospital quality. *Health Services Research*, 54(5) pages 971–980, September 2019. DOI 10.1111/1475-6773.13203.

Journal paper reporting results of study comparing hospitals reporting data breaches with those that didn't suffer breaches. Comparision based on response times (time to electrocardiogram) and mortality for patients with myocardial infarctions (heart attack). Results indicate mean response times for breached hospitals increased slightly as did 30-day acute myocardial infarction mortality in the 3-year period following a breach.

[cluster-management]

[6] Kevin Fu and Harold Thimbleby. Ransomware: How We Can Climb Out of This Mess, June 2017. Online at https://www.healthcareitnews.com/blog/ransomware-how-we-can-climb-out-mess.

Article advocates good practices for healthcare enterprises but also buildng systems with fewer flaws to start with.

[cluster-management, security, tutorial]

[7] Tom J. Haigh and Carl Landwehr. Building Code for Medical Device Software Security. Technical report, IEEE Cyber Security, May 2015. Online at https://ieeecs-media.computer.org/media/technical-activities/CYBSI/docs/BCMDSS.pdf.

The report documents an approach to specifying security requirements for medical device software to reduce the number of security vulnerabilities in delivered medical devices.
[cluster-management, design, implementation, medical-devices, security]

[8] M. Eric Johnson and Juhee Kwon. Patient Reaction to Healthcare Data Breaches. In *INFORMS Annual Conference*, November 2015. Online at http://meetings2.informs.org/wordpress/philadelphia/files/2015/10/Tuesday.pdf.

Study of hospitals that have suffered/not suffered multiple data breaches, in relation to outpatient vistis and admissions. Finding is that hospitals with multiple breaches experience declines relative to other geographically local institutions. (Poster only)
[cluster-management, privacy, sampling, security]

[9] Joseph Kannry, Patricia Sengstack, Thankam Paul Thyvalikakath, John Poikonen, Blackford Middleton, Thomas Payne, and Christoph U. Lehmann. The chief clinical informatics officer (CCIO): AMIA task force report on CCIO knowledge, education, and skillset requirements. *Applied Clinical Informatics*, 7(1) pages 143–176, March 2016. DOI 10.4338/ACI-2015-12-R-0174.

This report outlines the role of a 'Chief Clinical Informatics Officer' and recommends appropriate training and certification for people who will fill this role.
[clinical-study, cluster-management]

[10] Juhee Kwon and M. Eric Johnson. Meaningful Information Security. In *Production and Operations Managment Society Annual Conference (POMS)*, May 2015. Online at https://www.pomsmeetings.org/ConfProceedings/060/General.

Presentation only, assessing effects of the 'meaningful use' criterion on hospital data breaches.
[cluster-management, sampling, security]

[11] Juhee Kwon and M. Eric Johnson. The Market Effect of Healthcare Security: Do Patients Care about Data Breaches? In *Workshop on the Economics of Information Security (WEIS)*, June 2015. Online at https://pdfs.semanticscholar.org/f3c4/2d80583f5d87957a9dbd8bf0bdd4db3c279d.pdf.

Study of hospitals that have suffered/not suffered multiple data breaches, in relation to outpatient vistis and admissions. Finding is that hospitals with multiple breaches experience declines relative to other geographically local institutions.
[cluster-management, privacy, sampling, security]

[12] Juhee Kwon and M. Eric Johnson. Meaningful healthcare security: does meaningful-use attestation improve information security performance? *MIS Quarterly*, 42(4) pages 1043–1067, December 2018. DOI 10.25300/MISQ/2018/13580.

Study of hospitals that have/have not achieved Stage 1 'meaningful use' certification for EHR use to see effects on security breaches. Findings include that institutions reaching Stage 1 meaningful use standards experience a temporary reduction in external breaches and at the same time experience an increase in internal breaches, but do see reductions in both types in the longer term.
[cluster-management, sampling, security]

[13] Christoph U. Lehmann, Susan Kressly, Winston W. Hart, Kevin B. Johnson, and Mark E. Frisse. Barriers to pediatric health information exchange. *Pediatrics*, 139(5), May 2017. DOI 10.1542/peds.2016-2653.

Article describes the difficulties faced by ambulatory pediatricians in exchanging patient health data electronically and calls for improving incentives for construction and use of mechanisms for this purpose.

[cluster-management, medical-systems, opinion, survey]

[14] Muhammad Naveed. Hurdles for Genomic Data Usage Management. In *IEEE Security and Privacy Workshops*, pages 44–48. IEEE, May 2014. DOI 10.1109/spw.2014.44.

Workshop paper lays out characteristics of genomic data and the consequent challenges in storing, processing, and preserving those data.

[cluster-management, genomics, opinion, privacy, security]

[15] John Poikonen, Edward Fotsch, and Christoph U. Lehmann. Response to Lapkoff and Sittig – Who watches the watchers: working towards safety for clinical decision support knowledge resources. *Applied Clinical Informatics*, 8(3) pages 945–948, September 2017. DOI 10.4338/ACI2017050081.

Appears to be response to an editorial in the journal that advocated an oversight body to help assure Electronic Health Records.

[cluster-management, opinion]

[16] Howard Silverman, Christoph U. Lehmann, and Benson Munger. Milestones: critical elements in clinical informatics fellowship programs. *Applied Clinical Informatics*, 7(1) pages 177–190, March 2016. DOI 10.4338/ACI-2015-10-SOA-0141.

Paper discussing how to incorporate the evaluation of clinical informatics fellowships into the milestones defining the path of competency from novice to expert in clinical IT career path.

[cluster-management, opinion]

[17] Andrei Sleptchenko and M. Eric Johnson. The Impact of Security in Maintaining Reliable Distributed Control Systems. In *INFORMS Annual Conference*, November 2014. Online at http://meetings2.informs.org/sanfrancisco2014/poster.html.

Poster presented at 2014 INFORMS anuual meeting; not available for download. Evidently a preliminary version of paper published in INFORMS Journal on Computing in 2015, "Maintaining secure and reliable distributed control systems." That paper presents a stochastic model of a network in which nodes may either fail or be brought down by malicious attack, and in which knowledge of state is uncertain. The paper formulates the problem and develops a linear-programming based model to optimize repair priorities. The optimal repair policy follows a threshold indicator: either work on the real failures or the suspected ones.

[cluster-management, security]

[18] Jonathan P Weiner, Susan Yeh, and David Blumenthal. The impact of health information technology and e-health on the future demand for physician services. *Health Affairs*, 32(11) pages 1998–2004, November 2013. DOI 10.1377/hlthaff.2013.0680.

Article forecasts changes in future demand for physicians and other healthcare workers as a funciton of the adoption of healthcare information technology and e-health applications, based on extensive literature review.

[cluster-management, survey]

5 Encryption and trusted computing base

Outsourcing computation to third party providers without revealing sensitive information to those providers is a significant challenge. This cluster includes THaW research applying functional encryption and some aspects of multiparty computation and homomorphic encryption to enable secure and private outsourcing of health data processing. Other papers in this cluster report on vulnerabilities in ostensibly secure trusted computing bases such as Intel's SGX, which proves to be vulnerable to side channel attacks. Isolation mechanisms in the Android platform, provided by its trusted computing base, are another object of study, as is the detection of malicious apps that run on Android platforms.

References

[1] Soteris Demetriou. *Analyzing & designing the security of shared resources on smartphone operating systems*. PhD thesis, University of Illinois at Urbana-Champaign, April 2018. Online at https://www.ideals.illinois.edu/handle/2142/100907.

Ph.D. Dissertation studies Android platform, particularly isolation mechanisms and permission model, discovers weaknesses from side channels, third party libraries and various other aspects that may be exploited by untrustworthy application, including medical apps, and proposes mitigations for them.

[cluster-crypto-tcb, design, security, vulnerabilities]

[2] Soteris Demetriou, Nan Zhang, Yeonjoon Lee, XiaoFeng Wang, Carl A. Gunter, Xiaoyong Zhou, and Michael Grace. HanGuard: SDN-driven Protection of Smart Home WiFi Devices from Malicious Mobile Apps. In *ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, pages 122–133. ACM, July 2017. DOI 10.1145/3098243.3098251.

Paper presents an architecture for protecting IoT devices from some classes of threats, using concepts borrowed from Software-Defined Networking. Prototype implementations are developed and tested.

[architecture, cluster-crypto-tcb, implementation, security]

[3] Gabriel Kaptchuk, Matthew Green, and Aviel Rubin. Outsourcing Medical Dataset Analysis: A Possible Solution. In *Financial Cryptography and Data Security (FC)*, volume LNCS 10322, pages 98–123. Springer, Cham, April 2017. DOI 10.1007/978-3-319-70972-7_6.

The paper documents an effort to support outsourcing of medical data analysis without resorting to a trusted third party. Currently available methods for fully homomorphic encryption and differential privacy are described and applied in the context of a dataset of 2.5 million patient encounters, cost is considered, and the researchers conclude that the methods are practical.

[cluster-crypto-tcb, privacy, security]

[4] Kevin Kornegay and Willie Lee Thompson II. Decentralized Root-of-Trust Framework for Heterogeneous Networks, November 2020. Online at https://patents.google.com/patent/US20180196945A1/en.

A patent regarding an architecture comprised of distributed trusted platform modules (TPMs) configured to establish a root-of-trust.

[IoT, TPM, cluster-crypto-tcb, patent]

[5] Paul D. Martin, Michael Rushanan, Thomas Tantillo, Christoph U. Lehmann, and Aviel D. Rubin. Applications of Secure Location Sensing in Healthcare. In *ACM International Conference on Bioinformatics, Computational Biology, and Health Informatics (BCB)*, pages 58–67. ACM, October 2016. DOI 10.1145/2975167.2975173.

Paper describes a beacon system that provides authenticated location information and so is not subject to spoofing attacks that Apple iBeacon could be. Application to medical device asset tracking and other areas.

[cluster-crypto-tcb, design, medical-devices, security]

[6] Muhammad Naveed, Shashank Agrawal, Manoj Prabhakaran, XiaoFeng Wang, Erman Ayday, Jean-Pierre Hubaux, and Carl A. Gunter. Controlled Functional Encryption. In *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, pages 1280–1291. ACM, November 2014. DOI 10.1145/2660267.2660291.

As in functional encryption, a user is enabled to retrieve only cleartext related to a particular function of the ciphertext, rather than a complete decryption of the ciphertext. The 'Control' aspect requires that the user submit a fresh key request to the authority every time it wants to evaluate a function of the cyphertext. The paper includes protocols, implementations, and evaluations of the proposed CFE.

[cluster-crypto-tcb, implementation, security, validation]

[7] Muhammad Naveed, Manoj Prabhakaran, and Carl A Gunter. Dynamic Searchable Encryption via Blind Storage. In *IEEE Symposium on Security and Privacy (S&P)*. IEE, May 2014. DOI 10.1109/SP.2014.47.

Paper presents a new scheme for searching keywords in encrypted documents without decrypting the documents. A server is only required to support upload and download of documents, so the scheme is compatible with cloud based resources.

[cluster-crypto-tcb, privacy, security]

[8] Travis Peters, Reshma Lal, Srikanth Varadarajan, Pradeep Pappachan, and David Kotz. BASTION-SGX: Bluetooth and Architectural Support for Trusted I/O on SGX. In *International Workshop on Hardware and Architectural Support for Security and Privacy (HASP)*. ACM, June 2018. DOI 10.1145/3214292.3214295.

Paper documents an approach to provide a trusted path for data transmitted wirelessly over Bluetooth to an Intel SGX Trusted Execution Environment, eliminating the need to trust drivers, middleware, OS, or hypervisor.

[architecture, cluster-crypto-tcb, security]

[9] Travis W. Peters. A Survey of Trustworthy Computing on Mobile & Wearable Systems. Technical Report TR2017-823, Dartmouth College, May 2017. Online at http://www.cs.dartmouth.edu/reports/abstracts/TR2017-823/.

Describes current hardware/software approaches to provide security / trustworthiness on both 'unconstrained' (PC / server) platforms and 'constrained' (mobile, limited power/size) platforms.

[cluster-crypto-tcb, security, survey]

[10] Guliz S Tuncay, Soteris Demetriou, and Carl A. Gunter. Draco: A System for Uniform and Fine-grained Access Control for Web Code on Android. In *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, pages 104–115. ACM, October 2016. DOI 10.1145/2976749.2978322.

Develops in-app browser access controls for Android to support safe in-app browsing (using WebView) without heavyweight browser.

[cluster-crypto-tcb, design, implementation, security]

[11] Wenhao Wang, Guoxing Chen, Xiaorui Pan, Yinqian Zhang, XiaoFeng Wang, Vincent Bindschaedler, Haixu Tang, and Carl A. Gunter. Leaky Cauldron on the Dark Land: Understanding Memory Side-Channel Hazards in SGX. In *ACM Computer and Communications Security (CCS '17)*, pages 2421–2434, October 2017. DOI 10.1145/3133956.3134038.

Paper explores vulnerabiltiies of Intel's SGX platform, particularly memory side channel attacks.

[cluster-crypto-tcb, security, vulnerabilities]

[12] Wei Yang. *Adversarial-resilience assurance for mobile security systems*. PhD thesis, University of Illinois at Urbana-Champaign, April 2018. Online at http://seclab.illinois.edu/wp-content/uploads/2018/06/yang2018adversarial.pdf.

Ph.D. Dissertation focuses on Android app security: how to detect malicious apps, particularly based on characterizion of the app's behavior in context. Differences in structure in malware (command and control structure with remote communication) and non-malware apps Static analysis of app is part of the method.

[cluster-crypto-tcb, security, vulnerabilities]

6 Economics

Economic incentives are key influencers of both human behavior and the security features of systems. THaW research in this cluster includes determining optimal repair policies for networks where nodes may either fail or be brought down by malicious behavior and in which knowledge is uncertain. One THaW line of research has produced several auction-based models (INCEPTION, CENTURION, THESEUS) for incentivizing desired behaviors among mobile crowd sensing (MCS) participants. Studies of the effects of government regulation and both proactive and reactive investments by healthcare organizations in cybersecurity measures are also included in this cluster, as is a study that shows that, following a data breach, healthcare organization spending on advertising (presumably to recover lost reputation) increases.

References

[1] Sung J. Choi and M. Eric Johnson. Understanding the relationship between data breaches and hospital advertising expenditures. *The American Journal of Managed Care*, 25(1) pages e14–e20, January 2019. Online at https://www.ajmc.com/journals/issue/2019/2019-vol25-n1/understanding-the-relationship-between-data-breaches-and-hospital-advertising-expenditures.

Study to investigate advertising costs for healthcare institutions that have suffered data breaches. Finding is that advertising costs rise significantly in the period of two years following the breach.

[cluster-economics, sampling, vulnerabilities]

[2] Haiming Jin, Lu Su, Danyang Chen, Klara Nahrstedt, and Jinhui Xu. Quality of Information Aware Incentive Mechanisms for Mobile Crowd Sensing Systems. In *ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, pages 167–176. ACM Press, June 2015. DOI 10.1145/2746285.2746310.

Paper proposes an auction scheme to be used in mobile crowd sensing applications. The scheme takes into account an incentive for user Quality of Information (QoI). The incentive mechanism rewards higher information quality in a reverse cominatorial auction. Both single-minded and multi-minded cominatorial auctions are considered. Analysis and simulation are used to validate the model.

[cluster-economics, validation]

[3] Haiming Jin, Lu Su, Bolin Ding, Klara Nahrstedt, and Nikita Borisov. Enabling Privacy-Preserving Incentives for Mobile Crowd Sensing Systems. In *IEEE International Conference on Distributed Computing Systems (ICDCS)*, pages 344–353. IEEE, June 2016. DOI 10.1109/ICDCS.2016.50.

Paper proposes an auction scheme to be used in mobile crowd sensing applications. The scheme takes an approach based on differential privacy to protect users bid data. The scheme is analyzed and simulated to show its effectiveness.

[cluster-economics, privacy, validation]

[4] Haiming Jin, Lu Su, and Klara Nahrstedt. CENTURION: Incentivizing Multi-Requester Mobile Crowd Sensing. In *IEEE Conference on Computer Communications (INFOCOM)*. IEEE, May 2017. DOI 10.1109/INFOCOM.2017.8057111.

The paper reports a new scheme for crowd sourcing the task of sensing that addresses the case where there are multiple requestors of sensing tasks as well as multiple performers of sensing tasks (workers). A double-auction-based scheme provides the mechanism to incentivize both requestors and workers. The scheme is both analyzed and simulated to validate its properties.

[cluster-economics, validation]

[5] Haiming Jin, Lu Su, and Klara Nahrstedt. Theseus: Incentivizing Truth Discovery in Mobile Crowd Sensing Systems. In *ACM International Symposium on Mobile Ad Hoc Networking and Computing (Mobihoc)*, July 2017. DOI 10.1145/3084041.3084063.

Paper proposes a payment mechanism, THESEUS, to compensate participants in a mobile crowd sensing (MCS) system for the effort they devote to sensing. The overall scheme is designed to ensure that, at the Bayesian Nash Equilibrium of the non-cooperative game induced by Theseus, all participating workers will spend their maximum possible effort on sensing, which improves their data quality. As a result, the aggregated results calculated subsequently by truth discovery algorithms based on workers' data will be highly accurate. Analysis and simulation are employed to validate results.

[cluster-economics, validation]

[6] Haiming Jin, Lu Su, Houping Xiao, and Klara Nahrstedt. INCEPTION: Incentivizing Privacy-Preserving Data Aggregation for Mobile Crowd Sensing Systems. In *ACM International Symposium*

on Mobile Ad Hoc Networking and Computing (MobiHoc), pages 341–350. ACM, July 2016. DOI 10.1145/2942358.2942375.

Paper proposes an auction scheme to be used in mobile crowd sensing applications. The scheme takes into account an incentive, a data aggregation, and a data perturbation mechanism. The incentive mechanism rewards reliable workers and compensates their costs for sensing and privacy leakage, which meanwhile satisfies truthfulness and individual rationality. The scheme is analyzed and simulated to show its effectiveness.

[cluster-economics, validation]

[7] Juhee Kwon and M. Eric Johnson. Protecting patient data-the economic perspective of healthcare security. *IEEE Security & Privacy*, 13(5) pages 90–95, September 2015. DOI 10.1109/msp.2015.113.

Paper looks at the effects of government regulation and proactive and reactive investments by health care organizations in terms of their effects on the rate of data breaches. In organizations with more mature security programs, compliance with regulations has less effect than in organizations with less mature programs. Proactive investments are also seen as more effective than investments made in response to a breach event.

[cluster-economics, medical-systems, sampling, vulnerabilities]

[8] Andrei Sleptchenko and M. Eric Johnson. Maintaining secure and reliable distributed control systems. *INFORMS Journal on Computing*, 27(1) pages 103–117, February 2015. DOI 10.1287/ijoc.2014.0613.

Stochastic model of a network in which nodes may either fail or be brought down by malicious attack, and in which knowledge of state is uncertain. The paper formulates the problem and develops a linear-programming based model to optimize repair priorities. The optimal repair policy follows a threshold indicator: either work on the real failures or the suspected ones.

[cluster-economics, security]

7 Medicine / Epidemiology

Some THaW research has investigated "Learning Healthcare Systems" – that is, healthcare systems that incorporate digital information in a way that can lead to better treatment outcomes. Issues studied include the appropriate use of machine learning technologies to incorporate unstructured expert knowledge from web data, accurate predictions of discharge dates for neonates by applying natural language processing techniques to patient progress notes, effects of automated prescription writing systems, and more.

References

[1] Abhishek Bafna and Jenna Wiens. Learning Useful Abstractions from the Web. In *American Medical Informatics Association (AMIA) Annual Symposium*, November 2015. Online at http://www-personal.umich.edu/~wiensj/papers/AMIAAbstract2015.pdf.

Paper compares performance of alternative approaches to applying machine learning to electronic medical records. Specifically, compares conventional unsupervised dimensionality reduction techniques (e.g., Principal Component Analysis) to approaches that leverage large but unstructured expert knowledge available on the Web.

[AI, cluster-medicine, machine-learning, medical-systems]

[2] Kevin R. Dufendach and Christoph U. Lehmann. Topics in neonatal informatics: essential functionalities of the neonatal electronic health record. *NeoReviews*, 16(12) pages e668–e673, December 2015. DOI 10.1542/neo.16-12-e668.

This article describes the fundamental functionalities required in an EHR to provide safe and effective care to neonates, including neonatal data requirements and appropriate display of neonatal data; the need for the mother-infant dyad in the EHR; neonatology-specific scores; and special considerations for medication ordering, nutrition, newborn screening, transitions of care, and documentation.

[architecture, cluster-medicine, medical-systems]

[3] Charles Friedman, Joshua Rubin, Jeffrey Brown, Melinda Buntin, Milton Corn, Lynn Etheredge, Carl Gunter, Mark Musen, Richard Platt, William Stead, Kevin Sullivan, and Douglas Van Houweling. Toward a science of learning systems: a research agenda for the high-functioning learning health system. *Journal of the American Medical Informatics Association (JAMIA)*, 22(1) pages 43–50, January 2015. DOI 10.1136/amiajnl-2014-002977.

Paper reports the results of a workshop to identify research challenges in the development of a comprehensive healthcare system that is able to learn from the data it collects and accumulates.

[cluster-medicine, medical-systems]

[4] Jessica A. George, Paul S. Park, Joanne Hunsberger, Joanne E. Shay, Christoph U. Lehmann, Elizabeth D. White, Benjamin H. Lee, and Myron Yaster. An analysis of 34,218 pediatric outpatient controlled substance prescriptions. *Anesthesia & Analgesia*, 122(3) pages 807–813, March 2016. DOI 10.1213/ANE.0000000000001081.

Study of the efficacy of a computerized prescription writer that has been in use since 2007. Study concludes the tool 'eliminated most but not all the errors common to handwritten prescriptions.'

[clinical-study, cluster-medicine, validation]

[5] Stephane M. Meystre, Christian Lovis, T. Bürkle, Gabriella Tognola, Andrius Budrionis, and Christoph U. Lehmann. Clinical data reuse or secondary use: current status and potential future progress. *Yearbook of Medical Informatics*, 26(01) pages 38–52, August 2017. DOI 10.15265/iy-2017-007.

The paper reviews research in clinical data reuse or secondary use by surveying the literature published from 2005 - 2016 in MEDLINE (via PUBMED),conference proceedings, and the ACM Digital Library. It concludes that this fast-growing field holds promise for achieving high quality healthcare, improved healthcare management, reduced healthcare costs, population health management, and effective clinical research.

[cluster-medicine, survey]

[6] Michael L. Rinke, Hardeep Singh, Moonseong Heo, Jason S. Adelman, Heather C. O'Donnell, Steven J. Choi, Amanda Norton, Ruth E. K. Stein, Tammy M. Brady, Christoph U. Lehmann, Steven W. Kairys, Elizabeth Rice-Conboy, Keri Thiessen, and David G. Bundy. Diagnostic errors in primary care pediatrics: Project RedDE. *Academic Pediatrics*, 18(2) page 220–227, March 2018. DOI 10.1016/j.acap.2017.08.005.

Study of diagnostic errors in pediatrics, based on randomized collection of retrospective data. Significant frequencies of diagnostic errors and missed opportunities for diagnosis were found.

[clinical-study, cluster-medicine]

[7] Aston Zhang, Xun Lu, Carl A. Gunter, Shuochao Yao, Fangbo Tao, Rongda Zhu, Huan Gui, Daniel Fabbri, David Liebovitz, and Bradley Malin. De facto diagnosis specialties: recognition and discovery. *Learning Health Systems*, 2(3), June 2018. DOI 10.1002/lrh2.10057.

Paper applies AI methods (supervised/unsupervised learning) to study records of diagnoses in relation to identified medical specialties (listed in the Health Care Provider Taxonomy Code Set) in order to identify de facto diagnosis specialties and potentially identify new specialties. Existing specialties are confirmed and new de facto specialties in breast cancer and obesity are identified.

[AI, cluster-medicine, experiment, machine-learning, validation]

8 Audit

Auditing can reveal when software doesn't live up to its promised behavior. THaW researchers have audited large numbers of Android mHealth apps to reveal security and privacy shortcomings, as well as to monitor resource usage and detect exposure of user data through libraries used by apps.

References

[1] Soteris Demetriou, Whitney Merrill, Wei Yang, Aston Zhang, and Carl A. Gunter. Free for All! Assessing User Data Exposure to Advertising Libraries on Android. In *Network and Distributed System Security (NDSS) Symposium*. Internet Society, February 2016. DOI 10.14722/ndss.2016.23082.

Paper presents a system, Pluto, for detecting the exposure of user data to ad libraries incorporated in apps. Security and privacy risks are assessed for a range of apps, and are substantial.

[cluster-audit, privacy, security, vulnerabilities]

[2] Dongjing He, Muhammad Naveed, Carl A. Gunter, and Klara Nahrstedt. Security Concerns in Android mHealth Apps. In *AMIA Annual Symposium*, volume 2014, pages 645–54, November 2014. Online at https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4419898/.

A study of a random sample of 120 out of 1080 Android mHealth apps reveals common shortcomings in security and privacy when using communications and storage.

[cluster-audit, sampling, vulnerabilities]

[3] Qi Wang, Wajih Ul Hassan, Adam Bates, and Carl A. Gunter. Fear and Logging in the Internet of Things. In *Network and Distributed System Security Symposium (NDSS)*. Internet Society, February 2018. DOI 10.14722/ndss.2018.23282.

Paper proposes a platform-centric scheme for collecting audit data from IoT devices and providing provenance.

[architecture, cluster-audit, privacy, security]

[4] Ting-Yu Wang, Haiming Jin, and Klara Nahrstedt. mAuditor: Mobile Auditing Framework for mHealth Applications. In *ACM MobiHoc Workshop on Pervasive Wireless Healthcare (MobileHealth)*, pages 7–12. ACM, June 2015. DOI 10.1145/2757290.2757291.

Paper reports on a framework for real-time auditing of resource usage (network bandwidth and sensor access) of mHealth apps. Android logs are parsed and analyzed, and experimental results are reported.

[architecture, cluster-audit, implementation, security]

9 Other

Documents in this cluster include research agendas, viewpoints and perspectives, book introductions, and letters responding to other published works.

References

[1] Abhishek Bafna and Jenna Wiens. Automated Feature Learning: Mining Unstructured Data for Useful Abstractions. In *IEEE International Conference on Data Mining*, pages 703–708. IEEE, November 2015. DOI 10.1109/icdm.2015.115.

Paper describes an unsupervised feature-learning framework for building useful abstractions for categorical data. The method involves using unstructured data from the web to learn a hierarchincal Pachinko allocation model to discover a set of latent variables. Non-uniform distances among the variables are accounted for using the Earth Mover's Distance. A case study based on a healthcare application is reported.

[AI, cluster-other, experiment, machine-learning]

[2] Bo Chen, Zhisheng Yan, Haiming Jin, and Klara Nahrstedt. Event-driven stitching for tile-based live 360 video streaming. In *ACM Multimedia Systems Conference (MMSys '19)*, pages 1–12. ACM Press, June 2019. DOI 10.1145/3304109.3306234.

Paper presents an event-driven stitching algorithm for tile-based 360 video live streaming, which abstracts various semantic information as events and makes tiling scheme decisions based on a tile actuator. A streaming system is implemented based on an event-driven stitching scheme called LiveTexture. Evaluation by comparison with other baseline systems and shows that LiveTexture adapts well to various timing budgets by meeting 89.4% of the timing constraints while utilizing timing budget more efficiently.

[cluster-other, design, implementation, testing]

[3] Kevin Fu, John Halamka, Jack Kufahl, and Mary Logan. Commentary: Hospitals need better cybersecurity, not more fear, September 2016. Online at https://www.modernhealthcare.com/article/20160914/NEWS/160919950/commentary-hospitals-need-better-cybersecurity-not-more-fear.

Short opinion piece motivated by incident in which an investment firm publicized claimed vulnerabilities in medical devices, possibly motivated by driving movements in stock prices for the device manufacturer. The authors argue for a more disciplined and cooperative approach among researchers, vendors, and regulators so that reactions to vulnerabilities will be driven by knowledge rather than fear. The authors look toward a day when partnerships

between healthcare delivery professionals and device developers will enable devices and systems with stronger security properties.

[cluster-other, opinion]

[4] Reinhold Haux, Antoine Geissbuhler, Justice Holmes, Marie-Christine Jaulent, Sabine Koch, Casimir A. Kulikowski, Christoph U. Lehmann, Alexa T. McCray, Brigitte Séroussi, Lina Fatima Soualmia, and Jan H. van Bemmel. On contributing to the progress of medical informatics as publisher. *Yearbook of Medical Informatics*, 26(01) pages 9–15, August 2017. DOI 10.15265/iy-2017-003.

Paper is a laudatory account of the history of Dieter Breggeman as a publisher of bioinformatics journals and proceedings.

[cluster-other, opinion]

[5] M. Eric Johnson. Healthcare in the Age of Analytics, October 2015. Online at https://pubsonline.informs.org/editorscut/healthcareanalytics.

This is a curated website published by INFORMS that organizes some of the literature and podcasts in the general area of analytics applied to healthcare.

[cluster-other, medical-systems, survey]

[6] David Kotz, Kevin Fu, Carl A. Gunter, and Avi Rubin. Security for mobile and cloud frontiers in healthcare. *Communications of the ACM*, 58(8) pages 21–23, August 2015. DOI 10.1145/2790830.

Viewpoint calls out research challenges in healthcare systems security and privacy, including usable authentication, trustworthy control of medical devices, and trust through accountability.

[cluster-other, opinion, privacy, security]

[7] David Kotz, Carl A. Gunter, Santosh Kumar, and Jonathan P. Weiner. Privacy and security in mobile health: a research agenda. *Computer*, 49(6) pages 22–30, June 2016. DOI 10.1109/MC.2016.185.

Paper identifies health IT privacy and security challenges and proposes a research agenda to address issues in data sharing and consent management, access control and authentication, confidentiality and anonymity, behavioral privacy, continuous and unintended sensing, multiple-use sensors, mHealth smartphone apps, policies and compliance, accuracy and data provenance, and security technology.

[cluster-other, opinion, privacy, security, survey]

[8] Christoph U. Lehmann, Marie-Christine Jaulent, and Brigitte Séroussi. *Silver Anniversary: 25 Editions of the IMIA Yearbook*, volume Suppl 1. Yearbook of Medical Informatics, May 2016. DOI 10.15265/IYS-2016-s041.

Introduction to silver anniversary IMIA yearbook edition.

[cluster-other, opinion]

[9] Christopher U. Lehmann, Hyeoun-Ae Park, Edward H. Shortliffe, and Patrice Degoulet. The international academy of health sciences informatics: an academy of excellence. *Yearbook of Medical Informatics*, 26(01) pages 7–8, August 2017. DOI 10.15265/IY-2016-015.

Brief article announces the creation of the International Academy of Health Sciences Informatics and the membership of the inaugural membership class. The IAHSI is intended to be a national academy-like organization.

[cluster-other, opinion]

[10] Amy Tsou, Christoph Lehmann, Jeremy Michel, Ronni Solomon, Lorraine Possanza, and Tejal Gandhi. Safe practices for copy and paste in the EHR: systematic review, recommendations, and novel model for health IT collaboration. *Applied Clinical Informatics*, 8(01) pages 12–34, January 2017. DOI 10.4338/ACI-2016-09-R-0150.

Systematic literature review of publications addressing frequency, perceptions/attitudes, patient safety risks, existing guidance, and potential interventions and mitigation practices for the use of copy and paste operations in EHRs. Provides four best practice recommendations. [clinical-study, cluster-other, survey]

10 Conclusion

NSF's investment in the Trustworthy Health and Wellness grant has led to significant advances in understanding what is required for future more trustworthy, secure, and usable healthcare systems both for patients and for physicians, and how our aspirations for such systems may be achieved in practice. This annotated bibliography is provided both as documentation of that progress and as a tool for others to use in building upon it.

Acknowledgements

Many thanks to Shengsong (Peter) Gao for his assistance in collecting, verifying, and organizing THaW references prior to early drafts of this work. This research results from a research program supported by the National Science Foundation under award numbers CNS-1329686, 1329737, 1330142, and 1330491. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the sponsors.