Wunderliche Sensoren im Internet der Dinge

Verena Traubinger

Projekt „Miteinander“, Professur Medieninformatik, Technische Universität Chemnitz

verena-agathe.traubinger@informatik.tu-chemnitz.de

Zusammenfassung

Im Internet der Dinge (IoT) gibt es viele Vorgänge, die für Nutzer_innen nicht nachvollziehbar sind. Eine Antwort von HCI–Forscher_innen und Designer_innen darauf sind Critical Designs, die versuchen, die Nutzer_innen zu sensibilisieren. Eine Konfrontation mit Schwachstellen im System soll ihnen die Auswirkungen von IoT im Alltag bewusst machen In dieser Studie wird ein kritisches Design entwickelt und getestet, das unerwartete und fehlerhafte Rückmeldungen zurückgibt und so zur Reflexion einladen soll.

1 Einleitung

HCI–Forscher_innen diskutieren schon seit Jahren über die invasiveren Eingriffe von IoT–Systemen in die Privatsphären der Nutzer_innen und kritisieren die fehlende Nachvollziehbarkeit der Designs (Fritsch et al., 2018).

Das Konzept des „Critical Design“, 2001 von Dunne und Raby vorgestellt, ist ein Designansatz, der dieser Entwicklung entgegengesetzt werden kann. Bardzell und Bardzell (2013) führen die Wurzeln des Critical Design auf die „Kritische Theorie“ der Frankfurter Schule zurück. Auf den Designprozess umgelegt, soll durch die Reflexion, die das Design anstoßen kann, eine kritischere Haltung in der Öffentlichkeit entstehen und Designer angeregt werden, ihre eigenen Entwürfe zu reflektieren. Ein Critical Design soll durch die Benutzung aufzeigen, welche Annahmen, Ideologien, Werte, und Verhaltensnormen mit ihm und ähnlichen Produkten verbunden sind.

Für partizipative Forschung im Bereich „IoT im Zuhause“ wurde eine „Sensor Probe“ entwickelt (Berger et al., 2018), die in dieser Arbeit als technische Grundlagen dient. Bei der Sensor Probe handelt es sich um eine „Technology Probe“ (Hutchinson et al., 2003), inspiriert vom Konzept der „Cultural Probes” (Gaver 1999), und ist mit Sensoren, Aktuatoren und einem Raspberry Pi ausgestattet. Mit der Sensor Probe wurde hier ein Critical Design entwickelt, das ein stärkeres Bewusstsein zum Umgang mit Sensordaten aus der unmittelbaren Privatheit, also

Veröffentlicht durch die Gesellschaft für Informatik e. V. 2018 in
R. Dachselt, G. Weber (Hrsg.):
Mensch und Computer 2018 – Tagungsband, 02.–05. September 2018, Dresden.
 https://doi.org/10.18420/muc2018-mci-0408

der eigenen Wohnung, schaffen soll. Die Rückmeldungen des Systems an die Benutzer_innen werden verändert, um bei diesen eine Reflexion über ihr Vertrauen in die Technik anzustoßen. Dazu werden die im Kapitel 2 zusammen getragenen Strategien verwendet, um das IoT–System zu verfremden und Partizipant_innen zu einer Reaktion auf die Veränderungen in der gewohnten Benutzung zu bringen. Dabei wird erwartet, dass ein Misstrauen zu dem System entsteht und die Rückmeldungen aktiv hinterfragt werden. Über mehrere Workshops wurden Möglichkeiten für ein kritisches IoT–Design entworfen, von denen eines gebaut wurde. Im Folgenden werden Entwicklung und Aufbau des IoT–Systems, das Studiendesign und auch vorläufige Ergebnisse aus der ersten Feldphase besprochen.

2 Related Work

In ihrer Studie verwenden Khovanskaya et al. (2013) ein Browsertool um den Nutzer_innen mittels Benachrichtigungen die Art und das Ausmaß der gesammelten Daten aufzuzeigen. Sie verwenden drei Ansätze zur Formulierung: „Make it Creepy“, „Make it Malfunction“ und „Make it Strange“. Diese so veränderten Nachrichten stoßen durch ihre ungewohnte Sprache und Inhalte die Teilnehmer_innen zur Reflexion an: „Did you know that we’ve been recording your activity for 5 days? In that time we’ve seen you online for 200 total hours and recorded more than 200 sites you’ve visited.“ Dass nicht nur Inhalt und Sprache für ein Critical Design genutzt werden können, zeigen Pierce und Paulos (2014). Bei ihrer Methode der Zweckentfremdung ist der ursprüngliche Gegenstand zwar äußerlich erkennbar, hat aber wesentliche Funktionalitäten so verändert, dass der gewohnte und intendierte Gebrauch nicht mehr möglich ist. Sie verdeutlichen dies mit Digitalkameras, die beispielsweise nur eine begrenzte Zahl an Bildern aufnehmen oder dies zufällig und nicht durch das Drücken eines Knopfes auslösen; gegensätzlich dazu werben Hersteller mit immer größeren Speicherkapazitäten und ständiger Verfügbarkeit. Bei vernetzten Systemen werden die meisten Gefahren durch Angriffe von außen erwartet. Schurgot, et al. (2015) beschreiben, wie sich Anwender_innen durch Datenverfremdung gegen Angriffe wehren können. Bei einem einfachen IoT–System, das sie in einem Wohnraum installieren, werden die erzeugten Daten teilweise künstlich erzeugt, nicht weitergegeben oder zeitlich verzögert. Die Personen, die dieses System nutzen, wissen, auf welche Art die Daten verfälscht werden und können dies in der Weiterverarbeitung berücksichtigen. Menschen, die sich allerdings von außen unerlaubt Zugriff verschaffen, werden verwirrt, da sie den Wahrheitsgrad der angezeigten Daten nicht einschätzen können oder einfach nicht von verfälschten Daten ausgehen.

3 Studiendesign

Die zuvor vorgestellten Critical Designs dienen im Weiteren gleichzeitig als Inspiration und Grundlage. Jenseits des Critical Designs herrscht die allgemeine Annahme vor, IoT–Systeme liefen stets reibungslos und seien grundsätzlich mit einem Mehrwert für die Nutzer_innen angelegt (Fritsch et al., 2018). Diese Erwartungen werden in dem hier vorgestellten Studiendesign im Sinne der Zweckentfremdung (Pierce & Paulos, 2014) verdreht.

Für diese Studie wurden von der zuvor entwickelten Sensor Probe (Berger et al., 2018) nur die drei „SensorTags" (Texas Instruments, 2018) mit je acht Umwelt- und Lagesensoren (Luftfeuchtigkeit, Luftdruck, Raum- und Objekttemperatur, Beleuchtungsstärke, Accelerometer, Gyroskop, Magnetometer) und der Raspberry Pi verwendet. Die Programmierumgebung Node–RED erkennt durch festgesetzte Schwellwerte und Wertebereiche in den erhobenen Sensordaten bestimmte Vorgänge in der Wohnung, die über einen Messenger als Benachrichtigungen an die Teilnehmer_innen zurückgegeben werden. So stellt das System fest, dass die Sonne aufgegangen ist, sobald die Beleuchtungsstärke morgens über 2,5 Lux liegt. Nach dem gleichen Prinzip wird auch der Sonnenuntergang erkannt. Bei der Qualität des Raumklimas wird zwischen normaler, zu trockener und zu feuchter Luft unterschieden, sowie einer normalen, zu warmen und zu kühlen Raumtemperatur. Der am Kühlschrank befestigte SensorTag erzeugt durch die Drehung der Tür eine Benachrichtigung über die Anzahl der Öffnungen des Kühlschranks. Weiterhin werden die Dauer des Lüftens und der Zeitraum, in dem zwischen Mitternacht und vier Uhr morgens das Licht brennt, erkannt. Diese Ereignisse führen dazu, dass das System über einen Messenger eine Benachrichtigung ausgibt, beispielsweise: „Sie haben 13 Minuten gelüftet."

Der Systemaufbau wird eine Woche lang bei den Partizipant_innen installiert, die davon ausgehen, dass sie die Robustheit des Systems testen. Während der Woche verändert sich die Art der Benachrichtigungen so, dass die Aussagen provokanter formuliert sind und vermehrt Fehlinformationen eingestreut werden. Dazu werden je nach Zeitpunkt in der Feldphase unterschiedliche Benachrichtigungen verwendet. In den ersten drei Tagen verschickt das System einfache Rückmeldungen über die Vorgänge, am vierten und fünften Tag gibt es eine Änderung in der Ansprache und den Formulierungen, die an den letzten beiden Tagen noch verstärkt wird. So gibt es über wenige Tage hinweg eine Eskalation in der Kommunikation zwischen dem System und den Nutzer_innen. Durch die Verwendung der Methoden von Khovanskaya et al. (2013) werden die simplen Benachrichtigungen („Sie haben 13 Minuten gelüftet.") so verändert, dass sie in einen der drei Bereiche „Make it Creepy", „Make it Strange" und „Make it Malfunction" fallen („In den letzten 13 Minuten hätte ein Einbrecher statistisch gesehen 4-mal durch das Fenster kommen können.") Dabei werden auch Elemente zur Datenverfremdung (Schurgot et al., 2015) genutzt, wobei die gemessenen Zeitspannen verändert werden oder ganz wegfallen: „Im Vergleich lüften fast alle deine Nachbarn ergiebiger. Nur der gegenüber nicht."

Um zu verhindern, dass nicht nachvollziehbare Benachrichtigungen auf Mitbewohner_innen zurückgeführt werden, wird die Studie in Einzelhaushalten durchgeführt. Dort kann nur die_der Bewohner_in selbst beteiligt sein und weiß im Regelfall, an welchen Situationen sie_er beteiligt war. Am letzten Tag wird beispielsweise eine Benachrichtigung ausgegeben, die nicht auf realen Ereignissen beruht und zu einer Verunsicherung führen soll: „Heute Nacht wurde die Kühlschranktüre zwischen Mitternacht und Sonnenaufgang 3-mal geöffnet." Durch die Steigerung an Provokationen und Fehlinformationen wird zu einer kritischen Reflexion im Umgang mit persönlichen Sensordaten eingeladen. Auch nach der Studie soll diese Einstellungsänderung als Anregung für einen zukünftigen Umgang mit ähnlichen Geräten und Systemen dienen.

4 Fazit und Future Work

Nach einer ersten Feldphase zeigt sich, dass die technische Umsetzung dieses Studiendesigns funktioniert und zur Verhaltenserkennung in der Wohnung nutzbar ist. Erste Forschungsergebnisse zeigen jedoch, dass ein starkes Vertrauen in die Technik bei der Teilnehmerin dazu führt, dass die Veränderungen in der Ausgabe nicht nur hingenommen, sondern nur in ganz seltenen Fällen hinterfragt werden. Eine fehlerhafte Benachrichtigung, dass es dauerhaft zu warm im Raum sei, wurde etwa trotz gefallener Temperaturen in der Nacht zuvor nicht angezweifelt. In der ersten Phase der Benachrichtigungen wäre in der Zwischenzeit ein Hinweis auf die geänderten Temperaturen geschickt worden. Die weiteren Studienwiederholungen werden bei Personen durchgeführt, die einen technischen Hintergrund haben oder älter sind, um die Ergebnisse zuzuspitzen.

Literaturverzeichnis

Bardzell, J., & Bardzell, S. (2013, April). What is critical about critical design?. In *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 3297-3306). ACM.

Berger, A., Bischof, A., Totzauer, S., Storz, M., Lefeuvre, K. & Kurze, A. (2018). Sensing Home: Exploring the Intersection of Probes and Toolkits for the IoT in the Home. In: *i-com. Vol. 18. Nr.1. Berlin/Boston: Walter de Gruyter GmbH.*

Dunne, A., & Raby, F. (2001). *Design noir: The secret life of electronic objects.* Springer Science & Business Media.

Fritsch, E., Shklovski, I., & Douglas-Jones, R. (2018, April). Calling for a Revolution: An Analysis of IoT Manifestos. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (p. 302). ACM.

Gaver, B., Dunne, T., & Pacenti, E. (1999). Design: cultural probes. *interactions*, 6(1), 21-29.

Hutchinson, H., Mackay, W., Westerlund, B., Bederson, B. B., Druin, A., Plaisant, C., ... & Roussel, N. (2003, April). Technology probes: inspiring design for and with families. In *Proceedings of the SIGCHI conference on Human factors in computing systems*(pp. 17-24). ACM.

Khovanskaya, V., Baumer, E. P., Cosley, D., Voida, S., & Gay, G. (2013, April). Everybody knows what you're doing: a critical design approach to personal informatics. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 3403-3412). ACM.

Pierce, J., & Paulos, E. (2014, June). Counterfunctional things: exploring possibilities in designing digital limitations. In *Proceedings of the 2014 conference on Designing interactive systems* (pp. 375-384). ACM.

Schurgot, M. R., Shinberg, D. A., & Greenwald, L. G. (2015, June). Experiments with security and privacy in IoT networks. In *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2015 IEEE 16th International Symposium on a* (pp. 1-6). IEEE.

Texas Instruments Incorporated. (2018). Simplelink SensorTag - TI.com. Abgerufen am 06.07.2018 von http://www.ti.com/ww/en/wireless_connectivity/sensortag/