Dipl.-Ing.[in] Katharina Krombholz, BSc

© Martin Mulazzani/SBA Research

SBA Research gGmbH

Favoritenstraße 16
1040 Wien

Persönliches

geboren (Jahreszahl, Ort):	1987, Salzburg
Sprachen:	Deutsch (Muttersprache), Englisch, Spanisch, Portugiesisch, Französisch, Grundkenntnisse in Russisch und Japanisch
Familienstand:	ledig, in einer Beziehung
Hobbies:	Sport (Schifahren, Bikram Yoga), Singen (Chor), Reisen

Ausbildung

Seit 2013	Doktoratsstudium der technischen Wissenschaften, Informatik, Technische Universität Wien
2010 – 2012	Masterstudium Medieninformatik, Technische Universität Wien (Masterprüfung mit Auszeichnung)
2008	Erasmusstudentin an der Universidade de Coimbra (Portugal)
2005 – 2010	Bachelorstudium Medieninformatik (Schwerpunkt Design), Technische Universität Wien
2005	Matura am Bundesgymnasium Zaunergasse (Salzburg)

Berufslaufbahn

Seit 2012	Researcher bei SBA Research gGmbH
Seit 2014	Universitätslektorin an der Technischen Universität Wien (Digital Forensics, Introduction to Security)
Seit 2014	Lektorin an der FH Campus Wien (Information & Network Forensics)
Seit 2014	Lektorin an der FH Technikum Wien (Cloud Security)

2013	Dreimonatiges Forschungspraktikum am National Institute of Informatics (NII) in Tokio, Japan
2009 – 2011	Tutorin an der Technischen Universität Wien (Einführung in die Programmierung)
Sommer 2010	Praktikum bei A1 Telekom Austria in Wien (IP Multimedia Subsystem Core)
Sommer 2009	Praktikum bei T-Mobile NL in Den Haag, Niederlande (MMS Monitoring, Softwareentwicklung)
Sommer 2007	Praktikum bei Siemens PSE in Wien (Open Source Software Development)

Aktuelles Arbeitsgebiet

Meine Forschung beschäftigt sich hauptsächlich mit der Benutzbarkeit von Security- und Privacy-Mechanismen. Meist sind diese Sicherheitstechnologien für BenutzerInnen schwer verständlich, was zum einen oft zu Fehlern und Unzufriedenheit führt und zum anderen die Sicherheit des gesamten Systems gefährdet. Mit meiner Forschung will ich dazu beitragen, Sicherheitstechnologien benutzungsfreundlicher und somit auch sicherer zu gestalten.

Der Fokus meiner Forschung liegt derzeit in der Entwicklung von benutzbaren Privacy-Technologien für „Wearables“ (z.B. Smartwatches oder Datenbrillen wie Google Glass). Wearables sammeln kontinuierlich Daten der Trägerin bzw. des Trägers und der Umgebung undübertragen sie zu anderen Services. All diese Schritte implizieren Privatsphärerisiken für die BenutzerInnen, aber auch für Personen, die nur ganz zufällig von so einem Gerät erfasst werden. Insbesondere bei Geräten, die auch Personen in der Umgebung aufnehmen brauchen wir Technologien, die die analoge Lücke zwischen der ungefragt-aufgenommen Person und dem aufnehmenden Gerät schließen.

Des Weiteren beschäftige ich mich in meiner Forschung mit der Benutzbarkeit von kryptographischen Anwendungen, wie beispielsweise der dezentralen Krypto-Währung Bitcoin. Die Hauptschwierigkeit bei kryptografischen Anwendungen liegt in der Verwaltung von Schlüsseln.

Ein weiteres aktuelles Forschungsthema ist QR Code Sicherheit auf mobilen Endgeräten. QR Code Sicherheit ist wichtig, da diese Codes zur Informationsübertragung (oft auch von sensiblen Daten) verwendet werden und nicht menschenlesbar sind. Daher benötigt die/der menschliche BenutzerIn zuverlässige und benutzbare Software um QR Code-basierte Attacken zu erkennen und potentielle Schwachstellen zu schließen.

Weitere Forschungsthemen, an denen ich gearbeitet habe, beschäftigten sich mit digitaler Forensik, Hardware-Trojanern und Risikomanagement bei Cloud-Sicherheit.

Laufende (Forschungs-)projekte

P3F.at (netidee - Internet Foundation Austria)

Im Rahmen dieses Projekts entwickeln wir das Picture Privacy Policy Framework. Die Verbreitung von Digitalkameras in mobilen Geräten sowie die internetbasierte Veröffentlichung von Fotos auf Plattformen führten zu einem massiven Anstieg von Fotos mit unbeabsichtigt oder unfreiwillig fotografierten Menschen. P3F macht es möglich, Privacy Policies, also selbstgewählte Beschränkungen über die Publizierbarkeit von Fotos in Textilmuster hineinzukodieren. Dieser Ansatz basiert rein ausschließlich auf Mustererkennungsalgorithmen. Ziel ist es, Wege aufzuzeigen um die analoge Lücke zwischen Fotografien im öffentlichen Raum und zufällig fotografierten Individuen zu schließen.

DCloud (Fonds zur Förderung der wissenschaftlichen Forschung – FWF)

Im Rahmen dieses Projektes widmen wir uns dem Risikomanagement bei der Migration von Unternehmensinfrastruktur in die Cloud. Ziel ist es, eine Migrationsstrategie an Hand benutzerdefinierter Kriterien zu erarbeiten und das Risiko zu minimieren. Der Fokus liegt dabei vor allem auf Datensicherheit und Privatsphäre.

Mitgliedschaften

Association for Computing Machinery, Special Interest Group on Security, Audit and Control (ACM SIGSAC) – Vizepräsidentin des Vienna Chapter

Auszeichnungen

Mitglied des Students4Excellence High-Potential Programms (seit 2011)

Leistungsstipendium der Fakultät für Informatik an der TU Wien (2010)

Scientific Community Services

Mitglied in den Program Committees:

- 24th International World Wide Web Conference, Security & Privacy Track (/WWW 2015), http://www.www2015.it/
- The 7th/8th International Workshop on Digital Forensics (WSDF 2014 & 2015), http://www.ares-conference.eu/conference/workshops/wsdf-2015/

Ich betreue außerdem Master- und Bachelorarbeiten an der FH Technikum Wien und der Technischen Universität Wien.

Aktivitäten zur Förderung von Frauen

Gestaltung des techNIKE Workshops „Sicherheit im Internet – Facebook, WhatsApp, Instagram & Co“ (gemeinsam mit Martina Lindorfer). Dieser Workshop wurde bereits im Vorjahr vom Projekt genderfair in Kooperation mit dem wienXtra-ferienspiel angeboten und richtet sich an 10-14 jährige Mädchen. Die Gestaltung dieses Workshops liegt mir ganz besonders am Herzen, weil ich glaube, dass Mädchen schon so früh wie möglich an technische Themen herangeführt werden sollten. Der Umgang mit dem Internet und den eigenen sensiblen Daten stellt viele junge Menschen vor Herausforderungen und gerade bei Mädchen sind Sexting etc. wichtige Themen. Ziel dieses Workshops ist es daher, nicht mit „erhobenem Zeigefinger“ Regeln aufzustellen, sondern die Mädchen zu mündigen und selbstbestimmten Internetuserinnen heranreifen zu lassen, die ihr Verhalten reflektieren, sich der Implikationen ihres Handeln bewusst sind und ihre ganz eigenen Entscheidungen treffen. Schon sehr früh habe ich begonnen, an der TU Wien als Tutorin für „Einführung in das Programmieren“ zu arbeiten. Damals haben das nur ganz wenige Frauen gemacht und mein Ziel war es, für meine jüngeren Kolleginnen eine Art Vorbild bzw. Role Model zu sein, ohne jedoch Frauen zu bevorzugen. Einige junge Frauen aber auch Männer, die mein Tutorium besucht haben, sind immer noch mit mir in Kontakt und haben dann später auch gerne meine Vorlesungen besucht.

Statement „Frauen in naturwissenschaftlichen-technischen Berufen/ in der Forschung“

Ich habe mich als Frau in einem technischen Beruf eigentlich immer sehr wohl gefühlt. Die Zeit ist definitiv reif für Frauen in dieser männerdominierten Branche und ich habe mich von

meinen männlichen Kollegen immer respektiert und geschätzt gefühlt, auch wenn es natürlich Ausnahmen gab. Ich finde, wir dürfen uns nicht an diese Ausnahmen klammern und müssen über frauenfeindliche Vorfälle mit unseren KollegInnen sprechen. Kommunikation ist auch hier wohl die beste Voraussetzung! Wichtig finde ich auch, dass es weibliche Vorbilder gibt. Ich persönlich hatte immer männliche Vorbilder, ich habe aber auch schon die Erfahrung gemacht, dass einige Frauen einfach weibliche Vorbilder brauchen. Mein Ziel ist es, ein Vorbild zu sein, für weiblichen und männlichen ForscherInnenachwuchs gleichermaßen.

Ausgewählte Publikationen

K. Krombholz, A. Dabrowski, M. Smith, E.R. Weippl (2015): Ok Glass, Leave me Alone: Towards a Systematization of Privacy Enhancing Technologies for Wearable Computing, in 1st Workshop on Wearable Security and Privacy

J. Ullrich, K. Krombholz, H. Hobel, A. Dabrowski, E.R. Weippl (2015): IPv6 Security: Attacks and Countermeasures in a Nutshell, Magdeburger Journal zur Sicherheitsforschung, vol. 1

J. Ullrich, K. Krombholz, H. Hobel, A. Dabrowski, E.R. Weippl (2014): IPv6 Security: Attacks and Countermeasures in a Nutshell, in 8th USENIX Workshop on Offensive Technologies (WOOT)

K. Krombholz, P. Fruehwirt, P. Kieseberg, I. Kapsalis, M. Huber, E.R. Weippl (2014): QR Code Security: A Survey of Attacks and Challenges for Usable Security, Springer, pp. 79-90

A. Dabrowski, P. Fejes, J. Ullrich, K. Krombholz, H. Hobel, E.R. Weippl (2014): Poster NDSS 2014: Hardware Trojans–Detect and React?, Network and Distributed System Security (NDSS) Symposium 2014

A. Hudic, K. Krombholz, Th. Otterbein, Ch. Platzer, E.R. Weippl (2014): Automated Analysis of Underground Marketplaces, in Tenth Annual IFIP WG 11.9 International Conference on Digital Forensics

P. Fruehwirt, P. Kieseberg, K. Krombholz, E.R. Weippl (2014): Towards a forensic-aware database solution: Using a secured database replication protocol and transaction management for digital investigations, Digital Investigation, vol. 11, pp. 336-348

K. Krombholz, H. Hobel, M. Huber, E.R. Weippl (2014): Advanced social engineering attacks, Journal of Information Security and Applications

A. Dabrowski, H. Hobel, J. Ullrich, K. Krombholz, E.R. Weippl (2014): Towards a Hardware Trojan Detection Cycle, in Second International Workshop on Emerging Cyberthreats and Countermeasures, ARES ECTCM 2014

S. Islam, E.R. Weippl, K. (2014): A Decision Framework Model for Migration into Cloud: Business, Application, Security and Privacy Perspectives, in IIWAS 2014

A. Dabrowski, K. Krombholz, J. Ullrich, E.R. Weippl (2014): QR – Inception: Barcode in Barcode Attacks, in 4th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)

K. Krombholz, H. Hobel, M. Huber, E.R. Weippl (2013): Social engineering attacks on the knowledge worker, in Proceedings of the 6th International Conference on Security of Information and Networks, pp. 28-35

Ch. Krieg, A. Dabrowski, H. Hobel, K. Krombholz, E.R. Weippl (2013): Hardware Malware, Synthesis Lectures on Information Security, Privacy, and Trust, vol. 4, pp. 1-115

K. Krombholz, D. Merkl, E.R. Weippl (2012): Fake Identities in Social Media: A Case Study on the Sustainability of the Facebook Business Model, Journal of Service Science Research

Weiterführende Links

https://www.sba-research.org/team/researchers/katharina-krombholz/

http://scholar.google.at/citations?user=BkeawyUAAAAJ&hl=en

http://p3f.at