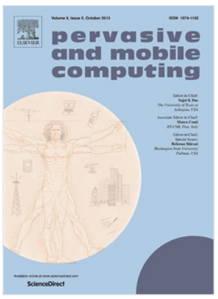
Accepted Manuscript



Moves like Jagger: Exploiting variations in instantaneous gait for spontaneous device pairing

Dominik Schürmann, Arne Brüsch, Ngu Nguyen, Stephan Sigg, Lars Wolf

PII: S1574-1192(17)30263-8
DOI: https://doi.org/10.1016/j.pmcj.2018.03.006
Reference: PMCJ 931

To appear in: *Pervasive and Mobile Computing*

Please cite this article as: D. Schürmann, A. Brüsch, N. Nguyen, S. Sigg, L. Wolf, Moves like Jagger: Exploiting variations in instantaneous gait for spontaneous device pairing, *Pervasive and Mobile Computing* (2018), https://doi.org/10.1016/j.pmcj.2018.03.006

Moves like Jagger: Exploiting variations in instantaneous gait for spontaneous device pairing☆

Dominik Schürmann[a], Arne Brüsch[a], Ngu Nguyen[b], Stephan Sigg[b], Lars Wolf[a]

[a] *Connected and Mobile Systems, Institute of Operating Systems and Computer Networks, TU Braunschweig, Mühlenpfordtstr. 23, Braunschweig, Germany*
[b] *Ambient Intelligence, Department of Communications and Networking, Aalto University, Maarintie 8, Espoo, Finland*

Abstract

Seamless device pairing conditioned on the context of use fosters novel application domains and ease of use. Examples are automatic device pairings with objects interacted with, such as instrumented shopping baskets, electronic tourist guides (e.g. tablets), fitness trackers or other fitness equipment. We propose a cryptographically secure spontaneous authentication scheme, BANDANA, that exploits correlation in acceleration sequences from devices worn or carried together by the same person to extract always-fresh secure secrets. On two real world datasets with 15 and 482 subjects, BANDANA generated fingerprints achieved intra- (50%) and inter-body (> 75%) similarity sufficient for secure key generation via fuzzy cryptography. Using BCH codes, best results are achieved with 48 bit fingerprints from 12 gait cycles generating 16 bit long keys. Statistical bias of the generated fingerprints has been evaluated as well as vulnerabilities towards relevant attack scenarios.

Keywords: gait, authentication, fuzzy cryptography, ad-hoc secure pairing

☆This paper is an extended version of "D. Schürmann, A. Brüsch, S. Sigg, L. Wolf, BANDANA – Body Area Network Device-to-device Authentication using Natural gAit".

Email addresses: schuermann@ibr.cs.tu-bs.de (Dominik Schürmann), bruesch@ibr.cs.tu-bs.de (Arne Brüsch), le.ngu.nguyen@aalto.fi (Ngu Nguyen), stephan.sigg@aalto.fi (Stephan Sigg), wolf@ibr.cs.tu-bs.de (Lars Wolf)