

Preface

The 24th International Security Protocols Workshop was held in April 2016 at the Mendel Museum of Masaryk University in Brno, Czech Republic. This former Augustinian abbey is where Gregor Mendel presented his seminal *Versuche ber Pflanzenhybriden* (Experiments on Plant Hybridization); in keeping with this location, the theme of the workshop was “Evolving Security.”

Security protocols evolve with their changing requirements, their changing mechanisms, and attackers’ changing agendas and capabilities. We saw examples of this presented at the workshop: Llewellyn-Jones, Jenkinson, and Stajano described how the Pico authentication system is evolving to support more flexible delegation mechanisms, while Pieczul and Foley brought a qualitative approach to the workshop in their longitudinal consideration of how security-sensitive software has evolved over time in one open-source software project. Sometimes, however, the evolution we see is not in security software but in the attacks against it. Jonker, Mauw, and Trujillo-Rasua described for the workshop how middleperson attacks have evolved over the years but models of them have not, while Kang, Gligor, and Sekar showed us the evolution of DDoS attacks against core Internet infrastructure. With an even more explicit Mendel connection, Ošťádal, Švenda, and Matyáš made use of genetic algorithms in the context of ad hoc network protocols to better model wireless attackers.

As is often the case, many papers and discussions did not fit the theme but were challenging and thought-provoking. We hope that all of these papers and transcripts — edited both by authors and by ourselves — will provoke further debate as our protocols and our understanding of them continue to evolve.

April 2017

Jonathan Anderson
Bruce Christianson
Vashek Matyáš
Frank Stajano

Security Protocols XXIV

24th International Workshop, Brno, Czech Republic,

April 7-8, 2016, Revised Selected Papers

Anderson, J.; Matyáš, V.; Christianson, B.; Stajano, F.
(Eds.)

2017, X, 233 p. 23 illus., Softcover

ISBN: 978-3-319-62032-9