Reverse Engineering a Java Card Memory Management Algorithm

Abdelhak Mesbah\textsuperscript{b,}\textsuperscript{*}, Jean-Louis Lanet\textsuperscript{a}, Mohamed Mezghiche\textsuperscript{b}

\textsuperscript{a}INRIA, LHS-PEC 263 Avenue Général Leclerc, 35042 Rennes, France
\textsuperscript{b}University of Boumerdes, Independence Avenue, 35000 Algeria

*Corresponding author

Email addresses: abdelhak.mesbah@univ-boumerdes.dz (Abdelhak Mesbah),
jean-louis.lanet@inria.fr (Jean-Louis Lanet), mohamed-mezghiche@univ-boumerdes.dz (Mohamed Mezghiche)

First author:
Abdelhak MESBAH is PhD student with the LIMOSE research laboratory at the University of M’HAMED BOUGARA, Algiers. He received his master’s degree in Software Engineering and Information Processing at the same university. His research interests focus on Attacks, Reverse Engineering as well as Security of smart card’s Applications and Systems.

Second author:
Jean-Louis Lanet is the director of the High Security Labs of Inria-RBA. Previously he was full Professor in the Computer Science Department at University of Limoges (2007-2014). He is also the team leader of SSD (Smart Secure Device) research group. Prior to that, he was a senior researcher at Gemplus Research Labs (1996-2007). During this period he spent two years at INRIA (Sophia-Antipolis) (2003-2005) as an engineer at DirDRI (Direction des Relations Industrielles) and as a senior research associate in the Everest team. He started his career as a researcher at Elecmca, Electronic division of the Snecma, now a part of the Safran group (1984-1995) and his field of research was on jet engine control. His research interests include security of small systems like smart cards and software engineering.

Third author:
Mohamed Mezghiche is a Professor in the Computer Science Department at the University of Boumerdes Algeria. He is also a team leader and the director of LIMOSE Laboratory at the same university. He received his Phd in theoretical computer science from the University Paris 6 (France). His research interests are formal methods, program certification, theorem proving, logic and functional programming.

Abstract

Smart cards are tamper resistant devices that manipulate assets in a secure way. Among the assets, one is of a particular interest the native layers. If some attacks have succeed in getting access to the applicative layer very few of them have had access to the native layers. We propose here to use applicative programs to perform data reverse engineering in order to understand the
دریافت فوری
متن کامل مقاله

امکان دانلود نسخه تمام متن مقالات انگلیسی
امکان دانلود نسخه ترجمه شده مقالات
پذیرش سفارش ترجمه تخصصی
امکان جستجو در آرشیو گامی از صدها موضوع و هزاران مقاله
امکان دانلود رایگان ۲ صفحه اول هر مقاله
امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
دانلود فوری مقاله پس از پرداخت آنلاین
پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات