securely connect to an online commerce site, enabling a mutually trusted relationship without the need of disclosing non-essential personal data. The second use case will focus on the enrolment process and physical access control to a secure-sensitive environment such as an airport. The airport scenario will effectively show how different derived identities, with different levels of privacy, can be used in different situations (e.g., airport access control, boarding control and duty free shops) combining attributes with different levels of assurance coming from different identity and attribute providers (e.g., national eID or passport and electronic boarding passes).

In terms of social transformation factors, ARIES will contribute to lower several barriers, including end-user acceptance, by providing a secure and privacy by design enabled solution. ARIES will endow users with the ability to anchor trust on a secure and high level assurance infrastructure that will be used to derive additional virtual identities supporting different levels of privacy-preserving and anonymization capabilities but relying on a law enforcement mechanism to obtain effective support in the event of identity-related crimes. This will make users feel more secure in these eID ecosystems, which ultimately will encourage the use of electronic identities and increase the trust in, and adoption of, ICT and online services across the EU by both citizens and businesses.

ARIES is a project that specifically aims to prevent and reduce the risk of identity theft and fraud crimes. This is achieved by the means of cryptographic links between derived, virtual and biometric identities and by the cryptographic proofs accessible at the secure wallet by law enforcement agencies that can leverage them when investigating identity crimes.

The ARIES project is a Research and Innovation Action funded by the European Commission's Horizon 2020 programme and the consortium carrying it out consists of a well-balanced mixture from six European countries consisting of industry partners, SMEs, public law enforcement bodies and also one retailer.

Links:
[L1] aries-project.eu/
[L2] twitter.com/AriesH2020

References:
[1] N. Robinson et al.: "Comparative Study on Legislative and Non Legislative Measures to Combat Identity Theft and Identity Related Crime"
[2] European Commission: "The European Agenda on Security", COM (2015) 185 final.
[3] I. Naumann, G. Hogben: "Privacy features of European eID card specifications" Network Security, Vol. 2008.

Please contact:
Nicolás Notario, Atos Research & Innovation, Spain
nicolas.notario@atos.net

Antonio Skarmeta, Jorge Bernal
Universidad de Murcia, Spain
skarmeta@um.es, jorgebernal@um.es

The KandISTI/UMC Online Open-Access Verification Framework

by Franco Mazzanti, Alessio Ferrari and Giorgio O. Spagnolo (ISTI-CNR)

ISTI-CNR provides an online open-access environment for the experimentation of design, analysis and verification of UML-based system models. Great as a didactic environment, it can successfully compete in terms of friendliness and usability with the most mainstream verification frameworks.

KandISTI [1] [L1] is an open-access, online, modelling and verification framework for software-intensive systems developed at ISTI by the FMT Laboratory. It is composed of a set of experimental analysis/verification tools (CMC, FMC, UMC, VMC) of which UMC is the most advanced component. To date, UMC has been applied to a range of case studies in the railway, automotive and telecommunications fields [2,3].

In UMC, a system is defined as a set of communicating state machines. Each state machine is described by a UML Statechart. The dynamic behaviour of a UML system can be: interactively explored; visualised as an evolutions graph; summarised by a minimal set of traces; model-checked using a parametric, branching-time state- and event-based, parametric, temporal logic.

The development of UMC started in 2001 and since then has been continuously improved with the support of several EU and regional projects (AGILE, SENSORIA, TRACE-IT). It has now reached version 4.4, and a maturity level that makes it usable not only for small prototypes but also for real-world systems.

The main feature of the framework is the high degree of usability of all its functionalities; also for this reason it has often been used with satisfaction as a didactic environment for teaching and experimenting formal verification principles, and for supporting PhD and master's degree projects.

During the interactive exploration of the system behaviour, it is possible to observe all the internal details of the reached system configurations. For each system component we can observe: the values of its local variables; the status of the event queue; the set of currently active states and fireable transitions; and the set of possible next states reachable by a run-to-completion step performed by the component.

If we request the visualisation of the graph that models the possible system evolutions, we can click over a node of the graph to display all the internal details of the corresponding system state.

After the verification of a logic formula, it is possible to request a detailed explanation of how the evaluation result has been reached. Given that the supported logic is a

branching-time logic, the counterexample does not have the shape of a simple execution trace. The explanation of the validity of a formula is indeed presented in an interactive way, and at any step of the explanation it is possible to observe all the internal details of the involved system configurations.

These characteristics of the UMC environment make it particularly suitable for the analysis and verification of designs in the early stages of system development, when the basic structures and ideas are being initially drawn, and are still likely to contain errors that the tool can discover, and allow the user to make sense of them.

The decision to make the overall framework publicly accessible through the web is driven by the desire to make UMC and the other tools accessible without overhead from any kind of platform (Unix, Linux, Windows, macOS) to all interested parties, while maintaining centralised control over its continuous improvement.

On the other hand, the web encapsulation allows a transparent integration of the locally developed tools (which are command-line oriented) with features provided from other frameworks (like minimisations with ltsmin and visualisation with graphviz), and allows the dynamic interactions with the user to be exploited in a natural and user-friendly way. For example, when the user clicks over a node of a visualised graph, a command is dispatched to a model exploration generation tool, which generates a new fragment of the state-space. This is saved as a '.dot' file, converted into '.svg' by another tool, embedded into an '.html' document and visualised again as a graph to the user. We are not aware of any other free verification environment that provides a comparable support for the dynamic analysis of UML system designs.

The KandISTI project is a long-term ISTI internal project. We have plans for improving the framework in several directions, among which a greater integration with other verification frameworks (like SPIN, LTSmin, CADP, NuSMV, mCRL2, DiVinE), a better exploitation of parallel/multicore architectures and the support of further specification/design languages.

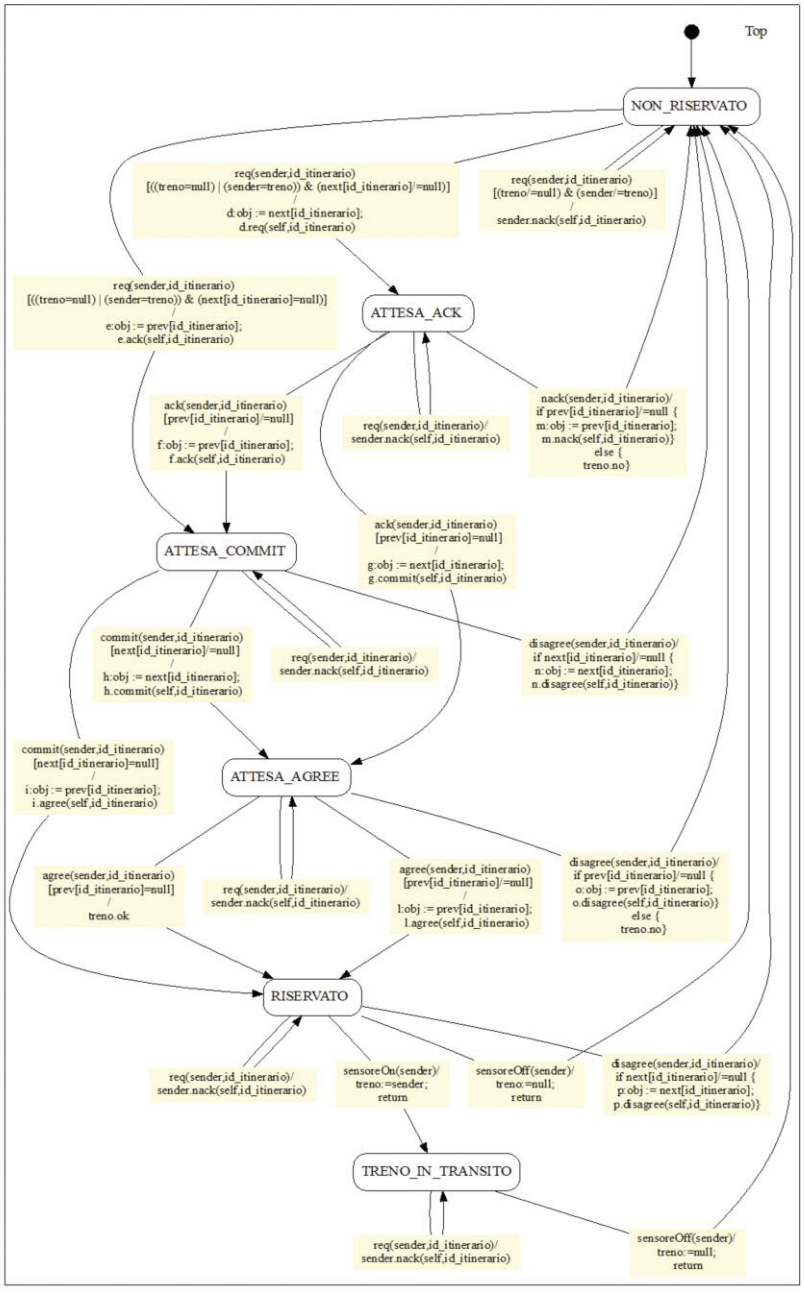

Figure 1: A component of an interlocking model.

Link:

[L1] http://fmt.isti.cnr.it/kandisti

References:

[1] M.H. ter Beek, S. Gnesi, F. Mazzanti: "From EU projects to a family of model checkers", Software, Services, and Systems, LNCS Vol. 8950, Springer, 2015, 312-328.

[2] F. Mazzanti, G.O. Spagnolo, S. Della Longa, A. Ferrari: "Deadlock avoidance in train scheduling: A model checking approach", in Proc. of the 19th International Workshop on Formal Methods for Industrial Critical Systems (FMICS'14), LNCS Vol. 8718, Springer, 2014, 109-123.

[3] M.H. ter Beek, S. Gnesi, F. Mazzanti, C. Moiso: "Formal Modelling and Verification of an Asynchronous Extension of SOAP", in Proc. of the 4th IEEE European Conference on Web Services (ECOWS'06), IEEE, 2006, 287-296.

Please contact:

Franco Mazzanti
ISTI-CNR, Italy
franco.mazzanti@isti.cnr.it