Assisting the Design of an Industrial Groupware System by Model Checking

by Maurice ter Beek, Stefania Gnesi, Diego Latella, Mieke Massink, Maurizio Sebastianis and Gianluca Trentanni

Researchers from the Formal Methods and Tools group of ISTI-CNR and think3, Inc. are collaborating on the application of formal modelling and verification techniques to enhance think3's Product Data Management (PDM) groupware application.

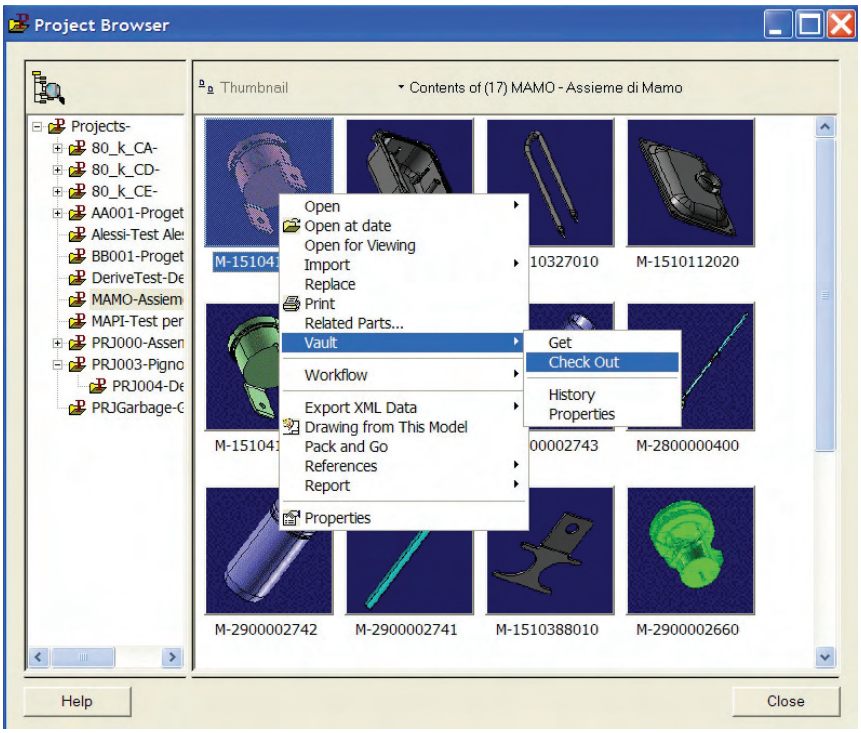
The Formal Methods and Tools (FM&&T) group of the Institute for Information Science and Technologies (ISTI) of the Italian National Research Council (CNR) has a longstanding experience in research on the development and application of formal methods and software tools to specify and verify complex computer systems. In recent years, researchers from FM&&T have worked together with think3, Inc. in order to apply formal modelling and verification techniques to enhance think3's Product Data Management (PDM) groupware application thinkteam. This activity is conducted in the context of the Italian research project tocai.it, which aims at the application and development of knowledge-based technologies to support the aggregation of enterprises over the Internet. think3 is one of the industrial partners in this project.

The goal of Product Lifecycle Management (PLM) is to effectively manage a company's products across their lifecycles. think3's thinkPLM is a suite of integrated PLM applications, built on the thinkteam application, to cater for the product/document management needs of design processes in the manufacturing industry. It allows enterprises to capture, organise, automate and share engineering information in an efficient way, and is used to manage data for products/documents with long or short lifecycles.

The thinkteam groupware products are in continuous evolution and are used by large manufacturing industries which commonly have several dislocated design departments, each of which needs reliable and efficient software systems in order to cooperate efficiently. The many inherent concurrency aspects that think3 needs to address when producing their software, and their awareness of the difficulties this implies when assessing the quality of their products, have led to them becoming interested in the use of model-checking techniques during the early phases of software design.

FM&&T and think3 are thus collaborating on the employment of model-checking techniques to formalise and verify several design options for thinkteam extensions. However, we are also applying model checking to verify a number of properties related to the correctness of groupware protocols in general, ie not limited to the context of thinkteam. One of the difficulties in this domain is that detailed models tend to generate very large state spaces due to the interleaving activity that comes with many asynchronously operating clients. Therefore, our approach is to generate small, abstract models that are intended to address very specific usability-related groupware issues. This collaboration shows that model checking can be of great help in an exploratory design phase, both for comparing different design options and for refining and improving the description of the proposed extensions.

This way of using model checking is in support of a prototyping-like modelling technique. The focus is on obtaining, relatively quickly, an informed but perhaps somewhat approximate idea of the consequences, both qualitative and quantitative, of adding specific features to an existing groupware system. This differs from the traditional use of model checking as a technique to develop rather complete specifications, with the aim of reaching a maximal level of confidence in the correctness of a complicated concurrent algorithm.



A user downloads a CAD file from thinkteam's document repository.

An important result of the joint research concerns the uptake of model-checking techniques by industry. think3 had no previous experience with such analysis techniques. This experience with model checking specifications of a thinkteam extension has been a true eye opener for them, leading them to fully recognize the extent of the many intricate and inherent concurrency aspects of groupware systems like thinkteam.

The relatively simple, lightweight and abstract high-level models that we have developed during the collaboration have turned out to be of great help to focus on the key issues of the development of the interface aspects of thinkteam, before turning to the more detailed design and implementation issues. think3 has now expressed their intention to become more acquainted with model checking and - ultimately - to acquire the skills to perform automated verification of the (groupware) protocols underlying their software systems themselves.

This shows that our approach, which starts with small models that require little time to fully understand but that nevertheless provides results that would be unfeasible to produce manually, and can be used to generate performance diagrams directly related to issues of interest, can be successfully transferred to industry.

Links:
thinkteam and thinkPLM are registered trademarks of think3, Inc.
http://www.think3.com/

Please contact:
Maurice ter Beek or Mieke Massink
ISTI-CNR, Italy
E-mail: m.terbeek@isti.cnr.it, m.massink@isti.cnr.it

A Banking Server's Display on your Key Chain

by Michael Baentsch, Peter Buhler, Reto Hermann, Frank Höring, Thorsten Kramp and Thomas Weigold

Hackers are becoming increasingly inventive in their schemes to attack financial transactions on the Internet. Internet banking systems are a particularly attractive target, so it is mainly this application at which work in the IBM Zurich Research Laboratory is aimed, with the invention and implementation of 'ZTIC', the Zone Trusted Information Channel. Its success is the result of establishing a secure channel between a server and a ZTIC connected to a user's PC.

Banks and other institutions handle the problem of transaction security with three techniques: authentication, confidentiality and integrity. SSL/TLS (Secure Socket Layer Security/Transport Layer Security) is commonly used for the latter two issues. Several solutions, such as one-time passwords or challenge-response protocols, are used for authentication. The use of these techniques goes a long way towards handling primitive Internet attacks. Unfortunately, they alone do not provide a complete solution for today's more sophisticated attacks.

In MITM or 'man-in-the-middle' attacks, a hacker intercepts and modifies in an unnoticeable fashion the messages flowing between a user and a financial institution. The modified messages look to the user like those from the financial institution, whereas those to the financial institution look like those from the client. Malware (malicious software) is even more fiendish. Here the attacker manages to install a virus or Trojan horse in a user's personal computer and is then free to manipulate the messages received and sent by the user. Thus malware attacks can redirect communication to the attacker's server and change the data displayed by the user's browser.

Figure 1: The secure channel is opened between the (bank's) server and the ZTIC. The user communicates as usual with the server via a PC.

ZTIC provides security in the presence of both of these attacks.

ZTIC, the Zone Trusted Information Channel, adds a trusted and tamper-resistant secure communication endpoint with integrated display to an otherwise untrustworthy client PC. Implemented as a USB device running the TLS/SSL protocol, a ZTIC is about the size of a memory stick and thus can be attached conveniently to a key chain. Through this endpoint, a user can then communicate securely with sensitive online services such as a banking server.

All communication between a user's Web browser and a server is passed through and processed by the ZTIC, which in turn is hooked into the communication path by a networking proxy running on the PC. ZTIC continuously scans the data exchanged between client and server for sensitive operations such as money transfers. For each sensitive operation, it intercepts the communication flow, extracts crucial information for display and verification, and proceeds only after the user has explicitly confirmed the operation by pressing an OK button on the ZTIC. Non-sensitive operations are passed along without the need for user interaction. In addition, ZTIC may serve as a holder of sensitive personal information, such as a private key used in SSL/TLS client authentication. If non-repudiation is a strong design goal of an