Name of Authors:	Julien BOTELLA (Smartesting), Phong CAO (THALES), Cédric CIVEIT (Thales Raytheon Systems), Daniel GIDOIN (THALES), Fabien PEUREUX (FEMTO-ST)
Name of Presenter:	Phong CAO / Fabien PEUREUX
E-mail of Contact Person:	fabien.peureux@femto-st.fr
Telephone Number:	+33 (0)381 666 663
Contact Address:	FEMTO-ST – 16, route de Gray – 25030 Besançon cedex - France
Presentation/Poster Title:	Model-based generation of aircraft traffic attack scenarios using ADS-B standard signals
Intended Audience:	QA Managers, Test engineers, Project Managers

Summary of Presentation/Poster

The purpose of this talk is to present an ongoing work and results about model-based security testing approach to validate the detection of SBS-1 malicious signals, formatted according to the ADS-B air-traffic control standard [1], which could be received by the control tower from the aircraft. More precisely, this approach consists to provide a tooled model-based testing generation process that aims to produce test sequences to validate the automatic or human detection of logical attacks launched by sending malicious SBS-1 signal data to air-control tower.
The ADS-B air-traffic control standard is all about communications between aircraft, and also between aircraft and ground by providing every second a broadcast of the aircraft status (including position, identity, velocity,... calculated using a Global Navigation Satellite System). ADS-B is an integral part of the planned efficiency drive towards 2020, and USA authorities have selected this standard to be a keystone of our "Next Generation Air Transportation" system (NextGen [2]). ADS-B standard is composed of two parts: ADS-B OUT provides a means of automated aircraft parameter transmission between the aircraft and the Air Traffic Control (ATC), while ADS-B IN provides automated aircraft parameter transmission between aircraft themselves [3]. The research results introduced in this presentation deal only with ADS-B OUT, which is designed to ease the ATC, enhancing safety and increasing airport capacity. In this context, ADS-B OUT is used to normalize data SBS-1 signals sent by aircraft and received by the control tower, and make it possible to generate a precise air picture for air traffic management (see Figure 1).

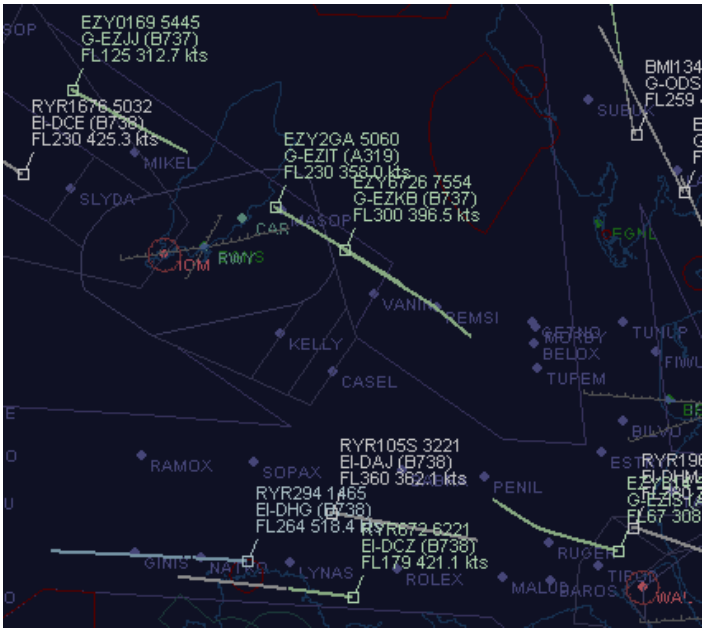

Figure 1: Aircraft data map of air-traffic control

However, the ADS-B standard is public and all the information transmitted using SBS-1 signals are unencrypted, and decoding them is not difficult (see Figure 2 in which each line defines a separate message). They can thus be easily gathered or fraudulently produced [4].

```
STA,,5,179,400AE7,10103,2008/11/28,14:58:51.153,2008/11/28,14:58:51.153,RM
MSG,4,5,211,4CA2D6,10057,2008/11/28,14:53:49.986,2008/11/28,14:58:51.153,,,408.3,146.4,,,64,,,,,
MSG,8,5,211,4CA2D6,10057,2008/11/28,14:53:50.391,2008/11/28,14:58:51.153,,,,,,,,,,,0
MSG,4,5,211,4CA2D6,10057,2008/11/28,14:53:50.391,2008/11/28,14:58:51.153,,,408.3,146.4,,,64,,,,,
MSG,3,5,211,4CA2D6,10057,2008/11/28,14:53:50.594,2008/11/28,14:58:51.153,,37000,,,51.45735,-1.02826,,,0,0,0,0
MSG,8,5,812,ABBEE3,10095,2008/11/28,14:53:50.594,2008/11/28,14:58:51.153,,,,,,,,,,,0
MSG,3,5,276,4010E9,10088,2008/11/28,14:53:49.986,2008/11/28,14:58:51.153,,28000,,,53.02551,-2.91389,,,0,0,0,0
MSG,4,5,276,4010E9,10088,2008/11/28,14:53:50.188,2008/11/28,14:58:51.153,,,459.4,20.2,,,64,,,,,
MSG,8,5,276,4010E9,10088,2008/11/28,14:53:50.594,2008/11/28,14:58:51.153,,,,,,,,,,,0
MSG,3,5,276,4010E9,10088,2008/11/28,14:53:50.594,2008/11/28,14:58:51.153,,28000,,,53.02677,-2.91310,,,0,0,0,0
MSG,4,5,769,4CA2CB,10061,2008/11/28,14:53:50.188,2008/11/28,14:58:51.153,,,367.7,138.6,,,-2432,,,,,
MSG,8,5,769,4CA2CB,10061,2008/11/28,14:53:50.391,2008/11/28,14:58:51.153,,,,,,,,,,,0
```

Figure 2: Excerpt of SBS-1 data stream

This situation thus allows a malicious exploitation of the ADS-B OUT communication and then enables potential threats, since we can easily capture clear text data of air traffic and/or transmit erroneous data broadcast. Moreover, the physical base station required to perform such a malicious use can be purchased by anyone, and vulnerability threat are real as demonstrated in [5].

Our research results aim at tackling the real-time detection of such vulnerability scenarios by using a tooled model-based testing approach. The global process of the approach is depicted in Figure 3.

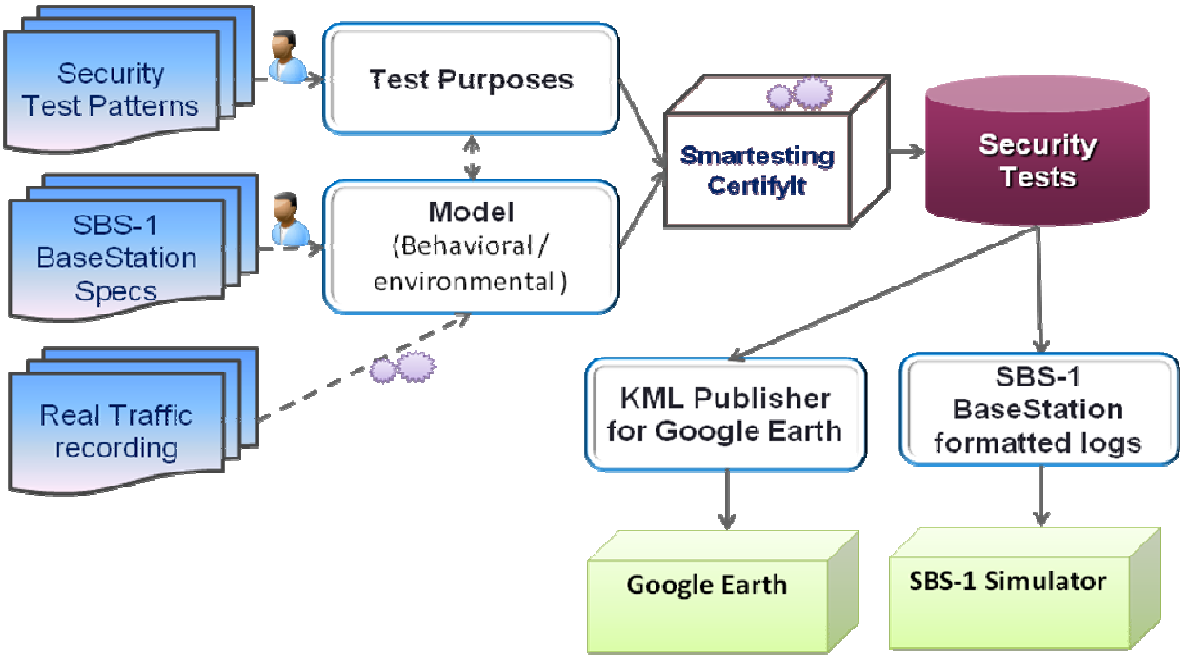

Figure 3: Security testing process overview

The proposed process to generate aircraft traffic attack scenarios based on ADS-B standard signals is based on the Smartesting Model-Based Testing tool (namely CertifyIt) [6], which allows to generate test sequences from UML behavioural models and security test purposes.
The behavioural model defines the environmental aspects of the domain to be tested in order to generate consistent (from a functional point of view) sequences of ADS-B signals. On the one hand, it includes the communication format of the SBS-1 message of the ADS-B standard (static aspect), and on the other hand, it captures real (or realistic) air-traffic scenarios (dynamic aspect).

The test purposes, which define the test objectives, are derived from generic security test patterns and take the form of regular expressions [7]. The language relies on combining keywords and instructions allowing updating and/or falsifying the real air-traffic scenarios described in the behavioural model.
The test generation algorithm, computed by the Smartesting CertifyIt tool, enables then to produce mutated real air-traffic scenarios (sequences of transmitted ADS-B signals) by changing and/or adding communication data, which simulate a malicious aircraft broadcast.
As example, from a real air-traffic configuration, test purposes can give rise to the production of vulnerability air-traffic scenarios including injection of "ghost" flights into a real configuration, injection of cancelled flights into a real configuration, introduction of (slight) variations in real flights, change of an apparent airliner into fighter(s),...

These automatically generated attack scenarios are next concretized to be simulated. We propose to execute them on a simulation tool (Google Earth representation using KML language scripts), or on a realistic test bench (SBS-1 Simulator using ADS-B formatted signals).
The objective of the generated tests is to evaluate the vulnerability detection rate of automated air-control system, and the corresponding human attitude during monitoring. It also can be relevant to develop and elaborate new warning protocol, and to improve existing countermeasures, which are today mainly based on data comparison between ADS-B and radar information, and to a latter extent visual inspection.

The presentation will be divided into the following parts:
- Context, motivation and key challenges
- Presentation of the Model-Based testing approach
- Illustration of the end-to-end process on a simple example
- Conclusion and future work

This research work is supported by the French FSN project DAST (see http://dast.univ-fcomte.fr/).

Evaluation Criteria

1. ***Which stage of adoption do the results presented in this proposal reflect?***
   b. Pilot ➔ results by a team as part of an evaluation

2. ***Main application area:***
   d. Transport (Aerospace)

3. ***What is the novelty in your presentation/poster?***

The novelty of the proposed approach concerns the use of generic security test purposes to drive a Model-Based testing approach. These security test purposes allow on the one hand to improve the accuracy and the relevance of the generated test cases, and on the other hand to propose a replicable approach to increase the automation level of testing activity.

4. ***How is your presentation/poster related to industrial application of automated testing?***

The proposed approach has been developed and experimented on a real case-study concerning a widespread air-traffic control communication standard. Moreover, this work has been done as part of a close collaboration involving a business domain expert (THALES), a testing tool provider (Smartesting) and a research academic laboratory (FEMTO-ST).

5. ***How can the approach or method be re-used by other organizations?***

The proposed test generation approach is illustrated using a specific case-study about air-traffic control standard. However, this result is not restricted to this process and can be applied in several communicating systems, which emphasise security of the exchanged data as a major issue.

Bibliography

1. U.S. Department of Transportation - Federal Aviation Administration. Web page about RTCA SC-186 ADS-B Support: http://adsb.tc.faa.gov/ADS-B.htm. Last visit in April 2013.
2. U.S. Department of Transportation - Federal Aviation Administration. Web page about Next Generation Air Transportation System: http://www.faa.gov/nextgen/. Last visit in April 2013.
3. C. Vigier. Automatic Dependent Surveillance Broadcast (ADS-B) - Surveillance development for Air Traffic Management. AIRBUS FAST Journal number 47. pages 8-13. January 2011. Available online at http://www.airbus.com/support/publications/. Last visit in April 2013.
4. D.L. McCallie. Exploring Potential ADS-B Vulnerabilites in the FAA's Nextgen Air Transportation System. Graduate Report Number AFIT/ICW/ENG/11-09 (public domain). Air Force Institute of Technology (U.S.). June 2011. Available online at https://www.hsdl.org/?view&did=697737. Last visit in April 2013.
5. B. Haines. Hackers + Airplanes: No Good Can Come Of This. Defcon'20 Conference. Las Vegas, NV,USA. July 2012. Video available at http://www.youtube.com/watch?v=CXv1j3GbgLk. Last visit in April 2013.
6. E. Bernard, F. Bouquet, A. Charbonnier, B. Legeard, F. Peureux, M. Utting, and E. Torreborre. Model-based testing from UML models. Int. Workshop on Model-based Testing (MBT'2006), LNCS, vol. 94. pages 223–230. Dresden, Germany. October 2006.
7. J. Botella, F. Bouquet, J.-F. Capuron, F. Lebeau, B. Legeard, and F. Schadle. Model-based Testing of Cryptographic Components Lessons Learned from Experience. Int. Conference on Software Testing, Verification and Validation (ICST'13). Luxembourg: IEEE CS, March 2013.