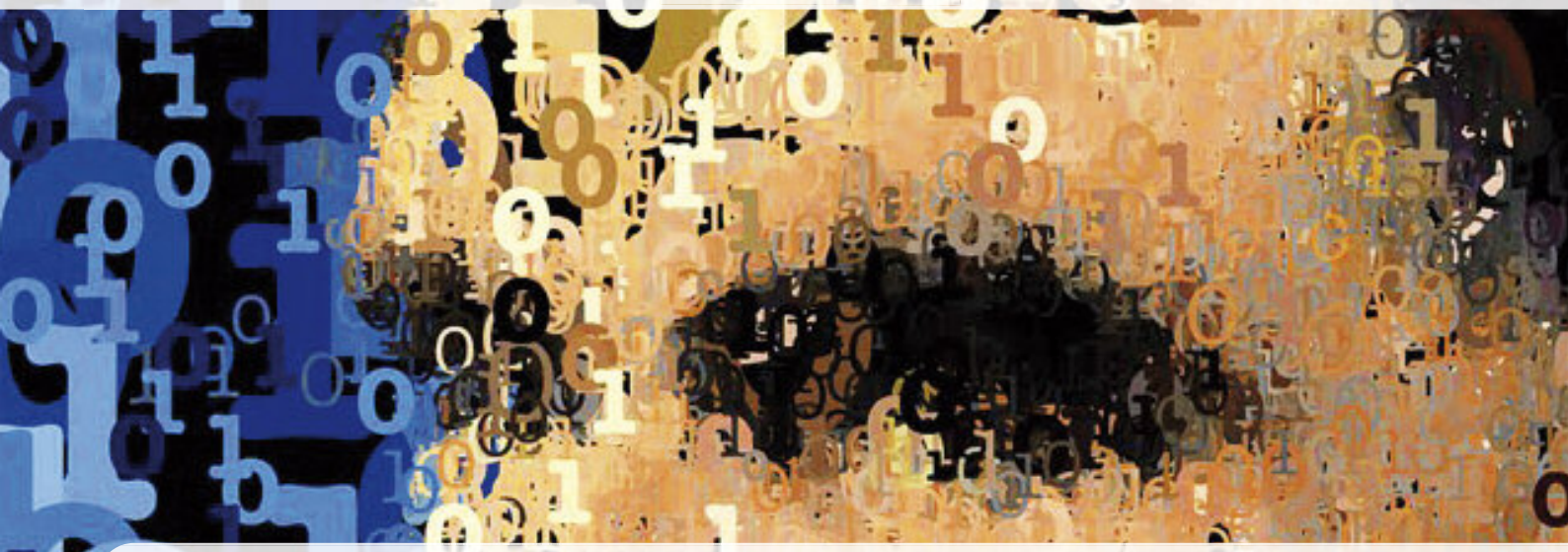
Number 91, October 2012

ERCIM NEWS

www.ercim.eu



Special theme:

What is Computation?

Alan Turing's Legacy

Also in this issue:

implements the protocol. A Reo compiler then generates the proper multi-threaded code for the application.

Figure 2 shows three examples of protocols expressed as Reo connectors: graphs of nodes and arcs, which we refer to as channels. Importantly, communicating parties remain oblivious to how a connector routes data: parties dispatching (fetching) data elements do not know where to (from) these elements go (come). The connector on the left, called MergerWithBuffer, specifies the same protocol as the one embedded in Figure 1.

Untangled from each other into separate computation and protocol modules, we can study, analyse, and verify the properties of each, independently of the others. We can combine the very same pieces of code that implement a set of producers and consumers with any of the connectors in Figures 2 to obtain different applications that manifest different protocols. We can reuse the same protocols, i.e., the connectors in Figure 2, with very different computational threads in entirely different applications. Reo turns interaction protocols into tangible, explicit, first-class concepts. We can connect the nodes of various instances of these Reo connectors to each other, to obtain connectors that implement more complex protocols. This protocol-level compositionality, a key feature of Reo, supports compositional, scalable construction, verification, analysis, and testing of protocols. Availability of the protocol of an application as an explicit, concrete piece of code enables efficient, dynamic scheduling and resource management.

Our on-going work on generating efficient code from Reo specifications to run on multi-core platforms has shown promising results, revealed interesting challenges, and confirms that the principles of "separation of concerns" and "modularity" apply equally well in the design, construction, verification, analysis, testing, and reuse of scalable protocols.

Link:
http://reo.project.cwi.nl; http://www.cwi.nl/~farhad

References:
[1] F. Arbab: "Puff, The Magic Protocol", in "Formal Modeling: Actors, Open Systems, Biological Systems", LNCS 7000, pp. 169-206, 2011, http://dx.doi.org/10.1007/978-3-642-24933-4_9

[2] F. Arbab: "Reo: a channel-based coordination model for component composition", MSCS 14(3), pp. 329–366, 2004, http://dx.doi.org/10.1017/S0960129504004153

[3] Sung-Shik T.Q. Jongmans, F Arbab: "Overview of Thirty Semantic Formalisms for Reo", SACS 22(1), pp. 201–251, 2012, http://dx.doi.org/10.7561/SACS.2012.1.201

Please contact:
Farhad Arbab, Sung-Shik Jongmans
CWI, The Netherlands
Tel: +31 20 592 4056, +31 20 592 4241
E-mail: farhad@cwi.nl, jongmans@cwi.nl

Cybercrime and the Security of Critical Infrastructures

by Florian Skopik and Thomas Bleier

In recent years, the Internet has rapidly expanded to a massive economic sphere of activity – not only for the new economy, where Internet-based businesses have grown from startups to multinational and billon-dollar enterprises, faster than any businesses before, but also for the "dark side" of entrepreneurship. Exploiting weaknesses in information and communications technology (ICT) systems has become a profitable business model. In order to better cope with these threats, we argue that tight cooperation between all parties in the digital society is necessary. The project CAIS deals with the implementation of a cyber attack information system on a national level, whose ultimate goal is to strengthen the resilience of today's interdependent networked services and increase their overall availability and trustworthiness.

In the early days of ICT, attacking other computers was mostly motivated by a desire for self-expression or competition between hackers but nowadays it has become a big business [1]. There is no clear picture of the volume of these markets, but the damage is huge. A Europol report [2] from 2011, for example, indicates losses of around € 750 billion annually. Today, spam emails are used to advertise goods and distribute phishing links or malware, viruses spread infections and carry dangerous payloads, and drive-by downloads are used to infect victims when they are accessing unsuspicious websites. Furthermore, rootkits hide the existence of other malware on a system, enabling them to act undetected for as long as possible, and botnets are used to control a large number of victim systems for malicious purposes. Even critical infrastructures, such as energy networks, transportation and financial services are becoming increasingly connected to the Internet in order to enable cost-efficient remote monitoring and maintenance. Furthermore, the pervasive use of novel computing paradigms, including mobile computing and cloud computing, makes society even more dependent on the proper functioning of ICT systems.

Methodology for Protecting Networks in the 21st Century

Traditional protection mechanisms, such as firewalls and anti-virus software are no longer able to guarantee an adequate level of security: attacks are too complex and specialized. Thus, these days we observe a major paradigm shift from prevention and remediation-focused approaches to response and containment strategies. This shift also requires organizations to move from common static policy-based security approaches towards intelligent mechanisms, incorporating identification of anomalies, analysis and reasoning of attacks, and in-time response strategies [3]. The basic properties of such approaches are:

- *Risk-based*: Prioritizing security for the most important assets.It is not economically viable for an organization or a nation to provide maximum security for all assets.
- *Contextual*: collecting huge amounts of intelligence data and use analytics to identify relevant data sources for

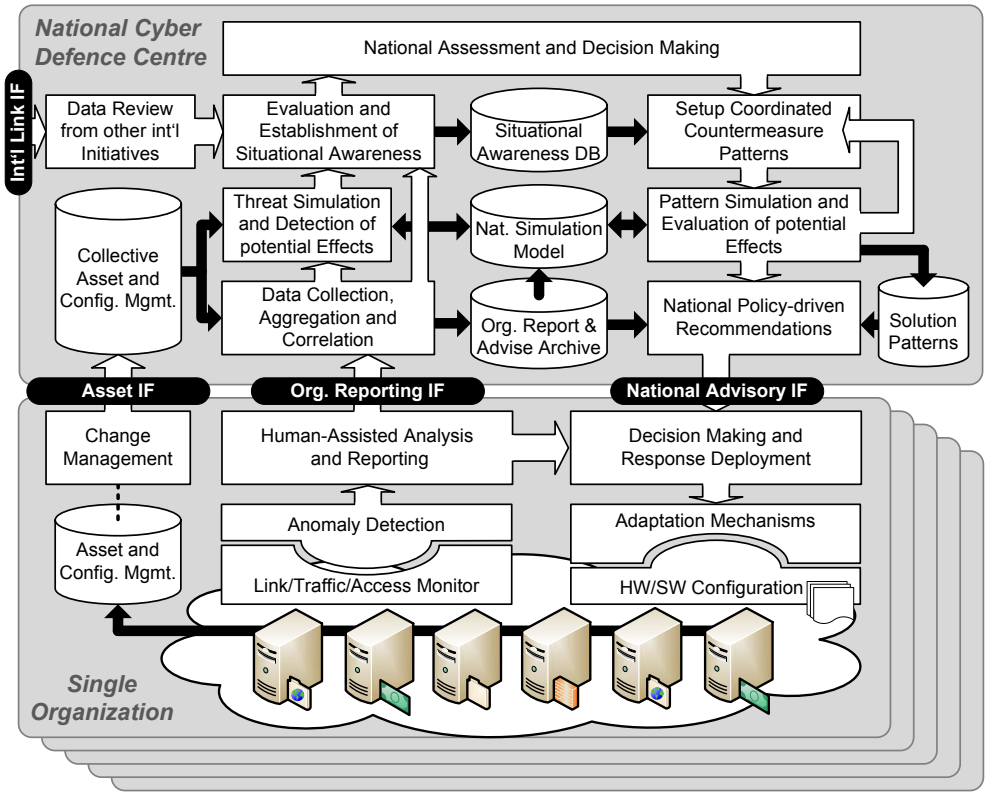


Figure 1: Overall architecture of the Cyber Attack Information System

anomaly detection. A context space is created by aggregating and correlating a wide variety of events, even if an attacker partially deleted his traces.
- *Agile*: enable fast responses to minimize the exploitable attack window and to keep (financial) losses to a minimum.

In order to cope with future advanced threats, we argue that tight cooperation between all parties in the digital society is necessary. In some domains, such as the banking sector, strategic alliances and information sharing within the community are already commonplace (e.g. to deal with phishing attacks). Furthermore, there exist relationships between organizations, such as national Computer Emergency Response Teams (CERTs), to support collaborative incident response activities. These, however, tend to be informally arranged between individual groups or are largely focused on securing infrastructures in the same operational domain. Whilst these activities have proven useful, a more comprehensive and formal approach to ensuring the security of national critical infrastructures, which spans numerous operational domains, will become necessary with the increasing use of ICT in interdependent critical infrastructure provisioning.

Contributions and Applied Solutions in CAIS

The project CAIS deals with the implementation of a Cyber Attack Information System on a national level (cf. Figure 1), whose ultimate goal is to strengthen the resilience of today's interdependent networked services, and increase their overall availability and trustworthiness. In particular, the following challenges are addressed and corresponding methodologies applied:
- Study of future cyber risks and emerging threats, particularly having the changing political and economic landscape in mind. Here, the well proven Delphi method – a systematic, interactive forecasting technique – is applied in consultation with an extended group of subject matter experts.
- Evaluation of novel anomaly detection techniques by composing available network tools for log file management with new pattern mining approaches inspired by models from the domain of bio informatics. Here, high performance and scalability is of paramount importance.
- Creation of highly modular infrastructure models on multiple layers, spanning hardware-centric physical aspects, over data flow and service deployment perspectives, to abstract inter-organizational dependencies.
- Innovative tools for attack simulations, using aforementioned infrastructure models and applying game-theoretic approaches as well as agent-based simulations in order to forecast the effects of attacks on interconnected infrastructures, as well as the impact of countermeasures on various levels and from multiple viewpoints.
- Investigate the deployment and instantiation of a CAIS (see Figure 1) that connects single organizations, links and coordinates isolated anomaly detection efforts, and facilitates information sharing and mutual aid between organizations.

CAIS Project Consortium

In order to attain these ambitious goals and finally ensure the wide applicability of developed tools, major stakeholders of Austria's security domain are involved. First, research institutions, such as the Austrian Institute of Technology and the University of Applied Sciences St. Poelten contribute their scientific expertise regarding anomaly detection techniques and infrastructure modelling and simulation. Furthermore, the OIIP Austrian Institute for International Affairs studies cyber threats and risks to national critical infrastructures caused by cyber crime. The major telecommunication service providers T-Mobile Austria and T-Systems Austria, as well as the national Austrian Computer Emergency Response Team (CERT) ensure a sound implementation on a technical layer and practical applicability and validation. The Austrian Federal Chancellery (BKA), Federal Ministry of

Interior (BMI) and the Federal Ministry of Defense (BMLVS) bring in requirements from a national security perspective. Moreover, CAIS consortium members are actively involved in international initiatives, such as the Multi National Experiment 7 (MNE7) which enables beneficial collaborations across Austria's borders. This two-year project runs from 2011 to 2013 and is financially supported by the Austrian security-research program KIRAS and by the Austrian Ministry for Transport, Innovation and Technology.

Links:
http://www.kiras.at/gefoerderte-projekte/detail/projekt/cais-cyber-attack-information-system/

http://www.ait.ac.at/research-services/research-services-safety-security/ict-security/cais-cyber-attack-information-system/?L=1

References:
[1] J. Radianti, E. Rich, J. Gonzalez: "Vulnerability Black Markets: Empirical Evidence and Scenario Simulation", in Proc. of the 42nd Hawaii International Conference on System Sciences, pp. 1-10, 2009

[2] Europol: Threat Assessment – Internet Facilitated Organised Crime iOCTA, 2011

[3] EMC Press Release: RSA Chief Rallies Industry to Improve Trust in the Digital World, After Year Filled with Cyber Attacks, RSA Conference 2011, San Francisco, CA, Feb. 28, 2012

Please contact:
Thomas Bleier, Florian Skopik
AIT Austrian Institute of Technology
E-mail: thomas.bleier@ait.ac.at, florian.skopik@ait.ac.at

VoterBallot - A New Application for ICT in Elections

by Zaza Tabagari, Zaza Sanikidze and George Giorgobiani

Many countries with emerging democracies aspire to a system similar to European democracy. International Organizations aim to help these countries to introduce a fairer election environment but their efforts are not always successful. Rigged elections mean that many electoral candidates are unfairly disadvantaged In this situation, tension can escalate and, in the worst case scenario, this can lead to military confrontation.

Researchers from the N. Muskhelishvili Institute of Computational Mathematics of the Georgian Technical University suggest a new way of applying ICT to improve the election process in a biased environment and avoid threats to democracy (see eg [1]). They propose VoterBallot, a management information communication system for electoral candidates. It includes four main components: physical infrastructure, software, structured information and training.

Physical infrastructure and software

At each polling station there is a trained representative of the candidate, equipped with a mobile device (or satellite phone) with extended media functions, connected through the Internet (free of any control) to the server (see eg [2]). The server is located at the electoral candidate's office (mirrors are in various places). The system's software contains: databases, forms, and various analytical programming modules, installed on the server. The main database is a three-dimen-

Editorial Information

ERCIM News is the magazine of ERCIM. Published quarterly, it reports on joint actions of the ERCIM partners, and aims to reflect the contribution made by ERCIM to the European Community in Information Technology and Applied Mathematics. Through short articles and news items, it provides a forum for the exchange of information between the institutes and also with the wider scientific community. This issue has a circulation of about 8,500 copies.
ERCIM News is published by ERCIM EEIG
BP 93, F-06902 Sophia Antipolis Cedex, France
Tel: +33 4 9238 5010, E-mail: contact@ercim.eu
Director: Jérôme Chailloux
ISSN 0926-4981

Editorial Board:
Central editor: Peter Kunz, ERCIM office (peter.kunz@ercim.eu)
Local Editors:
- *Austria: Erwin Schoitsch, (erwin.schoitsch@ait.ac.at)*
- *Belgium:Benoît Michel (benoit.michel@uclouvain.be)*
- *Cyprus: George Papadopoulos (george@cs.ucy.ac.cy)*
- *Czech Republic: Michal Haindl (haindl@utia.cas.cz)*
- *France: Thierry Priol (thierry.priol@inria.fr)*
- *Germany: Michael Krapp (michael.krapp@scai.fraunhofer.de)*
- *Greece: Eleni Orphanoudakis (eleni@ics.forth.gr), Artemios Voyiatzis (bogart@isi.gr)*
- *Hungary: Erzsébet Csuhaj-Varjú (csuhaj@inf.elte.hu)*
- *Italy: Carol Peters (carol.peters@isti.cnr.it)*
- *Luxembourg: Patrik Hitzelberger (hitzelbe@lippmann.lu)*
- *Norway: Truls Gjestland (truls.gjestland@ime.ntnu.no)*
- *Poland: Hung Son Nguyen (son@mimuw.edu.pl)*
- *Portugal: Joaquim Jorge (jorgej@ist.utl.pt)*
- *Spain: Silvia Abrahão (sabrahao@dsic.upv.es)*
- *Sweden: Kersti Hedman (kersti@sics.se)*
- *Switzerland: Harry Rudin (hrudin@smile.ch)*
- *The Netherlands: Annette Kik (Annette.Kik@cwi.nl)*
- *United Kingdom: Martin Prime (Martin.Prime@stfc.ac.uk)*
- *W3C: Marie-Claire Forgue (mcf@w3.org)*

Contributions
Contributions must be submitted to the local editor of your country

Copyright Notice
All authors, as identified in each article, retain copyright of their work

Advertising
For current advertising rates and conditions, see http://ercim-news.ercim.eu/ or contact peter.kunz@ercim.eu

ERCIM News online edition
The online edition is published at http://ercim-news.ercim.eu/

Subscription
Subscribe to ERCIM News by sending email to en-subscriptions@ercim.eu or by filling out the form at the ERCIM News website: http://ercim-news.ercim.eu/

Next issue
January 2013, Special theme: Smart Energy Systems