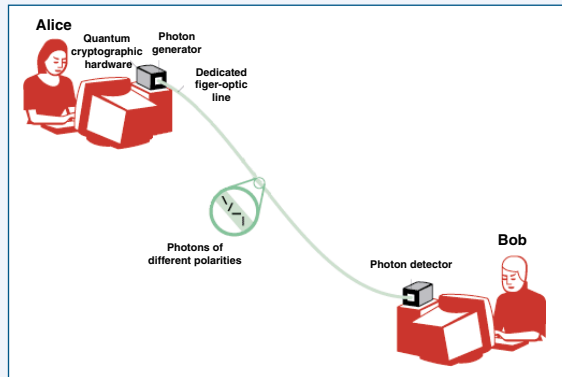


A particularly interesting feature of this so-called Bounded-Storage Model is ‘everlasting security’: if the adversary fails to store the mountain of data during the execution of the scheme, then her chance of breaking it is lost forever together with the data he failed to store. That would never change, even if he should obtain larger storage capacity sometime in the future. This is in sharp contrast to conventional computational cryptography, in which schemes may be broken ‘in retrospect’, once the adversary has gained sufficient computing power. On the other hand, while basing cryptography on computational assumptions allows for very efficient schemes, a major disadvantage of the Bounded-Storage Model is the immense amount of data that must be communicated (even for the honest users) in order to be able to swamp a potential adversary's memory.

Recently, in collaboration with researchers from Aarhus University (Denmark), CWI's Cryptology and Information Security Group has put forward and studied a variant of the Bounded-Storage Model which is based on swamping the adversary's quantum-memory: the Bounded-Quantum-Storage Model. Quantum mechanics provide a good platform for such an approach: on the one hand, according to Heisenberg's Uncertainty Principle,



Caption:

converting quantum information to classical information by measuring irreversibly destroys some of that information, and the challenge is to arrange it so that the adversary cannot afford this loss while honest users can. On the other hand, in contrast to classical information, storing quantum information is very difficult (at this point essentially impossible), and thus it requires very little to swamp the adversary's quantum memory.

In this model the CWI researchers have constructed a scheme for Oblivious Transfer, and thus indirectly for any Secure Cooperation. The scheme involves the transmission of a stream of single photons (or other atomic particles), and it is proven secure under the

sole assumptions that Heisenberg's Uncertainty Principle holds and that potential adversaries cannot store more than a large fraction of the transmitted photons, even though they may have infinite computing power and classical memory.

Apart from quantum cryptography, CWI's Cryptology and Information Security Research Group focuses on

all mathematical aspects of cryptology, such as algebraic secret sharing and secure multi-party computation, computational number theory (eg the Number Field Sieve Project for factoring RSA challenge numbers), information-theory-based cryptography, public-key cryptography in general (in particular, chosen cipher-text security for encryption schemes), cryptographic protocols, and formal security analysis.

Link:
<http://www.cwi.nl/crypto>

Please contact:
 Ronald Cramer, CWI, The Netherlands
 Tel: +31 20 592 4166
 E-mail: cramer@cwi.nl

Serge Fehr, CWI, The Netherlands
 Tel: +31 20 592 4166
 E-mail: fehr@cwi.nl

Building a Stochastic Model for Security and Trust Assessment Evaluation

by Karin Sallhammar, Svein Johan Knapskog and Bjarne Emil Helvik

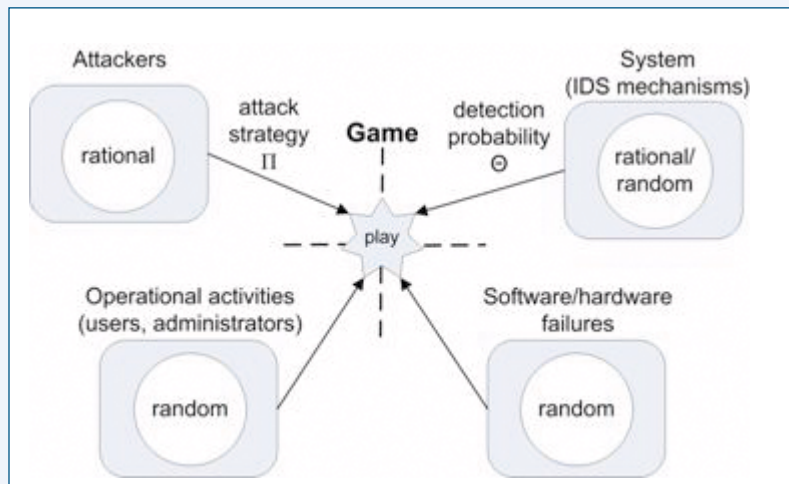
The ICT systems of today are complex inventions and we rely on their existence in almost all aspects of our everyday life. It is therefore crucial that they can provide the services we need whenever we require them. Due to the interconnection of networked systems, attacks are becoming increasingly sophisticated and can be performed remotely. To what degree can we trust that a system will perform its intended task in a secure and reliable manner?

The new paradigms of ubiquitous computing and high capacity data transfer have opened up the Internet as the main area for information interchange and electronic commerce. Attacks against the computer networks used by modern society and economics for

communication and finance can therefore threaten the economical and physical well-being of people and organizations. To allow continuous risk estimation of today's ICT systems, there is an urgent need for models providing probabilistic measures of operational security.

Stochastic Modelling

During the last decade, significant research has been performed on applying traditional dependability techniques to quantify the security attributes of ICT systems. In particular, stochastic modelling techniques such as Markov



The interactions between the attacker and the system modelled as a stochastic game.

chains or stochastic Petri nets have been identified as promising approaches. In a dependability context, a system will continuously be vulnerable to failures of software and hardware, which may transfer the system from a good state into a corresponding failed state. Usually, these methods do not consider failures due to malicious acts. However, by using an analogy between a system failure and a security breach, it is possible to model an intrusion attempt as one or more state changes that transfer the system into a security breach state, ie a state which deviates from the specified security policy. The use of a stochastic model, which combines security-related attacks with traditional dependability fault sources has a wide range of application:

- to quantify security: by using the steady-state probabilities of the stochastic model, one can calculate operational measures such as the 'mean time to security compromise' for the system
- for trade-off analysis: for example, one may evaluate the possible effect of security countermeasures before implementing them
- as a method to help administrators find optimal defence strategies and to calculate the expected loss associated with different strategies.

However, attacks may not always be well characterized by models of random nature. Most attackers will act with intent and will consider the possible consequences (satisfaction, profit and status versus the effort and risk of their actions) before they act. One of the

remaining challenges is therefore how to incorporate intelligent attacker behaviour into the stochastic models.

The Game Model

At the Q2S centre at NTNU, Norway, we are developing a stochastic model that can be used for assessing the security and trustworthiness of ICT systems. Our model considers all aspects that may affect the security or dependability attributes of the system, including:

- normal user behaviour
- administrative activities
- random software and hardware failures
- intentional attacks.

To incorporate intentional attacks in the model, the attacker behaviour must be predicted. By using a stochastic game model, we can compute the expected attacker behaviour for a number of different attacker profiles.

The game model in the figure is based on a reward/cost concept. This assumes that attackers will consider the reward of successful actions versus the possible cost of detection before they act, and that they will always try to maximize the expected outcome of the attack. The dynamics of the states of the stochastic games form a Markov chain, under the assumption that attackers, users and administrators do not change their behaviour over time. Having solved the stochastic game, the expected attacker behaviour can then be reflected in the transitions between states in the system

model, by weighting the transition rates according to a probability distribution. In the final step, the corresponding stochastic process is used to calculate security measures of the system, in a similar manner to the common availability and reliability analysis of ICT systems.

Previous research has shown that stochastic models can be used to model and analyse the trustworthiness of ICT systems in terms of both security and dependability attributes. Our current research indicates that game theory is a suitable tool for incorporating the expected attacker behaviour in such models. However, verifying the method's ability to predict real-life attacks will require further research, including validation of the model against empirical data.

Link:
<http://www.q2s.ntnu.no>

Please contact:
 Karin Sallhammar
 Centre for Quantifiable Quality of Service (Q2S), NTNU, Norway.
 E-mail: karin.sallhammar@q2s.ntnu.no