Games and Abstraction

RISCS
Research Institute in Science of Cyber Security

Minding the gap

In most scientific disciplines, you can see progress being made. Road safety, for example, improves progressively as we revamp vehicle design, add seat belts and airbags, and get better at training drivers. Similarly, we can see clear progress in the effectiveness of cancer treatments or the materials science behind tennis racquets. Not so in cybersecurity, where any progress we make is almost immediately negated by attackers finding new ways around it. That fact is the reason why many people – among them Chris Hankin, Pasquale Malacaria, and Carlos Cid – believe that game theory can provide good mathematical models for cybersecurity. Games and Abstraction: The Science of Cyber Security, Imperial College's contribution to the Research Institute in the Science of Cyber Security, seeks to address the challenge of making better security decisions by developing new approaches to decision support – using game theory, but adding sufficient complexity to close the gap between theory and practical application.

"The goal," says Hankin, director of the Institute for Security Science and Technology at Imperial College and the project's leader, "is to develop techniques to enable well-founded human security design decisions to be made."

Games and Abstraction brings together one of Hankin's primary research interests, his long history of work in semantics-based program analysis, with Malacaria's background in information theory - code security, rather than network security – and, in the later stages, machine learning.

"The aim of the project," says Malacaria, a reader at the School of Electronic Engineering and Computer Science at Queen Mary University of London, "is primarily to concentrate on the underlying engine of a system that would allow users to interact with possible security scenarios and countermeasures. The engine should churn data and outline possible good decisions for a system administrator, given a set of possible threats. Game theory provides the decision mechanism, abstract interpretation deals with computational complexity, and machine learning deals with partial information and emerging attacks."

In his 30 years of work on program analysis, Hankin has developed methods for examining software to infer how the program will behave without actually running it. Historically, he says, the results of this work were first used to optimise compilers (see boxout); latterly their use has broadened. Hankin's earliest work in this area was primarily qualitative, in lattice and domain theory. More recently, in collaboration with fellow Imperial researchers Alessandra Di Pierro and Herbert Wicklicky (see for example their 2005 paper "Measuring the Confinement of Probabilistic Systems", published in Theoretical Computer Science 340(1), 3-56), he has branched out into information flow analysis, timing leaks, and other techniques attempting to quantify how vulnerable a particular system is.

Game theory has a long history and, as the main mathematical modelling tool for adversarial contexts, ought to have been seen immediately as a natural candidate for the mathematics of cybersecurity. But despite a few influential pieces of work in the 1970s and 1980s, it took until the mid-1990s for serious interest to develop in using it in cybersecurity. As an example, the interactions between an attacker and an administrator can be modelled as a two-player stochastic game – that is, a game with a series of stages with payoffs at each stage – and computing the best response.

"Essentially," says Hankin, "there are decisions to be made at each point as to what the best strategy is, either for the attacker, optimising the payoff, or the defender in terms of the costs involved with different responses. Effectively, you build a statistics model in a very simple setting that shows how they should behave to achieve equilibrium."

Games and Abstraction research team members Manos Panaousis and Andrew Fielder

However, in real life, people don't behave in the simple ways traditionally modelled by game theory. They have hidden agendas. They have complex, conflicting, and sometimes self-destructive motives. Like tennis players, they seek not only to make their own strategies succeed but to frustrate their opponents.

In their forthcoming paper "Payoffs, Intentionality, and Abstraction in Games" (to be published in Abramsky Ffestschirft, LNCS 7890, Springer Verlag 2013), Hankin and Malacaria address criticisms that game theory's predictions of how real people will behave are unrealistic, arguing that the problem is not the concept of the Nash equilibrium itself but that the payoffs in the game need to be adjusted to more closely match reality. In the real world of cybersecurity, attackers adapt

Game theory

Game theory is the mathematical discipline of studying conflict and cooperation. Most people are familiar with one of the simplest theoretical games, the Prisoner's Dilemma, proposed in 1984. In it, two prisoners have the choice of cooperating with each other or defecting - that is, ratting each other out to the police. The incentives are balanced so that if only one prisoner defects that prisoner goes free while the other gets a stiffer sentence, but if both prisoners defect both get reduced sentences. The overall mutual optimal outcome is for both to co-operate; but lacking information about what the other is doing, the rational decision for each is to defect.

However, multiple players in situations with complex incentives do not always seem to behave in the "rational" way game theory might predict. Cybersecurity is such a situation. The motivations, persistence, and time scales of such possible attackers as hacktivists, organised crime, the cyber-equivalent of teenaged joyriders, and even journalists are vastly different. Today's attacks-as-a-service underground may see many players providing elements of a single attack; today's multi-stage attacks may target an organisation merely as a conduit to enable a bigger attack on many others. More complex dilemmas are needed.

A second problem – which Hankin is targeting based on his previous work in program analysis – is that multiple players, motivations, and interactions rapidly create a mathematical model with too many possibilities to calculate. Abstracting and simplifying these models should bring them back to a manageable scale.

in response to a constantly shifting environment and administrators must cope in real time with changes in attack methods, motives, and number of opponents. The difficulty is that the size of the state space explodes rapidly: even a simple model of possible interactions between a system administrator and an attacker may have billions of possible configurations.

“This kind of size is difficult to deal with in classical game theory,” says Malacaria. “Our idea is to make abstractions so that instead of having this huge state space we can reason in terms of simplified models.”

Hankin says, “If you want to statistically analyse these models, you have to have an abstraction - cut down to the important features in order to be able to answer specific questions about the way the program will behave.”

Games and Abstraction will marry these two approaches by applying the kinds of techniques developed for program analysis to game theoretical models.

“We believe those probabilistic techniques can be used to abstract game theory models and give a rigorous way of relating the inferences we make based on the abstracted models to what’s happening in the real world,” says Hankin. “As we progress we want to work with systems where there are both incomplete games where we don’t actually know what the attacker’s strategy is, and games with imperfect information where you know your state as defender, but although you know the attacker’s capabilities are you don’t know what they’re actually thinking at the moment.” As the theoretical work continues, “We plan to develop some machine learning techniques to spot emerging attack patterns as they occur.”

Malacaria adds, “The idea is to use this expertise that we know how to apply at the code level in contexts where both code and humans are involved.”

Although Games and Abstraction sounds purely theoretical, Hankin and Malacaria will be working with Imperial’s business school, which will carry out empirical studies in several sectors. First is university systems, the sector about which the classical papers were written. Second is the private sector; Hankin is hoping large banks will assist with data relating to the kinds of financially motivated attacks they face. Finally, Hankin is hoping to get access to either local or central government users. In all three cases, the data will consist of a series of network states based on logs and audit trails that make it possible to trace the movement of network traffic through time.

Games and Abstraction is one of four main themes of the Research Institute in the Science of Cyber Security, funded by EPSRC and GCHQ, a collaboration between government and a group of universities to consolidate existing research and build upon it in new directions in order to create a science of information security. Games and Abstraction is led by Chris Hankin, Pasquale Malacaria, and Carlos Cid. The other three themes are Cybercartographies, led by Lizzie Coles-Kemp at Royal Holloway; Choice Architectures, led by Aad van Moorsel at Newcastle; and Productive Security, led by Research Institute director Angela Sasse at UCL. The overall goal of the Research Institute is to create good science and also to have an impact on the world of security management.

Program analysis

It sounds like magic: using a variety of mathematical techniques to analyse program code to ensure that it does what it claims without running the code, especially when you consider that a piece of software like Windows 7 has an estimated 50 million lines of code. Compilers, the software such techniques have classically been used to analyse, generally have a fraction of that. These are well-established ideas: program analysis is as old as the use of compilers; semantics-based analysis dates to the 1970s.

More recently, such techniques have been adapted to automatically debug, verify, and certify code. Using it to verify code against security criteria, as in the Games and Abstraction project, is new.

The mathematics underlying computer science, such as the Halting Problem, have long proven that it is impossible to know everything about the behaviour of every program. However, partial answers can still answer some questions.

For more background on program analysis, Hankin’s book with Flemming Nielson and Hanne R Nielson, Principles of Program Analysis (2005, 2nd corrected printing).