[V-Research] Thesis Proposals on Cybersecurity

Francesco Beltramini[1] and Marco Rocchetto[1]

[1] *V-Research, Verona, Italy*

Overview We have a question: what is cybersecurity? Or, even better, what is a cyber-secure system? People believe that cybersecurity can be defined as a property (e.g., confidentiality) but, can we say that a system in which that property holds is actually secure? Obviously not, just publish any confidentiality scheme and wait 5 minutes :) Well... maybe cybersecurity is a set of properties? Again, show me that system in which those properties hold and I bet I'll find an insecurity somewhere. So, if a cybersecure system is the one without cybersecurity attacks, is there a set of properties that makes that system secure? No! That's the point! Those who wear a black hat don't care about how we define security. Nor the entire universe. A scientific hypothesis on what a cybersecure system is must predict the security and insecurities of that system so we can empirically test the predictions (i.e. trying to hack our way into the supposedly secure system). After, and only after, one can become the "momentary [cybersecurity] master of a fraction of a dot" or desperately hope in a "better luck next time".

It is evident that an attack (an authentication bypass) is made possible by a vulnerability (a sql-injection) which, in turn, is made possible by an error somewhere in the design or implementation of a system (or procedure, e.g., an authentication system).

A : So, what if we had a system (or a piece of code) that is error-free?

B : It's impossible!

A : Ok, but what if? Wouldn't we have a secure system?

B : Well, ok... you theorist! Is having an impossible secure system of any use?

A : Maybe? While it's true that a human being cannot fly, it's also true that there are interesting approximations such as airplanes or the ESS. So, let's stop with the chattering and start building a trivial ("thanks" Rice...) system secure by trying predicting all its errors!

B : Wait... what's an error?

Sorry, "there's no royal road to science" and while it may be easy to grasp the path we're following, there's a bit of math that you've got to digest before.

If you are interested in helping us “carrying the [cybersecurity] stone”, we’ll share with you our paper on a theory of error (and we’d be happy to discuss it with you) and collaborate to one of the following thesis.

Titles In the following we list three thesis which should be interpreted more as areas where the student will start her journey, rather than a “point” that the student should follow. In other words, we expect you to build and propose your own views on the subjects, to critically analyze your steps and. . . ours too. If you don’t know exactly what we mean, opt for “I’m a believer”.

1. “I’m a believer” or “A quantitative but non-inductive approach to cybersecurity risk assessment”. Several standards mandate a secure-by-design approach in which cybersecurity shall be considered at the very early stages of the design process. For example, the DO-326A – “Airworthiness Security Process Specification” requires a cybersecurity risk assessment of the design and “are the only Acceptable Means of Compliance (AMC) by FAA & EASA for aviation cybersecurity airworthiness certification, as of 2019” as pointed out by SAE. Standards do not describe in detail how to perform a cybersecurity risk assessment and only vaguely define the overall objective, which can be summarized as to provide an understanding of the potential cybersecurity risks.

   In this thesis, the student will work on the correlation between the hypothesis that errors can be used as a measure of the cybersecirity risk and focus on one of the following (or whatever great ideas you have):

   - choose a CPS type that she likes (automotive? aerospace?) and review a relevant cybersecurity (engineering) standard.
   - review current research approaches to the cybersecurity risk assessment (e.g. CORAS)

   Want more? We already reviewed many standards and approaches and we created our own risk assessment prototype, but we are still lacking many fundamental features such as:

   - a proper formalization of asset diagrams (what the business guys want to protect) and their correlation to the engineering of systems (what the tech guys have built).
   - Proper calculation of a risk matrix (likelihood and impact) – do you have an educated guess on the likelihood of an error and on the correlations to cybersecurity attacks?

2. “I’m an engineer” or ”A formal approach to the engineering of security protocols and cyber-physical systems”. The bulk of the question is, obviously, what you want to do with your system. Can you break it down to a number of functions so that we can try to predict errors at a microscopic scale? This engineering is far from trivial, and you’ll get to know how

loosely defined are the specifications of systems, but it is always rewarding living those 5 seconds where the whole engineering seems just perfect, working. . . and then inevitable falling apart, down to "how could I believe that it was working!"

In this thesis, the student will review current approaches and languages for the engineering of systems and security protocol. He will then focus on proposing all of the following:

- her engineering view on systems and protocols, and
- a prototype engineered system or protocol so that an estimation of the cybersecurity risk is provided as a correlation between known attacks to engineering choices or errors.

3. "Pff. . . I'm a scientist, give me a challenge!" or "An attacker model beyond the Dolev-Yao one". If errors can be correlated to the engineering of system, where is the creativity of an hacker? Can we replace or confine its creativity into the boundaries of the engineering of systems?

   In this thesis, the student will:

   - be helped in building a useless transition system with the SMT solver Z3, so that she understands the basic principles behind the use of model checkers for the identification of cybersecurity attacks in security protocols,
   - study the symbolic model of attacker for the automated identification of attacks in security protocols,
   - bravely dig into the completeness of those attacker models, trying to understand the correlations between attacker models and the errors in the engineering of a system.

   We warn you, this is no thesis for "people in a hurry".

What's V-Research? V-Research is a startup and a research center on cybersecurity engineering. We want to bridge foundational challenges and engineering needs. Our mission is to develop a more scientific approach to cybersecurity and, based on that, a tool-chain for the secure engineering of cyber-physical systems. Check out our website for more info at `https://v-research.it`.

Marco is a cybersecurity researcher, co-founder of V-Research. He received his PhD in Computer Science in 2015 from the University of Verona (Italy).

He worked as Senior Research Engineer in the Security Team of the Formal Methods Research Group at the United Technologies Research Center (2017-2019), and as a Researcher at the University of Luxembourg (2016-2017) and at the Singapore University of Technology and Design (2015-2016). His research interests covers Security Engineering, Formal Security

Verification, and Cyber-Physical Systems Security. He has several publications (in international conferences and journal), and patent applications in the field of Cybersecurity.

Francesco is a cybersecurity professional, co-founder of V-Research. He's also Head of Security Operations Engineering at Inmarsat, London UK.

He received his MSc in Computer Science in 2009 from the University of Verona (Italy). He worked for four years for the European Government in London, UK as a Security Administrator. In 2015 he moved to Inmarsat as Chief Security Engineer for the Satellite Control Centre, until 2019 when he became Head of Security Operations Engineering. In his career, Francesco had the opportunity of working on a number of high-end projects in the IT and OT space, ranging from Cloud to high-assurance systems in mission-critical infrastructure.