TIM Lecture Series Cybersecurity Metrics and Simulation

George Cybenko

> *“Given the continual onslaught of successful cyber-attacks against banks, governments, and retailers, one has to wonder whether any progress is being made in computer security at all. How is it possible to reconcile the huge investments that have been made in securing networks and computers with the fact that attackers are still routinely breaching what should be highly protected networks? What metrics can explain the situation and how can we evaluate those metrics through simulation or other means?”*
>
> George Cybenko
> Professor of Engineering, Dartmouth College

Overview

The TIM Lecture Series is hosted by the Technology Innovation Management program (timprogram.ca) at Carleton University in Ottawa, Canada. The lectures provide a forum to promote the transfer of knowledge between university research to technology company executives and entrepreneurs as well as research and development personnel. Readers are encouraged to share related insights or provide feedback on the presentation or the TIM Lecture Series, including recommendations of future speakers.

The sixth TIM lecture of 2014 was held at Carleton University on October 8th, and was presented by George Cybenko, the Dorothy and Walter Gramm Professor of Engineering at Dartmouth College in New Hampshire, United States. In the first part of his lecture, Cybenko provided an overview possible security metrics together with their pros and cons in the context of current IT security practices. In the second part of the lecture, Cybenko presented a modelling and simulation approach that produces meaningful quantitative security metrics as the basis for a more rigorous science of cybersecurity.

Summary

To begin his lecture, Cybenko highlighted the many high-profile cyber-attacks that dominate headlines today, which stand in contrast to massive investments in cybersecurity research and practices, as well as the creation of many cybersecurity companies, over the past 10 to 15 years. Thus, he then challenged the research community – himself included – to demonstrate greater progress over the next 10 years in terms of our capacity to mitigate the impacts of cyber-attacks. And, in introducing the key subject of his lecture, he pointed to the potential for cybersecurity metrics and simulation as a promising avenue to facilitate such progress.

To be effective, cybersecurity metrics should be:

1. *Reproducible:* when measuring a particular phenomenon, two people should be able to independently arrive at the same results.

2. *Relevant:* organizations must find the metrics operationally relevant and actionable.

3. *A basis for comparison:* metrics must facilitate comparisons between architectures, applications, systems, networks, etc.

4. *A basis for claims:* metrics must facilitate evaluations of systems and architectures to quantify their suitability to particular applications.

In developing metrics, we must also take into account the computer security lifecycle, which progresses from security concepts (i.e., an understanding of the technology and relevant threats), to architecture (i.e., an abstraction of the design), to implementation (i.e., code, hardware, support, and access), and then to operations (i.e., forensics on past events, real-time monitoring and patching of present conditions, and predicting future events). Metrics must be considered at each step in the lifecycle so that they can be effective once the operations stage is reached.

TIM Lecture Series – Cybersecurity Metrics and Simulation

George Cybenko

Next, Cybenko recognized a common skeptical view of security metrics, which, in its extreme form, rejects the need for metrics altogether, arguing that a system is either secure or it is not. However, when challenged to provide an example of a secure system, such skeptics struggle to come up with definitive examples. Thus, in practice, it is worthwhile recognizing a spectrum of computer security and using metrics to try to evaluate just how secure a given system is.

Proposed approaches to cybersecurity metrics include:

1. *Penetration testing:* automated tools that run a set of exploits against a network; by definition, penetration tests use only known exploits and cannot assess vulnerabilities or weaknesses that might be revealed by a human attacker.

2. *Red teams:* expert hackers hired to assess or attempt to break into a system; however, the perceived protection level is limited to the expenditure on testing (i.e., a company may pay a "Red Team" $X to assess a system, but hackers would expend effort exceeding $X to reach assets of greater value, and much greater human effort may expended for the same cost in countries where the labour rate is much lower).

3. *Compliance:* controls and standards for development, software, architecture, etc.; the protection level is only as good as the compliance standards; can redirect an organization's security expenditure away from novel and up-to-date approaches.

4. *Response times:* how quickly is a system patched? How quickly does an organization identify and respond to incidents? What is the optimal policy for disclosing vulnerabilities?

5. *Software size, complexity, and constructs:* may be indicators of security vulnerability

Each of these approaches has its benefits and shortcomings; however, it may be more useful to think about the field of cybersecurity metrics within the context of risk analysis. Thus, the expected cost of security may be calculated based on the probability and costs of potential losses. For example, in cases where expected losses due to fraud and intrusions exceed the costs of technology updates, the justification for improved technology becomes clear.

Next, in the second part of the lecture, Cybenko presented an alternative, simulation-based approach to cybersecurity metrics, which attempt to quantify cybersecurity. In particular, he focused on the QuERIES methodology, which was also detailed in Cybenko's 2013 article in the TIM Review (Hughes & Cybenko, 2013). The QuERIES methodology quantifies cybersecurity risk following an analogy from physical security, where the "time to compromise" in a system is a measureable performance metric. In cybersecurity, the time it takes an attacker to complete a successful attack against a protected software system provides a similar metric, which can be simulated and then presented in a probability distribution.

The QuERIES methodology simulates the value of success to an attacker if they are able to succeed within a particular amount of time. Thus, the value of the asset to an attacker changes over time because there is a cost to continued effort, and at some point, no amount of effort may be worth the value of the target asset. And, this type of risk-analysis approach is used to assess the progression of cyber-attack, it becomes possible to calculate the optimal time for an attacker to abandon an attack based on the cost of the attack and the value of the asset. Ideally, cybersecurity defenses could be sufficiently robust that the attacker's cost of attacking would be prohibitively high, and an attack would not even be initiated.

For a fuller explanation of the QuERIES methodology, see:

Hughes, J., & Cybenko, G. 2013. Quantitative Metrics and Risk Assessment: The Three Tenets Model of Cybersecurity. *Technology Innovation Management Review,* 3(8): 15–24. http://timreview.ca/article/712

TIM Lecture Series – Cybersecurity Metrics and Simulation

George Cybenko

About the Speaker

George Cybenko is the Dorothy and Walter Gramm Professor of Engineering at Dartmouth College in New Hampshire, United States. He has made multiple research contributions in signal processing, neural computing, information security, and computational behavioural analysis. He was the Founding Editor-in-Chief of both IEEE/AIP Computing in Science and Engineering and IEEE Security & Privacy. He has served on the Defense Science Board (2008–2009), on the US Air Force Scientific Advisory Board (2012–2015), and on review and advisory panels for DARPA, IDA, and Lawrence Livermore National Laboratory. Cybenko is a Fellow of the IEEE and received his BS (Toronto) and PhD (Princeton) degrees in Mathematics.

This report was written by Chris McPhee.

Citation: Cybenko, G. 2014. TIM Lecture – Cybersecurity Metrics and Simulation. *Technology Innovation Management Review*, 4(10): 43–45.
http://timreview.ca/article/839

Keywords: cybersecurity, metrics, simulation, modelling