Is the cloud secure or is chocolate good for you?

Kate Netkachova and Robin Bloomfield, City University of London and Adelard LLP

It's a lovely morning in a university classroom, the early spring sun streams through the windows making the atmosphere bright and cheerful. The smell of chocolate is in the air as the students – security professionals - are enthusiastically working on their task. It is the first day of the Assurance Cases module and they have just been introduced to the concept of Claims, Argument, Evidence (CAE) [1][2], which is used to develop complex engineering justifications. However, the engineering systems will come later. For now, the students are applying the approach to create a convincing argumentation about the chocolate they are eating.

The task is performed in groups with different teams working on contradictory top claims:

- Team 1: Chocolate is good for you
- Team 2: Chocolate is bad for you

But fear not, both teams are very positive they can demonstrate the truth of their claim. Students are actively collaborating to share ideas, split the top claim into subclaims, search the Internet for relevant evidence and counter evidence and develop a strong argument supporting the top claim. Along the way, they are becoming more fluent in CAE and gaining some initial practical experience in creating structured argumentation.

Finally, it is time to present the results. Both teams have done a great job and come up with a logical structured case supported by reliable evidence, such as research studies and scientific papers, showing that their top claim is true. The arguments are sound and convincing resulting in a reasoned conclusion that each of the top claims is true.

But how is it possible at all? The two claims are completely opposite yet both can be shown to be true.

That's the moment when the students can grasp the main focus of this assignment…

The importance of detail

The idea of the exercise is for students to recognise, early in the module, the importance of being precise about your claims, identify the specific context, environment and all the related details before coming to any conclusions.

With respect to the assignment, the ingredients are important. What is defined as chocolate? How much cocoa powder, sugar, saturated fat, soy lecithin, preservatives and other components are we looking in? Who is the claim about? The health effect may be very different for someone with obesity, diabetes or nut allergy compared to a perfectly healthy individual. What is the amount, are we implying it is consumed in moderation? Health benefits can be quickly outweighed by the risks if the amount is increased so it is essential to be clear about any assumptions we make.

For engineering systems this is even more paramount. The decision to trust an engineering system – whether to fly in an aircraft, to turn on a power station - can have real world, societal, environmental and economic consequences. Engineering arguments have a number of characteristics, they are multidisciplinary and science based with mathematical models and simulations supporting the justification. The overall confidence in any aspect of the system has to take into account a number of details. These range from technical considerations (e.g. to prove that the software works as intended) to various social aspects (e.g. whether we can trust the operators) and is always a judgement made within a particular organisational context to develop a view of the system as whole.

The context, the environment, the boundaries of the system and other specific details have to be clearly defined before any claim can be demonstrated or any important decision made.

The advent of cyber issues and the increasing sophistication of attackers bring even more challenges to the decision making process. A number of analyses need to be performed to address security aspects in addition to the traditional techniques used to assure the system and achieve confidence in engineering decisions. One approach to dealing with this complexity and taking into account a wide range of issues and technical considerations in a structured and rigorous way is assurance cases.

Assurance cases are used for justifying and communicating the trustworthiness of complex systems. The definition of an assurance case is: "a documented body of evidence that provides a convincing and valid argument that a system is adequately dependable for a given application in a given environment". [2]

Security-informed Assurance Cases

The module we teach is called Assurance Cases, but it is designed with the focus on cyber-security and is delivered within an MSc course in Management of Information Security and Risk.

Security analysis is frequently seen as a separate activity, with its own standards, regulations, culture and engineering. However, there is a growing realisation that security is closely interconnected with

other properties and should be integrated into the existing analyses rather than performed separately.

In order to create an integrated approach, we have enhanced the existing assurance case methodology to analyse and communicate security explicitly [3][4]. In this way, we can have cyber-security aspects considered with other critical system properties in an integrated manner within a security-informed assurance case.

Developing the approach, we have found that a significant portion of an assurance case will need to be changed in the light of security considerations [4]. Incorporating security impacts the design and implementation process as well as the assurance, and the approach to verification and validation. Some of the most significant considerations from a security perspective involve resilience and recovery capabilities of the system, both in response to malicious events that may change in nature and scope as the threat environment changes and non-malicious issues occurring during the operation. Other important aspects include supply-chain integrity and mitigation of the risks of system components being supplied compromised or having egregious vulnerabilities, design changes to address user interactions, training, configuration. Addressing software vulnerabilities might lead to additional functional requirements for security controls and new policies introduced within the organization.

Assurance cases support the rigorous argumentation. But it should be noted that the judgments in cases will not always be purely deductive. Assurance cases are complicated, they will contain inductive reasoning and require expert judgement to decide whether they provide sufficient confidence in the decision.

Assurance cases help to develop a wider view of the system and see a bigger picture, as they can combine the technical depth with a socio-technical view, analysing human aspects within the system, interdependencies, security culture and practices in place. Security-informed show how the technical security aspects fit in the broader system context, provide the method to systematically explore security issues, analysing their impact and achieving confidence in the security-related decisions made.

Combining security with a wide range of other issues is a complex endeavour and at the heart of this task is a full awareness and understanding of hazards. A detailed hazard analysis has to be conducted and integrated into the assurance case to become part of the overall decision making process. Below we present our approach to conducting such analysis with respect to security.

Hazops for Security

A hazard and operability study (Hazop) is a systematic approach to the identification of potential hazards and deviations from design and operating intention. It is widely used for industrial safety-critical system architectures as qualitative technique to identify potential hazards and operability problems.

Security considerations can have a significant impact on the analysis as cyber-issues present additional risks to integrity and availability of the system. To bring security into focus, we have developed a security-aware Hazop analysis by adapting the traditional Hazop method to explicitly address security and extending it with additional interpretation for the guidewords to facilitate the identification of security-related hazards. The common guidewords with some examples in a computer context are provided in the Table 1 below.

Table 1: Hazop analysis guidewords with examples

Guideword	**Example**
No	No message sent
Invalid	Illegal format
Wrong	Wrong data format
Inconsistent	Mismatch between data sets
As well as	Additional message
Other than	Wrong message source, destination
Part of	Element of message is missing

Prior to performing the analysis, a simplified architecture diagram is created to capture the most relevant components and system interfaces. Each interface on the diagram is then systematically analysed applying the guidewords above. For security-informed Hazop, the focus is on security-related causes while other types of (accidental) causes are considered for the full analysis. The following aspects needs to be addressed with respect to security:

- Identify potential attacks
- Assess if an attack has credible causes
- Capture any questions arising
- Explore potential consequences
- Record any recommendations to prevent cause(s) or reduce consequences
- Define any actions or follow-up activities needed

In practice, the security-informed Hazop analysis is conducted at enhanced multidisciplinary team meetings, which bring together the knowledge and expertise of people working on different areas of the system. One important aspect of the approach, which makes it very effective, is that the team is exploring the field while performing the analysis. As consultants, we explain the method and guide the process by facilitating the discussions and capturing all the input. But the main insight is provided by the experts in the system and our task is to leverage the experts and assist them in identifying security-related hazards and incorporating them into the assurance case.

This method for performing a security-informed hazard analysis is based on extensive Adelard's experience. We have used it in a number many complex systems and large-scale critical infrastructures and has shown to be useful in addressing security threats and assuring systems that need to be both safe and secure. This is an active research area and there are other related candidate approaches such as STRIDE [5] or cyber-security CMM [6][7] to consider as well.

Teaching the complex concepts

As security-informed assurance cases are complicated and rely on other methods and concepts, we need to adopt pedagogical approaches to deal with the complexity. The approach we use is a spiral learning (Figure 1), where first the basic concepts of the subject are introduced, and then the concepts are repeatedly revisited with more details building upon them [8]. Being practitioners ourselves, we very much support the idea of "hands-on learning" or "experiential learning", which shows that students learn best by doing (these have been extensively supported by the literature [9][10][11]. So we introduce various practical activities and workshops at different stages of the spiral model. Thus, both theoretical knowledge and practical skills are developed by the end of the module.

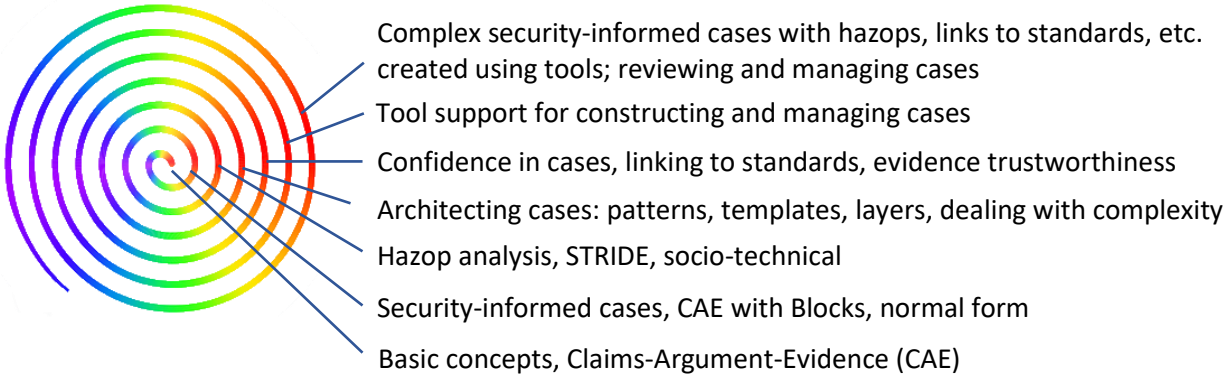

Figure 1: Spiral model for teaching security-informed assurance cases

To facilitate students learning, we use the case studies approach, which has been shown to be a useful pedagogical tool by a lot of educational research [12]. It is an effective way to involve students into the experiential learning cycle [13], expose them to real-world problems increasing motivation and interest in the subject. [14]

We use students' interest and real world problems to drive the case studies. This year the shared interest was cloud security. The students of our module are mature security professionals and many of them have worked for organisations that are using various cloud services or have plans to move into a cloud in the future. So they are interested to understand whether the cloud solutions are secure and assurance cases can be a useful approach to deal with this question.

Head in the clouds

Cloud computing is an increasingly growing market. According to the latest report by Gartner [15], the worldwide public cloud services market value is projected to be $246.8 billion in 2017. The highest growth of 36.8 percent will come from cloud system infrastructure services (IaaS) as their adoption becomes increasingly mainstream. The software as a service (SaaS) market will see a slightly slower growth and is projected to be up 20.1 percent in 2017 according to Gartner.

However, even though cloud computing can provide many benefits to organisations, such as greater business agility, scalability, flexibility and cost optimisation, information security remains a major concern. With cybercrimes being one of the fastest growing economic crimes [16] and digital technology driving many of the them, companies are increasingly interested in how to protect their data and minimise cyber risks when adopting cloud solutions.

The most common top claim students initially make is: 'a certain cloud solution is secure'. However, as demonstrated with the chocolate example, such a claim is too broad and too vague for meaningful analysis.

There is no such thing as absolute security. Various details relevant to a particular organisation need to be taken into account before any conclusion can be made. For example, the users of the service need to be clearly identified, the range of devices, data types and usage patterns analysed. As a result, a more specific top claim would probably look like this:

"The cloud solution A within organisation B provides sufficient level of security for its staff to use for corporate data C on devices D."

Starting from this top claim, the case will be expanded further to provide a more detailed analysis. Students will need to clearly identify the boundaries of the system, specific context and system

environment, responsibilities and legal obligations, requirements from regulators and other stakeholders. They will also need to identify what is considered to be sufficient in this context.

Security-informed Hazop analysis presented above is at the heart of the assurance case as many of the details will emerge while analysing the hazards. The results of the analysis needs to be fully integrated into the case with the integration clearly justified to make sure it becomes a proper part of the overall decision making process.

Another issue to address is that evidence has to be clearly distinguished from information. These two are often confused by students resulting in problems with the justification. Information can contain any data such as text documents, numbers, statistics, but it does not automatically lead to any conclusions. Evidence, on the contrary, is very specific, it is only relevant data supporting or undermining a claim. In the assurance case it needs to be very clear what exactly each piece of evidence is showing and what conclusions it supports.

Additionally, evidence should not be confused with claims. For example, one common mistake is to use SLA as an evidence for the achievement of certain requirements. However, SLAs only provide promises, not the actual evidence that the service has been delivered in accordance with the SLA. Therefore these should generate claims and require the supporting evidence that the SLAs are achieved.

Unfortunately, there is often a big difficulty for students to obtain the actual evidence documents from the manufacturers. Some cloud providers are very generous with the information they provide about their services but the actual evidence is hard to find. Oftentimes evidence may only be partial, or have restricted viewpoint. But it is still important for students to at least identify the evidence that needs to be obtained as this is an important skill in the professional context.

The overall cases produced by the students at the end of the module are quite detailed: this year's average case contains 93 nodes, with 37 claims, 25 arguments, 27 evidence and 4 other nodes. The students used the CAE Blocks approach [17] with some tool support [18] to help them structure their cases. On average, a coursework case contained 10 decompositions, 2 substitutions, 2 concretions, and 19 evidence incorporation blocks.

Conclusion

Going back to the question asked in the title, there is no right answer or one truth for a generic question like that. It's not possible to tell whether a cloud is secure or not, or if a chocolate is good or bad. But there are approaches that can help you to define more clearly the decision you are making, scope the issue, identify the relevant details, collect evidence, narrow down the options and

eventually make a decision for particular requirements within a certain context, with specific application and environment.

The claims, argument, evidence (CAE) framework is one such approach that we use and teach to students. CAE supports complex decision making processes by providing a method for creating structured argumentation. It requires scoping the issues, identifying the detailed claims, collecting specific evidence and developing a structured convincing and valid argument to justify the resulting decision.

But there is more to it than just a framework – it's a whole mindset change. In their evaluation reports, students have reported becoming more mindful of claims the make and more conscious about statements from others. They are more aware of the need to identify specific evidence, question the arguments and go deeper into analysing the issues rather than accepting generic claims.

Kate Netkachova is a lecturer and researcher at the Department of Computer Science at City, University of London and a product manager at Adelard LLP, a dependable systems consultancy. Contact her at kateryna.netkachova.2@city.ac.uk or kn@adelard.com.

Robin Bloomfield is a founder of Adelard LLP and a professor of system and software dependability in the Department of Computer Science at City, University of London. Contact him at reb@adelard.com or r.e.bloomfield@city.ac.uk.

Acknowledgements

This work has been partially supported by the UK EPSRC project "Communicating and Evaluating Cyber Risk and Dependencies (CEDRICS, EP/M002802/1)" and is part of the UK Research Institute in Trustworthy Industrial Control Systems (RiTICS).

References

1. ISO/IEC 15026-2:2011, "Systems and software engineering — Systems and software assurance, Part 2: Assurance case," 2011.
2. R. E. Bloomfield, P. G. Bishop, and C. C. M. Jones, P. K. D. Froome, "ASCAD – Adelard safety case development manual," London, 1998.
3. Netkachova, K. & Bloomfield, R. E. (2016). Security-Informed Safety. Computer, 49(6), pp. 98-102. doi: 10.1109/MC.2016.158

4. R. Bloomfield, K. Netkachova, and R. Stroud, “Security-Informed Safety: If It’s Not Secure, It’s Not Safe,” Software Eng. for Resilient Systems, A. Gorbenko, A. Romanovsky, and V. Kharchenko, eds., LNCS 8166, Springer, 2013, pp. 17–32.
5. The STRIDE threat model, 2005, Microsoft Corporation; https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx
6. Cyber Security Capability Maturity Model (CMM) - Pilot, Global Cyber Security Capacity Centre University of Oxford, 2014 retrieved from www.oxfordmartin.ox.ac.uk
7. US Department of Energy (DOE) Cyber-security Capability Maturity Model (BuildSecurityIn) Department of Homeland Security - https://cwe.mitre.org/top25/ 2016.
8. Bruner, J. (1960). The process of education. Cambridge, MA: Harvard University Press.
9. Gibbs, G., 1988. Learning by Doing: A Guide to Teaching and Learning Methods; http://www2.glos.ac.uk/gdn/gibbs/index.htm
10. Wenglinsky, H., 2000. How teaching matters: Bringing the classroom back into discussions of teacher quality, USA: Princeton, NJ: Educational Testing Service.
11. Beard, C., 2010. The experiential learning toolkit: blending practice with concepts. London: Kogan Page Limited.
12. Davis, C. and Wilcock, E. Teaching Materials Using Case Studies guide; http://www.materials.ac.uk/guides/casestudies.asp
13. Kolb, D. A., Experiential learning: experience as the source of learning and development, 1984.
14. Mustoe, L.R. and Croft, A. C. Motivating Engineering Students by Using Modern Case Studies, European Journal of Engineering Education, vol. 15, no. 6, pp. 469-476, 1999.
15. Gartner, Inc.; http://www.gartner.com/newsroom/id/3616417
16. Risk UK, http://www.risk-uk.com/double-digit-rise-in-crime-against-uk-corporates-as-cyber-becomes-fastest-growing-form-of-economic-criminality/
17. R. Bloomfield and K. Netkachova, “Building Blocks for Assurance Cases,” Proc. IEEE Int’l Symp. Software Reliability Eng. Workshops, (ISSREW 14), 2014, pp. 186–191.
18. K. Netkachova, O. Netkachov, and R. Bloomfield, “Tool Support for Assurance Case Building Blocks, Providing a Helping Hand with CAE,” Computer Safety, Reliability, and Security, F. Koornneef and C. van Gulijk, eds., LNCS 9338, Springer, 2015, pp. 62–71.