Developing a Secure Programming Module to cope with Modern Vulnerabilities

Mr Nigel McKelvey
Letterkenny Institute of Technology, Port Road, Letterkenny, Co Donegal, Ireland
e-mail: nigel.mckelvey@lyit.ie

ABSTRACT

A In a society reliant on software, it is imperative that students are provided with appropriate skills in order to deal with ever increasing types of attack. Facilitators should provide students with an understanding both of the theoretical concepts underpinning vulnerabilities and also how to implement remediation strategies in modern object oriented programming languages. Facilities should be provided that allow pupils to demonstrate an understanding of software constructs and practices that can result in problems either from malicious or inadvertent intent, and demonstrate how to defensively program for these in an object oriented programming language. They also need to be able to evaluate security implications and issues relevant to creating secure software. Finally, students need to be able to design and implement applications that use security management techniques. Graduating with these core skills should prepare industry better to deal with the issues they are facing daily.

Corresponding Author:
Mr Nigel McKelvey
Letterkenny Institute of Technology, Port Road, Letterkenny, Co Donegal, Ireland
e-mail: nigel.mckelvey@lyit.ie

1. INTRODUCTION

Even in today's security conscious world, secure code is something that still eludes many developers. It is apparent that many graduates are leaving colleges and universities without many of the skills necessary in order to develop and maintain secure applications. When developing a curriculum, it is important to introduce these core secure coding skills from the outset [1].

In their paper "What is the Curriculum Development Process?", Clarke and Stow state that the term curriculum is “a written plan which drives instruction. It delineates the skills and concepts taught and evaluated to enhance student achievement. Composed of a content area philosophy, strands with definitions, program goals, aligned scope and sequence, learner outcomes, and assessment tools, it is intentionally designed to meet district, state, and national standards.” [2]

2. DEVELOPING AN APPROPRIATE CURRICULUM

Often the issue with developing a curriculum for a module within an IT discipline is that technology is constantly evolving. As a result, a module can become quickly outdated and below standard. Students deserve a module that will teach them about technologies and concepts that are current and relevant to their future careers. Incorporating reflective practice as teaching professionals can greatly help with this common issue. Misguided or redundant concepts can be removed or updated incrementally. This in turn goes some way to developing a curriculum that satisfies the requirements. This review should provide some insights into how developing a curriculum for IT can be problematic and also present some thoughts on how this might be addressed.

It is imperative that teachers and facilitators strategically align programme learning outcomes with module learning outcomes so that students can acquire the technological skills required by both educational establishments as well as by society itself [3]. The responsibility for this curriculum falls on the facilitators and governing bodies of particular schools/colleges. With this responsibility comes accountability for the academic well-being of individuals and groups of people [4]. Ensuring that graduates in programming can create code that will withstand a potential attack is extremely important to both an employer and also the client that uses the product itself.

It is evident that planning a successful educational framework within IT requires certain elements to be addressed effectively. Three strands identified are: technological practice, knowledge and nature [5]. With regard to technological practice within an IT discipline, this entails students reviewing relevant case study material and/or implementing this knowledge through practical classes using the relevant software development tools. The technological knowledge itself should be generic and broad. So the students can have knowledge in as many different areas of their discipline as possible. Students should be encouraged to research and develop in areas that are not necessarily taught directly in the curriculum. Finally, the nature strand refers to the students' abilities to relate technology to and differentiate technology from human life [5]. This in turn provides students with invaluable skills before entering the workforce.

3. **SECURE CODING EVOLUTION**

The relevance and importance of secure coding has evolved in recent years. Figure 1 depicts some of the most famous recent hacks.

Some famous security breaches

![Figure 1. Famous security breaches](image)

As a result of these attacks (and lots more besides), companies are now becoming much more aware of the dangers that an attack can have. Loss of revenue, loss of hardware, loss of a customer base and a loss of reputation. It is therefore essential that employees, developing software on their behalf, have the ability to identify security holes in code, analyse the potential risk and devise a suitable plan to resolve the issues in a timely manner.

Providing students with these skills is essential if a computing course is to survive in today’s competitive market.

3.1. **Security in the Cloud**

Cloud computing is a hot topic at the minute. Its development has enthralled the imagination of the IT world about the possibilities the cloud will have in the future. However, the many benefits that the cloud promises have been equalled by the many issues that currently exist in the technology. Several companies have compiled check-lists that consumers should use to aid their decision in getting the right clouds provider. In June 2008, U.S analyst firm Gartner released a security risk assessment form that lists seven major security risks in the cloud that customers should question providers about when deciding upon the right vendor to select [6].

3.1.2. Gartner’s Seven Cloud-Computing Security Risks

a. **Privileged User Access**

This is one of the main cause of concern in the cloud. Who has access to the data? Customers fear over their sensitive data being accessed by an unauthorised user. The adoption of cloud computing relies
heavily on trust. Enterprises are unsure about the ramifications of giving away their data, especially sensitive data. It is a reasonable concern to have, as privacy has been an on-going issue in IT, long before the cloud was created. In today's world, several companies contain personal information about clients, partners etc. The introduction of the cloud, where that information is passed on to another company, sheds more light on the issue of privacy. The majority of companies are motivated by the cost savings of the cloud and not by security [7].

There are many privacy dangers that lie in the cloud, such as data leakage and disclosure. The very nature of the cloud presents privacy concerns. Is data safe in the cloud? When so much data from various organisations are stored in the one place, the data becomes more susceptible to getting lost. More so, the companies control over the data has been reduced as cloud provider employees have access to the data. This can lead to accidental or indeed deliberate discloser of data to other organisations, including rivals and companies under false pretences. Customers have every right to fear their privacy when data about them gets lost or given to advertisement agencies. It is strongly advised that consumers question the access control policies that vendors use and how well they control it.

b. Regulatory Compliance

Before the cloud was introduced, companies processed and stored their data in house. Logs would record data transactions and user access to ensure there has been no illegal activity. These logs can be audited to aid the monitoring of the company. However, auditing does not happen in the cloud, at least to say, by third parties. As stated by Gartners seven security risks, many cloud vendors refuse to allow auditors to come in and audit the cloud. From a consumers perspective, their is not a lot that they can do, other than to try and find a cloud provider that allows auditing. Their is no set standards at present, that would ensure cloud providers are compliant. Currently, many cloud computing vendors do not hold any security certificates and decline external audits taking place. Such vendors are advised to be avoided as ultimately, they leave the consumer responsible for their own data, even though they do not hold it in house.

c. Data Location

Consumers are usually unaware of the location of their data. Many organisations that use the cloud have no idea where the data is being stored, other then in the cloud. The cloud could be anywhere around the globe. This might not seem like an issue at all for several organisations, but when data is being stored in a different country that has a different jurisdiction, then it can become a problem [8].

Some Countries are very lax about law surrounding data, which could lead to a another legal issue if something where to happen the data. On the other hand, a Country could have laws prohibiting the use of specific data that organisations have, which again can lead to another legal issue. Enterprises must ensure for their own safety that the location of the data is specified, to reduce the risk associated with outsourcing to another country. The danger of this is that the location of the data could be in a different country that's law may prohibit certain data. Consumers have the right to know where there data is going and in certain cases, should be able to ask for their data to be kept in a specific jurisdiction.

d. Data segregation

In a public cloud, data from various different companies are generally in a shared environment. The consumer should have the right to know how the provider segregates data. Encryption is a common approach used by the cloud but is the encryption they use reliable enough that will ensure minimum risk of your data getting lost?

e. Recovery

If your data does go missing, how do you get back? Enterprises should be asking potential vendors about their recovery plan should anything such as the hard drive fail, power surges or even a natural disaster. The provider should have recovery plans in the event of such catastrophes. A cloud vendor might also decide to hold the data hostage in the event of a dispute, which would make recovery plans redundant.

f. Investigative Support

Investigating the activity of a cloud provider extremely di-cult. As mentioned above, many cloud providers do not allow audits to be performed. A enterprises cloud vendor should comply with audits to ensure it is not participating in any illegal activities.

g. Long-term Viability

Cloud computing has a very bright future but do all vendors have the same sustainability. No company can guarantee their customers they will not go out of business. Customers know what will happen if
the cloud company goes bust. Indeed the cloud can be bought over by another cloud vendor. Gartner believe the customer is entitled to know how to get there data back should anything happen the company [6].

3.2. Equipping Students

Providing students with the necessary skills is essential if graduates are to be capable of identifying and dealing with these issues/vulnerabilities. With regard to developing core secure programming skills, students should be able to implement code that deals with providing appropriate access visibility to classes/methods/variables, be able to facilitate trust boundaries, remove inference from thrown exceptions, understand the dangers of dynamic SQL, have the ability to interpret untrusted code, isolate unrelated code, be familiar with subclass behaviour, implement mutability correctly, code defensibly against partially initialized instances, avoid serialization, implement the Security Manager and comprehend context transformation.

Messages being intercepted and manipulated can have serious repercussions for a company who deal with Internet Protocols (IP) and network management [9]. Being capable of implementing correct encryption is paramount to any secure programmer.

Producing students with programming skills in these areas will ensure that their future employers will have considerably safer applications. Not implementing these skills into a module at third level would be doing considerable injustice to the students themselves.

4. CONCLUSION

In conclusion it is important to state that colleges and universities have to develop a curriculum for IT which will facilitate their marketability as well as their functionality in the educational and industrial markets, [10]. Using and incorporating Virtual Learning Environments (VLE) into a curriculum can help catapult a previously mundane module into the 21st Century. Within this "virtual reality", both the facilitator and the students can partake in a variety of curricular and extra-curricular activities [12]. This modern inclusion is a must moving forward when developing a curriculum for IT. A facilitator could easily teach elements of securing programming via this method which would obviously provide the students with instant feedback, thus ensuring bad habits are never started.

REFERENCES


BIBLIOGRAPHY OF AUTHORS

Nigel McKelvey Lecurer in Computing at the Letterkenny Institute of Technology, Co Donegal, Ireland.