Tele-Lab: Virtual AND Practical training in ICT Security

The future of training in ICT Security

The growing importance of the issue of Security in Information Technology, as presented in the media almost daily, and the serious consequences that can result from deficiencies in this matter, it ever increases the need for more awareness as well as the need for training in ICT Security, both theoretically, but also more importantly towards the acquisition of practical skills.

ICT Security is one of the most challenging areas regarding education and training, both in academic and professional level. The requirement for hands-on practice with realistic attacks in real systems makes the training of ICT Security a complex task, demanding in time, resources, expertise, with constant demands for renewal of educational material and upgrading of systems so that the training can cope with the real, constantly changing world.

Contemporary challenges and problems in "traditional" ICT Security training.

Traditionally, training in ICT Security takes place in laboratories with networked computers loaded with all sorts of systems and configurations, as well as many types of networking devices (such as routers, hubs / switches, servers running various services etc).

The implications and the difficulties arising from the abovementioned arrangement are many and complex. First, there is the issue of cost. By their nature, ICT Security training laboratories should be solely dedicated only for this specific purpose: this means high costs of purchasing and maintaining equipment that can not and should not be used for any other purposes. Furthermore, the continuous upgrading of all systems constantly requires skilled personnel to be present and this increases costs - plus the fact that after each exercise / attack / destruction, the systems must be restored, every time, back in their original state. In addition, each exercise requires a different configuration, so the alternation and reconfiguration of systems that is needed in order to meet the requirements of each exercise can be a full time occupation on its own.

Of course, there is the issue of security during the training itself: an ICT Security training lab should be completely isolated from the rest of the infrastructure of an educational institution or a company. Why? Simply, if, for example an exercise requires the destruction of a database on a server, then who can guarantee that the targeted database will not "accidentally" turn out to be a database of the university or company, rather than the training database! It's like there's a workshop inside the building with people learning how to "play" with explosives.
As we see, these difficulties and risks make practical training in ICT Security very demanding on resources / costs and expertise, often beyond the abilities of a educational institution or a company to implement it. On the other hand, the need for training staff and students in ICT Security still persists and growing! Every now and then we hear in the news about how easy it is for a hacker on the other side of world to hack into systems belonging to governments and large corporations and (sometimes, relatively easily!) to steal data, destroy software and bring total chaos. Many of these attacks become possible exactly because of lack of training of staff in those organizations: for example, what's the use of having the best firewall when employees can not recognize a phishing scam, and what's the use of having the most expensive security system when your technical staff forgets to update it, leaving it so prone to malicious hacker penetrations. This means, that training in ICT Security should not be limited solely to relevant technical and professional staff, but up to a certain degree it should be extended to train the rest of the staff of an organization.

**Is Virtual Training Sufficient?**

With the rise of Cloud Computing and online training, one can easily rush to give a "solution" to the problems of ICT Security training mentioned before: "Load the entire curriculum in an online e-learning system such as Moodle.org, Place 2-3 simulations and exercises in the form of Java / Flash animations, and leave learners to learn by themselves".

This model may work beautifully in other educational domains, but as far as ICT Security concerns, the existing half-virtual educational systems can not provide the necessary level of training that is required! You simply can't have a predominantly theoretical ICT Security training course: it is like trying to learn how to make love by reading a manual – without practice, it simply cannot be learned!

Therefore, it is not enough to just have a few simulations (which do not "play" with real systems and real machines, but rather with programmed animations) to deliver training in ICT Security in the proper depth and level. By contrast, it requires real machines, real attacks on real data, which can inflict actual interception and destruction to the targeted systems.

Additionally, any part of the online education should be combined with real-life teaching with the complementary guidance of a qualified instructor.

**Tele-Lab: A Step Further**

Tele-Lab is a training platform that provides both practical and academic training in ICT Security through the Internet. Beyond the traditional e-learning systems, in Tele-Lab, the learners can immediately apply the knowledge they have gained through practical exercises. The innovation here is that the practical exercises utilize dynamic virtual machines which replicate systems, data, network devices and topologies in an entirely realistic manner - essentially rendering the attacks in such a way as if they are taking place in a real «physical» environment.
In other words, on one hand Tele-Lab provides an entirely independent way of learning where learners need only a browser and an Internet connection to access knowledge at any time, and on the other hand it provides a sophisticated system that offers realistic practical training through virtual laboratories, which they replicate each attack environment by using virtual machines which are "born" on the initiation of an exercise and are destroyed at the end. This way of implementation offers more possibilities for practical training than other training systems that can only provide some simulations/animations.

In contrast to the aforementioned difficulties that exist in a physical ICT Security training laboratory, Tele-Lab overcomes those difficulties by offering "peace of mind", but without making any deductions from the valuable practical experience that a physical laboratory would provide. This is achieved by taking advantage of the virtual machines' ability, which allow easy and quick deployment of an operating system runtime environment, as well as quick and easy system restore in case of damage. Tele-Lab uses this feature to restore the virtual machines to their original state after each use (damaged by an attack in a practical exercise). This is an important advantage over the usual arrangement of a physical training laboratory since the baseline condition can be restored faster, more often and without the need for any manual handling by laboratory staff.

With the provided isolated virtual laboratory environment, Tele-lab allows learners to use and reconfigure the available resources and perform attacks as much as they want and in whatever way they want - without posing any risk to themselves, or server, or third parties. With the virtual network of Tele-Lab, in which the Virtual Machines are interconnected, it is possible to execute complex attacks, such as «Man-in-the-Middle» attacks, or scripted electronic communication with a virtual victim.

**Applications of Tele-Lab in ICT Security Training and Education**

Tele-Lab enables universities and enterprises to implement a training program on ICT Security with less costs of purchase and maintenance, and with less effort. It also allows applications to other service models, such as offering training subscriptions over the Internet to businesses and individuals (as said before, all that is needed is a browser).

More importantly, however, is that it enables collaboration and sharing of resources among partner institutions, in order to make the very demanding feat of ICT Security training feasible and successful.

As an example, such kind of cooperation among universities has been implemented between Hasso-Plattner-Institut ("HPI", University of Potsdam in Germany) and Vilnius Gediminas Technical University ("VGTU", Lithuania), where the Tele-Lab servers located at the two institutions share resources between them in order to provide dynamic virtual machines to each other whenever requested. For example, if a student from VGTU chooses to run a practical exercise, if at that particular instance the Tele-Lab server in VGTU has already reached the maximum limit of virtual machines that can allocate to users, then it automatically requests from the Tele-Lab server at HPI to allocate a virtual machine from its own resources (and vice versa, of course). This automated process runs seamlessly and smoothly, so the learner does not become aware of any interruption.
In the future, a cooperation like this could easily be extended to build a network of cooperation among several institutions, who will share between them the resources of each other's Tele-Lab server. This will achieve a uniform distribution of the total processing load, e.g. in times where there is a peak of demand for virtual machines at the campus of one of the partners.

The exchange and the creation of new syllabus modules and expertise among educational institutions through Tele-Lab constitutes another important dimension to cooperation. The system can easily be enhanced with new content. For example, in a partnership between universities and companies from Germany, Lithuania and Cyprus, new learning modules have been easily added to the Tele-Lab server of VGTU (http://telelab.vgtu.lt) and then have been shared between the partners' consortium. Furthermore, as part of the localization, the curriculum was translated to the Lithuanian language and integrated into the system, with plans for translation into Greek in the near future.

This implementation of the Tele-Lab project is a partnership of: Hasso-Plattner-Institut (University of Potsdam, Germany - www.hpi.uni-potsdam.de), Vilnius Gediminas Technical University (Lithuania - www.vgtu.lt), nSoft (Lithuania), and Amalgama Information Management Ltd (Cyprus - www.aimcy.eu). The Project "Tele-Lab - virtual IT Security Lab" has been funded with support from the European Commission under the program Leonardo da Vinci / Transfer of Innovation.

Orestis Tringides
orestis@tringides.com