

老师:

您好!

我们现在希望寻找吸引学生参与一个关于网络信息安全测试系统的工程项目。
(CAPSTONE PROJECT)

我们有崭新的无先例的技术能够阻止机器被攻击。我们正走向公共规范标准，目前我们寻找一些学生帮助我们做一些测试。你们学校能帮助我们找到一些你们认为有可能参与的学生小组吗（3-5 人）？

请将有可能参与的学生小组的联系方式转告我们。

以下是项目的简介

BLUEICON 技术

BI3 道德攻击的挑战

2011 年 创新安全机会

介绍

Blueicon 技术运作 Fielden 教授的 R&D 工作有很多年。在最新发展中，Fielden 教授显示了可能保护所有机器以防止网络攻击的一个新颖的机制。Blueicon 技术正为共同的标准检定准备。因为鉴定是一个昂贵的过程，Blueicon 技术希望对学生提供机会，在系统递交之前为了淘汰潜在的错误来测试各种各样的配置和评估安全模型。

这项技术强调恶意主人问题和恶意客户问题。为了通过充分保护计算机免受从网络的所有已知的或未知的弱点提供保护。

这项技术是对要求极端信息安全高水平组织和产业有意义，例如军事的，政府，石油，气体& 能源 项目。这项技术会对为希望提高安全级别的那些准备重新编写暗码的组织极有意义，因此费用/收益不一定值得。

项目描述（充分的计划简报在 2011 年 2 月提供）

评估一项承受网络攻击的新颖的信息设计系统结构。了解部署并且测试它。学生将需要评估新颖的安全结构和系统地考虑怎样可能发动攻击或者总结当系统看似安全但证实系统损失。

学生是不必要进入开发的 Windows 系统，亦不必进入任何机器或设备。相反，会提供一个实际的框架让用户测试 WINDOWS 的环境。本科学生和研究生会用那些被认为有弱点的过时的操作系统以证实他们可以阻止远端攻击。

虽然一部分项目涉及一些用传统渗透测试工具扫描这项技术，大部分工作将是集中在为找到进入通道分析模式和结构。这个项目将涉及建造特殊的实际配置然后测试由其他相似的大学的队实施。在项目能闯进另一个对的实施情况下，然后他们要求在一个恰当的配置的系统书面提供他们如何达到的。

宗旨（方案详情也许在任意时候会有变化。这是一个商业项目，并且在学术学期周期外面更新）

部分 A-系统的实施。了解一般结构，运用提供的工具和类装配实施。恰当地配置系统与提供的部署框架符合。

部分 B-被理想化的盘剥的结构。学习提供绝对信息安全 (TAIS) 的理论并且估计模型可能回避为了减弱信息系统的方式。若可能，修建盘剥并且适用于您自己和其他队的部署。如果适用，谈论怎么可能找到缺点。或者，认为系统看上去安全并且包括您的推理至于为什么如此。

部分 C-工具状态评估 谈论。提供的工具遵守绝对信息安全的理论服从的水平并且谈论什么按顺序仍然需要达到服从。包括宽广的讨论至于实施多远应该去达到实际的安全。提供一个评估(例如咨询角色)对系统的能力承受攻击。

特殊性

将要求小队在 Linux 或 Windows 机器遥远地工作使用主持的 OpenVPN 和的 VirtualBox 部署。BI3 仿真器原始代码是可利用在 Java 语言，虽然不编程被期望，除之外展开盘剥(如果必须)。学生将下载渗透检验的修造并且上载他们测试的自己的部署。机会存在提供反馈入安全模型，如果相信他们找到一个方式改进方法。工作参考可以由参与了的学生应要求提供。

特别强调：我们的 CAPSTONE PROJECT 第一学期招收学员将在 2011 年 3 月 7 日截止报名。

虽然官方注册将在 3 月 7 日关闭，如果你在北半球，我们会在不久的将来开始另一个学期的招生。

学生可以在学期之外的任何时间加入这个项目。虽然参加者会丧失一部分直接和其他参与一个入口的国际团队竞争的机会，但是他们仍然能上载由以前团队部署的图片并尝试利用他们。他们也能看到课业资料和论坛（这对做研究是很理想的）

如果我们的时间不适合你，但你仍然很感兴趣，请和我们直接联系，我们会感谢你的回复，并争取接受你的学生。

附件包括公司注册执照，最新 2011 年英文摘要。

对于更多信息请与大卫休斯联系+64 21 425 174, +64 9 4866884。 d@blueicon.com
或 中文邮件至翻译 Vivian 邮箱: admin.asia@blueicon.com

请点击以下英文网了解更多信息

<http://www.blueicon.com/>