Cybersecurity for the Masses

Hintergrund

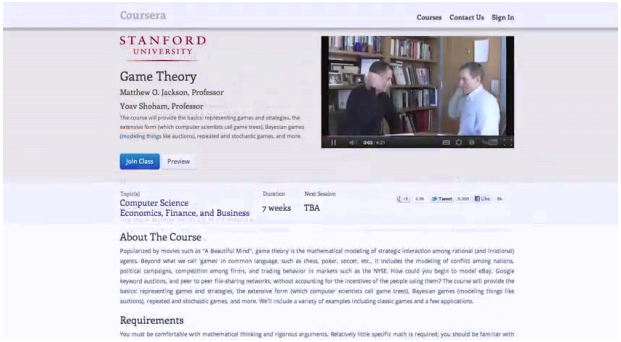

Abbildung 1: Coursera Web Interface

Massive Open Online Courses (MOOC) werden gerade zum vielbeachteten E-Learning Thema und sowohl von Forschung und Lehre als auch von Politik und Presse gleichermaßen wahrgenommen. „Massive“ in MOOC deutet dabei auf 4-, 5- oder sogar 6-stellige Teilnehmerzahlen hin, so gesehen beim ersten Kurs auf Udacity: die dort angebotene „Introduction to Artificial Intelligence“ zählte 160.000 Teilnehmer aus 190 Ländern [1]. Projekte wie Udacity, Coursera [2] oder das jüngst von MIT und Harvard University ins Leben gerufene edX [3] stellen auf ihren Plattformen nicht nur speziell aufgearbeitetes Kursmaterial (großteils in Form von kurzen Video-Schnipseln) sondern auch Tools für Kursplanung, studentisches Self-Assessment, Question- und Feedback-Management sowie kollaboratives Lernen zur Verfügung.

Die Erfahrungen am HPI mit der Lehre im Bereich der „Internet Security“ (bzw. Cybersecurity) zeigen, dass zwei Komponenten als besonders wichtig erachtet werden:

- Zum einen ist ein offensiver Lehransatz meist einem defensiven vorzuziehen. Studierende sollen lernen, wie ein Angreifer bestimmte Schwachstellen ausnutzen kann um ein System oder Netzwerk zu kompromittieren (anstatt lediglich Verteidigungsstrategien zu erlernen), um so auch bis dato noch unbekannten Gefahren besser begegnen zu können.

- Zum anderen ist das Sammeln praktischer Erfahrung höher einzuschätzen als das Studium von Standards oder Sekundärliteratur. Insbesondere bei der Implementierung sicherer Dienste oder bei der Konfiguration eine sicheren Systems ist Sorgfalt von besonderer Wichtigkeit, da bereits eine fehlerhafte Firewall-Regel ein ganzes Sicherheitskonzept aushebeln kann.

Diese Erkenntnisse sollen nun in die Gestaltung von Kursmodulen für einen Massive Open Online Course zu ausgewählten Themen der Netzwerksicherheit einfließen.

Beschreibung

Im Rahmen des Masterprojekts sollen folgende Leistungen erbracht werden:

1. Analyse der Inhalte existierender MOOC-Angebote sowie Vergleich von Toolunterstützung für Lehrkräfte und Studenten

2. Erstellung von Kursmodulen (aus Text, Multimedia, Quizzes für das Assessment) zu ausgewählten Sicherheitsthemen (z.B. Malware [4, vgl.], Eavesdropping und ARP Spoofing, E-Mail Security, etc.); dabei sollen (wo möglich und sinnvoll) auch vorhandene Videos aus dem tele-TASK Archiv genutzt oder zusätzliche Snippets konzipiert und aufgezeichnet werden

3. Implementierung eines Szenarios für praktische Übungen zu den jeweiligen Kursmodulen (basierend auf virtuellen Maschinen) sowie die Evaluation möglicher Modi zur Bereitstellung dieser praktischen Szenarien

Kontakt

Fachgebiet: Internet Technologien und -Systeme

- Fachgebietsleiter: Prof. Dr. Christoph Meinel
- Ansprechpartner: Christian Willems

Referenzen

[1] Udacity: http://udacity.com/us

[2] Coursera: http://www.coursera.org

[3] edX: http://www.edxonline.org

[4] Ch. Willems, Ch. Meinel: „Awareness Creation mit Tele-Lab IT-Security: Praktisches Sicherheitstraining im virtuellen Labor am Beispiel Trojanischer Pferde“. In *Proceedings zu Sicherheit 2008 (LNI)*, Seiten 513-532