Quo vadis, Sicherheitsaus-bildung?

Martin Mink, CASED (TU Darmstadt)

Workshop „Reaktive Sicherheit in der Lehre“ auf der DIMVA 2010

Inhalt

CASED

- Lehrangebote zum Thema reaktive Sicherheit
  - ohne Incident Management und Digitale Forensik
- Gliederung:
  - Themen der reaktiven Sicherheit
  - Standorte und Lehrveranstaltungen
  - Lehrformen
  - Lehrmaterialien
  - Workshops zur Lehrsituation an Hochschulen

Reaktive Sicherheit: Themen

CASED

- SIDAR:
  - Verwundbarkeitsanalyse
  - Intrusion Detection
  - Malware
  - Incident Management
  - Forensik
- "Verletzungen von Sicherheitsanforderungen erkennen und darauf reagieren" (Biskup, 2008)

Reaktive Sicherheit: Lehrveranstaltungen

CASED

- Veranstaltungen mit Inhalten im Bereich reaktiver Sicherheit
- Auswahl von Lehrveranstaltungen deutscher Hochschulen
  - exemplarische Vorstellung von
    - Standorten und
    - Themen
  - keine vollständige Liste
  - keine (aktuelle) Übersicht vorhanden

Lehrveranstaltungen: Überblick

CASED

- Wie lehrt man IT-Sicherheit am besten? – Überblick, Klassifikation und Basismodule
  - Diplomarbeit von Christian Mertens, 2007
  - Überblick und Klassifikation von Veranstaltungen zur IT-Sicherheit
    - national und international
- Liste von Jan Jürjens (TU München)
  - http://www4.in.tum.de/~juerjens/sicherheit-lehre.html
  - von 2005, nicht mehr aktuell
- Hochschullandkarte IT-Sicherheit
  - Liste von deutschen Sicherheitsveranstaltungen
  - benutzt Datenbank der informatik-relevanten Studiengänge
  - nicht mehr verfügbar

Vorlesungen

CASED

- Uni Bochum (Schwenk)
- TU Darmstadt (Katzenbeisser)
- TU Dortmund (Meier)
- FH Gelsenkirchen (Pohlmann)
- Uni Mannheim (Flegel/Freiling)
- Uni Passau (Posegga)
- Uni Potsdam (Meinel)
- ...

Vorlesungsinhalte

CASED

- TU Darmstadt: „IT-Sicherheit“
  - Cryptography, Security Engineering, Access Control, DRM & ERM, Authentication, Biometrics, Network Security, Software Security, Covert Channels, Privacy
- TU Dortmund: „Reaktive Sicherheit“
  - Verwundbarkeit(sanalyse), Sichere Programmierung, Malware(-Analyse), Rootkits, Honeypots, Intrusion Detection, Datenschutz
- Uni Mannheim: „Angewandte IT-Sicherheit“
  - Verwundbarkeiten (Programme, Netzwerk), Sicherheit von Webanwendungen, Honeypots, Malware(analyse), Intrusion Detection, Datenschutz

Praktika

CASED

- praktische Erfahrungen sammeln
  - häufig Verwendung von Angriffstechniken
- angeboten an (Auswahl):
  - Uni Bochum
  - TU Darmstadt
  - TU Dortmund
  - Uni Erlangen-Nürnberg
  - TU Magdeburg
  - Uni Mannheim
  - Uni Potsdam

Praktika

CASED

- Uni Bochum (Schwenk, Birk)
  - Sicherheit von Webanwendungen (u.a. XSS, CSRF, Session Hijacking, SQL Injection)
- TU Darmstadt (Mink)
  - Angriffe und Verteidigung im Netzwerk, CTF-relevante Themen
- Uni Erlangen-Nürnberg (Dressler)
  - 2-wöchige Veranstaltung im WS 08/09
  - Systemsicherheit (Schutz vor bösartigen Binaries, sichere Dateizugriffe), Netzwerksicherheit (Angriffserkennung u. Gegenmaßnahmen)
- Uni Mannheim (Freiling)
  - Netzwerksicherheit, Webanwendungssicherheit, Softwaresicherheit, Reverse Engineering, Incident Response

Lehrformen

CASED

- klassisch: Vorlesung (mit Übung)
- Praktika
- Seminare
- studentische Gruppen
- „motivierende Veranstaltungen“
- weitere?

Lehrformen: Praktikum

CASED

- praktische Auseinandersetzung mit IT-Sicherheit
- Kennenlernen von Sicherheitslücken, deren Ausnutzung und Gegenmaßnahmen
- verschiedenen Ausrichtungen
  - Netzwerksicherheit
  - auf bestimmtes Thema beschränkt
  - ...
- beide Seiten von IT-Sicherheit kennenlernen
  - die Angreifersicht
  - die Verteidigersicht

Lehrformen: Seminar

CASED

- Konferenzseminar
  - simulierte Konferenz mit CfP, Sessions, Conference Proceedings usw.
  - Studenten lernen kennen
    - den Ablauf einer Konferenz
    - das Erstellen von Gutachten
  - durchgeführt an TU Darmstadt, RWTH Aachen, Uni Mannheim
- Teleseminar
  - Simulation eines internationalen Projekts
  - Kooperation mit einer Hochschule im Ausland
    - Teilnehmer der einen Seite besuchen zum Projektstart die andere Seite
    - während Semester Zusammenarbeit über Telekooperation
    - zum Projektabschluss Besuch der anderen Seite
  - durchgeführt an Uni Mannheim

Lehrformen: Studentische Gruppe

CASED

- selbst-organisiert oder nicht selbst-organisiert
- verschiedene Ausrichtungen
  - Lese-/Diskussionskreis
  - „Hacker"-Gruppe
  - CTF-Team

Lehrformen: motivierende

CASED

- eigentlich keine eigenständige Lehrformen
- CTF (Capture-the-Flag) Wettbewerb
  - Teams spielen in Echtzeit gegeneinander
  - beide Seiten von IT-Sicherheit kennenlernen
  - Wettbewerbe der Vorjahre zum Nachspielen verfügbar
    - iCTF: http://ictf.cs.ucsb.edu/, CIPHER: http://www.cipher-ctf.org/
- Wargame
  - vorbereitete Challenges, meist Level-basiert
  - Browser- oder Kommandozeilen-basiert
  - stellt häufig typische Aufgaben eines Angreifers nach
- SPRING
  - SIDAR Graduierten-Workshop über Reaktive Sicherheit
  - Veranstaltung für den wissenschaftlichen Nachwuchs

Materialien

CASED

- die Unterlagen der meisten vorgestellten Vorlesungen sind online verfügbar
- Unterlagen für Praktika:
  - SEED (SEcurity EDucation)
    - vorbereitete Versuche, inkl. Unterlagen; Open Source
    - http://www.cis.syr.edu/~wedu/seed/
  - HTA Luzern
    - Unterlagen für IT-Sicherheitspraktikum, frei verfügbar
    - http://www.securitylabor.ch/
- Damn Vulnerable Linux (DVL)
  - Linux Live-DVD mit Sicherheitslücken und Tutorials
  - beinhaltet sicherheitsrelevante Programme

Weitere Materialien

CASED

- Webanwendungssicherheit
  - WebGoat
    - angeleitete Demo mit typischen Sicherheitslücken
    - von OWASP, http://www.owasp.org
  - HACME-Serie (Bank, Book, Travel, ...)
    - Webanwendungen mit konstruierten Sicherheitslücken
    - von Foundstone, http://www.foundstone.com
  - Jarlsberg
    - Online-Tutorial für Webentwickler
    - von Google Labs, http://jarlsberg.appspot.com/
- siehe auch Übersicht auf https://pi1.informatik.uni-mannheim.de/index.php?pagecontent=home%2F2.page%2FAbout_me.page&show=true

Lehre-Workshops

CASED

- August 2005
  - Köln, DLR
  - Inhalt: IT-Sicherheit in Hochschulausbildung, beruflicher Weiterbildung und Zertifizierung von Ausbildungsangeboten
  - organisiert von Felix Freiling
- April 2008
  - auf Sicherheit 2008 in Saarbrücken
  - Inhalt: Stand der IT-Sicherheitslehre an deutschen Universitäten
  - organisiert von Martin Mink

Workshop 2005

CASED

- Fragestellungen
  - Was sind die Ziele von universitären Ausbildungsprogramme?
  - Decken sie sich mit den Erwartungen der Industrie an Absolventen?
  - Macht ein einheitlicher Ausbildungskanon für IT-Sicherheit an Hochschulen Sinn?
- Teilnehmer
  - Vertreter von deutschen Universitäten, Fachhochschulen und Unternehmen
- Dokumentation: http://aib.informatik.rwth-aachen.de/2005/2005-20.ps.gz

Workshop 2005: Ergebnisse

CASED

- Aufnahme von IT-Sicherheitsthemen in relevante nicht-sicherheitsbezogene Informatikveranstaltungen
  - aber welche vorhandenen Themen ersetzen?
- kein Konsens bezüglich der Lehre von „ewigem Wissen“ und praktischem Anwendungswissen
  - Hochschulen: eher längerdauerndes Wissen
  - Industrie: starke Praxisanteile erwünscht
- keine Einigung über einen standardisierten Lehrplan in IT-Sicherheit
  - IT-Sicherheit noch zu unreif
  - abhängig von der Kompetenz der Dozenten
  - aber: Einbettung in Standard-Lehrplan

Workshop 2008

CASED

- Vorstellung der Angebote in Informationssicherheit an
  - Uni Bochum, TU Darmstadt
  - TU Dortmund, Uni Mannheim
  - Uni Potsdam, DFKI Saarbrücken
- Fragestellungen:
  - Wie ist der Stand der IT-Sicherheitsausbildung an Universitäten in Deutschland?
  - In welche Richtung steuert sie?
  - Was sind die Ziele der Ausbildungsprogramme?
  - Wird damit das gewünschte erreicht?
  - Wie unterscheiden sich die verschiedenen Ansätze?

GI-Empfehlungen

CASED

- IT-Sicherheit in der Ausbildung, Oktober 2006
- „Vorschläge zur Berücksichtigung der IT-Sicherheit in der schulischen und akademischen Ausbildung“
- Ausbildung an Hochschulen
  - Unterscheidung nach
    - informatik-nahe und nicht-informatik-nahe Studiengänge
    - Bachelor – Master – Nebenfach – Lehramt
  - generelle Aussage: unabhängig von der Fachrichtung
    - Einbeziehung von IT-Sicherheit so früh wie möglich
    - Bewusstseinsbildung um die möglichen Gefahren und Risiken zu erkennen

Diskussion

- …