Other Courses in Cyber Forensics and Security Technology

***ITMS539 / IT-S539: Steganography, Steganalysis & follow-on from ITMSx48 / IT-S448**

***ITMS549 / IT-S549: Follow-On Projects from ITMSx48 / IT-S448**

ITMS538 / IT-S538: Computer & Network Forensics

ITMSx43 / IT-S443: Vulnerability Analysis

ITMS555 / IT-S555: Mobile Device Forensics

ITMSx58 / IT-S458: Operating System Security

ITMS528 / IT-S528: Database Security

ITMS518 / IT-S518: Coding Security

ITMS549 / IT-S549

Follow-On Project from ITMSx48 / ITM-S448

Offered in spring semester

ITMS549 / IT-S549

A follow-on course will be offered this coming spring

- *Exams cover projects*
- *Continue and complete your team's work on projects started in this class (100% of grade)*
  - The 2-semester time frame allows you, as part of a team, to complete a really first class project
  - Such projects have been shown to have significantly influenced future employment
  - These projects have resulted in published papers

ITMS549 / IT-S549

We will meet during the class time to work on projects

Attendance at all the labs is required

It is at least one guaranteed time when everyone on a team is together

The top projects will be presented and demonstrated at ForenSecure15 in April 2015

In past years this has been a real opportunity for students to get exposure

In a number of cases, job offers have resulted

IT-S538 / ITMS538

Computer & Network Forensics

Usually taught in spring semester

IT-S538 / ITMS538

Computer & Network Forensics

A course related to x48 will be offered this coming spring

ITMS538 / IT-S538: Computer & Network Forensics

Computer & network **security**

Security deals with the future: How to prevent attacks

Computer & network **forensics**

Deals with what happened in the past or what is happening right now

Sort of cyber CSI Miami

IT-S538 / ITMS538
Computer & Network Forensics

Course content (briefly)

- *Forensics as a profession*
- *Investigations and evidence control*
- *Legal vs. civil issues*
- *Forensic tools*
- *Disk analysis*
  - Windows, Unix
  - File systems
- *Steganography and water marking*
- *Network & email back tracking if time permits*

IT-S538 / ITMS538
Computer & Network Forensics

Computer and Network Forensics

- *Detecting, obtaining and analyzing information for use as evidence in civil, criminal, or administrative cases.*
- *Ways of and technology for hiding information and code in network messages and on computer storage devices*
- *Ways of and technology for detecting the existence and recovery of hidden information*
- *How to do the above so that is legally accepted*

Forensics technology also applicable to disaster and data recovery

IT-S538 / ITMS538

Computer & Network Forensics

Students will become computer/network detectives

There are lots of places to hide information that the casual user would never see

After lecturing on how things are hidden and introducing forensic techniques and tools

We will give you USB disks and ask you to discover hidden information on them.

We will give you email messages and ask you to

Identify its real source

Discover hidden info in it

IT-S539 / ITMS539

Steganography & Steganalysis

Usually taught in spring semester

IT-S539 / ITMS539: Steganography & Steganalysis

Cryptography obscures the meaning of information but doesn't hide the fact that the information exists

- *A known file is encrypted so that only someone with a key can decrypt it*
- *A message is send from Alice to Bob. The villain Eve knows that the message is sent but can't discover what is in the message*

IT-S539 / ITMS539
Steganography & Steganalysis

Steganography hides the fact that the information exists at all

A file exists and may be encrypted but is not "visible". No one knows that the files exists

A message is send from Alice to Bob. The villain Eve doesn't know that the message is sent

Steganalysis tries to discover if anything is hidden in image or audio files

IT-S539 / ITMS539
Steganography & Steganalysis

Steganography Examples

- *Al-Qaeda attack plans hidden in a video*
- *Dead drop messages in eBay images*
- *Many non-cyber examples*
  - Invasion of Normandy, Invisible ink, Tatoos…

Seascape

Hide This Message

“This is a test to see if I can hide and then detect this message in this image of a seascape.”

Seascape With the Hidden Message

Which is Which? *

ITMSx43 / IT-S443
Vulnerability Analysis

Usually taught in fall semester

Basically a course in ethical hacking

ITMSx43 / IT-S443
Vulnerability Analysis

Contents include

- *Ethics of ethical hacking*
- *Cyber law*
- *Reconnaissance*
- *Scanning*
- *Gaining Access*
- *Password cracking*
- *Network attacks*
- *Exploits*
- *Anatomy of vulnerabilities*

ITMSx43 / IT-S443 Vulnerability Analysis

This course is designed to be taken either in person in the ForSec Lab (here) OR over the Internet

To take the course over the Internet, good Internet access to IIT is required from the remote location

All the labs can be done remotely

The ForSec Lab uses RADISH to do the remote labs

RADISH is the Remotely Accessible Dynamic Intranet for Students to Hack

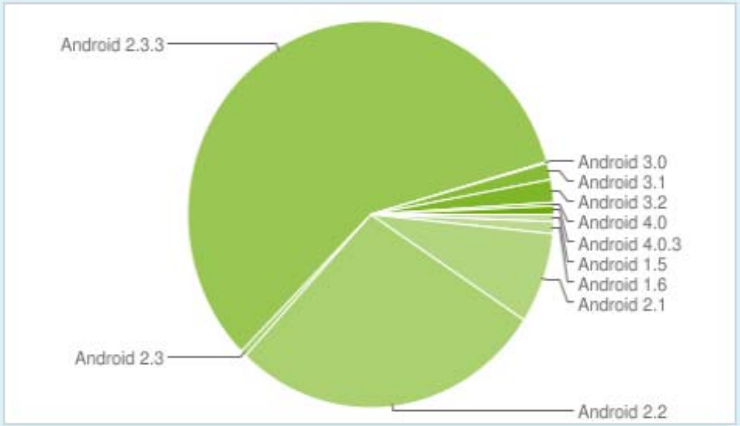
ITMS555 / IT-S555
Mobile Device Forensics

Taught in fall semester

ITMS555 / IT-S555
Mobile Device Forensics

- This course investigates the cyber forensic and security aspects of smartphones and tablets
- Students learn to capture the contents of mobile devices and analyze their contents
  - *Actual smart phones will be used*
- Students also investigate the security aspect of mobile devices and understand their vulnerabilities and what to do about them
- Hands-on Labs
- While this course uses RADISH, it must be taken in person in the ForSec Lab because of the use of real smart phones in the labs

Focus on Android



Platform	Codename	API Level	Distribution
Android 1.5	Cupcake	3	0.6%
Android 1.6	Donut	4	1.0%
Android 2.1	Eclair	7	7.6%
Android 2.2	Froyo	8	27.8%
Android 2.3 - Android 2.3.2	Gingerbread	9	0.5%
Android 2.3.3 - Android 2.3.7		10	58.1%
Android 3.0	Honeycomb	11	0.1%
Android 3.1		12	1.4%
Android 3.2		13	1.9%
Android 4.0 - Android 4.0.2	Ice Cream Sandwich	14	0.3%
Android 4.0.3		15	0.7%

ITMS555 / IT-S555
Mobile Device Forensics

Prerequisites / Co-requisite

IT-S440 or ITMSx40 or instructor's consent