Cryptography and Malware for Digital Forensics
DF 391

Instructor:	**David Burris, Ph.D., CCP, CSP**
Office:	**AB1 212-C**
Phone / web:	**294-1568, csc_dsb@shsu.edu** **Course information is available via Blackboard**
Location/Time:	**9:00-9:50 MWF, AB1-206**
Office Hours:	2-3 MWF, 8-9:30 TTh, others by appointment. I am actually on campus most of the time. I may not always be able to stop what I am doing, but you are free to drop by any time you need help.
Registration:	Undergraduate: DF 390.01. Classes will meet in AB1-206.

Departmental Course Objective:
Cryptography topics include integrity, authentication, confidentiality, non-repudiation, digital signatures, symmetric and asymmetric (public key) algorithms. Hash functions (SHA, MD5), cryptographic algorithms (DES, Triple DES, Blowfish, AES, etceteras), cost to break algorithms including key safety, Diffie-Hellmann, RSA, key stores, Secure Socket Layers, Virtual Private Networks (VPN), Certificate Authorities, and important cryptographic strategies such as digital envelopes are discussed. Steganography is introduced as an alternative or supplement to cryptography.

Writing and combating Malware will be discussed in depth. Topics include stack buffer overflow, file buffer overflow, function pointer overflow, environment variable attacks, system software attacks, writing and detection of virus/worm/time bombs, Intrusion Detection Systems (IDS), rook kits, and related topics. Operating system modifications to limit or prevent attacks will be discussed.

This course is designed to cover the theoretical and practical aspects of course concepts. Java, “C,” assembly, Perl and related languages will be utilized to demonstrate concepts. Both Microsoft and Linux will be used. Attendees need not have mastered all languages, operating systems, and concepts prior to the class. They must however have sufficient background and desire to master these topics in a restricted time frame.

Material will also include concepts and practical applications from:

1) Cryptography, digital signatures, public key (asymmetric) algorithms, symmetric algorithms, Diffie-Hellman, DES, Triple DES and the new federal replacement standard, RSA, Blowfish, Phrase Based Encryption (PBE), the

SKIP standard, hashing (digests), key generation, key distribution, and related topics in cryptography.

2) Socket programming.
3) Secure Socket Layer (SSL) technology.
4) Servlets (this will require some HTML, DHTML, XML).
5) Web based commerce including the use of cookies and session tracking.
6) Remote Method Invocation (RMI) and Common Object Request Broker Architecture (CORBA).
7) Database access including JDBC and ODBC.
8) Multi threading including race conditions, deadlock, and process coordination.
9) Steganography
10) Extensive development of operating system attack code and defense mechanisms.
11) Additional topics as time allows.
12) Malware topics include stack buffer overflow, file buffer overflow, function pointer overflow, environment variable attacks, system software attacks, writing and detection of virus/worm/time bombs, Intrusion Detection Systems (IDS), rook kits, and related topics.
13) Writing device drivers for MS-Windows and Linux.

Credit: 3 hours.

Background: Students should have completed at least three (preferably four) programming courses and have confidence in their ability to solve problems by writing original code. It is not necessary to have previously completed courses in database, data structures, networking, operating systems, Java, C++, or Ada. It is very helpful to have some knowledge assembly language and computer architecture. Sufficient background in these areas will be included as part of the lecture to allow for completion of lab assignments.

Instructor Specific Objectives:

Absence Policy: Students are encouraged to attend all classes, but <u>absences will not be used in computing the course grade</u>. *A zero will be recorded for all work missed due to absence unless arrangements to complete missed work are made <u>prior</u> to the class that is missed.*

Tentative test dates: September 14, October 12, November 9, and the final.

Grading: Four equally weighted exams will be administered during the semester including the final exam. Extensive use of essay questions is made on exams. Exams and labs will each constitute 50% of the course grade. The final exam will be comprehensive. In the event a student scores higher on the final exam than one of the regular tests, the lowest regular test grade, will be dropped and the grade on the final exam doubled, provided that **all** other assignments have been completed with a grade of 70 or higher. Under no circumstances will a course grade higher than a "C" be awarded to a student not making at least a "C" on every lab assignment. The scale of A = 90-100, B = 80-89, C = 70-79, D = 60-69, F= below 60 will be used.

Assignments are due at the start of class. Once class starts, anything turned in will be graded as "late" work. Assignments given to the departmental secretaries, placed in my mailbox, etc., will not be graded. All work must be given to me personally. Late work is subject to a penalty of zero to ten points per period it is late (at the discretion of the instructor). No credit will be allowed for assignments that specifically state they may not be submitted late. I do not encourage late labs but desire your best effort. Request to submit a lab late in order to complete a higher grading option should be made prior to the due date.

Copies of graded test and labs may be retained to meet department accreditation requirements.

Text: I recommend “Java, How to Program 7/E (or 6/E)” by Deitel and Deitel, Prentice Hall the tth edition. The 6th edition or another Java text will work but the 7th edition of Deitel is the superior Java reference. You are not however required to purchase a text. Please do not waste money unless you plan to read the text. Material will also be taken from “Applied Cryptography” by Bruce Schneier and “Java Cryptography” by Jonathan Knudsen. Additional materials utilized in the class will be referenced as they are utilized. Material covered by Greg Hoglund and James Butler in “Subverting The Windows Kernel ROOTKITS,” Addison-Wesley, ISBN 0-321-29431-9 will be used. “Hacking, The Art of Exploitation” by Jon Erickson, No Starch Press, ISBN 1-59327-007-0 will also be utilized.

You will learn a lot by reading the texts carefully from cover to cover several times during the semester. Again, if you are unwilling to spend time reading the text, please do not waste the money. You will only be unhappy with yourself, me, or both of us.

While I recommend a copy of the texts, no text is required for this course. All class my notes are available on Blackboard or the “T” drive. Students are urged to make a copy of the class notes in facilities operated by university Computer Services. Notes should be bound for use in class. The instructor retains all copyright privileges to instructional materials. Students registered for the class are authorized to make a copy of instructional material for their own use to complete the course. Instructional materials may not be distributed in part or whole to others without the expressed written approval of the instructor.

Class Notes and Software:

Please make a copy of the following notes to use in class. You are welcome to copy other notes you feel might be helpful. All software and programming examples used in class are located at T:\CSC\DSB\JAVA and its subdirectories. We will start with the cryptography notes on the first day of class.

BurrisJavaCrypto.doc

BurrisJavaRMI.doc
BurrisJavaCookies.docBurrisJavaServlets.doc
BurrisJavaServlets2.doc
BurrisJavaDBBasics.doc
BurrisJavaLink.doc
BurrisJavaMultiThread.docBurrisJavaFiles.doc
BohmJacopini.doc
BurrisJavaObjectOriented1.doc
BurrisJavaObjectOrient2.doc

There will be additional notes to copy but this is the great bulk. I will have to email updates to some of the notes as Java is changing. If you decide to work from a personnel laptop, you must have at least Java 1.2.5.0.0 Beta 2. The most current stable release of Java is recommended.

We will utilize the two online instructional tutorials ("Steganography Concepts," and "Cryptography Tutorial Using Java") at http://www.df.shsu.edu, select "Resources." Please watch the video "Network Box" security video at http://www.df.shsu.edu.

Additional notes used in class may be found at T:\CSC\DSB\DigitalForensics\Enrichments. Material utilized will include:
ACMGlobalizationReportSp06
BasicConceptsVocabulary
BioID
Booting
BufferOverFlow
BufferSmash
CraftingShellCode
CryptoKeyLength
CS431SuperComputer
DasdCdDvd
DigitalMoneyTransfer
EuclidsAlgorithm
InterruptProgramming
Kerberos
ManInTheMiddle
ProofOfAuthorship
ProtectingSearchableDatabase
Research
RoguePrograms
RootKits
SonyRootKit
Spooling
StackSmashing
Zfone

Most materials will be available from Blackboard. The exception is software. All software must be obtained directly from the “T” drive.

University Policy Statements:

Academic Integrity: All students are expected to engage in all academic pursuits in a manner that is above reproach. Students are expected to maintain honesty and integrity in the academic experiences both in and out of the classroom. Any student found guilty of dishonesty in any phase of academic work will be subject to disciplinary action. The University and its official representatives may initiate disciplinary proceedings against a student accused of any form of academic dishonesty including but not limited to, cheating on an examination or other academic work which is to be submitted, plagiarism, materials copied or purchased from a tutor, collusion and the abuse of resource materials. For a complete listing of the university policy, see:

http://www.shsu.edu/administrative/faculty/sectionb.html#dishonesty

Assignments made form one semester to the next are similar of necessity. Assignments are developed with the goal of providing a student with the opportunity to develop the desired level of intellectual achievement while not over burdening the student with excessive work. The use of work done by others including students (past or present) or tutors (paid or unpaid) will be construed as cheating. "Any" verifiable instance of cheating will normally result in a grade of "F" for the course for all individuals involved. Students should not have in their possession labs or tests belonging to other students from the current or previous semesters.

Students from previous semesters providing materials to students in following semesters will be subject to all disciplinary actions provided by the university.

Classroom Rules of Conduct: University policy states students will refrain from behavior in the classroom that intentionally or unintentionally disrupts the learning process and, thus, impedes the mission of the University. Cellular telephones and pagers and other disruptive devices must be turned off prior to the start of class. Students are prohibited from eating in class, using tobacco products, making offensive remarks, reading newspapers, sleeping, talking at inappropriate times, wearing inappropriate clothing, or engaging in any other form of distraction. Inappropriate behavior in the classroom shall result in a directive to leave class. Students who are especially disruptive will be subject to removal by University Police and / or reported to the Dean of Students for disciplinary action in accordance with university policy.

Visitors in the Classroom:

Only registered students may attend class. Exceptions can be made on a case-by-case basis by the professor. In all cases, visitors must not present a disruption to the class by their attendance. Students wishing to audit a class must apply to do so through the Registrar's Office.

Americans with Disabilities Act:

It is the policy of Sam Houston State University that individuals otherwise qualified shall not be excluded, solely by reason of their disability, from participation in any academic program of the university. Further, they shall not be denied the benefits of these programs nor shall they be subjected to discrimination. Students with disabilities that might affect their academic performance are expected to visit with the Office of Services for Students with Disabilities located in the Counseling Center. They should then make arrangements with their individual instructors so that appropriate strategies can be considered and helpful procedures can be developed to ensure that participation and achievement opportunities are not impaired.

SHSU adheres to all applicable federal, state, and local laws, regulations, and guidelines with respect to providing reasonable accommodations for students with disabilities. If you have a disability that may affect adversely your work in this class, then I encourage you to register with the SHSU Counseling Center and to talk with me about how I can best help you. All disclosures of disabilities will be kept strictly confidential. NOTE: No accommodation can be made until you register with the Counseling Center. For a complete listing of the university policy, see: http://www.shsu.edu/~vaf_www/aps/811006.html

Religious Holidays:

Section 51.911(b) of the Texas Education Code requires that an institution of higher education excuse a student from attending classes or other required activities, including examinations, for the observance of a religious holy day, including travel for that purpose. Section 51.911 (a) (2) defines a religious holy day as: “a holy day observed by a religion whose places of worship are exempt from property taxation under Section 11.20….” A student whose absence is excused under this subsection may not be penalized for that absence and shall be allowed to take an examination or complete an assignment from which the student is excused within a reasonable time after the absence.

University policy 861001 provides the procedures to be followed by the student and instructor. A student desiring to absent himself/herself from a scheduled class in order to observe (a) religious holy day(s) shall present to each instructor involved a written statement concerning the religious holy day(s). The instructor will complete a form notifying the student of a reasonable timeframe in which the missed assignments and/or examinations are to be completed. For a complete listing of the university policy, see: http://www.shsu.edu/~vaf_www/aps/documents/861001.pdf

Updated: August 2, 2007