

Computer and Network Security

SEC 250

Course Overview & Syllabus

N. Todd Pritsky
Fall 2007 Semester

[[[Link to Course Calendar](#)]]

Hello! and welcome to the *Computer and Network Security*. I hope that you find the course fun and interesting.

This course will provide an introduction to the many aspects of computer and data network security, and information assurance. We will examine the rationale and necessity for securing computer systems and data networks, as well as methodologies for implementing security, security policies, best current practices, testing security, and incident response. Course concepts are reinforced by demonstrations and research assignments. To this latter point I should emphasize that this is **not** a course in *hacking* and students will be expected to use the information that they learn in this class responsibly (as in, "Use your powers for good and not evil!"). You will be asked to sign a statement to that effect at the first class meeting.

The main objective of this course is to provide you with an understanding of the important security-related considerations when implementing computers, servers, and networks. To that end, we will cover a large set of topics, including:

- Defining security
- Viruses, worms, and Trojan horses
- Passwords, identification, and authentication
- Operating system security (Windows NT/2000 and Unix)
- TCP/IP security
- Firewalls, proxy servers, auditing, vulnerability assessment, and intrusion detection
- Offensive — and defensive — tools
- Cryptography and certificates
- Virtual private networks
- Ethics, hacking, and the law

This course will present varying levels of technical detail on the topics discussed but won't dwell too much on theory or mathematics. This is intended to be a general, practical course.

Course prerequisite: CIS 232 (Introduction to Data Communications)

It is expected that incoming students to this course have a basic understanding of network access, LAN, and WAN technologies; the OSI protocol reference model; TCP/IP; the role of operating systems; and at least passing familiarity with Windows and Unix/Linux. All of these topics will be discussed at some level of detail in this course and it is assumed that students have already had an introduction to these topics.

Student outcomes:

Upon completion of this course, students will be able to:

- Classify and summarize the major components of computer and network security, and information assurance.
- Analyze the impact of security policies and user security awareness to the "secure" operation of a network and the organization, in general.
- Evaluate the security vulnerabilities of common operating systems and data protocols.
- Design countermeasures and other ways to mitigate common security vulnerabilities.
- Plan a security policy for a given networking environment.
- Implement a plan by which you can keep current on security events and notices.
- Describe the ethical and legal considerations associated with "attacking" computer systems and networks.

Instructor contact information:

HOME OFFICE

215 Bog Road
Cambridge, VT 05444

Phone: +1 802-849-9836
Fax: +1 802-849-6186
Cell phone: +1 802-238-3436
E-mail: todd@pritsky.net
URL: <http://www.pritsky.net>

Texts and supplementary resources:

[Security+ Guide to Network Security Fundamentals, 2nd ed.](#) by Mark Ciampa (Course Technology, 2005) is the primary (i.e., **required**) text for this course. Although this course is not intended as a preparatory course for the Security+ certification, this book is an excellent introduction to the topic. Additional student resources and book updates are available at the [Course Technology](#) page.

[*SANS GIAC Certification: Security Essentials Toolkit \(GSEC\)*](#) by Eric Cole et al. (Que, 2002) is an **optional** text. This book provides a hands-on lab manual. I will provide everything you need for any hands-on exercises in the course but this book goes further than we will in class. (Full disclosure demands that I mention that I am a contributor to this book. I do not receive any royalties from book sales, however.)

There are so many security-related books that it is impossible to even start suggesting any supplementary references; it really depends upon what aspect of the field you want to study. There was a time when one could be a generalist in this field but those days are gone! Nevertheless, I'll mention four additional books anyway!

[*Security Engineering*](#) by Ross Anderson (John Wiley & Sons, 2001) is an excellent overview of security as an engineering discipline, which makes it unique in the security literature. It is based on solid engineering foundations, which means lots of math formulas, but also contains a wealth of anecdotes making this a very good text and a good professional reference. It is (mostly) easy and enjoyable to read, and based on real experiences and applications rather than pure theory of how it ought to be. This book actually discusses computer security in the way that other books only allude to: "Security is a process not a product." (This book is the primary text for the security course in the college's M.S. program in Managing Innovation and Information Technology.)

Another general text that describes in detail the entire gamut of computer and network security issues is [*Computer Security Handbook, 4th ed.*](#), edited by Sy Bosworth and Mich Kabay (John Wiley & Sons, 2002). This book discusses everything from policy to practice, each chapter written by a subject matter expert. Mich, by the way, is a professor at Norwich University and directs their B.S. and M.S. degree programs in Information Assurance. (Full disclosure again demands that I mention that I contributed three chapters to the handbook. I do not receive any royalties from book sales of this book, either.)

[*Hacking Exposed*](#) by Joel Scambray, Stuart McClure, and George Kurtz (McGraw-Hill, 2001) is a truly excellent and scary book. It doesn't describe security, per se, nor defense, per se — it describes hacking tools that can be used by the white-hats or the black-hats. It is really based on the premise that every tool is a two-edged sword, and that the defenders need to have the attacker tools in their arsenal so they know the bad guys' capabilities. In addition, the tools provide the defender with information, as well. Two of the authors are the CEO and CTO of [*Foundstone*](#), a leading security consultancy.

[*White-Hat Security Arsenal: Tackling the Threats*](#) by Aviel Rubin (Addison-Wesley, 2001) is another recommended text. This book discusses a number of important ways in which we can protect our systems better. Avi is a well-known security guru from AT&T and pretty much anything he writes is worth reading.

And a couple of other resources for you:

- My Web site, [GaryKessler.net](http://www.garykessler.net), has a number of papers and articles on topics related to this course and you should feel free to read and peruse them! In particular, my set of Security-Related URLs at <http://www.garykessler.net/library/securityurl.html> has some potentially useful pointers.
- Packet sniffers and protocol analyzers are very useful tools for monitoring a network and we will have many examples using one such tool called tcpdump (and its Windows equivalent, WinDump). Students are encouraged to obtain [tcpdump/WinDump and/or Ethereal/Analyzer](#). You might also find it useful to download this [TCP/IP Pocket Reference Guide](#).

Attendance, Homework, and Grading:

Success in this course depends upon continuity so it is important that you attend every class meeting, ask questions, and participate in discussions — in other words, *stay engaged!*. Homework and other assignments will be given in class and, usually, posted as *hot links* from the [course calendar](#). In general, assignments are due at the next class meeting after they are distributed/posted *unless otherwise noted*. Late assignments will be accepted only in extraordinary circumstances *and* only with the instructor's *prior* permission.

There is a standing writing assignment that will be assigned most weeks. This is a one- to two-page (single-spaced) assignment, consisting of a summary of the week's reading assignment plus a brief piece of independent research that I call your "Security Topic of the Week (STOW)," something from a Web site, news report, or other source that relates to the reading. I'd like to know what you found important or significant about the week's reading; what interested you, what resonated, what was new, etc., etc. — and *why*? And don't just give me a related article to read or a URL; instead, tell me why you chose a particular article and why you think it important. Think critically about these issues and involve yourself in your writing — e.g., a parallel government Internet sounds good at first blush but does it make sense; why or why not? The STOW needs to relate to the reading but can come from anywhere: a mailing list that you monitor, some security-related site, a friend, the *Burlington Free Press*, an experience from your workplace, etc. Use your imagination and get used to thinking about this.

Each of you will be asked to present at least one of your "standing assignments" to the class. And remember this quote from Herb Caen, former columnist for the *San Francisco Chronicle*: "Any clod can have the facts, but having an opinion is an art." Have an opinion!!!

There will be a final project in this course where you need to do some research on pretty much any information security-related topic of your choice. The project will have two parts; a paper and a presentation. More detail will be provided during the semester but you can start thinking about that now!

Grades will be weighted roughly as follows:

- Homework: 25%
- Mid-term: 20%
- Final exam: 20%
- Project: 20%
- Attendance and participation: 15%

I will use the College's standard numerical scale for calculating final grades:

A	A-	B+	B	B-	C+	C	C-	D+	D	D-	F
93+	90	87	83	80	77	73	70	67	63	60	59-

Applicability of Core Competencies

The Champlain College faculty and administration have committed that our curricula will address these seven critical core competencies:

- Technology
- Critical and Creative Thinking
- Global Studies
- Oral Communication
- Written Communication
- Quantitative Literacy
- Ethical Reasoning

This course addresses these competencies as outlined below.

Technology

Computer and network security is an important — and growing — area of concern by all segments of our society today, from business and government to education and recreation. By its nature, it is a technical topic. This course discusses a wide range of issues related to computer, network, and telecommunications technologies, including hardware, operating systems, software, network applications, communication protocols, local and wide area networks, and policies.

Students will be exposed to the myriad aspects of information security and the emerging field of "information assurance." Students will learn about defensive tools, policies, informational resources, and strategies as well as offensive tools and methods used by

attackers. In addition, security-related policies and procedures are also described, and discussion ranges from protecting personal systems to enterprise security.

Critical and Creative Thinking

Due to the broad and highly technical nature of computer and network security, the ability to think critically must become second nature to its practitioners. When implementing, designing, or altering any system, security of the individual component as well as the system as a whole must be considered. When a security vulnerability is found in one component of the network, one must anticipate other possible exposures or vulnerabilities. Policies and procedures must be defined that are relevant to an organization, functional, and useable — and enforceable. Abnormal computer and network events must be analyzed to determine if they are accidents, innocuous incidents, or purposeful attacks. The very nature of this business is critical thinking.

And there is more. An information security professional must build defensive systems while thinking like an attacker. All systems have a weak link from a security perspective; the infosec professional has to determine and shore up those weak points — and that means being able to think like the Bad Guy.

Finally, all of this has to be kept in perspective. Just as information technology supports an organization, information security must also be applied in a rational way that fits in with the business and the people. There is no such thing as perfect security; all we can do is mitigate the risks. The infosec professional, then, has to determine just how much security is enough, recognizing that there are several correct solutions.

Critical thinking is reinforced by homework assignments and classroom discussions. Rather than focus on bare "facts," the homework and class meetings focus more on how the subject matter integrates with other things that student know and will learn in the future. We also examine how students attitudes change as their level of knowledge — and responsibility — changes.

Global Studies

International awareness is not a major focus of this course and, in fact, there are few aspects of information assurance that are geography-specific. The technology is relatively universal and, therefore, the technical solutions are universal. Laws, however, vary country-by-country so that actions that are illegal in some countries are legal in others (such as unleashing a virus). Although not emphasized, the course does describe some of the geographical, political, and cultural differences as they apply to legal aspects, privacy expectations, and acceptable use policies. The relationship between information warfare and geopolitics is also briefly examined.

Oral and Written Communication

To be successful in the business world, professionals must be able to communicate in both written and oral form. While this course focuses on the technical aspects of information security, that knowledge is nearly useless if it cannot be communicated.

The information security professional must be able to communicate to many audiences on many levels:

- Communication with peers and managers at the technical level. This requires an understanding of computer, networking, and security concepts, as well as the proper vernacular.
- Communication with users, generally at a non-technical level. A successful technologist must be able to communicate the technical solution to a user's problem or business needs in understandable terms. This is often the most challenging portion of a professional's development.
- Communication with individuals at all levels within an organization with all levels of understanding. This includes upper management and supervisors to peers and subordinates, ranging from the technophobe to the technophile.

This course will provide students with ample opportunity to practice their communication skills through the weekly homework assignments and classroom discussions, but even more so through the research project that is part research paper, part oral presentation, and part presentation graphics. All assignments include grammar and composition as a component of grading.

Quantitative Literacy

Information security professionals have to be able to analyze patterns of activity to differentiate between normal and abnormal activity. Most of the information on computers and networks involves numbers and symbols, and the infosec professional needs to be able to find the connections between events and form a response strategy. This course will provide students with ample opportunity to practice quantitative literacy through the weekly homework assignments and classroom discussions.

Ethical Reasoning

The use of networks and information often requires ethical considerations -- e.g., how to employ individuals' private information that is stored on a server, appropriate use of corporate network resources, and how to respond to a potentially unethical request by a supervisor. Furthermore, information security managers are involved in the creation of infosec policies and procedures for an organization, generally requiring that users' activities be given a framework, including ethical behaviors. Ethical reasoning is specifically addressed in this course.

Students with Disabilities

If you believe that you have a disability requiring accommodations in this class, please contact the Coordinator of Support Services for Students with Disabilities as soon as possible. After you receive your accommodation form, please see me so I can work with you to implement them in a timely fashion.

Contact: Janine Allo – office: Hauke 007; phone: 802-651-5961; email: allo@champlain.edu

Academic Honesty Policy

The Champlain College Student Handbook (*The Rudder*) describes the College's Academic Honesty policy. It basically says that if I think you've cheated on an assignment — i.e., to either actually or attempt to knowingly give, receive, or use work that is not your own — I can give you a 0 on that assignment. I'll give you a slightly different bottom line — if you're going to cheat, I don't want you in the course. You may trick me, but you'll get killed once out in the workplace.

This is no way suggests that I am opposed to your collaboration with fellow students and others; in fact, I encourage as much collaboration as possible. The point of this policy is that work that you submit as your own *has* to be your own! If you work with another person or other resource that helps you learn an answer to something, that's fine — what I see, however, should be in your own words and clearly demonstrate **your** understanding. If you're unsure, tell me that you worked with others.

Finally, I will tolerate no excuse for cheating. That's another reason that you should keep your communication channels with me open. If there's a problem in your life that is rippling over into school, don't let it cause you to do something that will have unintended consequences.

Don't cheat; there's no margin in it!! If you have a problem, talk to me instead.

TCP/IP
TEL 315

Course Overview & Syllabus

N. Todd Pritsky
Fall 2007 Semester

[[[Link to Course Calendar](#)]]

Hello! and welcome to *TCP/IP*. We hope that you find the course fun, informative, and interesting.

This course will provide detailed coverage of the Transmission Control Protocol/Internet Protocol (TCP/IP) suite, the *lingua franca* of the Internet. Network professionals today need to be thoroughly familiar with the Internet and TCP/IP, so here we are! Luckily, the subject is an interesting one and the Internet is a network that we all use, so although this is going to be very different than what many of you have seen before, you already have some basic familiarity. Although we will cover some theoretical stuff, this is a practical applications-oriented course, relying heavily on hands-on exercises.

Course topics will include:

- The OSI Reference Model and data communications protocol suites
- The ARPANET, Internet, and TCP/IP
- Packet sniffing and protocol basics
 - LAN protocols (e.g., Ethernet)
 - Access protocols (e.g., HDLC, PPP, T1, frame relay)
 - TCP/IP Suite: IP, ICMP, TCP, UDP, application protocols
- IP: Operation, addressing, subnets, subnet masks, ICMP, ARP, IP version 6
- TCP: Operation, ports, error handling
- UDP: Operation, ports
- Overview of common TCP/IP application protocols (e.g., FTP, Telnet, SSH, DNS, SMTP, etc.)
- Security issues related to all aspects of TCP/IP, including the IP Security (IPsec) protocols, voice over IP (VoIP) and VPNs
- Protocol analysis with tcpdump/WinDump

Course prerequisite: CIS 232 (Introduction to Data Communications)

It is expected that incoming students to this course have a basic understanding of network access, LAN, and WAN technologies, and the OSI protocol reference model.

Course outcomes:

Upon completion of this course, students will be able to:

- Compare and contrast the TCP/IP protocol suite with other protocol suites, and cite advantages and disadvantages of using TCP/IP.
- Articulate and construct an IP-based subnet addressing plan, with particular understanding of private vs. public addressing and subnet masks.
- Explain the protocol operation of the major components of the TCP/IP suite, recognize the data unit formats, and understand basic troubleshooting (to include IP, ICMP, ARP, TCP, UDP, FTP, Telnet, Ping, HTTP, SMTP, POP, and DNS).

- Describe the relationship between IP, underlying network access protocols and technologies, and higher layer applications and services.
- Review the common security vulnerabilities associated with the TCP/IP protocol suite and ways to mitigate those vulnerabilities.
- Review the basic operation and function of IPsec and VPNs.
- Demonstrate the ability to troubleshoot IP-based networks using a protocol analyzer.

This course also addresses the college's core competencies in the following way:

- *Oral/written communication:* The applications and services that can be designed and implemented using the TCP/IP protocol suite often requires communication with an organization's non-technical management, customers, vendors, and users. Networking professionals have to be able to effectively communicate in both written and verbal form. These skills will extend those learned in other classes by use of papers, student presentations, and the demonstration of proper computer forensics techniques.
- *International awareness:* International issues are covered, as relevant. TCP/IP is the protocol used on the global Internet and there are few specific international issues.
- *Technology:* This course covers basic concepts related to networking protocols, and the application of TCP/IP protocols and services.
- *Critical Thinking:* Computer networks using TCP/IP often require performance analysis and troubleshooting, tasks that are more art than science. Extending TCP/IP to non-traditional applications and fitting those applications to the communication needs of an organization requires out-of-the-box thinking. Discussion and analysis of a variety of real and hypothetical scenarios will show students how to view TCP/IP as more than just getting two computers to talk with one another.

Instructor contact information:

HOME OFFICE

215 Bog Road
Cambridge, VT 05444

Phone: +1 802-849-9836
 Fax: +1 802-849-6186
 Cell phone: +1 802-238-3436
 E-mail: todd@pritsky.net
 URL: <http://www.pritsky.net>

Texts and supplementary resources:

- [Guide to TCP/IP](#), 2nd. ed. by Laura Chappell and Ed Tittel (Course Technology, 2004) is the **required text** for this course. It is a good, accurate, readable text and also pretty current. The text will be supplemented with outside reading from the Web.
- [TCP/IP Illustrated, Volume 1: The Protocols](#) by W. Richard Stevens (Addison-Wesley, 1994) is considered by many to be the "bible of TCP/IP" even though it is over ten years old. It is one of the best books available if you want a detailed treatment of the basic protocols comprising TCP/IP. Many changes have occurred to TCP/IP since the book was written, however, so there are many new protocols that the book doesn't cover — e.g., Secure Shell (SSH), Secure Sockets Layer (SSL), IP version 6 (IPv6).
- [Troubleshooting TCP/IP](#) by Mark Miller (John Wiley & Sons, 1999) is a really good take on TCP/IP from the perspective of troubleshooting and protocol analysis.
- [TCP/IP Architecture, Protocols and Implementation with IPv6 and IP Security](#) by Sidnie Feit (McGraw-Hill, 2000) is another good TCP/IP text, this more from the user and usage perspective. It is currently available for purchase as a downloadable PDF file (7.9MB, 900+ pages).
- The [GaryKessler.net](http://www.garykessler.net) Web site has a number of papers and articles on topics related to this course and you should feel free to read and peruse them! In particular, take a look at the TCP/IP tutorial available at <http://www.garykessler.net/library/tcpip.html>.
- Packet sniffers and protocol analyzers are very useful tools if trying to understand protocols in action on real networks. There is a lecture in the course on the use of one such tool called tcpdump (and its Windows equivalent, WinDump). Students are encouraged to obtain [tcpdump/WinDump and/or Ethereal/Analyzer](#). You might also find it useful to download this [TCP/IP Pocket Reference Guide](#).
- Some other resources worth knowing about include:
 - The Internet Society Web site (www.isoc.org)
 - The Internet Engineering Task Force Web site (www.ietf.org)
 - The RFC Editor's Web site (www.rfc-editor.org)
 - Cisco Systems' *The Internet Protocol Journal* (www.cisco.com/ipj)

Download the free Adobe Acrobat reader to be able to view course lecture notes and other course resources.

Grading:

There are a number of components that will be used to determine grades in this course. The bottom-line is that you demonstrate your understanding of the material. Since this is not a lab course (although there will be some lab-type homework), that demonstration will be primarily in written or verbal form.

There are, then, a number of mechanisms that will be used to evaluate students to determine a grade. First, this course depends a lot on student-instructor interactivity. Therefore, class attendance and active participation are very important and will count heavily towards the final grade. Second, there will be a fair amount of reading and written work, as well as mid-term and final exams. In general, homework is due the week following its assignment (unless a different due date is posted when the homework is distributed); homework will be accepted late only in extraordinary circumstances *and* only with the instructor's permission.

Finally, there is a research project associated with the course. The project will have a written portion *and* a presentation portion. The written portion must be completed using some word processing software and the presentation portion must be completed using some presentation graphics software. There will be more information on the project at mid-semester but this is a heads-up that you will need these skills. (Note that use of non-Office word processing and/or presentation graphics software is quite acceptable.)

Grades will be weighted roughly as follows:

- Midterm Exam: 20%
- Final exam: 20%
- Homework: 20%
- Project: 20%
- Attendance and participation: 20%

The College's standard numerical scale for calculating final grades will be used:

A	A-	B+	B	B-	C+	C	C-	D+	D	D-	F
93+	90	87	83	80	77	73	70	67	63	60	59-

Students with Disabilities

If you believe that you have a disability requiring accommodations in this class, please contact the Coordinator of Support Services for Students with Disabilities as soon as possible. After you receive your accommodation form, please see me so I can work with you to implement them in a timely fashion.

Contact: Janine Allo – office: Hauke 007; phone: 802-651-5961; email: allo@champlain.edu

Academic Honesty Policy

The Rudder, the Champlain College Student Handbook, describes the Academic Honesty policy. It basically says that if the instructor thinks that you have cheated on an assignment — i.e., to either actually or attempt to knowingly give, receive, or use work that is not your own — you can be given a 0 on that assignment. The point of all of this is that if you hand in work that is supposed to be your own, it should be. That also means that if you use external information sources, be sure to cite them and give appropriate credit.

This in no way suggests that the college or program is opposed to your collaboration with fellow students and others; in fact, many classes create teams for some assignments specifically to encourage as much collaboration as possible. The point of this policy is that work that you submit as your own *has* to be your own! If you work with another person or other resource that helps you learn an answer to something, that's fine — what you turn in, however, should be in your own words and clearly demonstrate **your** understanding. If you're unsure, indicate that you worked with others.

The bottom line is — there is **no** excuse for cheating. That's another reason that you should keep your communication channels with your instructor(s) and/or advisor open. If there's a problem in your life that is rippling over into school, don't let it cause you to do something that will have unintended consequences; talk to someone instead.