

General Information

Instructor

Matt Bishop

Office: 2209 Watershed Science

Office Hours: Tue 1:40–2:30pm; Wed 3:10–4:00pm; Thu 12:10–1:00pm; or by appointment; or by chance

Email: bishop@ucdavis.edu

Phone: (530) 752-8060

Lectures and Discussion Section

Lecture: TuTh 10:30am–11:50am in 1070 Bainer

Discussion section: *To be arranged*

Course Outline

Theoretical foundations of methods used to protect data in computer and communication systems. Access control matrix and undecidability of security; policies; Bell-LaPadula, Biba, Chinese Wall models; non-interference and non-deducibility; information flow and the confinement problem.

Course Goals

- Learn about the access control matrix model and its variants, and how it is used to analyze the security of classes of systems;
- Learn about the mathematics underlying security policies;
- Understand the composition of policies;
- Learn about the confinement problem and information flow; and
- Explore other topics of interest.

Prerequisite

ECS 235A, Computer and Information Security; ECS 150, Operating Systems, and ECS 120, Theory of Computation, are strongly recommended

Text

M. Bishop, *Computer Security: Art and Science*, Addison-Wesley, Boston, MA (2003). ISBN 0-201-44099-7.

Class Web Site

To access the class web site, go to SmartSite (<http://smartsite.ucdavis.edu>) and log in using your campus login and password. Then go to ECS 235B in your schedule. I will post Announcements, assignments, handouts, and grades there, and you *must* submit assignments there. The alternate web site, <http://nob.cs.ucdavis.edu/classes/ecs235b-2013-02>, has all the handouts, assignments, and announcements.

Grading

Homework is 45% of your grade, the project is 45% of your grade, and your in-class presentation is 10% of your grade. There is no final examination.

Academic Integrity

The UC Davis Code of Academic Conduct, available at <http://sja.ucdavis.edu/cac.html>, applies to this class. For this course, all submitted work must be your own. You may discuss your assignments with classmates or the instructor to get ideas or a critique of your ideas, but the ideas and words you submit must be your own. Unless *explicitly* stated otherwise, collaboration is considered cheating and will be dealt with accordingly.

All About Homework

All homework is due at 5:00pm on the due date, unless noted otherwise. I will grade and return these to you as quickly as possible. I'll try for three class periods, but can't guarantee it.

When you are asked to analyze something, or explain something, please be complete, and show your work (including any commands you give, and their output, to show how you did the problem). Otherwise, even if you get the right answer, you will get **ZERO** (that's *0*, *zip*, *nada*, *rien*, *nothing*) points. Think your answer through and do a rough draft. Students (and professionals, actually) often overlook this, but it is vital. Write clearly and cogently. If the question asks for an opinion, state your opinion clearly, justify it, and don't ramble. Answers that start, "My opinion is yes . . ." and conclude with ". . . on the other hand it could equally well be no" won't get much credit.

When you turn in homework, you must turn in an ASCII, a PostScript, or a PDF version of your answers (you can use any text processor you like to generate these). Please **do not** submit Microsoft Word or Open Office files. I sometimes grade homework on UNIX-based or Linux systems, and it can be difficult to read those files on such a system. If you submit PostScript, please be sure the file will print on our department printers (use *ghostscript(1)* or *gs(1)* to check this; if it displays the file properly, the file should print correctly).

When you turn in your file, please use an appropriate extension: ".pdf" for a PDF file, ".ps" for a PostScript file, and ".txt" for an ASCII file.

Please turn in your work electronically through Smartsite. If you need to turn in something on paper (for example, a diagram that you can't draw using your text processing program), please hand it to me before the assignment is due, and put a note in what you submit electronically that you have done this. That way, I will remember to look for something written, rather than mark you off for that problem.

Grades

Your grades will be posted to SmartSite when the homework assignment is graded. I will also post comments on why you gained, or lost, points.

Extra Credit

Extra credit is tallied separately from regular scores. It counts in your favor if you end up on a borderline between two grades at the end of the course. But not doing extra credit will never be counted against you, because grades are assigned on the basis of regular scores. You should do extra credit if you find it interesting and think that it might teach you something. Remember, though, it is not wise to skimp on the regular assignment in order to do extra credit!

Late Homework

As this is a graduate class, I expect that you can manage your own time. So if your homework is occasionally late, I will assume there is a very good reason. (If the reason is a a serious one, like a medical reason or a family emergency, I'd appreciate your letting me know.) So I will not deduct points without warning you. If this becomes a problem for an individual or the class, I reserve the right to begin imposing penalties, so please do not abuse this!

Also, I will not post my answers until *all* homework has been turned in, so it is to your classmates' benefit, as well as your own, not to be too late.

Grade Reviews

If you feel that there is an error in grading, please come see me and I'll look over it (and possibly talk with you about it). However, don't dally; any such request must be made within one week of when the grades were made available. After that, I won't change your grade.

Presentation

Part of graduate education is learning to present work. There are numerous papers that we will read; these are at the forefront of current work, or extend previous work in interesting ways. Each class member will present one of these papers.

The weeks for the presentations are listed in the Syllabus. Normally, they will be on the Thursday of that week. Each presentation should be 20 minutes long, and should explain the key results and how they were obtained. Pretend the paper is something you did; what would you want to communicate to the audience at a conference? Using that as a guideline is usually the best way to give a good talk. After the presentations, we will discuss the papers and the significance of the work, as well as future directions for the work.

After your presentation, please turn in a copy of your presentation materials (such as slides). If you do not use slides but use notes instead to talk from, please submit those.

Please pick a paper, then go to the class web page at <http://smartsite.ucdavis.edu>. Then go to the wiki there and edit it, adding your name and the paper. I put one for me in there, so you can see how to do it if you've never used a wiki. Please remember to leave a blank line above and below what you type.

Here are the papers to be presented, and the weeks in which they are to be presented.

- [B+07] M. Backes, M. Dümuth, and D. Unruh, “Information Flow in the Peer-Reviewing Process (Extended Abstract),” *Proceedings of the 2007 IEEE Symposium on Security and Privacy* pp. 187–191 (May 2007). doi: 10.1109/SP.2007.24
To be presented during week 8
- [B+09] B. Bowen, M. Ben Salem, S. Hershkop, A. Keromytis, and S. Stolfo, “Designing Host and Network Sensors to Mitigate the Insider Threat,” *IEEE Security & Privacy* **7**(6) pp. 22–29 (Nov. 2009). doi: 10.1109/MSP.2009.109
To be presented during week 10
- [E+03] A. El Kalam, R. El Baida, P. Balbiani, S. Benferhat, F. Cuppens, Y. Deswarte, A. Miège, C. Saurel, and G. Trouessin, “Organization Based Access Control,” *Proceedings of the IEEE 4th International Workshop on Policies for Distributed Systems and Networks* pp. 120–131 (June 2003). doi: 10.1109/POLICY.2003.1206966
To be presented during week 5
- [HS97] T. Himdi and R. Sandhu, “Lattice-Based Models for Controlled Sharing of Confidential Information in the Saudi Hajj System,” *Proceedings of the 13th Annual Computer Security Applications Conference* pp. 164–174 (Dec. 1997). doi: 10.1109/CSAC.1997.646186
To be presented during week 8
- [J+11] B. Javadi, D. Kondo, J.-M. Vincent, and D. Anderson, “Discovering Statistical Models of Availability in Large Distributed Systems: An Empirical Study of SETI@home,” *IEEE Transactions on Parallel and Distributed Systems* **22**(11) pp. 1896–1903 (Nov. 2011). doi: 10.1109/TPDS.2011.50
To be presented during week 5
- [KR02] C. Ko and T. Redmond, “Noninterference and Intrusion Detection,” *Proceedings of the 2002 IEEE Symposium on Security and Privacy* pp. 177–187 (May 2002). doi: 10.1109/SECPRI.2002.1004370
To be presented during week 7
- [Li89] T. Lin, “Chinese Wall Security Policy—An Aggressive Model,” *Proceedings of the 5th Annual Computer Security Applications Conference* pp. 282–289 (Dec. 1989). doi: 10.1109/CSAC.1989.81064
To be presented during week 6
- [LO10] G. Loukas and G. Öke, “Protection Against Denial of Service Attacks: A Survey,” *The Computer Journal* **53**(7) pp. 1020–1037 (2010). doi: 10.1093/comjnl/bxp078
To be presented during week 5

- [LT05] N. Li and M. Tripunitara, “On Safety in Discretionary Access Control,” *Proceedings of the 2005 IEEE Symposium on Security and Privacy* pp. 96–109 (May 2005). doi: 10.1109/SP.2005.14
To be presented during week 4
- [Ma02] H. Mantel, “On the Composition of Secure Systems,” *Proceedings of the 2002 IEEE Symposium on Security and Privacy* pp. 88–101 (May 2002). doi: 10.1109/SECPRI.2002.1004364
To be presented during week 7
- [S+06] G. Shah, A. Molna, and M. Blaze, “Keyboards and Covert Channels,” *Proceedings of the 15th USENIX Security Symposium* pp. 59–78 (Aug. 2006). url: <https://www.usenix.org/legacy/event/sec06/tech/shah/shah.pdf>
To be presented during week 9
- [S+09] B. Simidchieva, S. Engle, M. Clifford, A. Jones, S. Peisert, M. Bishop, L. Clarke, and L. Osterweil, “Modeling and Analyzing Faults to Improve Election Process Robustness.” *Proceedings of the 2010 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections* (Aug. 2010). url: https://www.usenix.org/legacy/events/evtwote10/tech/full_papers/Simidchieva.pdf
To be presented during week 10
- [SA06] J. Alves-Foss and J. Son, “Covert Timing Channel Analysis of Rate Monotonic Real-Time Scheduling Algorithm in MLS Systems,” *Proceedings of the 2006 IEEE Information Assurance Workshop* pp. 361–368 (June 2006). doi: 10.1109/IAW.2006.1652117
To be presented during week 9
- [SJ07] H. Shahriari and R. Jalili, “Vulnerability Take Grant (VTG): An Efficient Approach to Analyze Network Vulnerabilities,” *Computers & Security* **26**(5) pp. 349–360 (Aug. 2007). doi: 10.1016/j.cose.2007.03.002
To be presented during week 3
- [TL13] M. Tripunitara and N. Li, “The Foundational Work of Harrison-Ruzzo-Ullman Revisited,” *IEEE Transactions on Dependable and Secure Computing* **10**(1) pp. 28–39 (Jan. 2011). doi: 10.1109/TDSC.2012.77
To be presented during week 3
- [VC94] V. Varadharajan and C. Calvelli, “Extending the Schematic Protection Model. I. Conditional Tickets and Authentication,” *Proceedings of the 1994 IEEE Symposium on Research in Security and Privacy* pp. 213–229 (May 1994). doi: 10.1109/RISP.1994.296579
To be presented during week 4
- [WB04] T. Walcott and M. Bishop, “Traducement: A Model for Record Security,” *ACM Transactions on Information and System Security* **7**(4) pp. 576–590 (Nov. 2004). doi: 10.1145/1042031.1042035
To be presented during week 6
- [Z+05] X. Zhang, Y. Li, and D. Nalla, “An Attribute-Based Access Matrix Model,” *Proceedings of the 2005 ACM Symposium on Applied Computing* pp. 359–363 (Mar. 2005). doi: 10.1145/1066677.1066760
To be presented during week 4

Term Project

Why a Project?

This course covers a very large discipline, and—perhaps more so than many other areas of computer science—the discipline of computer security runs through many other areas. Because the class has a very limited amount of time, we will only touch the surface of many topics. The project is to give you an opportunity to explore one of these topics, or some other area or application of computer security that interests you, in some depth.

The Ground Rules

The project can be a detailed research paper or survey, or a programming project that focuses on validating or working with some formalism or implements a model so others can explore it thoroughly. It can be a formalism, a model, or something else theoretical that we do not cover in class. In any case, check with me before beginning to be sure it is a reasonable project and no-one else has chosen it. Please select something that interests you!

You may work individually, or in groups of up to 3 people (if you want to have more than 3, please come see me). Of course, the larger the group, the more I will expect from it.

Some Suggestions for Project and Report Topics

Below are some suggestions for projects. If you pick one of these, you will need to refine it or limit the scope of your project. You may also think of a project on your own.

- Develop a model of information flow through a network using the Take-Grant Protection Model, and demonstrate its utility by analyzing a situation of your choosing.
- Implement SPM (or ESPM) and use the implementation to demonstrate various configurations approaching their maximal state.
- Present a survey of confidentiality models other than the Bell-LaPadula Model.
- Examine the composition problem, and focus on advances in the nature of composition and restrictiveness.
- Create a model for a specific problem, such as electronic voting, and use it to reason about properties of the desired systems.
- Insert information flow analysis into a compiler or assembler and use it to detect flows that violate a policy specifying security/integrity levels for a program or system.
- Develop a formalism or model for analyzing some aspect of the “insider problem”.
- Build a run-time system that detects flows that violate a policy specifying security or integrity levels for a program or system.
- Develop a covert channel analyzing tool and use it to analyze a subsystem or some other entity.

What Is Due and When

Please submit the following on the dates indicated:

1. *Project selection*: due on Tuesday, January 21; 10% of project score. Submit a write-up with your team members consisting of a one-line title of your project, a one-paragraph description, and the names of all team members. If you’re doing a programming project, state the problem you want to solve and the requirements for a solution.
2. *Progress report*: due on Tuesday, February 4; 20% of project score. Submit a one-page progress report, and a bibliography of references that you have used or plan to use. ***Your group will present the idea for the project, what you have done so far, and what you think the results of your project will be, during the discussion section this week.***
3. *Completed project*: due on Friday, March 21 ***no later than 8:00pm*** (this is the date and time of the final exam); 70% of your project score. Turn in your final project.

In all cases, submit the project to SmartSite as described in **All About Homework**. If a team has multiple members, only one need submit the material, and the others simply submit a note saying who submitted the final project.