NEW YORK UNIVERSITY NYUParis

Introduction to Computer Security

CSCI-UA.9480, Spring 2019

Instructor:	Nadim Kobeissi	**Office Hours:**	4:30pm – 5:00pm.
Email:	nk76@nyu.edu	**Office Number:**	Room 4.06.

1 Course Information

- *Course number and section:* CSCI-UA9480.
- *Course title:* Introduction to Computer Security.
- *Course description:* Technology increasingly permeates every aspect of our lives, including communication, finance and health. The security of the computer systems that enable these services has become a critical issue. This course will cover basic principles of computer security and security engineering. It will introduce fundamental computer security concepts, principles, and techniques. It will also cover notions of real-world cryptography, the mathematical building blocks that underlie any digital security construction. This course will focus on security from an attacker's perspective (threat modeling) and the defender's perspective (building and deploying secure systems). Specific topics will include operating system security, network security, web security, applied cryptography, security economics and security psychology. Course projects will focus both on writing secure code and exploiting insecure code.
- *Prerequistes:* CSCI-UA.0201 (Computer Systems Organization) and experience with computer systems level programming languages (e.g. C, and C++ programming). Recommended prerequisite courses include CSCI-UA.0202 (Operating Systems), and CSCI-UA.0480-009 (Computer Networks). Experience with web development will also be helpful.
- *Class meeting days and times:* Mondays and Wednesdays, 3:00pm – 4:30pm. Room 4.06.
- *Term dates:* February 4, 2019 until May 16, 2019.
- *Course website:* `https://computerscience.paris/security`.

2 Course Overview and Goals

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

- Understand the principles of the cryptographic constructions underlying modern computer security.
- Acquire knowledge in important security topics such as operating system security, network security, web security, security economics and security psychology.
- Write secure code and exploit insecure code from an attacker's perspective (threat modeling) and the defender's perspective (building and deploying secure systems).

3 Course Requirements

- *Class participation:* You are expected to attend all classes. Missing a class can entail missing on important material. Discourse is encouraged during classes, but not mandatory.
- *Assigned readings:* Every lecture will be accompanied by outside readings that expand on what is discussed in class or present the same material in a different way. Neither the readings nor the lectures are a replacement for each other; deeply understanding the material will likely require attendance as well as reading. It is possible to read before or after class, depending on your learning style.
- *Problem sets:* Three problem sets will be assigned as homework. Problem sets must be submitted online *before* the start of class on the day that they are marked as due.
- *Practical assignments:* Two practical assignments will be organized during the course.
- *Exams:* A midterm exam and a final exam will be organized as part of this course.

4 Grading of Assignments

The grade for this course will be determined according to the following formula:
Class participation (10%), practical assignments (20%), problem sets (20%), midterm exam (25%) and final exam (25%).

Letter Grade	**Points**	**Description**
A	94	Outstanding
A-	90	Excellent
B+	87	Very Good
B	84	Good
B-	80	Satisfactory
C+	77	Above Average
C	74	Average
C-	70	Below Average
D+	67	Unsatisfactory
D	65	Low Pass
F	64	Fail

5 Course Schedule

- **0.0**: Introduction and Threat Modeling
  - *Security Engineering*, Chapter 1
  - *Serious Cryptography*, Chapter 1
  - *An Introduction to Approachable Threat Modeling*

Part 1: Cryptography ..... ≈ 8 sessions

- **1.1**: One-Way Functions and Hash Functions
  - *Security Engineering*, Chapter 3
  - *Serious Cryptography*, Chapter 6
- **1.2**: Symmetric Key Encryption
  - *Serious Cryptography*, Chapters 3, 4, 5
- **1.3**: Public Key Cryptography and Randomness
  - *Serious Cryptography*, Chapters 9, 11, 12, 2[a]
- **1.4**: Transport Layer Security
  - *Serious Cryptography*, Chapter 13
  - *Let's Encrypt: How It Works*
  - *The Illustrated TLS Connection*[b]
- **1.5**: Usable Security and Secure Messaging
  - *Security Engineering*, Chapter 2
  - *15 Reasons not to Start Using PGP*
  - *State of Knowledge: Secure Messaging*
  - *Automated Verification for Secure Messaging Protocols and their Implementations*
  - *More is Less: On the End-to-End Security of Group Chats in Signal, WhatsApp, and Threema*
- **1.6**: Attacking Cryptographic Systems
  - *Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS and Other Systems*
  - *Remote Timing Attacks are Practical*
  - *Transcript Collision Attacks: Breaking Authentication in TLS, IKE and SSH*
  - *On the Practical (In-)Security of 64-bit Block Ciphers*
  - *Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice*
  - *DROWN: Breaking TLS using SSLv2*
- **1.7**: Cryptocurrencies, Blockchains, Smart Contracts
  - **Problem Set 1 Due**
  - *Bitcoin and Cryptocurrency Technologies* Chapters 1, 2
  - *The Idea of Smart Contracts*
- **1.8**: E-Voting and Other Modern Uses of Cryptography
  - *E-Voting Crypto Protocols*
  - *The Remote Voting Minefield: from North Carolina to Switzerland*

[a] RSA will be briefly discussed in class.

[b] The Illustrated TLS Connection is an online interactive learning tool available at https://tls.ulfheim.net/.

Part 2: Network Security ..... ≈ 6 sessions

- **2.1**: Networking Basics, IP, TCP and DNS
  - *Security Engineering*, Chapter 21
  - *An Introduction to Computer Networks*, Chapters 1, 7, 22
  - *How DNSSec Works*
- **2.2**: Denial of Service
  - *Security Engineering*, Chapter 21.2
  - *Understanding the Mirai Botnet*
  - *How Netflix DDoSd Itself To Help Protect the Entire Internet*
- **2.3**: Designing Secure Network Systems
  - *WireGuard: Next Generation Kernel Network Tunnel*
  - *A Cryptographic Analysis of the WireGuard Protocol*
  - *An Analysis of the ProtonMail Cryptographic Architecture*
- **2.4**: New Secure Protocols
  - *Noise Explorer*[a]
- **Practical Assignment 1 Review**
- **Midterm Exam**

[a] Noise Explorer is an online interactive learning tool available at https://noiseexplorer.com.

Part 3: Software Security ..... ≈ 5 sessions

- **3.1**: Understanding and Preventing Vulnerabilities
  - *Software Security Knowledge Area*
- **3.2**: Control Flow Hijacking
  - **Problem Set 2 Due**
  - *Security Engineering*, Chapter 4.4
  - *Low-level Software Security: Attacks and Defenses*
- **3.3**: Systems Security and Isolation
  - *Security Engineering*, Chapter 4.3
  - *Security in Ordinary Operating Systems*
  - *Apple T2 Security Chip Overview*
- **3.4**: Mobile Security
  - *iOS Security Guide*
  - *Android Security: 2017 Year In Review*
  - *Google Blog: Titan M Makes Pixel 3 our Most Secure Phone Yet*
- **3.5**: Meltdown and Spectre: Diving Into Hardware Vulnerabilities
  - *Meltdown: Reading Kernel Memory from User Space*
  - *Spectre Attacks: Exploiting Speculative Execution*

Part 4: Web Security ..... ≈ 6 sessions

- **4.1**: Browser Security Model
  - **Problem Set 3 Due**
  - *OWASP Top 10 - 2017: The Ten Most Critical Web Application Security Risks*
  - *Browser Security Handbook, part 1*
  - *Browser Security Handbook, part 2*
- **4.2**: Web Application Security
  - *Introduction to Cross-Site Scripting*
  - *Password Storage Cheat Sheet*
  - *Why Don't we Follow Password Security Best Practices?*
  - *The unescape() Room*[a]
- **4.3**: Hybrid Runtimes: Electron and Node.js
  - *Electron Security Checklist: A Guide for Developers and Auditors*
- **Practical Assignment 2 Review**
- **4.4**: Web Privacy
  - *Tools from the EFF's Tech Team*
  - *Europe's New Privacy Law Will Change the Web, and More*
- **4.5**: Spam and Abuse
  - *Click Trajectories: End-to-End Analysis of the Spam Value Chain*

[a] The unescape() Room is an online interactive learning tool available at https://unescape-room.jobertabma.nl/.

Part 5: Security and Society ..... ≈ 3 sessions

- **5.1**: Economics, Ethics and Law
  - *Security Engineering*, Chapter 7.5
  - *Vulnerability Reporting FAQ*
- **5.2**: Censorship and Mass Surveillance
  - *Security Engineering*, Chapter 24.3
  - *Project Bullrun: Dual EC DRBG*
- **Final Exam**

6 Required Textbooks and Materials

Aside from the textbooks and materials, students will also require their own personal computer for various parts of this course. Windows, Linux and Mac computers are all suitable.

6.1 Textbooks

- Jean-Philippe Aumasson, *Serious Cryptography*, No Starch Press, 2017. ISBN-13: 978-1-59327-826-7.
- Ross Anderson, *Security Engineering*, Wiley, 2008. Available for free on the course website.

6.2 Online Readings

All of the online readings listed below are available for free on the course website.

- Kevin Riggle, *An Introduction to Approachable Threat Modeling*, Increment Magazine, 2018.
- Let's Encrypt, *Let's Encrypt: How It Works*, Linux Foundation, 2018.
- Paul C. Kocher, *Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS and Other Systems*, Cryptography Research, Inc., 1996.
- David Brumley and Dan Boneh, *Remote Timing Attacks are Practical*, USENIX Security Symposium, 2003.

- Karthikeyan Bhargavan and Gaëtan Leurent, *Transcript Collision Attacks: Breaking Authentication in TLS, IKE and SSH*, Network and Distributed Systems Symposium, 2016.
- Karthikeyan Bhargavan and Gaëtan Leurent, *On the Practical (In-)Security of 64-bit Block Ciphers*, ACM Computer and Communications Security, 2016.
- David Adrian, Karthikeyan Bhargavan, Zakir Durumeric, Pierrick Gaudry, Matthew Green, J. Alex Halderman, Nadia Heninger, Drew Springall, Emmanuel Thomé, Luke Valenta, Benjamin VanderSloot, Eric Wustrow, Santiago Zanella-Béguelin and Paul Zimmermann, *Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice*, ACM Computer and Communications Security, 2015.
- Nimrod Aviram, Sebastian Schinzel, Juraj Somorovsky, Nadia Heninger, Maik Dankel, Jens Steube, Luke Valenta, David Adrian, J. Alex Halderman, Viktor Dukhovni, Emilia Käsper, Shaanan Cohney, Susanne Engels, Christof Paar and Yuval Shavitt, *DROWN: Breaking TLS using SSLv2*, USENIX Security Symposium, 2016.
- Nik Unger, Sergei Dechand, Joseph Bonneau, Sascha Fahl, Henning Perl, Ian Goldberg and Matthew Smith, *State of Knowledge: Secure Messaging*, IEEE Symposium on Security and Privacy, 2015.
- SecuShare, *15 Reasons not to Start Using PGP*.
- Nadim Kobeissi, Karthikeyan Bhargavan and Bruno Blanchet, *Automated Verification for Secure Messaging Protocols and their Implementations: A Symbolic and Computational Approach*, IEEE European Symposium on Security and Privacy, 2017.
- Paul Rösler, Christina Mainka and Jörg Schwenk, *More is Less: On the End-to-End Security of Group Chats in Signal, WhatsApp, and Threema*, IEEE European Symposium on Security and Privacy, 2018.
- Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller and Steven Goldfeder, *Bitcoin and Cryptocurrency Technologies*, Princeton University Press, 2016.
- Nick Szabo, *The Idea of Smart Contracts*, University of Amsterdam, 1997.
- Jean-Philippe Aumasson, *E-Voting Crypto Protocols*, Kudelski Security, 2018.
- Bryan Ford, *The Remote Voting Minefield: from North Carolina to Switzerland*, EPFL, 2019.
- Peter L. Dordal, *An Introduction to Computer Networks*, Loyola University Chicago, 2018.
- Jason A. Donenfeld, *WireGuard: Next Generation Kernel Network Tunnel*, Network and Distributed Systems Security Symposium, 2017.
- Benjamin Dowling and Kenny Paterson, *A Cryptographic Analysis of the WireGuard Protocol*, Loyola University Chicago, 2018.
- Nadim Kobeissi, *An Analysis of the ProtonMail Cryptographic Architecture*, IACR ePrint Archive, 2019.
- Cloudflare, *How DNSSEC Works*.
- Manos Antonakakis, Tim April, Michael Bailey, Matthew Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J. Alex Halderman, Luca Invernizzi, Michalis Kallitsis, Deepak Kumar, Chaz Lever, Zane Ma, Joshua Mason, Damian Menscher, Chad Seaman, Nick Sullivan, Kurt Thomas and Yi Zhou, *Understanding the Mirai Botnet*, USENIX Security Symposium, 2017.
- Lily Hay Newman, *How Netflix DDoSd Itself to Help Protect the Entire Internet*, WIRED Magazine, 2017.

- Frank Piessens, *Software Security Knowledge Area*, University of Bristol Cyber Security Group, 2018.
- Stanford University Applied Cryptography Group, *Security in Ordinary Operating Systems*, Stanford University.
- Apple Inc., *iOS Security Guide*, Apple Inc., 2018.
- Apple Inc., *Apple T2 Security Chip Overview*, Apple Inc., 2018.
- Android Team, *Android Security: 2017 Year in Review*, Google Inc., 2018.
- Xiaowen Xin, *Google Blog: Titan M Makes Pixel 3 our Most Secure Phone Yet*, Google Inc., 2018.
- Moritz Lipp, Michael Schwarz, Daniel Gruss, Thomas Prescher, Werner Haas, Anders Fogh, Jann Horn, Stefan Mangard, Paul Kocher, Daniel Genkin, Yuval Yarom and Mike Hamburg, *Meltdown: Reading Kernel Memory from User Space*, USENIX Security Symposium, 2018.
- Paul Kocher, Jann Horn, Anders Fogh, Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lipp, Stefan Mangard, Thomas Prescher, Michael Schwarz and Yuval Yarom, *Spectre Attacks: Exploiting Speculative Execution*, IEEE Symposium on Security and Privacy, 2019.
- "dw", *The Mysterious Case of the Linux Page Table Isolation Patches*, `http://sweetness.hmmz.org`, 2018.
- Úlfar Erlingsson, *Low-level Software Security: Attacks and Defenses*, Microsoft Research and Reykjavík University, 2007.
- OWASP, *Password Storage Cheat Sheet*, OWASP, 2018.
- Emily Cain, *Why Don't we Follow Password Security Best Practices?*, Increment Magazine, 2018.
- Luca Carettoni, *Electron Security Checklist: A Guide for Developers and Auditors*, Doyensec, 2017.
- EFF Tech Team, *Tools from the EFF's Tech Team*, Electronic Frontier Foundation, 2018.
- Nitasha Tiku, *Europe's New Privacy Law Will Change the Web, and More*, WIRED Magazine, 2018.
- OWASP, *OWASP Top 10 - 2017: The Ten Most Critical Web Application Security Risks*, OWASP, 2017.
- Google Application Security, *Introduction to Cross-Site Scripting*, Google Inc.
- Michal Zalewski, *Browser Security Handbook, part 1*, Google Inc., 2009.
- Michal Zalewski, *Browser Security Handbook, part 2*, Google Inc., 2009.
- Kirill Levchenko, Andreas Pitsillidis, Neha Chachra, Brandon Enright, Márk Félegyházi, Chris Grier, Tristan Halvorson, Chris Kanich, Christian Kreibich, He Liu, Damon McCoy, Nicholas Weaver, Vern Paxson, Geoffrey M. Voelker, Stefan Savage, *Click Trajectories: End-to-End Analysis of the Spam Value Chain*, IEEE Symposium on Security and Privacy, 2011.
- Kurt Thomas, Danny Yuxing Huang, David Wang, Elie Bursztein, Chris Grier, Thomas J. Holt, Christopher Kruegel, Damon McCoy, Stefan Savage, Giovanni Vigna, *Framing Dependencies Introduced by Underground Commoditization*, Workshop on the Economics of Information Security, 2015.
- Coders Rights Project, *Vulnerability Reporting FAQ*, Electronic Frontier Foundation.
- Daniel J. Bernstein, Tanja Lange, Ruben Niederhagen, *Project Bullrun: Dual EC DRBG*, Projectbullrun.org, 2015.

7 Resources

- *Access your course materials:* NYU Classes (https://nyu.edu/its/classes).
- *Databases, journal articles and more:* Bobst Library (https://library.nyu.edu).
- *Assistance with strengthening your writing:* NYU Writing Center (https://nyu.mywconline.com).
- *Obtain 24/7 technology assistance:* IT Help Desk (https://nyu.edu/it/servicedesk).

8 Attendance and Tardiness

- Study abroad at Global Academic Centers is an academically intensive and immersive experience in which students from a wide range of backgrounds exchange ideas in discussion-based seminars. Learning in such an environment depends on the active participation of all students. And since classes typically meet once or twice a week, even a single absence can cause a student to miss a significant portion of a course. To ensure the integrity of this academic experience, class attendance at the centers is mandatory, and unexcused absences willăbe penalized with a two percent deduction from the students final course grade for every week's worth of classes missed. Students are responsible for making up any work missed due to absence. Repeated absences in a course may result in harsher penalties including failure.
- Unexcused absences will be penalized with a 2% deduction from the students final course grade.
- Absences are excused only for illness, religious observance, and emergencies.
- *Illness:* For a single absence, students may be required to provide a doctors note, at the discretion of the Associate Director of Academics. In the case of two consecutive absences, students must provide a doctors note. Exams, quizzes, and presentations will not be made up without a doctors note.
- *Religious observance:* Students observing a religious holiday during regularly scheduled class time are entitled to miss class without any penalty to their grade. This is for the holiday only and does not include the days of travel that may come before and/or after the holiday. Students must notify their instructor and the Academic Office in writing via email one week in advance before being absent for this purpose. If exams, quizzes, and presentations are scheduled on a holiday a student will observe, the Associate Director, in coordination with the instructor, will reschedule them.
- *Contact your professor:* if you are unable to attend class, you are required to email your professors directly to notify them.
- *Late assignment:* Late submission or work will be accepted only with justifiable reasons of health or family emergency.

9 Academic Honesty

At NYU, a commitment to excellence, fairness, honesty, and respect within and outside the classroom is essential to maintaining the integrity of our community. Plagiarism is defined as presenting others' work without adequate acknowledgement of its source, as though it were ones own.ă Plagiarism is a form of fraud.ă We all stand on the shoulders of others, and we must give credit to the creators of the works that we incorporate into products that we call our own. Some examples of plagiarism:

- A sequence of words incorporated without quotation marks or an unacknowledged passage paraphrased from another's work.

- The use of ideas, sound recordings, computer data or images created by others as though it were ones own.
- Submitting evaluations of group members work for an assigned group project which misrepresent the work that was performed by another group member.
- Altering or forging academic documents, including but not limited to admissions materials, academic records, grade reports, add/drop forms, course registration forms, etc.

Furthermore, my courses have a **zero tolerance policy for cheating**. Any instance of cheating will result in an immediate, non-negotiable grade of 0 on the pertinent assignment and a report to the university faculty:

- Your code has to be your own. No copying code (or rewriting it line by line based on someone else's code) will be tolerated.
- Any sharing of any answers on any assignment is considered cheating.
- Coaching another student by helping them writing their answers line by line is also cheating.
- Copying answers or code from the Internet or hiring someone to write your answers for you is cheating.

Explaining how to use systems or tools and helping others with high-level design issues is not cheating.

For further information, students are encouraged to check NYU's Academic Integrity Policy.

10 Disability Disclosure Statement

Academic accommodations are available for students with disabilities. Please contact the Moses Center for Students with Disabilities (212-998-4980 or mosescsd@nyu.edu) for further information. Students who are requesting academic accommodations are advised to reach out to the Moses Center as early as possible in the semester for assistance.

11 About Your Instructor

My name is Nadim and it is my distinct privilege to be your instructor for this course. I am a researcher with a focus on applied cryptography, protocol analysis and formal verification. In designing and deploying real-world cryptographic systems in the public and private sector, I have always attempted to combine both theoretical and applied approaches to cryptography. I received my Ph.D. after doing research at the Institut National de Recherche en Informatique et Automatique (INRIA) in Paris (accredited by École Normale Superieure) and have published peer-reviewed research focusing on applied cryptography and automated protocol verification. I have also maintained several open source projects and have been involved in digital privacy issues.