CPSC 526 / 626 NETWORK SYSTEM SECURITY

Administrivia

- Prof: Joel Reardon (joel.reardon@)
- TAs: Hasnain Naeem (hasnain.naeem@)
- Lectures: TR 1230–1345 in MS 319
- Website: https://pages.cpsc.ucalgary.ca/~joel.reardon/526/
- Tutorials: MW 1000–1050 in MS 252

What's Required?

- Prereq: CPSC 441 (computer networks)
  - you are expected to understand TCP/UDP/IP/ARP/DNS/DHCP
  - you should be able to write socket programs, client, server, etc.

Late Assignments

- assignment dates are firm
- extenuating circumstances are considered
  - likeliest outcome is moving weight to remaining assignments
  - will only be granted if
    - reasonable
    - requested ahead of deadline or as soon after as it practical
    - supported by appropriate documentation
- late assignments can still be graded
  - i.e., for your own understanding

Academic Misconduct

Academic Misconduct

I take academic misconduct extremely seriously.

Common Offenses

- sharing solutions, code, etc.
- posting your code publicly (e.g., github)
- using other people's code, solutions
- searching directly for solutions
- buying solutions or having someone/something else do the work

Misconduct

Misconduct

whenever you copy/paste text you didn't write yourself you need to cite it

Misconduct

whenever you copy/paste text you didn't write yourself you need to cite it

putting cites at end of submission isn't enough: you need to point out where you use them

Misconduct

whenever you copy/paste text you didn't write yourself you need to cite it

putting cites at end of submission isn't enough: you need to point out where you use them

if you have any text you did not write the text itself needs an indicator that this is not your own original work

Misconduct

whenever you copy/paste text you didn't
write yourself you need to cite it

putting cites at end of submission isn't enough:
you need to point out where you use them

if you have any text you did not write
the text itself needs an indicator that
this is not your own original work

copying someone else's text and replacing words
with synonyms ("tortured phrases") is misconduct

using citations

using citations
whenever you are copying/pasting
text or copying/pasting code to
answer a question, you should think:
is this a reasonable intellectual
effort to answer the question?

using citations
whenever you are copying/pasting
text or copying/pasting code to
answer a question, you should think:
is this a reasonable intellectual
effort to answer the question?
even if you cite it properly,
copying someone else's answer to the question
is almost certainly not what I have in mind
when giving an assignment

working with others

working with others
working with other people on the ideas is okay
as long as it doesn't feel like cheating

working with others

working with other people on the ideas is okay

as long as it doesn't feel like cheating

e.g., discuss question and solutions but don't take notes

working with others

working with other people on the ideas is okay

as long as it doesn't feel like cheating

e.g., discuss question and solutions but don't take notes

then do something else for 30 minutes

working with others

working with other people on the ideas is okay

as long as it doesn't feel like cheating

e.g., discuss question and solutions but don't take notes

then do something else for 30 minutes

whatever's still in your mind is yours to keep

Granted “feels like its cheating” is subjective
consider describing exactly what you did to me

Granted “feels like its cheating” is subjective
consider describing exactly what you did to me
does that description sound reasonable?

Granted “feels like its cheating” is subjective
consider describing exactly what you did to me
does that description sound reasonable?
You can always ask if you are unsure.

use of third party code

use of third party code
using other people's code is generally fine
as long as it is not a direct solution

use of third party code

using other people's code is generally fine

as long as it is not a direct solution

ask yourself: does this make this question trivial / pointless / devoid of any learning?

use of third party code

using other people's code is generally fine

as long as it is not a direct solution

ask yourself: does this make this question trivial / pointless / devoid of any learning?

ask yourself: does this code make me not have to do any work myself relevant to course?

use of third party code

using other people's code is generally fine

as long as it is not a direct solution

ask yourself: does this make this question trivial / pointless / devoid of any learning?

ask yourself: does this code make me not have to do any work myself relevant to course?

assignments are not about how good

you can search for an answer

use of third party code

using other people's code is generally fine

as long as it is not a direct solution

ask yourself: does this make this question trivial / pointless / devoid of any learning?

ask yourself: does this code make me not have to do any work myself relevant to course?

assignments are not about how good

you can search for an answer

exams will test knowledge from assignments

searching for answer

searching for answer
do not search directly for the question

searching for answer

do not search directly for the question

do not solicit answers to the question

searching for answer
do not search directly for the question
do not solicit answers to the question
if you accidentally see a specific answer
to a specific question your thinking is
polluted even if you try not to use it

searching for answer
do not search directly for the question
do not solicit answers to the question
if you accidentally see a specific answer
to a specific question your thinking is
polluted even if you try not to use it
your answer may converge to other
people's answers that are also polluted

Question: Suppose You Knew Ahead Of Time How Much Randomness You Needed, Like One Megabyte. Describe Two Approaches That Use...

Suppose you knew ahead of time how much randomness you needed, like one megabyte. Describe two approaches that use a small (e.g., 256-bit) seed to generate a one-megabyte stream of randomness that:

1. achieves rollback resistance *but not* prediction resistance
2. achieves prediction resistance *but not* rollback resistance

That is, two different approaches that each achieve exactly one of the two desired properties. You may assume standard cryptographic assumptions hold.

Be sure to express your design clearly (i.e., use pseudocode if necessary). You may use basic cryptographic functions but just define what they mean. You can use the previous question's pseudocode as a good idea as to expectations.

Hint: think about the one-way property of hash functions!

Suppose you knew ahead of time how much randomness you needed, like one megabyte.
Describe two approaches that use a small (e.g., 256-bit) seed to generate a one-megabyte
stream of randomness that:
1. achieves rollback resistance but not prediction resistance
2. achieves prediction resistance but not rollback resistance
That is, two different approaches that each achieve exactly one of the two desired prop-
erties. You may assume standard cryptographic assumptions hold. Be sure to express your design clearly (i.e., use pseudocode if necessary). You may use
basic cryptographic functions but just define what they mean. You can use the previous
question's pseudocode as a good idea as to expectations.
Hint: think about the one-way property of hash functions!

This is a solid applied cryptography question. You're asked to design **two pseudorandom generators (PRGs)** from a **small 256-bit seed**, which output a **1 MB stream** of randomness, under two distinct security goals:

🔐 Definitions Recap:

- **Prediction Resistance**:
  If you don't know the internal state of the generator, you cannot predict future outputs, even if

AI Statement

- you can use AI tools, including generative AI, as learning aids
- you are ultimately accountable for the work you submit
  - you must be able to understand and explain your own work
- use of AI and other resources (e.g., stackoverflow) must be documented
  - cited at the place it is used
  - conspicuously identified as what was copied

Ethics and Law

- we will discuss **attacks** on computer security
- NONE OF THIS IS IN **ANY WAY** AN INVITATION TO USE WHAT YOU LEARN OTHER THAN WITH INFORMED CONSENT OF ALL INVOLVED PARTIES
  - the existence of a vulnerability is not an excuse to exploit it
- this isn't just ethics but the law
  - some attacks are easy to do...
  - ...and people are in jail for doing them
- if you're ever unsure if you should be doing this then talk to us
- some of the tools we cover **cannot be used in practice**
  - as in, they work, but then you'll get letters from your ISP

Course Materials

- recommended textbook: Van Oorschot "Internet Security: Tools and Jewels"
  - lectures will focus on big picture principles of network attack and defense
  - readings from textbook will be posted on course webpage
- other supplementary readings will be made available
  - these can cover specific things discussed in class in detail
- lectures will cover some material that is **not** in the textbook
  - **and you will be tested on it!**

Tutorials

- tutorials occur twice a week unless canceled
- tutorials begin next week
- tutorials will involve discussion questions and exercises
- tutorials also for help with assignments
- tutorial topic will be posted on course webpage

Office Hours

- TR 1430–1530 in ICT 642
- reach out if you cannot make that time

Grading CPSC 526

- assignments 40%
  - five assignments each worth 8%
  - tentative dates sept 25, oct 13, oct 31, nov 19, dec 2
- two one-hour in-class midterms 20%
  - oct 7th
  - nov 6th
  - you must take at least one midterm
  - if excused, one missed midterm will move the weight to the exam
  - excused if
    - reasonable
    - requested ahead of exam or as soon after as it practical
    - supported by appropriate documentation
- final 40%
  - a C- or higher on the exam is necessary for a C- or higher in the course

Letter Grades

- ≥ 95 $A+$, ≥ 90 A, ≥ 85 $A-$
- ≥ 80 $B+$, ≥ 75 B, ≥ 70 $B-$
- ≥ 65 $C+$, ≥ 60 C, ≥ 55 $C-$
- ≥ 50 $D+$, ≥ 45 D, < 45 F
- FAQ:
  - Q: Can you inflate my grade?
  - A: No.

Grading CPSC 626

- assignments 40%
  - same as CPSC 526
- two in class midterms 20%
- final 40%
- students may do a course project in lieu of the midterms and exam
  - proposal 25%
    - sept 30
  - paper 50%
    - dec 5
  - presentation 25%
    - dec 4

Topics Covered

- three major themes
  - channel security
  - protocol security
  - web security

Channel Security

- understand threats
  - replay attack
  - man in the middle middle
  - mafia fraud
- understand the components of TLS
  - randomness
  - cryptographic primitives
  - certificates and PKI

Protocol Security

- look at core insecure protocols
- denial of service attacks
- TCP injection attack
- DNS poisoning
- ARP attacks
- DHCP attacks

Web Security

- web applications and threats
- cookies and authentication
- cross site scripting (XSS)
- cross site request forgery (XSRF)
- code injection attacks
- UI redress attacks