COURSE RECAP AND EXAM INFO
Lecture 36

COMPSCI 726
Network Defence and Countermeasures

Muhammad **Rizwan** Asghar

October 21, 2021

THE UNIVERSITY OF AUCKLAND
NEW ZEALAND

COURSE STRUCTURE: FIRST PART

- Lectures (Lecture 1 to Lecture 11 by Rizwan)
  - Introduction
  - Cryptography and PKI
  - Network models
  - SSL/TLS
- Lectures (Lecture 12 to Lecture 23 by Nalin)
  - DNS and DNSSEC
  - DoS and DDoS
  - Firewall and NAT
  - IDS and honeypots
  - IPv4, IPv6, and IPSec
  - Wireless security
  - BGP

COURSE STRUCTURE: SECOND PART

- Individual seminars by students
  - 18 seminars
  - 12 unique research articles
  - 2 research articles excluded
    - Research Article 3: [Bai-SP21]
    - Research Article 10: [Ma-USENIX21]

- Course recap and exam info
  - Focus of this lecture!

EXPECTED FROM STUDENTS

- Attend lectures and seminars
- Active class participation
- Present a research article
- Review a presentation
- Proposal (1 paragraph) and final report (7-10 pages)
  - Come up with novel research ideas
  - Group size 2
    - 10 reports by 20 students

MY TEACHING PHILOSOPHY

- Giving feedback to you
- Sharing my knowledge and experience
- Creating an environment to offer you enough learning opportunities
- Inspiring you to learn
- Encouraging inclusiveness

SUPPORT DURING THIS COURSE

- Discussion for selecting an article for seminar
- Feedback on research proposal
- Feedback on interim report

FUTURE POSSIBLITIES

- Extending report as a research article
- Thesis/dissertation
- Internship
- Job

LEARNING OUTCOMES

- Give basic advice on securing communication networks (Themes 1-6*)
- Criticise and appreciate technical literature on network security (Themes 1-5*)
- Demonstrate technical skills to increase security of communication networks (Themes 1-6*)
- Prepare and deliver an oral presentation on an advanced topic in network security (Themes 1, 2, 4, and 5*)
- Develop novel problem solving and research-informed ideas (Themes 1-6*)

*All the themes are defined in graduate profiles

ASSESSMENTS

- 15% individual seminar
- 25% group report
- 60% final exam

EXAM

- Study material for final exam
  - Lecture slides and resources
  - Seminars and class discussions
- Online exam
- 8 questions
  - Some questions have sub-questions (i.e., a and b)
  - You have to answer all of them
- 60 marks
- 2 hours plus extra time as set by the Exams office

OUR FEEDBACK

- Research proposal
- Interim report
- Seminars
  - Seminars are being evaluated
  - Grades and comments will be provided soon
- Group reports
  - Under evaluation

YOUR FEEDBACK: SET EVALUATIONS

- 20 students
- 9 responded
- Response rate: 45%
- Thanks to those who already responded!
- Request all other students to help us in achieving our target of 80% by Sunday, October 24

SAMPLE QUESTION: Q1

(5 marks) Euler Phi and modes of operation.

a) Compute $\phi(77)$. [2 marks]

b) Consider AES with ECB and CBC modes. Which one of these two modes is least vulnerable to frequency analysis? Explain why. [3 marks]

SAMPLE ANSWER: A1

a) Compute $\phi(77)$. [2 marks]

$= \phi(7 * 11)$

$= \phi(7) * \phi(11)$ given 7 and 11 are coprime, i.e., gcd(7,11)=1

$= 6 * 10$

$= 60$

SAMPLE ANSWER: A1

b) Consider AES with ECB and CBC modes. Which one of these two modes is least vulnerable to frequency analysis? Explain why. [3 marks]

In ECB, two same plaintext blocks map to the same ciphertext block. Whereas, CBC generates two ciphertext blocks for two same plaintext blocks. Frequency analysis refers to information that attackers can get from the ciphertext. We know that CBC is more secure than ECB. Hence, CBC is least vulnerable to frequency analysis compared to ECB....

SAMPLE QUESTION: Q2

(7 marks) User privacy in Domain Name System (DNS).

a) Describe how DNS queries may compromise user privacy. [3 marks]

b) Propose an approach for enabling DNS users to protect their privacy against eavesdroppers and privacy-invasive DNS servers. [4 marks]

SAMPLE ANSWER: A2

a) Describe how DNS queries may compromise user privacy. [3 marks]

DNS maintains public information, which does not compromise any user privacy unless no queries are made. However, a DNS server can compromise user privacy by monitoring DNS queries made by the user. The DNS server can learn how many queries are made by the user in a specific period, time when the queries made, etc. From that, the DNS server can infer user interests.

SAMPLE ANSWER: A2

b) Propose an approach for enabling DNS users to protect their privacy against eavesdroppers and privacy-invasive DNS servers. [4 marks]

The naive solution is to download all the DNS entries. However, this solution is not efficient. The user can use SSL/TLS for protecting queries from an eavesdropper. However, a DNS server can still learn all the queries.

One approach could be making k number of queries, where k > 1 and at least one query is the real one and the rest of the queries are fake so that the DNS server or eavesdropper cannot learn the actual query. Using this approach, together with SSL/TLS, we can achieve user privacy.

SAMPLE QUESTION: Q3

(7 marks) Refer to the article *"Cross Layer Attacks and How to Use Them (for DNS Cache Poisoning, Device Tracking and More)"* by Klein

a) Briefly explain how the LINUX prandom PRNG contributes to DNS cache poisoning attacks. [3 marks]

b) Propose a solution to mitigate the LINUX prandom PRNG issue. [4 marks]

SAMPLE ANSWER: A3

a) Briefly explain how the LINUX prandom PRNG contributes to DNS cache poisoning attacks. [3 marks]

An attacker can learn the PRNG core state of the victim. The core state can be extracted by collecting a burst of UDP packets (with different UDP source ports) from the victim. Using this information, the attacker can guess 31 bits port+ID in order to poison the cache.

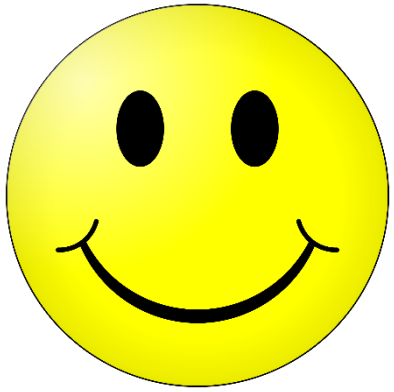
SAMPLE ANSWER: A3

b) Propose a solution to mitigate the LINUX prandom PRNG issue. [4 marks]

The attacks like DNS cache poisoning rely on the PRNG output being externally visible. A system can use pre-image resistance to minimise the likelihood of guessing the core state of PRNG…

CANVAS, COURSE WEBSITE, AND PIAZZA

- Canvas for almost everything
- All lectures were recorded and recording links were distributed through Canvas
  - https://canvas.auckland.ac.nz/courses/60584/external_tools/10150
- Canvas (week/lecture wise organisation)
  - https://canvas.auckland.ac.nz/courses/60584/modules
- Course website (topic wise organisation)
  - https://www.cs.auckland.ac.nz/courses/compsci726s2c
- Piazza
  - https://piazza.com/aucklanduni.ac.nz/semester22021/compsci726



Questions?

Thanks for your attention!