727 Crypto Management

Intro

GIOVANNI RUSSELLO

G.RUSSELLO@AUCKLAND.AC.NZ

Introductions

A/P Giovanni Russello

Office: 303s.583

No regular office hours: send me an email to fix an appointment if you want to see me

Your Turn

Tell me your name and which programme you are in

Assignment 3

Assignment 3 will be out soon.

I will ask you to write a short report (2 pages max) on security-related piece of news

You will need to describe the issue and come up with a possible solution to protect your infrastructure

The assignment is due by April 19 20:00

This assignment is 8% of your total mark

Research Project

Each of you have to chose a topic for a research project from a list we will give you

- You can also select a topic of your choice as long as is in line with the course aims – we could give you some feedback on its appropriateness

No more than 1 student per topic:

- First-in-first-served
- You will email me or Steven your three choices in decreasing order of preference
- We will reply back with the choice that is available
- If none of your choices is available, I will ask you for more

Submit your choice by March 22nd. Project allocation will be out by March 29th

IMPORTANT! Put this line as your email subject: “CS727 Research Project”

Research Project - RoE

It consists of three parts

- A report of 10 pages max (any format will do) – 16%
- An oral presentation (15 min + 10 min questions) to be done in the second part of the semester – 7% oral part and 3% for the questions you will ask
- **Questions asked in class could be used in the final exam**

Research Presentation

The presentations will start in the second part of the semester on week 8

- During week 6 and 7 you can talk to Steven and/or me to get feedback

We will have two presentations per day

The presentation should be short and focused

- 15 min plus 10 min for questions
- Everyone is asked to attend because of the exam questions

Each of you will have a form where you give some feedback on the presentation

- The form will be signed by you and we will collect them – so we can keep track of attendance

Questions for the Presenter

For each talk we will ask two students to ask interesting questions to the presenter

You will get a mark based on the quality of the question (3% of your final mark)

Questions have to show

- You have read about the topic of the talk
- You have a good understanding of the issue at hand
- Thought about some deep and challenging questions

Research Project Report

At the end of week 11, you need to hand in a report on your research project

The report counts for 16% of your final mark

Report Assessment:

- Sources: review the latest literature

- Accuracy: convey the information clearly

- Depth: understand the topic and if possible provide your own contribution

Make sure that you go over UoA Academic Integrity Resources:
https://www.auckland.ac.nz/en/about/learning-and-teaching/policies-guidelines-and-procedures/academic-integrity-info-for-staff/about-academic-integrity.html

Second Part Structure

Key Management and Distribution (week4)

Crypto System Examples (week 5)

Key Management and Distribution

Concerned with the management of keys and distribution of crypto material

It is a complex task that involves complex protocols and management considerations

Cryptographic tools can also be used depending on the scenario

Symmetric Key Distribution with Symmetric Key

A and B wants to establish a secure connection

There are several options

1) A selects a key and delivers it to B

2) A third party can delivery the key to A and B

3) A and B can use a previous key to securely transmit the new key

4) A and B have a secure connection to a third party that will deliver a new key over a secure link

Link vs End-to-End Encryption

Methods 1) and 2) call for physical deliver which is ok in a link encryption

Here we assume that the two parties are physically close

On the other hand, for end-to-end encryption that spans across a network manual delivery is awkward

End-to-end encryption can be done at the network/IP level

- Each pair of nodes in the path have to establish a key. With *N* nodes we need *N(N-1)/2* keys

Alternatively, end-to-end encryption can be done at app/process level

- For each pair of users a key needs to be establish

Q: in a typical scenario, why it is better to have end-to-end encryption at the network level ?

Dynamic Key Distribution

Method 3 can be used for generating new keys dynamically

- Main drawback: any adversary that has access to one key will be able to access any subsequent keys

Method 4 requires a so called Key Distribution Centre (KDC)

- KDC and the entities have pre-established **master keys**
- Using master keys, the KDC can transmit securely a **session key** to the entities for end-to-end communication – session keys are then discarded
- Again, *N(N-1)/2* session keys are needed with *N* entities
- However, you just need *N* master keys, one for each entity – thus master keys can be easily distributed

Establishing a Session Key via a KDC

KDC, A, B where A is the initiator; K_A and K_B master keys

A -> KDC: ID_A||ID_B||N_1

KDC -> A: E(K_A, (K_S||ID_A||ID_B||N_1)||E(K_B,(ID_A||K_S)))

A -> B: E(K_B,(ID_A || K_S))

B -> A: E(K_S, N_2)

A -> B: E(K_S, N_2)

Establishing a Session Key via a KDC

KDC, A, B where A is the initiator; K_A and K_B master keys

A -> KDC: ID_A||ID_B||N_1

KDC -> A: E(K_A, (K_S||ID_A||ID_B||N_1)||E(K_B,(ID_A||K_S)))

A -> B: E(K_B,(ID_A || K_S))

B -> A: E(K_S, N_2)

A -> B: E(K_S, N_2)

Q: Explain how to perform a Man-in-the-middle attack on this protocol and provide a solution to solve this issue.