Exam Revision

Bojan Božić

TU Dublin

April 28, 2020

Introduction

- Date and Time: 13th May 2020, 9am to 6pm.
- Place: Brightspace
- Type: Open Book Exam
- Contents:
  - Cryptographic Tools
  - User Authentication
  - Access Control
  - Malicious Software
  - Distributed Denial of Service Attacks
  - Intrusion Detection
  - Firewalls and Intrusion Prevention
- **NO PLAGIARISM!**

Cryptographic Tools

- Confidentiality with symmetric encryption
- Message authentication and hash functions
- Random and pseudorandom numbers
- Public-key encryption
- Digital signatures and key management

User Authentication

- Digital user authentication principles
- Password-based authentication
- Remote user authentication
- Security issues for user authentication

Access Control

- Subjects, objects, and access rights
- Discretionary access control
- UNIX file access control
- Role-based access control
- Attribute-based access control
- Identity, credential, and access management

Malicious Software

- Types of malicious software (malware)
- Advanced persistent threat
- Propagation-vulnerability exploit-worms
- Payload-stealthing-backdoors
- Propagation-social engineering-span E-mail
- Payload-system corruption
- Countermeasures

Distributed Denial of Service Attacks

- Distributed denial-of-service attacks
- Application-based bandwidth attacks
- Reflector and amplifier attacks•
- Denial-of-service attacks
- Flooding attacks
- Responding to a denial-of-service attack

Intrusion Detection

- Intruders
- Intrusion detection
- Analysis approaches
- Distributed or hybrid intrusion detection
- Honeypot

Firewalls and Intrusion Prevention

- The need for firewalls
- Firewall characteristics and access policy
- Types of firewalls
- Firewall basing
- Intrusion prevention systems

Example Exam Question

8.4 Consider the following login protocol.
user knows password P
user knows Hash function H(.) and has a mobile calculator
user gives login name N to machine
machine generates random number R
machine gives R to user
user computes X := Hash(P) XOR Hash(R)
user gives X to machine
machine uses N to obtain P from password table
machine computes Y := Hash(P) XOR Hash(R)
if X=Y then machine allows login

a. Explain what is wrong with it and how can it be broken.

b. Show a simple way to strengthen this protocol against your attack.

8.4 a. Adversary

- Sees the messages: N, R, X
- Computes Hash(R)
- Computes X XOR Hash(R) = Hash(P)

Later on:

- Adversary Requests Login, submits N.
- Machine generates random number R'.
- Adversary computes Hash(R').
- Adversary computes y = Hash(P) XOR Hash(R').
- Adversary submits y, and logs in as user.

b. To strengthen, simply require the protocol to compute
Hash(R XOR P) instead of Hash(R) XOR Hash(P)