CS471
Security & Info Assurance

Welcome!
2/08/2023

CS471
Security & Info Assurance

Course Schedule

Week #	Monday	Wednesday	Reading	Weekly Topic	Due	Assigned
1	01/16/23	01/18/23		Getting started		
2	01/23/23	01/25/23	Chapter 1	Introduction		Assignment 1
3	01/30/23	02/01/23	Chapter 2	Symmetric Encryption	Assignment 1	Assignment 2
4	02/06/23	02/08/23	Chapter 3	Asymmetric Encryption	Assignment 2	Assignment 3
5	02/13/23	02/15/23	Chapter 4	Key Distribution and Authentication	Assignment 3	
6	02/20/23	02/22/23	Chapters 1-4	Review : **Midterm 1**		
7	02/27/23	03/01/23	Chapter 5	Network Access Control		Assignment 4
8	03/06/23	03/08/23	Chapter 6	Transport Level Security	Assignment 4	Assignment 5
9	03/13/23	03/15/23	Chapter 7	Wireless Network Security		
10	03/20/23	03/22/23	Chapter 8	DNS and Email Security	Assignment 5	
11	03/27/23	03/29/23		Spring Break		
12	04/03/23	04/05/23	Chapters 1-8	Review : **Midterm 2**		
13	04/10/23	04/12/23	Chapter 9	IP Security		Assignment 6
14	04/17/23	04/19/23	Chapter 10	Malicious Software	Assignment 6	Assignment 7
15	04/24/23	04/26/23	Chapter 11	IDS		
16	05/01/23	05/03/23	Chapter 12	Firewalls	Assignment 7	
17	05/08/23	05/10/23		Finals Week		
	*No Meeting			Final Exam: **TBD**		

CS471
Security & Info Assurance

Today

– Assignment 2: Questions?
– Assignment 3: Brute force attacks

CS471
Security & Info Assurance

The X.800 service categories will be important for the entire semester.

As we examine security, this will be our measure.

- **X.800 Service Categories**
  - Authentication
  - Access control
  - Data confidentiality
  - Data integrity
  - Non-repudiation

CS471
Security & Info Assurance

Confidentiality

– What is ‘data confidentiality’?
  ”Keeping our secrets secret”
– How can we provide confidentiality?
  Encryption
– What are the challenges?
  Keys, Key Exchanges, Authentication

Do we *NEED* authentication to maintain confidentiality?
  Yes!

CS471
Security & Info Assurance

Authentication

– What is authentication?
    Identify the other party
– How do we provide authentication in the person?
    We use a token that is difficult to forge or copy.
    This must be from a trusted third party.
    Example: Driver's license or passport.
– How can we provide data authentication online?
    Public key authentication?..

CS471
Security & Info Assurance

Symmetric Encryption

– What is symmetric about some types of encryption?
– Can you name several types of symmetric encryption?
– How many keys?
– What is the size of the key and block?
– How many rounds?

CS471
Security & Info Assurance

Assignment 2:

Work with symmetric and asymmetric encryption using Kali Linux, gpg, md5sum, and steghide.

Questions?

CS471
Security & Info Assurance

Assignment 3:

Perform brute force password attacks against an SSH server using Hydra.

Use Wireshark to capture packets.

Analyze and discuss the results.

Demo Hydra

https://www.kali.org/tools/hydra/

CS471
Security & Info Assurance

Before next time:

- Read Chapter 4 from the textbook.
- Submit Assignment 2
- Start Assignment 3

Next Time:
Chapter 4: Key distribution and Authentication

CS471
Security & Info Assurance

Thank you!