

A decorative graphic on the left side of the slide, consisting of a network of white lines and small circles on a dark blue background, resembling a circuit board or a network topology.

COSC 417 Topics in Networking

TOPIC 1: COURSE INTRO



SCHEDULE

1. Syllabus – Topics, Grading, Miscellany

2. Major Course Topics

1. Routing


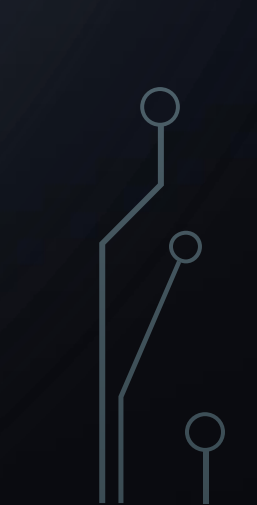
2. The DNS system

3. WLAN





SYLLABUS – COURSE OVERVIEW

- In this course, we'll be looking at certain aspects of networking (particularly via the World Wide Web) in detail
 - You've probably already learnt about these network components, but we'll be taking a deeper dive and really looking at how we can analyze and manipulate the network
 - An emphasis on security and low-level understanding of the network beyond protocols and packets
- 
- 

SYLLABUS – MAJOR COURSE TOPIC AREAS

- The course is roughly split into three areas of interest:
 1. Routing – How autonomous systems interact and route traffic, how to analyze this, and how routing policies can impact traffic flow
 2. The DNS system – How DNS works, running a DNS service, and manipulating the DNS system for good (and evil)
 3. WLAN – A look at security in a WLAN environment

SYLLABUS – PREREQUISITES

- This course has a prerequisite of third-year standing and a minimum of 60% in COSC 328 or a co-requisite of NTEN 317
- Also co-requisite with COSC 318
- I'm willing to waive prerequisites, but you should have at least a high-level understanding of networking and networking protocols to be successful in this course

SYLLABUS – COURSE MATERIALS

- As with my previous courses, there is no textbook or other required literature for this course
- All course content, including slides, labs, and other materials (study guides, important readings, etc) will be available through Moodle and GitHub

SYLLABUS - TENTATIVE SCHEDULE

- Topics/dates listed are tentative
- Quiz 1 will be towards the end of January, while Quiz 2 will be in the second week of March
- Study break Feb 17-21
- Possibly some time at the end for a TBD topic (I'm thinking encapsulation, but open to suggestions)

SYLLABUS – GRADING SCHEMA

- 6 Labs worth 40% of the total grade
 - DNS Project will be 15% of the grade (3 weeks)
 - Remaining 5 labs make up the other 25% of the grade
- 2 in-class quizzes worth 15% each (30% total)
- Final exam is worth 30%
- Possibility of practical test components (TBD)

SYLLABUS QUESTIONS

Any Questions?

- Prereqs
- Grading
- Labs
- Scheduling
- Project
- Topics

The background is a dark blue gradient. In the corners, there are white line-art illustrations of circuit traces and nodes. Top-left: A cluster of lines with several circular nodes. Top-right: A few lines with circular nodes. Bottom-left: A cluster of lines with several circular nodes. Bottom-right: A few lines with circular nodes.

MAJOR TOPICS: ROUTING

HOW WE LIKE TO THINK OF NETWORKS

- For simplicity, we generally think of networks (and the WWW in particular) in fairly simple terms
- When we model a web application, we generally model it as if the user is directly communicating with the server and vice-versa, even though this isn't realistic
- In many cases, this is fine — we can often develop software that works on the internet while safely ignoring the lower-level networking aspects

HOW NETWORKS ACTUALLY ARE

- In reality, when we use the World Wide Web, we're sending our data on a journey across often vast geographical distances, through potentially many independent routers and networks before it reaches it's final destination
- What we want to look at is how this journey is determined, and what impact that has on us as users

AUTONOMOUS SYSTEMS

- The WWW is actually a collection of sub-networks, known as *autonomous systems*
- Special algorithms, known as *routing protocols*, define how these autonomous systems direct traffic through the network, and interface with other autonomous systems
- We're going to look at these routing protocols in detail, to see how a given AS might decide to route our traffic

MAPPING AND ANALYSIS OF NETWORK ROUTES

- Using special *looking glass servers*, we can see the computed routing tables for a given router
- We can use this data to determine where incoming and outgoing traffic is going to be routed through the autonomous system, and use this to map the connections between these systems!
- We can also use this data to help analyze what *routing policies* have been put in place for a given AS

WHEN THINGS GO WRONG

- We'll also take a look at the problems that can arise within routing
- A classic example: The AS 7007 Incident (1997)
 - Accidentally created a networking “black hole”
 - Ended up becoming a preferred route for a lot of traffic
 - Result: Serious network issues as packets simply disappeared into a misconfigured router on AS 7007

The background is a dark blue gradient. In the corners, there are white, stylized circuit-like lines with small circles at the ends, resembling a network or data flow diagram.

MAJOR TOPICS: DNS

THE DNS SYSTEM

- Since humans are generally not very good at remembering long strings of numbers (like IP addresses), the World Wide Web uses a Domain Name Service, which allows us to associate a more memorable domain name with a given IP address that we should communicate with
- I.e. www.google.com → 64.233.160.0

DNS SERVERS

- An interesting aspect of the DNS system is that it is decentralized – you can create your own DNS servers if you want
- In addition, with a private DNS server you can actually change the IP → Domain Name relationship
- We'll be looking at how this can be used for good (blocking ads) or for evil (maliciously redirecting traffic)

PI-HOLE

- A good example of this (and hopefully one we'll be able to play with) is the Pi-Hole
- Uses a Raspberry Pi microcomputer as a fake DNS server, which returns illegitimate responses for domains associated with advertising
- Rather than adblock at a software level, we can use such systems to block advertisements at the network level!



DNS SECURITY

- The DNS system can also be abused by bad actors in attacks – we'll discuss how these attacks are performed and how they can be avoided
- This includes things like Man-In-The-Middle attacks, where a fake DNS server is used to redirect traffic to illegitimate servers, as well as things like DDoS amplification attacks

The background is a dark blue gradient. In the corners, there are white line-art illustrations of circuit boards or network diagrams, featuring lines and small circles representing components or nodes.

MAJOR TOPICS: WLAN

WIRELESS INTERNET

- With the proliferation of laptops, smartphones, and Internet-of-Things (IoT) devices, wireless networking (WLAN) has become a ubiquitous part of everyday life
- Wireless Internet is available in many venues and areas nowadays, but we often don't consider the security aspects of connecting to these public networks

WIRELESS INTERNET - SECURITY


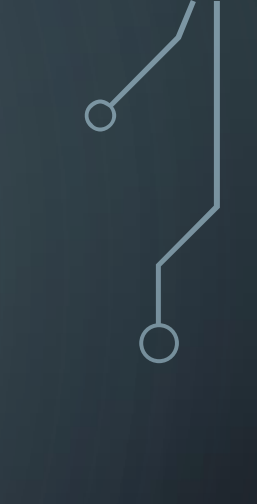
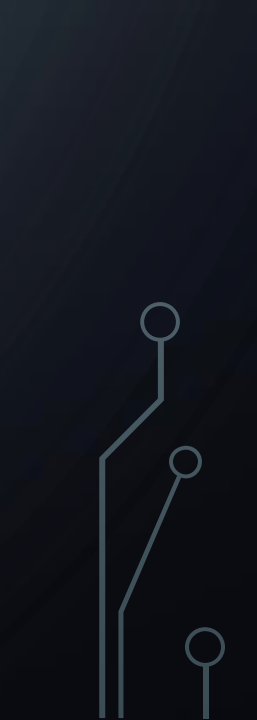
- We'll take a look at the general principles of securing a WLAN network, and some of the more common attacks used to target users on WLAN
- This includes:
 - Man-In-The-Middle attacks: intercepting traffic between users and the router
 - Packet sniffing: reading data destined for others on the network
 - WEP, WPA, WPA2 encryption

WLAN – IP AND MAC ADDRESS SPOOFING

- We will also take a look at how common security measures can be bypassed on a WLAN network via IP and MAC address spoofing
- This includes best practices for securing a WLAN, and how you can monitor your WLAN traffic for potential bad behaviour by unauthorized users or bots



NEXT LECTURE

- On Friday, we'll begin our dive into autonomous systems and the BGP and IGP routing protocols
 - We'll take a look at some of the major autonomous systems that serve our area, and how they route their traffic
 - Labs begin next week
- 
- 
- 



SCHEDULE

1. Syllabus – Topics, Grading, Miscellany

2. Major Course Topics

1. Routing

2. The DNS system

3. WLAN



The image features a dark blue gradient background with faint, stylized circuit board traces in the corners. These traces are composed of thin white lines and small white circles, resembling electronic components or data paths. They are located in the top-left, top-right, bottom-left, and bottom-right corners, framing the central text.

SO LONG, FOLKS!