SWINBURNE UNIVERSITY OF TECHNOLOGY

Network Security and Resilience / Advanced Security

Networks Review

Lecture two

Outline of Lecture

- Review of major access network technologies
- Discussion of their potential security weaknesses

Learning objectives

- You should be able to
  - Describe the major access network technologies
  - identify (in broad terms) their security weaknesses
  - Explain (in broad terms) how these security weaknesses can be managed

Networks

- Many ways to classify network technologies
  - Topological location: Core / Distribution / Access
  - Medium: Wireless / Copper / Fibre
  - Ownership: Public / Corporate / Home
  - Coverage: PAN / LAN / MAN / WAN
  - Capacity: 1000Ethernet / Cable Modem / ADSL2
  - Purpose: IoT, Voice, Data
- Mostly interested in access networks
  - Most likely to be subject to attack
  - include Ethernet, ADSL, Cable Modem, Wireless LAN, UMTS, GPRS, WiMax, HSPA, LTE
- But some interesting issues in core networks
  - BGP exploits
  - One known Lawful Interception exploit

Access networks

- Access networks concerned with 'last mile' problem
  - Provide connectivity to a geographically distributed population
- Core networks shift large volumes of traffic between different nodes in the network which may be located vast distances apart
- Many different access networks
  - appropriate network depends on many factors
    - population density of users to be connected
    - the distance to the nearest core network node (such as a telephone exchange or wireless base station)
    - existing installed network infrastructure
    - purpose of network

Access networks

- Not all kinds of Access Networks are available in all places at all times
  - coverage often limited
    - eg, coverage of some broadband wireless networks is often limited. WLAN for example has a range of only tens of metres
  - dependence on what other infrastructure has been deployed
    - eg, Cable Modem networks have usually been deployed in the wake of cable television deployment.
    - eg, ADSL networks are usually deployed on existing two-wire telephony infrastructure
    - Long history of cellular networks building data networks on voice networks
      - GPRS on GSM, HSPA on UMTS

Access networks

- Not all access networks have the same level of reliability
  - low reliability may be acceptable or may be incorporated into the network design
  - usually reflected as fluctuations in bandwidth
    - Example: wireless is inherently unreliable, but protocol design (such as TCP) ensures reliable delivery of data
- Not all access networks have the same usage and implementation costs
  - networks built on some technologies (such as LTE) are much more expensive to implement (and hence to use) than say wireless LAN networks
- Not all access networks have the same coverage
  - public networks usually have greater coverage than private networks

Access networks

- Not all access networks have the same capacity
  - usually a tradeoff of some kind
    - eg, LTE high coverage : but bit rate usually less than 1 Gbps
    - eg, WLAN small coverage: but bit rates up to 7 Gbps (802.11ac)
- Not all access networks are as secure as each other
    - wireless networks generally less secure than wired networks
- In summary, there are many different access network technologies with different capabilities, purposes and costs
- There is no single 'best' access network

Overview of access network technologies

- Can be differentiated by physical layer and data link layers
- Physical layer
  - transmission medium and how individual bits are encoded onto it
    - wireless, coaxial cable, twisted pair, optic fiber
    - bits encoded as variations in amplitude, phase, frequency, baseband
    - multiplexing TDM, FDM, CDM
- Data link layer
  - concerned with the transmission of blocks of bits called ‘frames’
  - multiple users accessing a single channel usually requires a Medium Access Control mechanism
  - possibly some error correction mechanism

Overview of access network technologies

- Connectionless and connection oriented networks
  - Connection oriented networks involve some initial signalling phase where a logical connection is set up between the source and the destination
  - Connectionless networks do not have such a signalling process
- Circuit switched and packet switched
  - Circuit switched connects two or more DTEs (data terminal equipment) and permits the exclusive use of a data circuit between them until the connection is released
  - Packet switched splits data into chunks which are separately routed over a shared network

Security of access networks

- Generally wireless networks less secure than wired networks
  - Difficult to constrain signal to a specific area (confidentiality)
  - More error prone (integrity)
  - Subject to interference (availability)
- Connectionless networks (generally) less secure than switched networks
  - Connectionless networks usually broadcast data, making sniffing possible
- Packet switched networks less secure than connection oriented networks
  - Packets can be copied and stored more easily than a stream of bits

Exercise

- If your organization proposed using the following technology would you be more or less concerned than if they used LTE?
  - Uses ISM band
  - Corporate ownership
  - No built in encryption
  - Low bit rate
  - Wireless technology
  - Broadcast
  - Some separation of users based on frequency and other factors but limited
  - Uses the Aloha protocol to deal with channel contention

Specific technologies

- Will review each of the following and make some comment on their inherent level of security
  - Ethernet
  - ADSL
  - Cable Modem
  - Wireless LAN
  - LTE
  - 5G NR
  - Bluetooth

Ethernet

- Frame-based LAN technology
- Defines frame formats, MAC controls
  - Mostly standardised by IEEE 802.3
- Development history
  - Originally shared coaxial cable
  - Problems with larger networks
    - One fault could stop all attached stations from transmitting
    - Increased broadcast domain
    - Led to ethernet bridges
  - Ethernet hub and UTP
  - Ethernet switches
  - Ethernet layer 3 switches

Security of Ethernet

- Switched Ethernet can be very secure
  - But can be subverted
  - Switch can be made to operate in broadcast mode
    - MAC flooding
    - causes switch MAC tables to be filled so that existing entries are deleted
    - frames with unknown MAC addresses are broadcast
    - Misconfiguration errors: Trunks and Access ports
    - Lots of configuration to prevent these but creates opportunities for misconfigurations
  - ARP poisoning

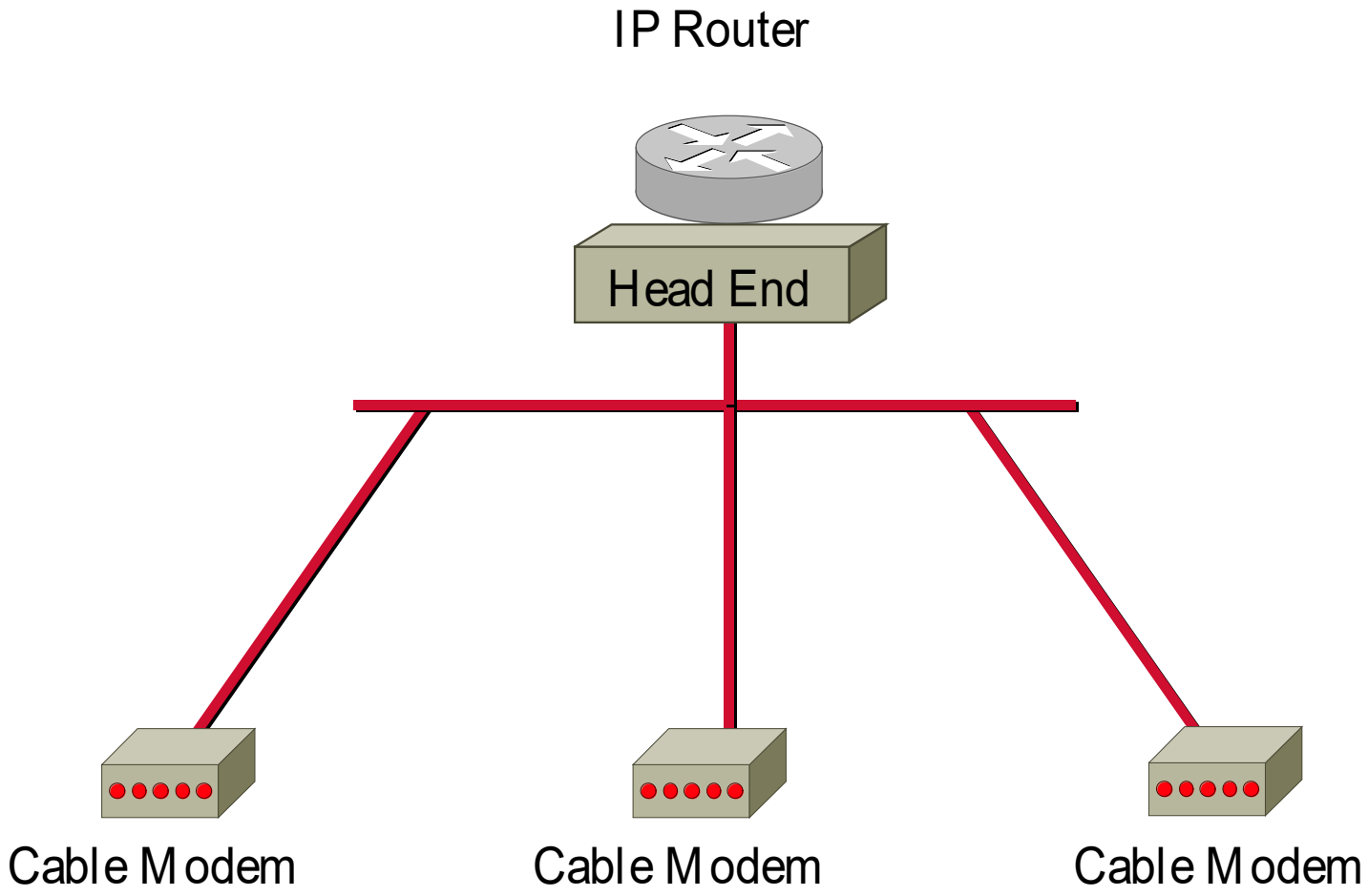
Cable Modem networks

- Cable Television based
- Use CATV infrastructure for data networking
- Implemented as an inverted tree
  - root of the tree referred to as the ‘head-end’
- An analog medium
  - 6 MHz broadcast channels
  - data from multiple users is modulated onto multiple 6MHz channels
- Usually an asymmetric network
  - high bit rate forward link
  - low in reverse link

Cable Modem

- Main standard is DOCSIS
  - Data Over Cable Service Interface Specification
  - Supports delivery of Ethernet frames between the cable modem and the head-end
  - Specifies a Medium Access Control mechanism for sharing of channels
- DOCSIS Architecture
  - Cable Modem (CM) at the Customer premises
  - Cable Modem Termination System (CMTS) at the head-end

Cable Modem Network Architecture



Security of Cable Modem networks

- DOCSIS has some useful built-in security mechanisms
  - but not always implemented
  - CMTS security provided by 'hooks' to other services (such as authentication via 802.1X)
- DOCSIS security has two protocol components:
  - an encapsulation protocol for encrypting packet data across the cable network
  - a key management protocol for providing the secure distribution of keying material from the CMTS to client CMs.

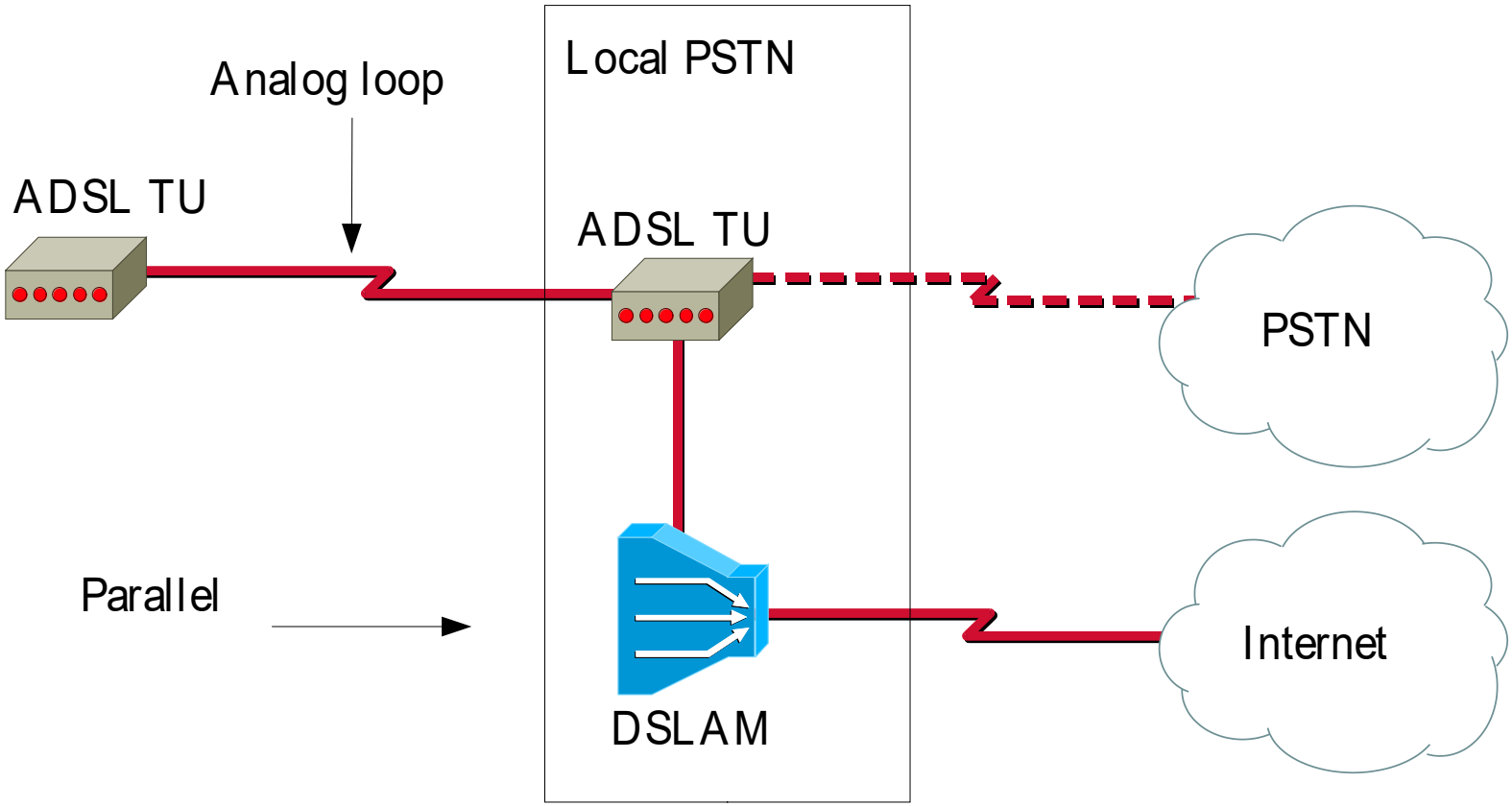
ADSL and VDSL

- Digital Subscriber Line technologies leverage existing telephone networks to provide broadband access.
- First major one was ISDN
- The most important of these technologies now are xDSL family
  - xDSL is a family of subscriber link technologies including Asymmetric DSL, High-speed DSL (HDSL), Very high speed DSL (VDSL) and variations of each
  - xDSL uses the existing PSTN twisted pair copper loop otherwise used for standard telephony.
  - Uses ATM for data transport
  - Operates in parallel with the existing telephone service but independently and without affecting it.
    - Uses different frequencies to that of standard telephony

xDSL Architecture

- At each end of the analog loop is an xDSL transmission unit
  - Modulates the digital bitstream onto the local analog loop using frequencies above those used by telephony
  - At the local PSTN exchange the bitstream is demodulated by another xDSL TU and passed onto the parallel data network via a DSL Access Module (DSLAM) which provides connectivity to the Internet
- xDSL is not an end-to-end networking technology.
  - Provides the last hop to a customer site
  - At the exchange, communications over the ADSL link are separated from any telephony communications and transferred through an entirely independent network.

ADSL Architecture



Security of xDSL

- Generally very secure
  - point to point
  - wired medium
  - risks are more at higher layers

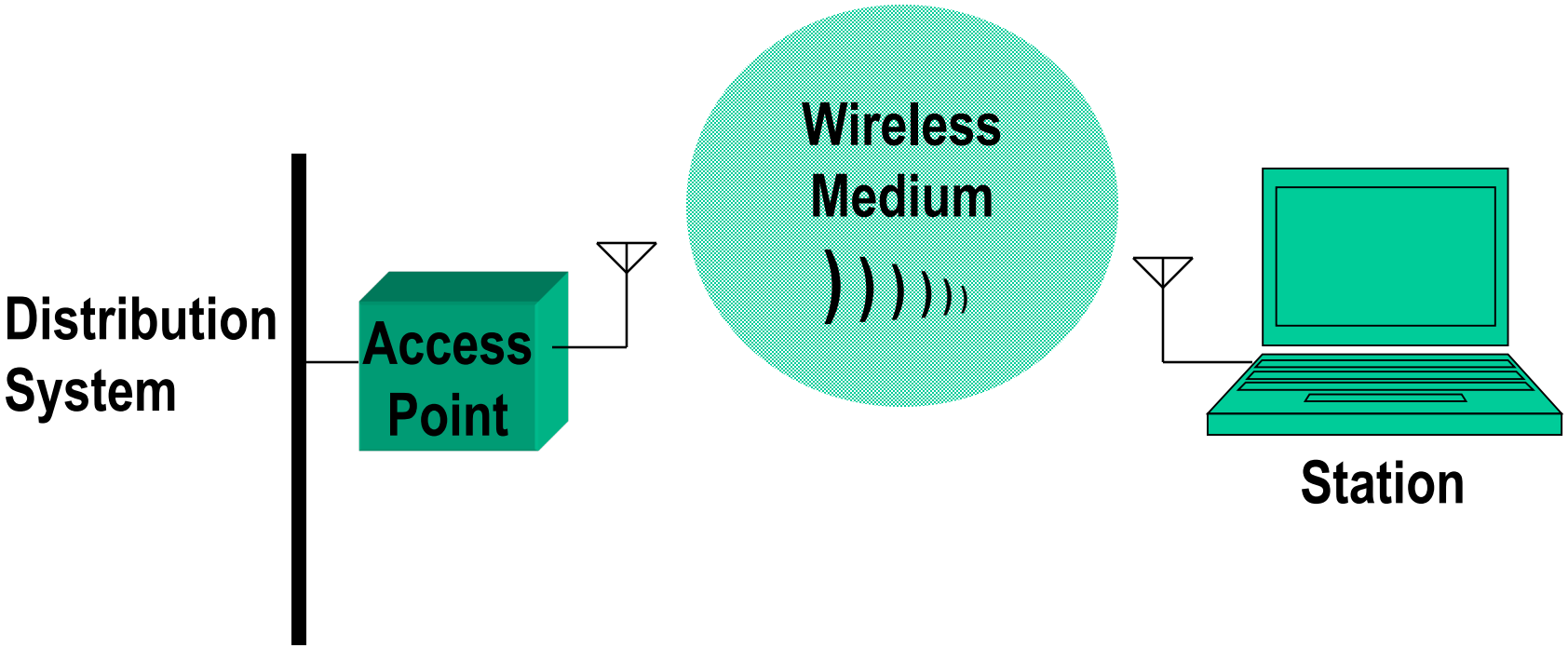
Wireless LANs

- Wireless LANs protocols defined by the IEEE 802.11 work group for the ISM band
  - All 802.11 networks use a common MAC layer, but vary in the physical layer details.
    - Most commonly used is the 802.11g and 802.11n standard operating in the 2.4 GHz Industrial, Scientific and Medical band (ISM).
    - 802.11n takes advantage of developments in transmitter receiver design (MIMO)
    - 802.11ac up to 7 Gbps (depending on configuration)

Wireless LANs

- Wireless LANs operate in the ISM band
  - An area of spectrum that is minimally regulated in which anyone may operate radio equipment subject to a minimal set of restraints, primarily on power levels
  - 802.11 is subject to interference from Bluetooth communications devices, some cordless telephones, and Microwave ovens.

Wireless LAN Architecture



Security in WLANs

- Historically a very weak area
  - Wireless communications can't be contained within a single building
  - Remarkable how far a usable signal can propagate
  - Authentication necessary to prevent 'back door' access into rest of network
- Wired Equivalence Privacy (WEP)
  - No longer in use
- Wi-Fi Protected Access (WPA and WPA2)
  - IEEE 802.11i standard
  - encryption and frequent change of keys
- Will deal with advances in 802.11 security in depth later in the subject

Long Term Evolution (LTE)

- Sometimes “4G”
- From the fourth generation cellular onwards the core and radio network were separated with the intention of allowing them to develop separately
  - LTE is radio access network and Evolved Packet System (EPS) is the network core
- LTE and EPS build on successful history of security of other cellular networks
- Flexible security architecture allowing for implementation of developments in cryptography

5G NR

- "Fifth Generation New Radio"
  - Fifth generation of cellular
- Three broad areas of activity defined by use cases
  - eMBB Enhanced Mobile Broadband
  - mMTC Massive Machine Type Communication
  - URLLC Ultra Reliable and Low Latency Communications
- These define what the network will do, not how they will do it
- But we can say a few things about implementation
  - eMBB is a straightforward evolution of LTE
  - mMTC will adapt existing cellular network technologies intended for IoT mainly NB-IoT and LTE-M
  - URLLC is the interesting one

5G NR

- URLLC
  - Will require development of technologies in 30+ GHz range
  - Consequent short range and many more base stations
    - (higher frequency means poorer propagation)
  - Will make available huge amounts of bandwidth
    - Will have 20 to 30 x previous BW
  - Will require changes to core network
    - Low latency
  - Complex ‘front haul’ and ‘back haul’ networks

5G NR Security

- Builds on successful LTE / EPC framework which is in turn derived from successful earlier generation security frameworks
- Fixes some limitations from earlier generations related to SIM card identifier (IMSI)
- Still not clear as to how to scale up NB-IoT and LTE-M to expected huge number of devices in mMTC

Bluetooth (IEEE 802.15.1)

- A cable replacement specification
- Short range, low bit rates
- Not really an access technology, but can be used in tandem with access technologies
  - Handsfree connection to mobile phone
  - Wireless connection of peripherals – keyboard, monitor, mouse to Personal Computer
  - PDA connection to Personal Computer
- Quite a few Bluetooth exploits
  - More (much more) later in the semester

Many emerging IoT network technologies

- General
  - LoraWAN, Bluetooth Low Energy, Bluetooth Mesh, 6LoWPAN
- Personal
  - ANT and ANT+
- Home automation
  - ZigBee integrated with IP
- Cellular
  - SigFox, NB-IoT, LTE- M (LTE for Machines)
- Industrial Internet of Things
  - PROFINET, TSN, UA, OPC

Conclusion

- Many access network technologies
- All with different strengths and weaknesses including different levels of security
- Important access networks are
  - Ethernet, ADSL, Cable Modem, Wireless LAN, 3G, WiMax, HSPA, LTE, Bluetooth
- Wireless networks intrinsically less secure than wired networks
  - require specific action to make them secure