University of Glasgow | School of Computing Science

Networks & Operating Systems Essentials

Dr Angelos Marnerides

<angelos.marnerides@glasgow.ac.uk>

School of Computing Science

Based on slides © 2017 Colin Perkins , ©2020 Angelos Marnerides

PRIVACY AND SECURITY (1)

Network Monitoring…not that private

- Possible to intercept traffic on a network
- Many countries monitor traffic for legal reasons
  - Much is desirable – good reasons for law enforcement to intercept some traffic – but Edward Snowden showed pervasive monitoring widespread
  - IETF consensus: "we cannot defend against the most nefarious actors while allowing monitoring by other actors no matter how benevolent some might consider them to be, since the actions required of the attacker are indistinguishable from other attacks" [RFC 7258 "Pervasive Monitoring is an Attack" – https://tools.ietf.org/html/rfc7258]
- Organisations may monitor traffic for business reasons
  - "Your call may be monitored for quality and training purposes" – regulatory requirements to be able to monitor some traffic
  - To support network operations and trouble-shooting
- Malicious users may monitor traffic on a link
  - For example, many Wi-Fi links have poor security allowing anyone on the same Wi-Fi network to observe all traffic on that network
  - Hacked routers may allow monitoring of backbone links
  - Steal data and user credentials; identity theft; active attacks

CIA Triad

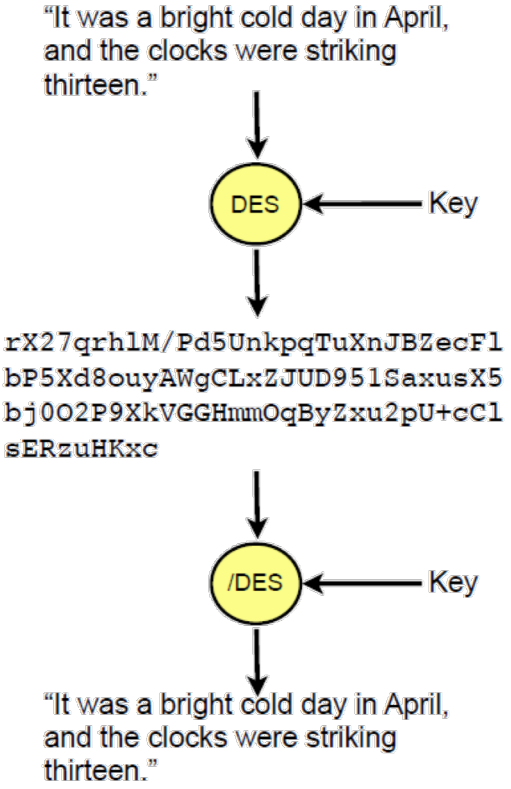
- **C**onfidentiality, **I**ntegrity, **A**vailability
  - ***Confidentiality*** : Who is allowed to access what
  - ***Integrity:*** Data to be protected and not tampered/modified/deleted by unauthorized party(ies)
  - ***Availability:*** data to be protected but also available when needed

Towards CIA

- Must encrypt data in a computationally efficient manner to serve the needs for CIA.
- Two basic approaches
  - Symmetric cryptography
    - Advanced Encryption Standard (AES)
  - Asymmetric (public key cryptography)
    - The Diffie-Hellman algorithm
    - The Rivest-Shamir-Adleman (RSA) algorithm
    - Elliptic curve-based algorithms
  - Complex mathematics – will not attempt to describe

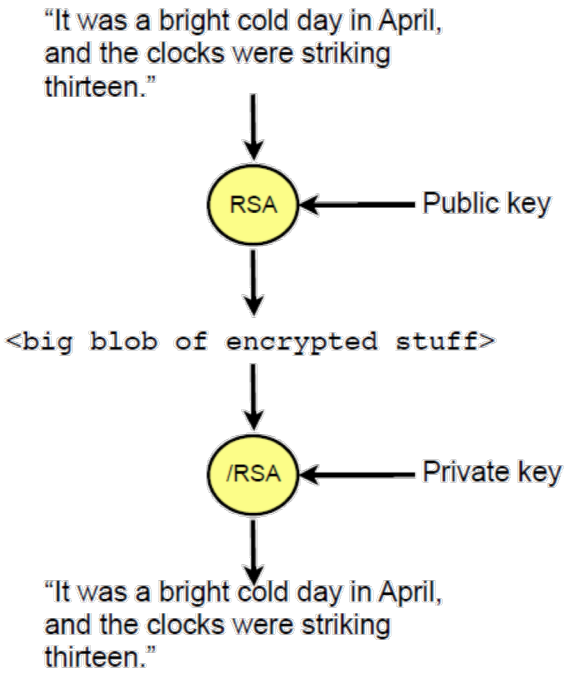
Cryptography

- Symmetric Cryptography
  - Function converts plain text into cipher-text
    - Fast – suitable for bulk encryption
    - Cipher-text is binary data, and may need base64 encoding
  - Conversation is protected by a secret key
    - The same key is used to encrypt as is used to decrypt
    - Key must be kept secret, else security lost
  - Problem: how to distribute the key?



Cryptography

- Public Key Cryptography
  - Key split into two parts
    - Public key – is widely distributed
    - Private key – must be kept secret
  - Encrypt using public key → need private key to decrypt
    - Public keys are published in a well known directory
      - Solves the key distribution problem
  - Problem: very slow to encrypt and decrypt



Cryptography

- Hybrid Cryptography
  - Use combination of public-key and symmetric cryptography for security and performance
    - Generate a random, ephemeral, session key that can be used with symmetric cryptography
    - Use a public-key system to securely distribute this session key – relatively fast, since session key is small
    - Encrypt the data using symmetric cryptography, keyed by the session key
  - Example: Transport Layer Security (TLS) protocol used with HTTP (i.e. HTTPS – more later)

Authentication

- Encryption can ensure confidentiality – but how to tell if a message has been tampered with (i.e. keeps its integrity)?
  - Use combination of a cryptographic hash and public key cryptography to produce a digital signature
  - Gives some confidence that there is no man-in-the-middle attack in progress
  - Can also be used to prove origin of data

Authentication

- Cryptographic Hash Functions
  - Generate a fixed length (e.g., 256 bit) hash code of an arbitrary length input value
    - Should not be feasible to derive input value from hash
    - Should not be feasible to generate a message with the same hash as another
  - Examples:
    - MD5 and SHA-1 (both are broken – do not use)
    - SHA-2 (a.k.a., SHA-256)

      SHA256("It was a bright cold day in April, and the clocks were striking thirteen")
      = 0fc5c1f4082e697b211cdfa12479b4b3dd57c8da69c8904f5e0fc32499cf4245

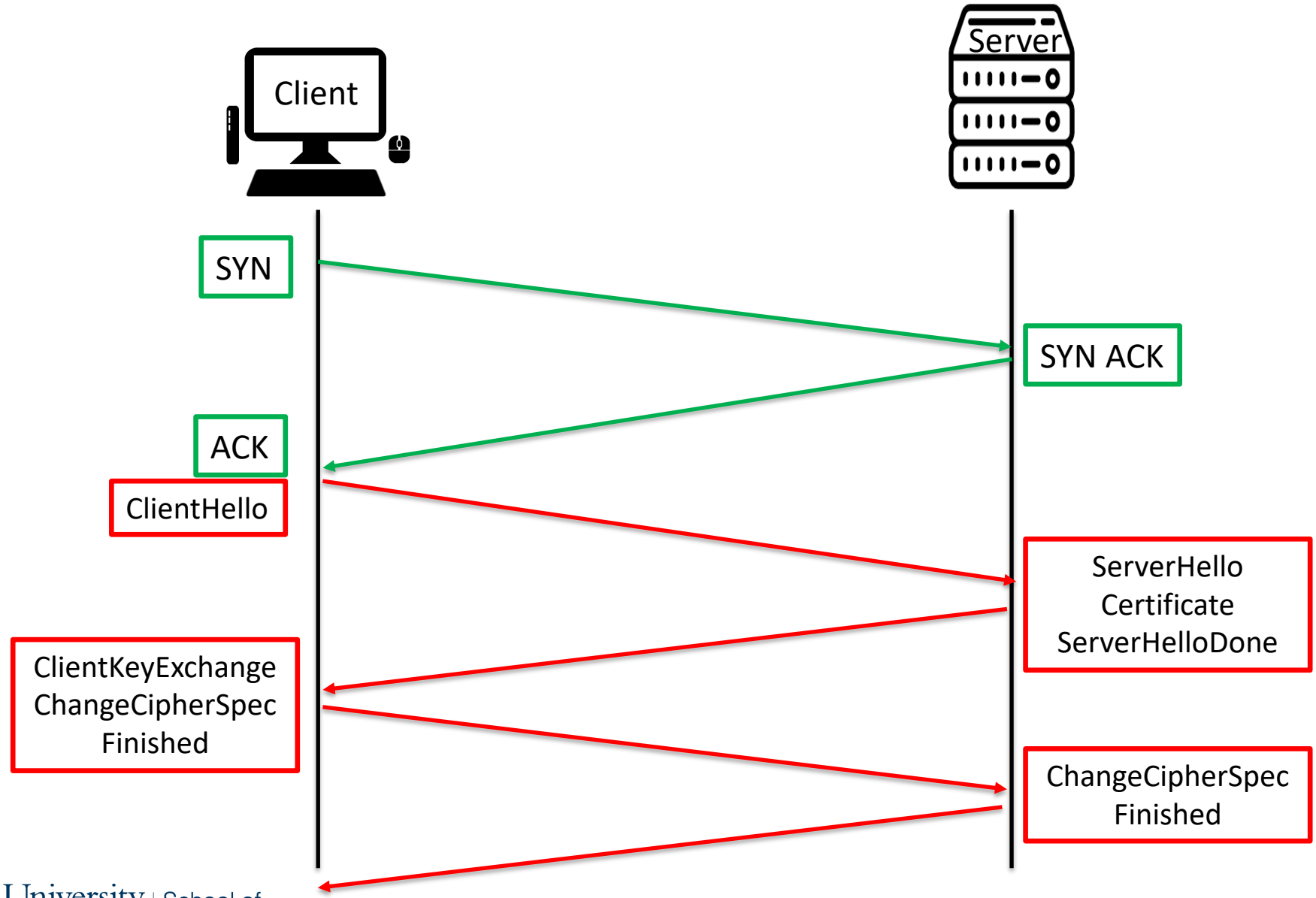
Authentication

- Digital Signature Algorithms
  - Generating a digital signature:
    - Generate a cryptographic hash of the data
    - Encrypt the hash with your private key to give a digital signature
  - Verifying a digital signature:
    - Re-calculate the cryptographic hash of the data
    - Decrypt the signature using the public key, compare with the calculated hash value → should match

Transport Layer Security (TLS)

- De facto standard/protocol for Internet security
- Enables privacy and data integrity between two communicating applications.
- Based on Secure Socket Layer protocol (SSL v.3)
- Used in every browser.
- Now we have versions 1.2 and 1.3.
- Reliable in terms of CIA

TLS basics (handshake) – HTTPS foundation

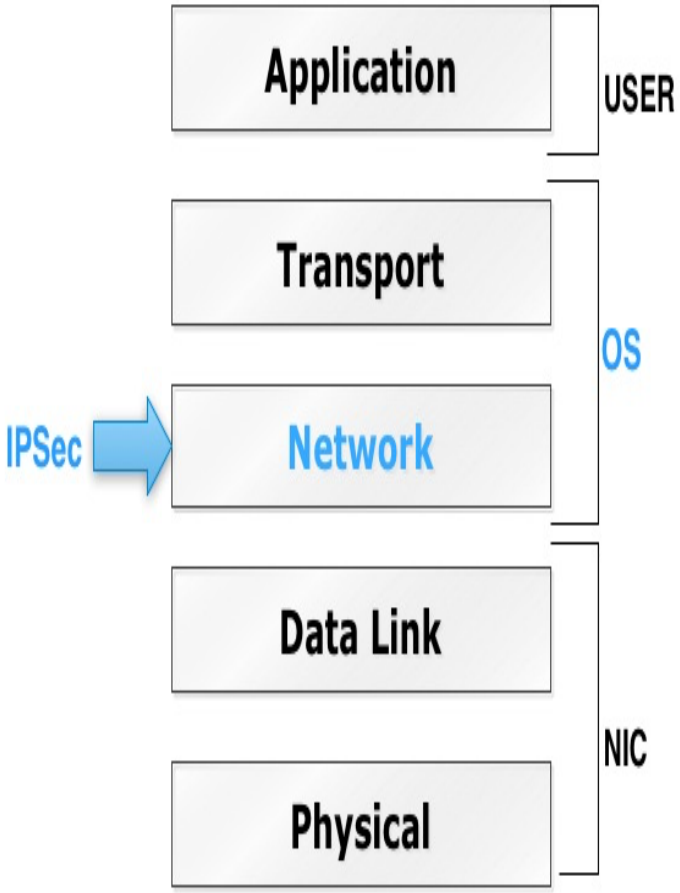


Aside: Using TLS

- IETF provides guidelines for how best to use TLS
  - https://tools.ietf.org/html/rfc7525
  - Read this if you use TLS in your application – and check for updates first
  - IETF "Using TLS in Applications" working group https://datatracker.ietf.org/wg/uta/charter/
- State-of-the-art in TLS implementations is in flux
  - OpenSSL is popular, but poor quality
    - Alternatives in rapid development – not clear which is the best long term option
  - For macOS or Windows, use the system libraries

IPSec

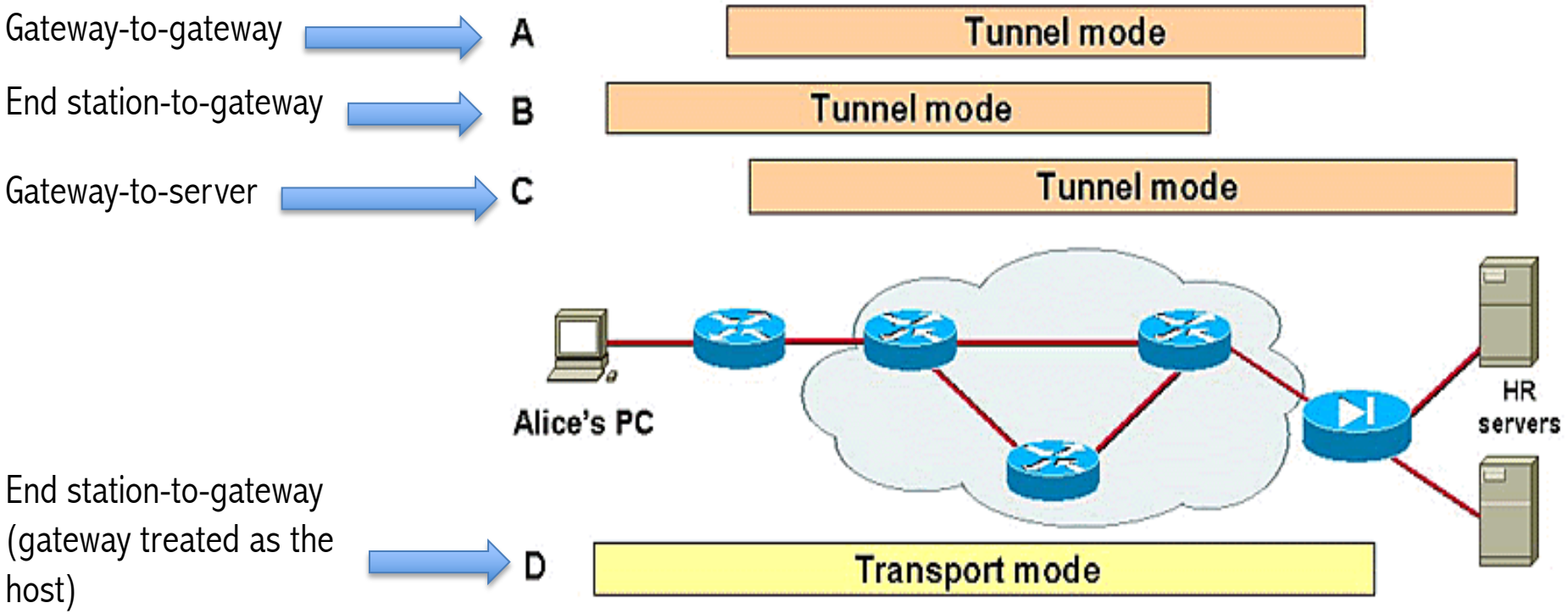
- A *framework* of open standards that incorporates/employs cryptographic secure services in IP networks.
- Initially developed by IETF in 1998 for IPv6, then adapted for IPv4.
- Resides on the network layer.
- Implemented in the OS-level (mainly).
- Quite complex. (a bunch of RFCs/over-engineered with many useless features)



IPSec Modes

- ***Tunnel mode***: between gateways, end-host to a gateway, or when gateway acts as a proxy for the hosts behind it.

- ***Transport mode:*** end-to-end security between hosts, e.g. between end-hosts, end-hosts and a gateway that acts as a host (vulnerable to eavesdroppers).



IPSec & ISAKMP

- **Security Association (SA):** shared security attributed between two network components.

- **SA**s in IPSec enabled by the **I**nternet **S**ecurity **A**ssociation & **K**ey **M**anagement **P**rotocols (**ISAKMP**).

- The ISAKMP protocol (RFC 2408) defines procedures for:
  1) Authentication
  2) Creation/Management of SAs
  3) Key generation /key transport techniques
  4) Mitigation of threats (e.g. DoS attacks, replay attacks)

IKE, ESP & AH

- **I**nternet **K**ey **E**xchange (**IKE**): used to establish SAs – it builds upon ISAKMP and the Oakley protocol.

- **E**ncapsulating **S**ecurity **P**ayload (**ESP**): payload encryption ensuring *authenticity, integrity* and *confidentiality.* – it does not provide integrity and authentication for the ENTIRE packet.

- **A**uthentication **H**eader (**AH**): authentication only for payload and header.

IPSec Negotiation Phases

IKE Negotiation Phase 1

→ Establishment of SAs between two entities

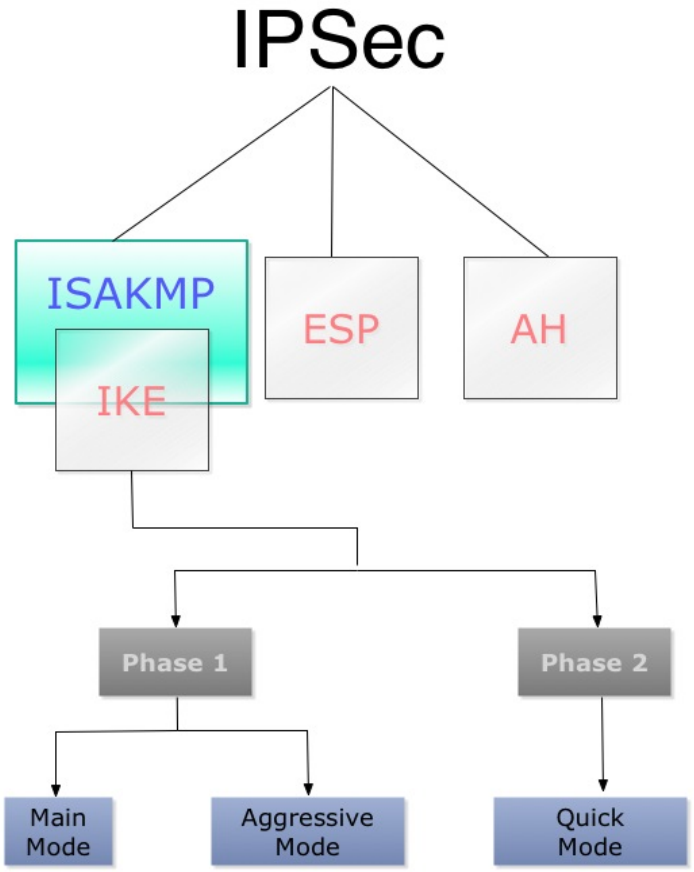
→ Two modes: Main or Aggressive

→ 4 techniques for authentication:

- Public key signatures
- Symmetric key
- Public key encryption
- Revised public key encryption

→ Uses ephemeral Diffie-Helman (EDH) to establish session key

→ Provides perfect forward secrecy



IKE Negotiation Phase 2

→ Establishment of SAs for ESP/AH protocols

→ One mode : Quick Mode

Aside: Existing Secure Protocols

- Existing security protocols give confidentiality and authentication
  - Secure Sockets Layer (SSL) – obsolete and broken, use TLS instead
  - Datagram TLS – for securing UDP-based applications
  - Secure RTP – for securing interactive multimedia applications
  - Secure shell (ssh) – for securing remote login applications
- Use them – don't try to invent your own!

Recommended Reading

- Peterson & Davie: Sections 8.1.1, 8.1.2, 8.4.3, 8.4.4
- Kurose & Ross: Sections 8.1, 8.2, 8.7