HSEP 314 notes

Root server: Small number of routers that control traffic for all high level domain names (.com .uk. cn etc) and if none of the routers along the path to that server can find the destination/IP address you are trying to connect to. For example if you are emailing someone outside of your country.

Physical Layer:

Key defining feature: Physical hardware within the various technologies that undergird internet functionality are housed.

Global distribution: Relatively even, determined by historical and emerging market development trends (basically, by global economics)

Logical Layer:

Key defining feature: Any syntactic element of the internet (mostly code, but occasionally physical (modems, etc)

Global distribution: Extremely uneven, determined by the hierarchical nature of the Domain Name System and the legacy of ownership of the root servers by western companies.

Information Layer:

Key Defining feature: Actual substantive information content that we put online. In other words, all information that relates to our non-functional interactions with the internet.

Global distribution: Determined in tiers of accessibility (who can see what content and in what form)

The User Layer:

Key Defining Feature: The physical corollaries of our digital presence

Global Distribution: Determined largely in terms of global population distribution, but not entirely. Because it is possible to fabricate or amplify online presence, the user layer is not a 1 for 1 representation of us in the real world.

-

Future Shock: The intensification of conflict and unprecedented security challenges follows massive structural changes in how society works as the world shifts to new paradigms of normal, with the result being societal inequality, information overload, malaise and subsequent turmoil.

Factors: Human factor (both design and use), path dependency, network externalities (the problem of scale)

Cybersecurity is a layered construct.

If the core function of new information technologies is to enable more efficient communication, then the first challenge in designing such systems is in how to customize information transmission mechanisms to ensure security.

Authentication: Information recipients need to be able to verify that incoming messages come from who they think they come from. In other words, we need to be able to figure out if they are who they say they are.

Authorization: Recipients need to be able to verify that others have the right to send what they're sending.

Cypher text only attacks: Attacks that use only the cipher and text without access to the plain text. The assumption is that the attacker has enough context to stand a chance of breaking the cipher.

Known plaintext attack: Attacks that succeed because the plain-text (or at least part of it) is already known to the attacker and where the attacker also possesses the cipher-text.

One way mathematical formulas. Some equations are easier to solve one way than the other, extremely hard to reverse engineer.

Layers: Information layer, logical layer, physical layer, user layer.

IP Spoofing: Fabrication of IP address information in packets in order to bypass IP based procedures.

Pocket Sniffing: Capture and reading of unencrypted packet information with specialized software.

Wifi cracking: Specific packet sniffing activity that captures packets and attempts to find login credentials.

Man in the middle attacks: Packet eavesdropping using specialized software to intercept packets, read them, block continued transmission and then mimic original content.

Worms are a subset of viruses; the difference is that a worm can spread itself. The virus spreads due to human action.

Denial of Service attacks: Use one (or very few) computers to disrupt network access by taking advantage of design features to limit bandwidth

Distributed Denial of Service attacks: Use of numerous computers (often a botnet) to disrupt legitimate network activity.

Application later DoS: Manipulation of a known vulnerability of the level of the application to disrupt network access for a specific program/function. Most often used as a distraction.

Diamond model of intrusion analysis: For every intrusion event there exists an adversary taking a step towards an intended goat by using a capability over infrastructure against a victim to produce a result.

Kill chain: Model of a life cycle of most cyber attacks

The attacker identifies targets, may look for services or individuals to exploit.

The attacker successfully executes malicious code on one or more systems, or the attacker is internal, using already granted access,

Attribution problem:

Conventional wisdom: The internet, as a medium, makes attribution of real world perpetrators difficult to the point of minimal legal or strategic utility.

Technical attribution is always possible. However, sophisticated threats demand significant commitments of time and resources to unravel. Sociopolitical attribution of intentions and actions Is far more difficult and virtually demands the commitment of immense intelligence resources to get it right.

Consequences: Aside from major implications for international cooperation the challenge of attribution means that we have often committed resources in inefficient ways and have incurred institutional drag with regards to addressing future manifestations.