Concepts & Terms

Concepts & Terms

During the course of the project, a number of concepts and terms were mentioned in passing that could not be covered in detail because of the very short amount of time available during the Excelerator program. This section is a list of those items along with definitions and/or pointers to further information.

Term	Definition
API	A defined set of commands, data formats, and conventions that let software components interact. APIs hide the internal workings of a system and expose predictable methods for exchanging data—like how apps talk to cloud services or databases.
Asymmetric encryption	Uses a pair of cryptographic keys: one public (shared openly) and one private (kept secret). Data encrypted with one key can only be decrypted with the other, enabling secure communication and digital signatures without sharing secrets in advance.
Backdoor	An alternate entry point into a computer system that bypasses normal authentication. It may be intentionally added by developers for support or secretly installed by attackers to regain access after compromise.
BookStack	BookStack is an open source, opinionated (it has a pre-defined organizational structure based on shelves, books, chapters, and pages) wiki application that you can host on your own server. It is great for collecting documentation and notes, and is the current application that runs the infrastructuresquad.com site. More information available at: https://www.bookstackapp.com
Ciphertext	Data transformed by encryption into an unreadable form. It looks random but can be decrypted back to the original message if the correct key is known.

Cleartext	Data stored or transmitted without encryption. Anyone with access to the data stream can read or modify it.
Containers: OS vs Docker	OS containers isolate applications within a single kernel using features like namespaces and cgroups. Docker adds tooling, packaging, and a registry system that make containers portable and easy to deploy across different environments.
DDOS (Distributed Denial of Service)	An attack in which many computers flood a target with traffic or requests to exhaust its resources, making websites or services unreachable.
DHCP (Dynamic Host Configuration Protocol)	Automatically assigns IP addresses and other network settings (like gateway and DNS) to devices joining a network. This avoids the need for manual configuration.
DNS (Domain Name System)	A hierarchical naming system that translates human-readable domain names (like example.com) into IP addresses used by computers to locate servers.
ICMP (Internet Control Message Protocol)	A support protocol used by routers and hosts to send diagnostic or error messages. Tools like ping and `traceroute` rely on ICMP.
IP spoofing	Falsifying the source IP address in a packet's header to disguise the sender's identity or impersonate another system, often used in attacks.
Linksys	A common consumer networking brand owned by Belkin, known for home routers, switches, and access points.
Mobile router ("mob rtr" on network design whiteboard)	A router that provides Internet connectivity via a cellular modem (LTE/5G) and shares that link to local devices over Ethernet or Wi-Fi. Used in vehicles or remote setups.
n8n	A self-hosted workflow automation platform that connects APIs and services through drag-and-drop logic, similar to Zapier but open source.
netcat (nc)	A versatile networking utility for reading and writing data across TCP or UDP connections. Used for testing ports, transferring files, and building simple servers or backdoors.

NTP (Network Time Protocol)	Synchronizes system clocks over the Internet to within milliseconds of global reference time sources. Essential for logs, authentication, and security systems.
OpenVPN	An open-source VPN framework that uses SSL/TLS encryption to create secure tunnels between clients and servers, protecting network traffic from interception.
Packet sniffing	The act of capturing network packets for analysis. Legitimate for troubleshooting or intrusion detection; malicious when used to intercept credentials or private data. We did demos of `tcpdump` and WireShark.
Pastebin	A web service for sharing text or code snippets publicly. Attackers sometimes use it to post stolen data or command instructions.
Phishing	A social engineering attack that uses fake messages or websites to trick users into revealing credentials or installing malware.
ping	Sends ICMP echo requests to test network reachability and measure latency. A quick way to confirm if a host is alive.
Proxmox	An open-source virtualization platform that manages virtual machines, containers, and storage through a web interface. Often used for home labs or small data centers.
Proxy (forward & reverse)	A forward proxy acts on behalf of clients to access external resources (for privacy or caching). A reverse proxy sits in front of servers, handling requests and routing them to internal services (for load balancing or security).
REST (Representational State Transfer)	An architectural style for designing web APIs. It treats data as resources identified by URLs and manipulated using standard HTTP verbs (GET, POST, PUT, DELETE).
RPi (Raspberry Pi)	A credit-card-sized computer that runs Linux, used for education, prototyping, and IoT. It exposes GPIO pins for hardware projects.
Sawing off your tree branch	An idiom describing self-inflicted outages—such as cutting off your own remote access by misconfiguring a firewall or deleting critical permissions.
SIEM (Security Information and Event Management)	Centralizes and correlates logs from many systems to detect suspicious activity and generate security alerts.
SQL (Structured Query Language)	A domain-specific language used to manage and query relational databases through operations like SELECT, INSERT, UPDATE, and DELETE.
SQLite	A small, self-contained SQL database stored in a single file. Common in mobile apps, IoT, and lightweight servers.
ssh (Secure Shell)	A cryptographic network protocol for securely accessing and managing remote systems. Replaces insecure tools like telnet and rsh.
Switch ("sw" on network design whiteboard)	A Layer 2 device that forwards Ethernet frames between devices on the same network based on MAC addresses, enabling efficient local communication.
Symmetric encryption	Uses one shared key for both encryption and decryption. Fast and efficient, but requires secure key exchange between parties.

Syncthing	A peer-to-peer file synchronization tool that keeps folders consistent across devices without centralized cloud storage, using encrypted connections.
Tailscale	A mesh VPN built on WireGuard that automatically connects devices under a single private network, using identity-based access control.
tcpdump	A command-line tool for capturing and analyzing network traffic at the packet level. Often used for diagnostics or security auditing.
telnet	An early remote terminal protocol that transmits data in plaintext. Deprecated due to lack of encryption but still useful for simple network tests.
traceroute, mtr	Utilities that map the path packets take through routers to a destination. `mtr` combines `ping` and `traceroute` into a continuous, real-time view.
TTL (Time To Live)	A counter in IP packets that limits their lifespan. Each router reduces it by one to prevent loops and stale data. DNS records also have a TTL field on each record, which limits the amount of time that a resolver can cache the response.
Tunnel	Encapsulates one network protocol inside another, often encrypted, to securely pass private data through public networks.
URL / URI (Uniform Resource Locator / Identifier)	A URI identifies a resource; a URL specifies where to find it. Example: https://example.com/file.txt is both a URI and a URL.
Virtual machine (VM)	A commercial OpenVPN client with advanced configuration management, used for secure remote access.
VLAN (Virtual Local Area Network)	Logically segments a physical network into separate broadcast domains, improving security and organization without extra hardware.
WireGuard	A modern, high-performance VPN protocol using state-of-the-art cryptography. Simpler and faster than IPsec or OpenVPN.
Wireshark	A GUI packet analyzer that decodes thousands of protocols, letting users inspect network conversations in detail.
Yubikey	A hardware security token that stores cryptographic keys and provides strong two-factor authentication for logins and encryption systems.

Revision #2
Created 2025-11-03 15:33:27 UTC by Michael Barrow
Updated 2025-11-03 18:43:44 UTC by Michael Barrow