Security: Attack, Entailment (attack vectors), Controls (protection, attack prevention) (SAEC)

Security or protection

- Environmental (popularly known as physical)
- Human businesses
- Commercial and enterprise-related activities
- Computing, Internet, Web and Attached-applications

Definition of terms (DOT)

- (General) The state of being free from danger or injury
  - Human being, properties and assets
- (Computing) A system that enforces boundaries between computers and networks.
- Supervisory Control and Data Acquisition (SCADA) are generally used to control dispersed assets using centralized data acquisition and supervisory control.
- Distributed Control Systems (DCS) are generally used to control production systems within a local area such as a factory using supervisory and regulatory control.

DOT continuation

- Programmable Logic Controller (PLCs) are generally used for discrete control for specific applications and generally provide regulatory control. Allow the automation of electromechanical processes such as those used to control machinery on factory assembly lines, amusement rides, or centrifuges for separating nuclear material.
- Attack (computing)
  - IETF, RFC 2828: An assault on system security that derives from an intelligent threat, i.e., an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.
  - US, CNSS Instruction No. 4009 dated 26 April 2010: Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.

DOT continuation

- Attack
  - US, CNSS Instruction No. 4009, led to term like cyberattack: An attack, via cyberspace, targeting an enterprise’s use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.
- Risk
  - ISO 31000: The 'effect of uncertainty on objectives'
- Vulnerability a weakness which allows an attacker to reduce a system's information assurance.
  - IETF, RFC 2828: A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.

DOT continuation

- Vulnerability
  - ISO 27005: A weakness of an asset or group of assets that can be exploited by one or more threats where an asset is anything that has value to the organization, its business operations and their continuity, including information resources that support the organization's mission.
  - NIST SP800-30: A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.
  - Open Group: The probability that threat capability exceeds the ability to resist the threat.

Definition of terms continuation

- Vulnerability
  - Common application (people, hazards et al): Refers to the inability to withstand the effects of a hostile environment. A **window of vulnerability** (WoV) is a time frame within which defensive measures are reduced, compromised or lacking.

Environmental security

- Infrastructure
- Food
- Airport
- School
- Shopping

. . . And so on

Human businesses

- What are you up to now?

Commercial and enterprise-related activities

- Homeland (military)
- Human security (political)
- Financial (monetary)
- Inter/national (political)
- Public (political)

Computing

- Computers
- Smartphones
- Embedded
- Networks
- IT as business facility
- Digital equipment, others

Internet

- Connectivity of computing-related equipment.
- Transmission of data.
- Underlying TCP/IP suites′ applications or services.

Web

- Browsing
- Games (ad hoc or web-based)
- Applications (computing-attached)
  - Productivity suites
  - Marketing and business-related engagement through social networking
- Services

Businesses and operations in CLASSED

- Air and space navigation

- Manufacturing
- Banking
- Power / nuclear
- Water storage dam

- Maritime and ports

Space control systems

- Spacecraft reaction control systems are used:
  - for attitude control during re-entry;
  - for stationkeeping in orbit;
  - For close maneuvering during docking procedures;
  - for control of orientation, or 'pointing the nose' of the craft;
  - as a backup means of deorbiting;
  - as ullage motors to prime the fuel system for a main engine burn.
- Spaceshuttle 1981 uses Intel 80386.

Air traffic control

- Main radio transmitter
- Flight progress monitor
- Runway lights activator
- Telephone systems

Nuclear security

- Physical protection
- Nuclear safety
- Material accounting and control

Water storage dam

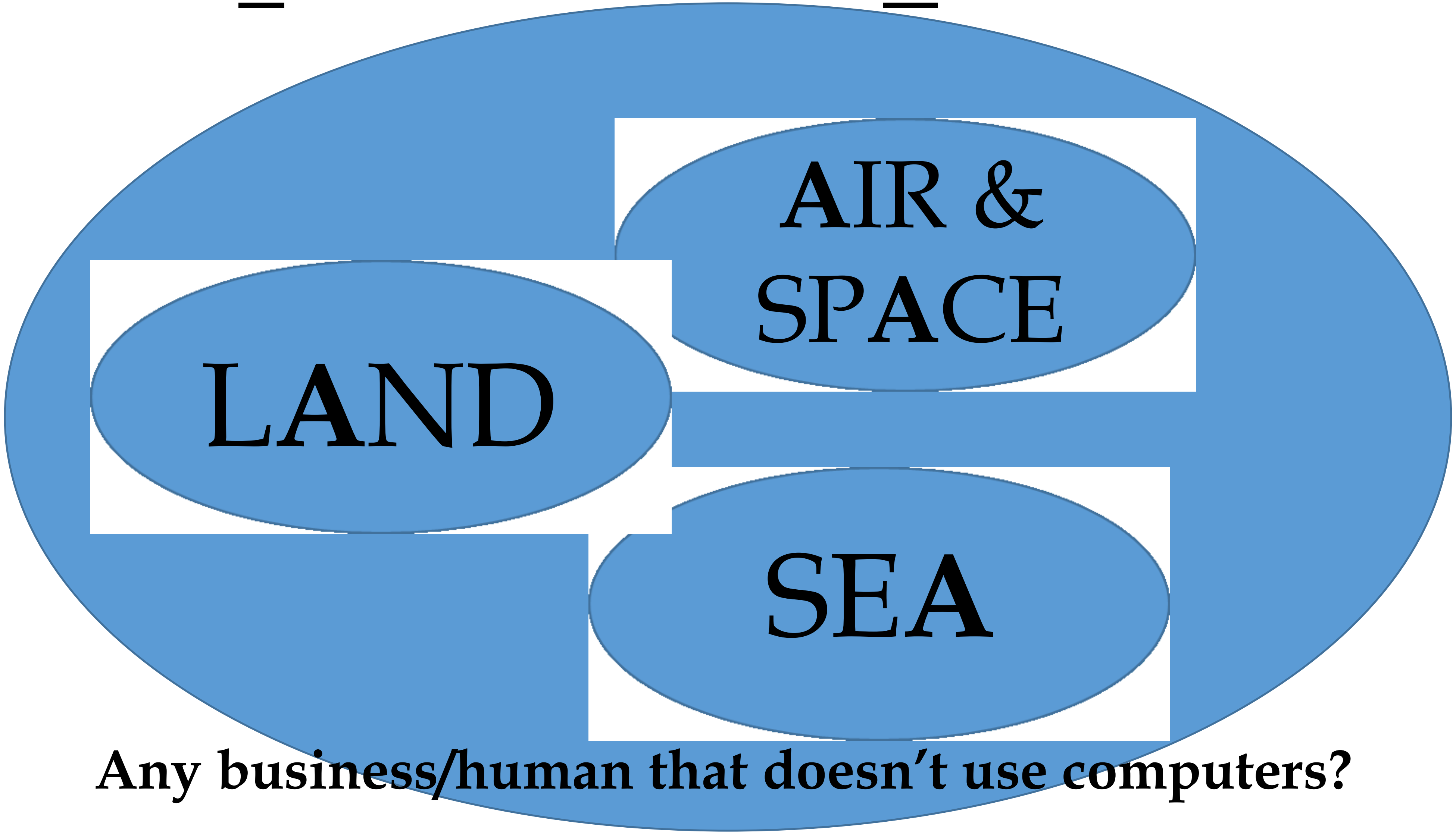
- Microwave towers
- Communications i.e. Ethernet, PSTN

Industrial control systems

- Supervisory Control and Data Acquisition (SCADA)
- Distributed Control Systems (DCS)
- Programmable Logic Controllers (PLC)

- These are typically used in industries such as electric, water and wastewater, oil and natural gas, transportation, chemical, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (e.g., automotive, aerospace, and durable goods).

CLASS environmental domains



AIR & SPACE

LAND

SEA

Any business/human that doesn’t use computers?

Cyberconnected Land, Air, Sea, Space Environmental Domains

Security practices incidents

- Vulnerability scanner
- Penetration testing

Security attack

- Can be
  - Passive, attempts to learn or make use of information from the system but does not affect system resources. (e.g. see wiretapping.)
  - Active, attempts to alter system resources or affect their operation.
- Can be perpetrated by
  - Inside attack, initiated by an entity inside the security perimeter (an "insider"), i.e., an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization.
  - Outside attack, initiated from outside the perimeter, by an unauthorized or illegitimate user of the system (an "outsider"). In the Internet, potential outside attackers range from amateur pranksters to organized criminals, international terrorists, and hostile governments.

Attack types

PASSIVE	ACTIVE
Network: Wiretapping, Port scanner, Idle port scan	**Denial of Service**: Ping flood, Ping of death, Smurf (not the Smurfs),
	Spoofing
	Network: Man in the middle (MITM), Address resolution protocol (ARP)
	Host: Overflow (buffer, heap, stack), Format string

Security risk

- The potential of losing something of value.
  - Values (such as physical health, social status, emotional well being or financial wealth) can be gained or lost when taking risk resulting from a given action, activity and/or inaction, foreseen or unforeseen.
- Any event that could result in the compromise of organizational assets i.e. the unauthorized use, loss, damage, disclosure or modification of organizational assets for the profit, personal interest or political interests of individuals, groups or other entities constitutes a compromise of the asset, and includes the risk of harm to people.

Risk practice areas include

- **Economic risk**
- Health
- Health, safety, and environment
- **Information technology and systems-related**
- Insurance
- **Business and management**
- **In human services**
- High reliability organizations (HROs)
- Finance
- **Security**
- **Human factors**
- Maintenance

Security risk and vulnerability

- Caveat: Risk and vulnerability are distinctive and have different meanings.
- A security risk may be classified as a vulnerability.
  - Vulnerabilities without risk: for example when the affected asset has no value to someone and/or organization.
- A security risk is tied to the potential of a significant loss.

0-day attack

- Exploits a previously unknown vulnerability in a computer application or operating system, one that developers have not had time to address and patch.
- The programmer has had zero days to fix the flaw (in other words, a patch is not available).
- It is common for individuals or companies who discover zero-day attacks to sell them to government agencies for use in cyberwarfare.

Entailment (attack vectors)

- Malware writers exploit zero-day vulnerabilities.
- E-mail attachments, which exploit vulnerabilities in the application i.e. email clients and servers.
- Various computing files and applications exploit to compromise systems or software that are vulnerable to steal confidential data i.e.
    - Bank accounts,
    - Personally identifiable information (PII),
    - Personal health information (PHI),
    - Personal financial information (PFI).

Entailment (attack vectors) continuation

- Reverse engineering can be used to "crack" software and media to remove their copy protection or to create a (possibly improved) copy or even a knockoff—usually the goal of a competitor analysis.
- Social engineering is psychological manipulation of people into performing actions or divulging confidential information.
  - Based on specific attributes of human decision-making known as cognitive biases.

Reverse engineering, common situation

- Reverse engineering of machines
- Reverse engineering of software
    - Binary software
        - Binary software techniques
    - Software classification
- Source code
- Reverse engineering of protocols
- Reverse engineering of integrated circuits/smart cards
- Reverse engineering for military applications
- Overlap with patent law

Social engineering, cognitive biases

- Bugs in the human hardware, exploited in various combinations to create attack techniques.
- Techniques
  - Pretexting
  - Diversion theft
  - Phishing
    - IVR or phone phishing
  - Baiting
  - Quid pro quo
  - Tailgating
  - Shoulder Surfing

Advance Persistent Threats (APT)

- A set of stealthy and continuous computer hacking processes, often orchestrated by human(s) targeting a specific entity. APT usually targets organizations and/or nations for business or political motives.
- Its processes require a high degree of covertness over a long period of time.
- The "**advanced**" process signifies sophisticated techniques using malware to exploit vulnerabilities in systems.
- The "**persistent**" process suggests that an external command and control system is continuously monitoring and extracting data from a specific target.
- The "**threat**" process indicates human involvement in orchestrating the attack.

APT continuation

- It usually refers to a group, such as a government, with both the capability and the intent to target, persistently and effectively, a specific entity.
- A technique in Internet-enabled espionage using a variety of intelligence gathering techniques to access sensitive information, but applies equally to other threats such as that of traditional espionage or attacks.
- Placing a custom malicious code on one or multiple computers for specific tasks and to remain undetected for the longest possible period.

APT posits

- *Advanced* – Operators behind the threat have a full spectrum of intelligence-gathering techniques at their disposal. These may include computer intrusion technologies and techniques, but also extend to conventional intelligence-gathering techniques such as telephone-interception technologies and satellite imaging. While individual components of the attack may not be classed as particularly "advanced" (e.g. malware components generated from commonly available do-it-yourself malware construction kits, or the use of easily procured exploit materials), their operators can typically access and develop more advanced tools as required. They often combine multiple targeting methods, tools, and techniques in order to reach and compromise their target and maintain access to it. Operators may also demonstrate a deliberate focus on operational security that differentiates them from "less advanced" threats.

APT posits continuation

- *Persistent* – Operators give priority to a specific task, rather than opportunistically seeking information for financial or other gain. This distinction implies that the attackers are guided by external entities. The targeting is conducted through continuous monitoring and interaction in order to achieve the defined objectives. It does not mean a barrage of constant attacks and malware updates. In fact, a "low-and-slow" approach is usually more successful. If the operator loses access to their target they usually will reattempt access, and most often, successfully. One of the operator's goals is to maintain long-term access to the target, in contrast to threats who only need access to execute a specific task.

APT posits continuation

- *Threat* – APTs are a threat because they have both capability and intent. APT attacks are executed by coordinated human actions, rather than by mindless and automated pieces of code. The operators have a specific objective and are skilled, motivated, organized and well funded.

APT recognized attack vectors

- Infected media,
- Supply chain compromise, and
- Social engineering.

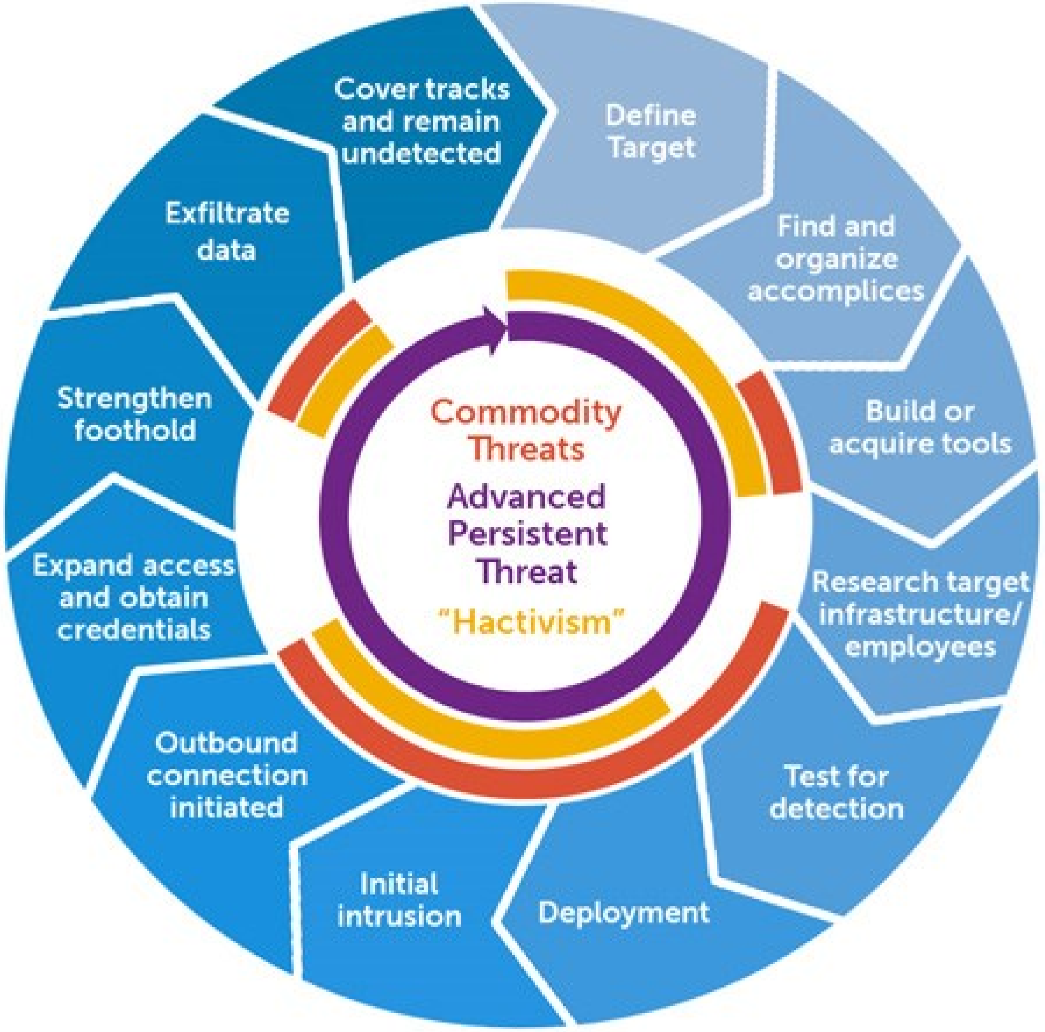
APT incursion

- Socially-engineered emails dropping trojans to exfiltrate sensitive information.
- Stuxnet computer worm.
  - Targeted the computer hardware of Iran's nuclear program.

APT criteria (by Bodmer, Kilger, Carpenter and Jones)

- Objectives – The end goal of the threat, your adversary.
- Timeliness – The time spent probing and accessing your system.
- Resources – The level of knowledge and tools used in the event (skills and methods will weigh on this point).
- Risk tolerance – The extent the threat will go to remain undetected.
- Skills and methods – The tools and techniques used throughout the event.
- Actions – The precise actions of a threat or numerous threats.
- Attack origination points – The number of points where the event originated.
- Numbers involved in the attack – How many internal and external systems were involved in the event, and how many people's systems have different influence/importance weights.
- Knowledge source – The ability to discern any information regarding any of the specific threats through online information gathering (you might be surprised by what you can find by being a little proactive).

APT lifecycle


Define Target
Find and organize accomplices
Build or acquire tools
Research target infrastructure/ employees
Test for detection
Deployment
Initial intrusion
Outbound connection initiated
Expand access and obtain credentials
Strengthen foothold
Exfiltrate data
Cover tracks and remain undetected
Commodity Threats
Advanced Persistent Threat
"Hactivism"

APT -> Stuxnet

- Stuxnet was designed to industrial programmable logic controller (see definition of terms).
- Exploiting four zero-day flaws, Stuxnet functions by targeting machines using the Microsoft Windows operating system and networks, then seeking out Siemens Step7 software.
- Causing the fast-spinning centrifuges to tear themselves apart.
    - It reportedly ruined almost one-fifth of Iran's nuclear centrifuges.
- Its design and architecture are not domain-specific and it could be tailored as a platform for attacking modern SCADA and PLC systems (e.g. in the automobile or power plants), the majority of which reside in Europe, Japan and the US.

Stuxnet 3 modules

- Worm, executes all routines related to the main payload of the attack;
- Link file, automatically executes the propagated copies of the worm; and
- Rootkit, component responsible for hiding all malicious files and processes, preventing detection of the presence of Stuxnet.

Stuxnet on Iran’s nuclear centrifuges

- Was typically introduced to the target environment via an infected USB flash drive.
- The worm then propagates across the network, scanning for Siemens Step7 software on computers controlling a PLC.
- In the absence of both criteria, Stuxnet becomes dormant inside the computer.
- If both the conditions are fulfilled, Stuxnet introduces the infected rootkit onto the PLC and Step7 software, modifying the codes and giving unexpected commands to the PLC while returning a loop of normal operations system values feedback to the users.

Security technologies or controls (protection, attack prevention mechanisms)

- Access control and permission policy
- Firewall
- Intrusion Detection Prevention Systems (ID|PS)
- Anti-virus
- Computing Events Monitoring and Management
- DDoS Protection
- Cryptography, data protection
- Human’s motherwit.

Firewall technology and architecture

TECHNOLOGY	ARCHITECTURE
Packet filter (1G)	Filtering routers
Stateful packet inspection (2G)	Dual homed
Application level, proxying (3G)	Bastion/screened host
Application, user and content-specific (NG)	Screened subnet / DMZ

Firewall technology

- First Generation (1G)
- Act by inspecting the "packets" which are transferred between computers on the Internet. If a packet matches the packet filter's set of rules, the packet filter will drop (silently discard) the packet or reject it (discard it, and send "error responses" to the source).
- This type of packet filtering pays no attention to whether a packet is part of an existing stream of traffic (i.e. it stores no information on connection "state").
- Filters each packet based only on information contained in the packet itself (most commonly using a combination of the packet's source and destination address, its protocol, and, for TCP and UDP traffic, the port number).
- Work mainly on the first three layers of the OSI reference model, which means most of the work is done between the network and physical layers, with a little bit of peeking into the transport layer to figure out source and destination port numbers.

OpenBSD pf

- **Macros:**User-defined variables that can hold IP addresses, interface names, etc.
- **Tables:**A structure used to hold lists of IP addresses.
- **Options:**Various options to control how PF works.
- **Queueing:**Provides bandwidth control and packet prioritization.
- **Filter Rules:** Allows the selective filtering or blocking of packets as they pass through any of the interfaces.

Stateful packet inspection

- Second Generation (2G)
- Keeps track of the state of network connections (such as TCP streams, UDP communication) traveling across it.
- Is programmed to distinguish legitimate packets for different types of connections.
- Packets matching, a known active connection will be allowed by the firewall; others will be rejected.
- Packet filtering alone is not regarded as providing enough protection.

Application-level proxying

- Third Generation (3G)
- Controls input, output, and/or access from, to, or by an application or service.
- It operates by monitoring and potentially blocking the input, output, or system service calls which do not meet the configured policy of the firewall.
- Built to control all network traffic on any OSI layer up to the application layer.
- Controls applications or services specifically, unlike a stateful network firewall which is - without additional software - unable to control network traffic regarding a specific application.

Application, user and content-specific

- Next Generation (NG)
- Enforces network security policies based on
  - Applications - identifies and classifies traffic by application, regardless of port, protocol, encryption, or evasive tactics.
  - Users - match applications and specific users to your enablement policies.
  - Content - stop both known and unknown threats with proprietary mechanisms, which sandboxes analysis to identify and block, especially, unknown threats.

Filtering routers

- Regulate transmission of packets based upon the protocol, address, and/or port identifier.
- *Application gateways* filter traffic using application-specific rules.
- *Circuit gateways* act as a TCP relay; an external remote host connects to a TCP port at the gateway and the gateway, in turn, establishes a TCP connection to the intended destination on the internal local network.

Filtering routers continuation

- *Direction*: Whether this rule is being used to filter an inbound or outbound packet, from the perspective of the router.
- *Action*: Whether this rule is being used to allow or block a particular packet type.
- *Protocol*: The protocol to which this rule applies (IP, TCP, UDP, or ICMP).

Filtering routers continuation

- *Address/Port Information*: An optional source and/or destination IP address (*from/to*) to identify the relevant hosts, and an optional source and/or destination port address (*source/destination*) to identify the application to which this rule applies.
- *Flags*: Used here to indicate whether this rule pertains to a TCP virtual circuit that is being initiated with this packet or to a TCP connection that has already been established (*estab*). This can usually be determined by examining the setting of the Flags field in the TCP segment Header. In particular, the Acknowledgement (ACK) flag is used to indicate whether the Acknowledgement Number in this segment is valid or not; it is usually set except in the first segment used for connection establishment. The Reset (RST) flag is used to force an immediate termination of a TCP connection. For filtering purposes, a TCP connection is considered to be established if the ACK or RST flag is set.

Dual homing

- An Ethernet device that has more than one network interface, for redundancy purposes, or in firewall technology, dual-homed is one of the firewall architectures for implementing preventive security.
- A computer that has separate network connections to two networks.
- Isolates two (or more for multihoming) networks from each other whilst retaining the ability to see traffic on these different networks.
- Enables services through proxy.

Bastion/screened host

- A special purpose computer on a network specifically designed and configured to withstand attacks.
- Adds an additional layer of security to the dual homed host architecture.

Screened subnet / demilitarized zone

- Provides a perimeter network and additional screening router to the screened host architecture.
  - Reduces the impact of the screened host being compromised.
- Enables security from external attacks, but it typically has no bearing on internal attacks such as sniffing communication via a packet analyzer or spoofing such as e-mail spoofing.