D4 Data and Ethics

Autumn 2022 | Lecture 2 - Part II

Focus: Information security & cybersecurity | Author: Prof. Dr. Petra Maria Asprion | FHNW

Agenda

Part I -- Intro: data & more	→ SD1
Part II -- From Yesterday to Today	→ SD2
Part III -- Organization Layer: preconditions	→ SD3
Part IV -- Organization Layer: GRC & Management	→ SD4
Coaching Session #2	→ SD5

→ SD = Slide Deck

Yesterday ---

With more usage, of the Internet it needs more security!

This learning took place very early ...

1930' Mainframes

- **Computer security** began immediately after the first mainframes* were developed
- Mainly mathematicians and physicists developed **code-breaking computations** during World War II
- They quickly figured out that not only **physical controls** were needed to limit access to authorized personnel to sensitive military locations
- Only rudimentary controls were available to defend against everything **--- physical theft, espionage,** and **sabotage**

Howard Aiken with Mark I in 1944. Bettmann / Getty Images

* By most measures, the first mainframe computer was the Harvard Mark I. Developed **starting in the 1930s**, the machine was not ready for use until 1943. It weighed five tons, filled an entire room and cost about $200,000 to build – which is something like $3,070,500 in 2020 dollars.

Have a look: https://www.thoughtco.com/howard-aiken-and-grace-hopper-4078389

Source: https://www.ifsecglobal.com/cyber-security/a-history-of-information-security/

Excurse I – Howard Aiken

- Howard Aiken (1900-1973) was a mathematician who invented **Mark I,** a forerunner of the modern electronic digital computer
- Aiken began work in 1939 on an **automatic calculating machine** that could perform any selected sequence of five arithmetical operations (addition, subtraction, multiplication, division, and reference to previous results) without human intervention. The first such machine, the **Mark I**, was completed by Aiken and his partners in February 1944
- The Mark I was programmed to solve problems by means of a paper tape on which coded instructions were punched. Once so programmed, the calculator could be operated by persons with little training.
- The Mark I was used by the U.S. Navy for work in gunnery, ballistics, and design. Continuing his work, Aiken completed an improved all-electric Mark II in 1947. He also authored numerous articles on electronics, switching theory, and data processing.

Howard Aiken (person in the middle) with Mark I

Source: www.britannica.com/biography/Howard-Aiken

Excurse II – Grace Hopper

- Grace Hopper (1906-1992) studied at Vassar College and Yale before she joined the Naval Reserve in 1943. In 1944, she started working with Aiken on the Harvard **Mark I** computer.
- One of Hopper's lesser-known claims to fame is that she was responsible for coining the term "**bug**" to describe a computer fault. The original bug was a moth that caused a hardware fault in the Mark II. Hopper got rid of it and fixed the problem and was the first person to "**debug**" a computer.
- She began research for the Eckert-Mauchly Computer Corporation in 1949 where she designed an improved compiler and was part of the team which developed **Flow-Matic, the first English-language data processing compiler**. She invented the language **APT** and verified the language **COBOL**.
- Hopper was the first computer science "Man of the Year" in 1969, and she received the National Medal of Technology in 1991. She died a year later, in 1992, in Arlington, Virginia.

Lieutenant (junior grade) Grace Hopper working at Harvard in 1946. Should would later become a rear admiral in the Navy. U.S. Department of Defense / public domain

Source: https://www.thoughtco.com/howard-aiken-and-grace-hopper-4078389

Enigma* 1930/40

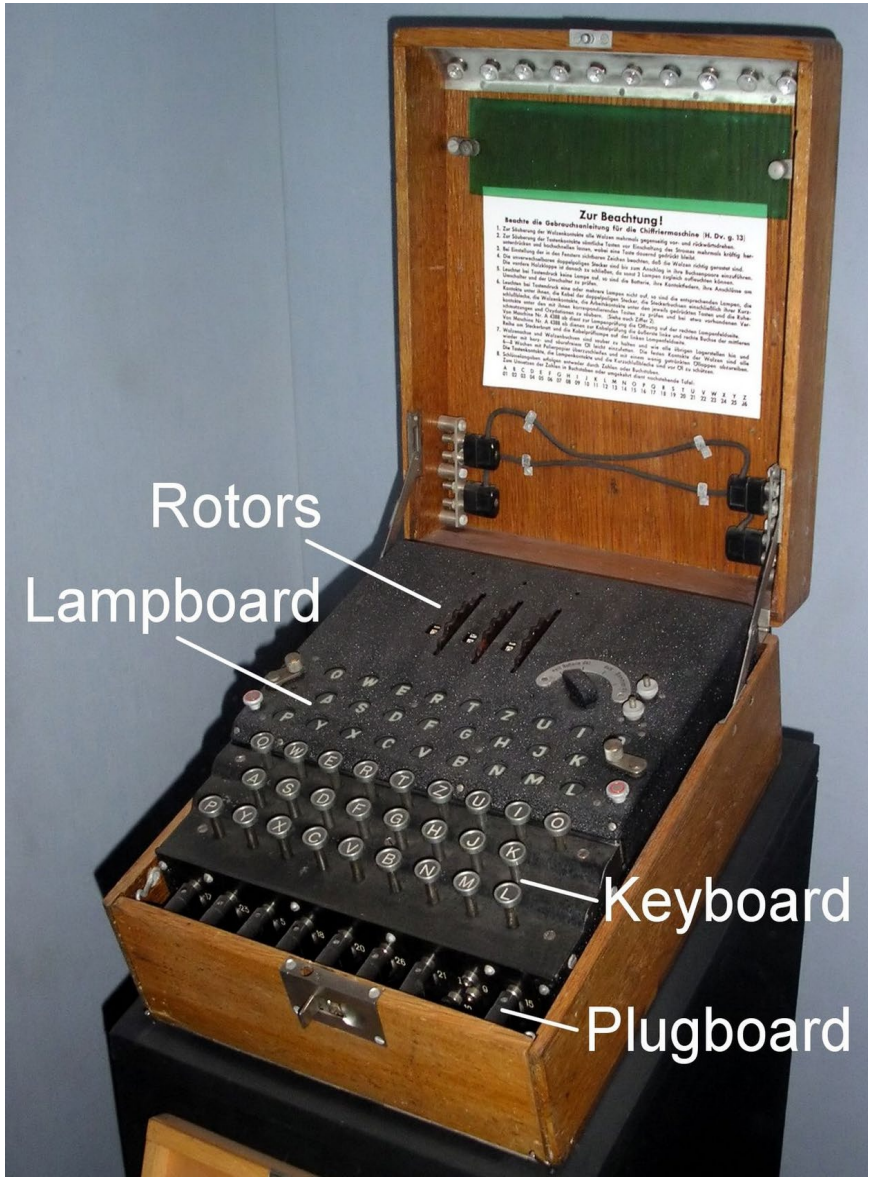
The Encryption Machine

Have a Look:

https://www.youtube.com/watch?v=mXZNayEPFKc (3:05 min)

How the Enigma works https://www.youtube.com/watch?v=G2_Q9FoD-oQ (11.51)

* from greek αἴνιγμα ‚Rätsel'/ Puzzle



Source. https://www.britannica.com/topic/Enigma-German-code-device

Enigma, device used by the German military command to encode strategic messages before and during World War II.

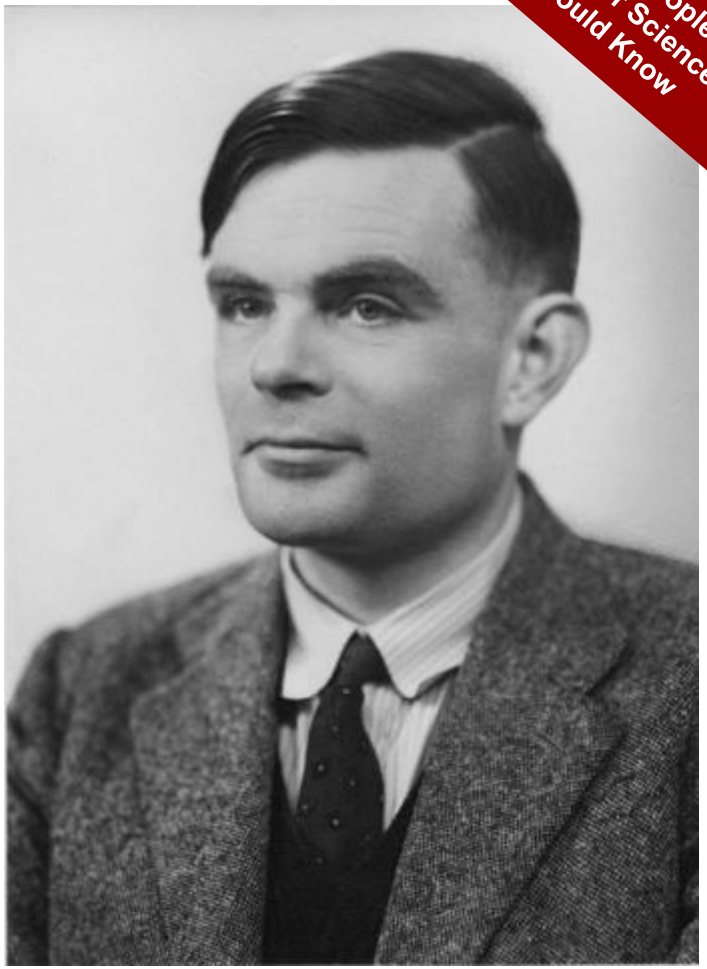
The number of permutations of settings available to the encoders made the Enigma code difficult to break. The operator set the machine's rotating wheels and plugboard to different predetermined positions according to daily orders, regularly changing the cipher.

Historians generally agree that the reading of secret messages sent by the German using Enigma machines shortened the war by at least two years, saved thousands of lives and deprived the Germans the time they needed to develop an atomic bomb," Perera said (Dec. 8, 2020)

Excurse III - Alan Turing

- Alan Turing was a brilliant mathematician. Born in London in 1912, he studied at both Cambridge and Princeton universities. He was already working part-time for the British Government's Code and Cypher School before the Second World War broke out. In 1939, Turing took up a full-time role at Bletchley Park in Buckinghamshire – where top secret work was carried out to decipher the military codes used by Germany and its allies.

- **Enigma and the Bombe**
  The main focus of Turing's work was in cracking the 'Enigma' code. He played a key role in this, inventing – along with fellow code-breaker Gordon Welchman – a machine known as the Bombe. This device helped to significantly reduce the work of the code-breakers. From mid-1940, German Air Force signals were being read at Bletchley and the intelligence gained from them was helping the war effort.



Alan Turing - © National Portrait Gallery

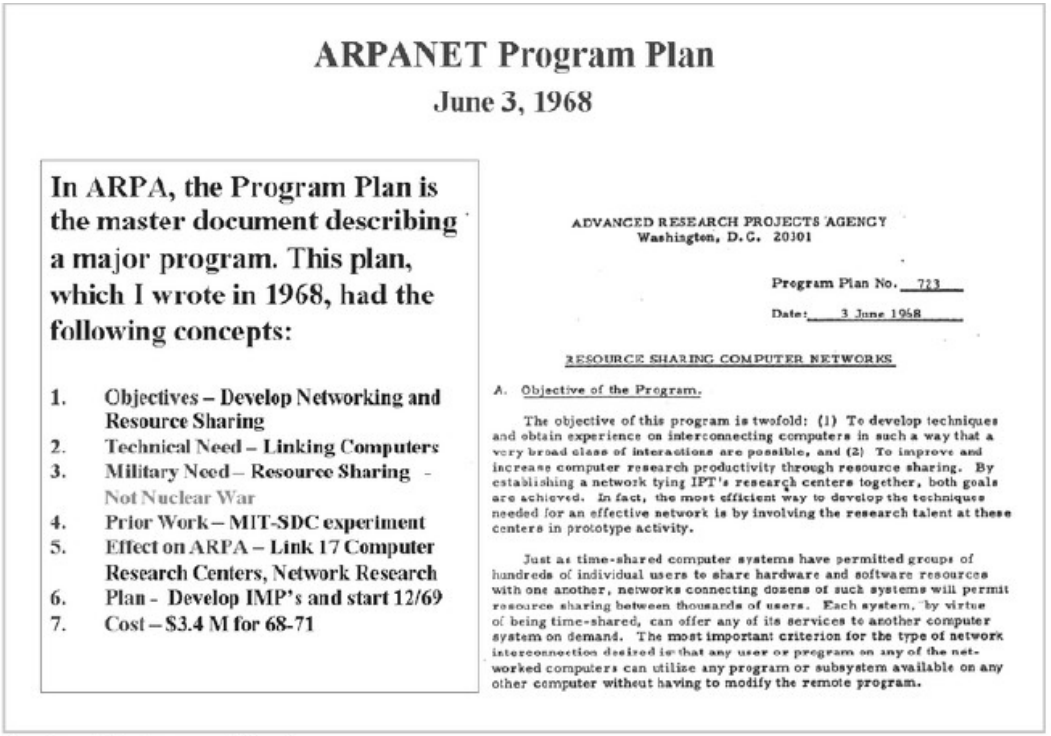
Note: **The Imitation Game**
The Imitation Game is a 2014 American historical drama film directed by Morten Tyldum and written by Graham Moore, based on the 1983 biography Alan Turing: The Enigma by Andrew Hodges.

Sources. https://www.thoughtco.com/howard-aiken-and-grace-hopper-4078389
https://www.iwm.org.uk/history/how-alan-turing-cracked-the-enigma-code

ARPANET 1968

- U.S. Department of Defence's **A**dvanced **R**esearch **P**roject **A**gency (ARPA) began researching the feasibility of a redundant networked communication …
- A researcher, Bob Thomas, created a computer program which was able to move ARPANET's network, leaving a small trail wherever it went. He named the program 'CREEPER', because of the printed message that was left when travelling across the network:

'I'M THE CREEPER: CATCH ME IF YOU CAN'.



ARPANET Program Plan

June 3, 1968

In ARPA, the Program Plan is the master document describing a major program. This plan, which I wrote in 1968, had the following concepts:

1. Objectives – Develop Networking and Resource Sharing
2. Technical Need – Linking Computers
3. Military Need – Resource Sharing - Not Nuclear War
4. Prior Work – MIT-SDC experiment
5. Effect on ARPA – Link 17 Computer Research Centers, Network Research
6. Plan - Develop IMP's and start 12/69
7. Cost – $3.4 M for 68-71

ADVANCED RESEARCH PROJECTS AGENCY
Washington, D.C. 20301

Program Plan No. 723

Date: 3 June 1968

RESOURCE SHARING COMPUTER NETWORKS

A. Objective of the Program.

The objective of this program is twofold: (1) To develop techniques and obtain experience on interconnecting computers in such a way that a very broad class of interactions are possible, and (2) To improve and increase computer research productivity through resource sharing. By establishing a network tying IPT's research centers together, both goals are achieved. In fact, the most efficient way to develop the techniques needed for an effective network is by involving the research talent at these centers in prototype activity.

Just as time-shared computer systems have permitted groups of hundreds of individual users to share hardware and software resources with one another, networks connecting dozens of such systems will permit resource sharing between thousands of users. Each system, by virtue of being time-shared, can offer any of its services to another computer system on demand. The most important criterion for the type of network interconnection desired is that any user or program on any of the networked computers can utilize any program or subsystem available on any other computer without having to modify the remote program.

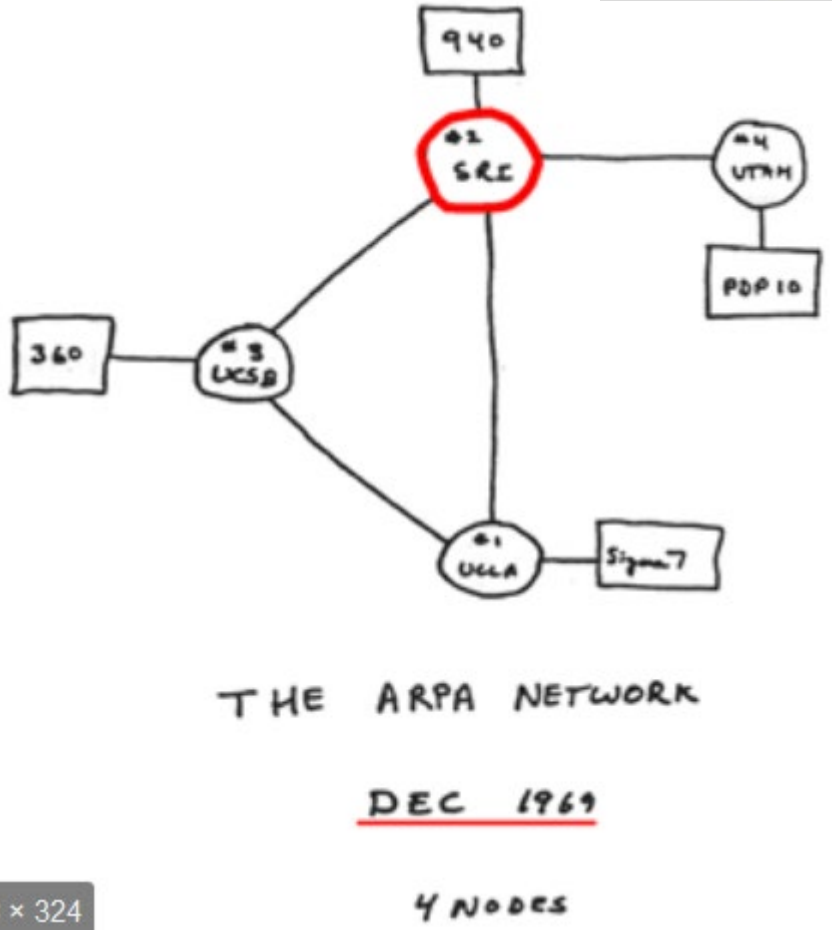
Courtesy of Dr. Lawrence Roberts

FIGURE 1-2 ARPANET Program Plan[4]

Source. http://walden-family.com/bbn/arpanet-completion-report.pdf

ARPANET development 1970-1980

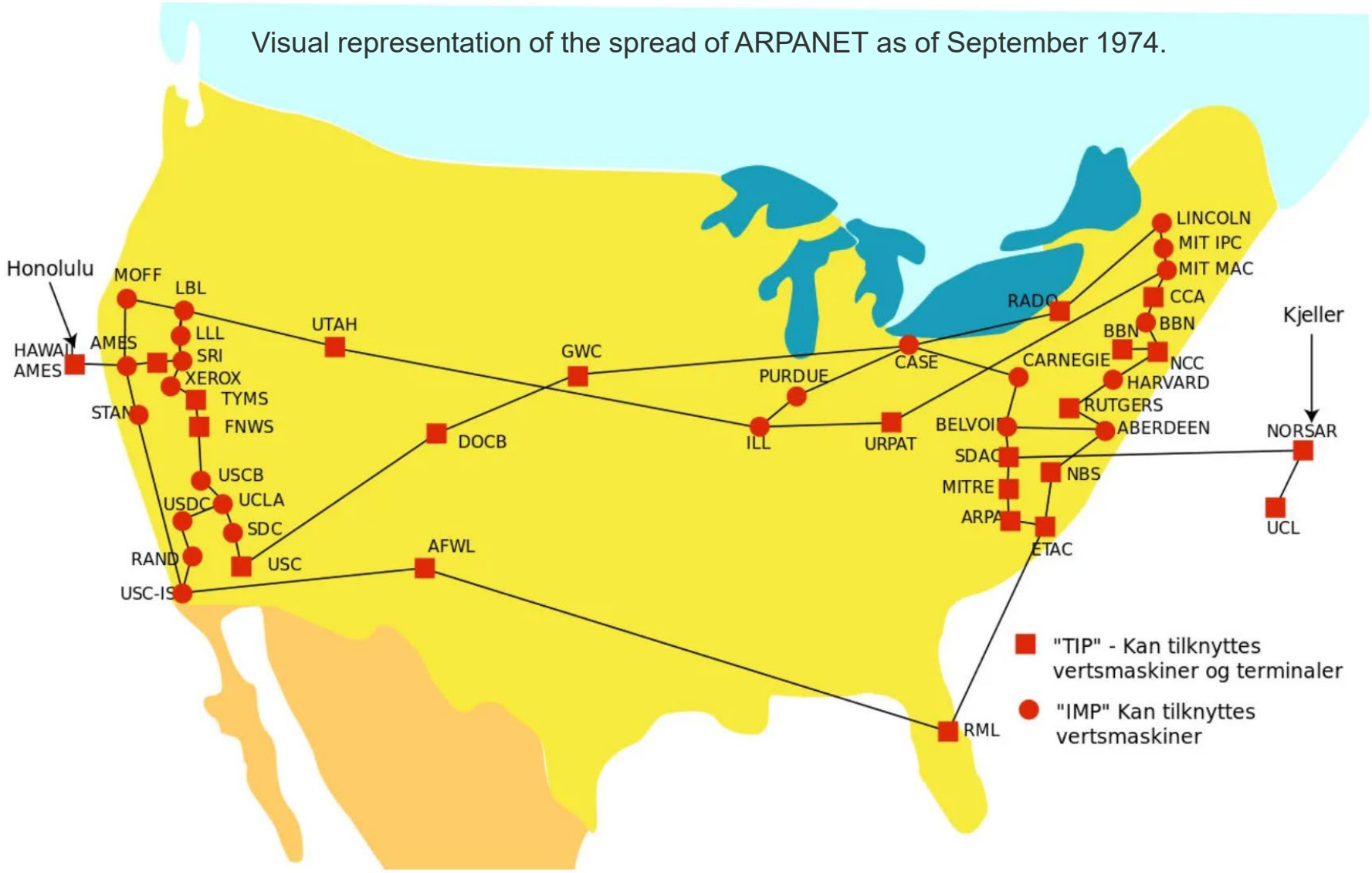
- ARPANET was the first wide-area packet-switched network with distributed control and one of the first networks to implement the TCP/IP protocol suite. Both technologies became the technical foundation of the Internet.
- The popularity of ARPANET grew and with it its potential for misuse
- Fundamental problems with ARPANET security were identified
- User identification and authorization to the system were non-existent
- In the late 1970s the microprocessor expanded computing capabilities and security threats



28 × 324

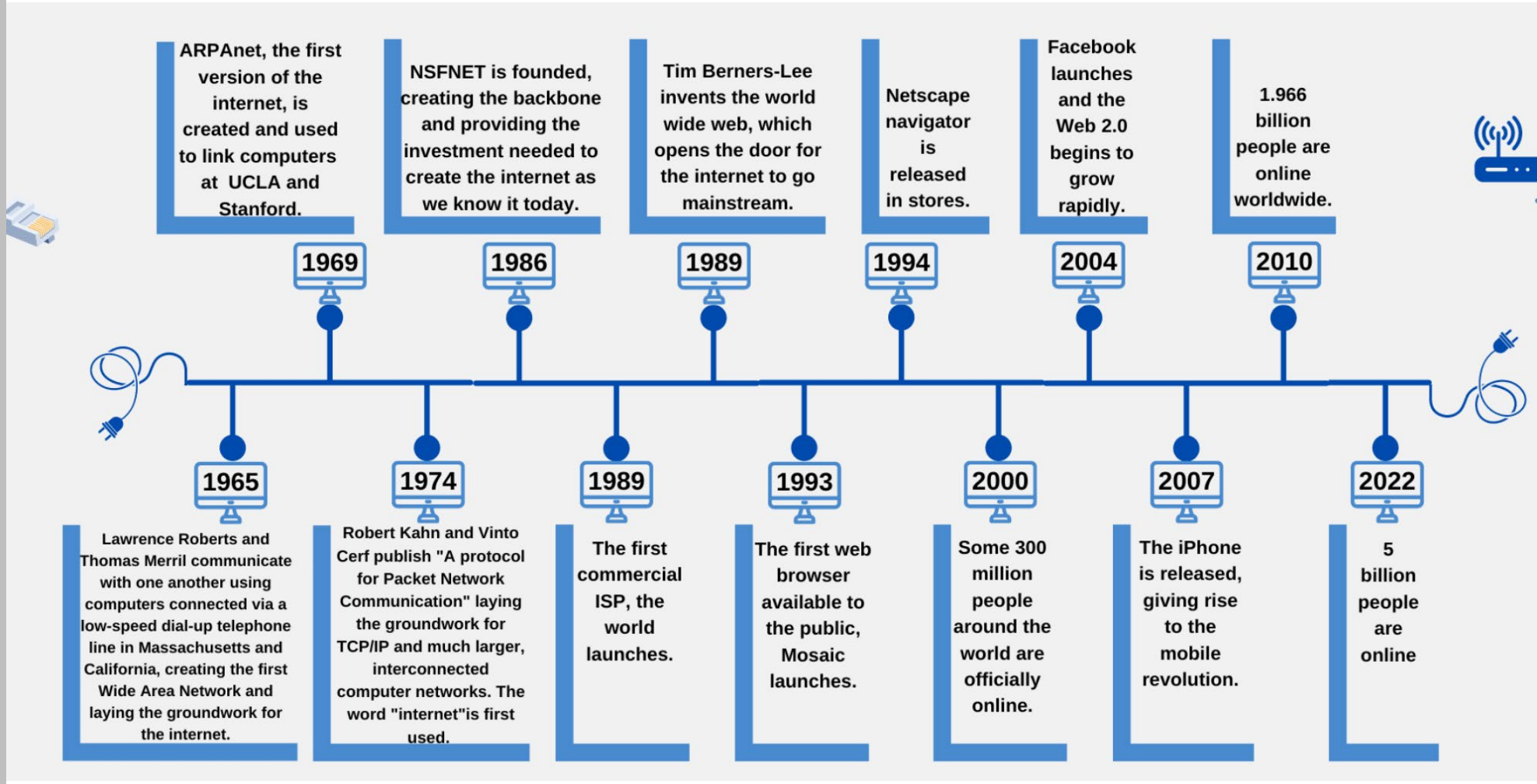
Have a look: https://www.youtube.com/watch?v=nsdFNTeGqIg

ARPANET spread in 1974



https://www.britannica.com/biography/J-C-R-Licklider

The Internet in a timeline …



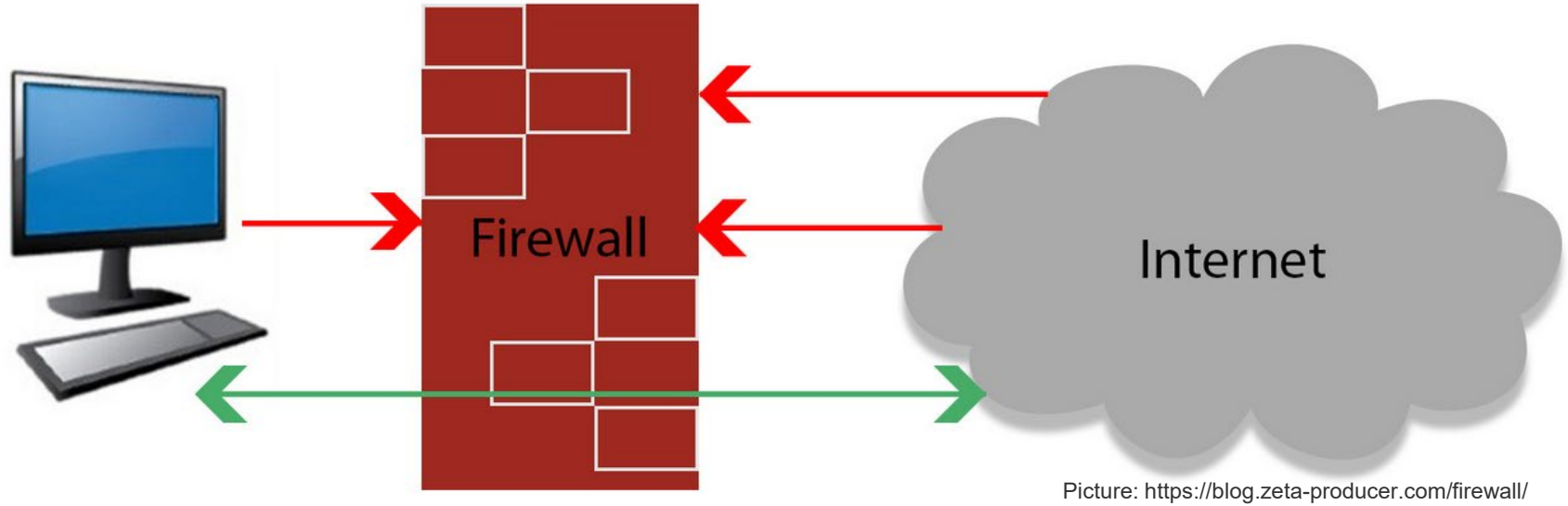
Source. https://www.broadbandsearch.net/blog/who-invented-the-internet-full-history

Interesting Links: https://www.internethalloffame.org/internet-history/timeline
Have a look: https://www.scienceandmediamuseum.org.uk/objects-and-stories/short-history-internet

The 1990

- By the late 80's, network usage was expanding rapidly. Universities, militaries, and governments were connecting. Computer worms (predecessors to viruses) came into fruition ...
- In the 90s, networks of computers became more common resulted on the **Internet** - the first manifestation of a global network and an **anarchic place**.
- Also in the 90s, with the early Internet deployments, **security was treated as a low priority**.
- By the middle of the 90s, network security threats had increased exponentially and, as such, **firewalls** and **antivirus programs** had to be produced. A NASA researcher gets the credit for the creation of the first firewall program design. Their research center in California was attacked by a computer virus in 1988. This spurred them to design a virtual **firewall**.
- Essentially, **routers** were the strength behind the design. The routers separated the network into smaller units so that an attack would not have the ability to destroy the complete system.

A Firewall



Picture: https://blog.zeta-producer.com/firewall/

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

Firewalls have been **a first line of defense in network security for over 25 years**. They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet.

A firewall can be hardware, software, software-as-a service (SaaS), public cloud, or private cloud (virtual).

Source. https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html
Have a look: CISCO Video (1:42) https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

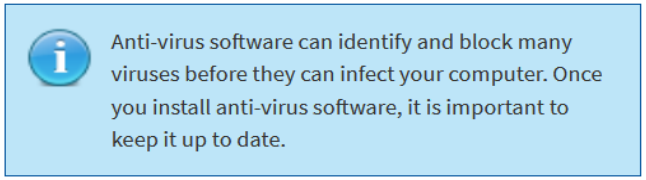
Anti-virus Software (1/2)

Although details may vary between packages, anti-virus software scans files or your computer's memory **for certain patterns** that may indicate the presence of malicious software (i.e., malware).

Anti-virus software (sometimes more broadly referred to as anti-malware software) looks for patterns based on the signatures or definitions of known malware.

Anti-virus vendors find new and updated malware daily, so it is important that you have the latest updates installed on your computer.

Once you have installed an anti-virus package, you should scan your entire computer periodically.



Automatic scans – Most anti-virus software can be configured to automatically scan specific files or directories in real time and prompt you at set intervals to perform complete scans.

Manual scans – If your anti-virus software does not automatically scan new files, you should manually scan files and media you receive from an outside source before opening them.

Source. https://www.cisa.gov/uscert/ncas/tips/ST04-005

Anti-virus Approach (2/2)

Defining "**Virus**" - A computer virus is a type of malware. It's a code or program designed to covertly enter a device. Then, when the device runs the virus's code, the virus replicates itself within a device and transmits itself to other devices.
The replicating virus can slow down the device and cause it to crash. Users may also see a large number of emails being sent from their accounts that they did not send. This is the virus spreading itself to other devices.

Anti-virus software is a type of security software designed to protect users from multiple types of malware, not just viruses.

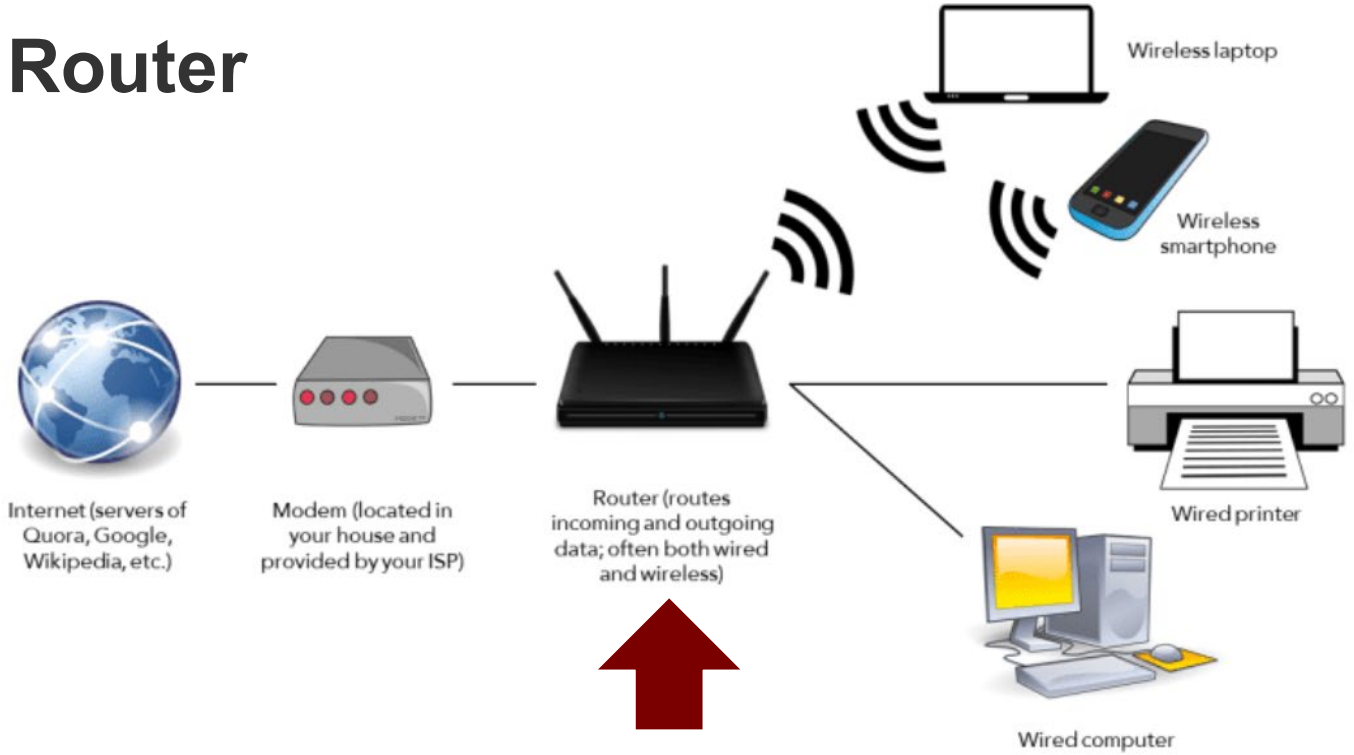
The software is a **risk management tool** that scans devices regularly and on-demand for known malware and suspicious behavior associated with malware. Antimalware software is similar to antivirus software but tends to be more specific to the malware it defends against.

When malware is detected by antivirus software, the user will be alerted to the threat and the malware will be deleted.

Sometimes the antivirus will ask the user first before deletion. Asking first is a useful attribute when the detection of malware is a false positive, which is a possibility when the antivirus uses certain detection techniques.

Source. https://www.sdxcentral.com/security/definitions/what-is-antivirus-software-definition/

A Router



Picture:https://www.hellotech.com/blog/what-is-the-difference-between-a-router-and-a-modem

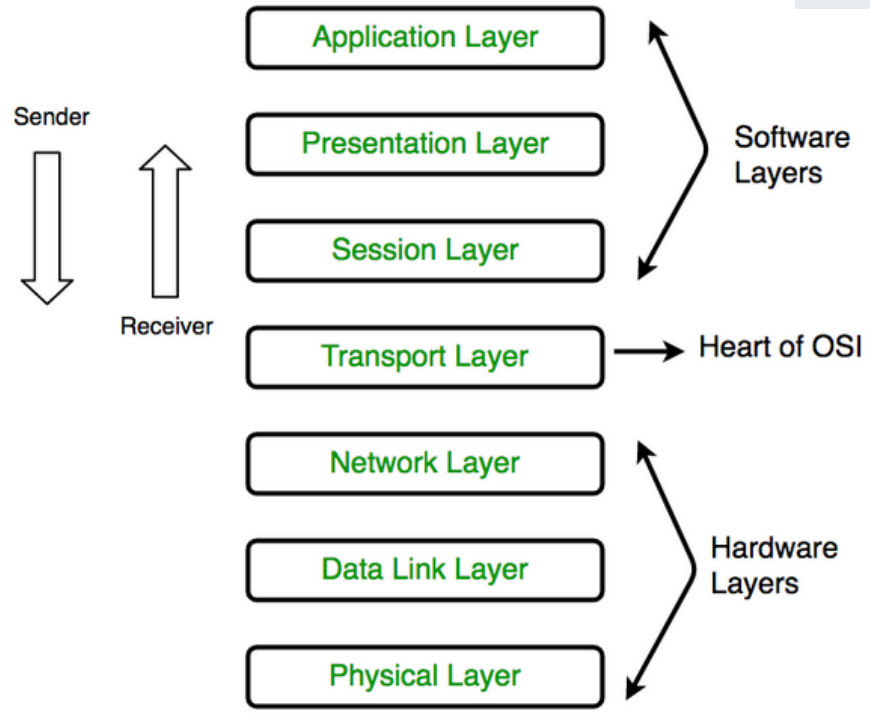
A router is a network device that connects different computer networks by routing packets from one network to the other. This device is usually connected to two or more different networks.
When a data packet comes to a router port, the router reads the address information in the packet to determine out which port the packet will be sent (e.g. a router provides you with the internet access by connecting your LAN with the Internet).

A router is considered a **Layer 3 device** of the **OSI model** because its primary forwarding decision is based on the information of the OSI Layer 3 (the destination IP address). If two hosts from different networks want to communicate with each other, they will need a router between them.

Source. https://geek-university.com/what-is-a-router/

1984: The OSI model (1/2)

7 Layer OSI/ISO reference model



Picture: https://www.geeksforgeeks.org/layers-of-osi-model/

OSI stands for

→ Open Systems Interconnection

It has been developed by ISO – the '**International Organization for Standardization**', in 1984.

It is a 7 layer architecture with each layer having specific functionality to perform.
All these 7 layers work collaboratively to transmit the data from one person to another across the globe.

Why It Matters
Standardizing communication across a network, including external networks (e.g., the cloud internet), facilitates communication regardless of where data is sent or from where it is received. The OSI Model enables manufacturers to create their own protocols and equipment standards while allowing for interconnectivity with other manufacturers.

Source. https://www.geeksforgeeks.org/layers-of-osi-model
https://www.iso.org/ics/35.100/x/

The OSI/ISO reference model (2/2)

Detailed view

OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example		Central Device/ Protocols		DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management		**User Applications** SMTP	GATEWAY Can be used on all layers	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**		JPEG/ASCII EBDIC/TIFF/GIF PICT		
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		**Logical Ports** RPC/SQL/NFS NetBIOS names		
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING	TCP/SPX/UDP		Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP		Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch Bridge WAP** PPP/SLIP	Land Based Layers	Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**		

Picture: https://blogs.cisco.com/cloud/an-osi-model-for-cloud

Source. https://blogs.cisco.com/cloud/an-osi-model-for-cloud
Recommended to read: https://www.proofpoint.com/us/threat-reference/osi-model

Today ---

With more usage, it needs more security!

This learning took place very early ...

Today ---

With more usage, more data needs secured!

it's all about (digital) data ...

DATA IS THE NEW GOLD

HOW CHEMISTRY 4.0 IS CHANGING WORK EFFICIENCY

Mark C… n: "Data is the new gold

…logy companies are constantly innovating. Credit Suisse supports them
…of ways, including its unique networking platform, the Credit Suisse Pri
Company Summit

…the structural shift toward more enriching online experiences
…ique networking platform – the Credit Suisse Private Internet
…redit Suisse brought together technology-focused entrepren

Data Analytics: The New Gold Standard In Drug Value

Data analytics is moving from a nice-to-have add-on to a foundation of strategic thinking

EUROPEAN BUSINESS REVIEW

Data is the new gold. This is how it can benefit everyone – while harming no one

COVID-19 has dealt the world a twin crisis. We face not only our greatest global health shock but also our greatest economic shock in a century

PharmaSUG 2021 - Paper RW-160

Patient Registries – New Gold Standard for Real World Data

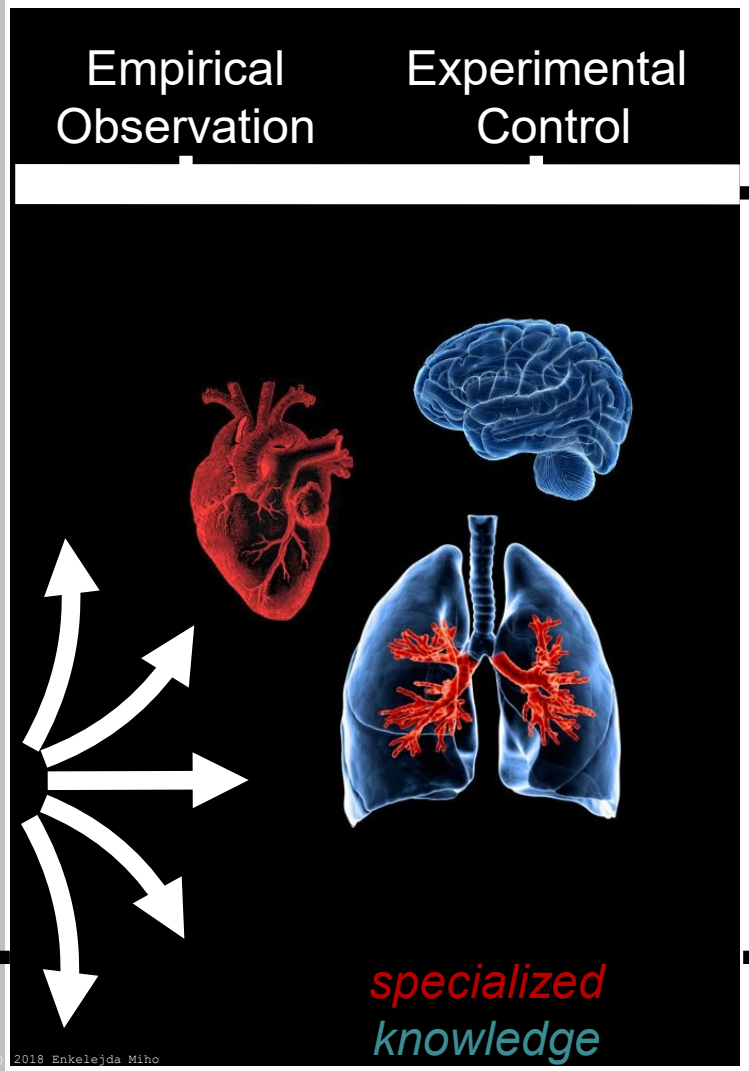
Neha Srivastava; Lavanya Peddibhotla; Sivasankar Konda, Covance by Labcorp

Deloitte.

Data is the new gold

The future of real estate service providers

Real World Data – The new Gold



Digital Information

2018

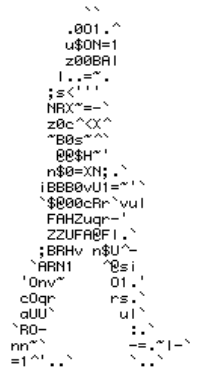
Tomorrow

?

Social

Molecular

Phenotypic



Diagnostic

Treatment

artificial intelligence

integrated intelligence

Grimberg F., Asprion P.M., Schneider B., et al. (2021). The Real-World Data Challenges Radar: A Review on the Challenges and Risks regarding the Use of Real-World Data. June 2021. Digital Biomarkers 5(2):148-157. DOI: 10.1159/000516178

Conclusion

Data becomes a valuable commodity

**Data must be professionally protected --
confidentiality, integrity and accessibility are now a must!**

What have we discussed so far?

A little bit of history – to become a security freak at some point

Important personalities who founded the discipline

The beginnings of the internet – without security thoughts

Respond to security threats - Firewall, Antivirus, Router

Standardizing communication: The 7 Layer OSI/ISO reference Model

And one of the most important trigger ...

Data the new gold!

And needs to be secured …