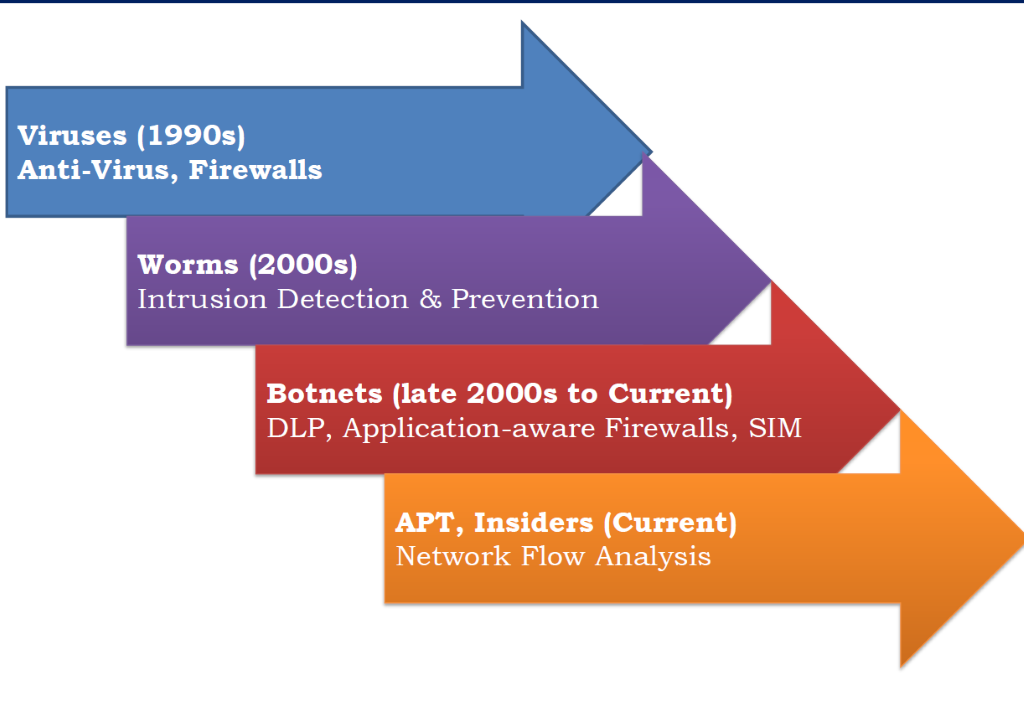
**Evolution of cyber security**



**The birth of the first computer virus**

The first computer virus was born because of an innocent mishap. If we look at the early 1970s, BBN Technologies engineer Bob Thomas, created a code which would result in an easy movement of the program between computer systems that were connected by ARPANET, the foundation version of the internet. The program code had no intention to cause any harm, but it displayed a funny message, “I’m the Creeper: Catch me if you can!” In response, Bob Thomas’ friend Ray Tomlinson (inventor of email) coded an advanced version of the program that can duplicate itself on the connected computer systems. Now, this program called Reaper, would delete Bob Thomas’ original program and copy itself on it. The war between the Creeper and Reaper was a significant moment in the history of cybersecurity.

**Cybersecurity acts**

The three main cybersecurity regulations are the 1996 [Health Insurance Portability and Accountability Act](https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act) (HIPAA), the 1999 [Gramm-Leach-Bliley Act](https://en.wikipedia.org/wiki/Gramm-Leach-Bliley_Act), and the 2002 [Homeland Security Act](https://en.wikipedia.org/wiki/Homeland_Security_Act), which included the [Federal Information Security Management Act](https://en.wikipedia.org/wiki/Federal_Information_Security_Management_Act) (FISMA).

**Cascade virus**

The **Cascade virus** (also known as **Herbstlaub** in Germany) is a prominent [computer virus](https://en.wikipedia.org/wiki/Computer_virus) that was a resident written in [assembly language](https://en.wikipedia.org/wiki/Assembly_language) that was widespread in the 1980s and early 1990s. It infected.[COM files](https://en.wikipedia.org/wiki/COM_file) and had the effect of making text on the screen fall (or cascade) down and form a heap at the bottom of the screen. It was notable for using an [encryption](https://en.wikipedia.org/wiki/Encryption) algorithm to avoid being detected. However, one could see that infected files had their size increased by 1701 or 1704 bytes. In response, [IBM](https://en.wikipedia.org/wiki/IBM) developed its own [antivirus software](https://en.wikipedia.org/wiki/Antivirus_software).

**Buffer overflow/ Buffer overrun**

Buffers are areas of memory set aside to hold data, often while moving it from one section of a program to another, or between programs. Buffer overflows can often be triggered by malformed inputs; if one assumes all inputs will be smaller than a certain size and the buffer is created to be that size, then an anomalous transaction that produces more data could cause it to write past the end of the buffer. If this overwrites adjacent data or executable code, this may result in erratic program behaviour, including memory access errors, incorrect results, and [crashes](https://en.wikipedia.org/wiki/Crash_(computing)).