CS23MTECH11026 - Asg 2

Task 1: “Reflection on Trusting Trust” by Ken Thompson

In this paper, Ken Thompson presents simple code snippets and scenarios that a programmer can include in the source code (some software, programs, etc.) such that it affects the system's security, which leads to the conclusion that “ trusting the people who wrote the program is more important than trusting some statement verifying that this program is free from viruses, worms, etc.” A programmer can do this in 3 stages.

1.) Self-reproducing program - creating a source code that, when compiled and executed, produces output the same as the source code. It has two properties. (i) It can be written in any programming language. (ii) the main functional program can include additional unnecessary elements, which are also outputted as source code is compiled and executed.

2.) Learning phase (independent of the system) - even if some new character / unprintable character (other than once which the compiler already knows, like newline, tab, format changer, etc.) is inserted in that self-reproducing program, the recompilation happens, and the compiler learns or perpetuates the knowledge. Learn once and use later.

3.) Using it for malicious activity - modifying the source code into some bugged source code (which does some malicious action). The bugged machine-level code, generated after compilation, is used, and the bug from the source code is removed so that detection becomes hard because there is no trace of a bug in the source code.

All the above stages can be done in any programming language and at the source program, assembler, loader, or hardware level. As we get near the hardware, it gets even harder to trace the bug. Hence, we cannot trust the program that we did not completely create.

Task 2: Designing the Internet by David D Clark (Talks at Google)

The National Science Foundation funded a project called "Future Internet Architecture," which inspired the book "Designing the Internet." In this talk, David D Clark talked about this book. Initially, the focus was on making technical stuff work, like getting protocols to function correctly in the 1970s. TCP, a protocol for communication between different systems, took about two years to become manageable.

Fast forward to the 1980s, and David D Clark chaired the Internet Activity Board. The first protocol David was into is BGP (Border Gateway protocol). To handle system scaling, they used hierarchy, and the only way they knew back then. Thus, made routing, BGP, iBGP, DNS, etc, in the hierarchy. Also, video streaming was done, but it was not deployed back then due to its economic viability.

The 1990s got messy when the National Science Foundation decided to commercialize the internet, leading to the end of NSFNET. They tried to improve service quality with protocols like DiffServ and IntServ, but because of the competitive interface, the Internet Service Providers (ISPs) were not willing to spend a lot of money to help others make money.

For the internet to last, it needed to adapt to changes. Flexibility and adaptability became essential. They also thought about security but not perfectly. Security had four main problems: people trusting third parties, attacks during service connections, the internet's inherent flaws, and denial-of-service attacks.

Security isn't a straightforward fix it involves confidentiality, integrity, and availability. The availability part needed more attention. In conclusion, the Internet is the general platform to carry packets, and applications can be built on top of it. Designing the internet is more about the requirements, not just technical but also about the economic viability, network management, longevity of the Internet, security, and political factors to keep evolving and successful.

Task 3: Online Black Markets: An Investigation of a Digital Infrastructure in the Dark

The paper is about investigating and functioning of online black markets (OBMs) operating on the Darknet. The authors did that by analyzing the same thing (dynamics of interactions among actors and marketplace technologies) over the years.

OBMs (Online Black Markets) are websites where people, without revealing their identities, can buy and sell illegal goods and services. These platforms use technologies created by communities to design, build, and keep them running. Researchers identified the three mechanisms on which OBMs operate despite facing challenges such as police raids, scams, and market breakdowns. Those key mechanisms are Commoditization, Platformization, and Resilience.

Commoditization: The structure of the OBMs marketplace is similar to the conventional OMs i.e. transform illegal goods and services into standardized products with clear descriptions, ratings, and reviews, making them easier to buy and sell.

Platformization: Platforms that connect buyers and sellers, providing essential features like escrow services and communication tools.

Resilience: When something goes wrong the user community hold up and find new ways to keep going their business. Thus the ability to bounce back and work even after the setbacks is called resilience.

The first OBM marketplace, SilkRoad, was established in January 2011 and operated for 33 months. It was the first e-commerce platform organized within the Tor network for clients seeking to purchase goods anonymously. SilkRoad's success shaped the structure of OBMs marketplaces, which now resemble the actual e-commerce websites with escrow functions, and cryptocurrency payments. To build trust between vendors and buyers, the buyers are called to rate the vendors. PGP keys were used to build their reputation while remaining anonymous.

The offer includes product descriptions, customer rankings, accepted payment systems, and escrow mechanisms for secure exchanges. OBMs marketplaces use similar logic that of legitimate e-commerce sites, with product descriptions, shipping information, and payment systems (we can see the example of the credit card given in the paper). Trust is central in OBMs marketplaces, with buyers encouraged to rate vendors so that trust is build. The exit scam happens when the grown business stops delivering the orders but will continue to accept payments for new order.

After the seizure of the Silk Road there were other 122 online black market were emerged and 9 of them were closed by LEAs and other 42 were closed by admins through exit scam.
The Silk Road seizure did not halt vendors' activities, as they migrated to new marketplaces using encrypted signatures. The Silk Road was not an exit scam, and hence, the reputation of vendors remained intact, and trust in the infrastructure was not lost.

Enterprise like IITH can implement the cybersecurity measures such as firewall, antivirus software and encryption to protect their data. To spread awareness about the strong password practice, strict access control etc. Regular backups of important data should be taken, and employees should be trained to identify and report suspicious activities. Basic Cybersecurity education should be take by an individual and enterprise member to ge some awareness so that in future some bad thing happens, they can protect themselves.