**Assignment - 2**

**-Yug Patel**

**CS23MTECH14019**

#### (1) Summary of "Reflections on Trusting Trust" by Ken Thompson

The paper "Reflections on Trusting Trust" by Ken Thompson discusses a concept known as the "Trusting Trust" attack. "Trusting Trust" is the potential risk of trusting software you have not coded and are using as the foundation for your software. Ken explained three steps to modify a C compiler binary to insert a backdoor, spyware, or any form of malicious behaviour when compiling the UNIX login command code while at the same time leaving no traces in the source code [**(Cox)**](#_x31jwvlfi06o).

In the paper, Ken described a three-stage method for how trojan horses can be pumped into software that might remain undetectable for a long period. Consider a compromised compiler—let's call it compiler A—that includes subtle modifications that introduce a backdoor into the compiled output under certain conditions. Compiler A can compile programs, including itself, and it may insert backdoors based on specific conditions. If the modification detects that the program being compiled is Compiler-A itself, it includes the backdoor. The compiled programs, including Compiler-A with its modifications, are distributed to other systems. When these programs are executed on other systems, they may contain the modified version of Compiler-A, creating a chain of untrust. [**(“How it works”)**](#_x31jwvlfi06o)

In summary, the paper says that if the compiler is compromised, then it compromises all the software it compiles, including itself. So, it should be taken as a serious crime and must have the same social stigma as breaking into a neighbour's house, whether locked or unlocked.

#### (2) Summary of how the Internet (including its security) was designed by watching a YouTube talk by David D. Clark

#### 

The Google talk is given by David Clark who is a computer scientist at MIT. Throughout the talk, he discussed the different pillars of networking and internet security, upon which he wrote his book "Designing the Internet". He Broadly talked about the following main topics from his book personal history, economics, longevity, network management, and security. Speaking about today's internet he mentioned how early works in the field focused research only on short-term internet and the whole research community was sucked into it as everything was wrong with it, thankful to the national science foundation's project "Future Internet Architecture" with the aim of how the internet would look down 15-20 years' late. It turned out to be the stepping stone to what the internet today is.

Brushing up his personal history he recalled the decades from the 1970s to 1990s, from having little knowledge and working in building protocols in 1070's, adding hierarchy to everything known in the 1980s as it was the best reflex thing to do at that time to shaping the industry structure in 1990's. It is a long journey that the internet today has taken.

Economics on the Internet popped up as not every requirement is technical. It focuses on designing the architecture/ protocol that is viable for the industry. While mentioning economics, he mentioned that the way internet service provider looks the way they do is the internet protocol was specified the way it was.

For the Internet to be successful, the protocol must age long. Flexibility and adaptability are the key ingredients to longevity. As one may observe even if something is perfectly fine today, changes in the requirements over time change everything. Also equally important is the stability, stability of IP which allows innovators to sit on top of it. He outlines 27 different ways in which a system can be designed so it survives longer. Network Management is something that the networking community wants to kind of neglect. He referred to it as a technical area where they have screwed up.

Talking about security he mentioned that security was a thing that was being thought from the very beginning but not in the right way, the way it was supposed to be. Security is not the dimension that you optimize and it is perfectly fine. It is a multi-dimensional space where different observations compete. It is important to build a secure internet, to build a secure internet means building a compromise that allows for a solution to survive. But the thing is the whole essence of the internet is that no one oversees it. He emphasized how the focus of security people on Confidentiality/ Disclosure Control and Integrity has screwed up the Availability. Because availability is not something that can be fixed by sprinkling crypto on it. He took this stand by giving an example of a security system without plan b, that leaves the user dead is equivalent to a 100% successful security attack along the dimension of security. Lastly, he talked about the idea of being attacked, which portrays that the misbehaviour in today's web is not due to bad implementation; it's because of deliberate design decisions.

In summary, the entire talk focused on how the internet was then and how it got shaped the way it is today passing through a sequence of re-engineering steps of specification and technical changes.

#### (3) Summary on Paper “Online Black-Markets: An Investigation of a Digital Infrastructure in the Dark”

The paper "Online Black-Markets: An Investigation of a Digital Infrastructure in the Dark" describes the world of Online Black-Markets (OBM) Infrastructure, broadly talking about its three identified generative mechanisms commoditization, platformization, and resilience. These mechanism work on the building blocks of structural elements and result in events (observational). They simultaneously interact to enable infrastructure operations whereas individual mechanism fails to produce this outcome independently

**Overview of Online Marketplace (OMs)**

An online marketplace (or online e-commerce marketplace) is a type of e-commerce website where product or service information is provided by multiple third parties. In an online marketplace, consumer transactions are processed by the marketplace operator and then delivered and fulfilled by the participating retailers or wholesalers’ technologies [**(“Online marketplace”)**](#_x31jwvlfi06o). The reach of OMs has expanded because to social media's growing popularity.

**Overview of Online Black Market (OBMs)**

Online Black Markets (OBMs), sometimes called darknet marketplaces or cryptomarkets in scholarly literature, constitute a sociotechnical structure involving systems, individuals, and organizations. OBMs consist of covert marketplaces connecting buyers and vendors engaged in the illicit exchange of products and services. These transactions leverage technologies like cryptocurrencies, the Tor network, and other anonymizing services to ensure confidentiality. OBMs are created, implemented, maintained, and adopted by collaborative online communities. The transaction herein happens via decentralized systems like cryptocurrencies and public key infrastructure or some third-party services like escrow. Here the actors are involved using distributed discussion systems such as IRC and USENET. These tools are utilised in conjunction with blogs and online forums like reddit.com

**What makes OBMs different from OMs?**

OBM marketplace structures are largely like those of traditional, enabling vendors and buyers to meet and trade. What makes the OBMs different is the risk. The risk is accentuated in OBMs, given the lack of transparency, law enforcement control, legal protection, and centralized governance. Despite these risks, data suggests that the illegal commodities trade is flourishing online and successfully supporting both suppliers and customers.

**Generative Mechanisms of OBMs**

1. Commoditization: Commoditization is described as a process in which the infrastructure of Online Black Markets (OBMs) empowers vendors to establish their reputation and ensures transaction security through decentralized controls. Successful transactions attract a significant number of users, encouraging the exchange of a wider range of products and services. It leads to sales and interaction.

2. Platformization: OBMs act as platforms where new digital goods and services, like malware or datasets for phishing, are developed and traded. Marketplaces evolve to meet the needs of the criminal community, often incorporating new features and technologies [**(“Platformization”)**](#_x31jwvlfi06o). It includes Site establishment, Market offering, and Morphing.

3. Resilience: Refers to the response to sudden and unpredictable changes in the infrastructure, including law enforcement raids or exit scams that occur inside the organization. They morph their technologies and schemes in response to these challenges, often leading to innovations that are more mature and decentralized removing the central point of control like peer-to-peer markets i.e. openbazaar. It include Exit scam and Police raids.

**A Black-Market Service mentioned in the paper: Stolen Credit Card Data & Exit Scam**

The paper mentions a lot of marketplaces some of which include the Silk Road being the first of its kind, sheepMarket, DarkMarket, Evolution, AlphaBay, Hansa, and Evolution. It describes a prevalent service in OBMs, the sale of stolen credit card data. Marketplaces like SilkRoad provided a structure like conventional e-commerce platforms, where vendors could list stolen credit card details along with information like the card number, CVV, expiry date, name, address, and sometimes phone numbers. A usual offer includes an image showcasing the products, ratings from customers to evaluate the vendor, accepted payment methods, and a secure escrow system for a safe transaction. Payment for these illegal goods is typically made using cryptocurrencies, and transactions are conducted anonymously. To build trust, buyers rate vendors, and marketplaces often implement escrow services, in which money is withheld until the buyer certifies that the items have been received.

An exit scam occurs when an established business stops shipping orders while continuing to receive payments for new orders. Exit scams are common in OBMs. The paper mentions two such kinds performed by SheepMarket and EvolutionThe operator of SheepMarket, a marketplace that had been up and running since February 2013, carried out an exit scam in November 2013 and stole $6 million in Bitcoin. The Evolution marketplace was shut down in March 2015 when the administrator carried out an exit scam and stole the whole escrow fund, which was believed to be worth $12 million in Bitcoin. Furthermore, because Evolution was the second-largest marketplace at the time, the Evolution hoax caused a significant disruption.

**Countermeasures for cyberattacks** [**(“Countermeasures for Cyber Attacks”)**](#_x31jwvlfi06o)

To counteract cybercrime, individuals, and enterprises can implement the following measures:

1. Enhanced Cybersecurity Practices: Regularly update security protocols and software to protect against new forms of malware and hacking techniques prevalent in OBMs.

2. Education and Awareness: Train staff and individuals on the latest cyber threats and the importance of secure online practices.

3. Utilize Advanced Monitoring Tools: Implement tools that can detect unusual network activities indicative of cyber threats.

4. Collaboration with Law Enforcement: Work closely with law enforcement agencies to stay informed about the latest cybercrime trends and response strategies.

In conclusion, understanding the dynamics of OBMs and their resilience mechanisms is crucial for developing effective strategies against cybercrime. As these markets evolve, so must the countermeasures by individuals, enterprises, and law enforcement agencies.

#### References

**“Countermeasures for Cyber Attacks.”** htttp://www.chat.openai.com.

**Cox, Russ. “Running the “Reflections on Trusting Trust” Compiler.”** *research!rsc*, 25 October 2023, https://research.swtch.com/nih. Accessed 14 January 2024.

**“How it works.”** *How the three stages namely self-reproducing code (quine), compiling compiler, and modification of compiler adds a backdoor trojan horse*, https://www.chat.openai.com.

**“Online marketplace.”** *Wikipedia*, https://en.wikipedia.org/wiki/Online\_marketplace. Accessed 14 January 2024.

**“Platformization”** http://chat.openai.com