1. bccstego: A Framework for Investigating Network Covert Channels

* malware exfiltrate data (1)
* no much focus on IPV6 – but IPV6 are most targetted(1)
* This framework has high throughput – deep packet inspection poses scalability issues (1)
* Handling v4/v6 conversion issues (1)
* Uses BPF – can be exteneded to different protocols (2)
* Tool collects statastical info and better performance (2)
* State is neglected. Only general statastics is measured – less memory and less overhead (3)
* Uses python (4)
* Focuses on specific protocols and techniques (4)
* Compiled with makefile to create single executable (4)
* Behavioural changes in bin for different channels (5)
* Suddent increase in bin number is an indication of attack (6)
* The tool has to be integrated with other frameworks to perform better(7)

1. CCgen: Injecting Covert Channels into Network Traffic

* Tool to inject covert channel into network (1)
* Open source tool implemented in python and scapy (1)
* Covert channels used for criminal activities (1)
* But there are application of covert channel – digital watermarking, traceback etc (1)
* Covert channels are classified based on the statstical challenged posed by them (2)
* Security systems are incapable of detection of covert channel (2)
* Inject multiple covert channels in the same capture(2)
* Discussion on unique types of covert channels provided by framework(2 – 3)

1. Code Augmentation for Detecting Covert Channels Targeting the IPv6 Flow Label

* IPV6 attract more attacks (1)
* Generalizability and scalability is an issue for covert detection system (1)
* they can be used to exfiltrate stolen information, orchestrate nodes of a botnet or implement multi-stage loading architectures to extend malware functionalities at runtime (1)
* Flow Label of IPV6 is exploited (1)
* BPF is an effective way of gathering statastical data (1)

1. Detecting Covert Channels Through Code Augmentation

* Extended BPF helps in spotting covert channel (1)
* Use of code augumentation in linux kernel to gather data (1) – hooks can be used to insert various monitoring codes without disturbing a whole design.
* Covert channel usage is a new trend to evade detection (1)
* Malware exfiltrate data with covert channel and orchestrate a botnet (2)
* Task cannot be generalized (2, 5) – Generalization affects perfomance to a great exent (5)
* Testing on realistic senario and IPV6 is next target (2, 5)
* Common terms Definitions (3)
* Local covert channel (3)
* Malware attacks using network covert channel (4)
* V4/v6 transission is a disadavantage in while injecting covert channel (5)
* Data collection – counting the possible values assumed by the field and analysing the pattern to indentify anomalies (6)
* Testing channel with VM (7)
* eBPF can be used for both local and network covert channel (6) – eBPF adds the minimum overhead to the traffic, thus suitable for real traffic (9)
* Graphical analysis of covert channel patterns (10)
* Higher rate of transmission is detectable easilt bcz of the spike (10), low rate of transmission is not easily detectable, but takes longer amount of time (11)

1. pcapStego: A Tool for Generating Traffic Traces for Experimenting with Network Covert Channels

* Dataset generator with real world traffic traces and replayable coversations (1)
* Data exfiltration(1)
* Covert communication is neglected (2)
* Gathering info from real network is not ethical (2)
* Large data is required for building AI solution (2,8) – common approach is to use AI for detectection of malacious activities (8)
* This realworld traces dataset generated by tool is better than other toy datasets (2)
* IPV6 is the nextarget and pcapStego helps generating this data (2)
* Storage v/s timing channel (3)
* Different headers that are exploited to create covert channel by the tool (3)
* Either select the mode of covert channel and info, or automate the task using the tool (4)
* Tool uses python 3 and scapy 2.4.4 (4)
* Composition of the software (5) and usage (5-6)
* CAIDA used for realworld traffic traces of IPV6

1. Covert Channel Detection: Machine Learning Approaches

* Covert channel is used for malacious activity (1)
* Countermesures cannot be generalized (1,4)
* Covert channel have both advantages and disadvantages (2)
* Types of covert channel (2)
* Covert channel explotation by IoT devices (2)
* Distributed covert channels (3) – Spreads covert channel over different hiding techniques
* Packet reordering covert channel (3)
* vulnerabilities of the IPv6 and its incomplete implementation (3)
* VoLTE interepacket delay exploitation is not possible since it is fixed (3)
* Video packet reordering in VoLTE (3)
* Preventive mechanism in protocol itself (3)
* Dataset unavailabilty (4)
* SVM is the best aproach (4)
* Statstical variation must be clear for covert channel, otheriwise it will be undetected (4) addition of Noise makes it difficult to detect covert channel (4-5)
* Python, Wireshark, Scapy, Orange Software – for preprocessing (5)
* Discussion on already implemented models and tools (6 -10)
* Model needs to be updated priodically to stay up to date (12)