Abertay University

A Taxonomy of Malicious Traffic for Intrusion Detection Systems

Hanan Hindy

PhD Student, Division of Cyber Security,

Abertay University, Dundee Scotland

hananhindy.com

Cyber SA 2018

June 11-12, 2018

Scotland, UK

Agenda

- Introduction
- Background
- Why Taxonomy for Malicious Traffic?
- Proposed Taxonomy (V1 & V2)
- Conclusion and Future Work
- References

Introduction

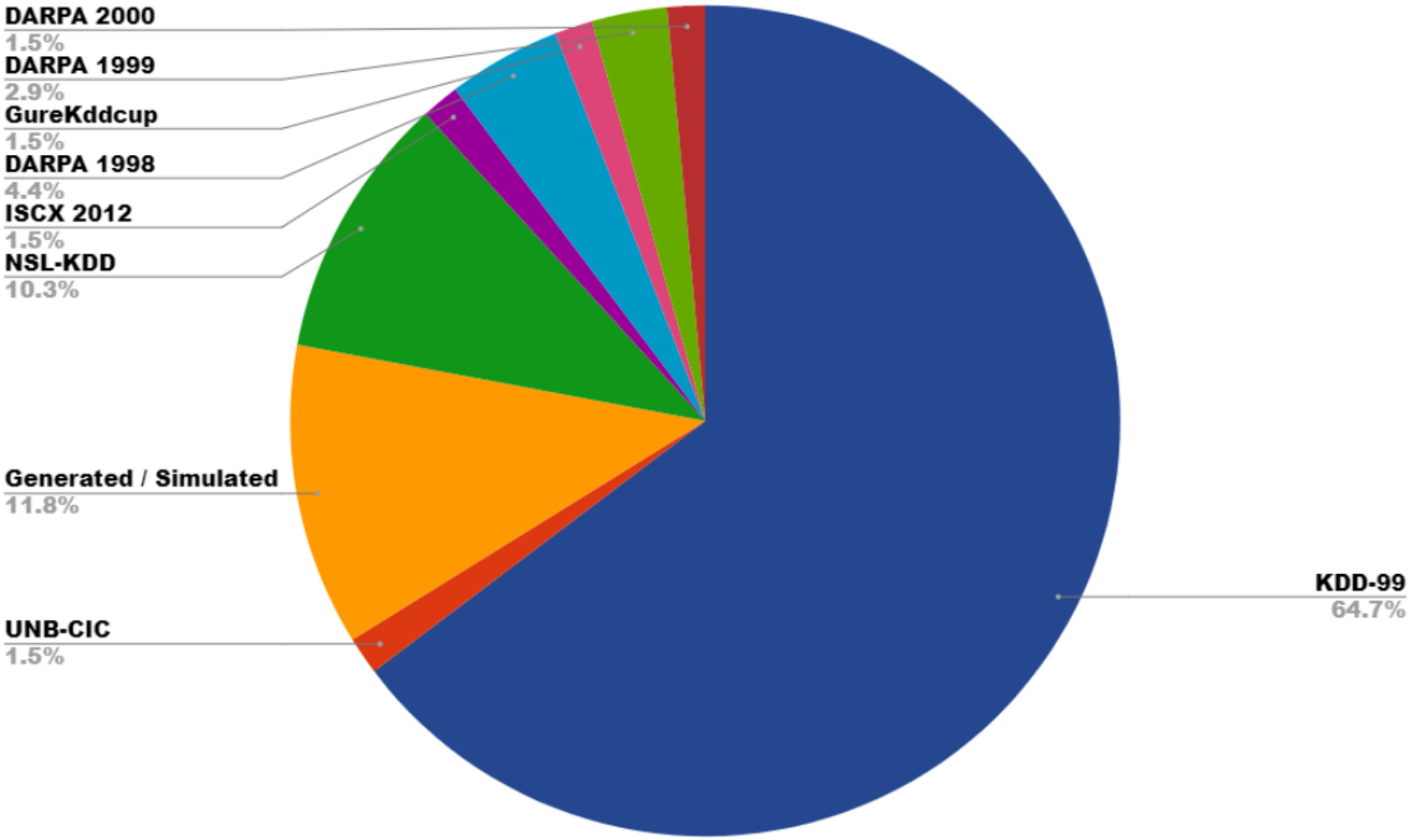
- Number of network threats are increasing, with the world being dependent on machines and automation.
- Cisco predicts that there will be **50 billion devices** connected to the Internet by 2020.
- Attacks are becoming more **complex** and users are becoming more **aware**.

Background

Based on prominent IDS in the past decade (2008 – 2018)

- Available Intrusion Detection Systems (IDS) – *both signature and anomaly based* – detect rely on available datasets, that are mostly outdated.

Background

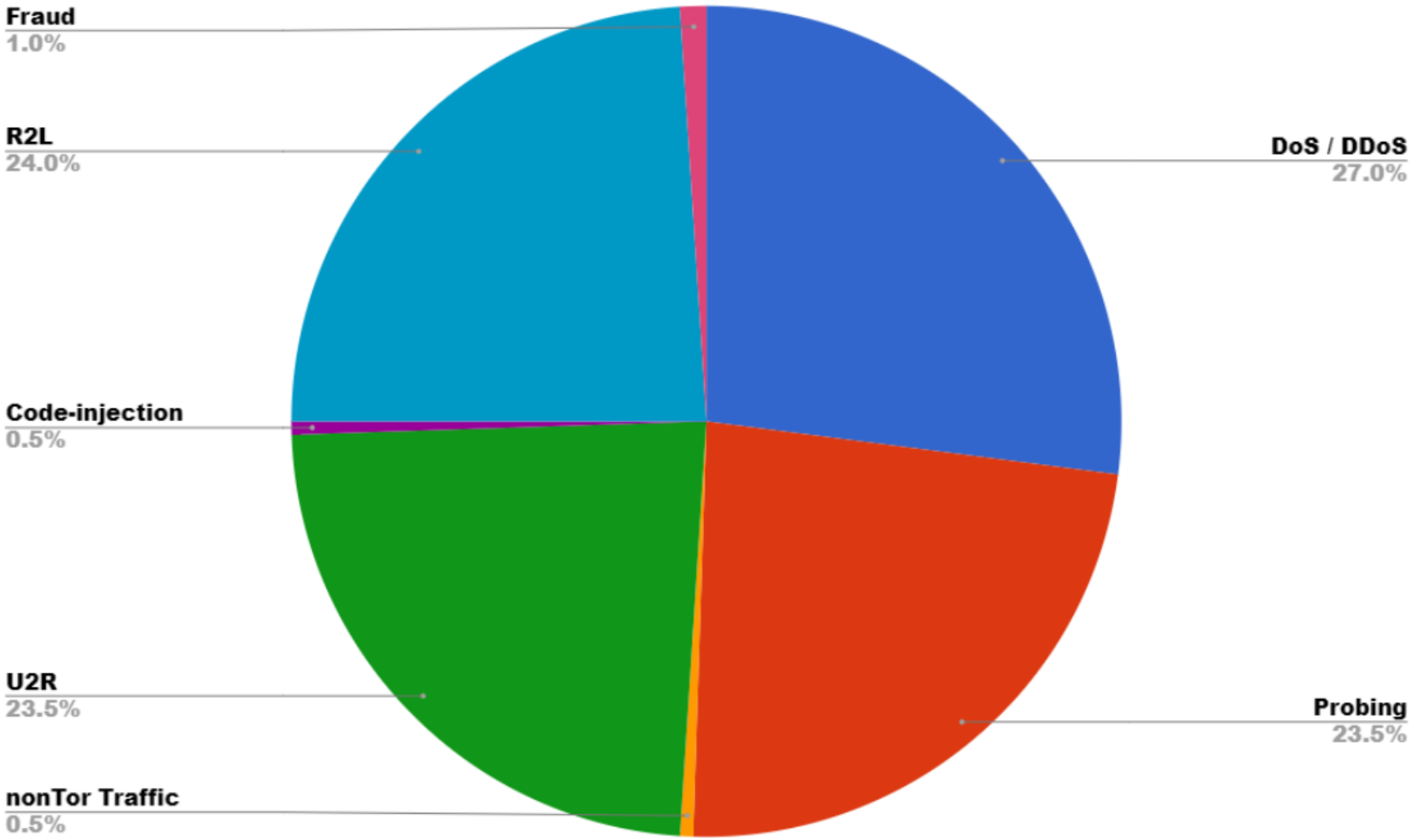

DARPA 2000
1.5%
DARPA 1999
2.9%
GureKddcup
1.5%
DARPA 1998
4.4%
ISCX 2012
1.5%
NSL-KDD
10.3%
Generated / Simulated
11.8%
UNB-CIC
1.5%
KDD-99
64.7%

Background

Based on prominent IDS in the past decade (2008 – 2018)

- Available Intrusion Detection Systems (IDS) – *both signature and anomaly based* – detect rely on available datasets, that are mostly outdated.
- Therefore, they detect a subset of the known attacks.

Background


Fraud
1.0%
R2L
24.0%
Code-injection
0.5%
U2R
23.5%
nonTor Traffic
0.5%
DoS / DDoS
27.0%
Probing
23.5%

Why Taxonomy for Malicious Traffic?

- Available taxonomies focus of **specific** systems/tools.

With the taxonomy, researchers can

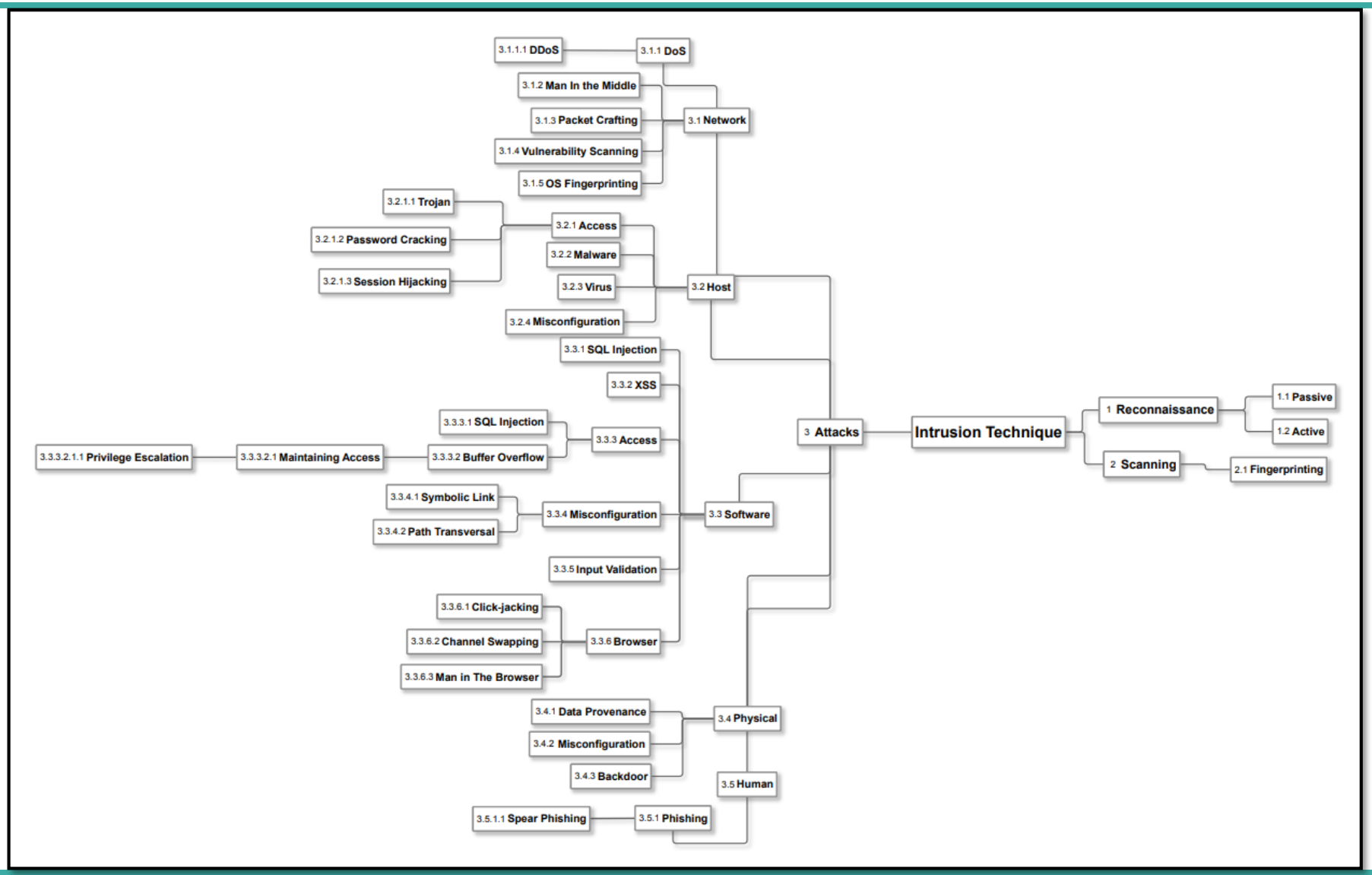
- Design up-to-date detection tools and find ways to prevent and predict these attacks.
- Build better datasets that cover more attacks and have the real world property.

Proposed Taxonomy

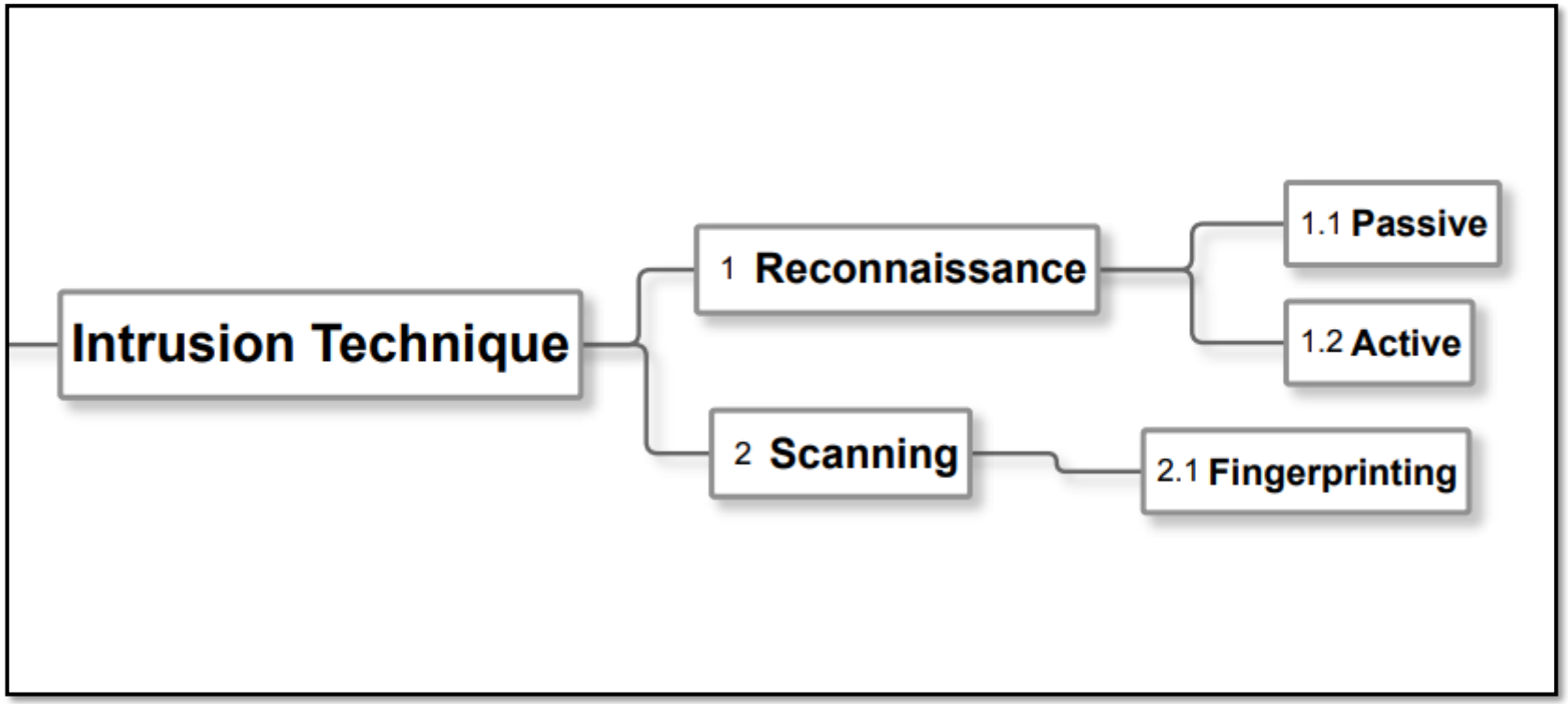
The taxonomy is presented as three control stages:

1. Reconnaissance
2. Scanning
3. Attack

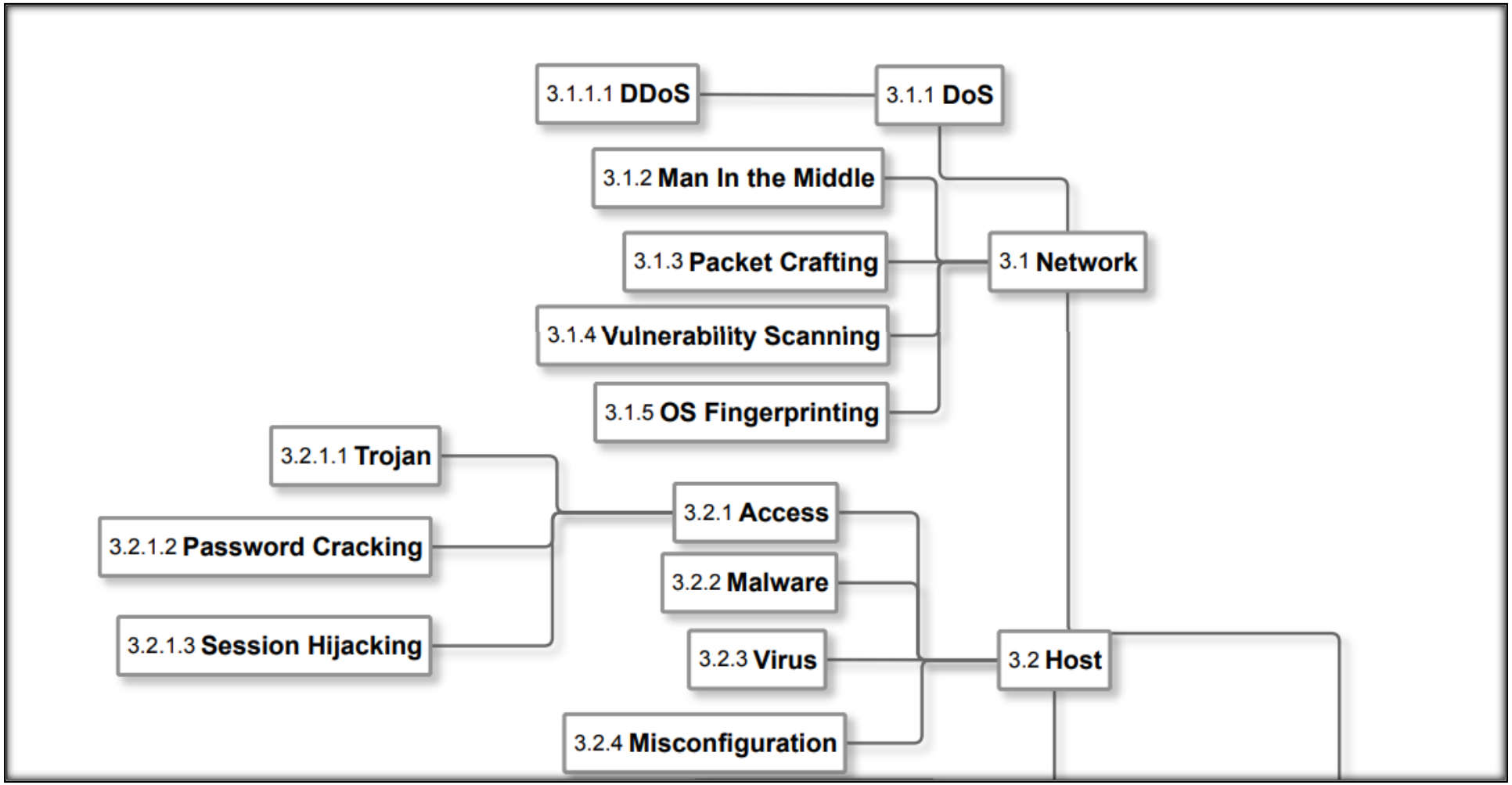
Proposed Taxonomy V1



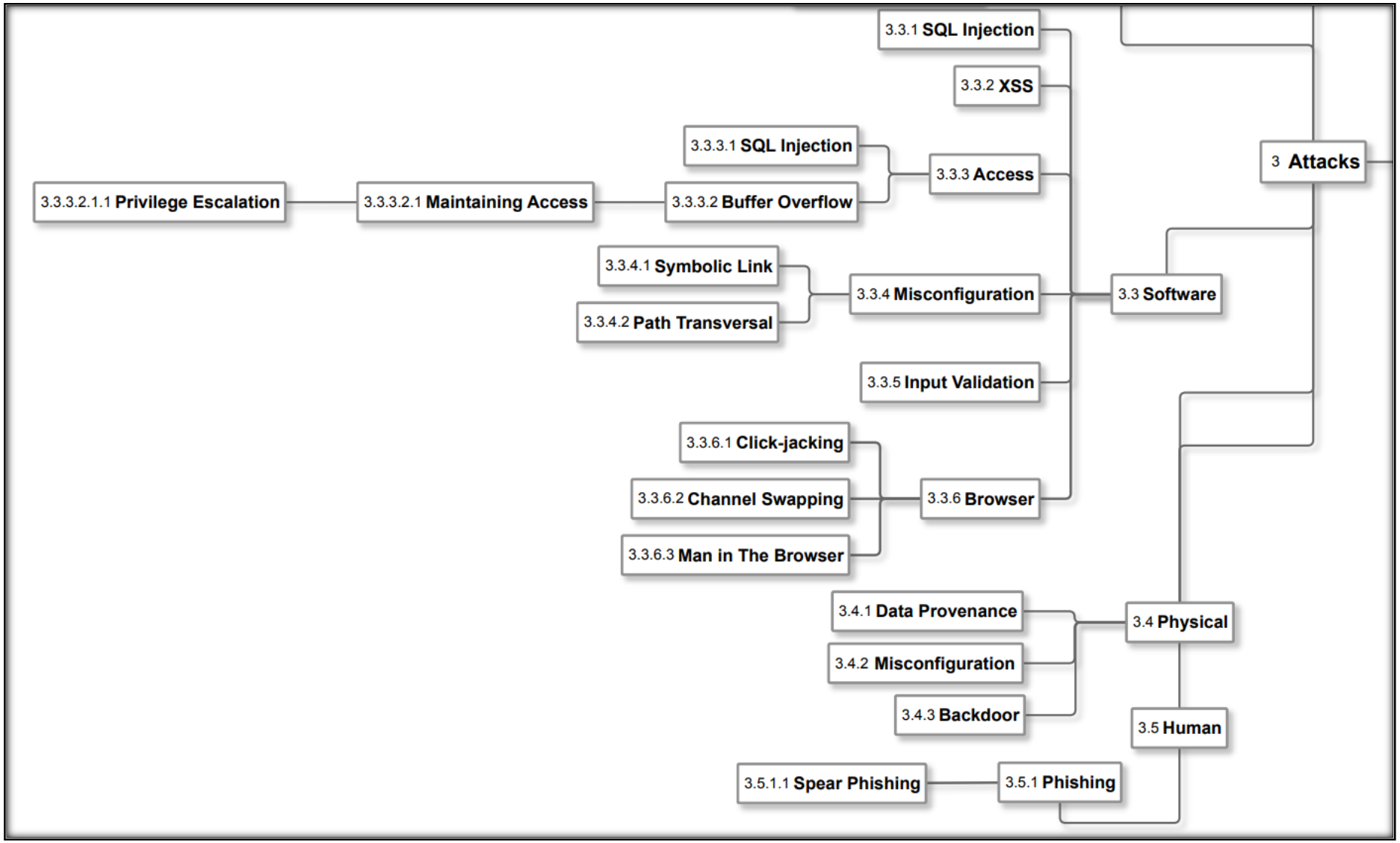
Proposed Taxonomy V1



Proposed Taxonomy V1 (Cont.)

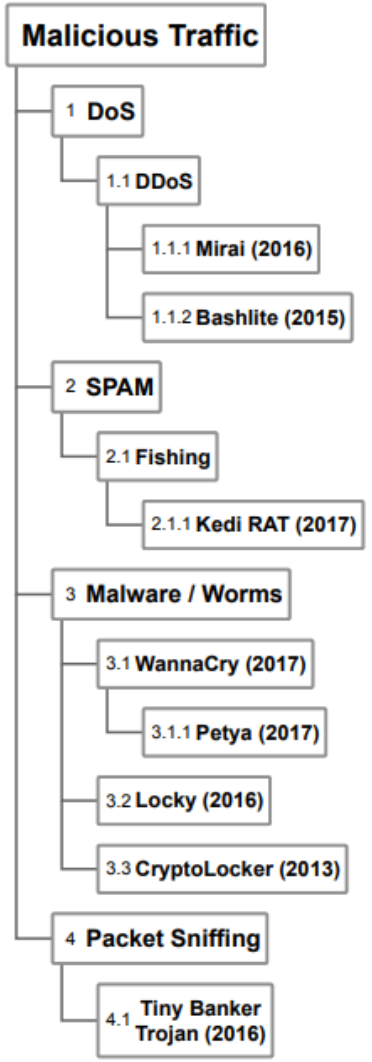


Proposed Taxonomy V1 (Cont.)



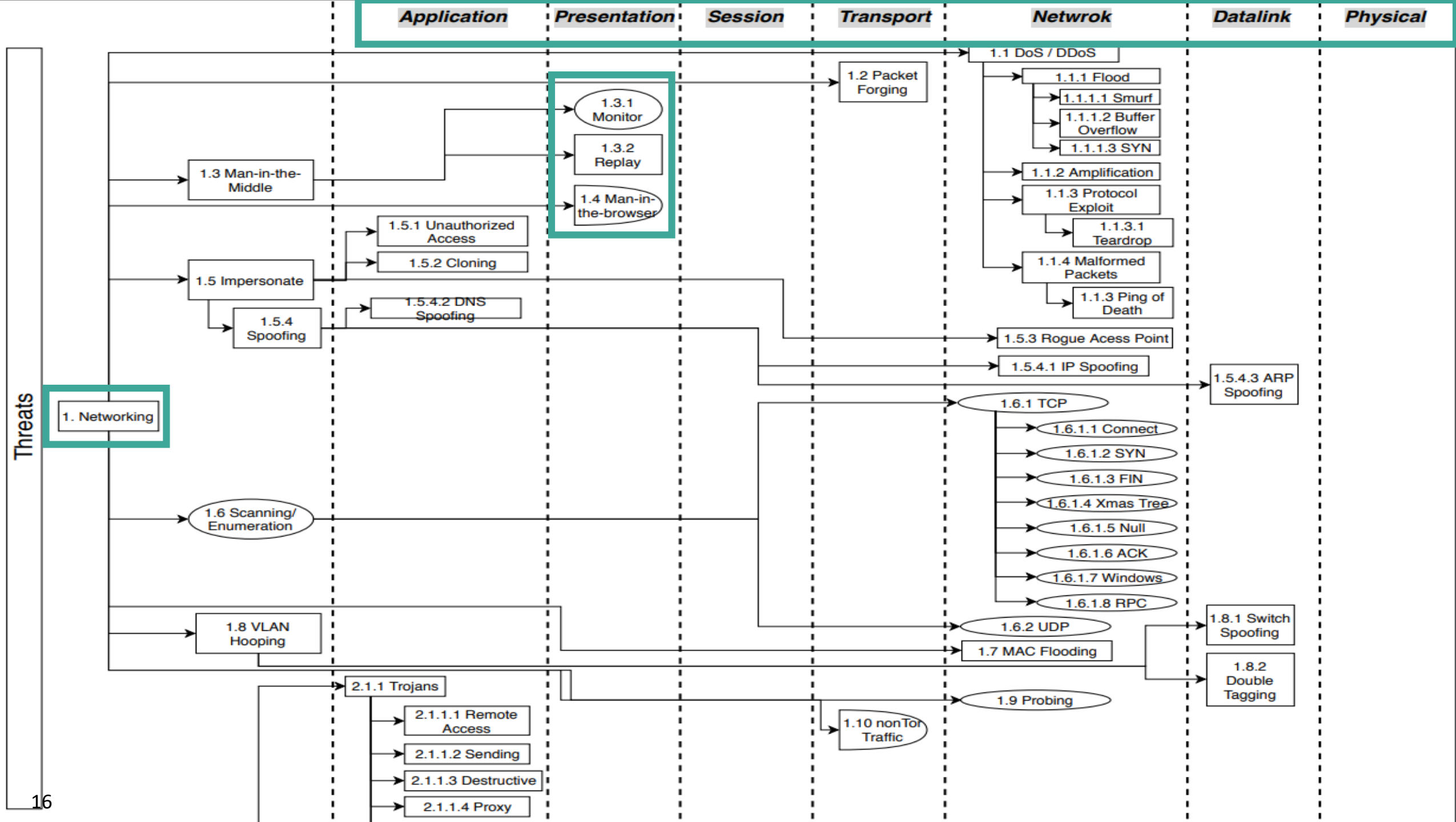
Recent Attacks

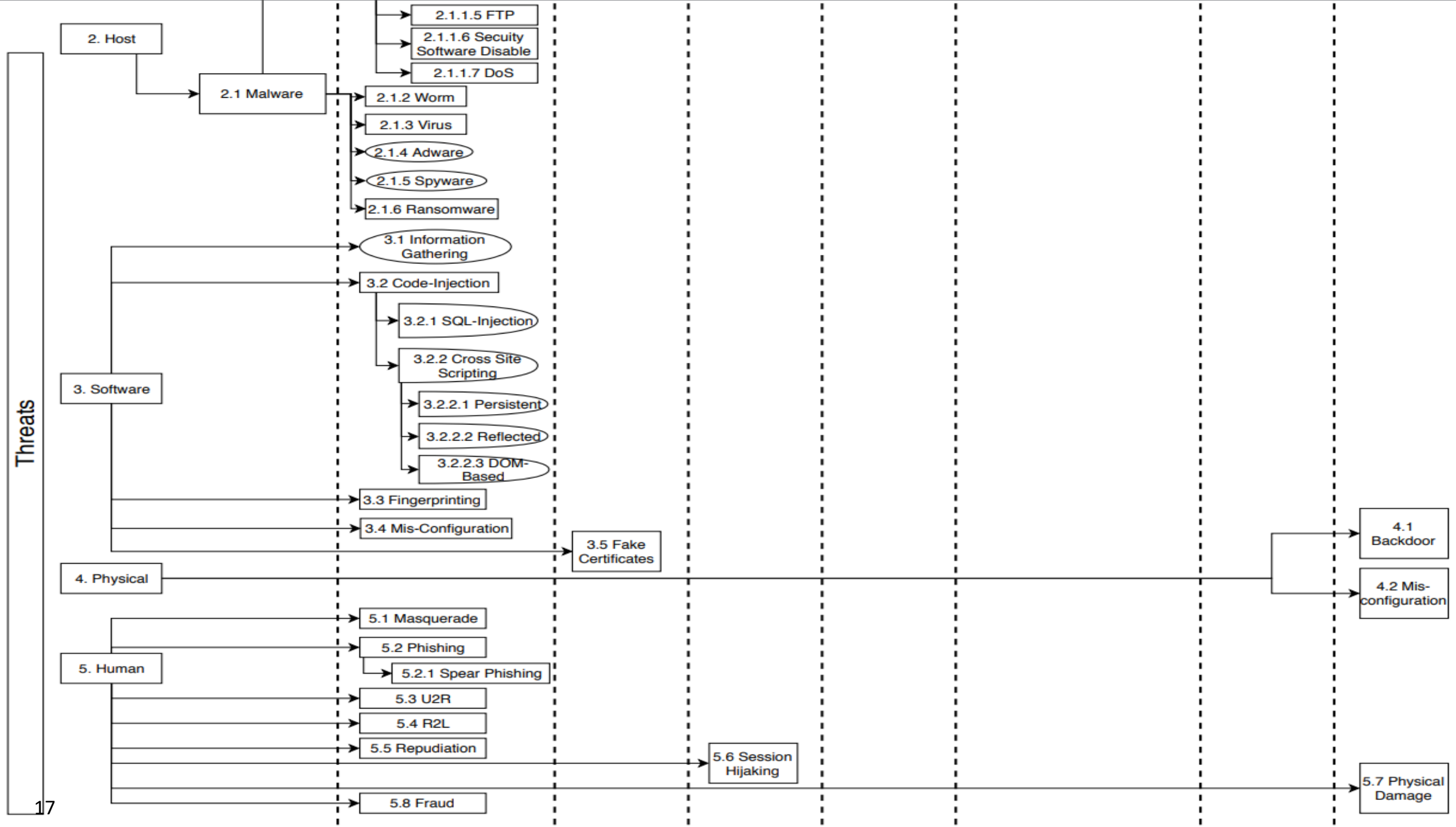
- Although recent attacks are reported, they are barely included in the datasets



Proposed Taxonomy V2

- An extended version of the taxonomy is built.
- Attacks are classified based on:
  - Affected OSI Layer
  - Source
  - Active/Passive


Application
Presentation
Session
Transport
Netwrok
Datalink
Physical
Threats
1. Networking
1.1 DoS / DDoS
1.1.1 Flood
1.1.1.1 Smurf
1.1.1.2 Buffer Overflow
1.1.1.3 SYN
1.1.2 Amplification
1.1.3 Protocol Exploit
1.1.3.1 Teardrop
1.1.4 Malformed Packets
1.1.3 Ping of Death
1.2 Packet Forging
1.3 Man-in-the-Middle
1.3.1 Monitor
1.3.2 Replay
1.4 Man-in-the-browser
1.5 Impersonate
1.5.1 Unauthorized Access
1.5.2 Cloning
1.5.4 Spoofing
1.5.4.2 DNS Spoofing
1.5.3 Rogue Acess Point
1.5.4.1 IP Spoofing
1.5.4.3 ARP Spoofing
1.6 Scanning/ Enumeration
1.6.1 TCP
1.6.1.1 Connect
1.6.1.2 SYN
1.6.1.3 FIN
1.6.1.4 Xmas Tree
1.6.1.5 Null
1.6.1.6 ACK
1.6.1.7 Windows
1.6.1.8 RPC
1.6.2 UDP
1.7 MAC Flooding
1.8 VLAN Hooping
1.8.1 Switch Spoofing
1.8.2 Double Tagging
1.9 Probing
1.10 nonTor Traffic
2.1.1 Trojans
2.1.1.1 Remote Access
2.1.1.2 Sending
2.1.1.3 Destructive
2.1.1.4 Proxy


Threats
2. Host
2.1 Malware
2.1.1.5 FTP
2.1.1.6 Secuity Software Disable
2.1.1.7 DoS
2.1.2 Worm
2.1.3 Virus
2.1.4 Adware
2.1.5 Spyware
2.1.6 Ransomware
3. Software
3.1 Information Gathering
3.2 Code-Injection
3.2.1 SQL-Injection
3.2.2 Cross Site Scripting
3.2.2.1 Persistent
3.2.2.2 Reflected
3.2.2.3 DOM-Based
3.3 Fingerprinting
3.4 Mis-Configuration
3.5 Fake Certificates
4. Physical
4.1 Backdoor
4.2 Mis-configuration
5. Human
5.1 Masquerade
5.2 Phishing
5.2.1 Spear Phishing
5.3 U2R
5.4 R2L
5.5 Repudiation
5.6 Session Hijaking
5.7 Physical Damage
5.8 Fraud

Conclusion and Future Work

- The aim is to build an extendable, full taxonomy of network threats to help researchers build up-to-date datasets and robust IDS.

- The taxonomy should be kept up to date and its effect on building new IDS should be analysed.

Questions

Hanan Hindy

PhD Student, Division of Cyber Security,

Abertay University, Dundee Scotland

1704847@abertay.ac.uk

hananhindy.com