APPENDIX A

KDDCup99 data set

The KDDCup99 data set stems from data gathered at MIT Lincoln Laboratory under sponsorship of the Defense Advanced Research Projects Agency (DARPA) to evaluate Intrusion Detection Systems (IDSs) in 1998 and 1999. These two data sets are referred to as DARPA98 and DARPA99, which consist of raw *tcpdump* data from a simulated medium sized US air force base. The KDDCup99 data set was provided by Stolfo and Lee for the Knowledge Discovery and Data Mining Tools competition (and associated conference) in 1999 [27]. This is a transformed version of the DARPA *tcpdump* data, consisting of a set of features considered suitable for classification with machine learning algorithms. The data set consists of 41 features, some of which are intrinsic to the network connections, whilst other are created using domain knowledge.

DERIVED FEATURES

Stolfo et al. defined higher-level features that help in distinguishing normal connections from attacks. There are several categories of derived features.

The “same host” features examine only the connections in the past two seconds that have the same destination host as the current connection, and calculate statistics related to protocol behavior, service, etc.

The similar ``same service" features examine only the connections in the past two seconds that have the same service as the current connection.

"Same host" and "same service" features are together called time-based traffic features of the connection records.

Some probing attacks scan the hosts (or ports) using a much larger time interval than two seconds, for example once per minute. Therefore, connection records were also sorted by

destination host, and features were constructed using a window of 100 connections to the same host instead of a time window. This yields a set of so-called host-based traffic features.

Unlike most of the DOS and probing attacks, there appear to be no sequential patterns that are frequent in records of R2L and U2R attacks. This is because the DOS and probing attacks involve many connections to some host(s) in a very short period of time, but the R2L and U2R attacks are embedded in the data portions of packets, and normally involve only a single connection.

Useful algorithms for mining the unstructured data portions of packets automatically are an open research question. Stolfo et al. used domain knowledge to add features that look for suspicious behavior in the data portions, such as the number of failed login attempts. These features are called ``content'' features.

Features are grouped into four categories:

Basic Features: These features are directly obtained from packet headers.

***Content Features*:** Domain knowledge is applied to assess data portion of the TCP packets. Features like number of failed login attempts are content features.

***Time-based Traffic Features*:** These features are designed to capture properties that mature over a 2 second temporal window. One example of such a feature would be the number of connections to the same host over the 2 second interval.

***Host-based Traffic Features*:** Some probing attacks scan the hosts (or ports) using a much larger time interval than two seconds, for example once per minute. Therefore, connection records were also sorted by destination host, and features were constructed using a window of 100 connections to the same host instead of a time window.

A complete listing of the set of features defined for the connection records is given in the Table A-1 below.

Table A-1: Features with descriptions and their types

Feature No.	Feature Name	Description	Feature Type
1	duration	Duration of the connection	Continuous
2	protocol_type	Connection protocol (e.g. tcp, udp)	Categorical

3	service	Destination service (e.g. telnet, ftp)	Categorical
4	flag	Status flag of the connection	Categorical
5	src_bytes	Bytes sent from source to destination	Continuous
6	dst_bytes	Bytes sent from destination to source	Continuous
7	land	1 if connection is from/to the same host/port; 0 otherwise	Categorical
8	Wrong_fragment	number of wrong fragments	Continuous
9	Urgent	number of urgent packets	Continuous
10	hot	number of "hot" indicators	Continuous
11	num_failed_login	number of failed logins	Continuous
12	logged_in	1 if successfully logged in; 0 otherwise	Categorical
13	num_compromised	number of "compromised" conditions	Continuous
14	root_shell	1 if root shell is obtained; 0 otherwise	Categorical
15	su_attempted	1 if "su root" command attempted; 0 otherwise	Categorical
16	num_root	number of "root" accesses	Continuous
17	num_file_creations	number of file creation operations	Continuous
18	num_shells	number of shell prompts	Continuous
19	num_access_files	number of operations on access control files	Continuous
20	num_outbound_cmds	number of outbound commands in an ftp session	Continuous
21	is_host_login	1 if the login belongs to the	Categorical

		"host"	
22	is_guest_login	1 if the login is a "guest" login; 0 Otherwise	Categorical
23	count	number of connections to the same host as the current connection in the past two seconds	Continuous
24	srv_count	number of connections to the same service as the current connection in the past two seconds	Continuous
25	serror_rate	% of connections that have “SYN" Errors	Continuous
26	srv_serror_rate	% of connections that have “SYN" Errors	Continuous
27	rerror_rate	% of connections that have “REJ" Errors	Continuous
28	srv_rerror_rate	% of connections that have “REJ" errors	Continuous
29	same_srv_rate	% of connections to the same service	Continuous
30	diff_srv_rate	% of connections to different services	Continuous
31	srv_diff_host_rate	% of connections to different hosts	Continuous
32	dst_host_count	count of connections having the same destination host	Continuous
33	dst_host_srv_count	count of connections having the same destination host and using the same service	Continuous

34	dst_host_same_srv_rate	% of connections having the same destination host and using the same service	Continuous
35	dst_host_diff_ srv_rate	% of different services on the current host	Continuous
36	dst_host_same_src_port_rate	% of connections to the current host having the same src port	Continuous
37	dst_host_srv_diff_host _rate	% of connections to the same service coming from different hosts	Continuous
38	dst_host_serror_rate	% of connections to the current host that have an S0 error	Continuous
39	dst_host_srv_serror_rate	% of connections to the current host and specified service that have an S0 error	Continuous
40	dst_host_rerror_rate	% of connections to the current host that have an RST error	Continuous
41	dst_host_srv_rerror_rate	% of connections to the current host and specified service that have RST error	Continuous

There are three partitions of the KDDCup99 data available online: a full training set (4,898,431 instances), a 10% version of this training set, and a test set (311,029 instances). The test set includes 17 new attacks. The intrusions are commonly grouped into 4 classes, according to the taxonomy of Kendall (1999): Denial of Service (DOS), Remote to Local (R2L, User to Root (U2R) and Probe. Some intrusions in the KDDCup99 data set are not described by Kendall (1999), but are grouped here according

to that of the KDD contest [27], with two exceptions due to inconsistencies. According to the KDD classification, three attacks were present in two categories: *httptunnel* and *multihop* were present in *U2R* and *R2L*, but are kept only as *R2L* here; *warezmaster* was classified as *R2L* for training, but as DOS during testing, but is consistently kept as *R2L* here. An overview of the intrusions, grouped according to these classes, is provided in Table A-2. Description of each attack is given in Table A-3. The numbers of instances for each of the attack types are listed in Table A-4, followed by the proportions of each attack class in Table A.5.

Table A-2: Attack Types Grouped to respective Class

Category of attacks	Types of attacks
Denial of Service (DOS)	back, Neptune, ping of death, land, pod, smurf, teardrop,
Remote to Local (R2L)	ftp_write, multihop, phf, spy, warezclient, warezmaster, imap, guess_passwd
User to root (U2R)	buffer_overflow, loadmodule, perl, rootkit
Probe	ipsweep, nmap, satan, portsweep

Table A-3: Description of Attacks

Types of Attacks	Description
Back	Denial of service attack against apache web server where a client requests a URL containing many backslashes
neptune	Syn flood denial of service on one or more ports
Land	Denial of service where a remote host is sent a UDP packet with the same source and destination
Pod	Denial of service ping of death
smurf	Denial of service icmp echo reply flood
teardrop	Denial of service where mis-fragmented UDP packets cause some systems to reboot
multihop	Multi-day scenario in which a user first breaks into one machine

Phf	Exploitable CGI script which allows a client to execute arbitrary commands on a machine with a mis-configured web server.
Spy	Multi-day scenario in which a user breaks into a machine with the purpose of finding important information where the user tries to avoid detection. Uses several different exploit methods to gain access
warezclient	Users downloading illegal software which was previously posted via anonymous FTP by the warezmaster
warezmaster	Anonymous FTP upload of Warez (usually illegal copies of copy writed software) onto FTP server
Imap	Remote buffer overflow using imap port leads to root shell
loadmodule	Non-stealthy loadmodule attack which resets IFS for a normal user and creates a root shell
Perl	Perl attack which sets the user id to root in a perl script and creates a root shell
rootkit	Multi-day scenario where a user installs one or more components of a rootkit
ipsweep	Surveillance sweep performing either a port sweep or ping on multiple host addresses
nmap	Network mapping using the nmap tool. Mode of exploring network will vary-options include SYN
satan	Network probing tool which looks for well-known weaknesses. Operates at three different levels. Level 0 is light
portsweep	Surveillance sweep through many ports to determine which services are supported on a single host.
dict	Guess passwords for a valid user using simple variants of the account name over a telnet connection
eject	Buffer overflow using eject program on Solaris. Leads to a user->root transition if successful
ffb	Buffer overflow using the ffbconfig UNIX system command leads to root shell

format	Buffer overflow using the fdformat UNIX system command leads to root shell
ftp-write	Remote FTP user creates .rhost file in world writable anonymous FTP directory and obtains local login
guest	Try to guess password via telnet for guest account
syslog	Denial of service for the syslog service connects to port 514 with unresolvable source ip
warez	User logs into anonymous FTP site and creates a hidden directory

Table: A-4: Number of instances of each attack

Types of Attacks	Class	Training (Full)	Training (10%)	Test
back	DOS	2203	2203	1098
neptune	DOS	1072017	1072017	58001
land	DOS	21	21	09
pod	DOS	264	264	87
smurf	DOS	2807886	280790	164091
teardrop	DOS	979	979	12
ftp_write	R2L	8	8	3
multihop	R2L	7	7	18
phf	R2L	4	4	2
spy	R2L	2	2	-
warezclient	R2L	1020	1020	-
warezmaster	R2L	20	20	1602
imap	R2L	12	12	1
guess_passwd	R2L	53	53	4367
load module	U2R	9	9	2
perl	U2R	3	3	2
rootkit	U2R	10	10	13

ip sweep	Probe	12481	1247	306
nmap	Probe	2316	231	84
satan	Probe	15892	1589	1633
port sweep	Probe	10413	1040	354
buffer_overflow	U2R	30	30	22
normal	Normal	972780	97278	60593
apache2	DOS	-	-	794
http tunnel	R2L	-	-	158
mail bomb	DOS	-	-	5000
mscan	Probe	-	-	1053
named	R2L	-	-	17
process table	DOS	-	-	759
ps	U2R	-	-	16
saint	Probe	-	-	736
send mail	R2L	-	-	17
snmpget attack	R2L	-	-	7741
snmp guess	R2L	-	-	2406
sql attack	U2R	-	-	2
udp storm	DOS	-	-	2
worm	R2L	-	-	2
xlock	R2L	-	-	9
xsnoop	R2L	-	-	4
xterm	U2R	-	-	13
	Total	4898430	494021	311029

Table A-5: Proportions of attack classes

Class	Training (Full)	Training (10%)	Test
Normal	972780 (19.86%)	97278 (19.69%)	60593 (19.48%)
DOS	3883370 (79.30%)	391458 (79.24%)	229853 (73.90%)
R2L	1126 (0.02%)	1126 (0.23%)	16347 (5.23%)
U2R	52 (0.00%)	52 (0.01%)	70 (0.02%)
Probe	41102 (0.84%)	4107 (0.83%)	4166 (1.34%)

The most relevant feature for each type of attack with feature name and corresponding class of attack is given in Table A-6 below.

Table A-6: Most relevant feature for normal and each attack

Types of Attacks	Most Relevant Features	Feature Name	Class
back	5	src_bytes	DOS
neptune	5	src_bytes	DOS
land	7	land	DOS
pod	8	wrong_fragment	DOS
smurf	5	src_bytes	DOS
teardrop	8	wrong_fragment	DOS
ftp_write	23	count	R2L
multihop	23	count	R2L
phf	6	dst_bytes	R2L
spy	39	dst_host_srv_serror_rate	R2L
warez client	3	service	R2L
warez master	6	dst_bytes	R2L
imap	3	service	R2L
guess_passwd	11	num_failed_login	R2L
load module	36	dst_host_same_src_port_rate	U2R

perl	14	root_shell	U2R
rootkit	24	srv_count	U2R
ip sweep	36	dst_host_same_src_port_rate	Probe
nmap	5	src_bytes	Probe
satan	30	diff_srv_rate	Probe
port sweep	28	srv_rerror_rate	Probe
buffer_overflow	3	service	U2R
normal	29	same_srv_rate	Normal