Botnet & DDoS Deep Dive – Part II

The Business Context for Cybersecurity Management

COMP90073
Security Analytics

Dr. Yi Han, CIS

Semester 2, 2021

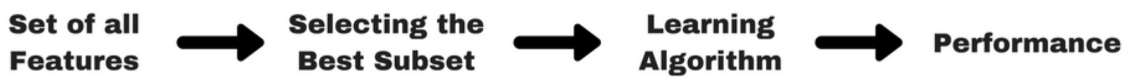
THE UNIVERSITY OF MELBOURNE

Overview

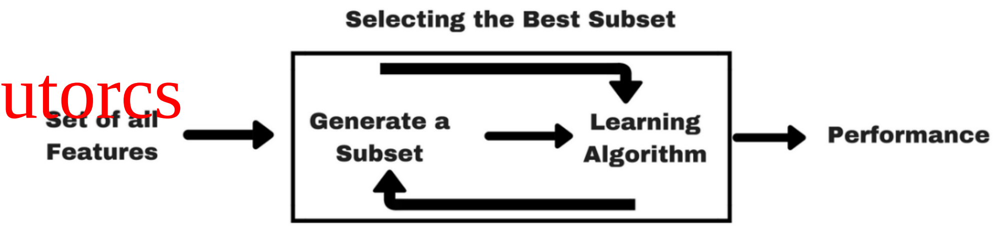
- Botnet, DDoS detection
  - Feature selection
  - Performance comparison
  - Honeypot-based analysis
- DDoS prevention
  - Ingress/egress filtering
  - Router-based filtering
- DDoS reaction
  - Destination-end
  - Intermediate network
  - Source-end

Feature Selection

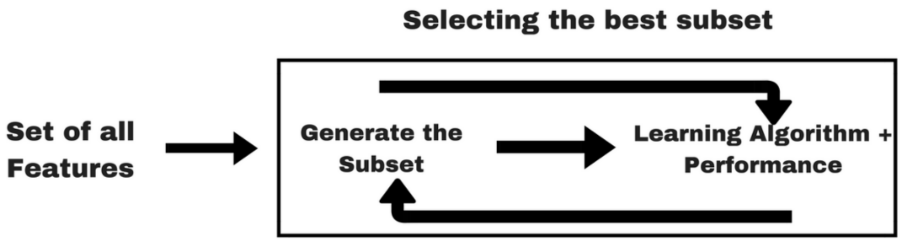
- Filter-based methods
  - Information Gain
  - Chi-square Test
  - Fisher's Score
  - Correlation Coefficient
  - Variance Threshold
  - …



- Wrapper-based methods
  - Forward Feature Selection
  - Backward Feature Elimination



- Embedded methods
  - Lasso regression (L1 regularization)
  - Ridge regression (L2 regularization)



https://www.analyticsvidhya.com/blog/2016/12/introduction-to-feature-selection-methods-with-an-example-or-how-to-select-the-right-variables/

Feature Selection – IG

- Information gain (IG)
  - There are *k* classes in dataset *S*, $S = \{S_1, S_2, \ldots S_k\}$
  - Entropy for dataset *S*,

$$H(S) = -\sum_{i=1}^{k} p_i log p_i = -\sum_{i=1}^{k} \frac{|S_i|}{|S|} log \frac{|S_i|}{|S|}$$

  - Feature *F* has *m* values: $v_1, v_2, \ldots v_m$
  - Subset with feature *F* being v_j, $S_{F=v_j}$
  - The conditional entropy of *S* given feature F,

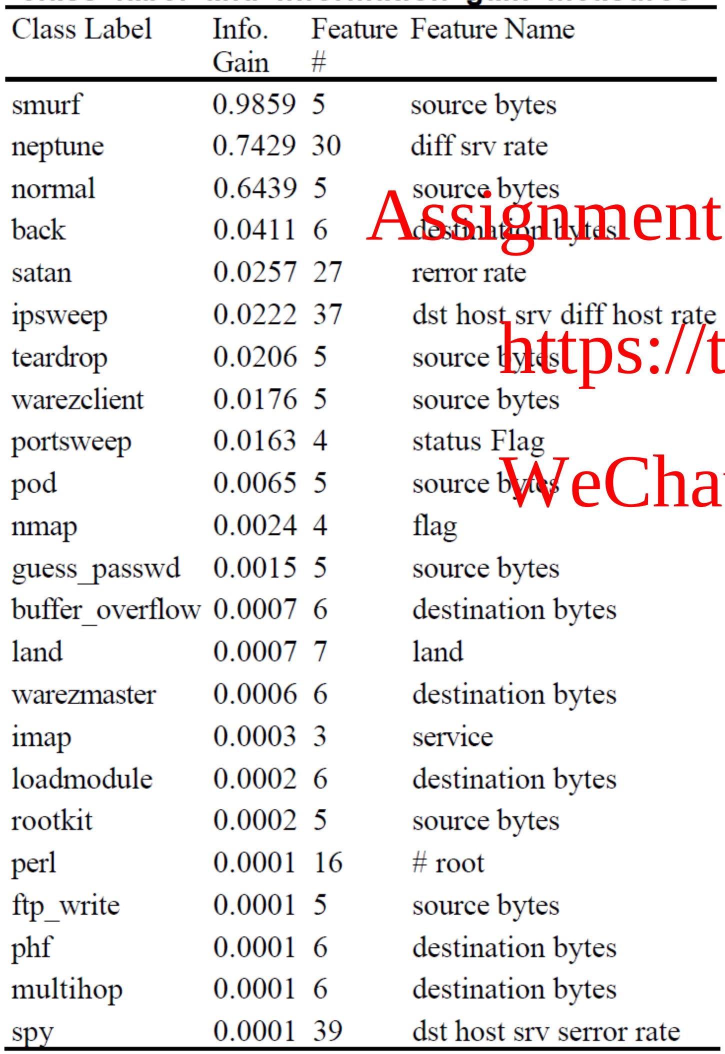
$$H(S|F) = \sum_{j=1}^{m} \frac{\left|S_{F=v_j}\right|}{|S|} \cdot H\left(S_{F=v_j}\right)$$

  - $IG(S,F) = H(S) - H(S|F)$

Feature Selection – KDD Cup 99

- Results of feature selection on KDD Cup 99 using information gain [1]

Table 3. Most relevant features for each class label and information gain measures



Class Label	Info. Gain	Feature #	Feature Name
smurf	0.9859	5	source bytes
neptune	0.7429	30	diff srv rate
normal	0.6439	5	source bytes
back	0.0411	6	destination bytes
satan	0.0257	27	rerror rate
ipsweep	0.0222	37	dst host srv diff host rate
teardrop	0.0206	5	source bytes
warezclient	0.0176	5	source bytes
portsweep	0.0163	4	status Flag
pod	0.0065	5	source bytes
nmap	0.0024	4	flag
guess_passwd	0.0015	5	source bytes
buffer_overflow	0.0007	6	destination bytes
land	0.0007	7	land
warezmaster	0.0006	6	destination bytes
imap	0.0003	3	service
loadmodule	0.0002	6	destination bytes
rootkit	0.0002	5	source bytes
perl	0.0001	16	# root
ftp_write	0.0001	5	source bytes
phf	0.0001	6	destination bytes
multihop	0.0001	6	destination bytes
spy	0.0001	39	dst host srv serror rate

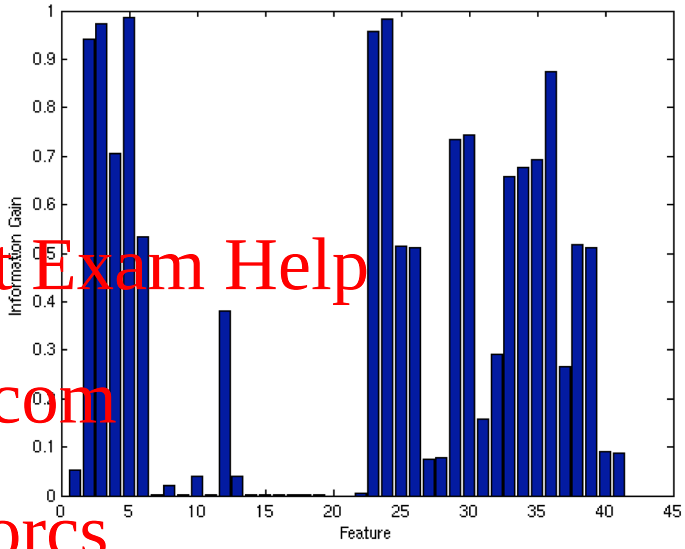
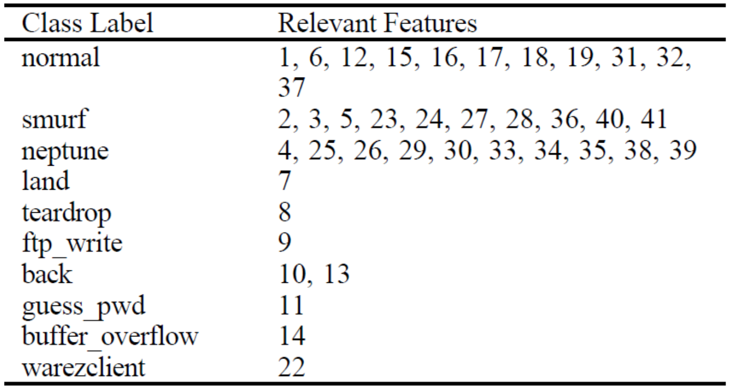


Figure 1. Information gain of each feature

Table 4. List of features for which the class is selected most relevant



Class Label	Relevant Features
normal	1, 6, 12, 15, 16, 17, 18, 19, 31, 32, 37
smurf	2, 3, 5, 23, 24, 27, 28, 36, 40, 41
neptune	4, 25, 26, 29, 30, 33, 34, 35, 38, 39
land	7
teardrop	8
ftp_write	9
back	10, 13
guess_pwd	11
buffer_overflow	14
warezclient	22

THE UNIVERSITY OF MELBOURNE

Feature Selection – CFS

- Correlation-based Feature Selector [2]
  - Heuristic “merit” of a feature subset *S*: $M_s = \frac{k \cdot \overline{r_{cf}}}{\sqrt{k+k(k-1)\overline{r_{ff}}}}$
    - *k*: the number of features
    - $\overline{r_{cf}}$: the average feature-class correlation ($f \in S$)
    - $\overline{r_{ff}}$: the average feature-feature intercorrelation
  - Objectives:
    - Increase feature-to-class correlation ($\overline{r_{cf}}$)
    - Reduce feature-to-feature correlation ($\overline{r_{ff}}$)

Feature Selection – NSL KDD

- Results of feature selection on NSL KDD [3]
  - Wrapper-based: 4, 5, 6, 12, 26, 30
  - Filter-based: the global minima were achieved with the top 10 features (5, 3, 6, 4, 30, 29, 33, 34, 35, 38)

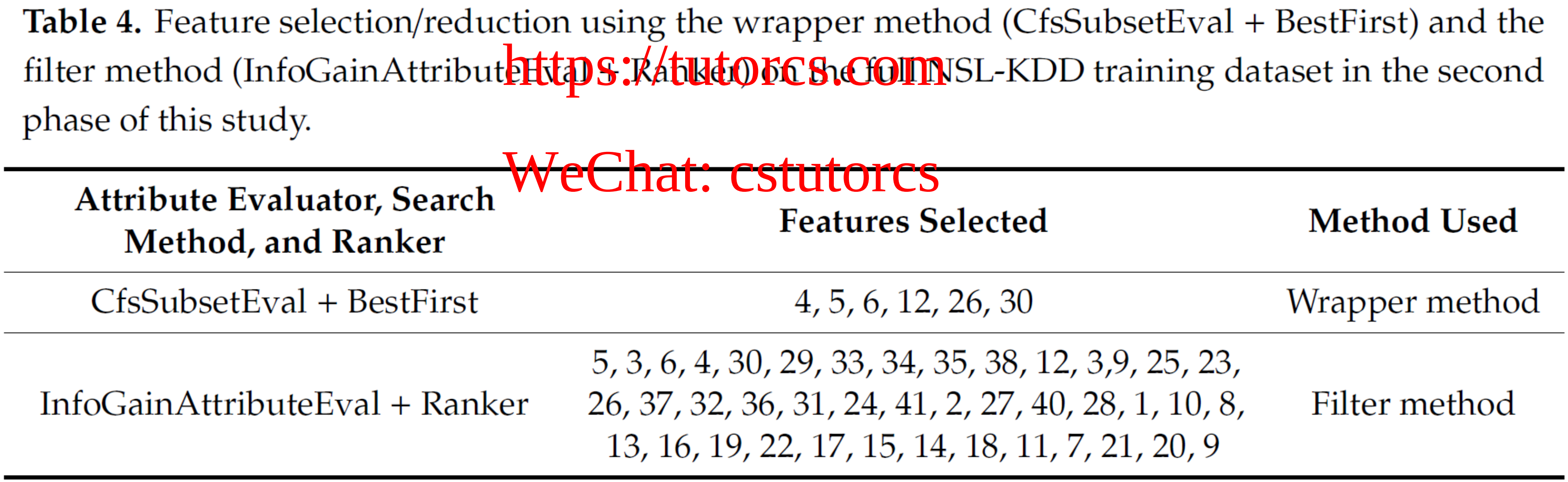


Table 4. Feature selection/reduction using the wrapper method (CfsSubsetEval + BestFirst) and the filter method (InfoGainAttributeEval + Ranker) on the full NSL-KDD training dataset in the second phase of this study.

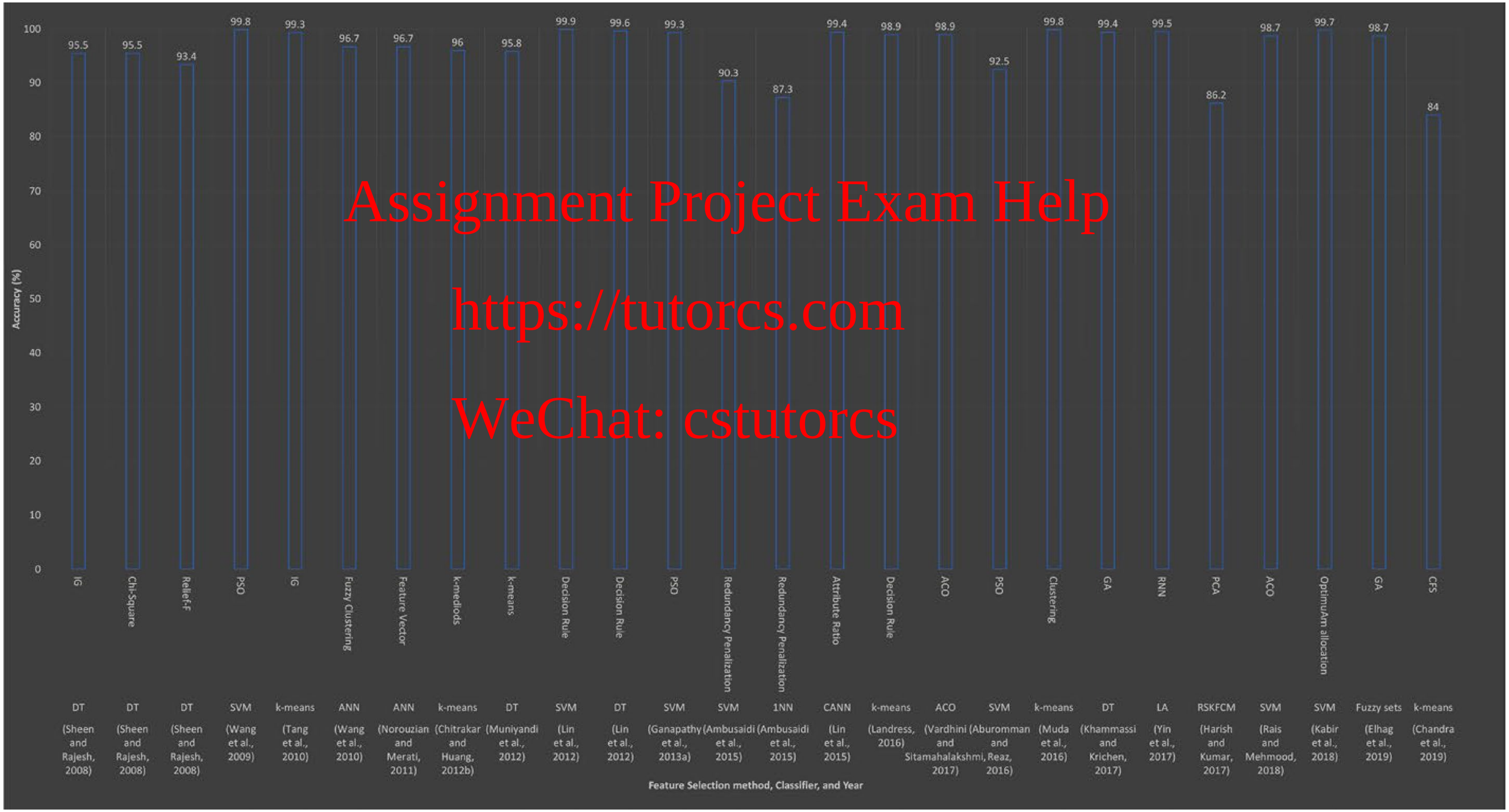
Attribute Evaluator, Search Method, and Ranker	Features Selected	Method Used
CfsSubsetEval + BestFirst	4, 5, 6, 12, 26, 30	Wrapper method
InfoGainAttributeEval + Ranker	5, 3, 6, 4, 30, 29, 33, 34, 35, 38, 12, 3,9, 25, 23, 26, 37, 32, 36, 31, 24, 41, 2, 27, 40, 28, 1, 10, 8, 13, 16, 19, 22, 17, 15, 14, 18, 11, 7, 21, 20, 9	Filter method

Overview

- Botnet, DDoS detection
  - Feature selection
  - Performance comparison
  - Honeypot-based analysis
- DDoS prevention
  - Ingress/egress filtering
  - Router-based filtering
- DDoS reaction
  - Destination-end
  - Intermediate network
  - Source-end

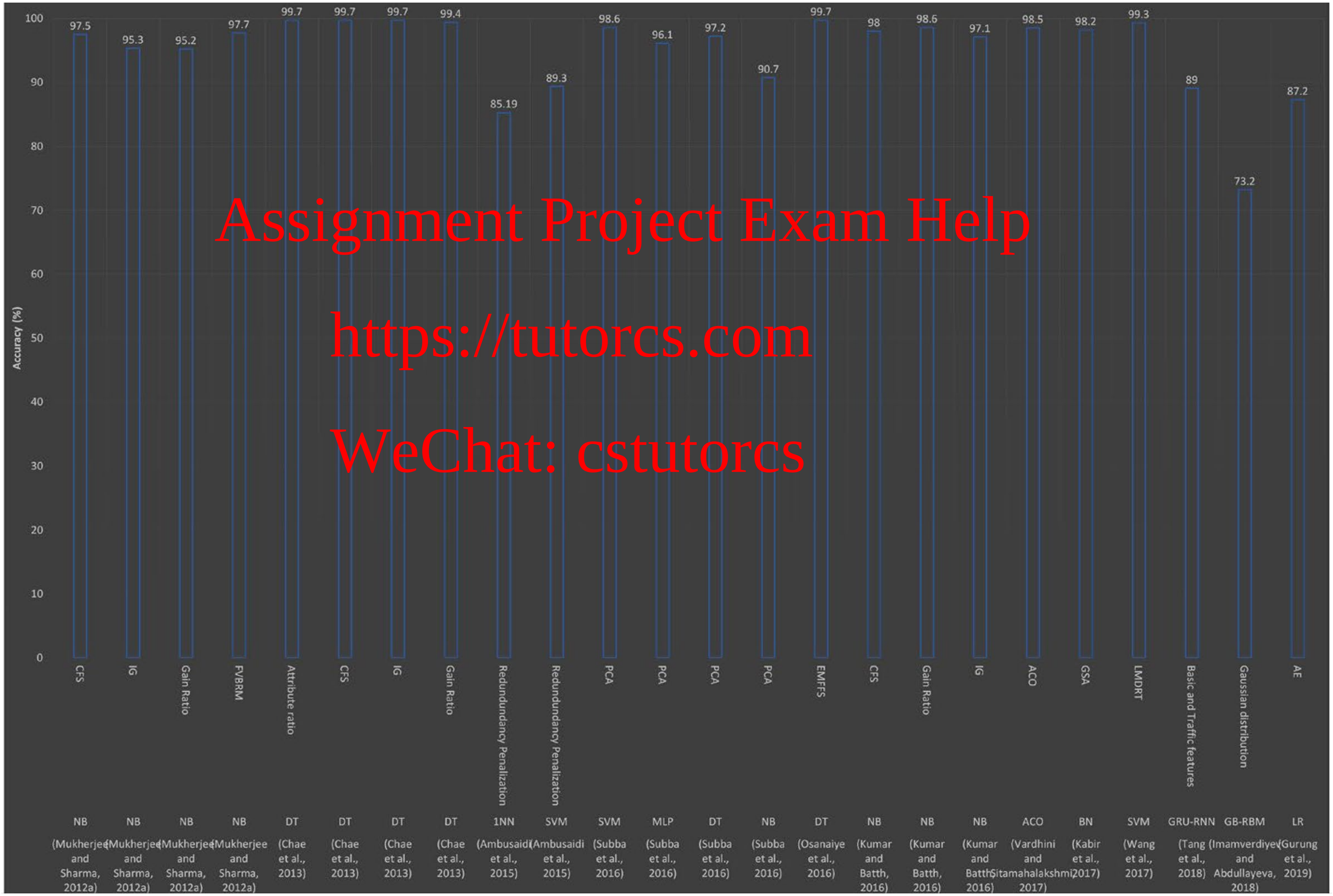
Botnet Detection – KDD Cup 99

- Accuracy comparison on KDD Cup 99 [4]



Botnet Detection – NSL KDD

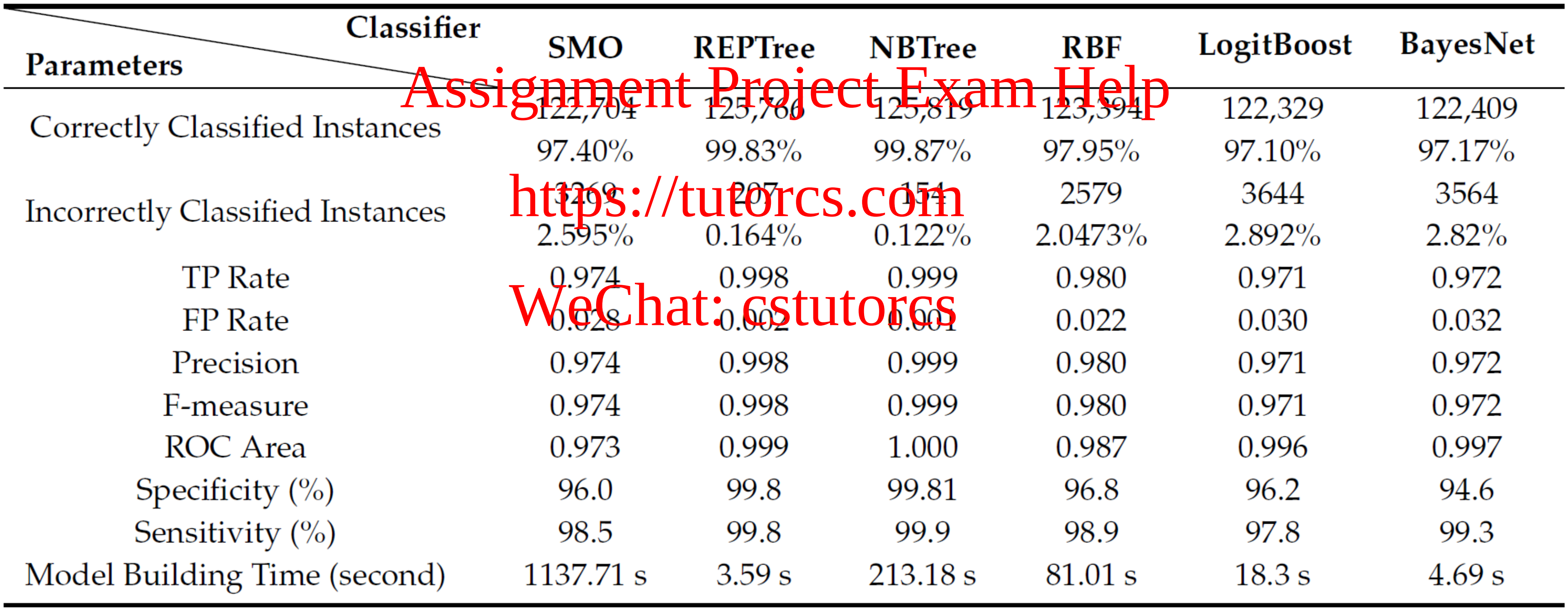
- Accuracy comparison on NSL KDD [4]



Botnet Detection – NSL KDD

- Performance comparison of six classifiers [3]

Table 2. Performance of the six classifiers using 10-fold cross-validation.

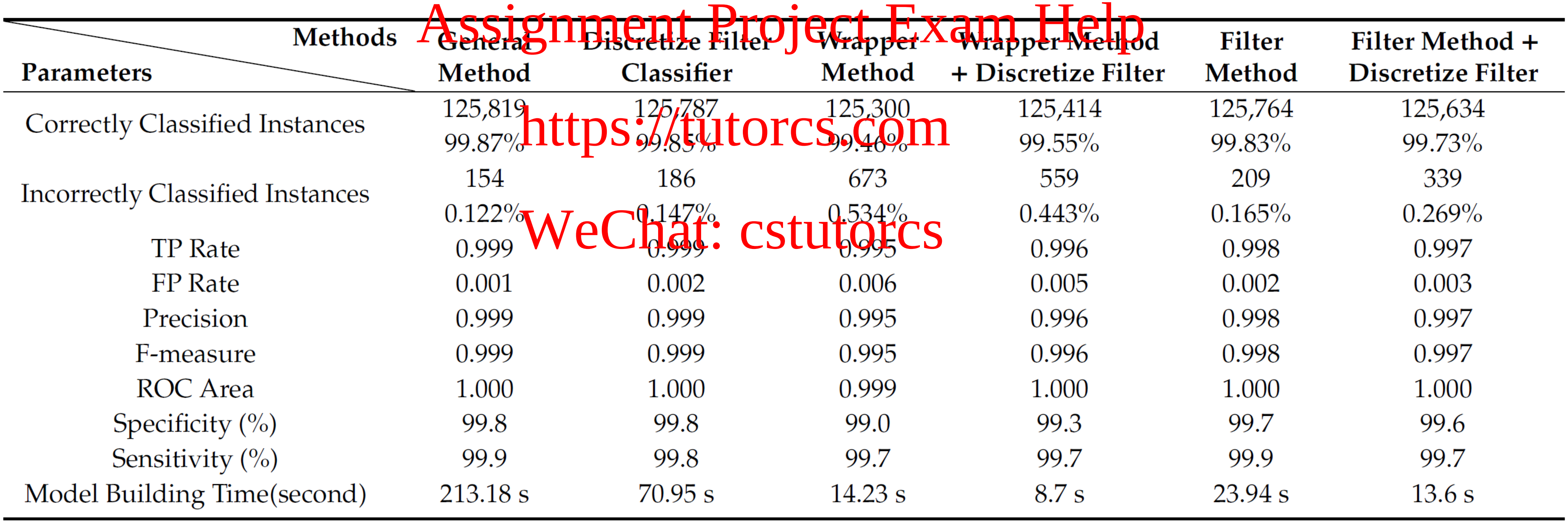


Classifier Parameters	SMO	REPTree	NBTree	RBF	LogitBoost	BayesNet
Correctly Classified Instances	122,704	125,766	125,819	123,394	122,329	122,409
	97.40%	99.83%	99.87%	97.95%	97.10%	97.17%
Incorrectly Classified Instances	3269	207	154	2579	3644	3564
	2.595%	0.164%	0.122%	2.0473%	2.892%	2.82%
TP Rate	0.974	0.998	0.999	0.980	0.971	0.972
FP Rate	0.028	0.002	0.001	0.022	0.030	0.032
Precision	0.974	0.998	0.999	0.980	0.971	0.972
F-measure	0.974	0.998	0.999	0.980	0.971	0.972
ROC Area	0.973	0.999	1.000	0.987	0.996	0.997
Specificity (%)	96.0	99.8	99.81	96.8	96.2	94.6
Sensitivity (%)	98.5	99.8	99.9	98.9	97.8	99.3
Model Building Time (second)	1137.71 s	3.59 s	213.18 s	81.01 s	18.3 s	4.69 s

Botnet Detection – NSL KDD

- Impact of feature selection on the performance [3]

Table 11. Performance of the NBTree classifier on the NSL-KDD training dataset using different feature selection/reduction methods.



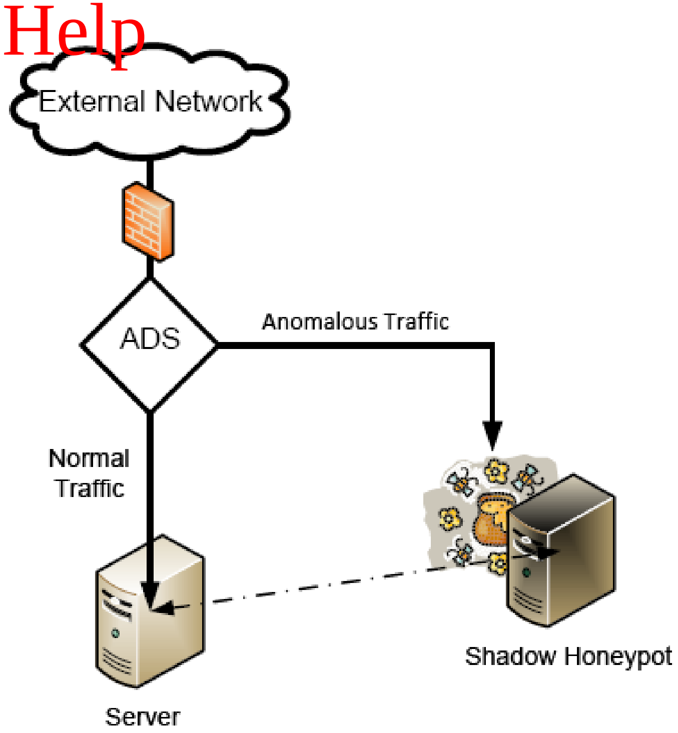
Parameters \ Methods	General Method	Discretize Filter Classifier	Wrapper Method	Wrapper Method + Discretize Filter	Filter Method	Filter Method + Discretize Filter
Correctly Classified Instances	125,819 99.87%	125,787 99.85%	125,300 99.46%	125,414 99.55%	125,764 99.83%	125,634 99.73%
Incorrectly Classified Instances	154 0.122%	186 0.147%	673 0.534%	559 0.443%	209 0.165%	339 0.269%
TP Rate	0.999	0.999	0.995	0.996	0.998	0.997
FP Rate	0.001	0.002	0.006	0.005	0.002	0.003
Precision	0.999	0.999	0.995	0.996	0.998	0.997
F-measure	0.999	0.999	0.995	0.996	0.998	0.997
ROC Area	1.000	1.000	0.999	1.000	1.000	1.000
Specificity (%)	99.8	99.8	99.0	99.3	99.7	99.6
Sensitivity (%)	99.9	99.8	99.7	99.7	99.9	99.7
Model Building Time(second)	213.18 s	70.95 s	14.23 s	8.7 s	23.94 s	13.6 s

Overview

- Botnet, DDoS detection
  - Feature selection
  - Performance comparison
  - Honeypot-based analysis
- DDoS prevention
  - Ingress/egress filtering
  - Router-based filtering
- DDoS reaction
  - Destination-end
  - Intermediate network
  - Source-end

Botnet Detection

- Honeypot-based analysis
  - Mimic the actual server to trap the attacker
  - Deliberately expose vulnerabilities/materials
  - Educational purposes vs security purposes
  - Limitations
    - Encrypted traffic
    - Unknown attacks
    - Attacker may move laterally to infiltrate the real production network



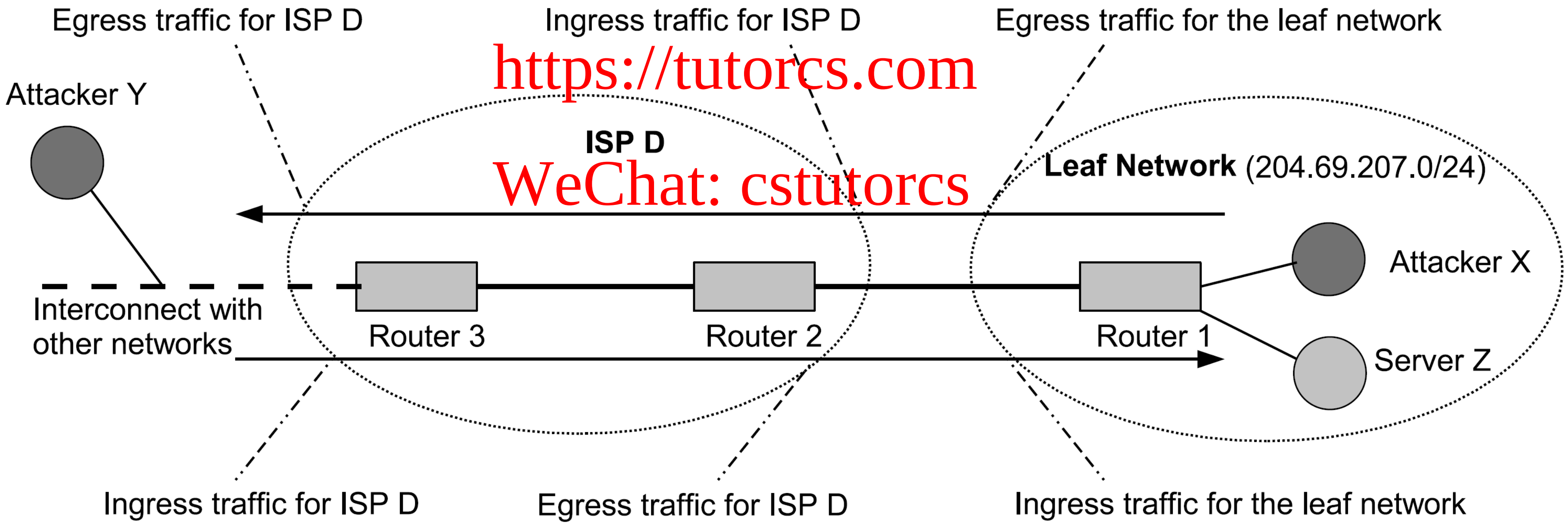
https://www.cse.wustl.edu/~jain/cse571-09/ftp/honey/

Overview

- Botnet, DDoS detection
  - Feature selection
  - Performance comparison
  - Honeypot-based analysis
- DDoS prevention
  - Ingress/egress filtering
  - Router-based filtering
- DDoS reaction
  - Destination-end
  - Intermediate network
  - Source-end

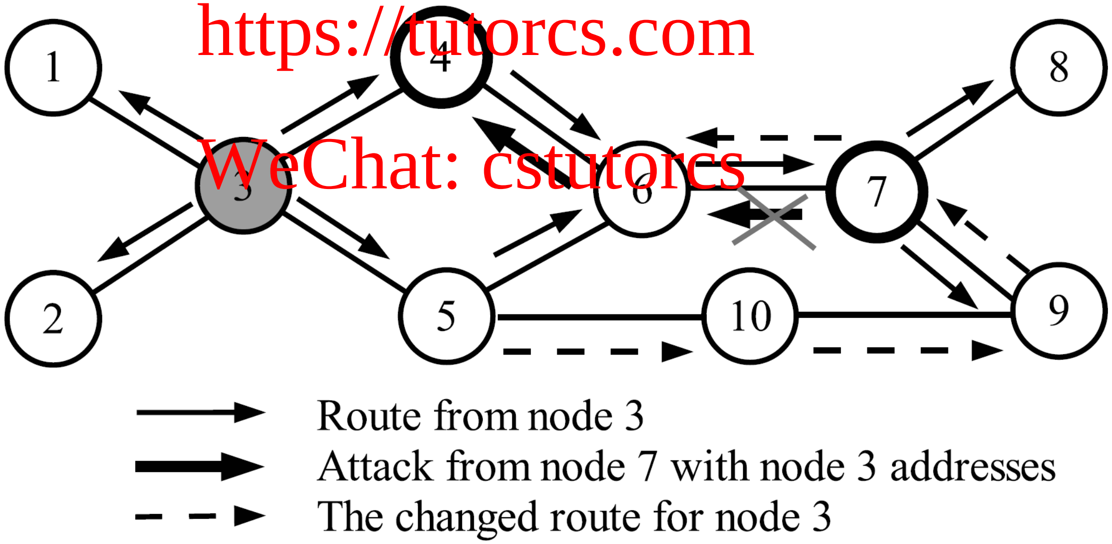
DDoS Prevention

- Ingress/egress filtering [2]: only allow traffic to enter/leave the network if its source addresses are within the expected IP address range
  - E.g., Router 1 only allows packets having a source IP address with the 204.69.207.0/24 prefix to leave the network


Egress traffic for ISP D
Ingress traffic for ISP D
Egress traffic for the leaf network
Attacker Y
ISP D
Leaf Network (204.69.207.0/24)
Attacker X
Interconnect with other networks
Router 3
Router 2
Router 1
Server Z
Ingress traffic for ISP D
Egress traffic for ISP D
Ingress traffic for the leaf network

DDoS Prevention

- Router-based filtering: use information about the BGP routing topology to filter traffic with spoofed source addresses
  - E.g., attack traffic from AS7 (spoofed as AS3) to AS4; router-based filtering deployed at AS6; attack traffic from AS7 can be filtered if AS6 knows the BGP routing topology

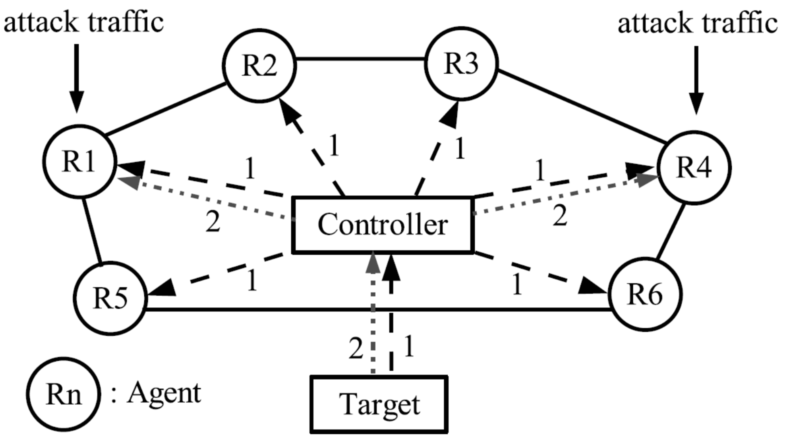

1
4
8
3
6
7
2
5
10
9
Route from node 3
Attack from node 7 with node 3 addresses
The changed route for node 3

Overview

- Botnet, DDoS detection
  - Feature selection
  - Performance comparison
  - Honeypot-based analysis
- DDoS prevention
  - Ingress/egress filtering
  - Router-based filtering
- DDoS reaction
  - Destination-end
  - Intermediate network
  - Source-end

DDoS Reaction

- Destination/target-end reaction
  - Bottleneck resource management: protect bottleneck resource
  - E.g., expanding server capacity, history-based IP filtering
- Intermediate network reaction
  - Filter attack traffic close to attack sources
  - E.g., agent-controller model
- Source-end reaction
  - Filter attack traffic at the source
  - E.g., D-WARD

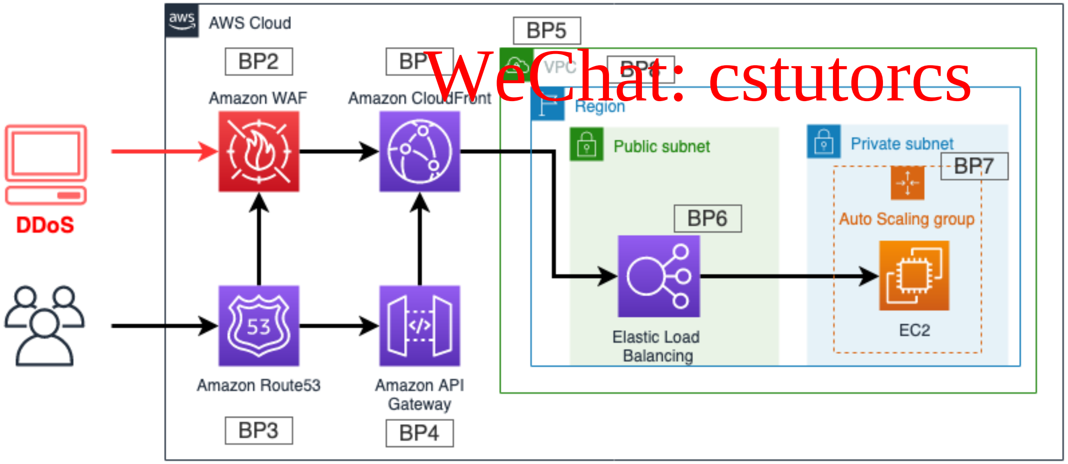


1. The target detects attacks and agents are directed to mark all the incoming packets to the victim.
2. The target locates attack entry points and asks relating agents to filter attack traffic

Agent-controller model

DDoS Reaction

- Mitigation Techniques at AWS
  - Infrastructure Layer Defence
    - Amazon EC2 with Auto Scaling
    - Choice of Region
    - Elastic Load Balancing
  - Application Layer Defence



https://docs.aws.amazon.com/whitepapers/latest/aws-best-practices-ddos-resiliency/mitigation-techniques.html

Summary

- Examples of Botnet/DDoS detection on KDD Cup, NSL KDD
  - Feature selection
    - Example 1: information gain applied on KDD Cup
    - Example 2: CFS applied on NSL KDD
  - Performance comparison
    - Feature selection can reduce model building time without impacting the performance
- DDoS prevention
  - Ingress/egress filtering at leaf networks
  - Router-based filtering
- DDoS reaction
  - Destination-end, intermediate network, source-end

Reference

- [1] Kayacik, H.G., Zincir-Heywood, A.N., Heywood, M.I.: Selecting Features for Intrusion Detection: A Feature Relevance Analysis on KDD 99 Intrusion Detection Datasets. In: Proc. of the Third Annual Conference on Privacy, Security and Trust (2005)
- [2] M. A. Hall (1998). Correlation-based Feature Subset Selection for Machine Learning. Hamilton, New Zealand.
- [3] Alabdulwahab, Saleh & Moon, Bong-Kyo. (2020). Feature Selection Methods Simultaneously Improve the Detection Accuracy and Model Building Time of Machine Learning Classifiers. Symmetry. 12. 1424. 10.3390/sym12091424.
- [4] Thakkar, A., Lohiya, R. A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions. *Artif Intell Rev* (2021). https://doi.org/10.1007/s10462-021-10037-9

Reference

- [5] Eric Chou and Rich Groves, 2016, Distributed Denial of Service, O'Reilly Media, Inc.
- [6] Tao Peng, Chris Leckie, and Katagiri Ramamohanorao, *Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems*, ACM Computing Surveys

THE UNIVERSITY OF
MELBOURNE

The Business Context for Cybersecurity Management

COMP90073
Security Analytics

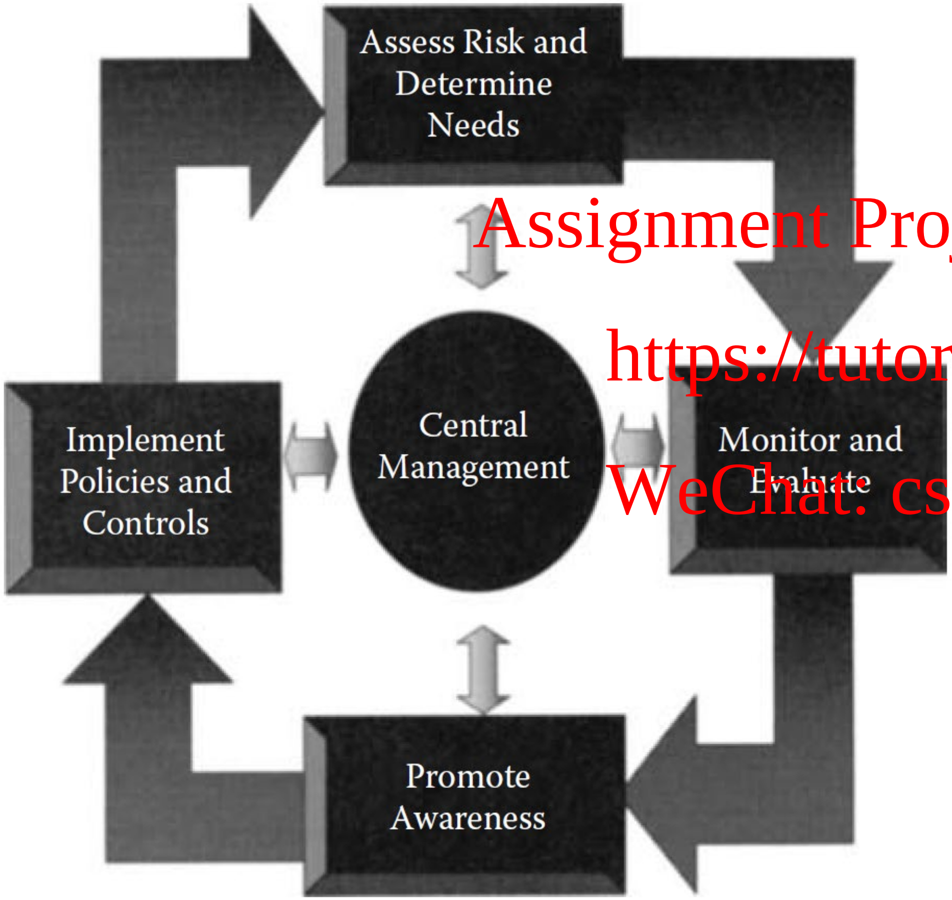
Dr. Yi Han, CIS

Semester 2, 2021

Outline

- Security and Risk Management Practice
- Information Security Management Governance
- Organizational Behaviour
- Ethics

Security and Risk Management Practice


Assess Risk and Determine Needs
Implement Policies and Controls
Central Management
Monitor and Evaluate
Promote Awareness

Security and Risk Management relationships (Source: [1])

- Security management ensures
  - Risks are identified
  - An adequate control environment is established to mitigate the risks
  - Interrelationships among
    - Assessing risk
    - Implementing policies and controls in response to the risks
    - Promoting awareness of the expectations
    - Monitoring the effectiveness of the controls

Information Security Management Governance

- According to IT Governance Institute (ITGI)

The Board of Directors should

- Be informed about information security
- Set direction to drive policy and strategy
- Provide resources to security efforts
- Assign management responsibilities
- Set priorities
- Support changes required
- Define cultural values related to risk assessment
- Obtain assurance from internal or external auditors
- Insist that security investments are made measurable and reported on for program effectiveness

Information Security Management Governance

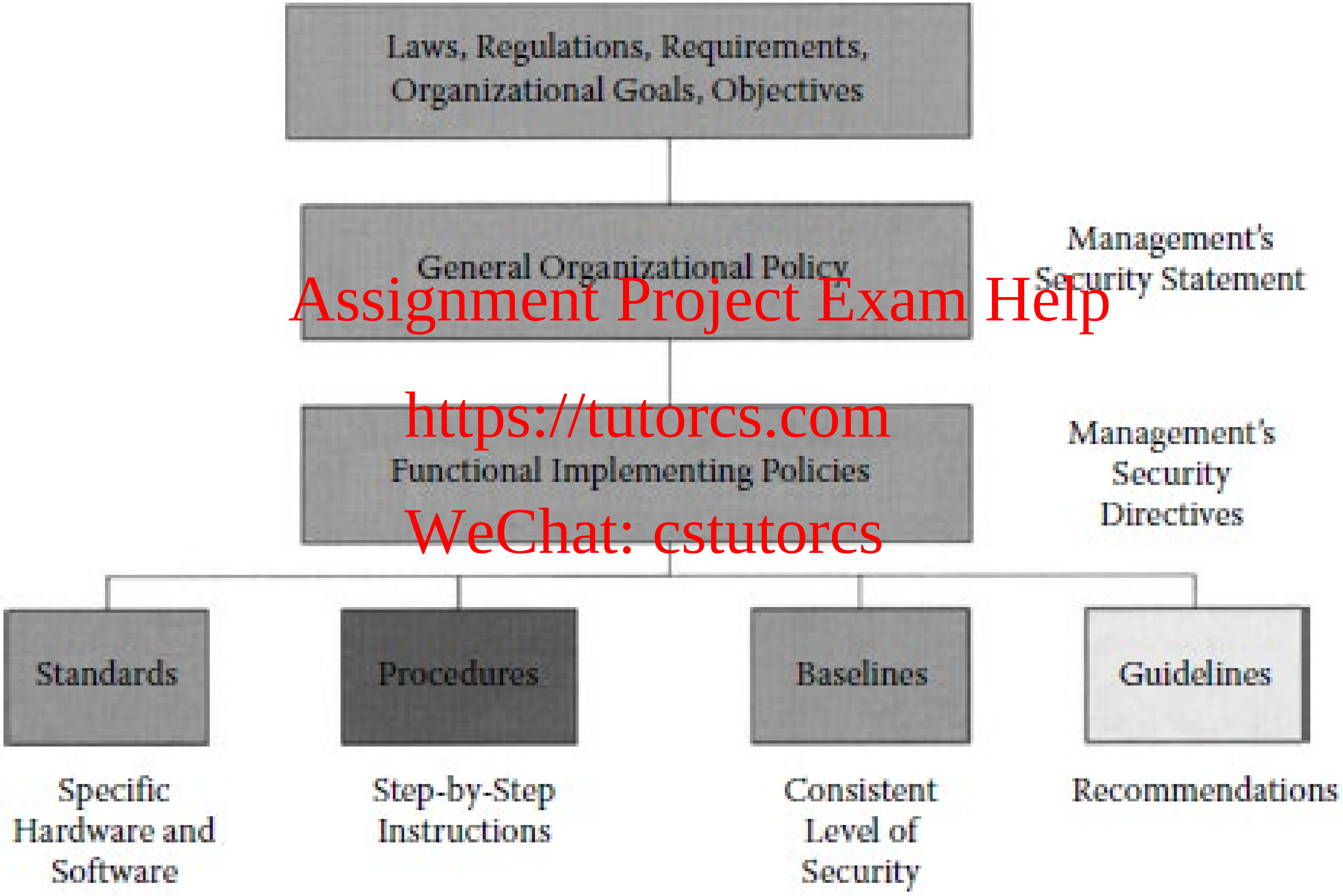
The Management should

- Write security policies with business input
- Ensure that roles and responsibilities are defined and clearly understood
- Identify threats and vulnerabilities
- Implement security infrastructures and control frameworks (standards, guidelines, baselines, and procedures)
- Ensure that policy is approved by the governing body
- Establish priorities and implement security projects in a timely manner
- Monitor breaches
- Conduct periodic reviews and tests
- Reinforce awareness education as critical
- Build security into the systems development life cycle

Information Security Management Governance

- Security Policies, Procedures, Standards, Guidelines, and Baselines
- What's Risk Management
- Risk Management Principles
- Risk Assessment

Security Policies, Procedures, Standards, Guidelines, and Baselines


Laws, Regulations, Requirements, Organizational Goals, Objectives
General Organizational Policy
Management's Security Statement
Functional Implementing Policies
Management's Security Directives
Standards
Procedures
Baselines
Guidelines
Specific Hardware and Software
Step-by-Step Instructions
Consistent Level of Security
Recommendations

Relationships among policies, standards, procedures, baselines, and guidelines (Source: [1])

What’s Risk Management

- “*A discipline for living with the possibility that future events may cause harm, it reduces risks by defining and controlling threats and vulnerabilities*”

  - by (ISC)² (The International Information System Security Certification Consortium)

Risk Management Principles

- **Risk avoidance**

  The practice of coming up with alternatives so that the risk in question is not realized

  e.g., Parents won't allow underage child to drive the family car to avoid the risks of poor driving performance or the cost of insurance for the child

- **Risk transfer**

  The practice of passing on the risk in question to another entity, such as an insurance company

Risk Management Principles

- **Risk mitigation**

  The practice of the elimination of, or the significant decrease in the level of risk presented

  e.g., Organizations put countermeasures in place such as firewalls, IDSs/IPSs, and other mechanisms to deter malicious outsiders from accessing personal and financial information to lessen the risk of exposing this highly sensitive and confidential information

- **Risk acceptance**

  The practice of accepting certain risk(s), typically based on a business decision that may also weigh the cost versus the benefit of dealing with the risk in another way

Risk Assessment

- Identify vulnerabilities
- Identify threats
- Qualitative assessment
- Quantitative assessment
- Reporting findings
- Countermeasure selection
- Information valuation

Risk Assessment

- Identify Vulnerabilities
  - Vulnerability: "*a flaw* or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy" – by NIST (National Institute of Standards and Technology)
  - Examples of vulnerabilities
    - Absence of a receptionist, mantrap, or other physical security mechanism upon entrance to a facility
    - Inadequate integrity checking in financial transaction software
    - Neglecting to require users to sign an acknowledgment of their responsibilities with regard to security, as well as an acknowledgment that they have read, understand, and agree to abide by the organization's security policies
    - Patching and configuration of an organization's information systems are done on an ad hoc basis, and, therefore, are neither documented nor up to date

Risk Assessment

- Identify Threats
  - Threats: "*the potential for a particular threat-source to successfully exercise a particular vulnerability*" – by NIST
  - Threat source: "*either (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) a situation and method that may accidentally trigger a vulnerability*" – by NIST

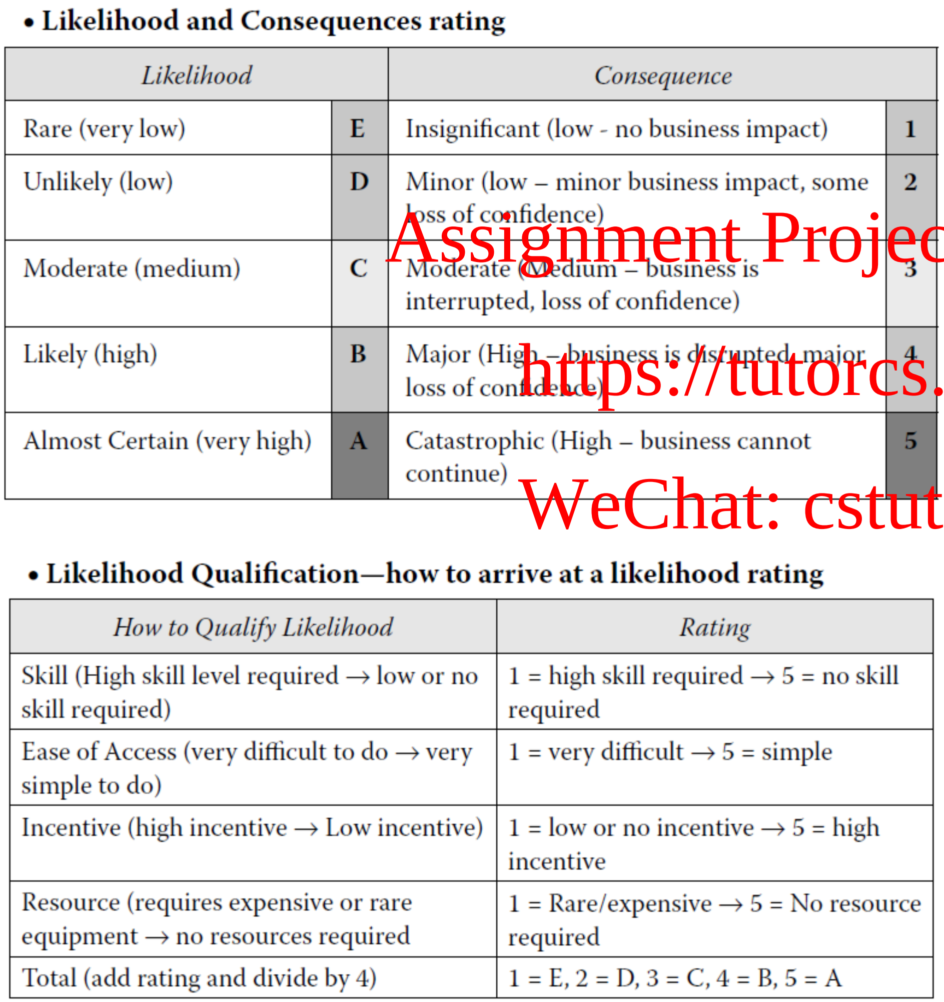
Risk Assessment

– Threat source category

- **Human**: Malicious outsider, malicious insider, (bio)terrorist, saboteur, spy political or competitive operative, loss of key personnel, errors made by human intervention, cultural issues
- **Natural**: Fire, flood, tornado, hurricane, snow storm, earthquake
- **Technical**: Hardware failure, software failure, malicious code, unauthorized use, use of emerging services, such as wireless, new technologies
- **Physical**: Closed-circuit TV failure, perimeter defence failure
- **Environmental**: Hazardous waste, biological agent, utility failure
- **Operational**: A process (manual or automated) that affects confidentiality, integrity, or availability

Qualitative Assessment

- Determination of likelihood and impact



- **Likelihood and Consequences rating**

Likelihood		*Consequence*	
Rare (very low)	E	Insignificant (low - no business impact)	1
Unlikely (low)	D	Minor (low – minor business impact, some loss of confidence)	2
Moderate (medium)	C	Moderate (Medium – business is interrupted, loss of confidence)	3
Likely (high)	B	Major (High – business is disrupted, major loss of confidence)	4
Almost Certain (very high)	A	Catastrophic (High – business cannot continue)	5

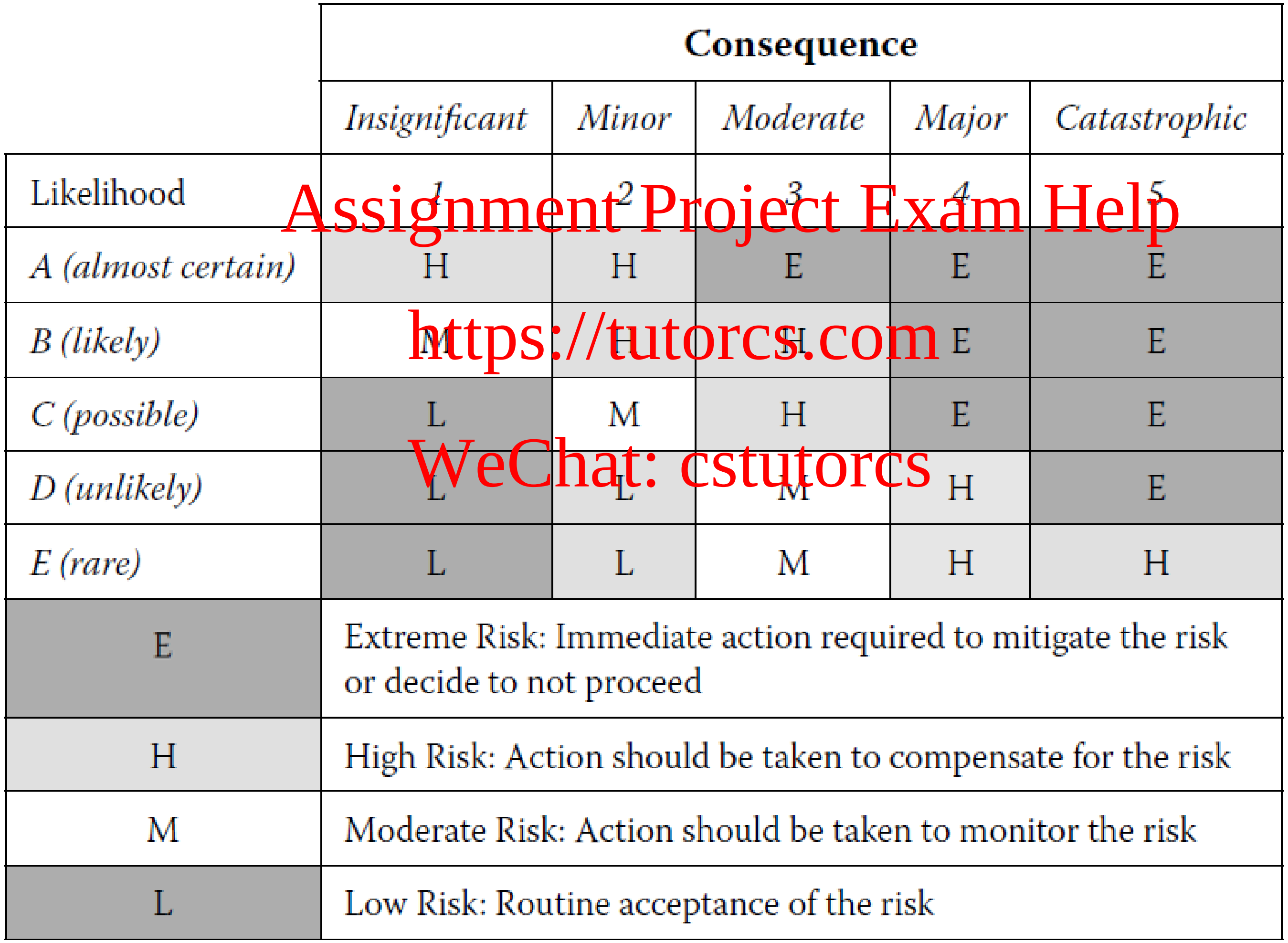
- **Likelihood Qualification—how to arrive at a likelihood rating**

How to Qualify Likelihood	*Rating*
Skill (High skill level required → low or no skill required)	1 = high skill required → 5 = no skill required
Ease of Access (very difficult to do → very simple to do)	1 = very difficult → 5 = simple
Incentive (high incentive → Low incentive)	1 = low or no incentive → 5 = high incentive
Resource (requires expensive or rare equipment → no resources required	1 = Rare/expensive → 5 = No resource required
Total (add rating and divide by 4)	1 = E, 2 = D, 3 = C, 4 = B, 5 = A

Rating likelihood and consequences (Source: [1])

Qualitative Assessment

- Determination of risk - the product of likelihood and impact



	Consequence				
	Insignificant	*Minor*	*Moderate*	*Major*	*Catastrophic*
Likelihood	*1*	*2*	*3*	*4*	*5*
A (almost certain)	H	H	E	E	E
B (likely)	M	H	H	E	E
C (possible)	L	M	H	E	E
D (unlikely)	L	L	M	H	E
E (rare)	L	L	M	H	H

E	Extreme Risk: Immediate action required to mitigate the risk or decide to not proceed
H	High Risk: Action should be taken to compensate for the risk
M	Moderate Risk: Action should be taken to monitor the risk
L	Low Risk: Routine acceptance of the risk

ANZ 4360 risk levels (Source: [1])

Qualitative Assessment

- Example
  - An exploit has a likelihood of 4 (high) and an impact of 3 (moderate), what is the risk level?

Answer: High risk

Quantitative Assessment

- **Single loss expectancy (SLE)**: the difference between the original value and the remaining value of an asset after a single exploit

SLE = asset value (in $) × exposure factor (loss in successful threat exploit, as %)

- **Annualized rate of occurrence (ARO)**: an estimate of how often a threat will be successful in exploiting a vulnerability over the period of a year

- **Annualized loss expectancy (ALE)**: a product of the yearly estimate for the exploit (ARO) and the loss in value of an asset after a single exploitation (SLE)

ALE = ARO × SLE

Quantitative Assessment

- Example
  - Company A’s intellectual property on racing car design is worth $600,000, the exposure factor is 80%, and the annualized rate of occurrence is 5%. What’s the annualized loss expectancy?

Answer:

SLE = $600,000 x 80% = $480,000

ALE = ARO x SLE = 5% x $480,000 = $24,000

Risk Assessment

- Reporting findings
  - Once the findings from the assessment have been consolidated and the calculations have been completed, it is time to present a finalized report to senior management

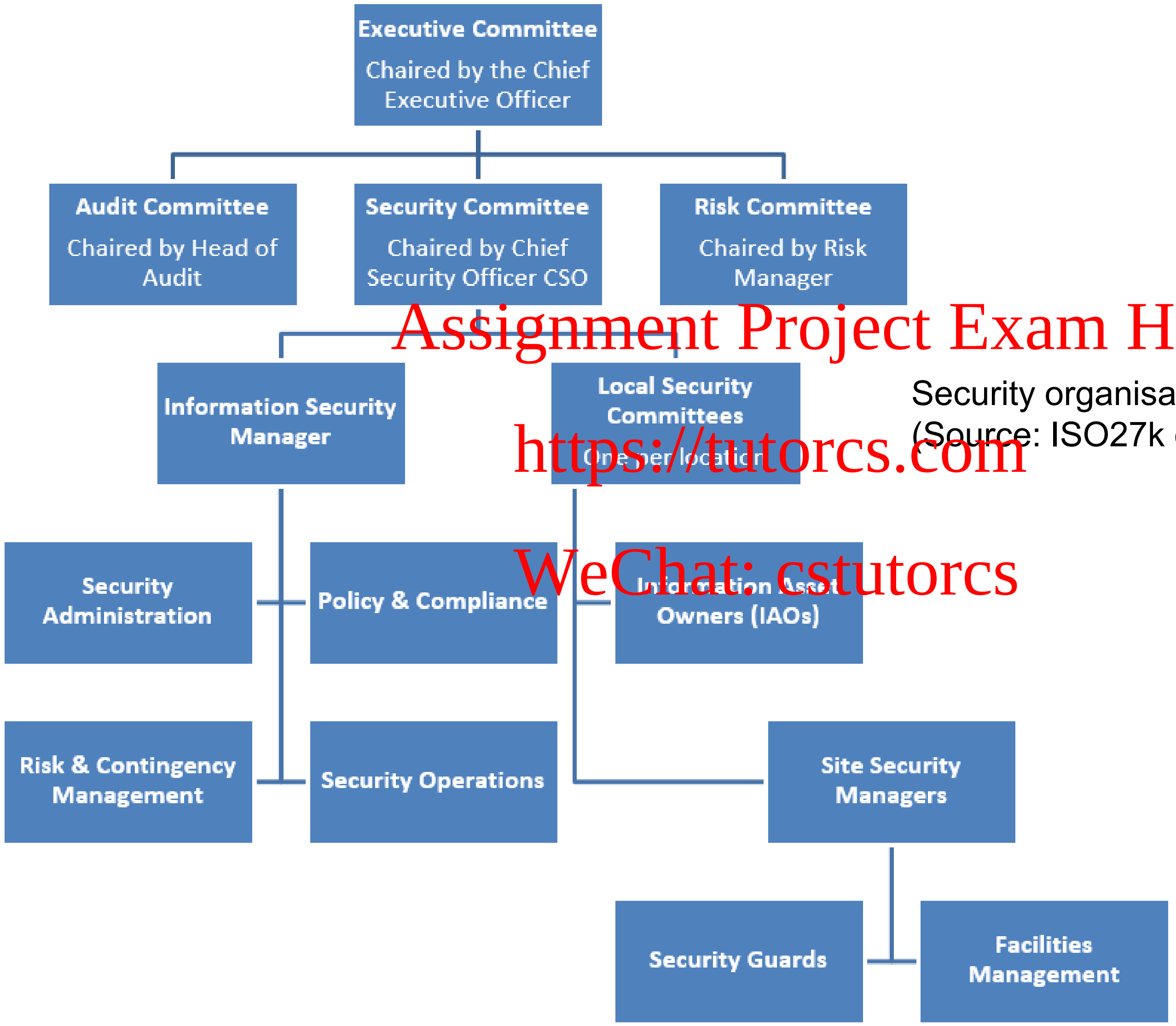
- Countermeasure selection
  - Considerations for countermeasures
    - Accountability (can be held responsible)
    - Auditability (can it be tested?)
    - Publicly available, simple design (the construction and the nature of the countermeasure are not secret)
    - Trusted source (source is known)
    - Independence (self-determining)
    - Consistently applied
    - Cost-effective
    - Reliable
    - Distinct from other countermeasures (no overlap)

Risk Assessment

  - Ease of use
  - Minimum manual intervention
  - Sustainable
  - Secure
  - Protects confidentiality, integrity, and availability of assets
  - Can be "backed out" in event of issue
  - Creates no additional issues during operation
  - Leaves no residual data from its function

- Information valuation
  - Periodically attempt to properly value information assets, as information may lose its value
    - Over time
    - If it is modified, improperly disclosed
    - Not had its proper value calculated

Organizational Behavior – Structure



Executive Committee
Chaired by the Chief Executive Officer

Audit Committee
Chaired by Head of Audit

Security Committee
Chaired by Chief Security Officer CSO

Risk Committee
Chaired by Risk Manager

Information Security Manager

Local Security Committees
One per location

Security Administration

Policy & Compliance

Information Asset Owners (IAOs)

Risk & Contingency Management

Security Operations

Site Security Managers

Security Guards

Facilities Management

Security organisational structure
(Source: ISO27k organization of information security)

Organizational Behaviour – Best Practices

- Job rotation
- Separation of duties
- Least privilege
- Mandatory vacations
- Job position sensitivity
- Budget for Information Security Activities
- Policies, Procedures, Baselines, Standards, and Guidelines
- Security Awareness Program
- Understand Business Objectives

- Maintain Awareness of Emerging Threats and Vulnerabilities
- Evaluate Security Incidents and Response
- Develop Security Compliance Program
- Establish Security Metrics
- Participate in Management Meetings
- Ensure Compliance with Government and Industry Regulations
- Assist Internal and External Auditors
- Stay Abreast of Emerging Technologies

Ethics

- Common computer ethics fallacies
  - Computer game fallacy
    - Computer users tend to think that computers will generally prevent them from cheating and doing wrong
  - Law-abiding citizen fallacy
    - Sometimes users confuse what is legal with regard to computer use with what is reasonable behaviour for using computers. Laws basically define the minimum standard about which actions can be reasonably judged, but such laws also call for individual judgment
  - Shatterproof fallacy
    - Computer users believe that they can do little harm accidentally with a computer beyond perhaps erasing or messing up a file

Ethics

- Candy-from-a-baby fallacy
  - Illegal and unethical activity, such as software piracy and plagiarism, are very easy to do with a computer. However, just because it is easy does not mean that it is right
- Hacker fallacy
  - Numerous reports and publications of the commonly accepted hacker belief is that it is acceptable to do anything with a computer as long as the motivation is to learn and not to gain or make a profit from such activities
- Free information fallacy
  - The notion that information “wants to be free” ignores the fact the copying and distribution of data are completely under the control of the author who allow it to happen

Ethics

- Sample code of conduct - (ISC)^2
  - Code of Ethics Preamble
    - Safety of the commonwealth, duty to our principals, and to each other requires that we adhere, and be seen to adhere, to the highest ethical standards of behaviour
  - Code of Ethics Canons
    - Protect society, the commonwealth, and the infrastructure
      - Promote and preserve public trust and confidence in information and systems
      - Promote the understanding and acceptance of prudent information security measures
      - Preserve and strengthen the integrity of the public infrastructure
      - Discourage unsafe practice

Ethics

- Act honourably, honestly, justly, responsibly, and legally
  - Tell the truth; make all stakeholders aware of your actions on a timely basis
  - Observe all contracts and agreements, express or implied
  - Treat all constituents fairly. In resolving conflicts, consider public safety and duties to principals, individuals, and the profession in that order
  - Give prudent advice; avoid raising unnecessary alarm or giving unwarranted comfort. Take care to be truthful, objective, cautious, and within your competence
  - When resolving differing laws in different jurisdictions, give preference to the laws of the jurisdiction in which you render your service

Ethics

- Provide diligent and competent service to principals
  - Preserve the value of their systems, applications, and information
  - Respect their trust and the privileges that they grant you
  - Avoid conflicts of interest or the appearance thereof
  - Render only those services for which you are fully competent and qualified

- Advance and protect the profession
  - Sponsor for professional advancement those best qualified. All other things equal, prefer those who are certified and who adhere to these canons. Avoid professional association with those whose practices or reputation might diminish the profession
  - Take care not to injure the reputation of other professionals through malice or indifference
  - Maintain your competence; keep your skills and knowledge current. Give generously of your time and knowledge in training others

Summary

- Security and Risk Management Practice
  - Explain relationships of security and risk management
- Information Security Management Governance
  - Describe risk management and four risk management principles
  - Explain risk assessment process
  - Determine qualitative risks
  - Calculate quantitative risks
- Organizational Behaviour
  - Understand best practices
- Ethics
  - Explain common computer ethics fallacies

Reference

- [1] Harold F. Tipton, 2010, *Official (ISC)2 guide to the CISSP CBK, Second Edition*, SciTech Book News