IN2120 Information Security
University of Oslo
Autumn 2018

Review

Audun Jøsang and Nils Gruschka

General Security Concepts

- Understand information security properties/services
  - Definition of information security (ISO27000)
  - Definitions of CIA (Confidentiality, Integrity and Availability) services
  - Privacy and GDPR
- Meaning of, and difference between other security concepts
  - authentication
  - non-repudiation
  - access control
  - authorization
- Perspectives on security controls:
  - 3 categories of security controls: physical, technical, administrative
  - Preventive, detective, corrective security controls.
  - Security controls during storage, transmission, processing.

Security Management

- Know what ISO27K series is about
- ISO27000, ISO27001& ISO27002
  - Title and purpose of each standard
- Elements of ISMS (cycle)

Cryptography

- Hash functions and symmetric ciphers
  - Status/usage of SHA-1, SHA-2 and SHA-3
  - Parameters (block and key size) of AES
  - Applications
- MAC (Message Authentication Code)
  - Basic principle: keyed hash function
  - Security services
- Asymmetric ciphers + Key Exchange
  - Understand usage of keys in encryption and digital signature
  - Digital signature, security services
- Threat to classical crypto from quantum computing

Key Management

- Crypto period
- Key distribution problem. Understand requirements for
  - Key distributions with and without PKI
  - Type of protection needed (confidentiality or integrity)
- Certificates and PKI:
  - Ideas, content, issuing, managing
  - PKI trust model
  - Revocation: CRL, OCSP
  - CAA, CT

Risk Management

- Understand the factors that contribute to risk
  - Attacker/threat agent, vulnerability, impact
  - And how they are related: Understand diagram
  - Risk management process (ISO 27005)
- Threat scenario modelling:
  - Attacker centric, architecture centric, and asset centric
- Models for risk level estimation:
  - Qualitative
  - Quantitative
- Risk treatment strategies
  - Reduce, share, retain/accept, avoid

Computer Security

- Protection rings in microprocessor architecture
- Virtual machines
  - Understand hypervisor, VM/guest OS, host OS
  - Type 1 and type 2 virtualization architecture
  - Protection ring assignment to hypervisor, host, VM, apps etc.
  - Security advantages of running VMs
- Security functions supported by TPM

Incident Response and Forensics

- Elements if IR (Incident Response) policy
- Types of IR teams: permanent, virtual, hybrid
- Phases of IR

User Authentication

- Types of authentication tokens
  - Clock-based, counter-based, challenge-response
- Password storage security
  - hashing, salting
- Biometrics systems
  - Criteria for biometric characteristics
- E-Government user authentication frameworks
  - Assurance levels
  - eIDAS
  - Assurance requirement classes

Identity and Access Management

- Meaning of entity/identity/identifier/digital identity
- IAM phases (configuration and operation) with steps.
- Identity management models
  - Silo model / federated model
  - Advantages and disadvantages of silo and federated models
- Centralized/distributed federation models
- Meaning and principle of MAC, DAC, RBAC and ABAC

Communication Security

- TLS
  - Protocols
  - Security services
  - Key establishment (RSA / DH)
  - TLS stripping attack / HSTS
- VPN
  - IPSec
  - Tor

Perimeter Security

- Firewall types
  - Principles of different firewalls
  - Strengths and weaknesses
- Location of entities: DMZ or production network
- TLS inspection in firewalls
- Intrusion detection principles

Application Security

- Malware types
- What is OWASP and the top 10 vulnerabilities list
- Explain main vulnerabilities
  - SQL Injection
  - XSS - Cross-Site Scripting
  - Broken authentication and session management
- Secure Software development
  - Security by design
  - Privacy by design / Data protection

Grading Scheme

- Approximate weighing:
  - Home exam: approximately 0.4 relative weight
  - Digital exam: approximately 0.6 relative weight
- You must pass both exams to pass the course!
  - E.g. score 100% on home-ex. and score 50% on digital-ex. → total score 70% which normally gives mark C.
  - Score 100% on home exam, and score 30% on digital exam normally gives mark F.
  - Score from home exam will be available before the digital exam
- It's important that you don't fail the digital exam!
  - If digital exam score is close to 40%, the weight of the home exam is reduced, i.e. only the digital exam counts.

Digital exam

- 11. December 2018, 14:30h, Silurveien 2 (!)
- Digital exam, with a variety of question types, e.g.
  - Write text as answer
  - Fill in word / short text as answer
  - Fill in numerical value as answer
  - Select correct statement / multiple choice answers
- Related to lecture presentations and workshop questions.
  - Many workshop questions are not suitable as exam questions
- 4 hours working time
- Good Luck ☺

Exam information

- The exam contains 44 questions with a total of 100 points (= 100 %).
- The questions are grouped under 10 parts that correspond approximately to 10 of the lectures in this course.
- Be concise. When answering a question, it is often sufficient to write a single expression or sentence to describe each concept that the question asks for.
- In the navigation bar on the bottom of the screen, blue bars indicate completed questions/parts.
- Answers can be written in English or in Norwegian.

Grading

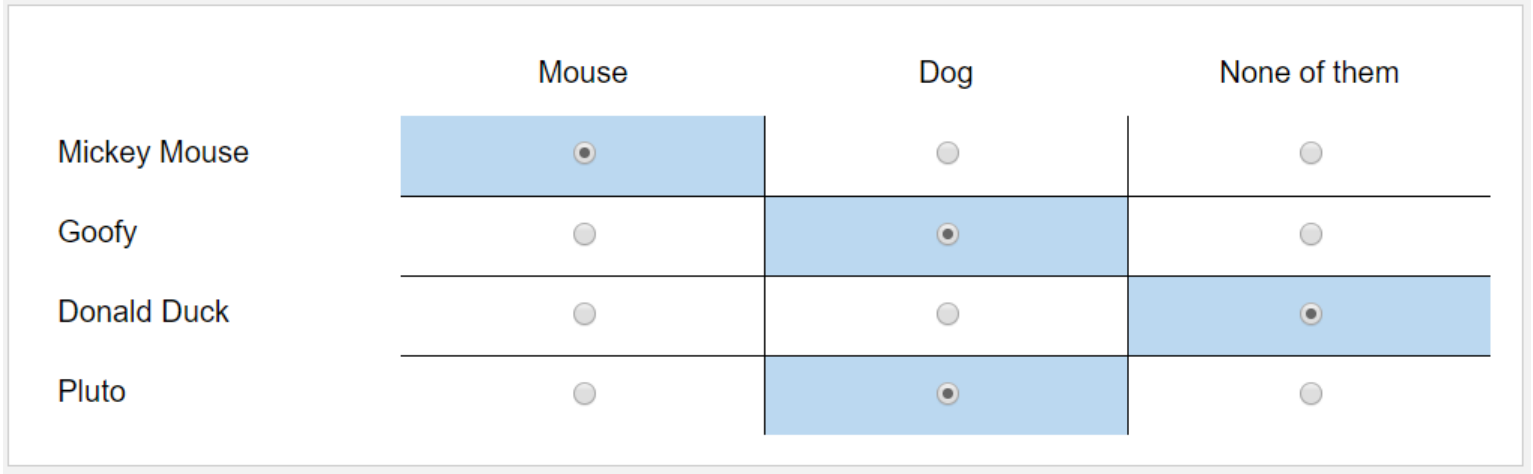
- Each question states explicitly the marking scheme. **There can be negative points for incorrect answers/selections.** However, the overall score for the total question is always at least 0 points (even if the sum over all answers is negative).

Example 1

- Select the correct species.
  Points: 1 for each correct, -1 for wrong, 0 for no selection
- **Please match the values:**

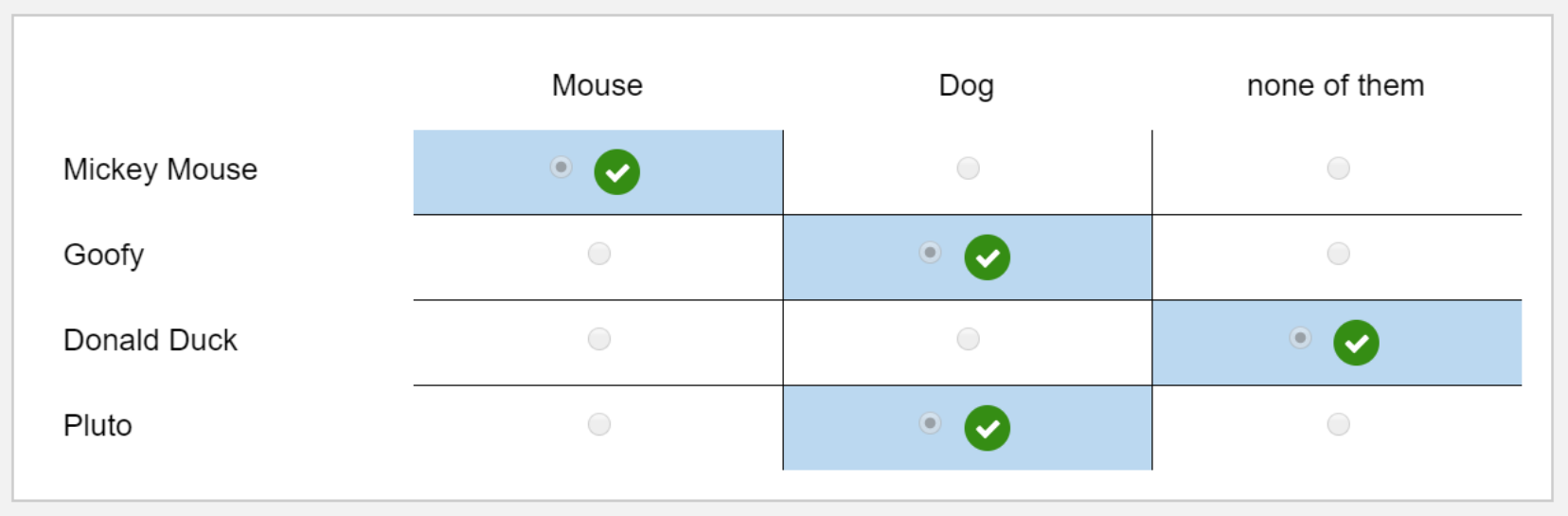
	Mouse	Dog	None of them
Mickey Mouse	○	○	○
Goofy	○	○	○
Donald Duck	○	○	○
Pluto	○	○	○

Example 1



	Mouse	Dog	None of them
Mickey Mouse	◉	○	○
Goofy	○	◉	○
Donald Duck	○	○	◉
Pluto	○	◉	○

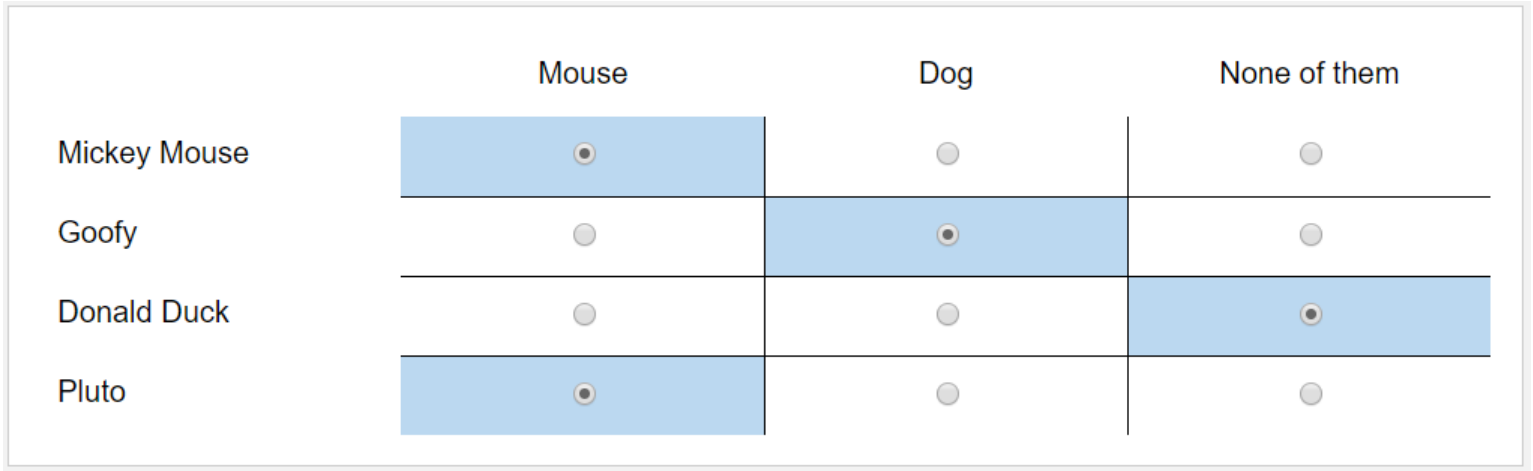
Example 1



	Mouse	Dog	none of them
Mickey Mouse	✓		
Goofy		✓	
Donald Duck			✓
Pluto		✓	

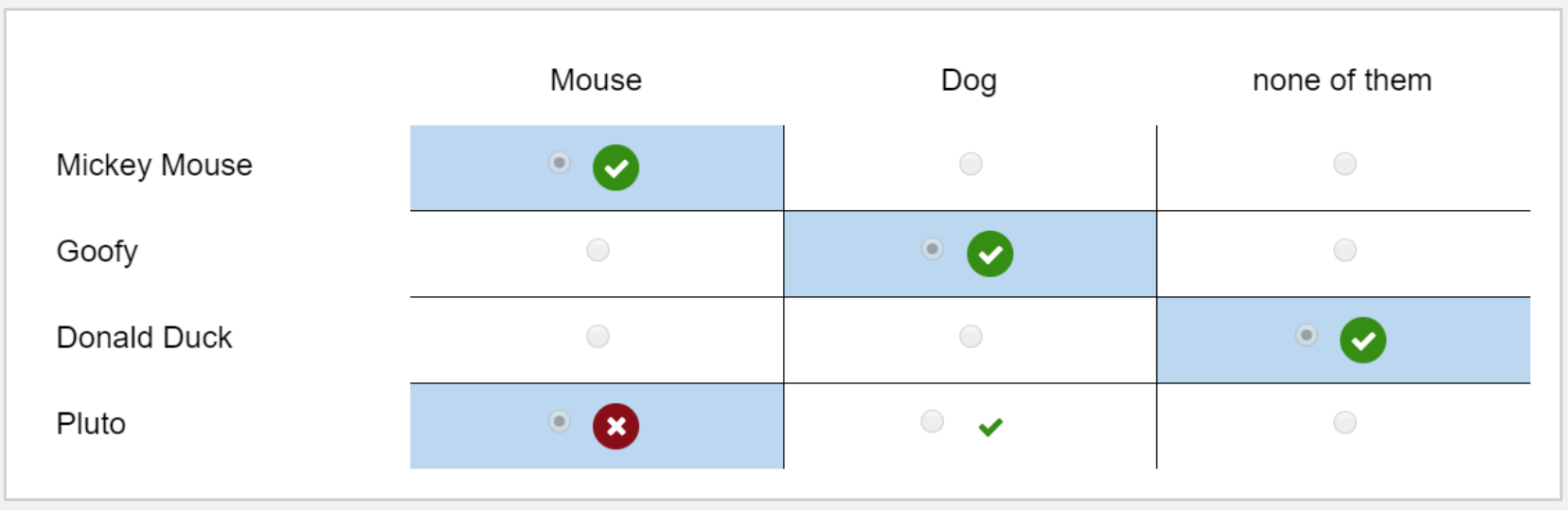
4 Points

Example 1



	Mouse	Dog	None of them
Mickey Mouse	◉	○	○
Goofy	○	◉	○
Donald Duck	○	○	◉
Pluto	◉	○	○

Example 1

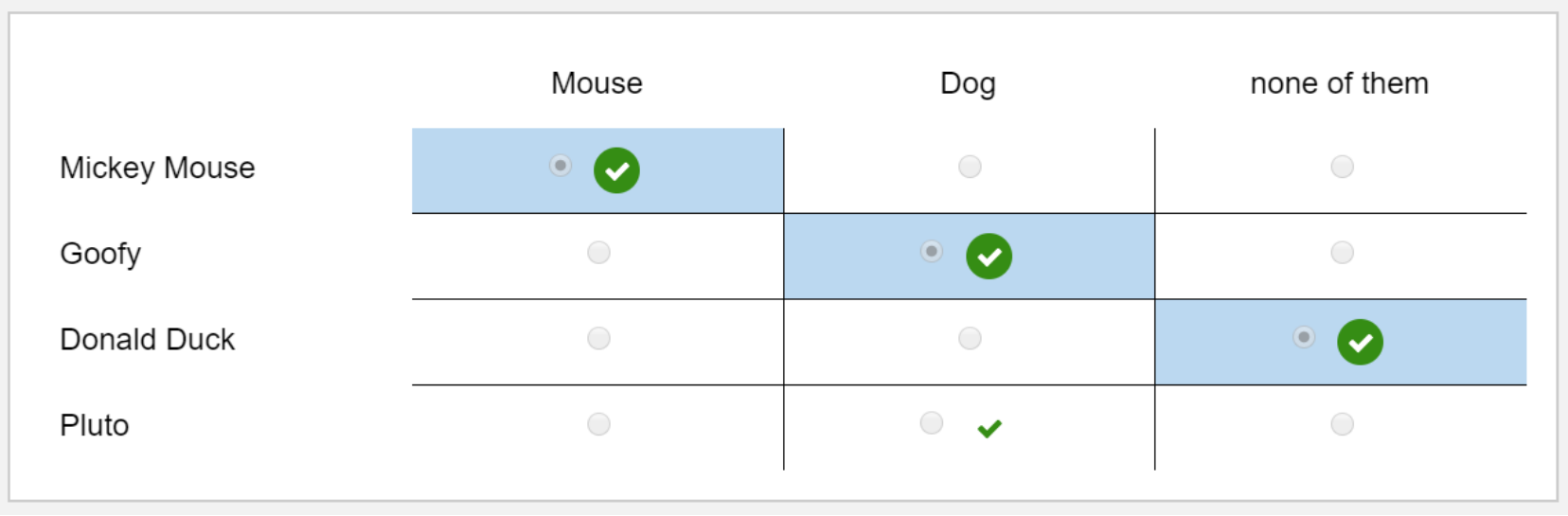


2 Points

Example 1

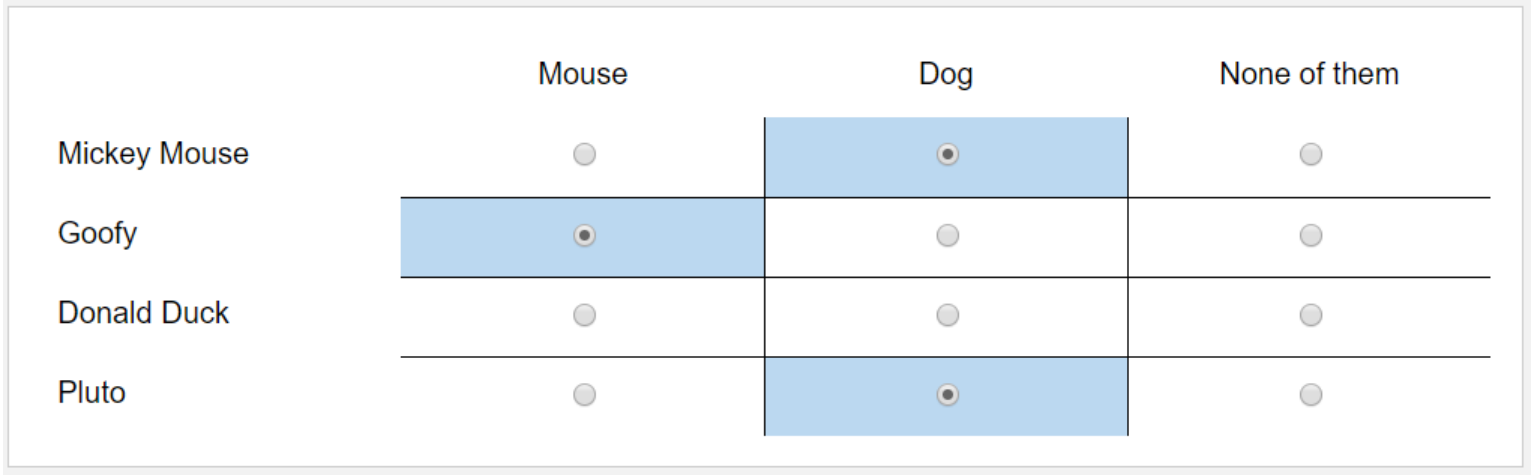
	Mouse	Dog	None of them
Mickey Mouse	◉	○	○
Goofy	○	◉	○
Donald Duck	○	○	◉
Pluto	○	○	○

Example 1



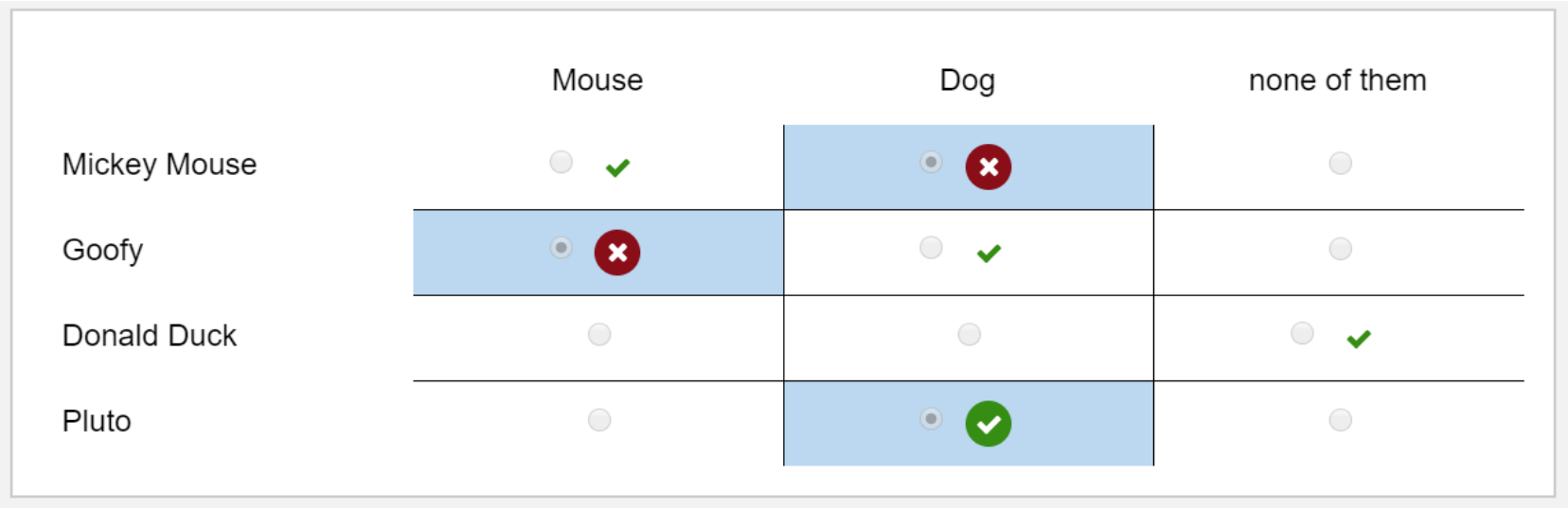
3 Points

Example 1



	Mouse	Dog	None of them
Mickey Mouse	○	◉	○
Goofy	◉	○	○
Donald Duck	○	○	○
Pluto	○	◉	○

Example 1



	Mouse	Dog	none of them
Mickey Mouse	✓	✗	
Goofy	✗	✓	
Donald Duck			✓
Pluto		✓	

0 Points

Example 2

Which of these characters are dogs?

Points: 1 for each correct, -1 for each wrong, 0 for no selection, max 2 total score

Select one or more alternatives:

- [ ] Donald Duck
- [ ] Pluto
- [ ] Goofy
- [ ] Mickey Mouse

Example 3

Numeric

Order these characters by size from smallest (="1") to highest (="3").

Points: 3 for all correct, 0 if any mistake

Donald:

Goofy:

Pluto: