Introducing Mindful Teaching and Learning at Kingston -- Lightning Talk

Presentation by:
Eckhard Pfluegel, Senior Lecturer &
James Denholm-Price, Associate Professor and School Director Learning and Teaching
Faculty of SEC, Kingston University

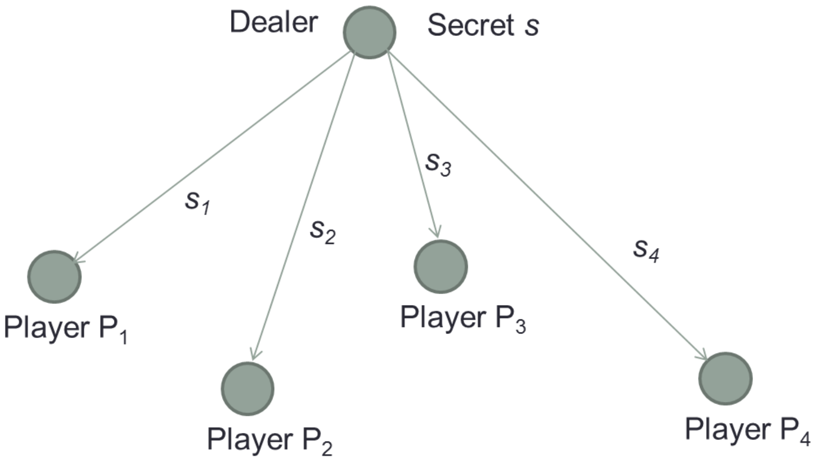
- Motivation and Background
    - Universities both in the UK and elsewhere have begun to recognise the need to address the impact of student stress on learning.
    - Mindfulness is increasingly being used in educational environments as a proven way to help students.
    - Context of "Mindful Teaching" L&T Dean's Award 2016/17: we have introduced innovative mindful teaching delivery for a Level 6 CSM Module.
- Mindful Teaching and Learning: Our Approach
    - Mindful Teaching Delivery -- Sessions structured around Mindful Break
        - 60' lecture
        - 5' mindful break -- students to reflect on their physical sensations, thoughts & emotions w.r.t. the teaching session
        - 25' lecture
    - Learning Technology Framework -- Using WorkFlowy
        - A learning technology framework was devised, enabling mindful teaching and learning at Kingston, based on integration of the cloud-based content management system WorkFlowy and Canvas/Box environment.
        - A set of learning materials supporting mindful learning were created, using the created framework as a feasibility demonstration.
        - This learning material is organised in a hierarchical fashion.
            - Branches can be viewed collapsed, expanded, and also zoomed in.
            - Ideal for exploration by students, but also for delivering the material during lectures.
            - This creates a unique novel way of teaching which might be preferable to a "linear" PowerPoint-based lecture.
        - Example Learning Material "Linear WorkFlowy"
            - CI6240 TB2 Lecture 3: Secret Sharing
              (PDF for download: https://kingston.box.com/s/x8xxladofi0bn9kuh3arzdav2kmr6oku)
                - Internet Security (CI6240) Lecture 3 -- Secret Sharing
                    - ![](https://www.dropbox.com/s/7hba0wpjnfhp95f/ss-puzzle.jpg?dl=1)

  - Eckhard Pfluegel
- Revision from Last Week
  - Be familiar with the Diffie-Hellman key agreement protocol
  - Improve the main weakness of Diffie-Hellman using the Station-to-Station protocol
- Learning Objectives -- Basic Secret Sharing
  - Be able to motivate the need for and use of secret sharing through the awareness of applications in networking and computer science
  - Explain the concept of a (t, n) threshold secret sharing scheme
  - Understand the principle of Shamir’s secret sharing scheme
  - Be able to compute shares of a given secret, using Shamir's scheme
  - Discuss the security, cost and memory requirements of Shamir's approach
- Cryptographic Techniques
  - Cryptography is a popular control, addressing the common security requirements CIA
  - Main cryptographic techniques
    - Information Protection (Encryption)
    - Information Fingerprinting (Secure Hash Functions)
    - Information Distribution (Secret Sharing)
    - Information Hiding (Steganography)
- Safeguarding a Cryptographic Key
  - Consider the task of storing a key safely, in the context of data encryption.
  - We are facing -- again -- a chicken-and-egg situation (why?).
    - ![] (https://www.dropbox.com/s/1sfl8794mjk37cp/encryption-

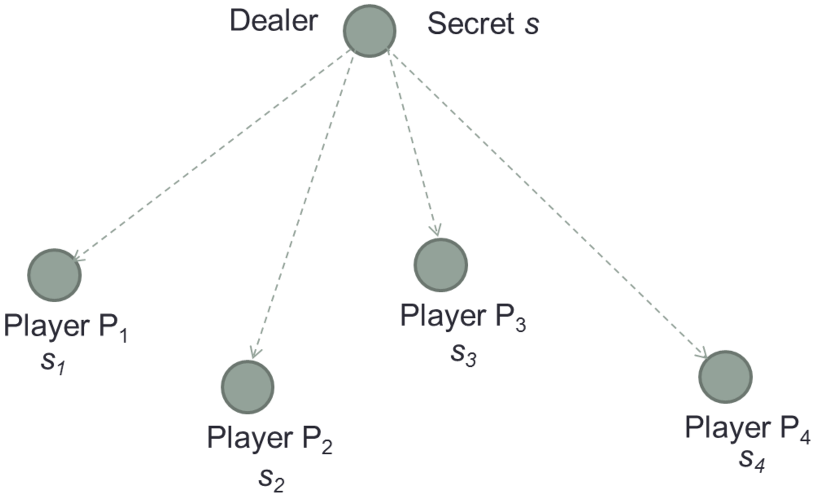
on-paper-with-key.jpg?dl=1)

- Cloud Computing Scenario
    - Consider a scenario where Alice has some confidential data, which she would like to store on a public cloud.
    - However, she is using Dropbox, which does not offer end-to-end encryption.
    - Hence she would like to implement the following security goals:
        - Confidentiality versus the cloud provider (and external parties).
        - Availability (redundancy) in case of hard disk failure or unavailability of Dropbox.
    - This can be achieved using secret sharing!
- Motivation
    - We want to protect sensitive information (a “secret”)
    - Secret sharing: divide secret into several pieces and distribute to “shareholders”
    - Historical use: Pirates tore treasure maps into pieces and gave them to allies
    - Let's do a jigsaw puzzle!
- Secret Sharing -- Concept
    - Secret sharing can protect information by distributing it amongst several parties.
    - The following terminology is commonly used: given a **secret* s, a *dealer* will divide it into *shares* and send them to n *shareholders* (or *players*).
    - We have a (t,n)-threshold scheme, if for $1 \leq t \leq n$:
        - The secret s can be divided into n shares.
        - The individual shares do not reveal s.
        - If (at least) t shares are combined, they can reconstruct s.
    - A (n, n)-threshold scheme is also referred to as **secret splitting*.

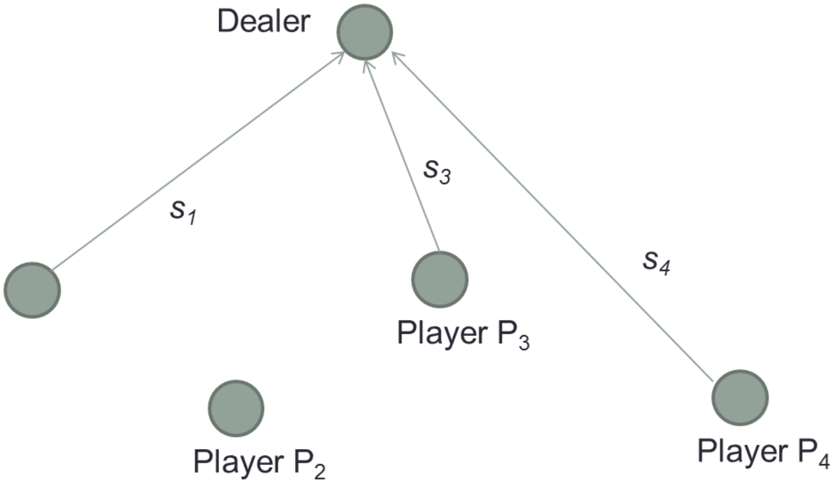
    - Developed in the late 80’s, secret sharing is not a new technique, but it is still an active research area and new applications are emerging.
- Illustration: (3,4) Threshold Scheme - Distribution
    - ![](https://www.dropbox.com/s/my9wh1oqyhe36w8/ss-distribution.png?dl=1)



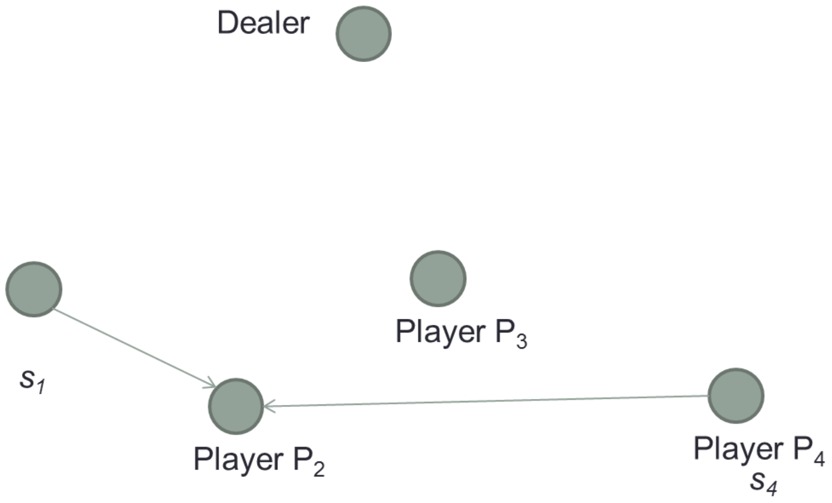
- Illustration: (3,4) Threshold Scheme - Shared Secret
    - ![](https://www.dropbox.com/s/cdxiyjal5o9vgm2/ss-shared-secret.png?dl=1)



- Illustration: (3,4) Threshold Scheme - Dealer Combining
    - ![](https://www.dropbox.com/s/ufl1vzjmrc31742/ss-dealer-combining.png?dl=1)

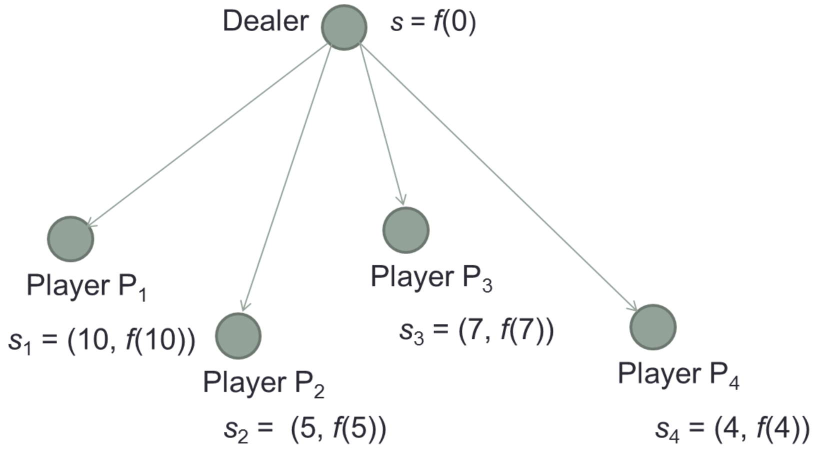


- Illustration: (2,4) Threshold Scheme - Player Combining
  - ![](https://www.dropbox.com/s/5vml3sihvfcwvya/ss-player-combining.png?dl=1)

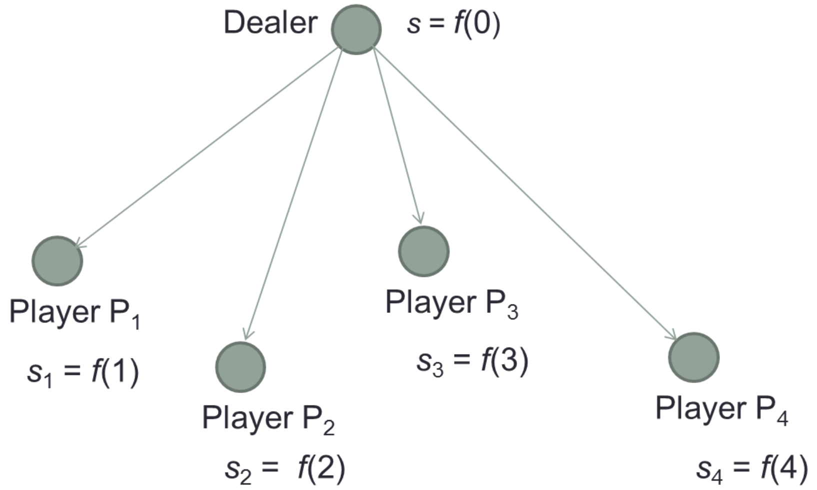


- Shamir's Secret Sharing Scheme
  - Secret sharing schemes are generally using mathematical objects that allow sharing and reconstructing.
  - The underlying idea of this scheme is to convert the secret s to a polynomial $f(x)$ with suitable degree and coefficients.
    - The degree of f is $t-1$.
    - The secret s will be stored in $f(0)$ -- this is the constant term of f.
    - All other coefficients of f are drawn at random.
  - Distribution of shares works by **evaluating* f:
    - We share n distinct points $P_i(x_i, f(x_i))$ (for $(i = 1, \ldots, n)$ amongst the n players.
  - Reconstruction of the secret is based on **interpolation**.
    - A polynomial $f(x)$ of degree $t-1$ is uniquely determined by t different points.

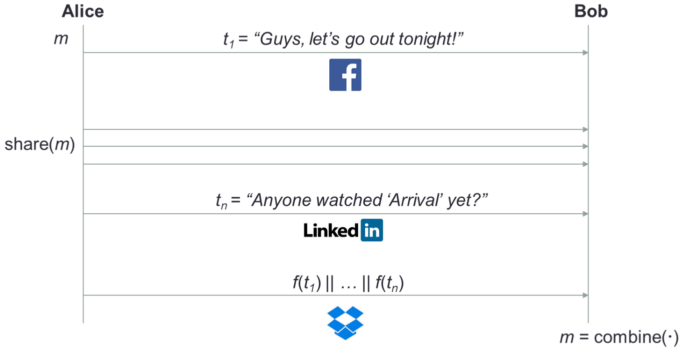
    - Hence a coalition of t players can reconstruct f, using interpolation.
    - Any set of t distinct points will be valid.
  - This implemenst all properties required for a (t, n) threshold scheme.
- Illustration: Shamir's Scheme
  - ![](https://www.dropbox.com/s/alottc1kdonfk2q/ss-shamir-inefficient-illustration.png?dl=1)



- Shamir's Scheme: Choice of Evaluation Points
  - If we are working with the integers modulo p, then the x_i can simply be the values $x_1 = 1$, $x_2 = 2$, $x_3 = 3$...
  - The x_i could also be computed from some unique information related to the players, e.g. using a secure hash function H, from an ID value: $x_i = H(ID_i)$.
  - This point generating algorithm could be made public.
  - Hence there would be no need to actually send the x_i.
  - This would reduce the size of the data that needs distributing by 50%!
- Illustration: Space-Efficient Shamir
  - ![](https://www.dropbox.com/s/gqykalgmfrmgr15/ss-shamir-illustration.png?dl=1)



- Shamir’s Scheme: Discussion
    - Security
        - Shamir’s scheme is a **perfect** secret sharing scheme.
        - This means that no information about the initial secret is revealed to a coalition of less than the threshold number (t) of players.
    - Space-Requirements
        - When done naively, for each share we require twice the size of the secret s.
        - This can be reduced to a share size of $|s|$ e.g. by using a public evaluation point function.
    - Computational Cost
        - Polynomial evaluation can be done in the order of t arithmetic operations.
        - The same holds for interpolation.
- Applications of Secret Sharing
    - We review the use of secret Sharing for our initial scenarios:
        - Safekeeping of cryptographic keys
            - PGP client software uses a (5,3) secret sharing scheme to store the user's private key.
        - Cloud computing scenario
            - Alice splits her data into several "pieces" and stores each on a different cloud (Dropbox, iCloud, Google Drive etc.)
            - This needs be done in such a way that none of the cloud providers can read the original information
            - Entire data can be restored from a subset of t pieces
            - What is the redundancy?
        - Another Application is in Social Networks
            - ![](https://www.dropbox.com/s/ye03jozxwn03ei5/undetectable-distributed.png?dl=1)


Alice
Bob
m
t_1 = “Guys, let’s go out tonight!”
share(m)
t_n = “Anyone watched ‘Arrival’ yet?”
Linkedin
$f(t_1)$ || … || $f(t_n)$
m = combine(·)

- Further Reading (Watching..)

            - http://youtu.be/kkMps3X_tEE
            -
        - Summary -- Basic Secret Sharing
            - Be able to motivate the need for and use of secret sharing through the awareness of applications in networking and computer science
            - Explain the concept of a (t, n) threshold secret sharing scheme
            - Understand the principle of Shamir’s secret sharing scheme
            - Be able to compute shares of a given secret, using Shamir's scheme
            - Discuss the security, cost and memory requirements of Shamir's approach

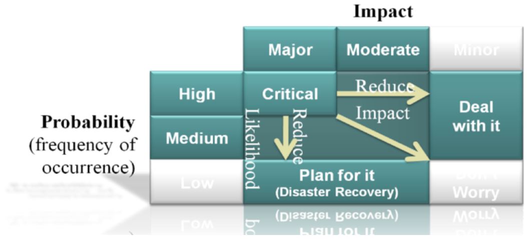
- Example Learning Material "WorkFlowy Knowledge Tree"
    - The topics currently covered in this repository are an introduction to information security assessment principles and an overview of frameworks such as OCTAVE, STRIDE, NIST RMF and ISO 27000.
    - These topics are extremely relevant for cyber security knowledge but students often find them difficult to engage with. It is hoped that the novel way of accessing and delivering the learning material might help with student learning.
    - CI6240 TB2 Lecture 4 & 5: Security Assessment

      (PDF for download (linear, ppt-based -- see announcements, click here if URL not shown) https://kingston.box.com/s/ealljqim38hld220g1pfymkfpwdfe90o)
        - Internet Security (CI6240) Lecture 4 & 5 -- Security Assessment
            - Eckhard Pfluegel
        - Revision from Last Week
            - Be able to motivate the need for and use of secret sharing through the awareness of applications in networking and computer science
            - Explain the concept of a (t, n) threshold secret sharing scheme
            - Understand the principle of Shamir’s secret sharing scheme
            - Be able to compute shares of a given secret, using Shamir's scheme
            - Discuss the security, cost and memory requirements of Shamir's approach
        - Learning Objectives -- Security Assessment
            - Understand the concept and principle of security management and assessment
            - Know context and basic approach of Risk Analysis
            - Be able to differentiate between mature frameworks and standards for security management and assessment

    - Have an overview of the OCTAVE and STRIDE frameworks, and an awareness of ISO 27000
    - Be able to create a threat and risk profile for a given security scenario
- **SECURITY MANAGEMENT AND ASSESSMENT KNOWLEDGE TREE**
    - It is important to distinguish the terminology between (general) **security management** and (more specifically) **risk management**.
        - Security Management is assessing, identifying, analysing, establishing and evaluating the security of a system or organisation in the most general way.
            - In practice, this can be done with focus on different domains.
                - Information Security
                - Network Security
                - System and Software Security
                - Cybersecurity
            - Security Assessment is one particular step of the Security Management process.
                - The main methodologies are **top-down** (risk-based) or **bottom-up** (vulnerability/system-based).
                - Security Assessment -- when should we choose top-down or bottom-up?
                    - Top-down helps to see the bigger picture and to align the use of resources with the companies mission.
                    - It might also help with focus on critical few systems or assets, in particular when information assets are examined.
                    - Bottom-up is appropriate if the system is easy to oversee.
                - Security Assessment can be a challenging task.
                    - Perfectly secure systems do not exist and accidents, attacks and intrusions will happen -- so organisations need to deal with them (business continuity)
                    - However, the resources an organisation can dedicate to security are limited.
                        - Time
                        - Staff
                        - Budget

            - Expertise
        - We can identify some typical examples of Security Assessment Exercises.
            - 1. Vulnerability Assessment
                - Scope is technology & polices/procedures
                - Snapshot at a single point in time
                - Traditionally a bottom-up approach
                - Usually Internally performed -- this is of lower cost than outsourcing
                - But could also be carried out by external pen-tester
            - 2. Information Security Assessment
                - Applied to information is held in an electronic form, e.g.
                    - Database with customer information
                    - User Generated Content in Social network websites
                    - Personal data on a hard disk
                - Top down approach is most suitable , but should include technological review of systems and infrastructure
            - 3. Independent Information System Audit
                - Independently performed
                - Purpose
                    - Assurance of {management, regulatory bodies, shareholders}
                    - Legal / regulatory ramifications
                - Can be very costly
- Risk Management is the risk-based approach of information security management which comprises the areas of disaster recovery, business continuity, policy and physical security.

- According to the NIST, Risk Management can be further divided into assessing, responding to and monitoring of risk within the organisational context.
  - Prior to risk assessment, critical assets and their security requirements are determined.
  - Risk assessment itself is usually a cyclical process, consisting of risk identification and analysis.
    - A crucial step is to conduct a risk analysis.
      - An important aspect and crucial activity is how to measure risk: either **qualitatively** or **quantitatively**.
        - Quantitative: we want to know the estimated likelihood that an attack actually happens.
          - Often used equation:
            - Risk = Probability x Impact
  - This helps with prioritising which asset to protect, and to devise suitable response mechanisms.
    - Illustration: Risk Matrix ![](https://www.dropbox.com/s/fhlfo7xiabmmj45/risk%20matrix.png?dl=1)



- Mature open and close methodologies have been adopted by organisations and national and national as well as international standards exist.
  - OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) -- a well-documented, open information security risk assessment methodology.
    - OCTAVE -- Overview
      - Set of tools, techniques and methods for risk-based information security strategic assessment and planning

  - Developed by Christopher Alberts at Carnegie Mellon University (CMU)
  - Published by Software Engineering Institute (SEI) at CMU in 1999
  - More information is available at http://www.cert.org/octave/
- OCTAVE -- Characteristics
  - Philosophy/Vision
    - Focuses on strategy
    - Take into account the organisation's needs
  - Risk Assessment:
    - Top-down approach
    - Threat-per-asset based
    - Qualitative approach
  - Implementation:
    - Process-driven
    - Flexible: Can be customized
    - Self-directed: led by organisation's employee
- OCTAVE Variants
  - OCTAVE (large organizations ≥ 300 employees)
    - Phase 1: Build asset-based *_threat profiles_*
      - Process 1: Determine critical assets and how they are currently protected
      - Process 2: Identify security requirements for each critical asset.
      - Process 3: Identify organisational vulnerabilities within existing practices
      - Process 4: Create a threat profile for each critical asset
        - Threat Profile – Asset (what is at risk)
          - The (critical) asset that is potentially affected by the threat
          - Remember the asset categories:
            - Data
            - Software

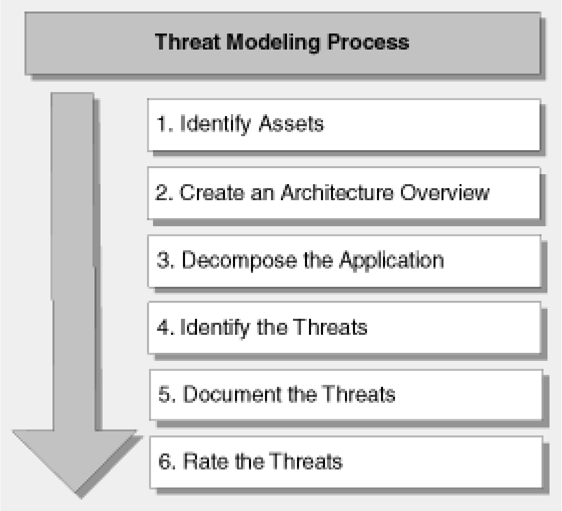
    - Hardware
    - People
- Threat Profile – Actor (origin of the threat)
  - We distinguish between the actors "nature" and "human"
- Threat Motive (reason for the attack)
  - Amateurs
  - Script Kiddies
  - Geeks
  - White Hat (Ethical) Hackers
  - Grey Hat Hackers
  - Black Hat Hackers (Computer Criminals)
- Threat Profile -- Access (how the asset is reached)
  - An *attack vector* is a path or means by which the attacker can gain access to an asset
  - Attack vectors enable the exploitation of system vulnerabilities, including the human element.
  - Examples:
    - A web interface with an XSS vulnerability
    - An employee with a weak password
- Threat Profile -- Outcome (damage likely to be caused)
  - The outcome is measured by the impact on the organisation -- the weighted cost of losing an asset
  - Depends on:
    - Asset characteristics
    - Asset value for the organisation

  - Is one of the following: disclosure, modification, loss/destruction, interruption, or other
- Threat Profile – Examples
  - Asset (e.g. customer data, pc,)
  - Access (e.g. private/public network, web page)
  - Actor (Source of threat)
  - Internal (e.g. staff), External (e.g. hacker)
  - Motive (accidental, deliberate)
  - Outcome (Impact of asset e.g. data)

- Phase 2: Identify infrastructure vulnerabilities
  - Process 5: Identify network access paths and IT components related to critical assets
  - Process 6: Evaluate identified IT components
- Phase 3: Develop security strategy and mitigation plans
  - Process 7: Conduct risk analysis
    - Identify & evaluate the impact of threats to critical assets
    - OCTAVES forms a *_risk profile_* by expanding the threat profile by a description of impact and impact values:
      - Impact description -- "*The disclosure of the sensitive documents mean that our competitors know our trade secrets and might be able to come out with a competitive new product.*"
      - Impact value -- usually chosen from {low, medium, high}

                - Impact Areas:
                    - Reputation/customer confidence
                    - Life/health of customer
                    - Fines/Legal penalties
                    - Financial
                    - Other
        - Process 8: Develop protection strategy and mitigation plan
            - Information generated by Phases 1 and 2 are analysed to:
                - Identify risks to critical assets - prioritise
                - Develop protection strategies
                - Develop mitigation plans
                - Propose next steps
            - Will need Senior Management approval
- OCTAVE-S (organizations ≤ 300 employees)
    - Developed in 2003 in response to needs of smaller organisations
    - Meets same OCTAVE criteria but is adapted to more limited means and unique constraints of small organizations
        - Small organisation with a simple hierarchical structure
        - Small interdisciplinary analysis team (3-5 employees)
    - Uses more streamlined processes and different worksheets, but produces the same type of results
    - Includes a limited exploration of the computing infrastructure during Phase 2
- OCTAVE-Allegro (focuses on information assets)
    - Developed in 2007 due to the increased need to protect data
    - Unlike previous OCTAVE approaches, it focuses on information assets:

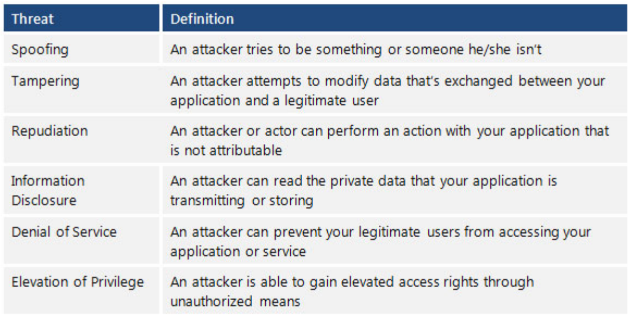
            - Where they are stored, transported, and processed
            - How they are used
            - How they are exposed to threats, vulnerabilities, and disruptions as a result
        - Suitable to perform risk assessment without extensive organisational involvement, expertise, or input.
    - OCTAVE – Advantages
        - Well-documented through published academic papers and freely available resources
        - Flexible as organisations may choose to implement portions that they find appropriate
        - Comprehensive and thorough
        - Strategic as it focuses on important and relevant risks
        - “Cheap” as it is self-led
    - OCTAVE – Shortcomings
        - Needs extensive preparation and is complex when done correctly
        - Qualitative methodology means that OCTAVE does not allow for the mathematical modelling of risks
        - Risk Analysis is simplistic as done on a single asset
- STRIDE & DREAD -- a (Web) Application Security Risk Assessment framework, developed for Microsoft's Threat Model.
    - STRIDE was originally designed for testing web application security.
        - Developed by Microsoft in 2005
        - Now also recommended by OWASP
        - Is top-down: focuses on threats (“threat/risk modelling”)
        - A simple approach
        - An iterative process
    - Illustration -- STRIDE is part of the bigger picture of threat modelling.
      https://i-msdn.sec.s-msft.com/dynimg/IC101260.gif



Threat Modeling Process

1. Identify Assets
2. Create an Architecture Overview
3. Decompose the Application
4. Identify the Threats
5. Document the Threats
6. Rate the Threats

- The STRIDE mnemonic conveniently covers most relevant threats to CIA.
    - [https://i-technet.sec.s-msft.com/en-us/security/hh855044.STRIDE-definitions(en-us,MSDN.10).jpg]



Threat	Definition
Spoofing	An attacker tries to be something or someone he/she isn't
Tampering	An attacker attempts to modify data that's exchanged between your application and a legitimate user
Repudiation	An attacker or actor can perform an action with your application that is not attributable
Information Disclosure	An attacker can read the private data that your application is transmitting or storing
Denial of Service	An attacker can prevent your legitimate users from accessing your application or service
Elevation of Privilege	An attacker is able to gain elevated access rights through unauthorized means

- STRIDE consists of 4 steps.
    - Step 1. Create a list including all known threats, mapped against their impact.
    - Step 2. Rank threats by criticality, or impact and likelihood.
        - DREAD, a mnemonic for risk rating security threats, can be used for this risk-assessing activity.
            - Damage - how bad would an attack be?
            - Reproducibility - how easy is it to reproduce the attack?
            - Exploitability - how much work is it to launch the attack?
            - Affected users - how many people will be impacted?
            - Discoverability - how easy is it to discover the threat?
        - Some organizations have either moved to a DREAD-D "DREAD minus D" scale

(which omits Discoverability) or always assume that Discoverability is at its maximum rating.

    - DREAD is part of a system for risk-assessing computer security threats
    - It was initially proposed for threat modeling, but it was discovered that the ratings are not very consistent and are subject to debate.
    - It was previously used at Microsoft and currently used by OpenStack and many other corporations.
    - It was out of use at Microsoft by 2008.
    - When a given threat is assessed using DREAD, each category is given a rating.
        - For example, 3 for high, 2 for medium, 1 for low and 0 for none.
        - Rating scales running from 0 to 10 are common.
        - The sum of all ratings for a given exploit can be used to prioritize among different exploits.
    - Discoverability Debate
        - Some security experts feel that including the "Discoverability" element as the last D rewards Security through obscurity.[4][5]
  - Assign 2 numbers for each threat:
    - For criticality (1→10; 10 is most severe)
    - For likelihood (1→10; 10 is least likely to occur)
  - Calculate: overall risk = Criticality/likelihood
- Step 3. Select a mitigation technique or technology for each threat
- Step 4. Start again (Step 1) as the project evolves

        - We conclude that STRIDE is simple and effective, but different to OCTAVE.
            - STRIDE was originally designed for building secure web applications, whereas OCTAVE targets (information) security of an organisation.
            - Both frameworks are top-down, but the OCTAVE has a more formal approach for identifying critical assets and their vulnerabilities.
            - In OCTAVE, threat profiling is very generic, whereas the STRIDE acronym helps to identify relevant threat categories.
            - OCTAVE also lacks specific guidelines for risk analysis, STRIDE has developed the DREAD categorisation for threat outcomes.
        - References
            - [https://en.wikipedia.org/wiki/STRIDE_(security)]
            - [https://en.wikipedia.org/wiki/DREAD_(risk_assessment_model)]
    - NIST RMF: US National Standard for Risk Management
    - ISO/IEC 27000-series: International Standard for security management
        - Information Security Management Systems (ISMS) Family of Standards
            - ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organisation’s information security
            - Consists of inter-related standards - 23 standards available, 11 under development
            - Covers the following areas:
                - Information assets & relevant requirements identification
                - Risk Assessment & Treatment
                - Controls Selection & implementation
                - Monitor, maintain and improve the effectiveness of controls associated with assets
        - Framework Overview
            - Advantages

  - Framework is made out of (international) standards
  - Supported by several other frameworks
  - Flexibility in the choice of complementary low-level Risk Assessment method
- Shortcomings
  - Documentation is not free
  - Risk Analysis process is described at a very abstract level
  - Third-party Risk Assessment method required in order to carry out a comprehensive Risk Assessment
  - Highly complex

- Whilst a formal security assessment exercise leads to thorough review of threats and vulnerabilities and will improve security, it might have inaccurate findings and generally lull into a false feeling of security.
- Summary
  - Understand the concept and principle of security management and assessment
  - Know context and basic approach of Risk Analysis
  - Be able to differentiate between mature frameworks and standards for security management and assessment
  - Have an overview of the OCTAVE and STRIDE frameworks, and an awareness of ISO 27000
  - Be able to create a threat and risk profile for a given security scenario

- Evaluation
  - The effectiveness of this teaching approach was evaluated after delivering teaching sessions for module CI6240 throughout TB2 2016/17
  - Result: 65% of the students agreed or strongly agreed that it had advantages compared to using PowerPoint.
- Conclusion
  - Our framework can improve the learning and teaching of students, demonstrated in the subject area of computing/mathematics, but potentially also in other areas.
  - We think that it can actually bring advantages for lecturers as well!
  - There have also been some lessons to be learnt.
  - The obtained positive feedback and evaluation encourages us to run (an extended version) of our approach again in the next academic year.
  - We are keen to receive feedback and suggestion for future collaborations in this novel area.