Risk Assessment (IPICS)

Dr Luke Hebbes
Email: l.hebbes@kingston.ac.uk
Blog: http://blog.rlr-uk.com
Twitter: lhebbes

Kingston University London

Introduction

- In a world where everything is connected we require very good security, but what do we secure and how?
- Perimeter defence sits at the edge protecting from the outside world
- Infrastructure security focuses on internal systems, dependability, information flow, etc.
- We will look at risk analysis and how to decide which security practices &policies to implement

Kingston University London

Introduction

- Security is not always an exact science
- Every system will have different priorities and constraints
- There is no single solution for all systems
- We can't all afford governmental security...
- ...and it might hinder, so we don't want it!

Kingston University London

System-Holistic Approach to Security

Why SHA?

- Security perceived as mess of ill-defined and often conflicting opinions & ideas, built on specific pools of knowledge
- Must address main security facets:
  - Authentication (Identification)
  - Integrity
  - Confidentiality
  - Availability
- Are these in order?

Kingston University London

System-Holistic Approach to Security

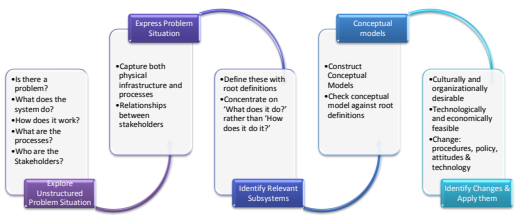
What is SHA?

- Conceptual model
- Facilitates understanding of ICT security problems relating to existing systems in specific contexts
- Current systems are increasing in complexity
- SHA aims to analyse the whole rather than parts including non-technical aspects as well as technical ones

Kingston University London

System-Holistic Approach to Security

Soft System Methodology



Kingston University London

System-Holistic Approach to Security

10 Hallmarks of General Systems Theory

1. Objects and attributes within a system have interrelationships and interdependencies – facilitates delimiting system and identifying independent elements that should not be granted access or authorization privileges
2. A system is more than the sum of its parts – technological solutions may not perform as expected in a new environment
3. All systems are goal seeking – security goals must be tightly specified and measured

Kingston University London

System-Holistic Approach to Security

10 Hallmarks of General Systems Theory

4. All systems are open, in that they require input to produce output – wrong, false or untimely input can wreak havoc and must be controlled
5. Systems exist to transform inputs to outputs – input not used for processing can cause harm and should not be allowed (e.g. Malware)
6. There always exists a degree of structural order or disorder – additional controls or information required to compensate
7. All systems require management to achieve goals

Kingston University London

System-Holistic Approach to Security

10 Hallmarks of General Systems Theory

8. Natural hierarchies exist within systems – systems are made up of subsystems that must be structured in such a way as to provide security; coordinate functional & non-functional
9. In complex systems, specialised units perform specialised functions – security management & operation should be treated as such for adaptability
10. There exist different valid ways to reach the same goals

Kingston University London

Philosophy – Pragmatism

- The resources an organisation can dedicate to security are **limited**
  - Time, staff, budget, expertise…
- Perfectly secure systems do not exist
  - Accidents, attacks & penetrations will happen – so plan to deal with them
- See the bigger picture
  - Align the use of resources with the company's mission
- Focus
  - On critical few systems or assets

Kingston University London

Trust versus Control

Approaches to overall security	• Restrictive (Whitelist) • Permissive (Blacklist)
Approaches to trust	• Trust everyone all of the time • Trust no one at any time • Trust some people some of the time

Kingston University London

Key Terms

Asset : something of value to the enterprise

- Information technology assets are grouped into specific classes
  - information, systems, software, hardware, people

Threat : indication of a potential undesirable event

- the existence of a situation in which
  - a **person** could do something undesirable
  - a **natural occurrence** could cause an undesirable outcome
- Threats have defined properties
  - asset, actor, motive, access, outcome

Kingston University London

Key Terms

Vulnerability : a weakness in:

- an information system, system security practices and procedures, administrative controls, internal controls, implementation, or physical layout

that could be exploited by a **threat** to:

- gain unauthorized access to information to disrupt processing

Kingston University London

Key Terms

Risk : the possibility of suffering harm or loss

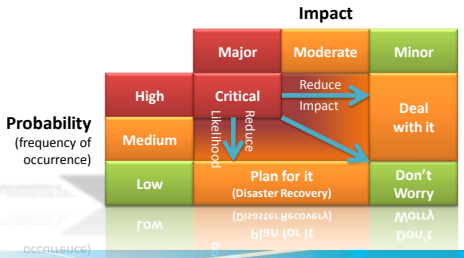
- a situation in which there is the **potential** for either :
  - a person doing something undesirable
  - a natural occurrence causing an undesirable outcome
- resulting in a negative impact or consequence.

Vulnerability + *Threat* = *Risk* to an *Asset*

Kingston University London

Risk

Risk = probability × impact



Kingston University London

Risk

- Previous table doesn't take into account cost
  - High risk may be cheap to fix (e.g. patches, etc.)
  - Low risk may be expensive (e.g. Require training)
- Another useful measure for risk is:

$$concern = \frac{priority}{progress}$$

- Priority is assessment of risk

Kingston University London

Threat Ratings

Rating	Meaning
Negligible	Unlikely to occur
Very Low	Likely to occur only two or three times every five years
Low	Likely to occur within a year or less
Medium	Likely to occur every six months or less
High	Likely to occur after a month or less
Very High	Likely to occur multiple times per month or less
Extreme	Likely to occur multiple times each day

ACSI 33 – Information Security Group of the Australian Government's Defence Signals Directorate

Kingston University London

Consequences

Description	Consequences
Insignificant	Can be dealt with by normal operations
Minor	Could threaten the system's efficiency or effectiveness but can be dealt with internally
Moderate	Does not threaten the system, but could cause major review and modification of operating procedures
Major	Threatens the continuation of basic functions of the system and requires senior-level management intervention
Catastrophic	Threatens the continuation of the system and causes major problems for the organisation and customers

ACSI 33 – Information Security Group of the Australian Government's Defence Signals Directorate

Kingston University London

Common Criteria Security Framework

- **Security environment**
  - Laws, organizational security policies, etc., which define the context in which the Target of Evaluation (TOE) is to be used
  - Threats present in the environment are also included
- **Security objectives**
  - A statement of intent to counter identified threats and/or satisfy intended organizational security policies and assumptions

Kingston University London

Common Criteria Security Framework

- **TOE security requirements**
  - Refinement of IT security objectives into a set of technical requirements for security functions & assurance, covering TOE & IT environment
- **TOE security specifications**
  - Define actual or proposed implementation for Target of Evaluation
- **TOE implementation**
  - Realisation of TOE in accordance with spec.

Kingston University London

Approaches to Info. Sec. Evaluation

- 1. Vulnerability Assessment
  - Usually **Internally** performed
  - Systematic
  - Snapshot at a single point in time
  - Scope is technology & polices/procedures
- 2. Information System **Audit**
  - **Independently** performed
  - Purpose
    - Assurance of {management, regulatory bodies, shareholders}
    - Legal / regulatory ramifications

Kingston University London

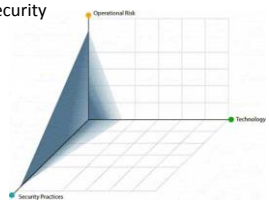
Approaches to Info. Sec. Evaluation

- 3. Information Security Risk Evaluation — Octave
  - Corporate / organisational review of policies and practices
  - Technological review of systems and infrastructure
- 4. Managed Service Provider
  - Outsourcing security responsibilities to 3rd party
    - [-] Cost
    - [+] Useful where in-house skills are limited (e.g. small businesses)

Kingston University London

OCTAVE

- OCTAVE® - Operationally Critical Threat, Asset, and Vulnerability Evaluation℠
- Risk-based strategic assessment and planning technique for security



http://www.cert.org/octave/

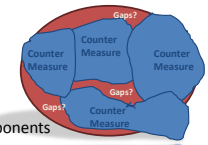
Kingston University London

OCTAVE – Differences

OCTAVE	Other Evaluations
Organisation evaluation	System evaluation
Focus on security practices	Focus on technology
Strategic issues	Tactical issues
Self direction	Expert led

Kingston University London

OCTAVE - Differences



- Current Security Practices
  - Bottom up – start with individual components
  - Seeking Technological 'silver bullet'
  - Focus on computing infrastructure

Weakness → End up protecting what can be protected rather than what **needs** to be protected

- Octave
  - Top down
  - Driven by business's missions & objectives

Protection of what needs it, awareness of risk

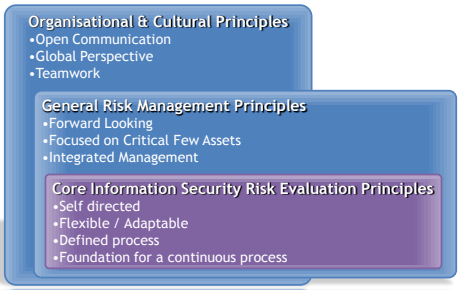
Kingston University London

OCTAVE - Criteria

- The OCTAVE criteria define a standard approach for a risk-driven, asset- and practice-based information security evaluation
- Two recognized methods:
  - OCTAVE Method – for large organizations
  - OCTAVE-S – for smaller organizations

Kingston University London

OCTAVE Principles



Kingston University London

Octave Aspects

- Small interdisciplinary analysis team of 3-5 people leads OCTAVE-S
  - Team members must have broad insight into organisation's business & security processes, sufficient to conduct activities
  - It does not require formal data gathering workshops
- Includes limited exploration of infrastructure
  - SMEs frequently outsource IT services & functions
  - Typically don't have capabilities for running & interpreting vulnerability evaluation tools
  - Examine processes employed to securely configure and maintain computing infrastructure

Kingston University London

Phase 1: Build Asset-Based Threat Profiles

- Identify Organizational Information (Process 1)
  - Establish Impact Evaluation Criteria
  - Identify Organizational Assets
  - Evaluate Organizational Security Practices
- Create Threat Profiles (Process 2)
  - Select Critical Assets
  - Identify Security Requirements for Critical Assets
  - Identify Threats to Critical Assets
  - Analyze Technology-Related Processes

Kingston University London

Phase 2: Identify Infrastructure Vulnerabilities

- Examine Computing Infrastructure in Relation to Critical Assets (Process 3)
  - Examine Access Paths
  - Analyze Technology-Related Processes

Kingston University London

Phase 3: Develop Security Strategy and Plans

- Identify and Analyze Risks (Process 4)
  - Evaluate Impacts of Threats
  - Establish Probability Evaluation Criteria
  - Evaluate Probabilities of Threats
- Develop Protection Strategy & Mitigation Plans (5)
  - Describe Current Protection Strategy
  - Select Mitigation Approaches
  - Develop Risk Mitigation Plans
  - Identify Changes to Protection Strategy
  - Identify Next Steps

Kingston University London

OCTAVE-S Outputs

- Main results include:
  - organization-wide protection strategy – strategy outlines direction with respect to information security practice
  - risk mitigation plans – are intended to mitigate risks to critical assets by improving selected security practices
  - action list – includes short-term action items needed to address specific weaknesses

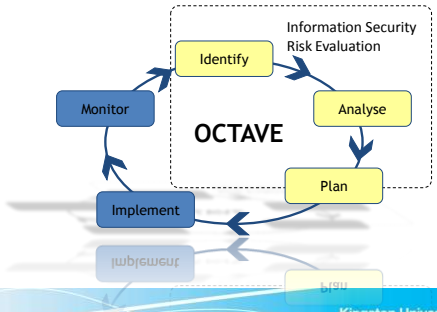
Kingston University London

OCTAVE-S Outputs

- Other useful outputs include:
  - a listing of important information-related assets supporting the organization's business goals and objectives
  - survey results showing the extent to which the organization is following good security practice
  - a risk profile for each critical asset depicting a range of risks to that asset

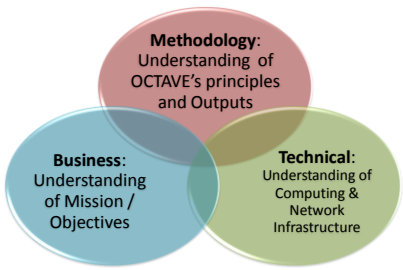
Kingston University London

OCTAVE-S – Scope



Kingston University London

Summary



Kingston University London

Three Card RAG / Obstacle Poker

What is Obstacle Poker?

- Security Obstacle Mitigation Model (SOMM) for developing trustworthy information systems
- Definitions:
  - Mitigation – procedure that will counter obstacle
  - Obstacle – will obstruct trust assumption & affect security requirements (malicious or inadvertant)
  - RAG Code – 'traffic light' approach to ranking vulnerability

Kingston University London

Three Card RAG / Obstacle Poker

RAG Code

- Red, Amber and Green
  - Red – stop and mitigate
  - Amber – proceed with caution
  - Green – continue with trust
- An issue is discussed, then all members of team rate it, revealing their cards all at once
  - Agreement – state of play
  - Disagreement – further discussion & further round completed
- Agreement reached quickly between disparate groups

Kingston University London

Three Card RAG / Obstacle Poker

Obstacle Poker in use

- Representatives of all roles must be included to meet needs of organisation
- ICT departments & technologists don't necessarily know business processes
- Those outside ICT usually have little or no knowledge of technical landscape or what's possible/feasible
- Need common way to converse and make decisions

Kingston University London

Three Card RAG / Obstacle Poker

Obstacle Poker in use

- Issues that are more obvious will be dealt with quickly
- Those requiring more discussion will be given a fair hearing
- Used to decide on Critical Assets and Threat Ratings
- Simply put: red = priority; amber = secondary; green = safely ignored until next iteration (N.B. not ignored completely or never discussed again)

Kingston University London

Conclusions

- Majority of security assessment strategies technology focused concentrating on system evaluation & tactical issues
- Organisational evaluation, focused on security practices and strategic issues
- Top down approach driven by business issues & objectives leading to **protection of what needs it and awareness of risk**
- Bottom up practices start with individual components & infrastructure, leading to **protecting what can be protected rather than what needs to be protected**
- Ongoing cyclical process

Kingston University London

Conclusions

Standards

- Many standards for different organisations and different businesses, but risk assessment principles relevant to all
  - PCI Standards
  - ISO 38500
  - ISO 27000
  - Etc.
- Sometimes forced by regulatory agencies

Kingston University London

References

- System-Holistic Approach to ICT Security – Christopher Wills & Louise Yngström, *Securing Information and Communications Systems – Principles, Technologies and Applications*, Chapter 14, 2008, ISBN-13: 978-1-59693-228-9
- OCTAVE® – http://www.cert.org/octave/
- Obstacle Poker – Vic Page, PhD Thesis (writing up) and *Security risk mitigation for information systems*, BT Technology Journal, Vol. 25, No. 1, January 2007, ISSN: 1358-3948

Kingston University London