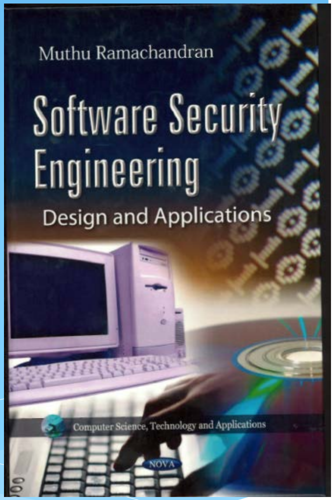
Software Security Requirements Engineering: State of the Art

Muthu Ramachandran

MSc MTech PhD FBCS SFHEA MIEEE MACM

Principal Lecturer
Head of Software Engineering Research
School of Computing, Creative Technologies and Engineering
Leeds Beckett University
Leeds LS6 3QS UK
Email: M.Ramachandran@leedsbeckett.ac.uk
www.leedsbeckett.ac.uk
Research Projects
www.soft-research.com


Muthu Ramachandran
Software Security Engineering
Design and Applications
Computer Science, Technology and Applications
NOVA

LEEDS
BECKETT
UNIVERSITY

Keynote Talk 16th September 2015 ICGS3, London

Outline

- Why Software Security Engineering?
- Software Security RE: Concepts, Definitions & Perspectives
- Design For Software Security: A Unique Chapter in My book
- SSRE Processes
- Software Security Requirements Process Simulation with OPNET & BPMN
- Conclusion & Questions

Why Software Security Engineering?

Everyone and everything is moving into the Cloud…

We all enjoy. However, security, privacy & trust are the key to its success!

Embrace technology and focus on humanity

"No, you weren't downloaded. Your were born."

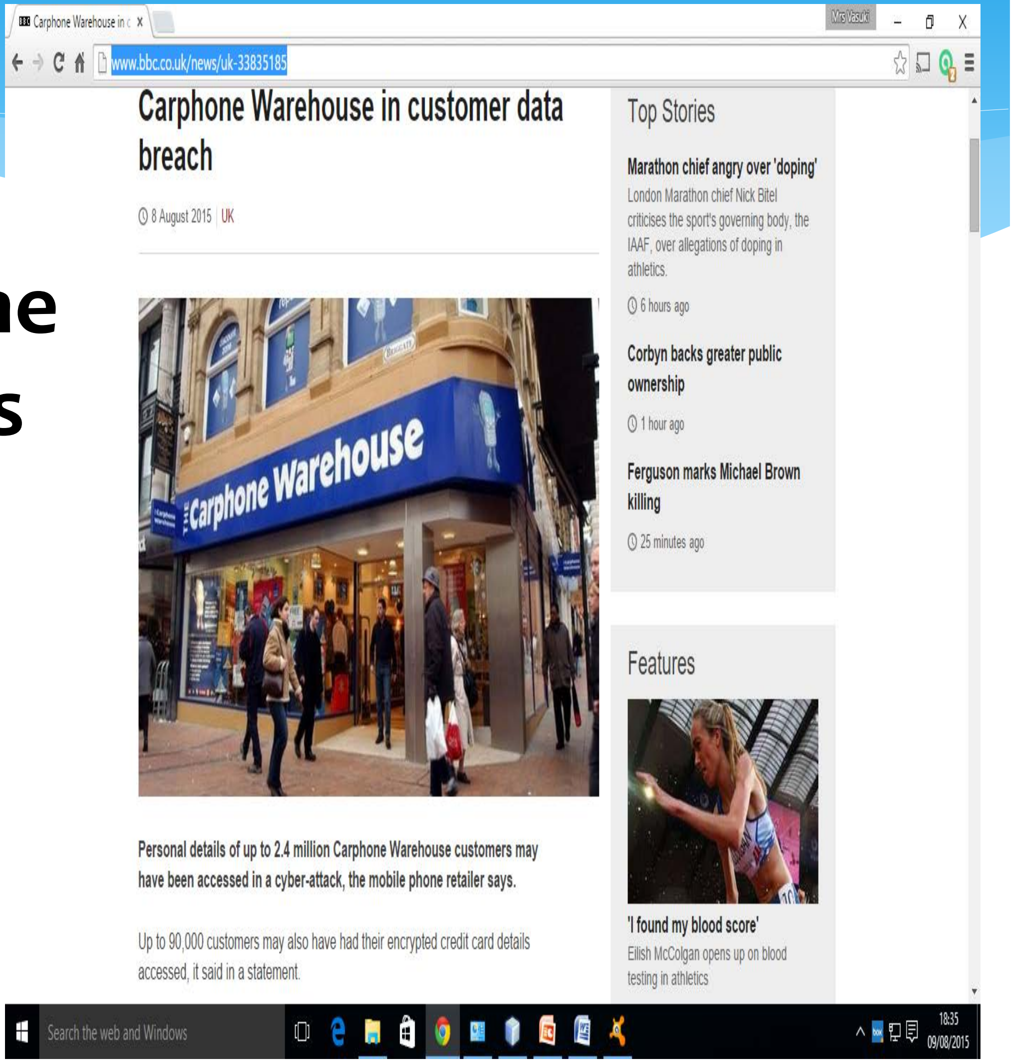
Gerd FUTURIST

LEEDS BECKETT UNIVERSITY

Committing to secure SDLC way of showing our gratitude and thankfulness to our consumers

Cyber-attack on 8th August 2015

Personal details of up to 2.4 million Carphone Warehouse customers may have been accessed in a cyber-attack, the mobile phone retailer says.



Carphone Warehouse in customer data breach

8 August 2015 | UK

Personal details of up to 2.4 million Carphone Warehouse customers may have been accessed in a cyber-attack, the mobile phone retailer says.

Up to 90,000 customers may also have had their encrypted credit card details accessed, it said in a statement.

Top Stories

Marathon chief angry over 'doping'
London Marathon chief Nick Bitel criticises the sport's governing body, the IAAF, over allegations of doping in athletics.
6 hours ago

Corbyn backs greater public ownership
1 hour ago

Ferguson marks Michael Brown killing
25 minutes ago

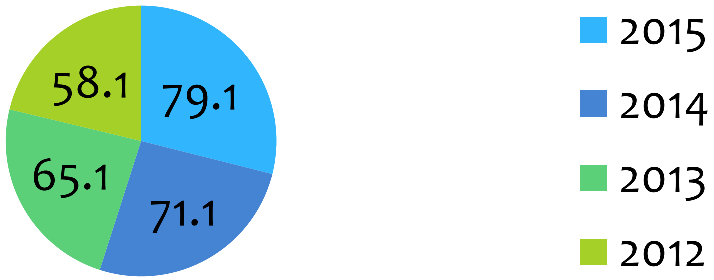
Features

'I found my blood score'
Eilish McColgan opens up on blood testing in athletics

http://www.bbc.co.uk/news/uk-33835185

Why Research into Software Security?

Annual Spending on Information Security in Billion Dollars Worldwide



http://www.gartner.com/newsroom/id/2828722

What we have discovered is only a handful on cyber-attacks and software vulnerabilities

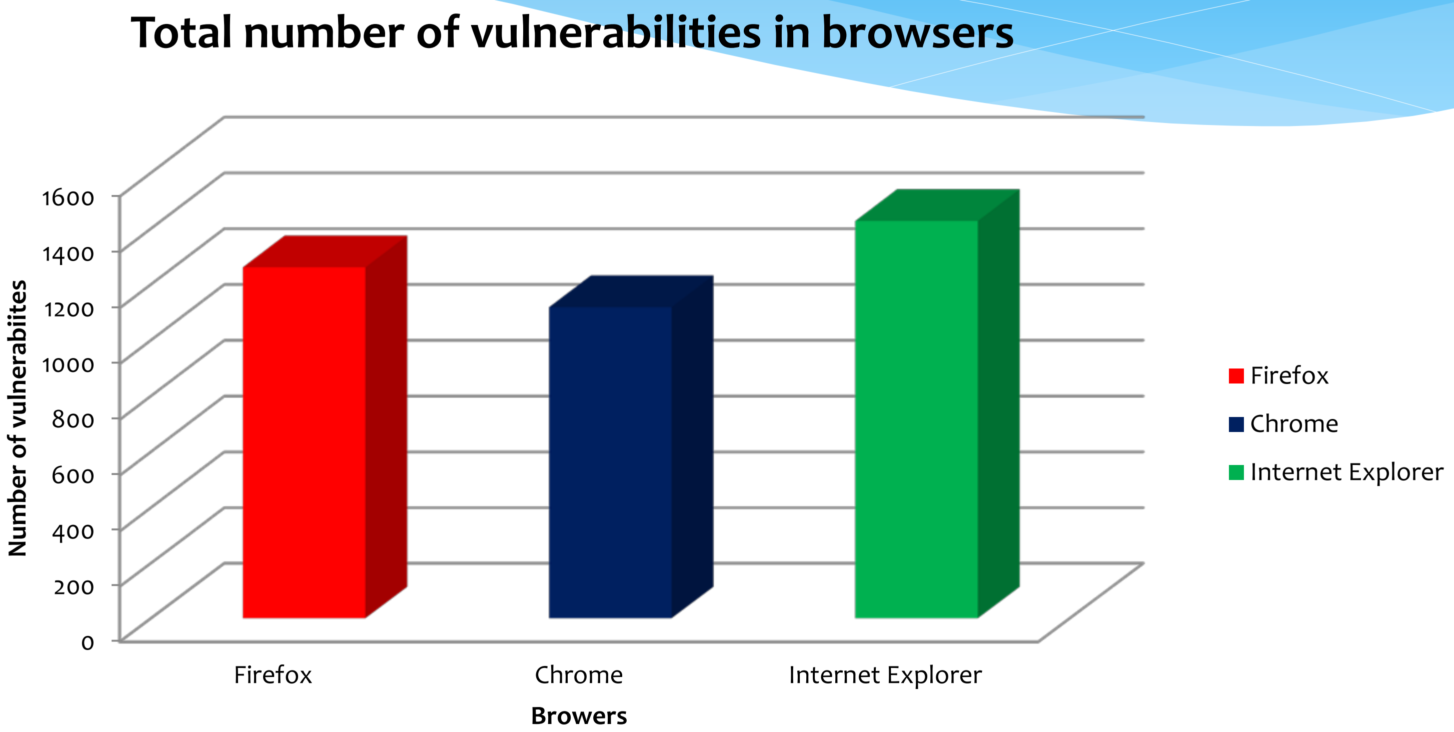
My Personal Moto Learned from childhood : As Avvaiyar (a Tamil Lady poet from 1st-2nd Century of C.E (roughly 2000 years ago Common Era or A.D) wrote (wikipedia):

"Katrathu Kai Mann Alavu, Kallathathu Ulagalavu"

meaning roughly "What you have learned is only a handful; What you haven't learned is the size of the world"

NASA link to Avvaiyar from 4th Century

Known Vulnerabilities: A History of Knowledge



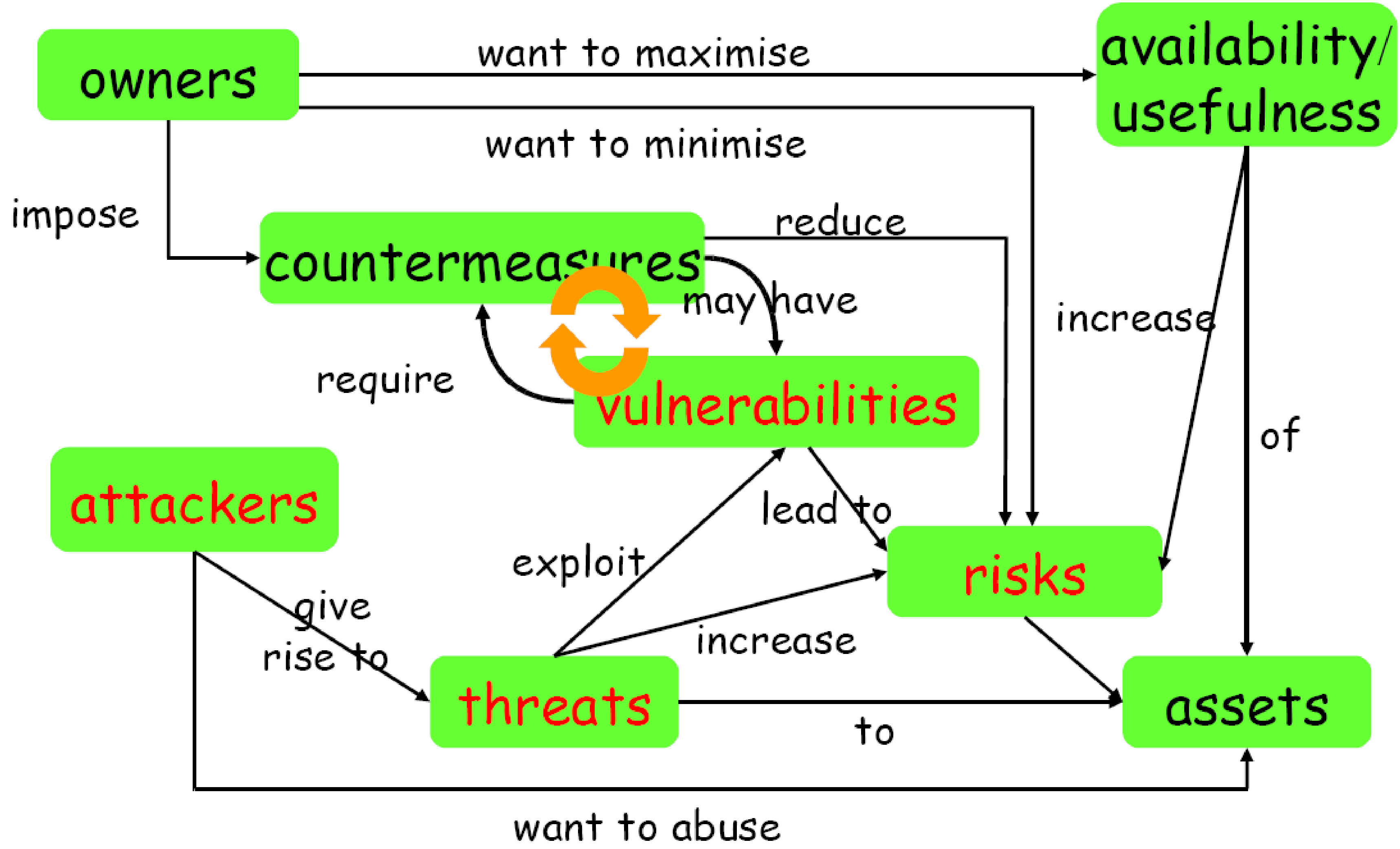
Software Security RE

Software Security Definitions and Perspective

Building Trust into Software Systems

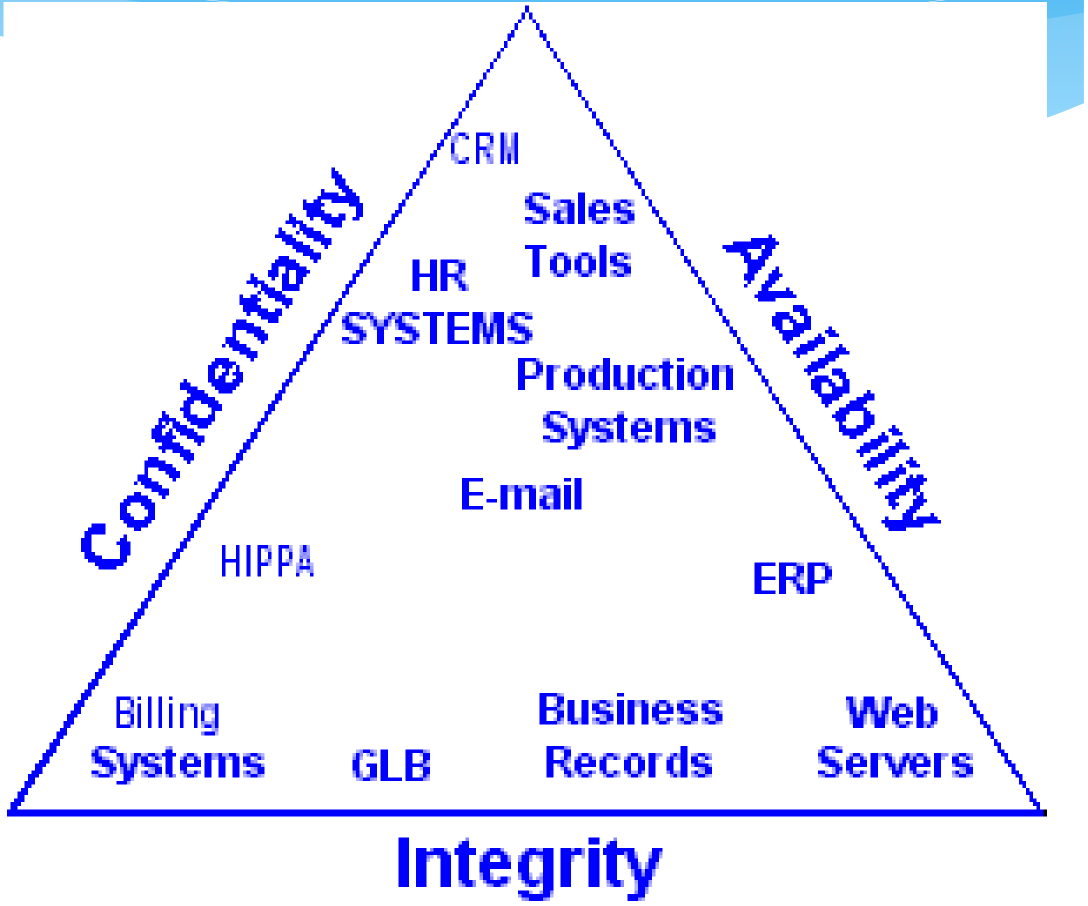
Security Concepts

What is Security?

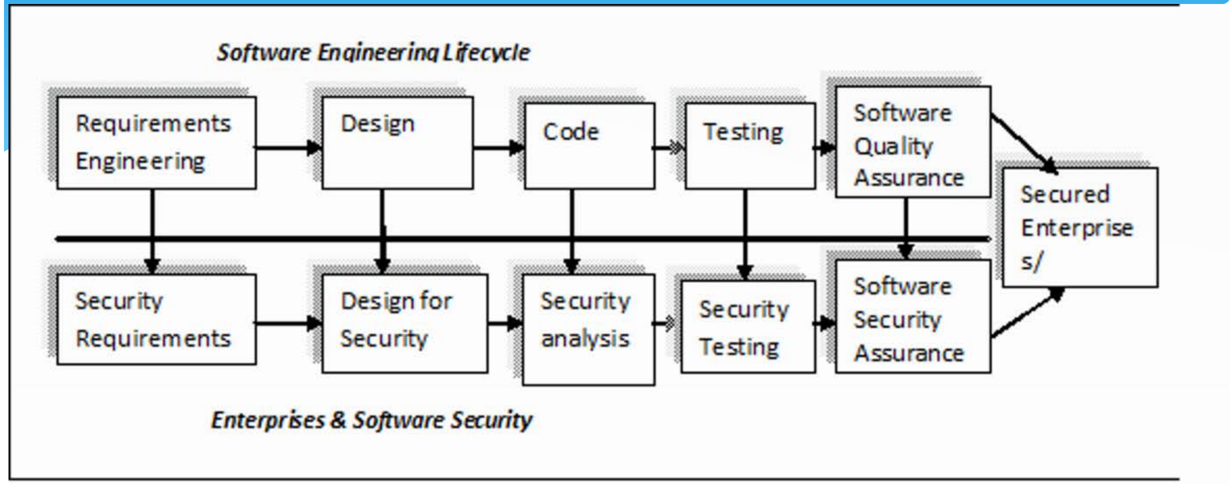


Classical Security Triangle

We need include socio-technical perspective and trust in the current and emerging technologies



Software Security vs Computer Security vs Information Security

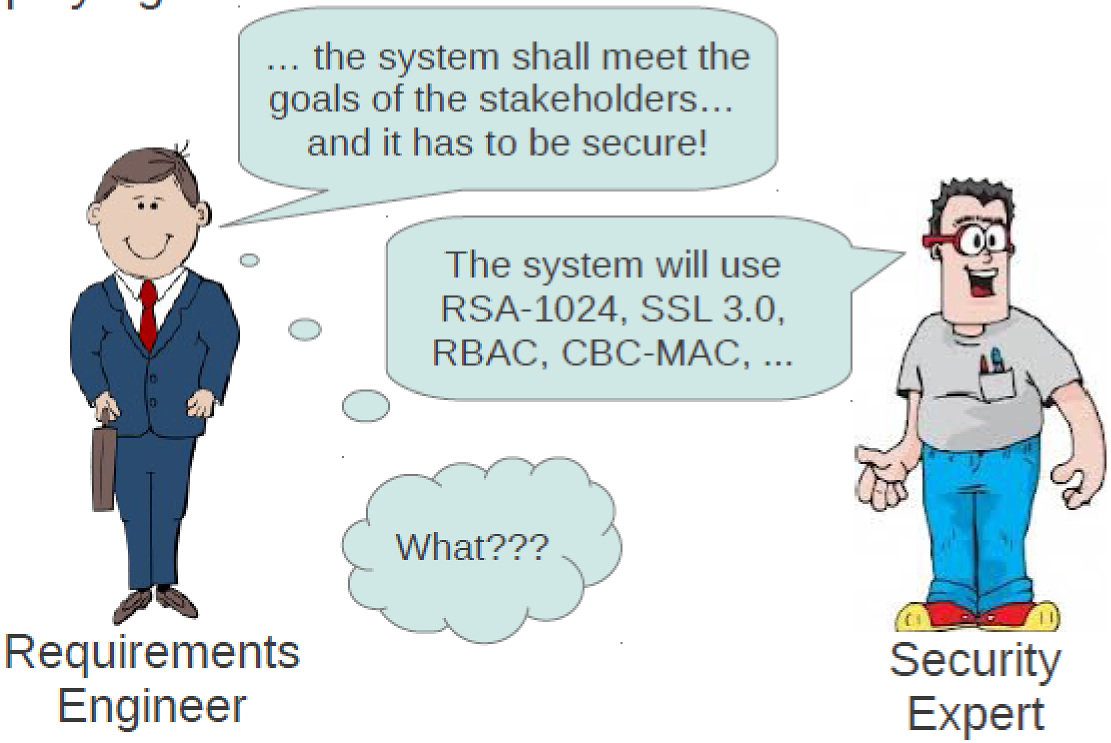


- Software Engineering has established techniques, methods and technology over two decades.
- However, due to the lack of understanding of software security vulnerabilities, we have not been so successful in applying software engineering principles when developing secure software systems.
- Security can’t be just added later to a delivered product

Why Security RE?

Distinction between functional and service requirements vs quality requirements such as Security

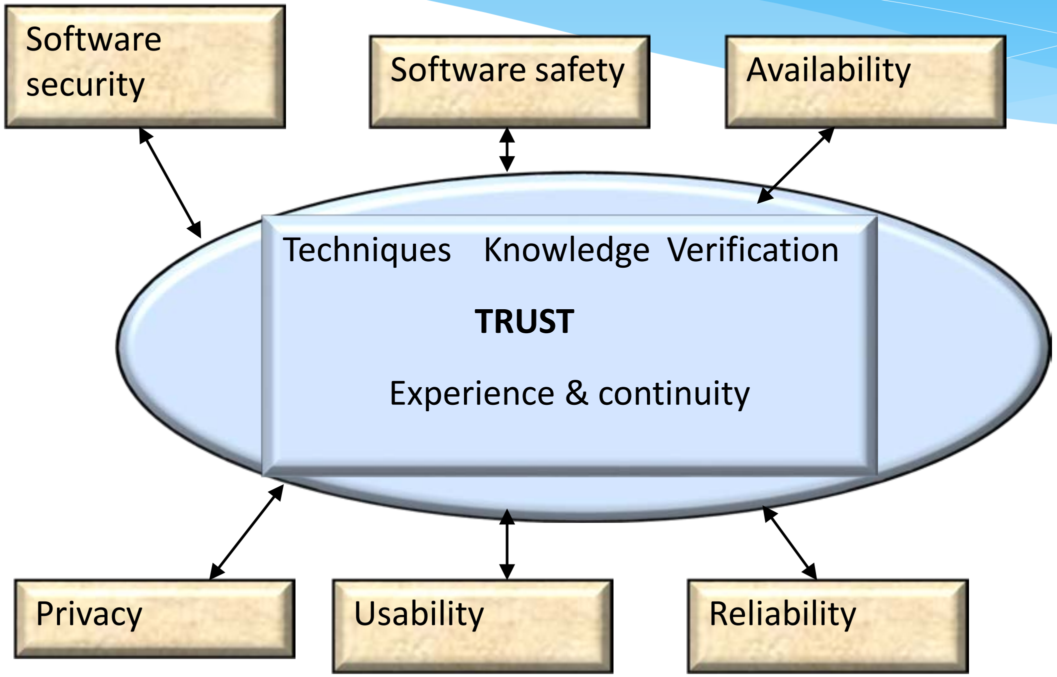
Oversimplifying...


... the system shall meet the goals of the stakeholders... and it has to be secure!
The system will use RSA-1024, SSL 3.0, RBAC, CBC-MAC, ...
What???
Requirements Engineer
Security Expert

Different perspectives, primitives, and vocabularies

LEEDS BECKETT UNIVERSITY

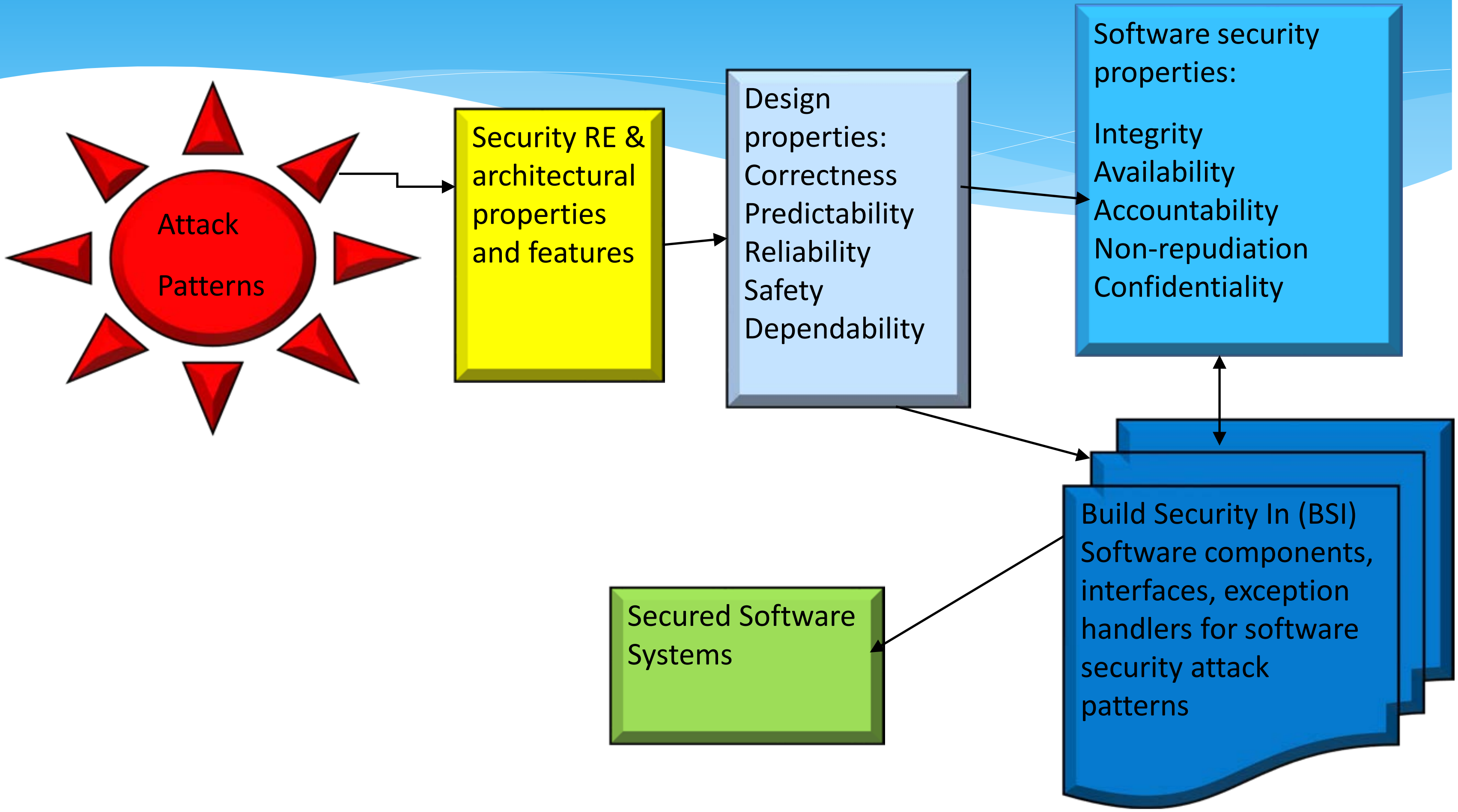
Trust and resiliency model for software security



Wee need to include trust modelling (relationships and agreements) and resilient computing (survivability modelling)

Design For Software Security
A unique Chapter in my book

Design For Software Security



Attack Patterns

Security RE & architectural properties and features

Design properties:
Correctness
Predictability
Reliability
Safety
Dependability

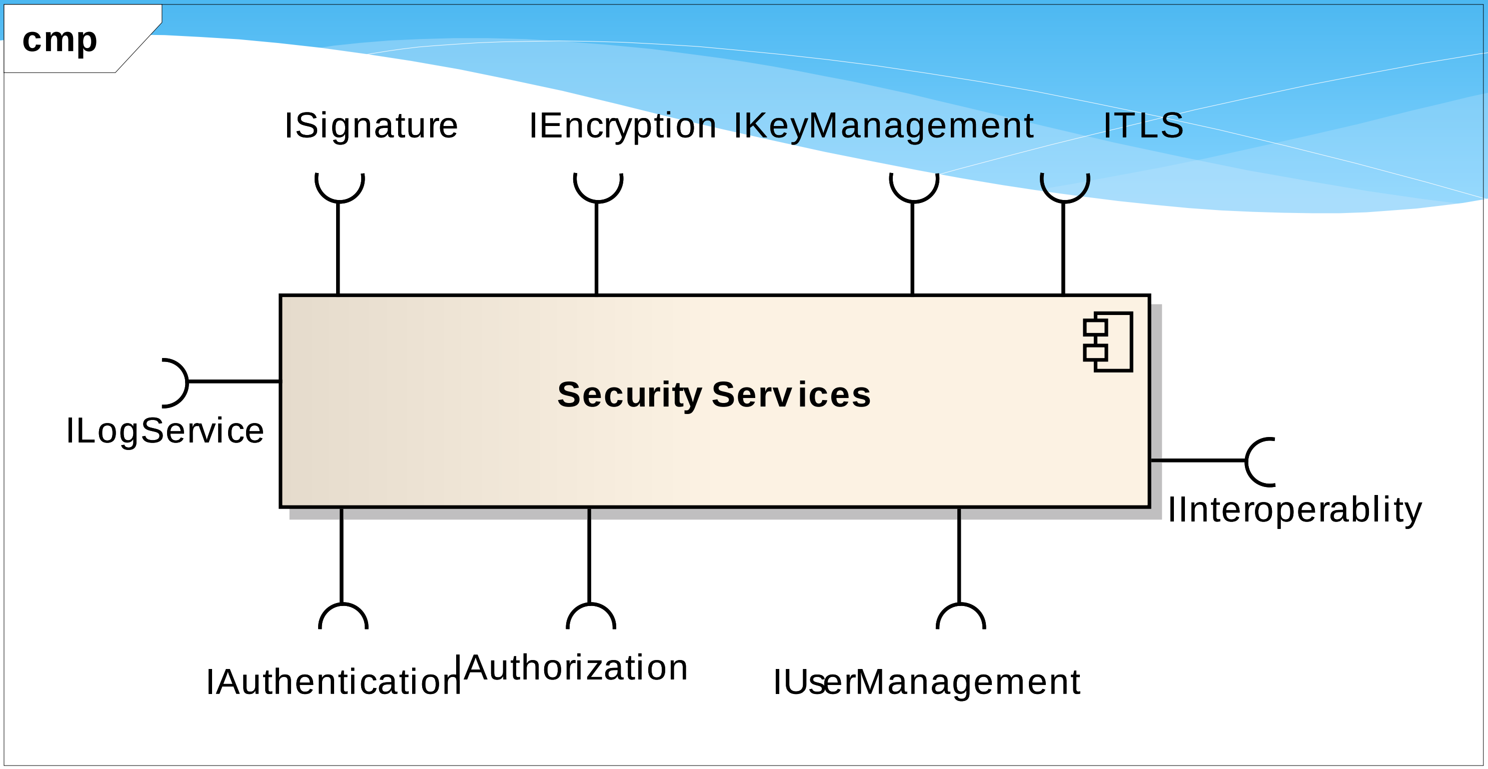
Software security properties:

Integrity
Availability
Accountability
Non-repudiation
Confidentiality

Build Security In (BSI) Software components, interfaces, exception handlers for software security attack patterns

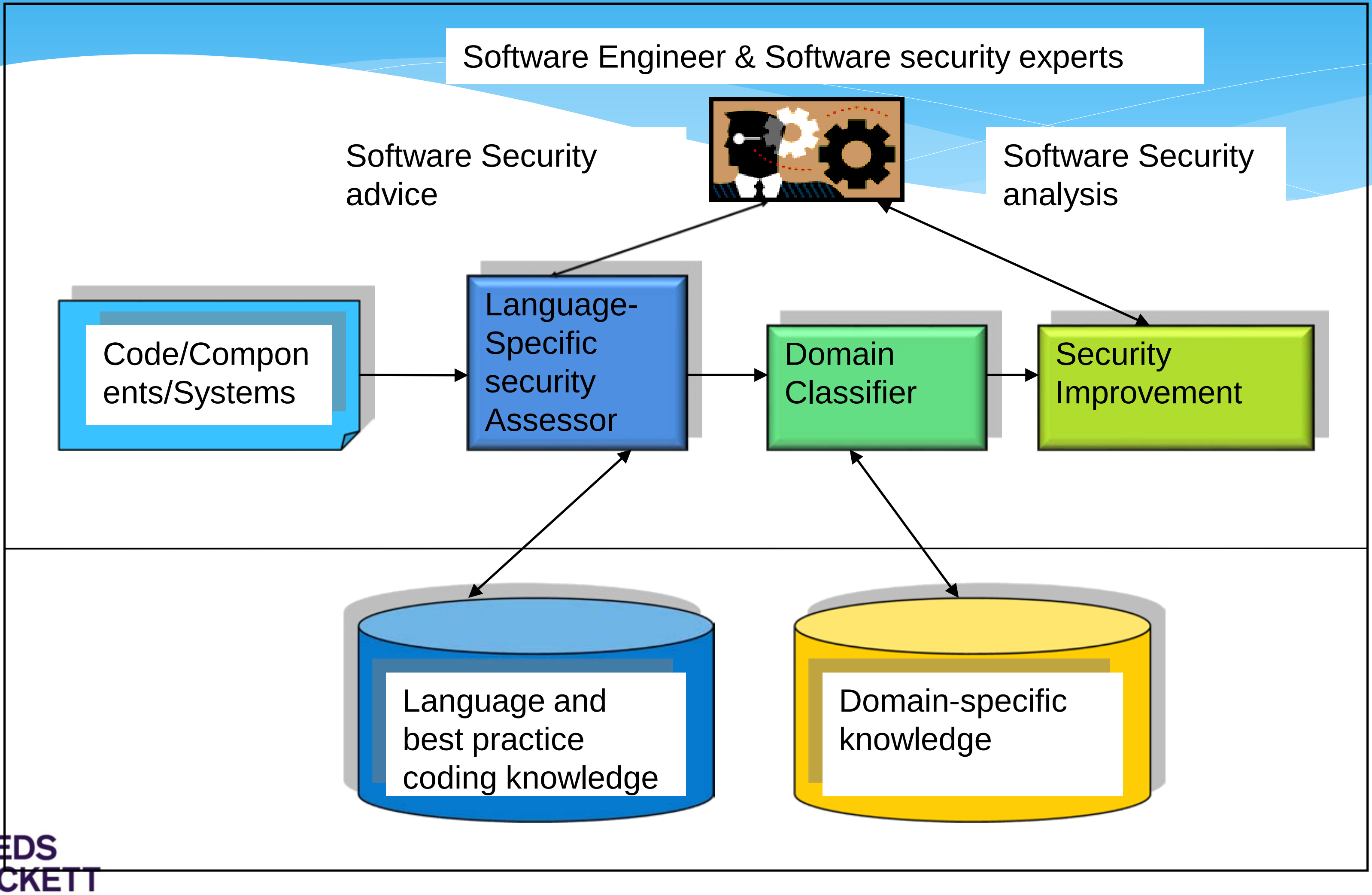
Secured Software Systems

Build Security In (BSI) Component Model: Independent and Pluggable to Any Applications



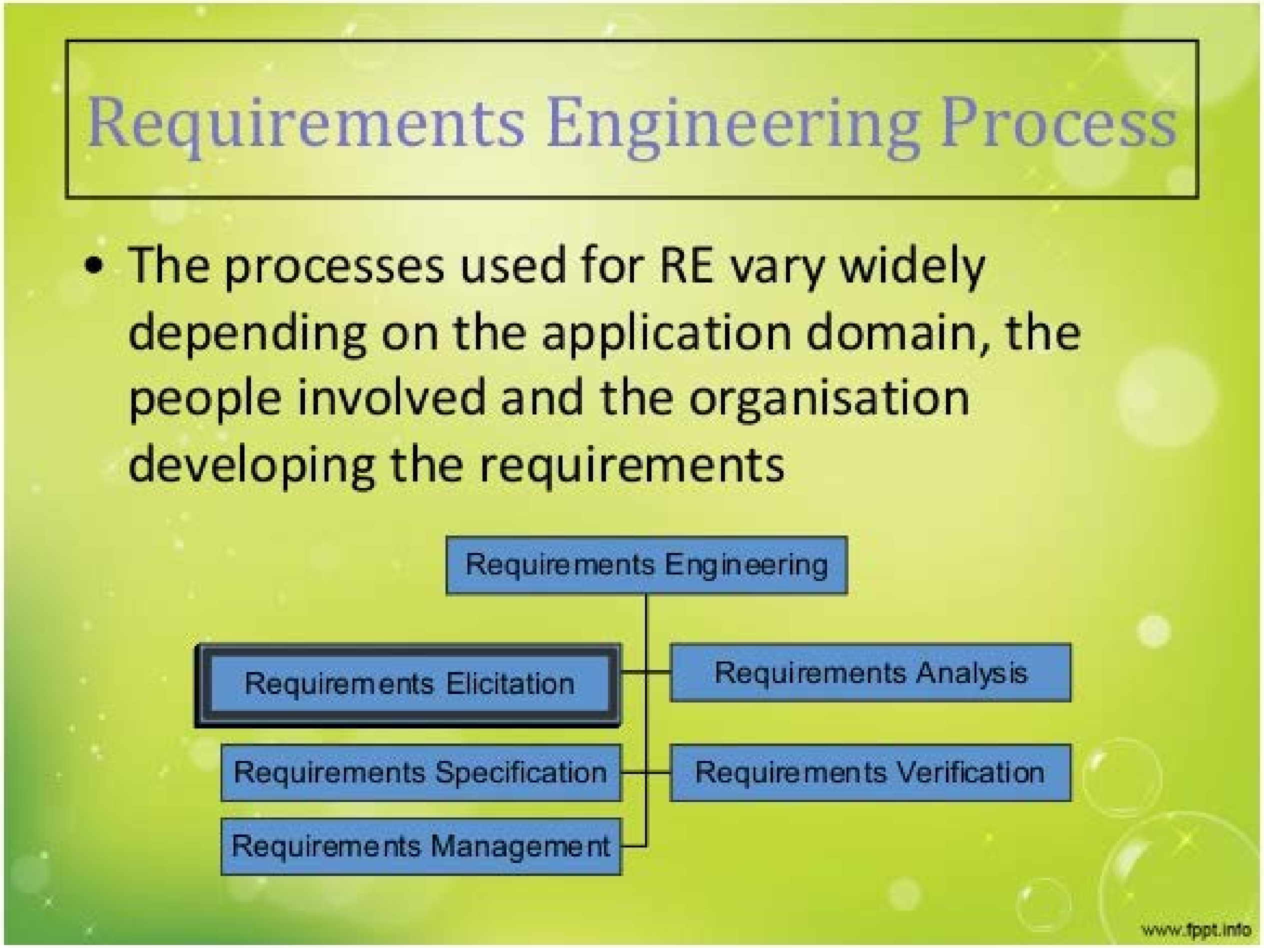
An example of design for software security

Automated Secure Code Improvement


Software Engineer & Software security experts
Software Security advice
Software Security analysis
Code/Components/Systems
Language-Specific security Assessor
Domain Classifier
Security Improvement
Language and best practice coding knowledge
Domain-specific knowledge

SSRE Processes

Traditional RE Process



Requirements Engineering Process

- The processes used for RE vary widely depending on the application domain, the people involved and the organisation developing the requirements

Requirements Engineering

Requirements Elicitation

Requirements Analysis

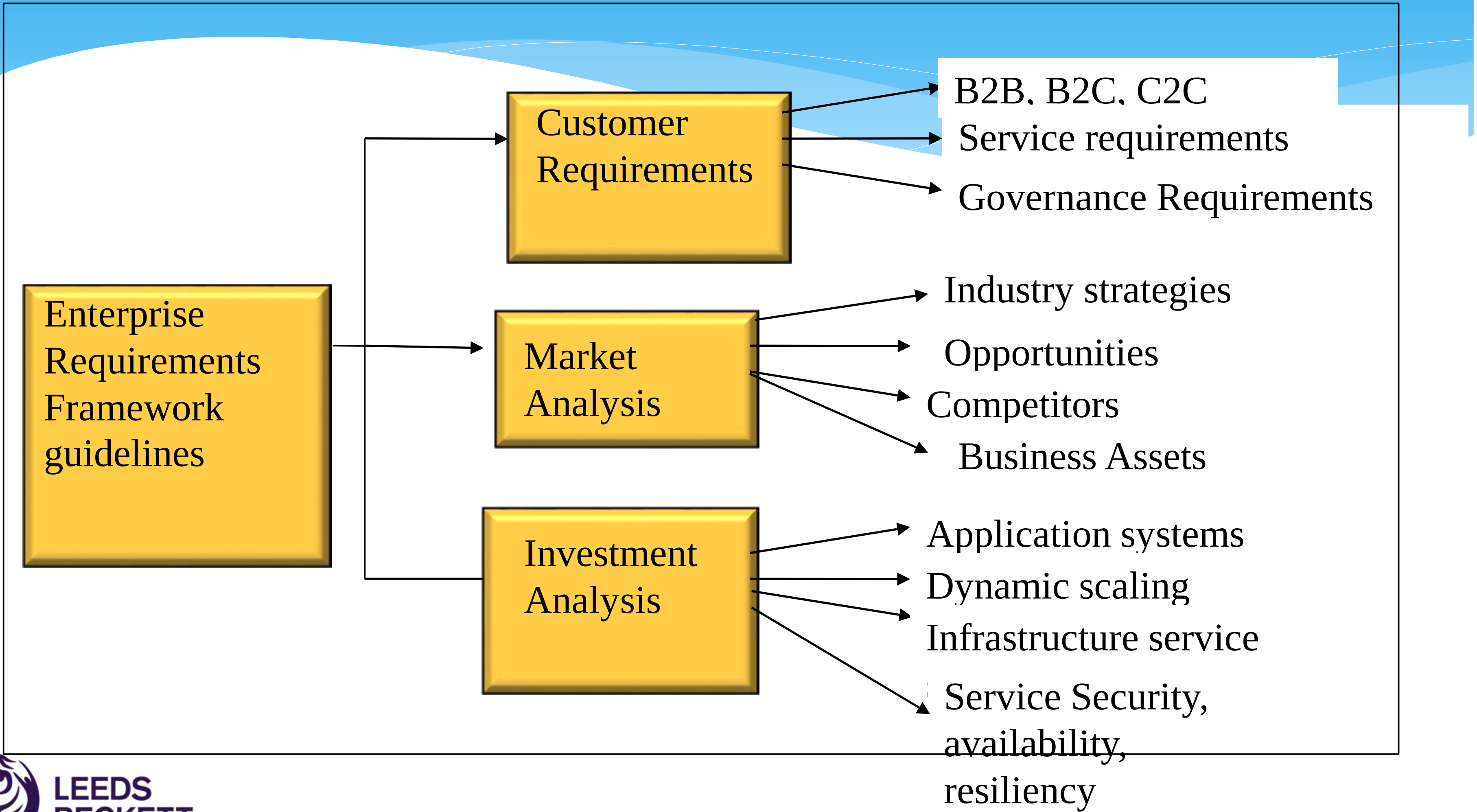
Requirements Specification

Requirements Verification

Requirements Management

www.fppt.info

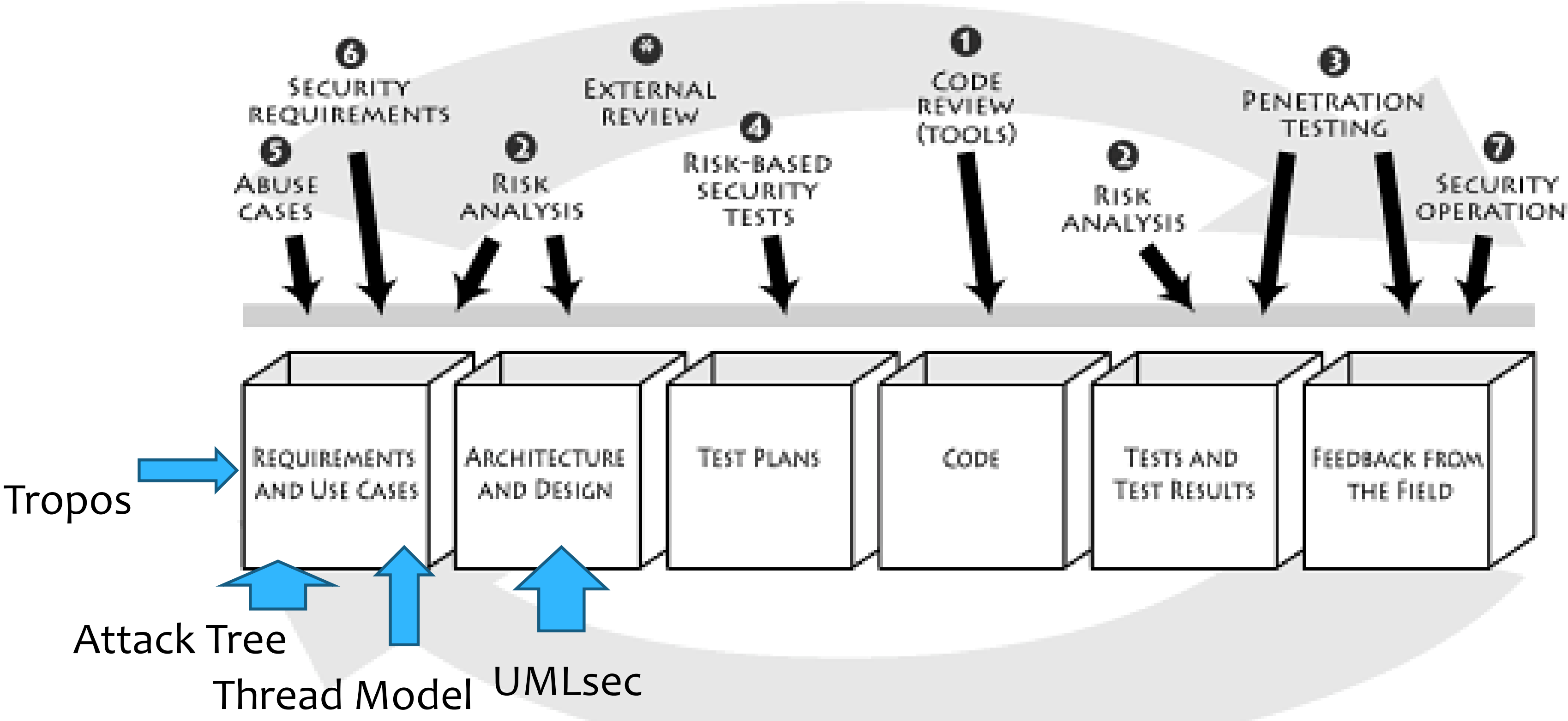
Requirements Classification



Best Practices SSRE

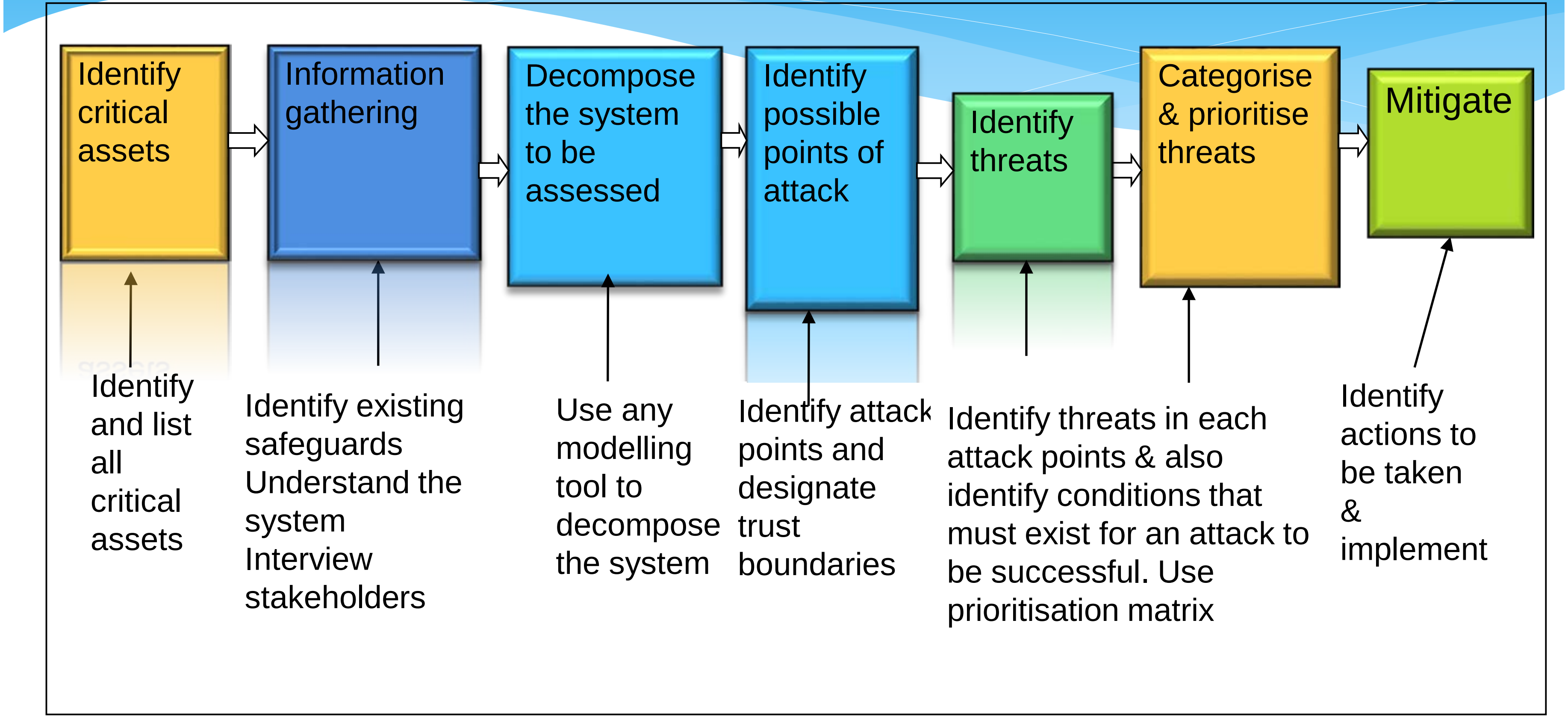
- Eliciting and extracting requirements for software security explicitly with visual notations
- Prioritising software security requirements
- Risk assessment and mitigation for software security requirements
- Use security modelling techniques Tropos, MS Threat Modelling, Attack Tree, Attack Patterns
- Design and implement software security requirements
- Providing SDLC life-cycle support

Secure SDLC Touchpoints



SDLC security touchpoints (Allen et al 2008, p248)

Threat Modelling Process



Identify critical assets

Identify and list all critical assets

Information gathering

Identify existing safeguards
Understand the system
Interview stakeholders

Decompose the system to be assessed

Use any modelling tool to decompose the system

Identify possible points of attack

Identify attack points and designate trust boundaries

Identify threats

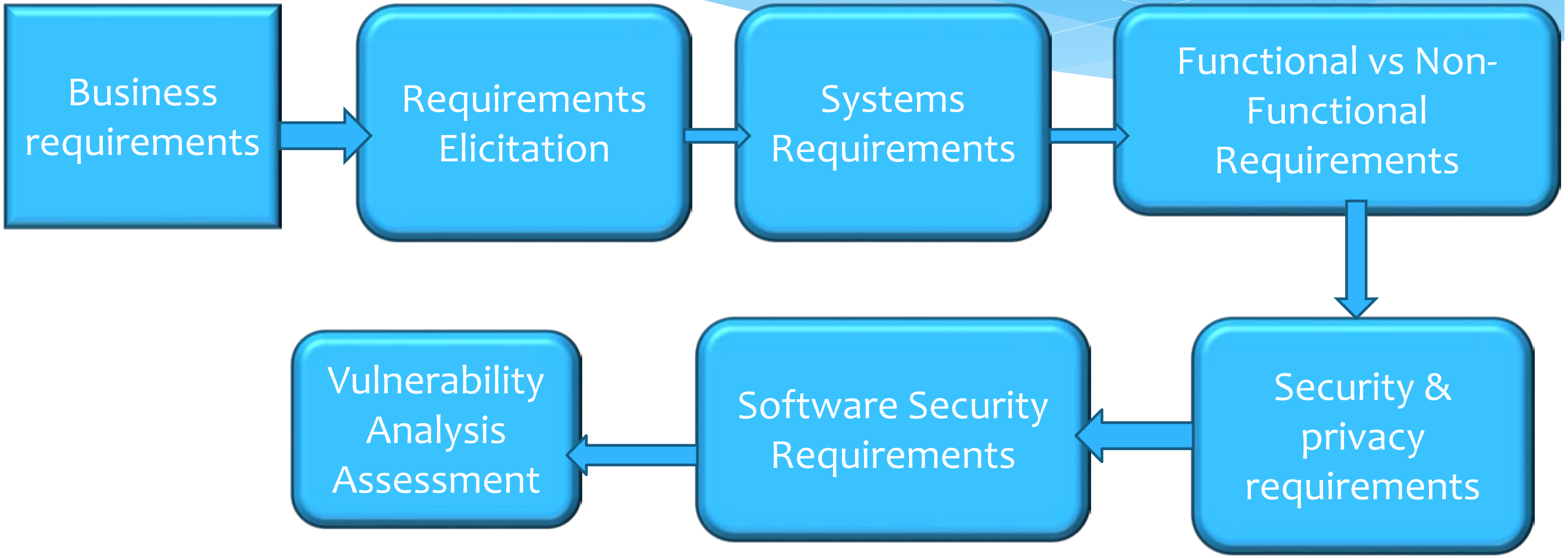
Identify threats in each attack points & also identify conditions that must exist for an attack to be successful. Use prioritisation matrix

Categorise & prioritise threats

Mitigate

Identify actions to be taken & implement

Software Security RE Process


Business requirements

Requirements Elicitation

Systems Requirements

Functional vs Non-Functional Requirements

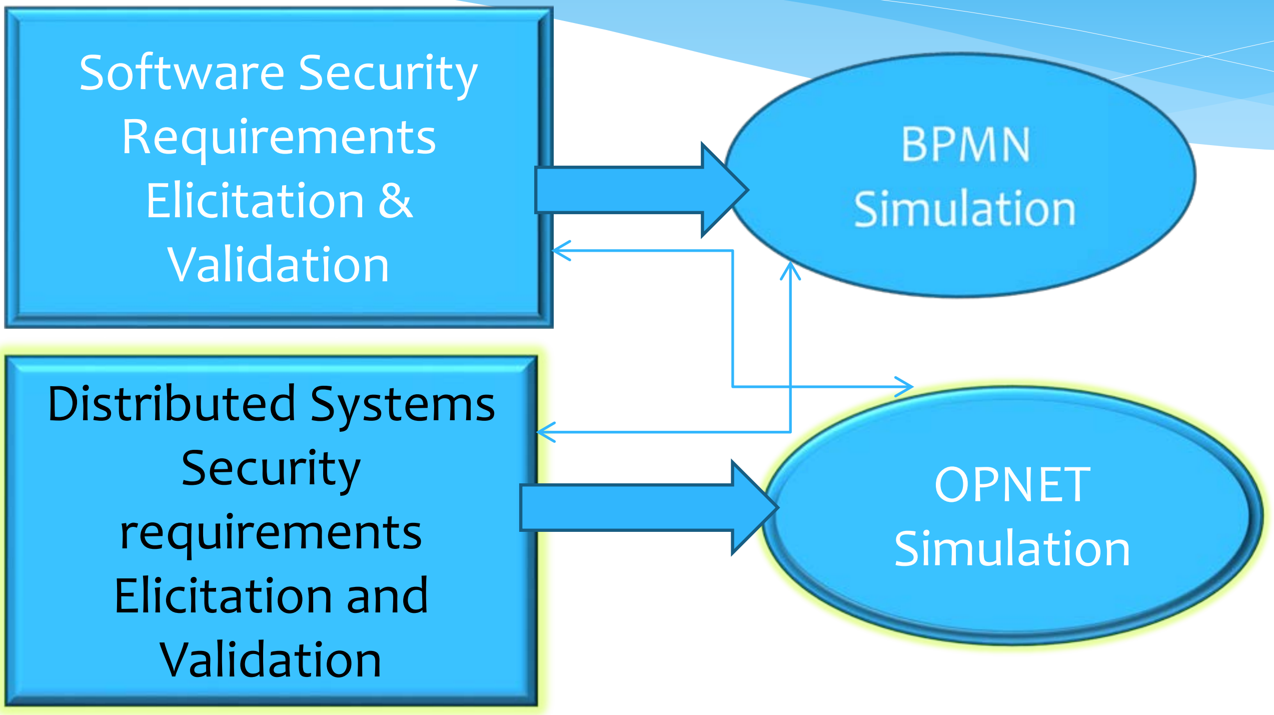
Security & privacy requirements

Software Security Requirements

Vulnerability Analysis Assessment

LEEDS BECKETT UNIVERSITY

Integrated SSRE Process Validation Tools


Software Security Requirements Elicitation & Validation

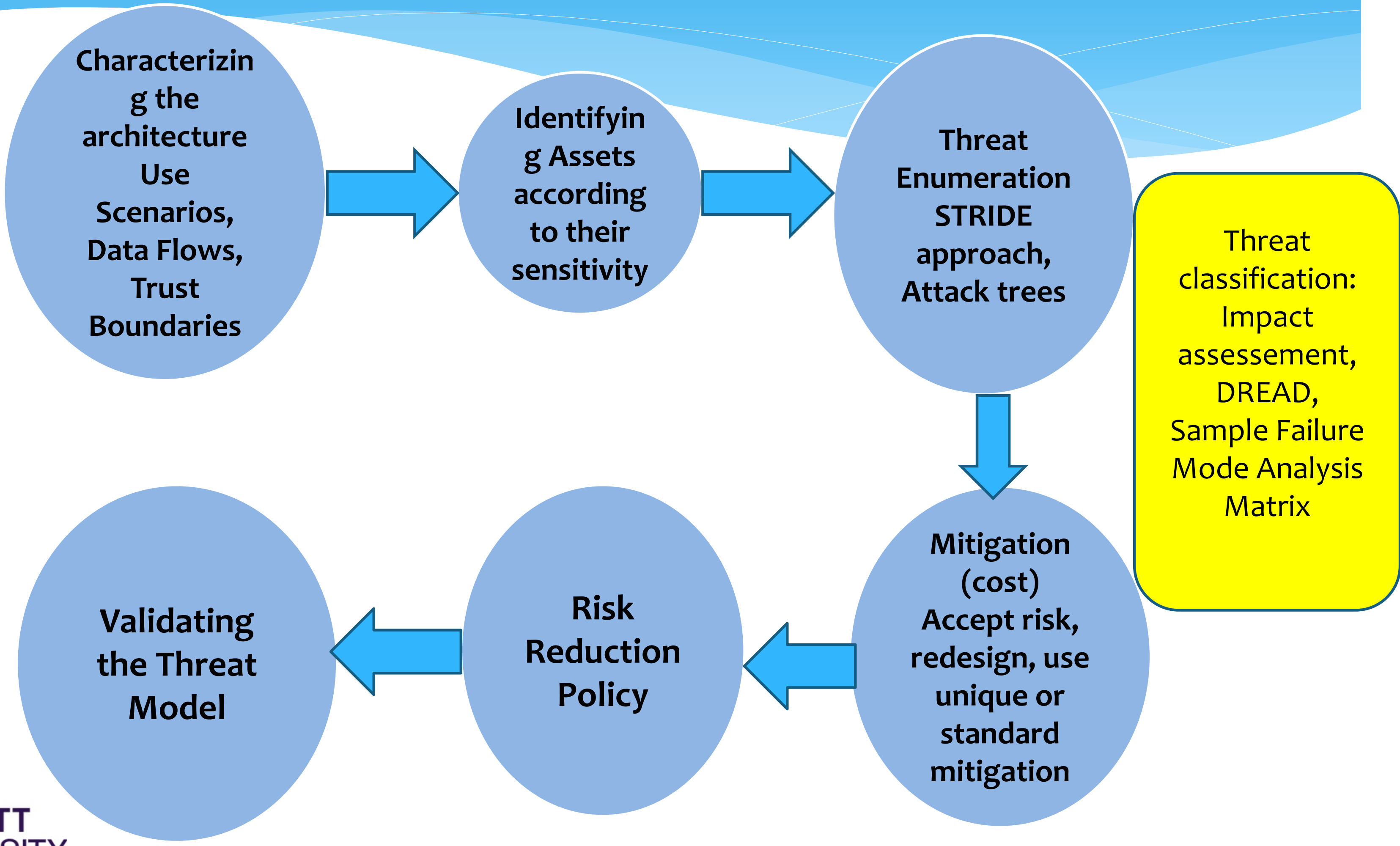
BPMN Simulation

Distributed Systems Security requirements Elicitation and Validation

OPNET Simulation

Allows to validate security requirements

Threat Modeling Framework



Characterizing the architecture Use Scenarios, Data Flows, Trust Boundaries

Identifying Assets according to their sensitivity

Threat Enumeration STRIDE approach, Attack trees

Threat classification: Impact assessement, DREAD, Sample Failure Mode Analysis Matrix

Mitigation (cost) Accept risk, redesign, use unique or standard mitigation

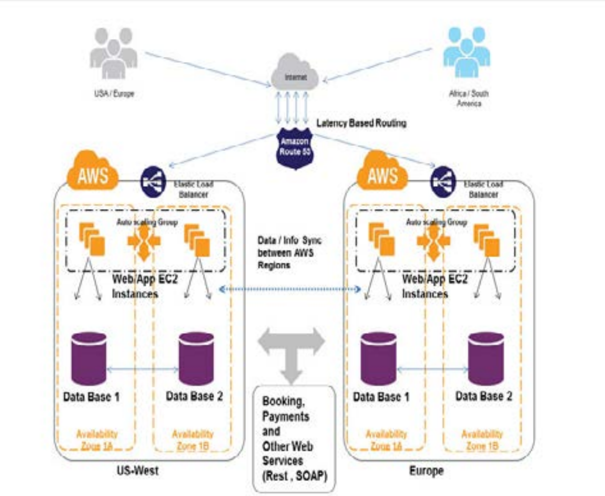
Risk Reduction Policy

Validating the Threat Model

LEEDS BECKETT UNIVERSITY

Amazon EC2 Architectural Simulation

1

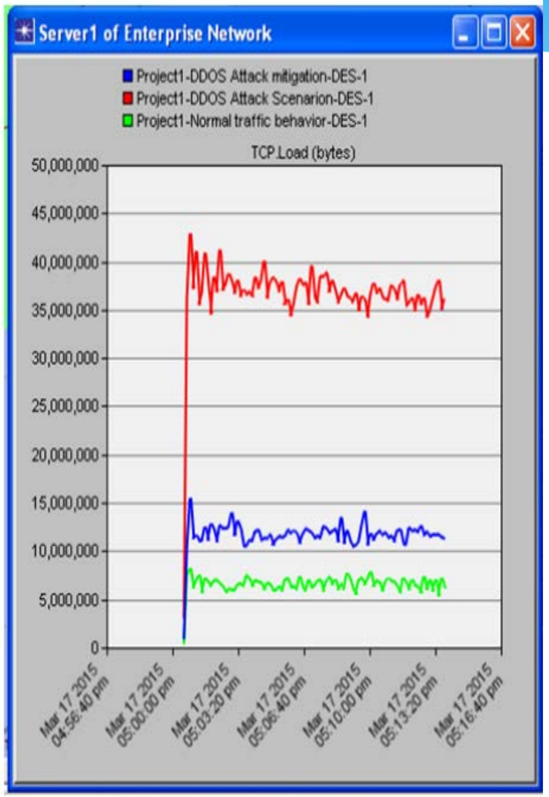


2

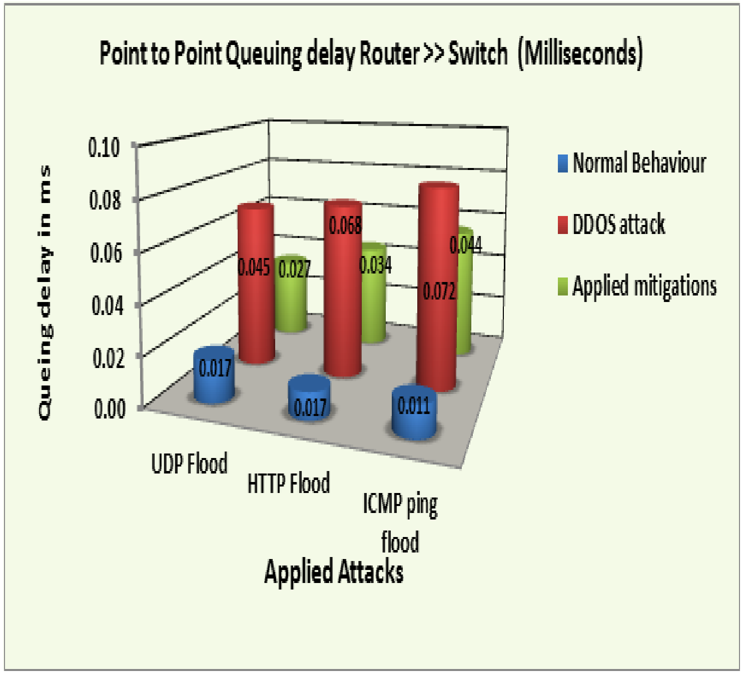
3

4

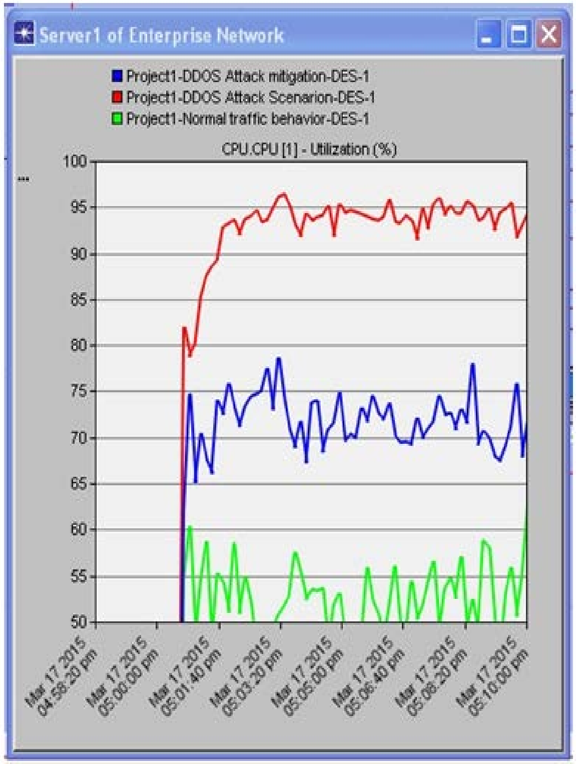
Results and Analysis



Performance Simulation: Network Load



Queuing Delay DDoS Attck Scenario Simulation

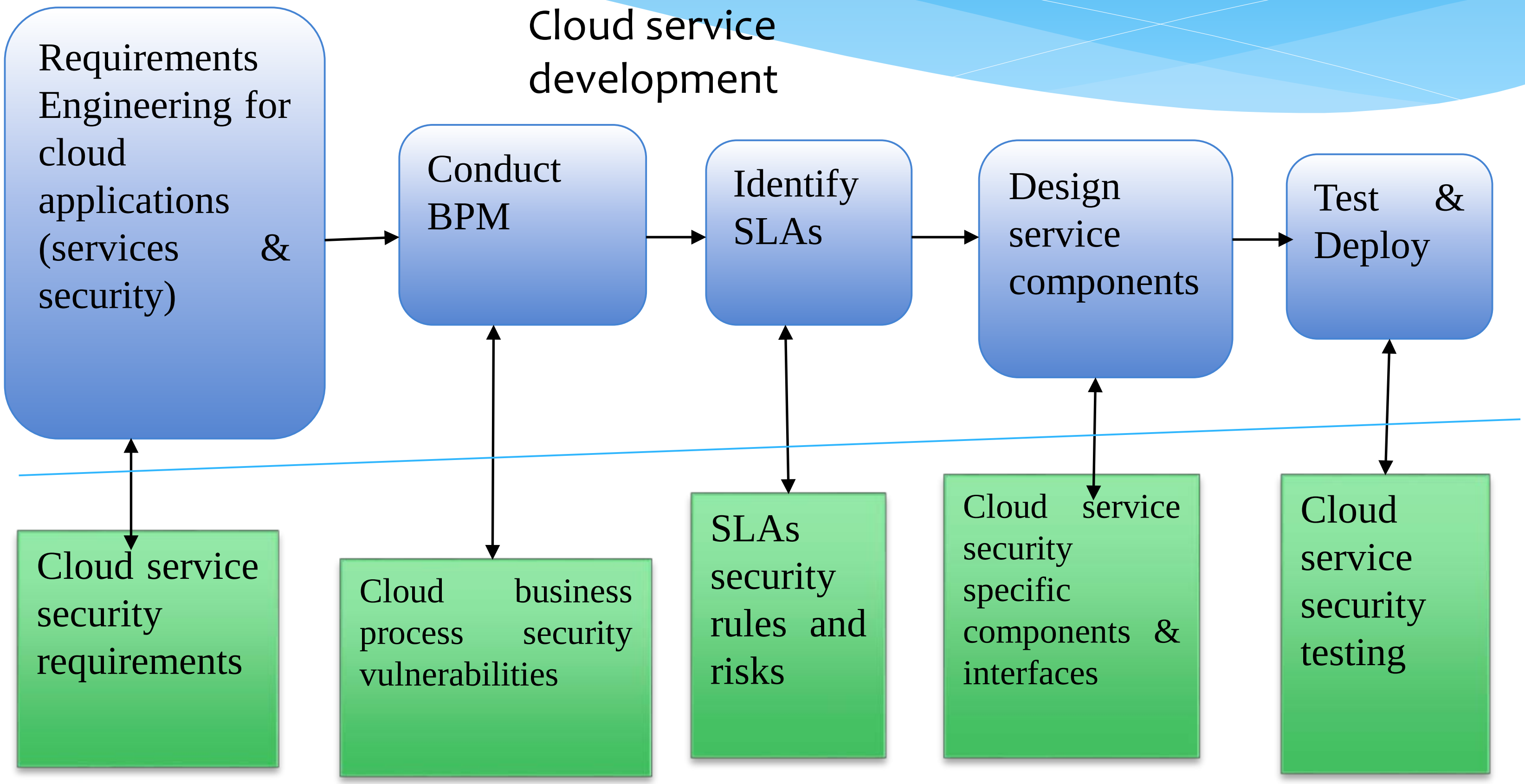


EC2 Server Utilization Simulation

LEEDS
BECKETT
UNIVERSITY

Security Requirements Process Simulation with OPNET & BPMN

Cloud service security development process with build in security – Our Systematic Approach to adopt BSI as part of CCAF



Cloud service development

Requirements Engineering for cloud applications (services & security)

Conduct BPM

Identify SLAs

Design service components

Test & Deploy

Cloud service security requirements

Cloud business process security vulnerabilities

SLAs security rules and risks

Cloud service security specific components & interfaces

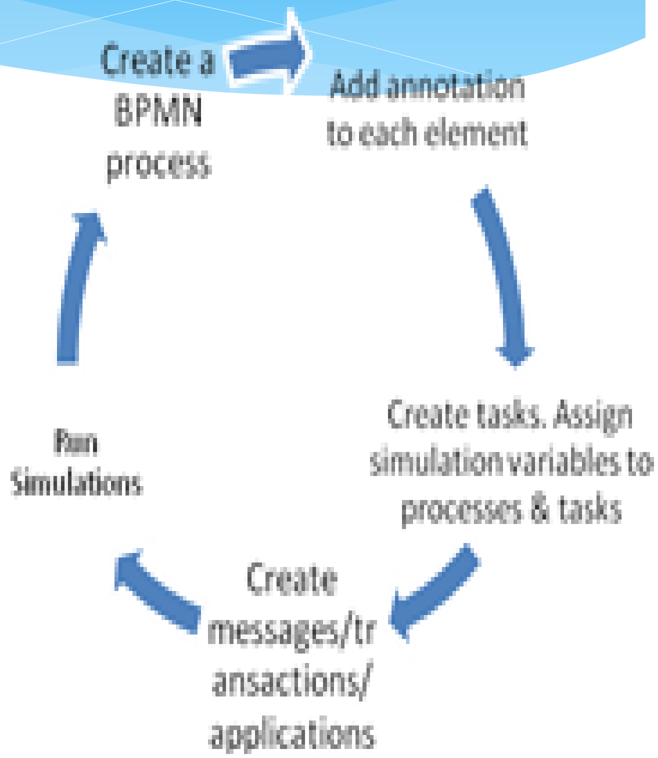
Cloud service security testing

LEEDS BECKETT UNIVERSITY

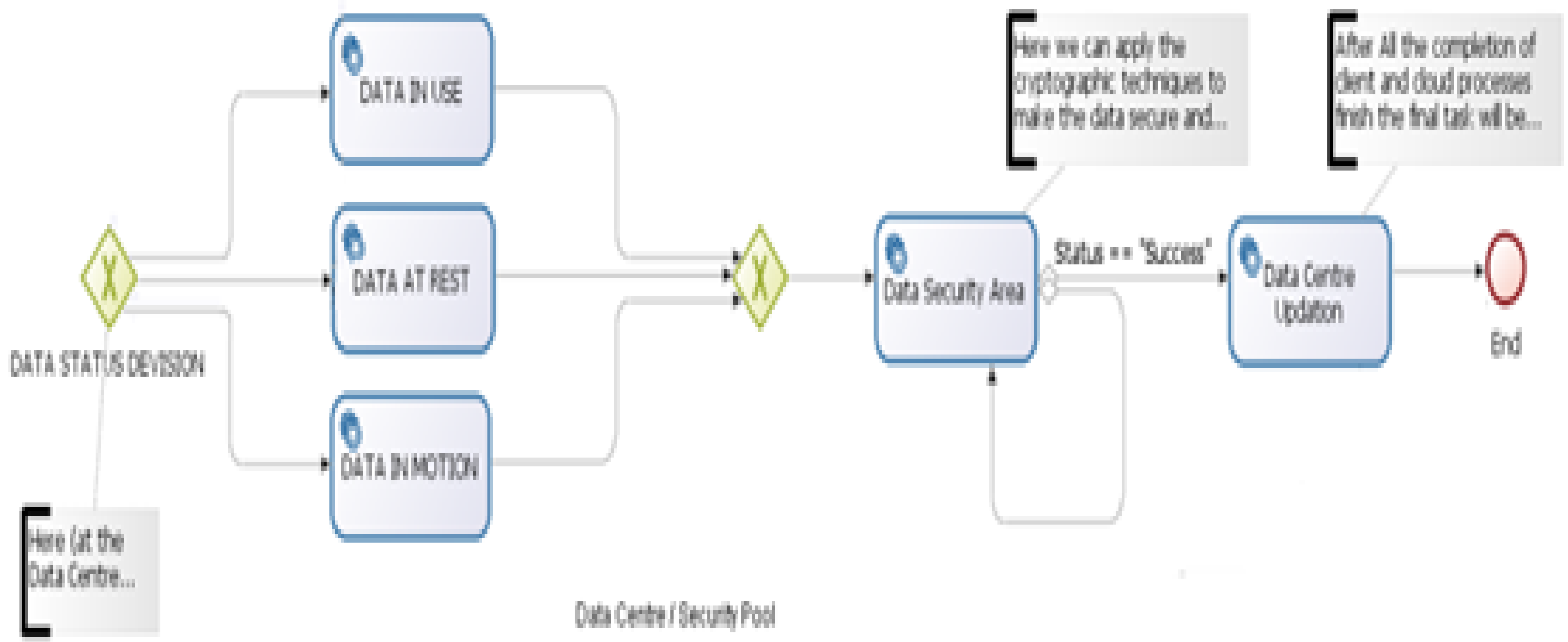
Build Cloud Security In – Cloud service development with build-in security

BPMN Simulation Process

BPMN simulation process consists of a number of cyclic phases as shown in this illustration. BPMN starts with an actor called Client with a small circle notation which sends a message to a process (Data Request with rounded square) which task has been devoted to take action based the request and therefore send a message to the cloud (finishing circle). The second phase is to annotate each element in the process and thirdly to create tasks, assign simulation variables (different types of requests both valid and invalid) to process and tasks with that process. Finally, create messages between elements in the process and run a number of simulations.

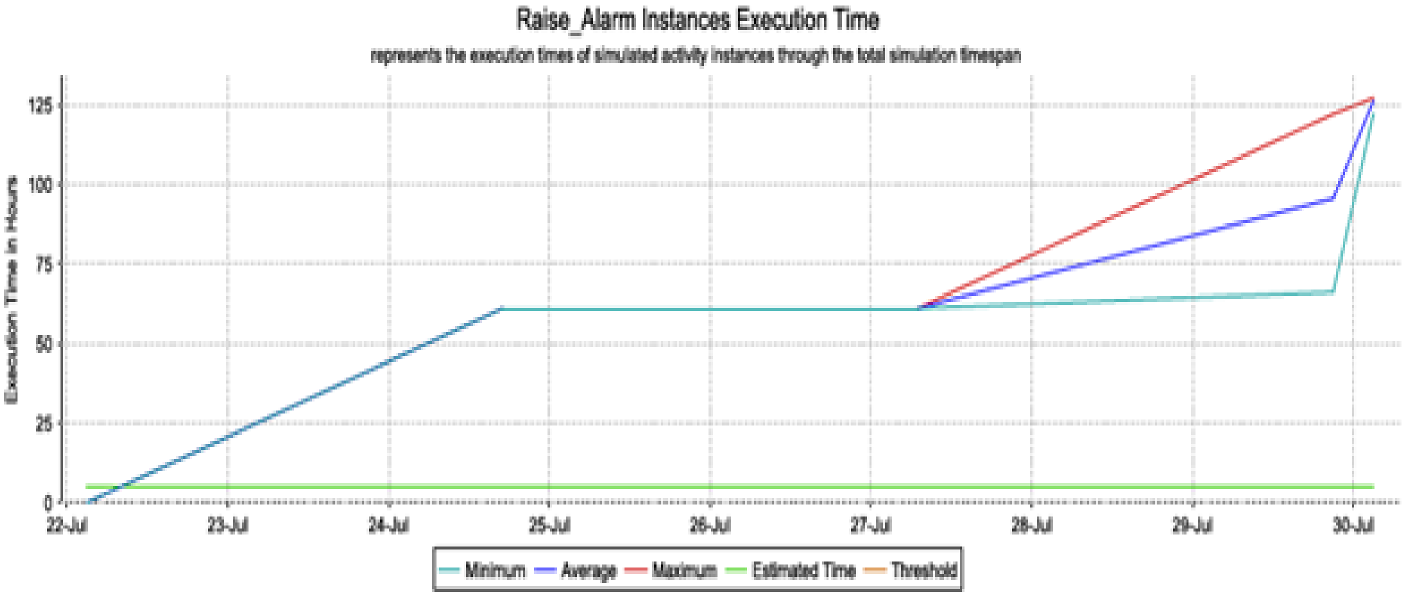

Create a BPMN process
Add annotation to each element
Create tasks. Assign simulation variables to processes & tasks
Create messages/transactions/applications
Run Simulations

Amazon EC2: Large Scale Case Study: Cloud Data Security


DATA IN USE
DATA AT REST
DATA IN MOTION
DATA STATUS DEVISION
Here (at the Data Centre...
Data Centre / Security Pool
Here we can apply the cryptographic techniques to make the data secure and...
Data Security Area
Status == 'Success'
After All the completion of client and cloud processes finish the final task will be...
Data Centre Updation
End

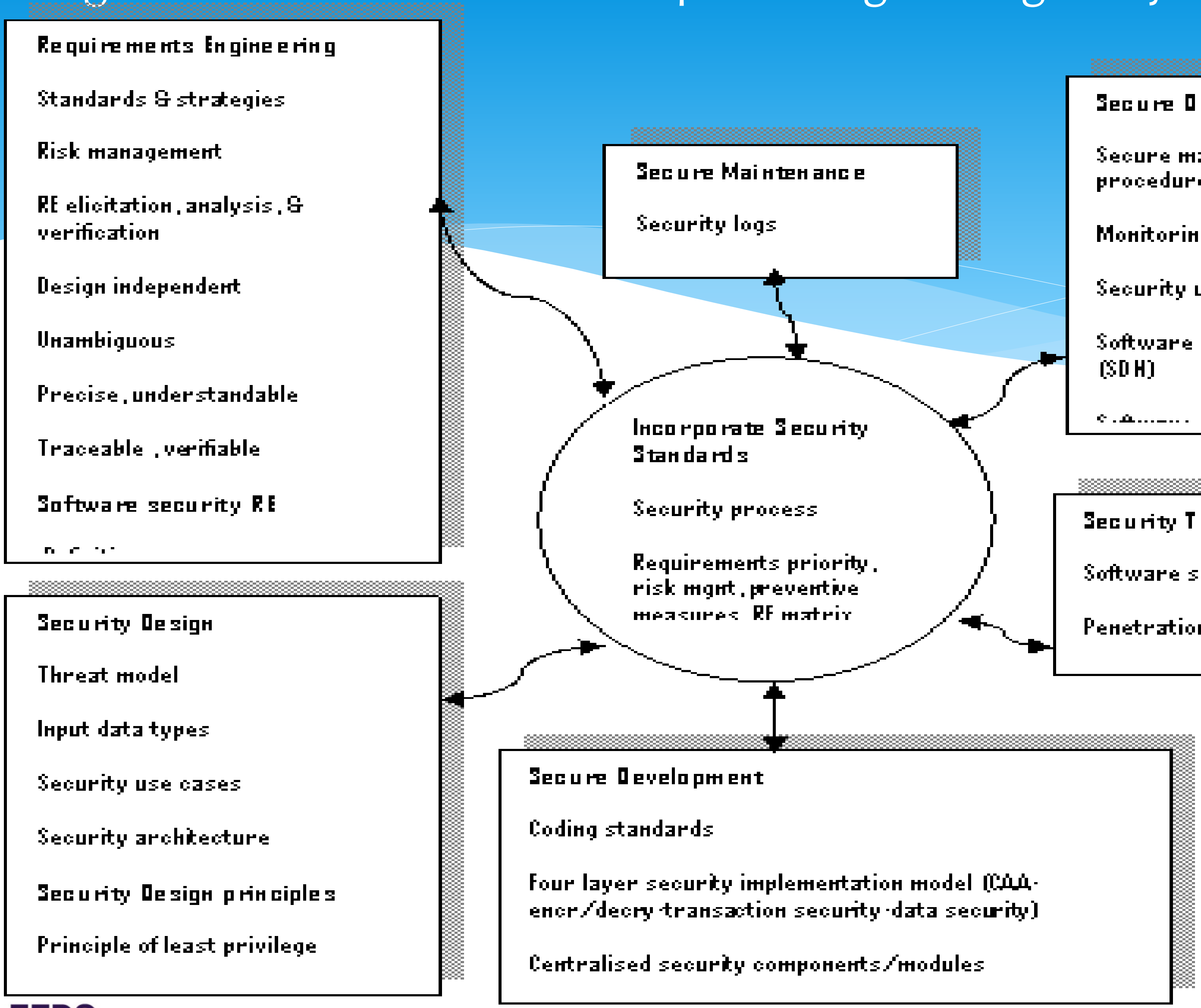
Security measures impacts on execution time

The implications of this result show that data security instances execution time can be high when data was constantly in use. On the other hand, the execution time was less than 2 hours if data was not in use.



LEEDS BECKETT UNIVERSITY

Integrated secure software development engineering life cycle (IS-SDLC)



Requirements Engineering

Standards & strategies

Risk management

RE elicitation, analysis, & verification

Design independent

Unambiguous

Precise, understandable

Traceable , verifiable

Software security RE

Secure Maintenance

Security logs

Secure Deployment

Secure management procedures

Monitoring requirements

Security upgrade procedures

Software defined networking (SDN)

Incorporate Security Standards

Security process

Requirements priority, risk mgnt, preventive measures, RE matrix

Security Testing

Software security testing

Penetration testing

Security Design

Threat model

Input data types

Security use cases

Security architecture

Security Design principles

Principle of least privilege

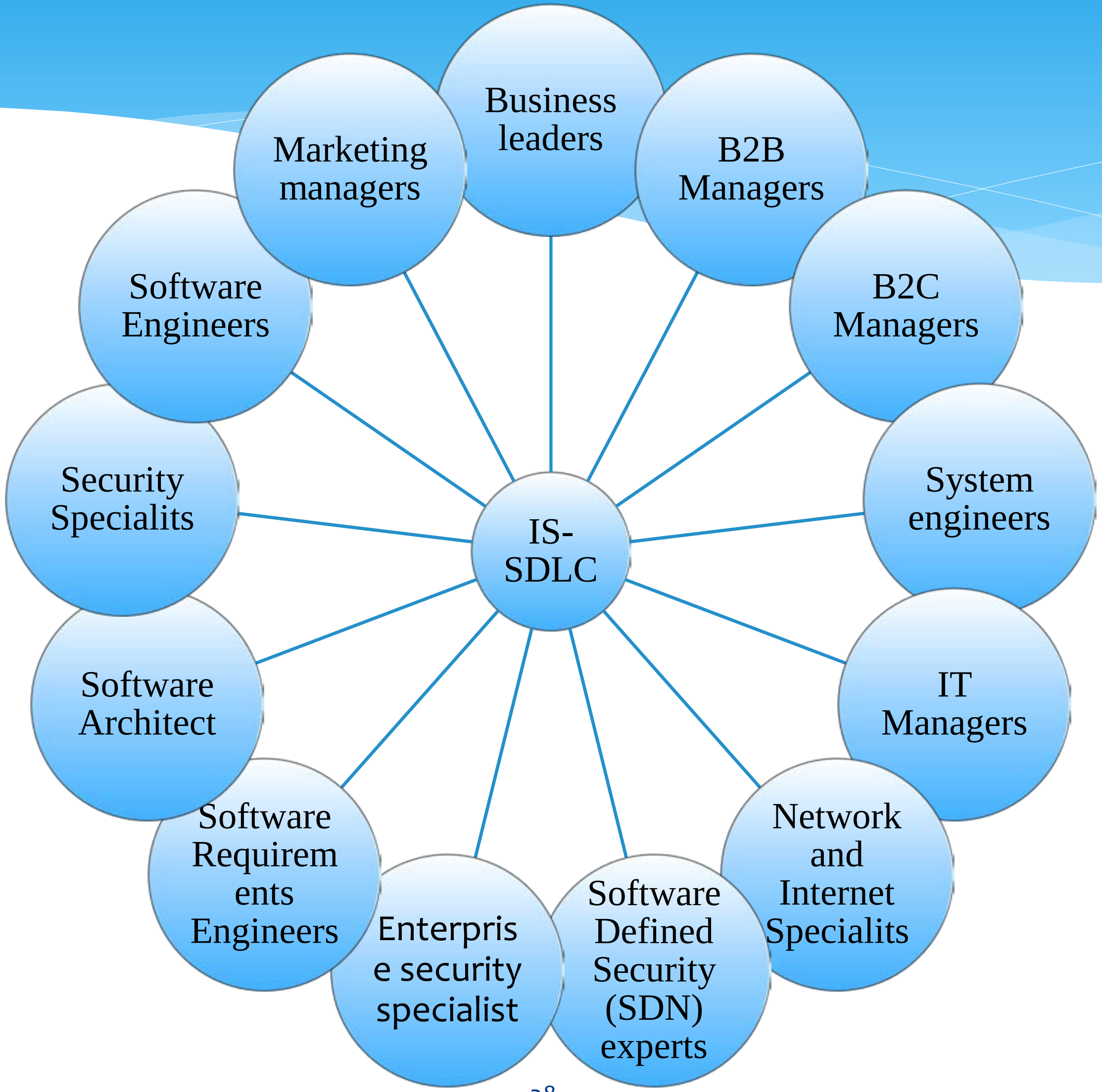
Secure Development

Coding standards

Four layer security implementation model (CAA-encr/decry-transaction security-data security)

Centralised security components/modules

Stakeholders in SSE



IS-SDLC

Business leaders

B2B Managers

B2C Managers

System engineers

IT Managers

Network and Internet Specialits

Software Defined Security (SDN) experts

Enterpris e security specialist

Software Requirem ents Engineers

Software Architect

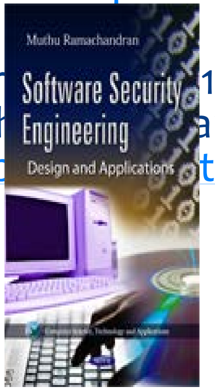
Security Specialits

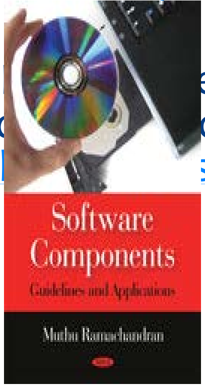
Software Engineers

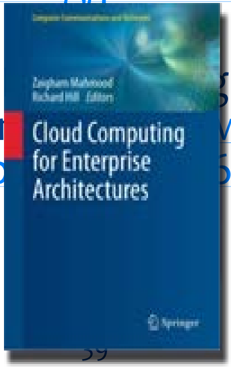
Marketing managers

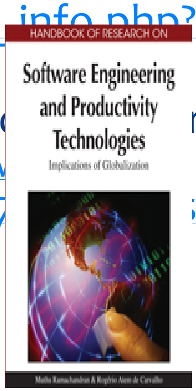
References

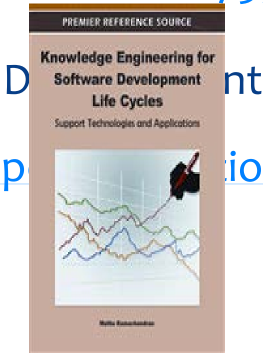
- **Ramachandran, M (2012) Software Security Engineering: Design and Applications, Nova Science Publishers, New York, USA, 2011, ISBN: 978-1-61470-128-6,** https://www.novapublishers.com/catalog/product_info.php?products_id=26331
- **Ramachandran, M (2014) Advances in Cloud Computing Research, Nova, 2014**
- **Ramachandran, M (2013) Business Requirements Engineering for Developing Cloud Computing Services,** Springer, Software Engineering Frameworks for Cloud Computing Paradigm, Mahmood, Z and Saeed, S (eds.), http://www.springer.com/computer/communication+networks/book/978-1-4471-5030-5
- Ramachandran, M (2011) Software components for cloud computing architectures and applications, Springer, Mahmmood, Z and Hill, R (eds.).
- Ramachandran, M (2014) **Enterprise Security Framework for Cloud Data Security**, Book chapter "Delivery and Adoption of Cloud Computing Services in Contemporary Organizations, Chang, V (ed.) IGI Global
- Ramachandran, M (2008) Software Components: Guidelines and Applications, Nova Science Publishers, New York, USA. ISBN: 978-1-60456-870-7, October/November 2008, https://www.novapublishers.com/catalog/product_info.php?products_id=7577 Pages 410
- Ramachandr 1) e g fo re D nt Life Cycles: Support Tech anc or ww global.com/b titl sp 617 typ ion








HANDBOOK OF RESEARCH ON
Software Engineering and Productivity Technologies
Implications of Globalization
Muthu Ramachandran & Rogério Atem de Carvalho


PREMIER REFERENCE SOURCE
Knowledge Engineering for Software Development Life Cycles
Support Technologies and Applications
Muthu Ramachandran

Conclusion , Questions & Thank You

- **Security can’t just be added after release instead it should be Build Security In (BSI)**
- Secure software should continue to operate correctly even under attack
- Secure software can recognize attack patterns and avoid or withstand recognized attacks
- Secure software must be built-in with known vulnerabilities
- Build-In Trust and Resiliency remain a challenge for researchers

LEEDS BECKETT UNIVERSITY