Information Aggregation

David C. Osbourn

david.osbourn@bt.com

March 17, 2006

Abstract

Rather than treat aggregation as an individual problem it is possible to implement the described model and produce a component that dovetails into existing systems. Furthermore, these existing systems can remain widely unchanged, yet still address the aggregation problem.

Overview/Objectives

Information Security

Information Security

- Three Aspects of Information Security:
  - Confidentiality
  - Integrity
  - Availability

Information Security

- Three Aspects of Information Security:
  - Confidentiality
  - Integrity
  - Availability
- More commonly referred to as CIA

Information Security

- Three Aspects of Information Security:
  - Confidentiality
  - Integrity
  - Availability
- More commonly referred to as CIA
- Existing Information Security Models:
  - Confidentiality: Bell-LaPadula, Denning's Lattice
  - Integrity: Biba, Clark-Wilson

Information Security

- Three Aspects of Information Security:
  - Confidentiality
  - Integrity
  - Availability
- More commonly referred to as CIA
- Existing Information Security Models:
  - Confidentiality: Bell-LaPadula, Denning's Lattice
  - Integrity: Biba, Clark-Wilson
- Three Areas of Organisational Information Security:
  - Policy – What the organisation must do
  - Implementation – How the policy is to be carried out
  - Data – The assets the organisation owns.

Aggregation of Information

Aggregation of Information

- Aggregation occurs when information from multiple sources is combined

Aggregation of Information

- Aggregation occurs when information from multiple sources is combined
- Leads to two problems:
  - Aggregation Problem – the whole is greater than the sum of its constituent parts
  - Inference Problem – Information at a higher level can be worked out/inferred

Aggregation of Information

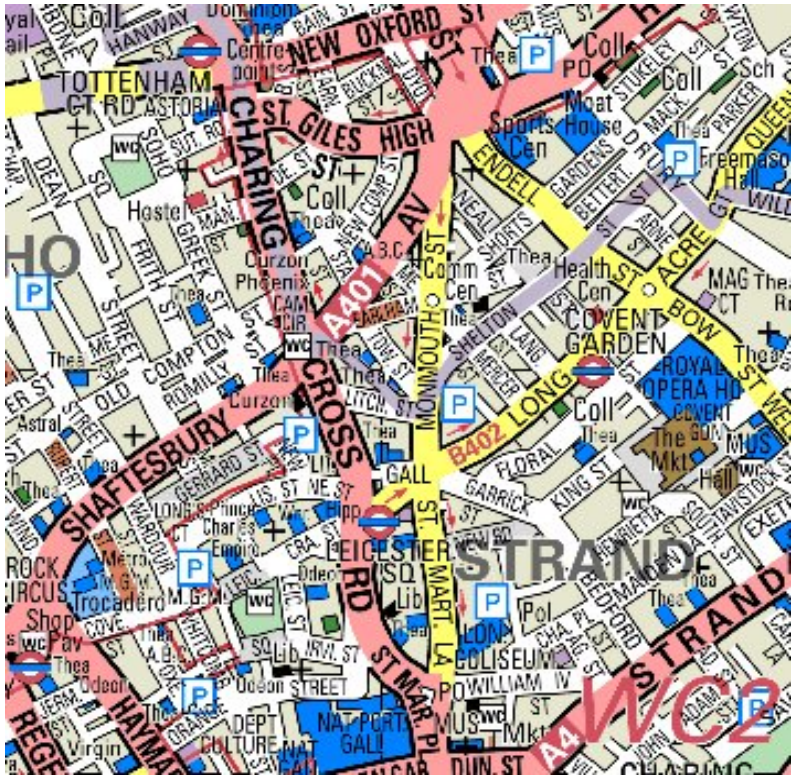
- Aggregation occurs when information from multiple sources is combined
- Leads to two problems:
  - Aggregation Problem – the whole is greater than the sum of its constituent parts
  - Inference Problem – Information at a higher level can be worked out/inferred
- n single assets can be aggregated in $2^n - (n+1)$ permutations
  - a, b, c $(3) \Longrightarrow ab, ac, bc, abc$ $(2^3 - (3+1) = 4)$

Aggregation of Information

- Aggregation occurs when information from multiple sources is combined
- Leads to two problems:
  - Aggregation Problem – the whole is greater than the sum of its constituent parts
  - Inference Problem – Information at a higher level can be worked out/inferred
- n single assets can be aggregated in $2^n - (n+1)$ permutations
  - a, b, c $(3) \Longrightarrow ab, ac, bc, abc$ $(2^3 - (3+1) = 4)$
- Assuming the single assets are classified, it would be impractical to manually classify all the aggregated assets.

Case Study ❶

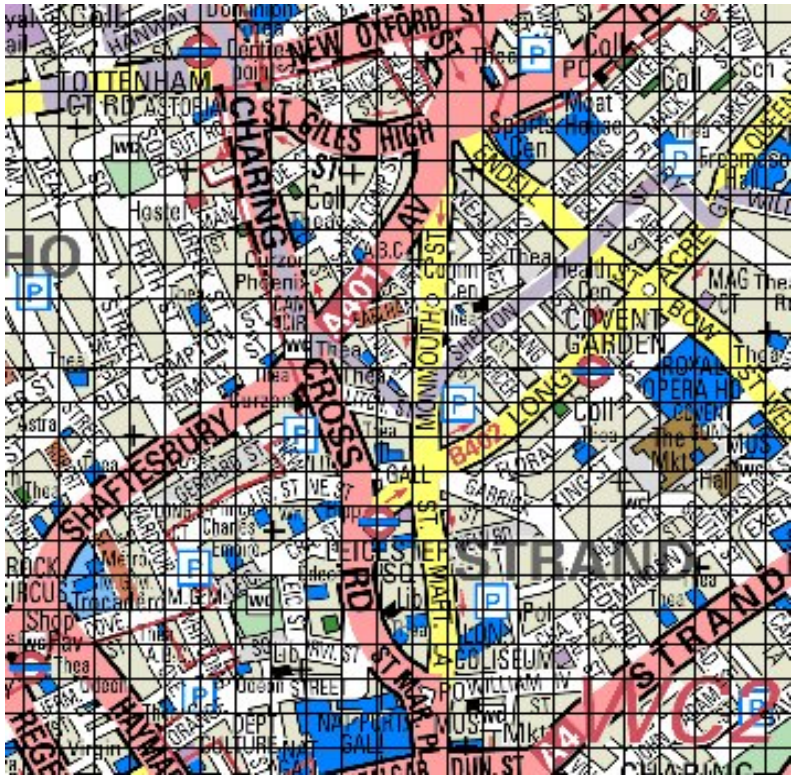
Telephone Network Operator:



Map from `http://www.streetmap.co.uk/newmap.srf?x=529750&y=181250`

Case Study ❶

Telephone Network Operator:

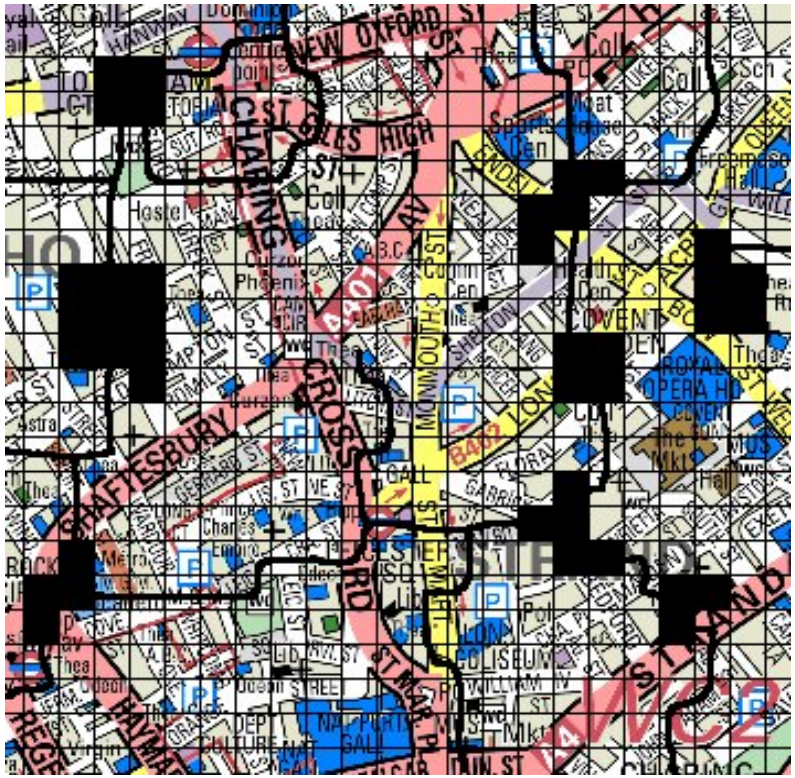


- Overlaid with grid/partitions

Map from `http://www.streetmap.co.uk/newmap.srf?x=529750&y=181250`

Case Study ❶

Telephone Network Operator:

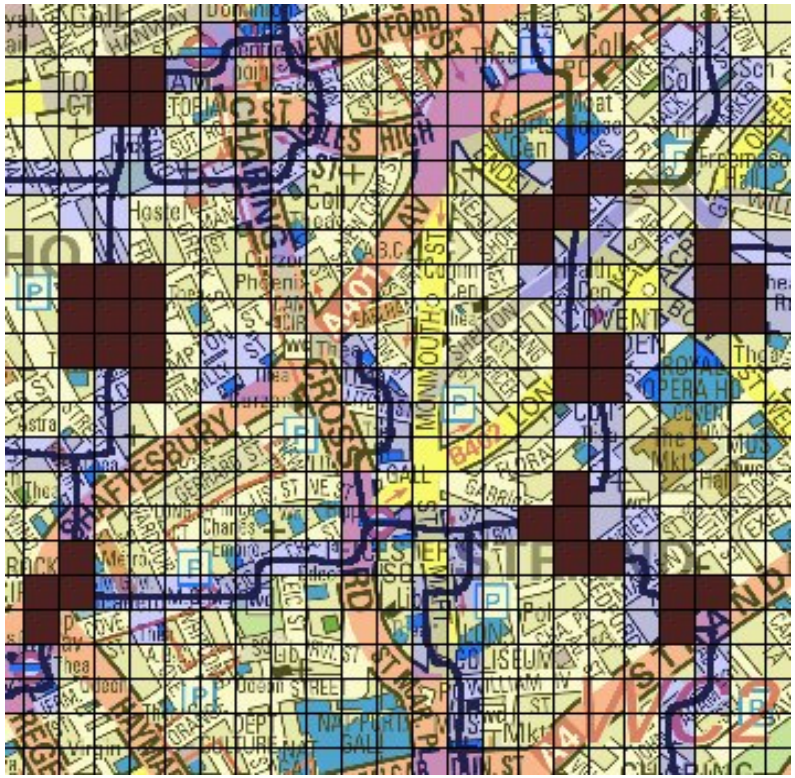


- Overlaid with grid/partitions
- Sensitive locations & interconnects marked

Map from `http://www.streetmap.co.uk/newmap.srf?x=529750&y=181250`

Case Study ❶

Telephone Network Operator:

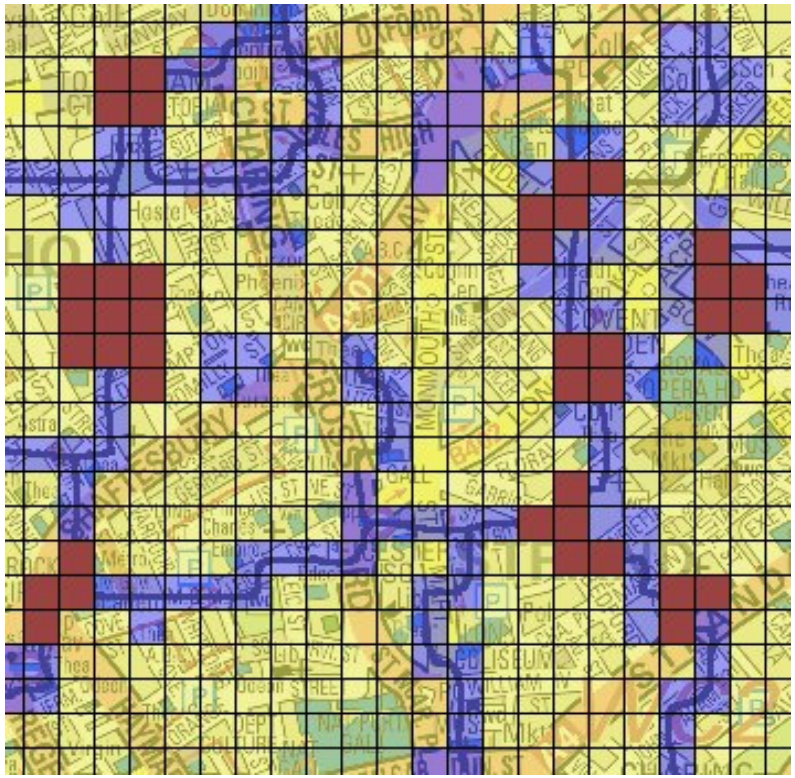


- Overlaid with grid/partitions
- Sensitive locations & interconnects marked
- Classification scheme applied
  - Red = Top Secret (3)
  - Blue = Secret (2)
  - Yellow = Unclassified (1)

Map from `http://www.streetmap.co.uk/newmap.srf?x=529750&y=181250`

Case Study ❶

Telephone Network Operator:

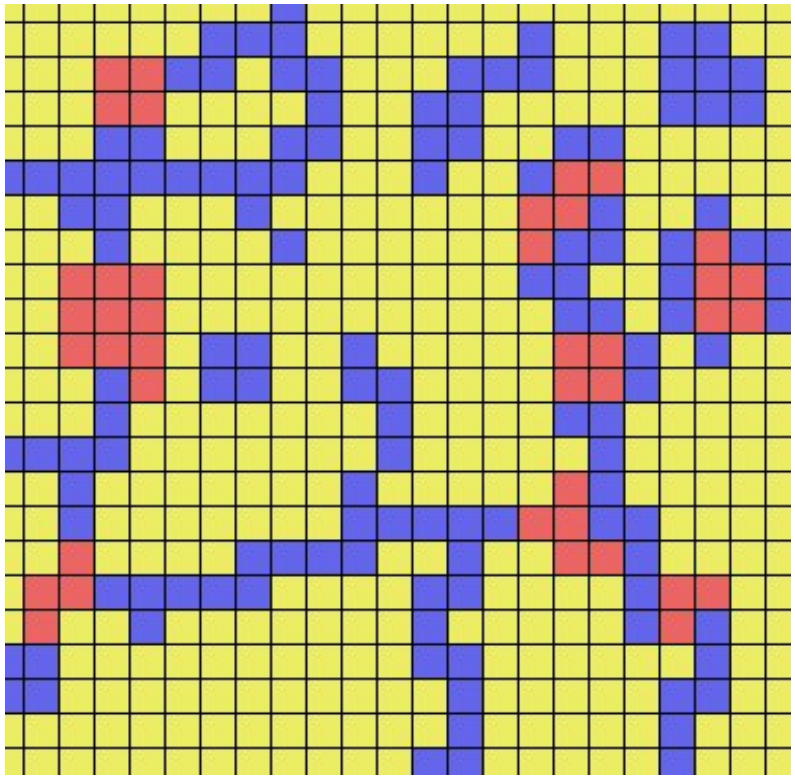


- Overlaid with grid/partitions
- Sensitive locations & interconnects marked
- Classification scheme applied
  - Red = Top Secret (3)
  - Blue = Secret (2)
  - Yellow = Unclassified (1)

Map from `http://www.streetmap.co.uk/newmap.srf?x=529750&y=181250`

Case Study ❶

Telephone Network Operator:

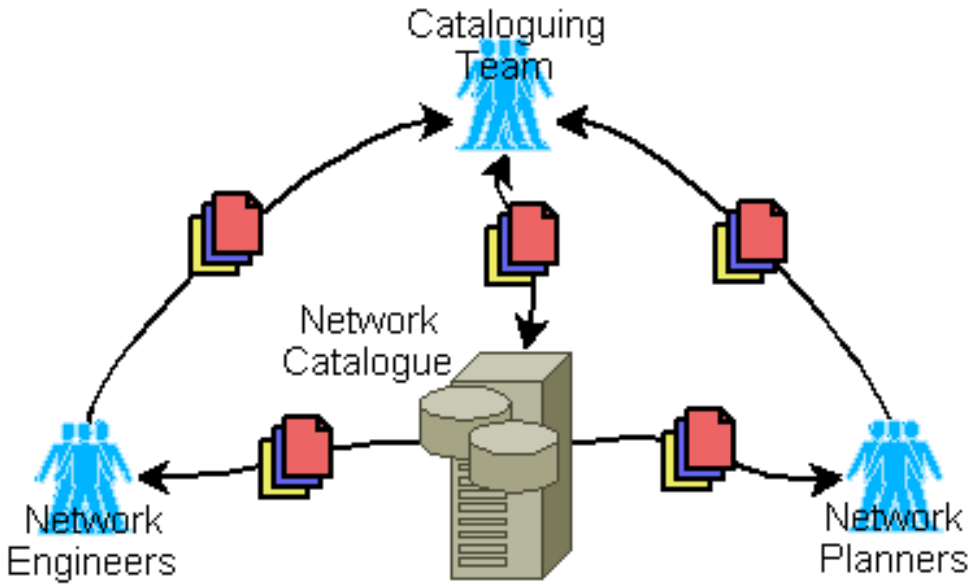


- Overlaid with grid/partitions
- Sensitive locations & interconnects marked
- Classification scheme applied
  - Red = Top Secret (3)
  - Blue = Secret (2)
  - Yellow = Unclassified (1)

Map from `http://www.streetmap.co.uk/newmap.srf?x=529750&y=181250`

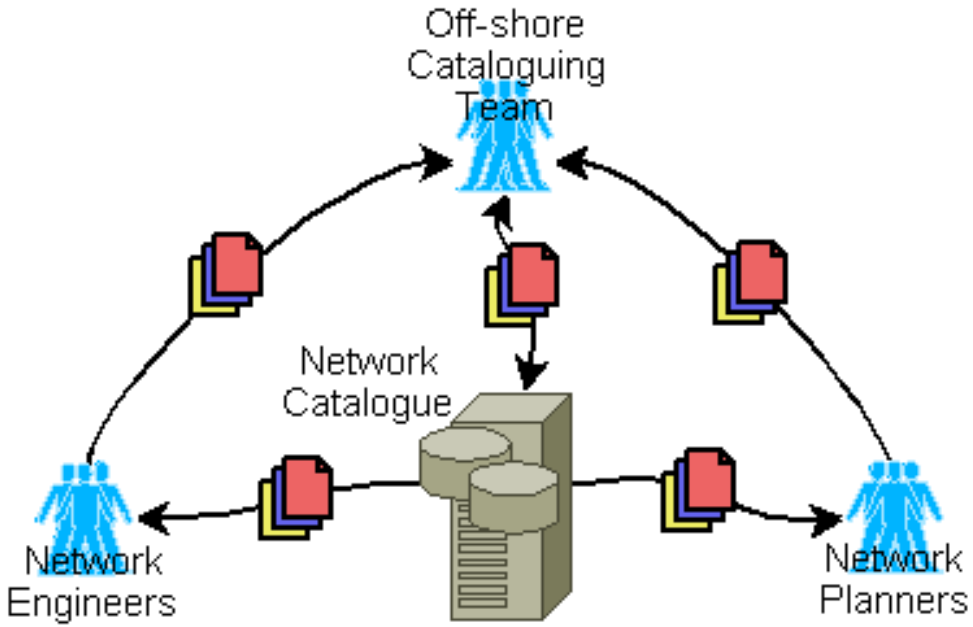
Case Study ❷

Current



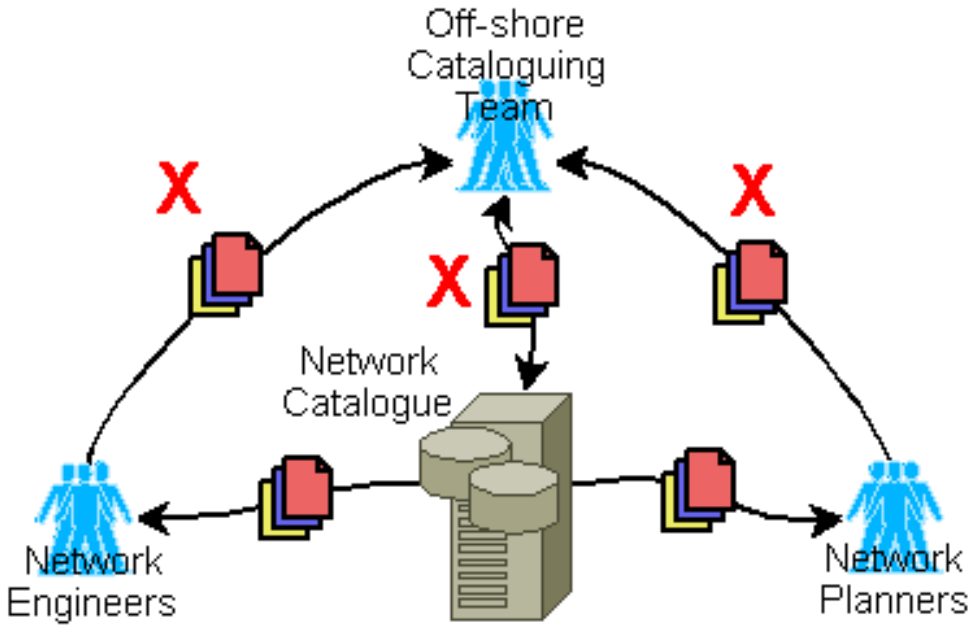
Case Study ❷

Proposed 1



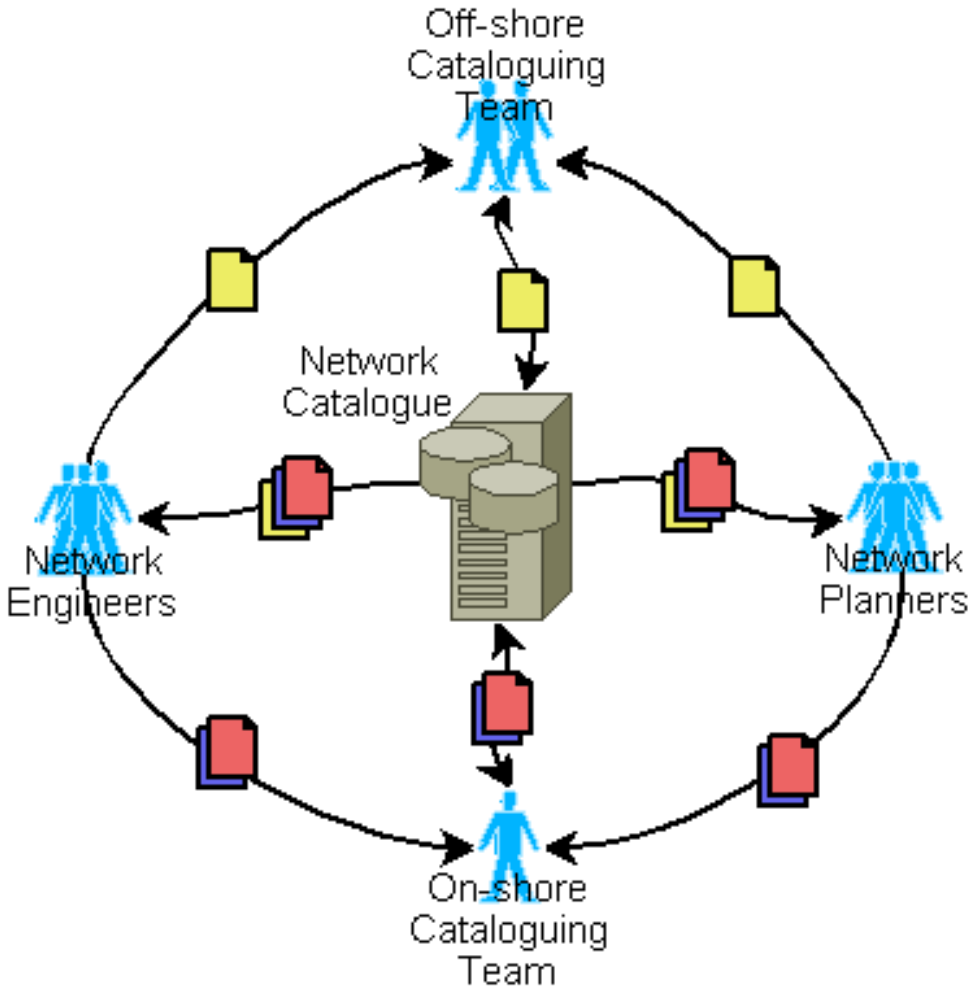
Case Study ❷

Proposed 1



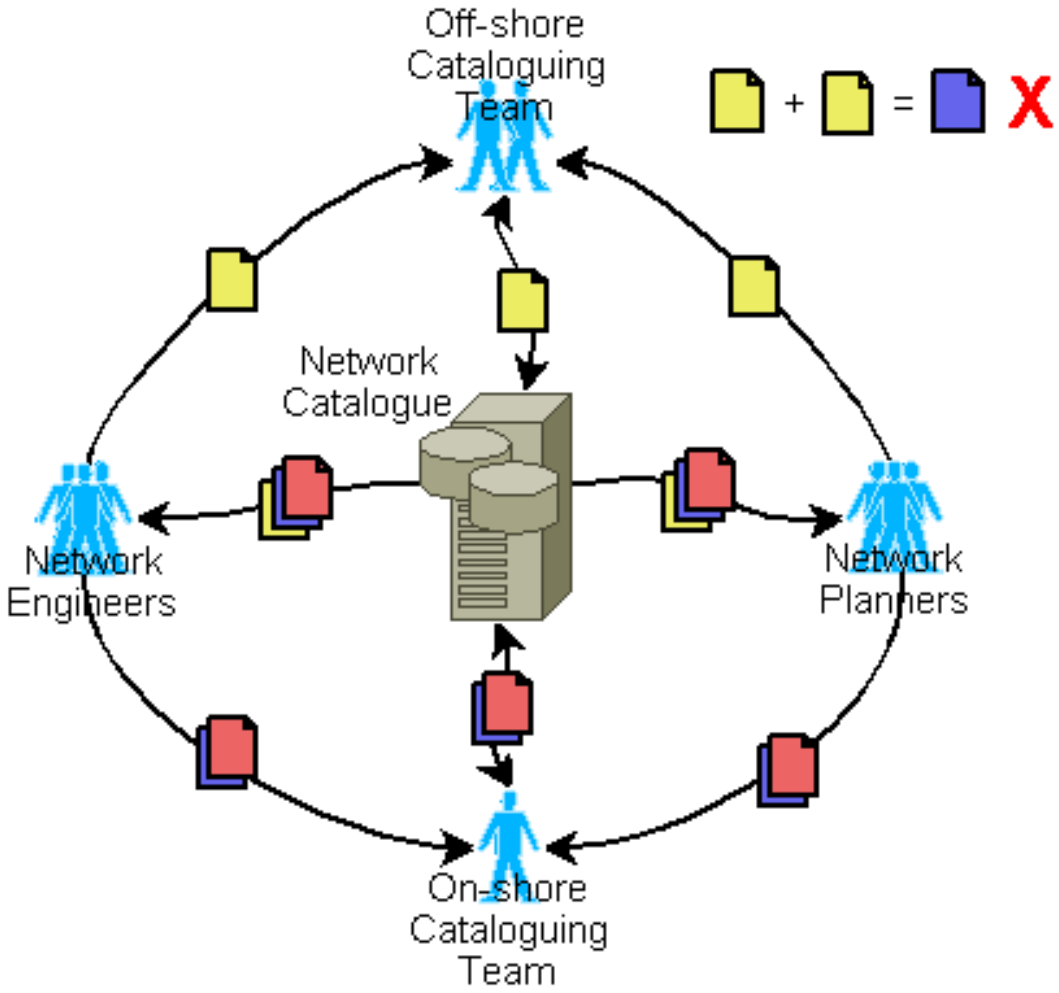
Case Study ❷

Proposed 2



Case Study ❷

Proposed 2



Summary

Summary

- Multiple map partitions representing the physical network

Summary

- Multiple map partitions representing the physical network
- An existing classification scheme and access control mechanisms for the individual map partitions/assets

Summary

- Multiple map partitions representing the physical network
- An existing classification scheme and access control mechanisms for the individual map partitions/assets
- Business requirement to cut costs by out-sourcing suitable cataloguing work

Summary

- Multiple map partitions representing the physical network
- An existing classification scheme and access control mechanisms for the individual map partitions/assets
- Business requirement to cut costs by out-sourcing suitable cataloguing work
- Legal & Contractual obligations complicate the out-sourcing process

Summary

- Multiple map partitions representing the physical network
- An existing classification scheme and access control mechanisms for the individual map partitions/assets
- Business requirement to cut costs by out-sourcing suitable cataloguing work
- Legal & Contractual obligations complicate the out-sourcing process
- Impractical, even impossible, to manually classify all the aggregated assets.

Approach ❶

Approach ❶

- The study was intended to be split into two distinct phases:

Approach ❶

- The study was intended to be split into two distinct phases:
- Investigative Phase – Identify & Frame the Problem
  - Background reading and high-level understanding
  - Scope solution domain
  - Construct an activity based SSM model
  - Identify key sub-processes
  - Analyse and recommend

Approach ❶

- The study was intended to be split into two distinct phases:
- Investigative Phase – Identify & Frame the Problem
  - Background reading and high-level understanding
  - Scope solution domain
  - Construct an activity based SSM model
  - Identify key sub-processes
  - Analyse and recommend
- Engineering Phase – Propose & Develop a Solution
  - Expand requirements into a detailed specification
  - Solution design
  - Implementation, testing and acceptance
  - Iterative stage.

Approach ❷

Approach ❷

- Using SSM in the Investigative Phase will:
  - Give an understanding of the real world domain
  - Translate this into an abstract view
  - Compare this abstract view with what actually happens in the real world
  - Allow making changes to the real world

Approach ❷

- Using SSM in the Investigative Phase will:
  - Give an understanding of the real world domain
  - Translate this into an abstract view
  - Compare this abstract view with what actually happens in the real world
  - Allow making changes to the real world
- Using an Iterative Waterfall approach in the Engineering Phase will:
  - Allow iterative development of core functionality
  - Allows poorly defined areas to be refined.

Activities ❶

Activities ❶

- Finding A Problem
  - Information Security domain sought
  - Security Compliance Team brought up Aggregation
  - Identify & Draw-up TNO Case Study
  - Plan Timescales & Desired Deliverables

Activities ❶

- Finding A Problem
  - Information Security domain sought
  - Security Compliance Team brought up Aggregation
  - Identify & Draw-up TNO Case Study
  - Plan Timescales & Desired Deliverables
- Background Reading & Analysis
  - Understanding the Information Security Domain
  - Understanding & Analysing Existing Models

Activities ❶

- Finding A Problem
  - Information Security domain sought
  - Security Compliance Team brought up Aggregation
  - Identify & Draw-up TNO Case Study
  - Plan Timescales & Desired Deliverables
- Background Reading & Analysis
  - Understanding the Information Security Domain
  - Understanding & Analysing Existing Models
- Defining the Problem - Part One

Activities ❶

- Finding A Problem
  - Information Security domain sought
  - Security Compliance Team brought up Aggregation
  - Identify & Draw-up TNO Case Study
  - Plan Timescales & Desired Deliverables
- Background Reading & Analysis
  - Understanding the Information Security Domain
  - Understanding & Analysing Existing Models
- Defining the Problem - Part One
  - SSM Analysis on TNO Case Study from four view-points:
    - Managing Director's
    - Financial Director's
    - Security Officer's
    - IT Director's.

Activities ❷

Activities ❷

- Defining the Problem - Part Two

Activities ❷

- Defining the Problem - Part Two
  - Consider the Existing Models of Confidentiality
  - Using a Mathematical Notation Identify why they Fail to Solve the Aggregation Problem

Activities ❷

- Defining the Problem - Part Two
  - Consider the Existing Models of Confidentiality
  - Using a Mathematical Notation Identify why they Fail to Solve the Aggregation Problem
- Propose a Suitable Solution

Activities ❷

- Defining the Problem - Part Two
  - Consider the Existing Models of Confidentiality
  - Using a Mathematical Notation Identify why they Fail to Solve the Aggregation Problem
- Propose a Suitable Solution
- Develop the Solution to Resolve this Failure.

Problems With Approach

Problems With Approach

- Using SSM did not Deliver the Desired Results
  - Aggregation is a "hard" data issue, not a HAS
  - One SSM model was partially completed before Identifying the Unsuitability
  - SSM was not the "only option"
  - The MSc calls for Relevance, Appropriateness and Correctness

Problems With Approach

- Using SSM did not Deliver the Desired Results
  - Aggregation is a "hard" data issue, not a HAS
  - One SSM model was partially completed before Identifying the Unsuitability
  - SSM was not the "only option"
  - The MSc calls for Relevance, Appropriateness and Correctness
- Iterative Waterfall Approach was not Providing Quick enough Feedback
  - Observe & Experiment Approach Introduced
  - Allows Quicker Feedback Loops
  - Allows Ideas to be Tested and Evolved.

Requirement

Provide a mechanism to ensure that a classification level may be derived for an aggregated information asset, allowing other established models of confidentiality to operate unchanged, in an environment containing aggregated information assets.

Axioms

Axioms

- The following Axioms capture facts about aggregation:

Axioms

- The following Axioms capture facts about aggregation:

1. Commutative Property – There is no order in the final aggregated asset:

$$a, b = b, a$$

Axioms

- The following Axioms capture facts about aggregation:

1. Commutative Property – There is no order in the final aggregated asset:

$$a, b = b, a$$

2. Distinct Property – There is no duplication of assets when aggregating:

$$a, a = a$$

Axioms

- The following Axioms capture facts about aggregation:

1. Commutative Property – There is no order in the final aggregated asset:
$$a, b = b, a$$
2. Distinct Property – There is no duplication of assets when aggregating:
$$a, a = a$$
3. Associative Property – The order in which the aggregation occurs does not matter:
$$ab, c = a, bc = ac, b$$

Axioms

- The following Axioms capture facts about aggregation:

1. Commutative Property – There is no order in the final aggregated asset:
$$a, b = b, a$$
2. Distinct Property – There is no duplication of assets when aggregating:
$$a, a = a$$
3. Associative Property – The order in which the aggregation occurs does not matter:
$$ab, c = a, bc = ac, b$$
4. Emptyset Property – Aggregating an asset a, with the emptyset results in a:
$$a, \emptyset = a$$

General Aspects

General Aspects

- From the existing models of Confidentiality:

General Aspects

- From the existing models of Confidentiality:
- They each have a classification/sensitivity schema – Classification
  - "The associated asset requires this level of protection/has this value"
  - Top Secret, Secret, Unclassifed

General Aspects

- From the existing models of Confidentiality:
- They each have a classification/sensitivity schema – Classification
  - "The associated asset requires this level of protection/has this value"
  - Top Secret, Secret, Unclassifed
- They each have a sub-division mechanism – Category
  - "The associated asset relates to this real-world topic"
  - *PERSONNEL, HOME, FOREIGN*.

Aggregation Specific

Aggregation Specific

- From considering Confidentiality within Aggregagtion the following Aspects were identified:

Aggregation Specific

- From considering Confidentiality within Aggregagtion the following Aspects were identified:
- A relationship between assets which have a "geographical" closeness – Adjacancy
  - An Adjacency Level captures the number of other assets with which the associated asset can be aggregated before there is a perceived breach of Confidentiality.
  - This is a Numeric or Special Value
  - Derived via Risk Analysis process

Aggregation Specific

- From considering Confidentiality within Aggregagtion the following Aspects were identified:
- A relationship between assets which have a "geographical" closeness – Adjacancy
  - An Adjacency Level captures the number of other assets with which the associated asset can be aggregated before there is a perceived breach of Confidentiality.
  - This is a Numeric or Special Value
  - Derived via Risk Analysis process
- A further sub-division of the data – Context

Aggregation Specific

- From considering Confidentiality within Aggregagtion the following Aspects were identified:
- A relationship between assets which have a "geographical" closeness – Adjacancy
  - An Adjacency Level captures the number of other assets with which the associated asset can be aggregated before there is a perceived breach of Confidentiality.
  - This is a Numeric or Special Value
  - Derived via Risk Analysis process
- A further sub-division of the data – Context
  - "The associated asset relates to this real-world entity"
  - *A. Smith, B. Jones*.

Contextless Model

Asset	Class.	Category	Adj_1	Adj_2	$Count_1$	$Count_2$
a	1	A	5	2	1	0
b	2	B	4	4	0	1

Asset
x, y
a, b

Asset
x, y
a, b

Asset
x, y
a, b

Functions:

Contextless Model

Asset	Class.	Category	Adj_1	Adj_2	$Count_1$	$Count_2$
a	1	A	5	2	1	0
b	2	B	4	4	0	1

Asset	Classification
x, y	$max(class(x), class(y))$
a, b	$(1, 2) = 2$

Asset
x, y
a, b

Asset
x, y
a, b

Functions:

- $max(X, Y)$ - Maximum value of X and Y.
- $class(p)$ - Asset p's classification.

Contextless Model

Asset	Class.	Category	Adj_1	Adj_2	$Count_1$	$Count_2$
a	1	A	5	2	1	0
b	2	B	4	4	0	1

Asset	Classification	Category
x, y	$max(class(x), class(y))$	$cat(x) + cat(y)$
a, b	$(1, 2) = 2$	$A + B = A, B$

Asset
x, y
a, b

Asset
x, y
a, b

Functions:

- $max(X, Y)$ - Maximum value of X and Y.
- $class(p)$ - Asset p's classification.
- $cat(p)$ - Asset p's category.

Contextless Model

Asset	Class.	Category	Adj_1	Adj_2	Count_1	Count_2
a	1	A	5	2	1	0
b	2	B	4	4	0	1

Asset	Classification	Category
x, y	$max(class(x), class(y))$	$cat(x) + cat(y)$
a, b	$(1, 2) = 2$	$A + B = A, B$

Asset	Adj_n $(n = 1)$
x, y	$min(adj(x, n) - count(y, n), adj(y, n) - count(x, n))$
a, b	$(5 - 0 , 4 - 1) = (5, 3) = 3$

Asset
x, y
a, b

Functions:

- $max(X, Y)$ - Maximum value of X and Y.
- $class(p)$ - Asset p's classification.
- $cat(p)$ - Asset p's category.
- $min(X, Y)$ - Minimum value of X and Y.
- $adj(p, i)$ - Asset p's adjacency level at classification level i.
- $count(p, i)$ - Asset p's count value at classification level i.

Contextless Model

Asset	Class.	Category	Adj_1	Adj_2	Count_1	Count_2
a	1	A	5	2	1	0
b	2	B	4	4	0	1

Asset	Classification	Category
x, y	$max(class(x), class(y))$	$cat(x) + cat(y)$
a, b	$(1, 2) = 2$	$A + B = A, B$

Asset	Adj_n $(n = 1)$	Count_n $(n = 1)$
x, y	$min(adj(x, n) - count(y, n), adj(y, n) - count(x, n))$	$count(x, n) + count(y, n)$
a, b	$(5 - 0 , 4 - 1) = (5, 3) = 3$	$(1 + 0) = 1$

Asset
x, y
a, b

Functions:

- $max(X, Y)$ - Maximum value of X and Y.
- $class(p)$ - Asset p's classification.
- $cat(p)$ - Asset p's category.
- $min(X, Y)$ - Minimum value of X and Y.
- $adj(p, i)$ - Asset p's adjacency level at classification level i.
- $count(p, i)$ - Asset p's count value at classification level i.

Contextless Model

Asset	Class.	Category	Adj_1	Adj_2	Count_1	Count_2
a	1	A	5	2	1	0
b	2	B	4	4	0	1

Asset	Classification	Category
x, y	$max(class(x), class(y))$	$cat(x) + cat(y)$
a, b	$(1, 2) = 2$	$A + B = A, B$

Asset	Adj_n $(n = 1)$	Count_n $(n = 1)$
x, y	$min(adj(x, n) - count(y, n), adj(y, n) - count(x, n))$	$count(x, n) + count(y, n)$
a, b	$(5 - 0 , 4 - 1) = (5, 3) = 3$	$(1 + 0) = 1$

Asset	Adj_n $(n = 2)$
x, y	$min(adj(x, n) - count(y, n), adj(y, n) - count(x, n))$
a, b	$(2 - 1 , 4 - 0) = (1, 4) = 1$

Functions:

- $max(X, Y)$ - Maximum value of X and Y.
- $class(p)$ - Asset p's classification.
- $cat(p)$ - Asset p's category.
- $min(X, Y)$ - Minimum value of X and Y.
- $adj(p, i)$ - Asset p's adjacency level at classification level i.
- $count(p, i)$ - Asset p's count value at classification level i.

Contextless Model

Asset	Class.	Category	Adj_1	Adj_2	Count_1	Count_2
a	1	A	5	2	1	0
b	2	B	4	4	0	1

Asset	Classification	Category
x, y	$max(class(x), class(y))$	$cat(x) + cat(y)$
a, b	$(1, 2) = 2$	$A + B = A, B$

Asset	Adj_n $(n = 1)$	Count_n $(n = 1)$
x, y	$min(adj(x, n) - count(y, n), adj(y, n) - count(x, n))$	$count(x, n) + count(y, n)$
a, b	$(5 - 0 , 4 - 1) = (5, 3) = 3$	$(1 + 0) = 1$

Asset	Adj_n $(n = 2)$	Count_n $(n = 2)$
x, y	$min(adj(x, n) - count(y, n), adj(y, n) - count(x, n))$	$count(x, n) + count(y, n)$
a, b	$(2 - 1 , 4 - 0) = (1, 4) = 1$	$(0 + 1) = 1$

Functions:

- $max(X, Y)$ - Maximum value of X and Y.
- $class(p)$ - Asset p's classification.
- $cat(p)$ - Asset p's category.
- $min(X, Y)$ - Minimum value of X and Y.
- $adj(p, i)$ - Asset p's adjacency level at classification level i.
- $count(p, i)$ - Asset p's count value at classification level i.

Contextless Model

Asset	Class.	Category	Adj_1	Adj_2	Count_1	Count_2
a	1	A	5	2	1	0
b	2	B	4	4	0	1
ab	2	A, B	3	1	1	1

Asset	Classification	Category
x, y	$max(class(x), class(y))$	$cat(x) + cat(y)$
a, b	$(1, 2) = 2$	$A + B = A, B$

Asset	Adj_n $(n = 1)$	Count_n $(n = 1)$
x, y	$min(adj(x, n) - count(y, n), adj(y, n) - count(x, n))$	$count(x, n) + count(y, n)$
a, b	$(5 - 0 , 4 - 1) = (5, 3) = 3$	$(1 + 0) = 1$

Asset	Adj_n $(n = 2)$	Count_n $(n = 2)$
x, y	$min(adj(x, n) - count(y, n), adj(y, n) - count(x, n))$	$count(x, n) + count(y, n)$
a, b	$(2 - 1 , 4 - 0) = (1, 4) = 1$	$(0 + 1) = 1$

Functions:

- $max(X, Y)$ - Maximum value of X and Y.
- $class(p)$ - Asset p's classification.
- $cat(p)$ - Asset p's category.
- $min(X, Y)$ - Minimum value of X and Y.
- $adj(p, i)$ - Asset p's adjacency level at classification level i.
- $count(p, i)$ - Asset p's count value at classification level i.

Contextual Model ❶

Asset	Class.	Context	Adj_1	Adj_2	$Count_1$	$Count_2$
a	1	V	$5, 7$	$2, 4$	1	0
b	1	V, W	$4, *, 5$	$4, *, 6$	$1, 1$	$0, 0$

Asset
x, y
a, b

Asset
x, y
a, b

Asset
x, y
a, b

Functions:

Contextual Model ❶

Asset	Class.	Context	Adj_1	Adj_2	$Count_1$	$Count_2$
a	1	V	$5, 7$	$2, 4$	1	0
b	1	V, W	$4, *, 5$	$4, *, 6$	$1, 1$	$0, 0$

Asset	Classification
x, y	$max(class(x), class(y))$
a, b	$(1, 1) = 1$

Asset
x, y
a, b

Asset
x, y
a, b

Functions:

- $max(X, Y)$ - Maximum value of X and Y.
- $class(p)$ - Asset p's classification.

Contextual Model ❶

Asset	Class.	Context	Adj_1	Adj_2	$Count_1$	$Count_2$
a	1	V	$5, 7$	$2, 4$	1	0
b	1	V, W	$4, *, 5$	$4, *, 6$	$1, 1$	$0, 0$

Asset	Classification	Context
x, y	$max(class(x), class(y))$	$context(x) + context(y)$
a, b	$(1, 1) = 1$	$V + V, W = V, W$

Asset
x, y
a, b

Asset
x, y
a, b

Functions:

- $max(X, Y)$ - Maximum value of X and Y.
- $class(p)$ - Asset p's classification.
- $context(p)$ - Asset p's context.

Contextual Model ❶

Asset	Class.	Context	Adj_1	Adj_2	Count_1	Count_2
a	1	V	5,7	2, 4	1	0
b	1	V, W	$4, *, 5$	$4, *, 6$	$1, 1$	$0, 0$

Asset	Classification	Context
x, y	$max(class(x), class(y))$	$context(x) + context(y)$
a, b	$(1, 1) = 1$	$V + V, W = V, W$

Asset	Adj_1 $(n = 1)$
x, y	$T : min(adj(x, n, T) - count(y, n, T), adj(y, n, T) - count(x, n, T))$ $\$: min(adj(x, n, \$) - count(y, n, \$), adj(y, n, \$) - count(x, n, \$))$
a, b	$V : (5 - 1, 4 - 1) = (4, 3) = 3$ $W : (7 - 1, * - 0) = (6, *) = *$ $\$: (7 - 1, 5 - 0) = (6, 5) = 5$

Asset
x, y
a, b

Functions:

- $max(X, Y)$ - Maximum value of X and Y.
- $class(p)$ - Asset p's classification.
- $context(p)$ - Asset p's context.
- $min(X, Y)$ - Minimum value of X and Y.
- $adj(p, i, t)$ - Asset p's adjacency level at classification level i in context t.
- $count(p, i, t)$ - Asset p's count value at classification level i in context t.

Contextual Model ❶

Asset	Class.	Context	Adj_1	Adj_2	Count_1	Count_2
a	1	V	$5, 7$	$2, 4$	1	0
b	1	V, W	$4, *, 5$	$4, *, 6$	$1, 1$	$0, 0$

Asset	Classification	Context
x, y	$max(class(x), class(y))$	$context(x) + context(y)$
a, b	$(1, 1) = 1$	$V + V, W = V, W$

Asset	Adj_1 $(n = 1)$
x, y	$T : min(adj(x, n, T) - count(y, n, T), adj(y, n, T) - count(x, n, T))$ $\$: min(adj(x, n, \$) - count(y, n, \$), adj(y, n, \$) - count(x, n, \$))$
a, b	$V : (\ 5 - 1, 4 - 1\ ) = (4, 3) = 3$ $W : (\ 7 - 1\ , * - 0) = (6, *) = *$ $\$: (\ 7 - 1\ , 5 - 0) = (6, 5) = 5$

Asset	Count_n $(n = 1)$
x, y	T: $count(x, n, T) + count(y, n, T)$
a, b	$V : (\ 1 + 1\ ) = 2$ $W : (\ 0 + 1\ ) = 1$

Functions:

- $max(X, Y)$ - Maximum value of X and Y.
- $class(p)$ - Asset p's classification.
- $context(p)$ - Asset p's context.
- $min(X, Y)$ - Minimum value of X and Y.
- $adj(p, i, t)$ - Asset p's adjacency level at classification level i in context t.
- $count(p, i, t)$ - Asset p's count value at classification level i in context t.

Contextual Model ❷

Asset	Class.	Context	Adj_1	Adj_2	Count_1	Count_2
a	1	V	5, 7	2,4	1	0
b	1	V, W	4, $*$, 5	4, $*$, 6	1, 1	0, 0

Asset	Adj_1 $(n = 2)$
x, y	$T : min(adj(x, n, T) - count(y, n, T), adj(y, n, T) - count(x, n, T))$ $\$: min(adj(x, n, \$) - count(y, n, \$), adj(y, n, \$) - count(x, n, \$))$
a, b	$V : (\ 2 - 0, 4 - 0\ ) = (2, 4) = 2$ $W : (\ 4 - 0\ ,\ * - 0) = (4, *) = *$ $\$: (\ 4 - 0\ , 6 - 0) = (4, 6) = 4$

Asset
x, y
a, b

Functions:

- $min(X, Y)$ - Minimum value of X and Y.
- $adj(p, i, t)$ - Asset p's adjacency level at classification level i in context t.
- $count(p, i, t)$ - Asset p's count value at classification level i in context t.

Contextual Model ❷

Asset	Class.	Context	Adj_1	Adj_2	Count_1	Count_2
a	1	V	$5, 7$	$2, 4$	1	0
b	1	V, W	$4, *, 5$	$4, *, 6$	$1, 1$	$0, 0$

Asset	Adj_1 $(n = 2)$
x, y	$T : min(adj(x, n, T) - count(y, n, T), adj(y, n, T) - count(x, n, T))$ $\$: min(adj(x, n, \$) - count(y, n, \$), adj(y, n, \$) - count(x, n, \$))$
a, b	$V : (\ 2 - 0, 4 - 0\ ) = (2, 4) = 2$ $W : (\ 4 - 0\ ,\ * - 0) = (4, *) = *$ $\$: (\ 4 - 0\ ,\ 6 - 0) = (4, 6) = 4$

Asset	Count_n $(n = 2)$
x, y	T: $count(x, n, T) + count(y, n, T)$
a, b	$V : (\ 0 + 0\ ) = 0$ $W : (0 + 0\ ) = 0$

Functions:

- $min(X, Y)$ - Minimum value of X and Y.
- $adj(p, i, t)$ - Asset p's adjacency level at classification level i in context t.
- $count(p, i, t)$ - Asset p's count value at classification level i in context t.

Contextual Model ❷

Asset	Class.	Context	Adj_1	Adj_2	Count_1	Count_2
a	1	V	$5, 7$	$2, 4$	1	0
b	1	V, W	$4, *, 5$	$4, *, 6$	$1, 1$	$0, 0$
ab	1	V, W	$3, *, 5$	$2, *, 4$	$2, 1$	$0, 0$

Asset	Adj_1 $(n = 2)$
x, y	$T : min(adj(x, n, T) - count(y, n, T), adj(y, n, T) - count(x, n, T))$ $\$: min(adj(x, n, \$) - count(y, n, \$), adj(y, n, \$) - count(x, n, \$))$
a, b	$V : (\ 2 - 0, 4 - 0\ ) = (2, 4) = 2$ $W : (\ 4 - 0\ ,\ * - 0) = (4, *) = *$ $\$: (\ 4 - 0\ ,\ 6 - 0) = (4, 6) = 4$

Asset	Count_n $(n = 2)$
x, y	T: $count(x, n, T) + count(y, n, T)$
a, b	$V : (\ 0 + 0\ ) = 0$ $W : (0 + 0\ ) = 0$

Functions:

- $min(X, Y)$ - Minimum value of X and Y.
- $adj(p, i, t)$ - Asset p's adjacency level at classification level i in context t.
- $count(p, i, t)$ - Asset p's count value at classification level i in context t.

Green & Blue Rules

Green & Blue Rules

- Green Rule: Synonymous with the HWM Classification Rule

Green & Blue Rules

- Green Rule: Synonymous with the HWM Classification Rule
- After Repeated Subtraction in Adjacency Levels a Negative Value will Appear.

Green & Blue Rules

- Green Rule: Synonymous with the HWM Classification Rule
- After Repeated Subtraction in Adjacency Levels a Negative Value will Appear.
- Simple Heuristic: Negative Value Requires Classification Upgrade and Value Reset

Green & Blue Rules

- Green Rule: Synonymous with the HWM Classification Rule
- After Repeated Subtraction in Adjacency Levels a Negative Value will Appear.
- Simple Heuristic: Negative Value Requires Classification Upgrade and Value Reset
- Blue does not Actually perform any Upgrades

Green & Blue Rules

- Green Rule: Synonymous with the HWM Classification Rule
- After Repeated Subtraction in Adjacency Levels a Negative Value will Appear.
- Simple Heuristic: Negative Value Requires Classification Upgrade and Value Reset
- Blue does not Actually perform any Upgrades

Contextless					
	Asset	Class.	Context	Adj_1	Adj_2
Pre-Blue Rule	ghi, j	2		$\ldots = (-\mathbf{2}, -\mathbf{1}) = -\mathbf{2}$	$\ldots = (1, 3) = \mathbf{1}$
Post-Blue Rule	ghi, j	2		-1 **1**	1 **0**

Contextual					
Pre-Blue Rule	ghi, j	2	$V, \$$	$V : \ldots = (-\mathbf{2}, -\mathbf{1}) = -\mathbf{2}$ $\$: \ldots = (4, 5) = 4$	$V : \ldots = (1, 3) = \mathbf{1}$ $\$: \ldots = (4, 3) = 3$
Post-Blue Rule	ghi, j	2	$V, \$$	$-2, 4$ **1, 4**	1, 3 **0**, 3

Orange & Red Rules

Orange & Red Rules

- Both Orange and Red Rules do Upgrades Classification Levels

Orange & Red Rules

- Both Orange and Red Rules do Upgrades Classification Levels
- Both also "Reset" Negative Values to the Lowest of the Individual Assets

Orange & Red Rules

- Both Orange and Red Rules do Upgrades Classification Levels
- Both also "Reset" Negative Values to the Lowest of the Individual Assets
- Orange Rule applies to all but the Highest Classification Level

Orange & Red Rules

- Both Orange and Red Rules do Upgrades Classification Levels
- Both also "Reset" Negative Values to the Lowest of the Individual Assets
- Orange Rule applies to all but the Highest Classification Level

Contextless							
	Asset	Class.	Context	Adj_1	Adj_2	Count_1	Count_2
Pre-Orange Rule	de, f	**1**		$\ldots = -\mathbf{1}$	2	3	0
Post-Orange Rule	de, f	1 **2**		$\ldots = -1$ **1**	2	3	0
Contextual							
Pre-Orange Rule	de, f	**1**	$V, \$$	$\ldots = -\mathbf{1}, 5$	2, 2	3	0
Post-Orange Rule	de, f	1 **2**	$V, \$$	$\ldots = -1, 5$ **1, 5**	2, 2	3	0

Orange & Red Rules

Orange & Red Rules

- Red Rule only upgrades from the Second Highest to Highest Classification Level

Orange & Red Rules

- Red Rule only upgrades from the Second Highest to Highest Classification Level
- Resets Values at All Levels, not just affected level

Orange & Red Rules

- Red Rule only upgrades from the Second Highest to Highest Classification Level
- Resets Values at All Levels, not just affected level

Contextless							
	Asset	Class.	Context	Adj_1	Adj_2	Count_1	Count_2
Pre-Red Rule	$ghij, k$	2		-2	$-\mathbf{1}$	3	2
Post-Red Rule	$ghij, k$	2 **3**		-2 **1**	-1 **2**	3	2

Contextual							
Pre-Red Rule	$ghij, k$	2	$V, \$$	$-2, 4$	$-\mathbf{1}, 3$	3	2
Post-Red Rule	$ghij, k$	2 **3**	$V, \$$	$-2, 4$ **1, 4**	$-1, 3$ **2, 3**	3	2

Prototype

Prototype

- Developed in Perl to run on a WWW server

Prototype

- Developed in Perl to run on a WWW server
- Endeavours to exhibit the abstract functional constructs detailed in Contextual Model

Prototype

- Developed in Perl to run on a WWW server
- Endeavours to exhibit the abstract functional constructs detailed in Contextual Model
- Gives a level of confidence about satisfying associative property

Prototype

- Developed in Perl to run on a WWW server
- Endeavours to exhibit the abstract functional constructs detailed in Contextual Model
- Gives a level of confidence about satisfying associative property
- Other axioms are left to the user's discretion

Prototype

- Developed in Perl to run on a WWW server
- Endeavours to exhibit the abstract functional constructs detailed in Contextual Model
- Gives a level of confidence about satisfying associative property
- Other axioms are left to the user's discretion
- A useful tool when developing the model as it allowed ideas to be quickly implemented and tested in bulk.

Learning

Learning

- Approach had to be flexible and adaptive

Learning

- Approach had to be flexible and adaptive
- SSM is unsuitable for these "hard" data-centric problems

Learning

- Approach had to be flexible and adaptive
- SSM is unsuitable for these "hard" data-centric problems
- Better time management skills

Learning

- Approach had to be flexible and adaptive
- SSM is unsuitable for these "hard" data-centric problems
- Better time management skills
- Peer review and peer support are invaluable in this type of project

Learning

- Approach had to be flexible and adaptive
- SSM is unsuitable for these "hard" data-centric problems
- Better time management skills
- Peer review and peer support are invaluable in this type of project
- 30 year old formal models of Information Security are still relevant.

Shortfalls

Shortfalls

- Problems with compliance to associative property in "out-of-context"

Shortfalls

- Problems with compliance to associative property in "out-of-context"
- No full-scale development or associated testing

Shortfalls

- Problems with compliance to associative property in "out-of-context"
- No full-scale development or associated testing
- No consideration of disaggregation of aggregated assets

Shortfalls

- Problems with compliance to associative property in "out-of-context"
- No full-scale development or associated testing
- No consideration of disaggregation of aggregated assets
- No investigation of Integrity or Availability.

Summary of Findings

Summary of Findings

- Identified shortfalls and problems with existing approaches

Summary of Findings

- Identified shortfalls and problems with existing approaches
- Identified a number of rules of aggregation

Summary of Findings

- Identified shortfalls and problems with existing approaches
- Identified a number of rules of aggregation
- It is possible to develop a solution to dove-tail to existing models

Summary of Findings

- Identified shortfalls and problems with existing approaches
- Identified a number of rules of aggregation
- It is possible to develop a solution to dove-tail to existing models
- The problem solution, although abstract, could potentially be applied to resolve the issues in the case study

Summary of Findings

- Identified shortfalls and problems with existing approaches
- Identified a number of rules of aggregation
- It is possible to develop a solution to dove-tail to existing models
- The problem solution, although abstract, could potentially be applied to resolve the issues in the case study
- Solution is neat, compact and has high complexity yet not complicated (?!).

The Future

The Future

- There are several logical extensions or related areas of future research:

The Future

- There are several logical extensions or related areas of future research:
  - Risk assessment derivation of Adjacency Levels

The Future

- There are several logical extensions or related areas of future research:
  - Risk assessment derivation of Adjacency Levels
  - Compliance to associative property

The Future

- There are several logical extensions or related areas of future research:
  - Risk assessment derivation of Adjacency Levels
  - Compliance to associative property
  - Full scale development and CAT deployment

The Future

- There are several logical extensions or related areas of future research:
  - Risk assessment derivation of Adjacency Levels
  - Compliance to associative property
  - Full scale development and CAT deployment
  - Aggregation in Integrity and Availability aspects

The Future

- There are several logical extensions or related areas of future research:
  - Risk assessment derivation of Adjacency Levels
  - Compliance to associative property
  - Full scale development and CAT deployment
  - Aggregation in Integrity and Availability aspects
  - Develop and understanding why only 30 year old research exists.

– End of Presentation –