Threat Modelling

ITWeb Security Summit Workshop

Agenda

- Why Threat Model – 5 mins
- Definition & Semantic Squabbles – 15 mins
  - Semantic Bingo Prac – 10 mins
- Risk Equation – 15 mins

Agenda - Approaches

- Attack Trees – 20 mins
  - Break – 10 mins
- Octave Allegro – 20 mins
  - Break – 5 mins
- Microsoft – 25 mins
  - Break – 5 mins
- Corporate Threat Modelling Tool – 30 mins
  - Break – 10 mins
- CTM Practical – 1 hr

About Me

- Dominic White

- Work:

Security Manager
Security Auditor / Pentester
Security Consultant

- Academic:

MSc in Security
Ongoing research

Introduction

What is TM
Why TM
Definitions

Why Threat Model?

Usual Drivers of Controls

- Audit reports
  - Prioritises: financial systems, audit house priorities, auditor skills, rotation plan, known systems
- Vendor marketing
  - Prioritises: new problems, overinflated problems, product as solution
- New Attacks
  - Prioritises: popular vulnerability research, complex attacks
- Individual Experience
  - Prioritises: past experience, new systems, individual motives

Why Threat Model?

Threat Modelling provides:

- All (most) risks
  - systematic enumeration of risks
- Prioritisation of risks
  - puts known risks in their place & compares new risks
- Justification
  - model not appeal to authority
- Decision Making
  - scenario modeling to test decisions
- Education
  - involves whole team

What is Threat Modelling?

A threat model is:

"A systematic, non-provable, internally consistent method of modeling a system, enumerating risks against it, and prioritising them."

- Systematic
- Non-Provable
- Internally Consistent
- System Model
- Risk Enumeration
- Prioritisation

Definitions & Semantic Squabbles

- Threat modeling is attack focused risk assessment
- People muddied the waters with “threat”

- Little consistency across industry for:
  - Risk
  - Threat
  - Vulnerability
  - Impact

Practical Semantic Bingo

Risk

risk |risk|

noun

a situation involving exposure to danger *: flouting the law was too much of a risk | all outdoor activities carry an element of risk.*

- [in sing.] the possibility that something unpleasant or unwelcome will happen *: **reduce the risk of heart disease | [as adj.] a high consumption of caffeine was suggested as a risk factor for loss of bone mass.***
- [usu. in sing.] [with adj.] a person or thing regarded as likely to turn out well or badly, as specified, in a particular context or respect *: Western banks regarded Romania as a good risk.*
- [with adj.] a person or thing regarded as a threat to something in need of protection *: she's a security risk.*
- [with adj.] a thing regarded as likely to result in a specified danger *: gloss paint can burn strongly and pose a fire risk.*
- (usu. **risks) a possibility of harm or damage against which something is insured.**
- the possibility of financial loss : [as adj.] *project finance is essentially an exercise in risk management.*

Threat

threat |θret|

noun

1 a statement of an intention to inflict pain, injury, damage, or other hostile action on someone in retribution for something done or not done : *members of her family have received death threats*.

- Law a menace of bodily harm, such as may restrain a person's freedom of action.

2 a person or thing likely to cause damage or danger : *hurricane damage poses a major threat to many coastal communities*.

- [in sing.] the possibility of trouble, danger, or ruin : *the company faces the threat of bankruptcy | thousands of railroad jobs came* ***under threat*.**

Vulnerability

vulnerable |ˈvəln(ə)rəbəl|

adjective

susceptible to physical or emotional attack or harm *: we were in a vulnerable position | small fish are* ***vulnerable to predators.***

- Bridge (of a partnership) liable to higher penalties, either by convention or through having won one game toward a rubber.

DERIVATIVES

vulnerability |ˌvəln(ə)rəˈbilitē| noun (pl. -ties)

Impact

impact

noun |ˈimˌpakt|

• the effect or influence of one person, thing, or action, on another *: our regional measures have had a significant* ***impact on unemployment.***

verb |imˈpakt|

• have a strong effect *: high interest rates have* ***impacted on retail spending | [trans.] the move is not expected to impact the company's employees.***

USAGE The phrasal verb **impact on, as in** ***: when produce is lost, it always impacts on the bottom line, has been in the language since the 1960s. Many people disapprove of it despite its relative frequency, saying that make an impact on or other equivalent wordings should be used instead. This may be partly because, in general, new formations of verbs from nouns (as in the case of impact) are regarded as somehow inferior. As a verb, impact remains rather vague and rarely carries the noun's original sense of forceful collision. Careful writers are advised to use more exact verbs that will leave their readers in no doubt about the intended meaning. In addition, since the use of impact is associated with business and commercial writing, it has a peripheral status of 'jargon,' which makes it doubly disliked.***

Risk Equation

- Understand concepts in relation to each other
  - Discrete
  - Individually necessary
  - Collectively sufficient

risk = threat x vulnerability x impact

Definitions

- Vulnerability
  - A vulnerability is a weakness in an asset which could be exploited by a threat. A vulnerability usually refers to “flaws or misconfigurations that cause a weakness in the security of a system”.
- Threat
  - ISO/IEC 13335-1 defines a threat generally as “a potential cause of an unwanted impact to a system or organisation.“ More specifically a threat is an entity with both the capability and the intention to exploit a vulnerability in an asset. Some sources define a threat source as the actual entity and the threat as “capabilities, intentions, and attack methods of adversaries to exploit, damage, or alter information or an information system .”
- Exploit
  - An exploit is either; a process or tool that will attack a vulnerability in an asset; or it is the action of attacking a vulnerability (exploiting a vulnerability) thereby realising the threat against that asset. Malware in the form of viruses, Trojans, root-kits and most often worms frequently (but not always) use exploits. For example, while phishing is an example of exploiting human trust, in this document exploits refer to tools or processes specifically aimed at exploiting vulnerabilities in software and electronic systems.

Likelihood

risk = threat x vulnerability x impact

likelihood = threat x vulnerability

risk = likelihood x impact

Approaches

Attack Trees

Octave Allegro

Microsoft Threat Modeling

Attack Trees

Quick Attack Modeling

Attack Trees

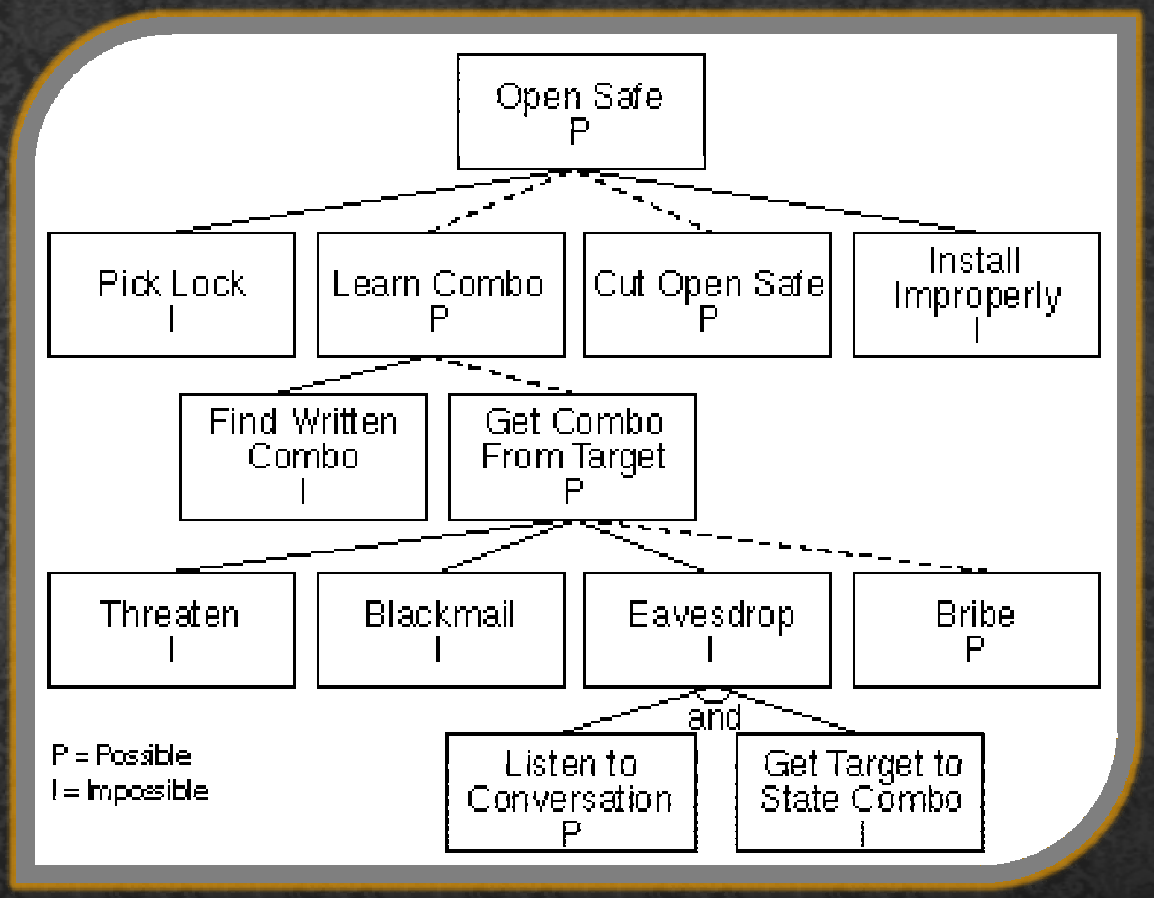
- Early form of Threat Modeling
- Popularised by Bruce Schneier in 1999
  - http://www.schneier.com/paper-attacktrees-ddj-ft.html

"Basically, you represent attacks against a system in a tree structure, with the goal as the root node and different ways of achieving that goal as leaf nodes."

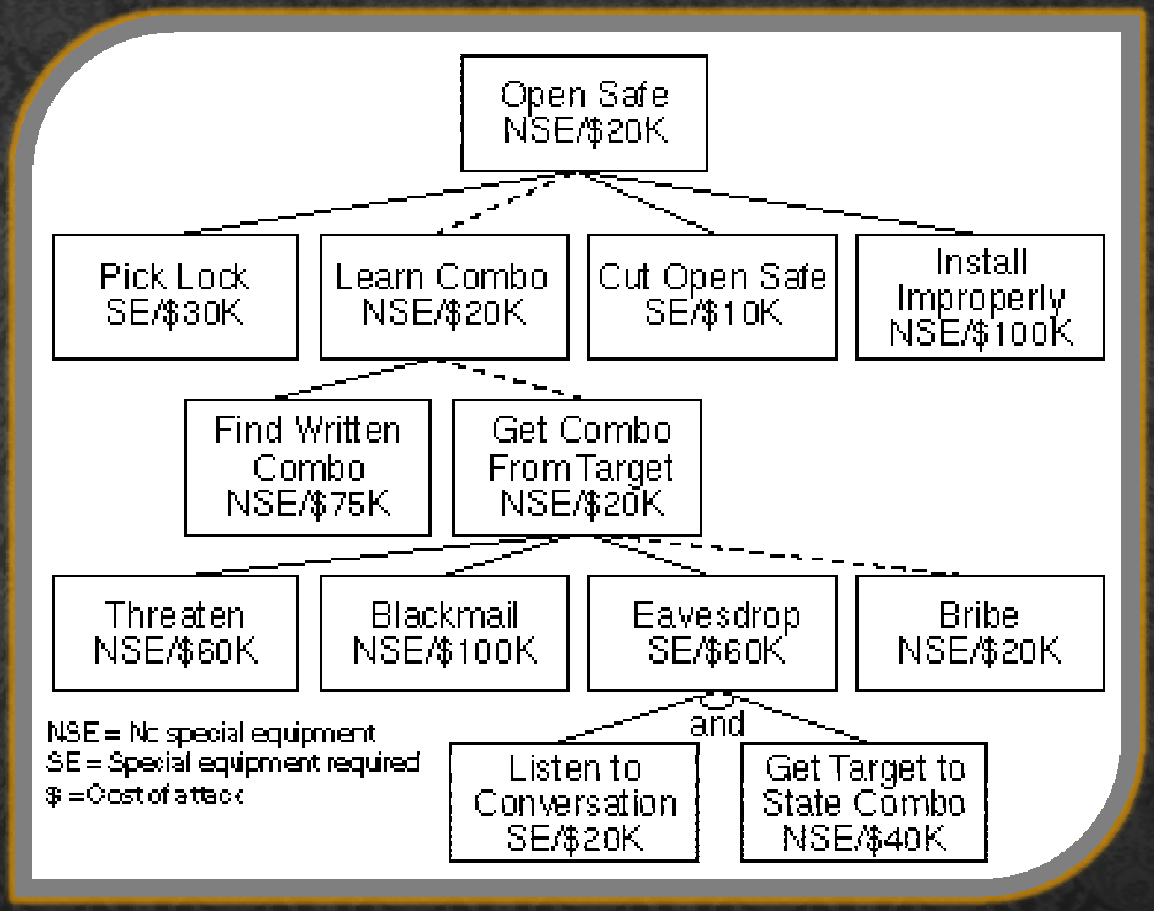
Attack Trees

- Root Node – Goal
- Leaf Node – Way of achieving goal
- Sub Node – Sub Goal of Root Node
- AND vs OR nodes
- Node attributes
- Attack Paths

Attack Trees – Example 1



Attack Trees – Example 2



Creating Attack Trees

- Think of your Goals, place as root nodes of individual trees
- Think of all attacks that would achieve this goal
  - For each attack, think of relevant attributes
- For each sub-goal, repeat previous step
- Give to someone else, repeat previous 2 steps
- Separate out common attack trees (modular)

Practical – Attack Tree

- System: Internet Banking
- Goal: Steal funds

- Brainstorm sub-goals
- Split into groups to discuss
- Contribute back to group

Attack Trees – Pros/Cons

- Pros
  - Easy to start
  - Trees can be reused
  - Flexible
- Cons
  - Tree required per goal
  - Difficult to have common sub trees
  - Only represents attacks
  - Inconsistent attributes
  - Difficult to guess attacks if not experienced

Break

Octave Allegro

Formalised Risk Model

4

Octave Allegro

- A cert.org project out of Carnegie Mellon
  - http://www.cert.org/octave/

"OCTAVE® (Operationally Critical Threat, Asset, and Vulnerability EvaluationSM) is a suite of tools, techniques, and methods for risk-based information security strategic assessment and planning."

- OCTAVE-Allegro, a streamlined approach for information security assessment and assurance
- Highly formalised

Octage Allegro – 8 Steps

1. Establish Risk Measurement Criteria
2. Develop an Information Asset Profile
3. Identify Information Asset Containers
4. Identify Areas of Concern
5. Identify Threat Scenarios
6. Identify Risks
7. Analyse Risks
8. Select Mitigation Approach

Octave Allegro
Establish Risk Management Criteria

- Qualitative set against which effect of risk is measured
- Consistent set representative of senior management views
- Used across all risk assessments
- Highly specific to organisation
- Step 1 – Define Criteria:
  - Reputation, Financial, Productivity, Health & Safety, Fines & Legal Penalties
- Step 2 - Prioritise:
  - Most important 5, Least important 1

Octave Allegro
Develop an Information Asset Profile

- Asset is something of value to organisation
- Focus on information assets
- Technology & people assets are containers
- Steps:

1. Brainstorm critical information assets
2. Select critical few by thinking of impact if:
   - Disclosed
   - Modified
   - Lost or Destroyed
   - Interrupted

Next steps are based on **one** critical asset

Octave Allegro
Develop an Information Asset Profile

- Steps (continued):

3. Select one critical information asset
4. Document rationale for selection
5. Describe asset: number, distribution, media, common name, applicable regulation, consuming processess etc.
6. Identify owner/s (primary responsibility) by position & name
7. Record CIA security requirements
8. Select most important security requirement

Octave Allegro
Identify Information Asset Containers

- Where info assets are; stored, transported or processed
- Points of vulnerability & control
- Internal & external
- Types:
  - Technical
  - Physical
  - People
- Owner of container == custodian of asset
- Use questionaaires

Octave Allegro
Identify Areas of Concern

- Real world scenarios representing threats and corresponding outcomes
- Quickly capture situations that come to mind, don't list all possible
- Consider; actors, motives & outcomes
- Perform for each container
- Each AoC will be modeled separately and capture a single risk

Octave Allegro
Identify Threat Scenarios

- Expand areas of concern through guided questions
- Questionnaires for each container type: technical, physical, people
- Based on threat trees
  - Actor: Internal vs External
  - Motive: Accidental vs Deliberate
  - Outcome: Disclosure, Modification, Interruption, Destruction
- Create new area of concern for each identified threat scenario
- Determine probability – high, medium or low (optional)

Octave Allegro
Identify Risks

- Determine how threat scenarios/areas of concern could impact organisation
- Describe consequences mindful of outcome and risk criteria
- Equation
  - **Threat (condition) + Impact (consequence) = Risk**
  - **[Steps 4 and 5] + [Step 6] = Risk**

  - **Actually: Impact = Risk ☹**

Octave Allegro
Analyse Risks

- Qualitative measure of organisational impact
- Calculated “risk score”
- Record “high, med or low” impact against each risk criteria
  - Consider all consequences lists
- Weighted based on risk criteria prioritisation
  - Multiply impact by risk criteria priority
- Sum the score for each risk criteria area
- Total is relative risk score (actually impact score)

Octave Allegro
Select Mitigation Approach

- Impact & Probability considered, not combined
- Options:
  - Avoid – controls to prevent
  - Limit – limit impact

1. Prioritise & order risks
2. Assign approach: mitigate, accept or defer
3. Develop mitigation strategy
   - Prevent: actor, means, motive, outcome
   - Reduce: probability, impact,

Octage Allegro – Pros/Cons

- Pros
  - Thorough
  - Formalised
  - Includes Organisational Risk
  - Includes Asset Identification
  - Includes Organisational Structure
  - Guided threat identification
- Cons
  - Takes a long time
  - Conflates risk with impact & optional probability
  - Provides basic view of potential threats

Break

Microsoft Threat Modeling

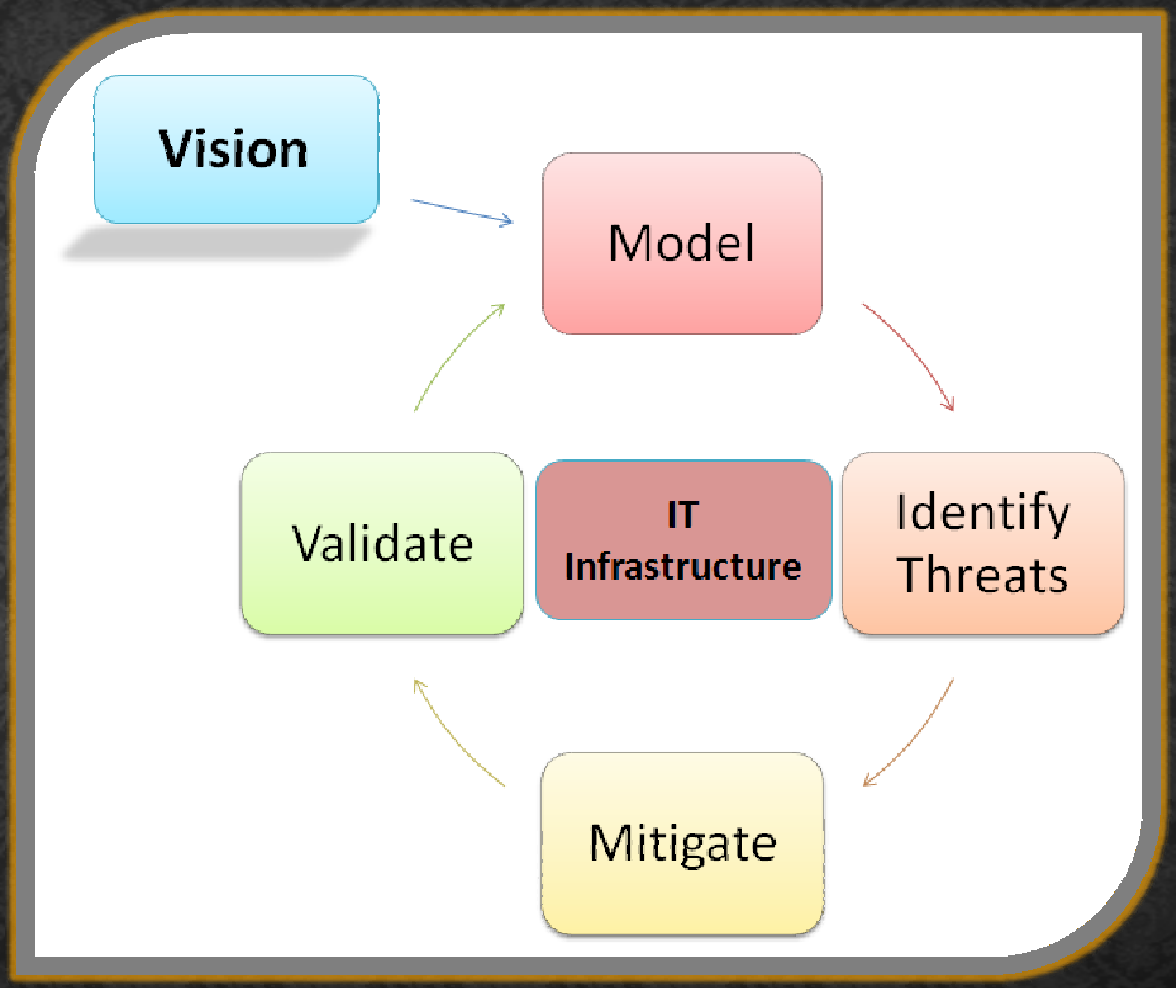
Development &
Infrastructure Focused

5

Microsoft Threat Modeling

- Initially part of Microsoft's SDL
- Very development / developer focused
  - Focused on design analysis
- STRIDE model underpins enumeration of threats
  - http://msdn.microsoft.com/en-us/magazine/cc163519.aspx
- No calculation
- Recently released "IT Infrastructure Threat Modeling"
  - http://go.microsoft.com/fwlink/?LinkId=154010

MS Infrastructure TM
5 Steps



MS Infrastructure TM Vision

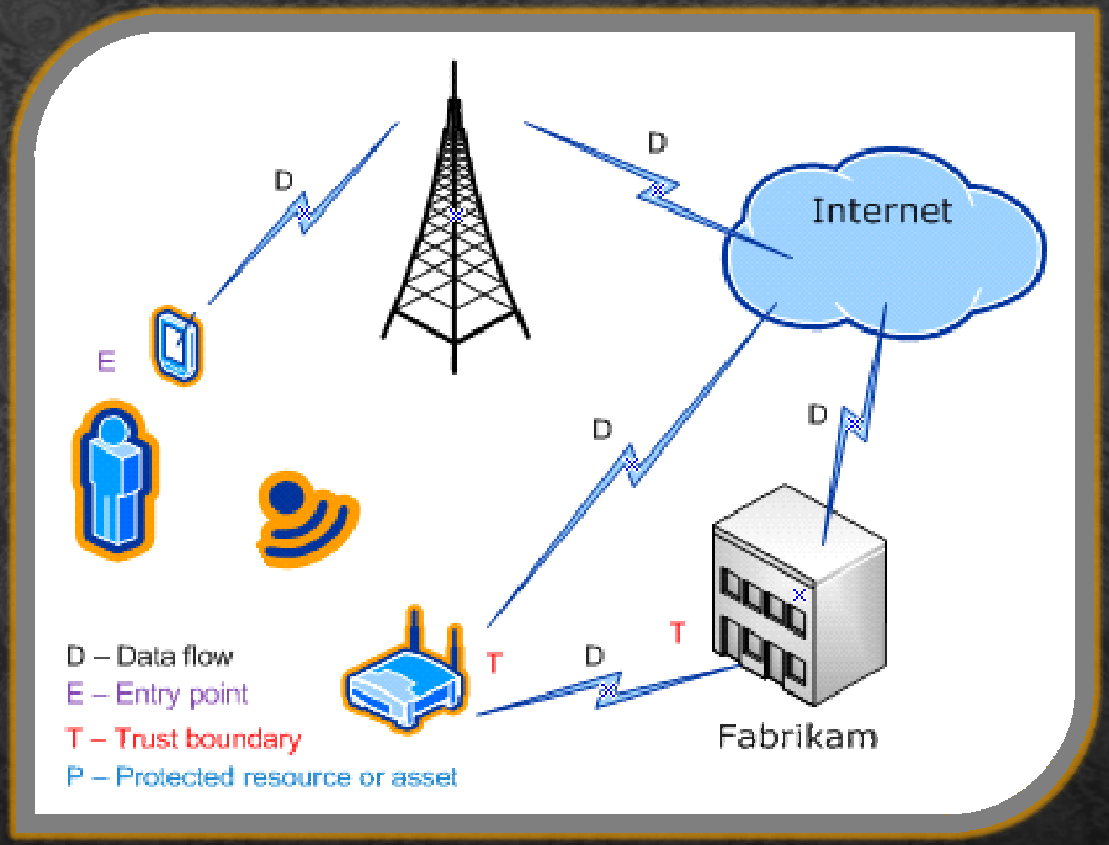
- Develop a vision for each component
  - Where will the component be used?
  - How will the component be used?
- High level conceptual architecture

MS Infrastructure TM Model

- Level 1 Diagram
  - High-level; single component / scenario
- Level 2 Diagram
  - Low-level; detailed subcomponents and dependencies
- Level 3 Diagram
  - Much more detailed
- Identify
  - Data Flow
  - Entry Point
  - Trust Boundary
  - Asset

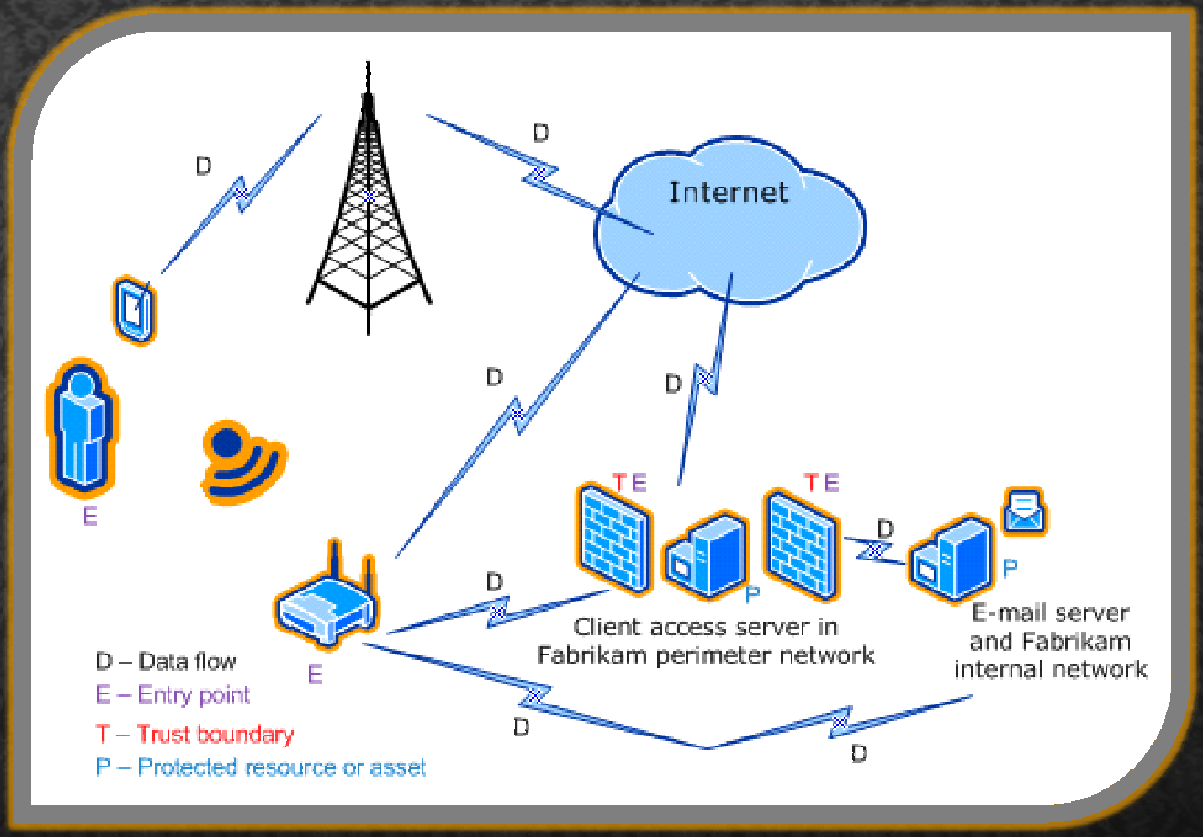
MS Infrastructure TM Model

- High-level scenario



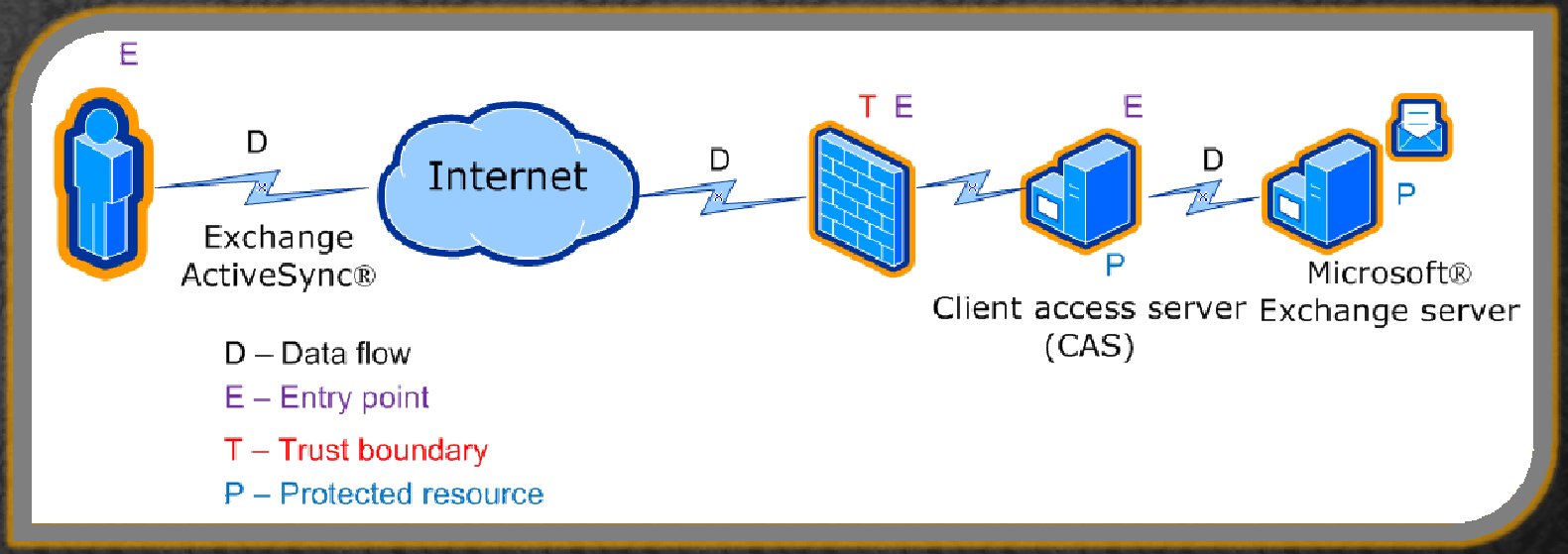
MS Infrastructure TM Model

- Low-level; detailed subcomponents and dependencies

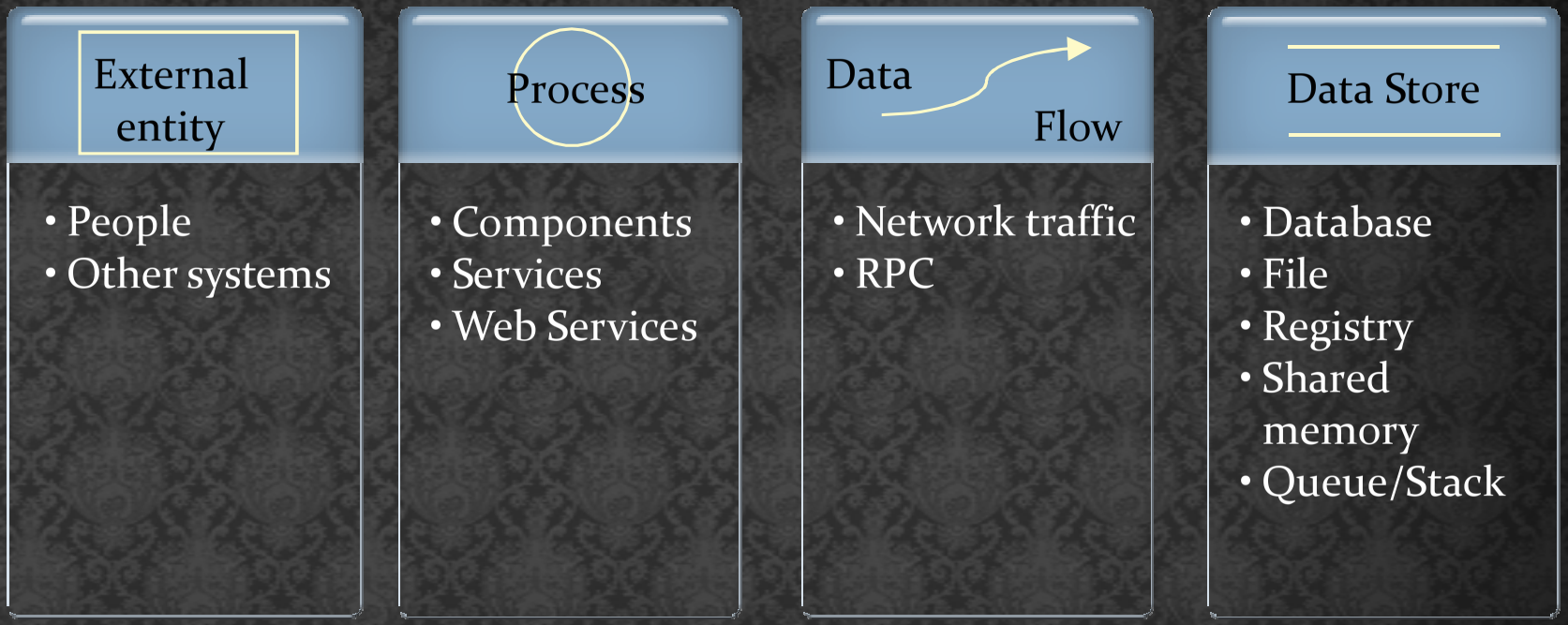


MS Infrastructure TM Model

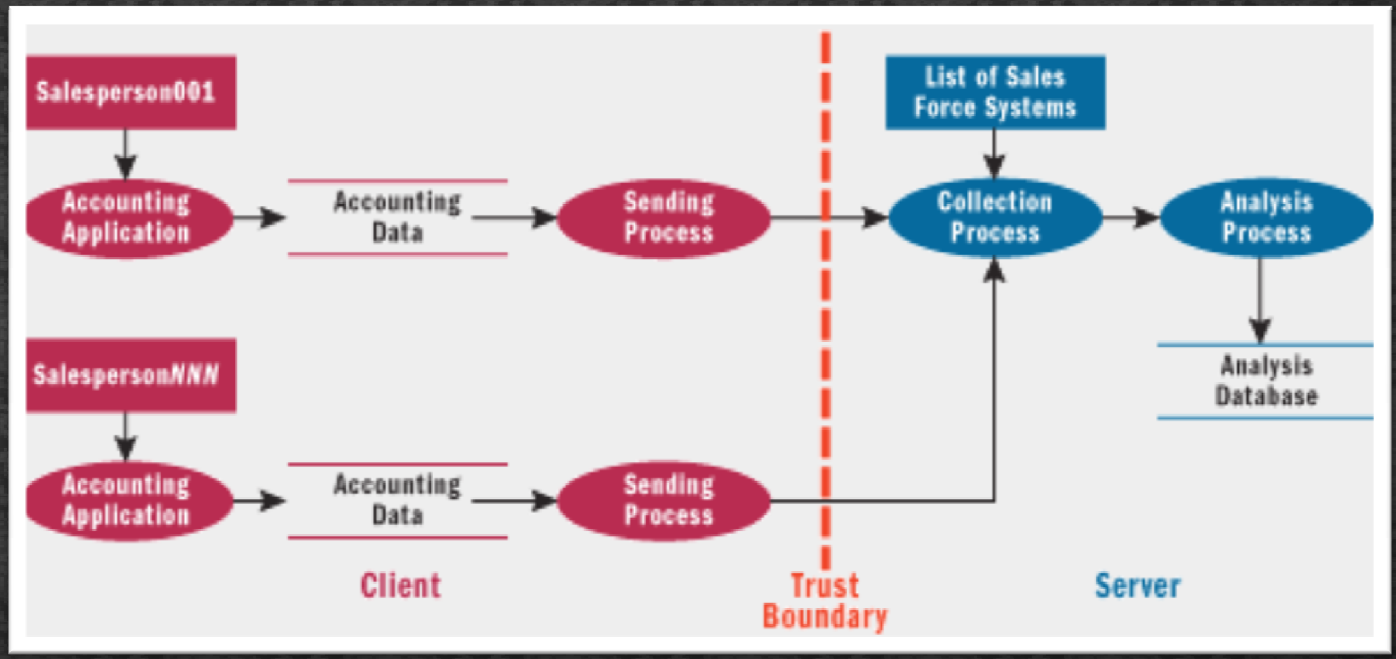
- More detailed; product, technology, and protocol-specific



MS Infrastructure TM Model - DFD

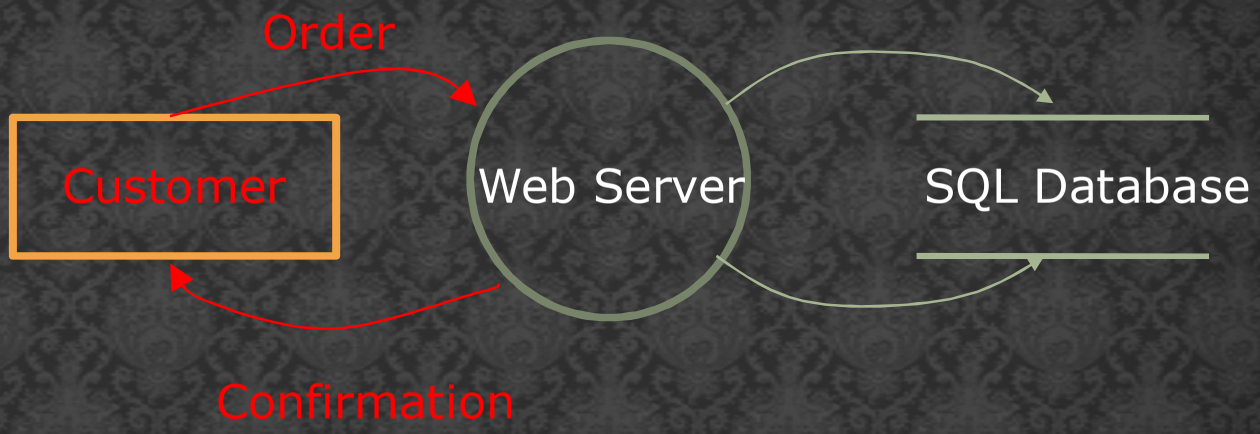


MS Infrastructure TM Model - DFD



MS Infrastructure TM Model – DFD Validation

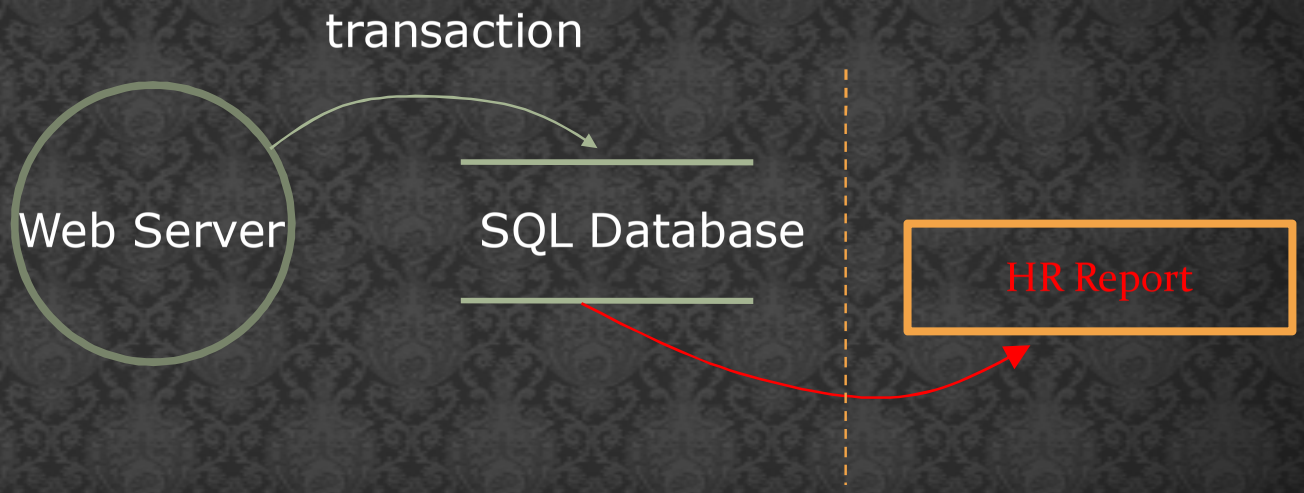
- Does data magically appear?



Data comes from external entities or data stores

MS Infrastructure TM Model – DFD Validation

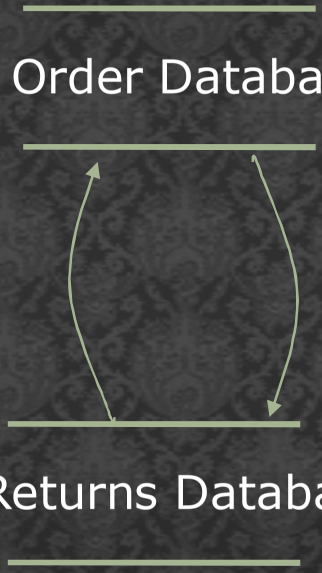
- Are there data sinks?

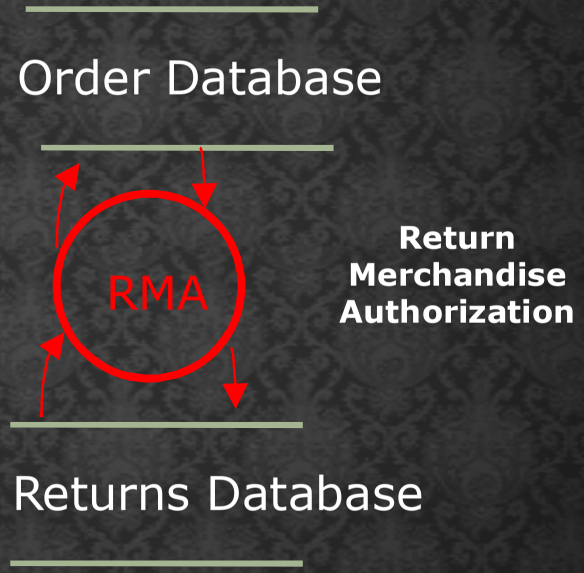


You write to a store for a reason; someone uses it

MS Infrastructure TM Model – DFD Validation

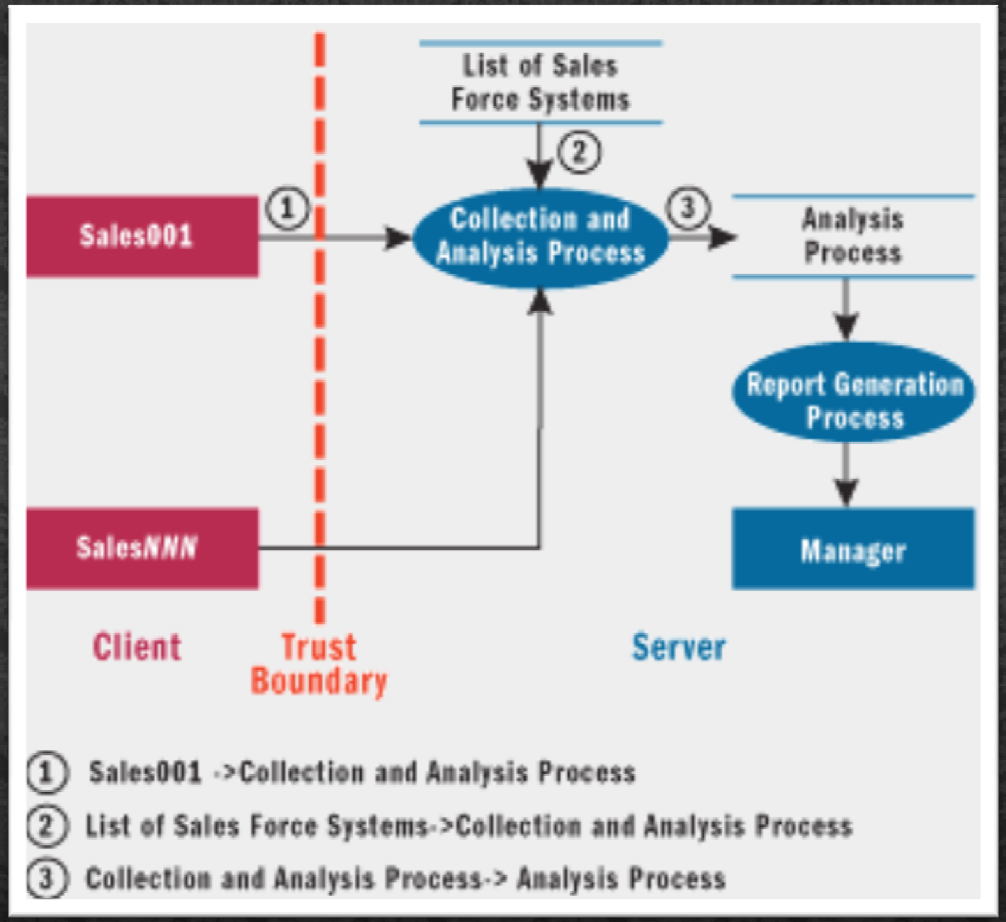
Data doesn't flow magically...



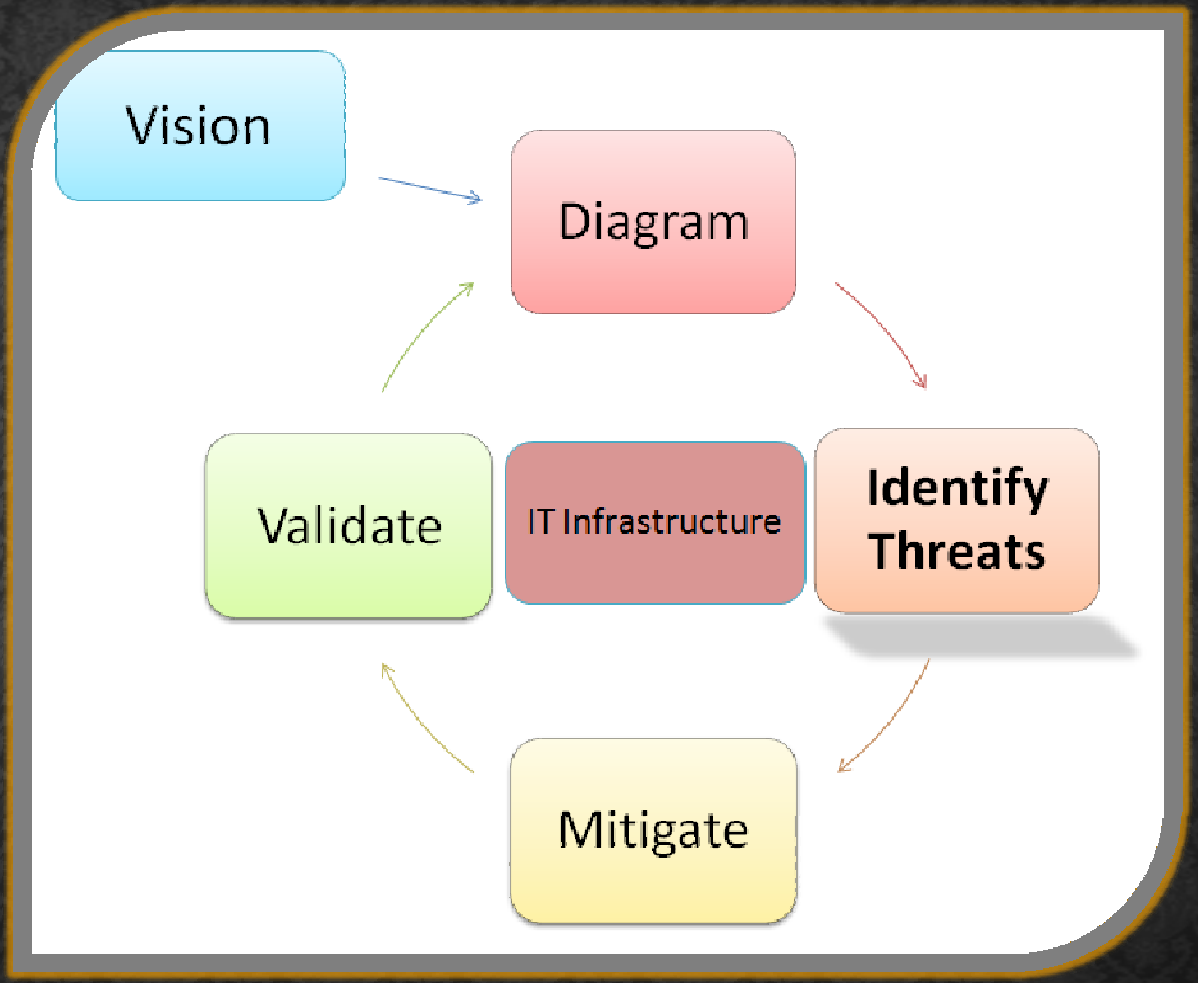


...it goes through a process

MS Infrastructure TM Model - DFD



MS Infrastructure TM
Identify Threats



MS Infrastructure TM Identify Threats

- Guided Brainstorming
- Use STRIDE to step through the diagram elements
  - Think specifically about how threats are manifested

Threat	Property we want to focus on
Spoofing	Authentication
Tampering	Integrity
Repudiation	Non-repudiation
Information Disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

MS Infrastructure TM Identify Threats

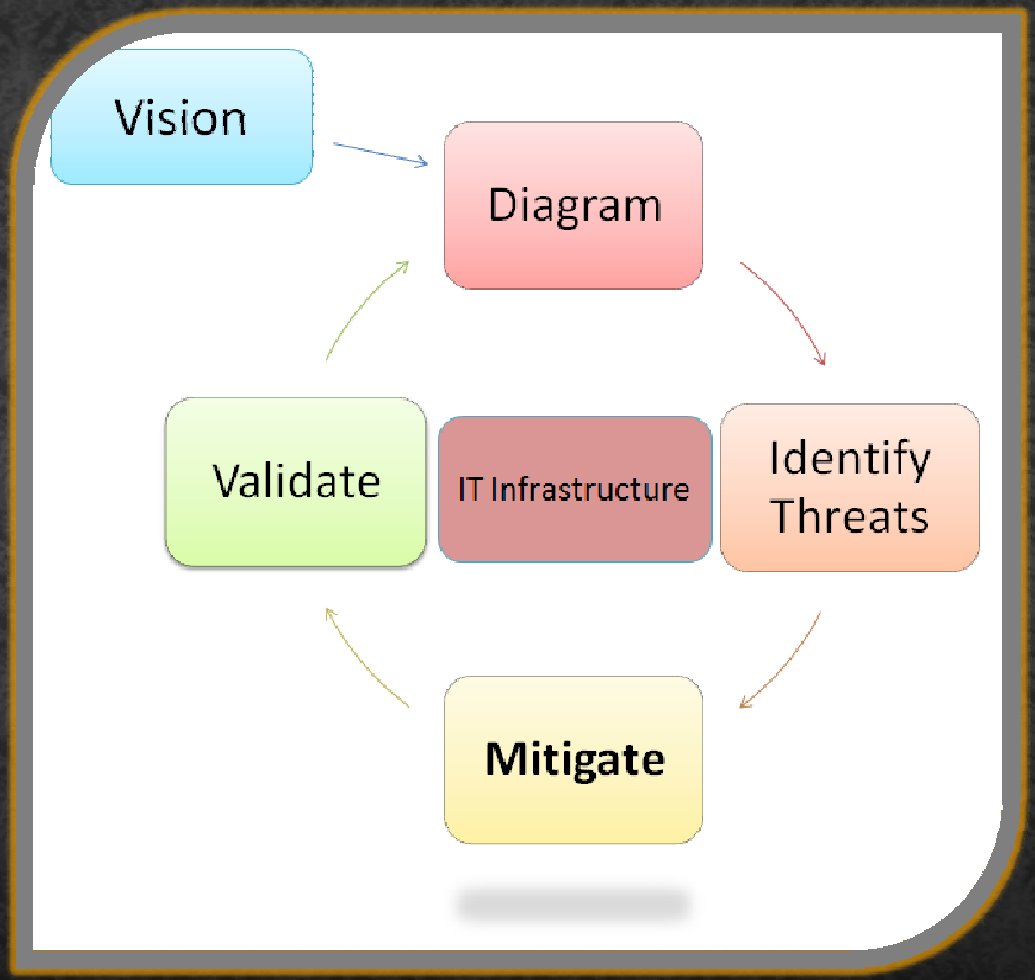
Threat	Property	Definition	Example
Spoofing	Authentication	Impersonating something or someone else	Pretending to be the CEO, or microsoft.com, or ntdll.dll.
Tampering	Integrity	Modifying data or code	Modifying a DLL on disk or DVD, or a packet as it traverses the LAN.
Repudiation	Non-repudiation	Claiming to have not performed an action	"I didn't send that e-mail," "I didn't modify that file," "I certainly didn't visit that Web site, dear!"
Information Disclosure	Confidentiality	Exposing information to someone not authorized to see it	Allowing someone to read the Windows® source code; publishing a list of customers to a Web site.
Denial of Service	Availability	Deny or degrade service to users	Crashing Windows or a Web site, sending a packet and absorbing seconds of CPU time, or routing packets into a black hole.
Elevation of Privilege	Authorization	Gain capabilities without proper authorization	Allowing a remote internet user to run commands is the classic example, but going from a limited user to admin is also EoP.

MS Infrastructure TM Identify Threats

- Different threats affect each type of element

Element	S	T	R	I	D	E
External entity	✓		✓			
Process	✓	✓	✓	✓	✓	✓
Data store		✓	✓	✓	✓	
Dataflow		✓		✓	✓	

MS Infrastructure TM
Mitigate



MS Infrastructure TM
Mitigate

- Mitigation is the point of MS' threat modeling
- Mitigation is the act of addressing or alleviating a risk
  - Protect resources
  - Implement secure systems
- Microsoft refers to risks as threats here
- Technical focus, no acceptance or deference

MS Infrastructure TM Mitigate

- There are four ways to mitigate risks:
  - Redesign to eliminate
  - Apply standard mitigations
  - Invent new mitigations (riskier)
  - Accept vulnerability in architecture or implementation
- Ensure that you mitigate each risk

MS Infrastructure TM Mitigate - Examples

Spoofing	Authentication	Basic authentication Digest authentication Cookie authentication Windows authentication (NTLM) Kerberos authentication PKI systems such as SSL/TLS and certificates Digital signatures Hashes
Tampering	Integrity	ACLs Digital signatures Message Authentication Codes
Repudiation	Non Repudiation	Strong Authentication Secure logging and auditing Digital Signatures Secure time stamps Trusted third parties

* Not a complete list

MS Infrastructure TM
Mitigate – Examples (cont)

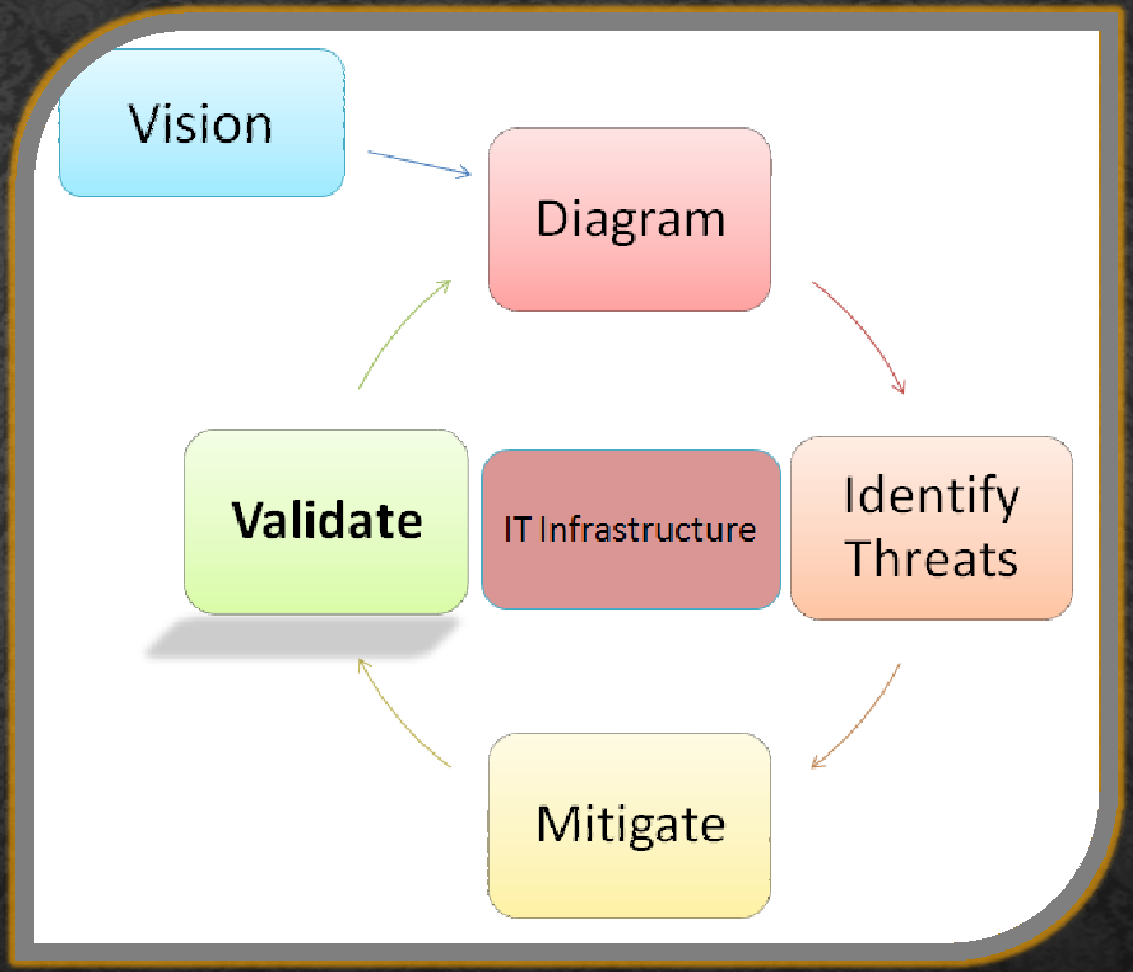
Information Disclosure	Confidentiality	Encryption ACLS
Denial of Service	Availability	Filtering Quotas Authorization High availability designs
Elevation of privilege	Authorization	ACLs Group or role membership Privilege ownership Permissions Input validation

* Not a complete list

MS Infrastructure TM Mitigate

- Mitigations are an area of expertise like networking, databases, or cryptography
- Amateurs make mistakes, so do pros
- Inadequate mitigations will appear to work
  - Until an expert looks at them
  - Tend to fail over time due to non-standard processes
- When you need to invent mitigations
  - Get expert help
  - Ensure that you test them

MS Infrastructure TM
Validate



MS Infrastructure TM Validate

- Validate everything
  - Diagram – match implementation
  - Elements – modeled correctly
  - Risks – valid
  - STRIDE applied to all elements
  - Mitigations – effective and tested
  - Dependencies – captured correctly
  - Assumptions - valid

Practical
Microsoft Elevation of Privilege

- Card Game

Microsoft TM - Pros/Cons

- Pros
  - Flexible
  - Guided thinking
  - In heavy use
  - Tools, Games & Many Publications
- Cons
  - Specific uses
  - Technology specific
  - Doesn’t involve wider business goals

Break

SensePost Corporate Threat Modelling

Security Manager &
Large Scope Focused
Threat Modeling

6

SensePost CTM

- Developed for consultative role
  - i.e. likely not the person making the changes
- Focus is on:
  - Providing decision making information
  - Rapid initial model creation
- Hybrid approach
  - Bit of all the others
  - Some parts we just threw out
- Highly flexible
- Detailed & aggregated results

SensePost CTM Architectural Overview

- Start with Architectural Overview
- Diagram is a result of much
  - Meeting
  - Understanding
  - Testing
- Use your favourite approach, modify based on complexity & scope
- Focus on technology containers
  - Criticality based on information contained & services provided
- Example - Bank

SensePost CTM Risk Equation

$$risk = \left(\begin{array}{c} likelihood \times \\ \left(percentage \left(average \begin{pmatrix} inverse(usertrust) + \\ inverse(locationtrust) \end{pmatrix} \right) \right) \\ + \\ \begin{pmatrix} interfacevalue \times \\ percentage(impactofattack) \end{pmatrix} \end{array} \right)$$

SensePost CTM Risk Equation

risk = applied likelihood + value at risk

applied likelihood =

attack likelihood (reduced by)

user trust + location trust

value at risk =

value of asset (reduced by)

amount of asset exposed by attack

SensePost CTM Modelling Overview

- Locations
  - trust of location
- Users
  - trust of user
- Interfaces
  - method of access
  - asset value
- Threats (misnamed risks)
  - attack
  - likelihood

SensePost CTM Locations

- Represent trust of location – how much control
- Interfaces exposed at locations
- Users present at locations
- Three types:
  - Physical
    - Data centers, Head Office, Remote Sites
  - Network
    - Internet, DMZ, Server Network, User Network
  - Logical
    - Systems/Applications
    - Authorisation levels

SensePost CTM
Users

- Enforceable trust of user group
  - i.e. contractual or controlled trust
- Users mapped to locations
- Interfaces exposed to users via locations
- Three types:
  - External Users
    - anonymous, suppliers, contractors
  - Internal Users
    - normal, administrative, call centre
  - Systematic
    - Automated system interactions

SensePost CTM Interfaces

- Methods of interacting with an asset/system
- Expose value of asset – consistent across system
- General structure:
  - System 1
    - Functionality
      - Authenticated functionality
      - Administrative functionality
    - Interfaces
      - Client interfaces
      - Backend interfaces
      - Physical interfaces

SensePost CTM Mapping

- Users to Location
  - Anonymous if no auth, even if internal user
  - Automated system interactions only within logical locations
  - Super User to Admin Functionality
  - Normal Users to Authenticated Functionality
- Interfaces to Location
  - Physical interfaces only to physical locations
  - Client & Backend int only to network loc
  - Functionality interfaces only to system locations

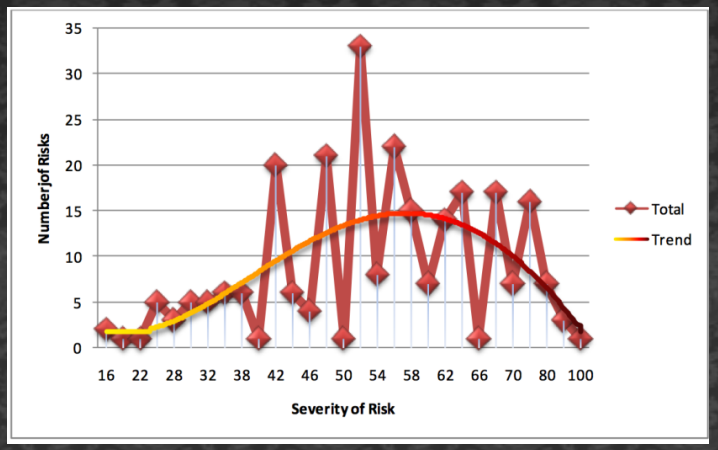
SensePost CTM Risks

- Actually threats
- Attacks applies to an interface that expose value
- Some attacks expose more value than others
- Some attacks are more likely to succeed against certain interfaces
- Mapping
  - Physical risk to Physical Interface
  - Process risk only to Functionality Interfaces

SensePost CTM Risks

- Likelihood
  - Don't account for user or location trust
  - Popularity, capability, motive, means, population should influence
- Impact
  - Moderator (percentage) of value → value at risk
  - Worst case scenario compromise of interface

SensePost CTM Scenario Modelling



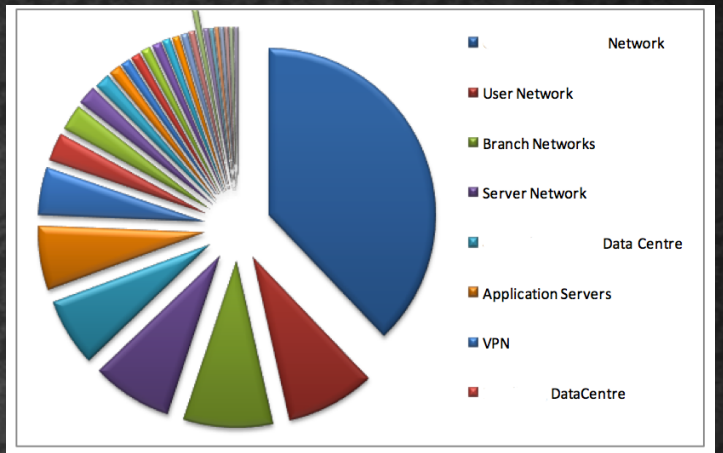
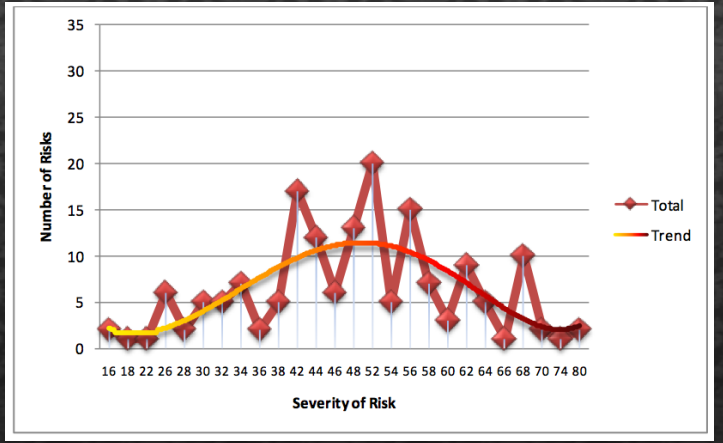


Figure Number and Severity of Risks per Location



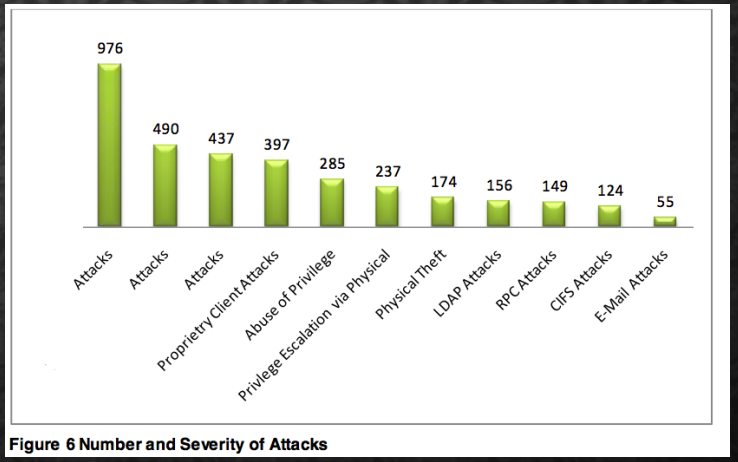


Figure 6 Number and Severity of Attacks