Universidad de los Andes
DEPARTAMENTO DE SISTEMAS

Arquitectura y Diseño de Software

Atributo de Calidad Seguridad

Seguridad

- Cómo definir Software Seguro
  - Protección del Software una vez construido?
  - Construir Software Seguro
  - Diseñar Software Seguro
  - Saber si el software es seguro
  - Protejer los sistemas de software una vez terminados
  - Educar a todos los participantes en la construcción de software

Seguridad

- Seguridad de Aplicaciones Versus Seguridad de Software
- El software es transversal a muchos escenarios de seguridad
- Cuando no se construye el software se requieren ayudas adicionales
  - Firewalls

Seguridad

Software Seguro

Imagen tomada de "Sotware Security:Building Security In" Gary McGraw

Seguridad en el Software

- Manejo del Riesgo
  - Análisis de riesgo a nivel arquitectural
    - Threat modeling
  - Análisis de riesgos a lo largo del ciclo de desarrollo
- Puntos de Contacto en Seguridad
  - Seguridad en el Software no es Software para Seguridad
  - Seguridad es un atributo de calidad en el software tanto como desempeño, escalabilidad, etc.

Seguridad en el Software

- La seguridad es fundamental durante el desarrollo de software
  - Ejemplo: Microsoft's Trustworthy Computing Initiative
- Los desarrolladores, arquitectos y analistas no toman en cuenta la seguridad
- La seguridad no es solamente un password o usar SSL

Seguridad en el Software

Puntos de Contacto en Seguridad

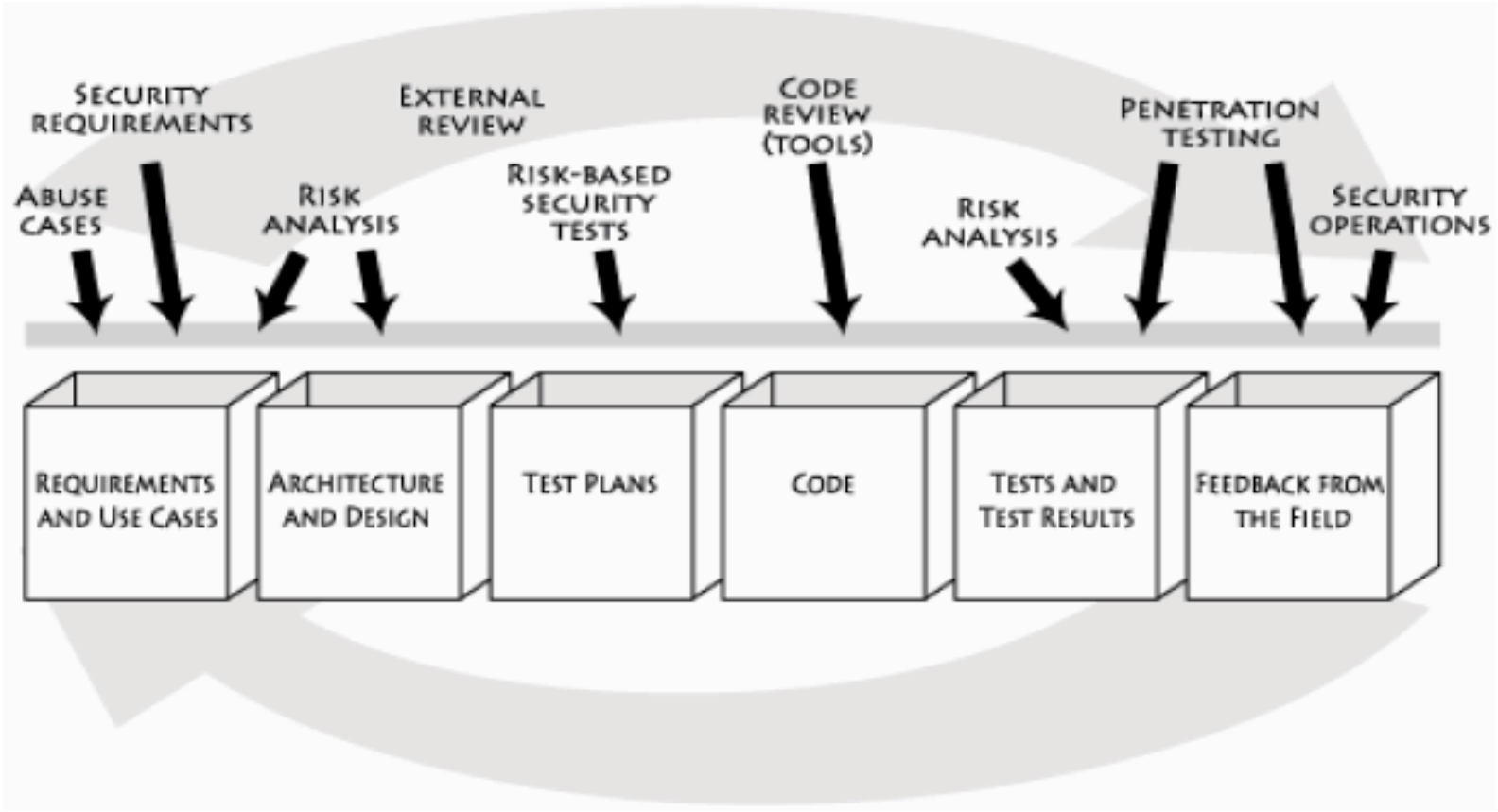


Imagen tomada de "Sotware Security:Building Security In" Gary McGraw

Seguridad en el Software

- Los puntos de contacto
  - No están diseñados para un ciclo de desarrollo particular
  - Cascada
  - RUP
  - XP / Metodologías Agiles
  - FDD

Seguridad en el Software

- Conocimiento
  - Administración del conocimiento de la organización
  - Conocimiento sobre seguridad
    - Principios
    - Guías
    - Reglas
    - Vulnerabilidades
    - Patrones de Ataque
    - Riesgos históricos

Seguridad en el Software

Manejo de Conocimiento

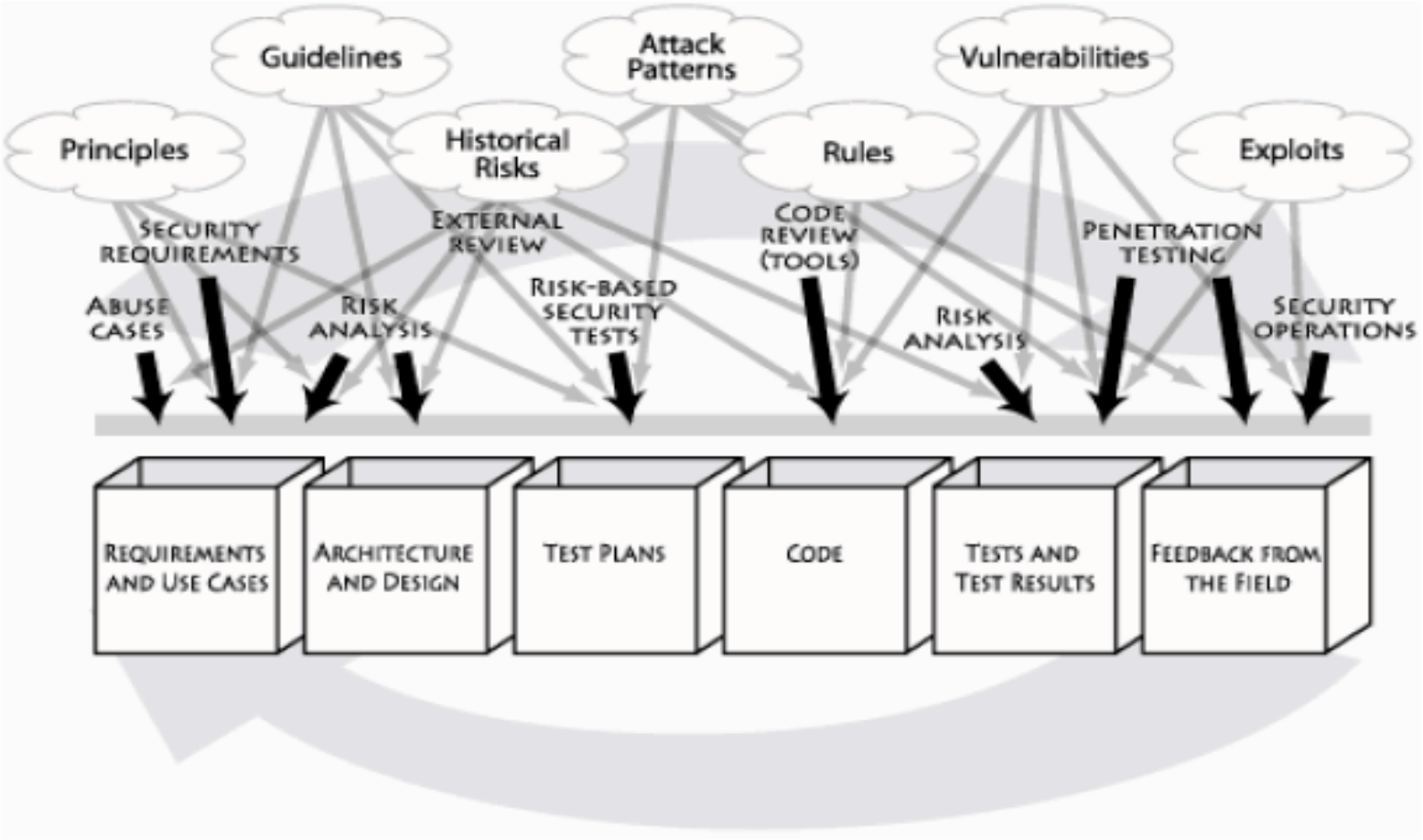


Imagen tomada de "Sotware Security:Building Security In" Gary McGraw

Marco para Manejo de Riesgos

- Cinco etapas principales

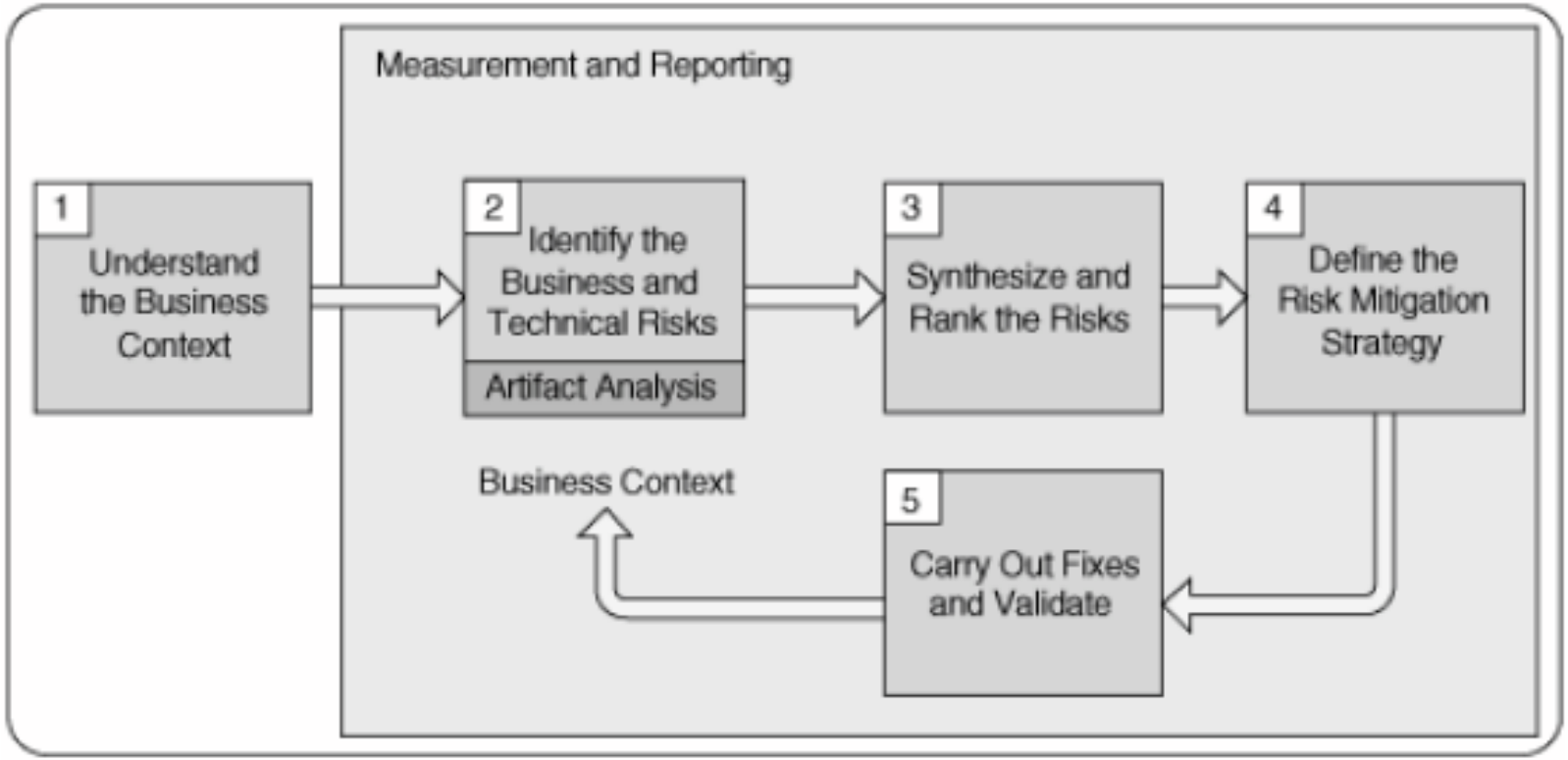


Imagen tomada de "Sotware Security:Building Security In" Gary McGraw

Marco para Manejo de Riesgos

- 1. Entender el contexto de negocio
  - Hacer explícito los motivadores de negocio
  - Niveles de servicio establecidos
  - Retorno de la inversión
- 2. Identificar los riesgos técnicos y de negocio
  - Los riesgos de negocio van encontra de los objetivos de negocio

Marco para Manejo de Riesgos

- Identificar los riesgos de negocio ayuda a definir los artefactos de software claves para mitigar los riesgos de seguridad
- Un riesgo técnico es una situación que va encontra del diseño y/o la implementación de un sistema en consideración

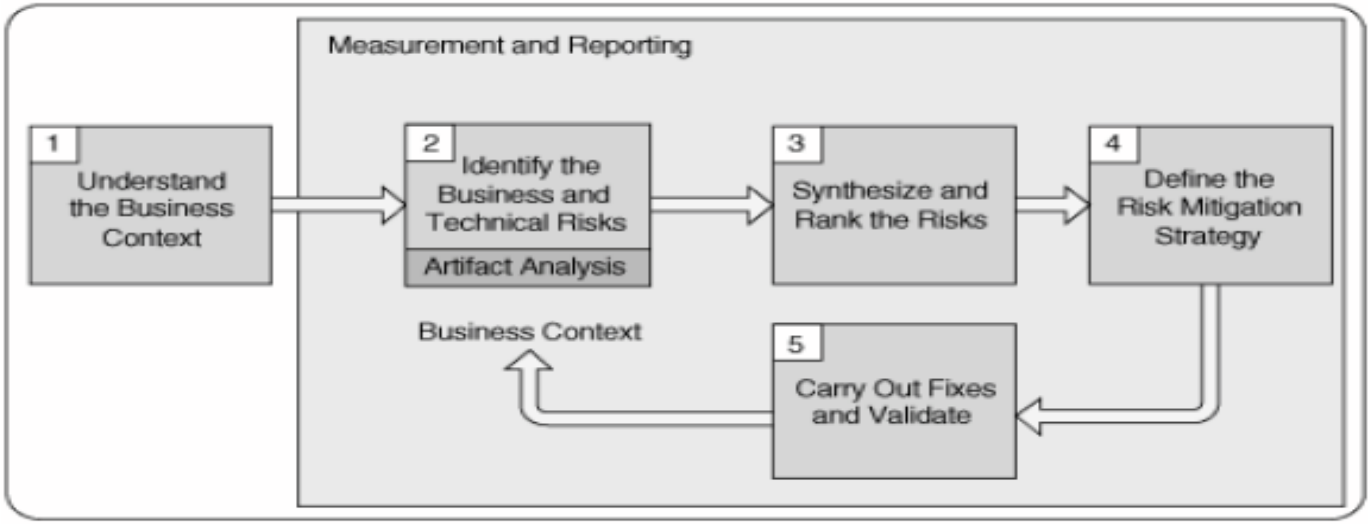
- 3. Priorizar los Riesgos
  - Esta labor toma en cuenta los objetivos de negocio de la empresa
  - Se tiene en cuenta el impacto que generaría el riesgo

Marco para Manejo de Riesgos

- 4. Definir la estrategía de mitigación del riesgo
  - Tan importante como descubrir los riesgos técnicos es saber como mitigarlos
  - Se debe generar una estrategia de mitigación de riesgos
- 5. Ejecutar la estrategia de mitigación
  - Los artefactos donde se hayan identificado fallas deben ser corregidos

Marco para Manejo de Riesgos

Desarrollo de la Hoja de Trabajo 1



ID	Riesgo Tecnológico	Indicador	Prioridad	Impacto	Método de Mitigación
1	Mala selección de Passwords	Número de passwords vulnerados	M	M	• Cambios frecuentes • Longitud mínima • Listas negras

Agenda

- Introducción
- Presentación Caso de Estudio
- Marco para Manejo de Riesgos
- **Puntos de Contacto en Seguridad**
- Casos de Abuso

Puntos de Contacto en Seguridad

- Buenas prácticas en desarrollo de software seguro
- Relativamente fáciles de integrar en el proceso de desarrollo de software
  - Conocer y entender riesgos de seguridad
  - Diseñar pensando en seguridad
  - Análisis y pruebas de los artefactos principales desde el punto de vista de seguridad

Puntos de Contacto en Seguridad

- Los siete puntos de contacto

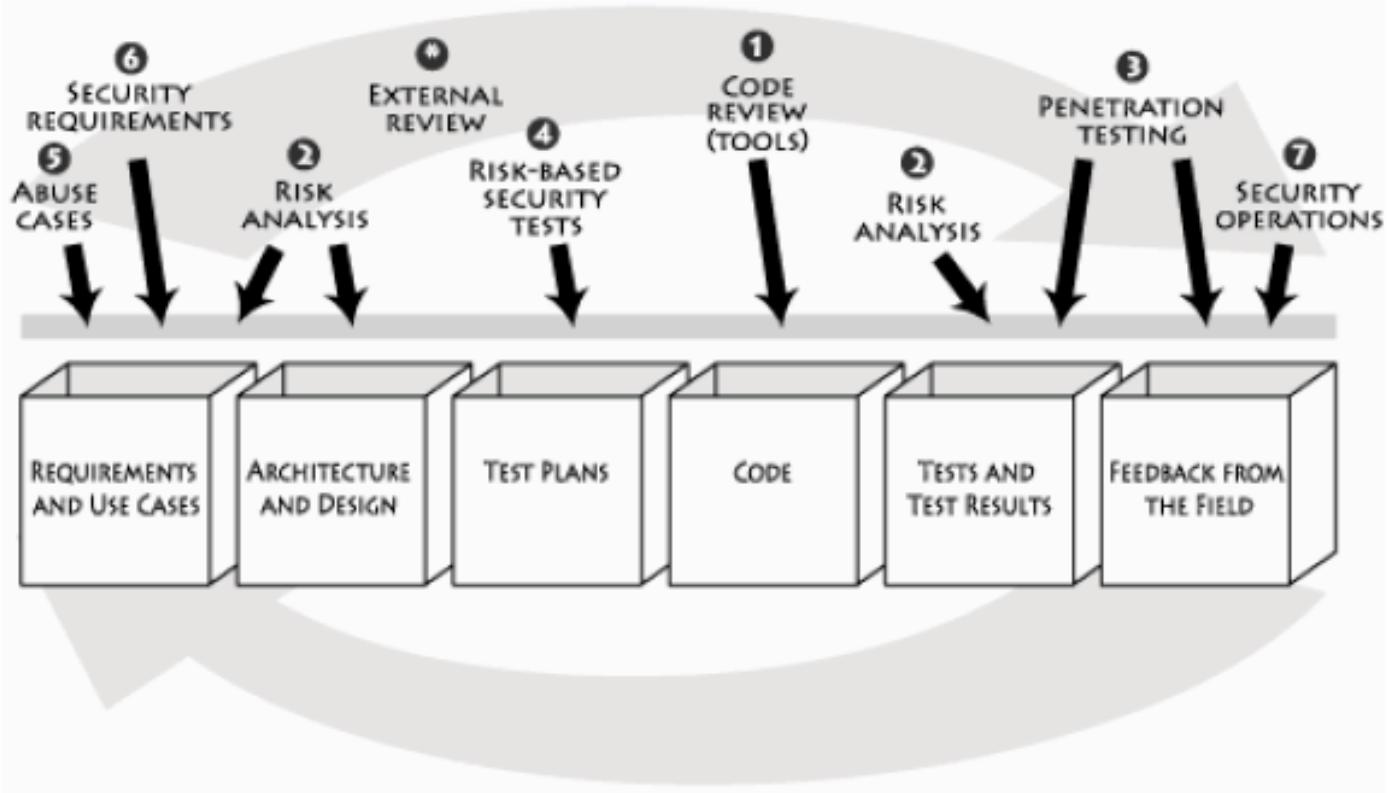


Imagen tomada de "Sotware Security:Building Security In" Gary McGraw

Puntos de Contacto en Seguridad

- 1. Revisiones de Código
  - Proceso de revisión de código
  - Mecanismo de verificación y validación estático
  - Normalmente se utiliza una lista de chequeo contra la cual se revisa e inspecciona el código
  - Revisión por pares

Puntos de Contacto en Seguridad

- 2. Análisis de riesgos arquitecturales
  - Se enfoca en los artefactos de especificación y diseño
  - Se buscan Defectos en
    - Autenticación
    - Seguridad de los Componentes
    - Seguridad de los nodos de ejecución
    - Problemas de protección de los datos

Puntos de Contacto en Seguridad

- 3. Pruebas de Penetración
  - Se utilizan los análisis de la evaluación de arquitectura
  - Permite probar el software en su ambiente de ejecución
  - Usualmente llamado hacking ético
  - Ejecutadas tarde en el ciclo de desarrollo
  - Guiadas por los casos de abuso
  - Se quiere saber cómo se comporta el sistema bajo ataque

Puntos de Contacto en Seguridad

- 4. Pruebas de seguridad basadas en riesgos
  - Se ejecutan pruebas basadas en
    - Patrones de ataque
    - Análisis de riesgos
    - Casos de abuso
  - Pueden ser ejecutada a nivel de componentes unitarios
  - En algunos casos construidas antes del desarrollo del software

Puntos de Contacto en Seguridad

- 5. Casos de Abuso
  - Se enfocan en los artefactos de requerimientos y casos de uso
  - Es una forma de entrar en la mente de los atacantes
  - Similares a los casos de uso
  - Describen el comportamiento del sistema bajo ataque
  - Se debe conocer lo que se quiere proteger, de quién y por cuanto tiempo

Puntos de Contacto en Seguridad

- 6. Requerimientos de Seguridad
  - Se detallan requerimientos de seguridad
  - Se especifican claramente
    - Entradas
    - Salidas
    - Cursos básicos de acción
    - Caminos de extensión y excepción
  - Es importante identificar y mantener los requerimientos de seguridad

Puntos de Contacto en Seguridad

- 7. Operaciones de Seguridad
  - Elementos de seguridad que enmarcan la ejecución del software
  - Seguridad de la red

Puntos de Contacto en Seguridad

- El objetivo de los puntos de contacto es desarrollar el software de manera segura
- Adicionalmente, encontrar y prevenir defectos de seguridad durante todo el ciclo de desarrollo de software
  - Se utilizan métodos estáticos y dinámicos de verificación y validación

Puntos de Contacto en Seguridad

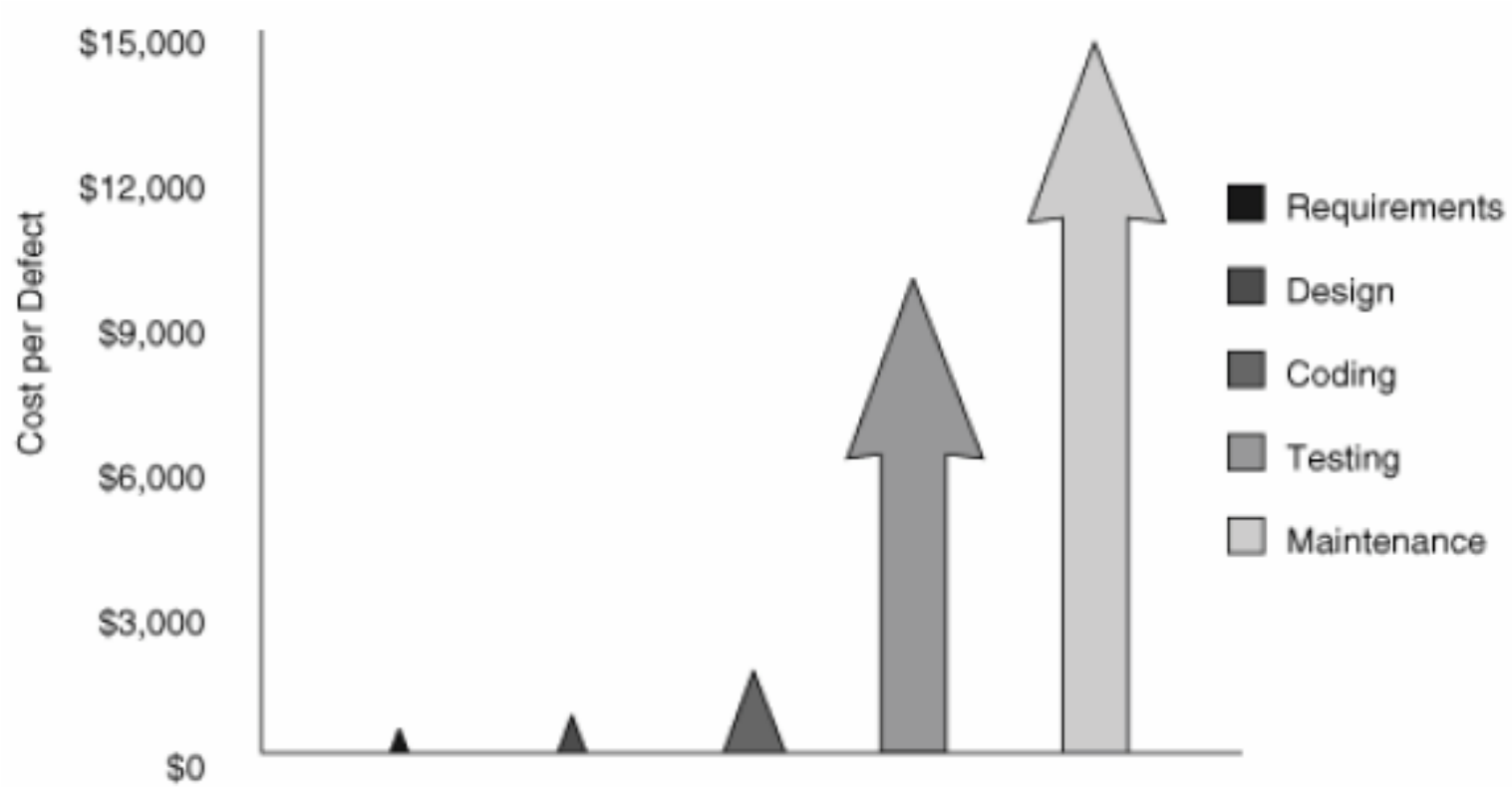


Imagen tomada de "Sotware Security:Building Security In" Gary McGraw

Casos de Abuso

- La seguridad es una propiedad del software no una característica
- Cuando actuamos como diseñadores de un sistema tenemos una ventaja sobre los atacantes … conocemos mejor el software
- Este conocimiento es utilizado para mejorar la seguridad

Casos de Abuso

- Cómo diseñadores de nuestro sistema debemos preguntarnos
  - Cuáles suposiciones están implícitas en nuestro sistema ?
  - Qué cosas harían estas suposiciones falsas?
  - Qué clases de patrones de ataque usaría un atacante?

Casos de Abuso

- Casos de Abuso
  - Propuestos inicialmente en 1999 (McDermont)
  - Extensión de los casos de uso con casos de mal uso (Opdahl 2000)
  - Uno de los objetivos de los casos de abuso es decidir y documentar cómo debe reaccionar el software ante su uso ilegítimo

Casos de Abuso

- Cómo crear los casos de abuso?
  - Inicialmente responsabilidad de los diseñadores y los analistas de seguridad
  - Toman como entrada
    - Conjunto de Casos de Uso
    - Lista de patrones de ataque
  - El primer paso es identificar y documentar actores o agentes que podrían ejecutar un ataque
  - El segundo paso es crear anti-requerimientos
  - El tercer paso es crear un modelo de ataque

Casos de Abuso

- Anti-requerimientos
  - Creados por los analistas de seguridad
  - Se analizan los casos de uso contra la lista de potenciales atacantes
  - Se documentan los ataques que causarian que el requerimiento fallara
  - Anti-requerimientos ayudan a entender como una amaneza puede abusar del sistema
  - Usualmente ligados a la ausencia o falla de una función de seguridad

Casos de Abuso

- Crear un modelo de ataque
  - Dada una lista de casos de uso y una lista de amenazas se hace una comparación contra una lista de ataques
  - Se pueden utilizar patrones de ataque / STRIDE
  - Seleccione patrones de ataque relevantes para el sistema
  - Construya casos de abuso que describan como su sistema reacciona a un ataque

Casos de Abuso

- STRIDE
  - Spoofing
    - Pretender ser otra persona
  - Tampering
    - Modificar datos o código
  - Repudiation
    - Negar una acción
  - Information Disclosure
    - Exponer información a alguien no autorizado
  - Deniel of Service
    - Denegar o degradar el servicio a los usuarios
  - Elevation of Privilege
    - Ganar privilegios sin autorización

Casos de Abuso

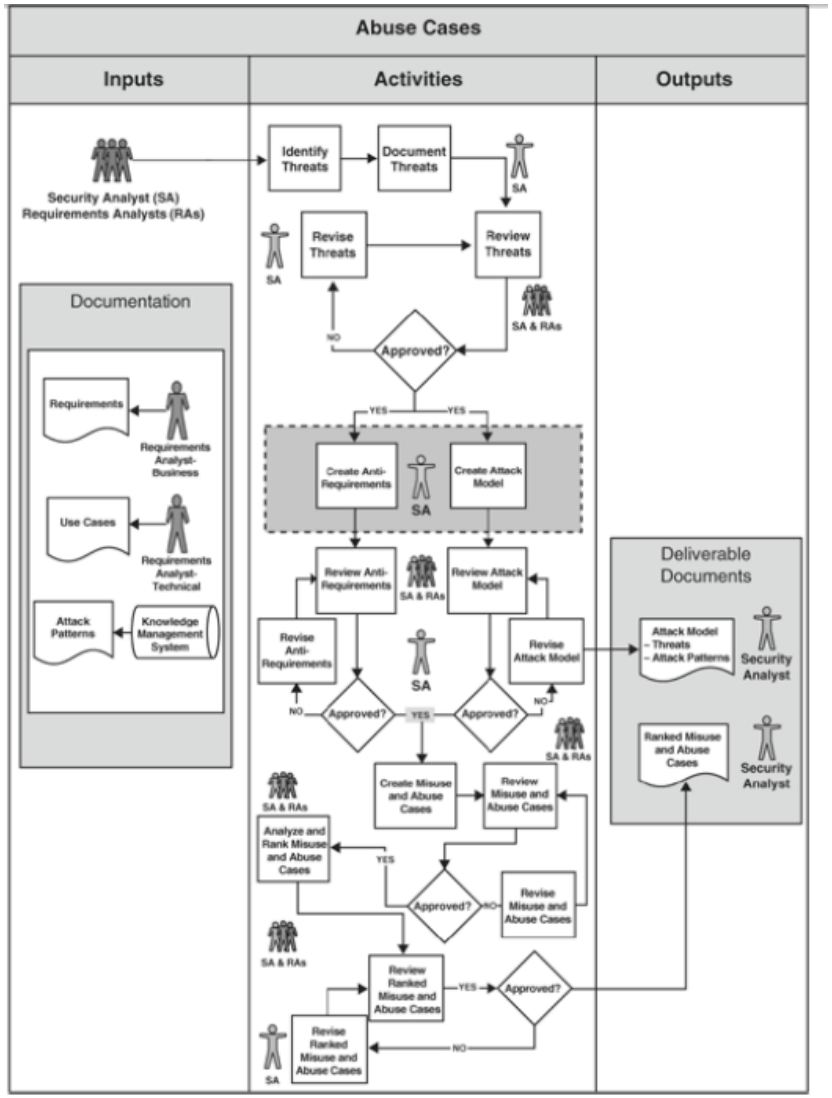


Imagen tomada de "Sotware Security:Building Security In" Gary McGraw

ISO/IEC 15408-2:2005

- Provee un conjunto común de requerimientos de seguridad de IT
- Procedimiento de evaluación para establecer un nivel de confianza
- Sirve como guía para el desarrollo de sistemas de software
- El sistema bajo evaluación se denomina ***Target of Evaluation (TOE)***

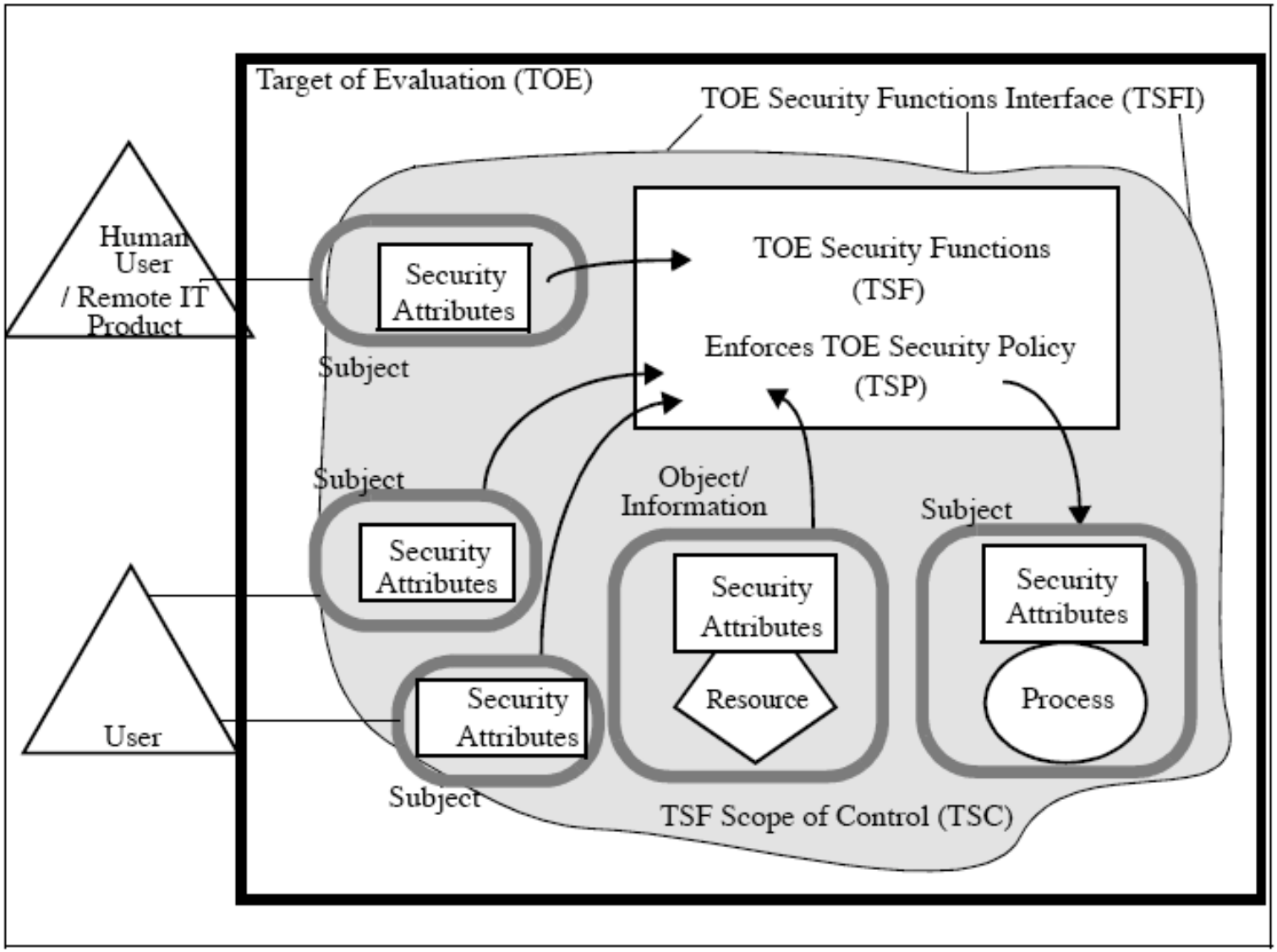
ISO/IEC 15408-2:2005

- Direccionado a definir requerimientos para la protección de información en sistemas de software
  - Confidencialidad
  - Integridad
  - Disponibilidad

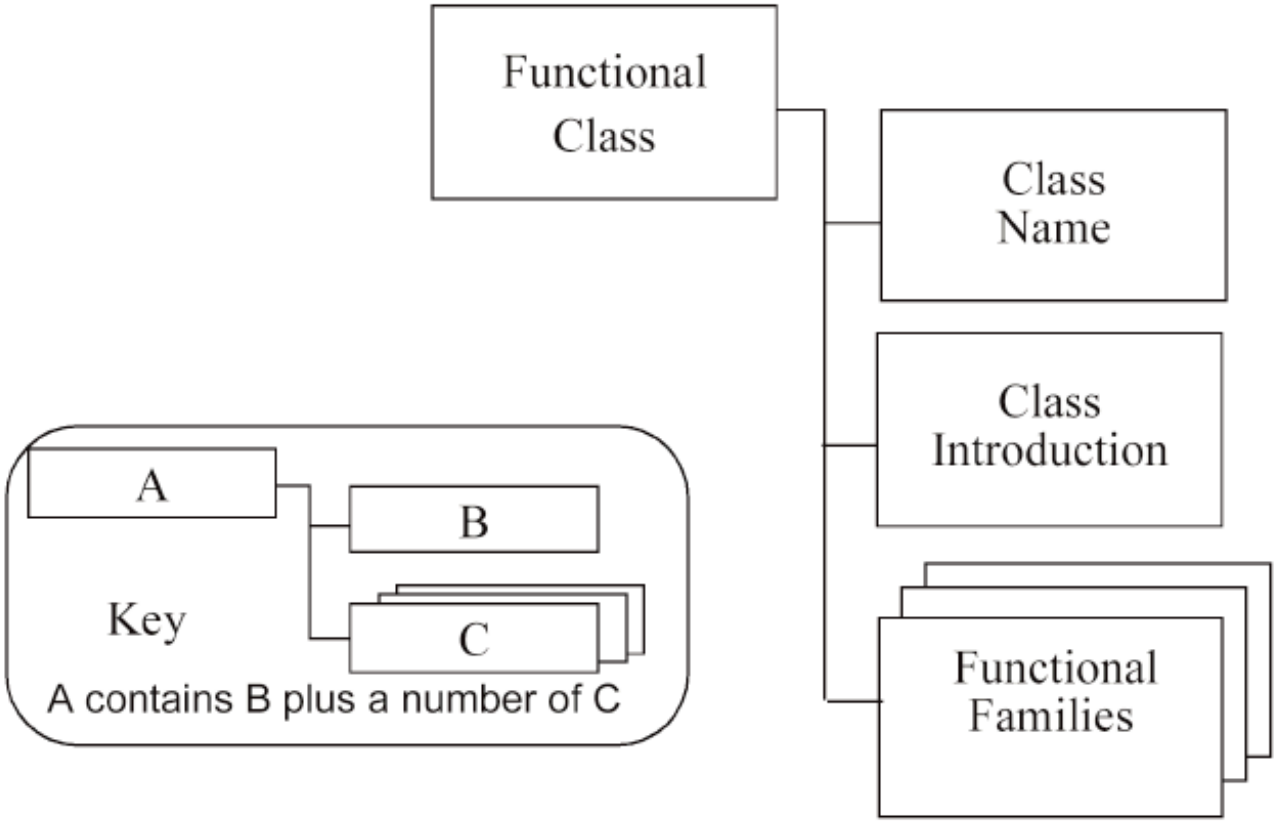
ISO/IEC 15408-2:2005

- Parte 2 – Requerimientos Funcionales de Seguridad
  - Establece un conjunto de componentes funcionales para expresar requerimientos de seguridad en un TOE
    - Componentes
    - Familias
    - Clases
  - Se utiliza como guía y referencia para la formulación de requerimientos de seguridad

ISO/IEC 15408-2:2005

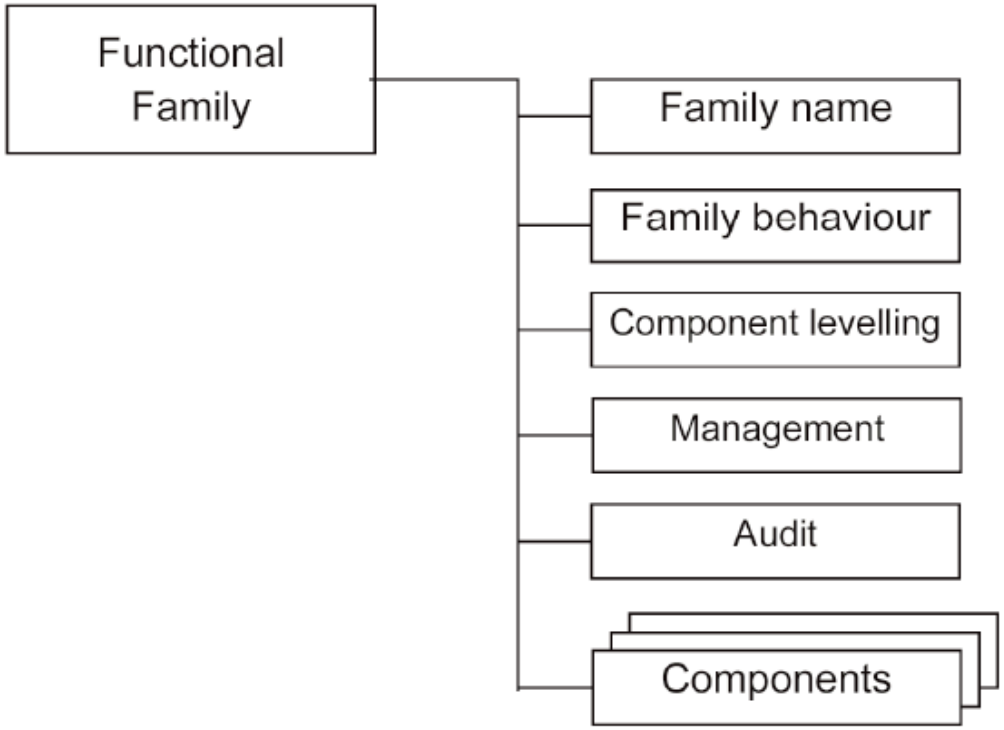


ISO/IEC 15408-2:2005



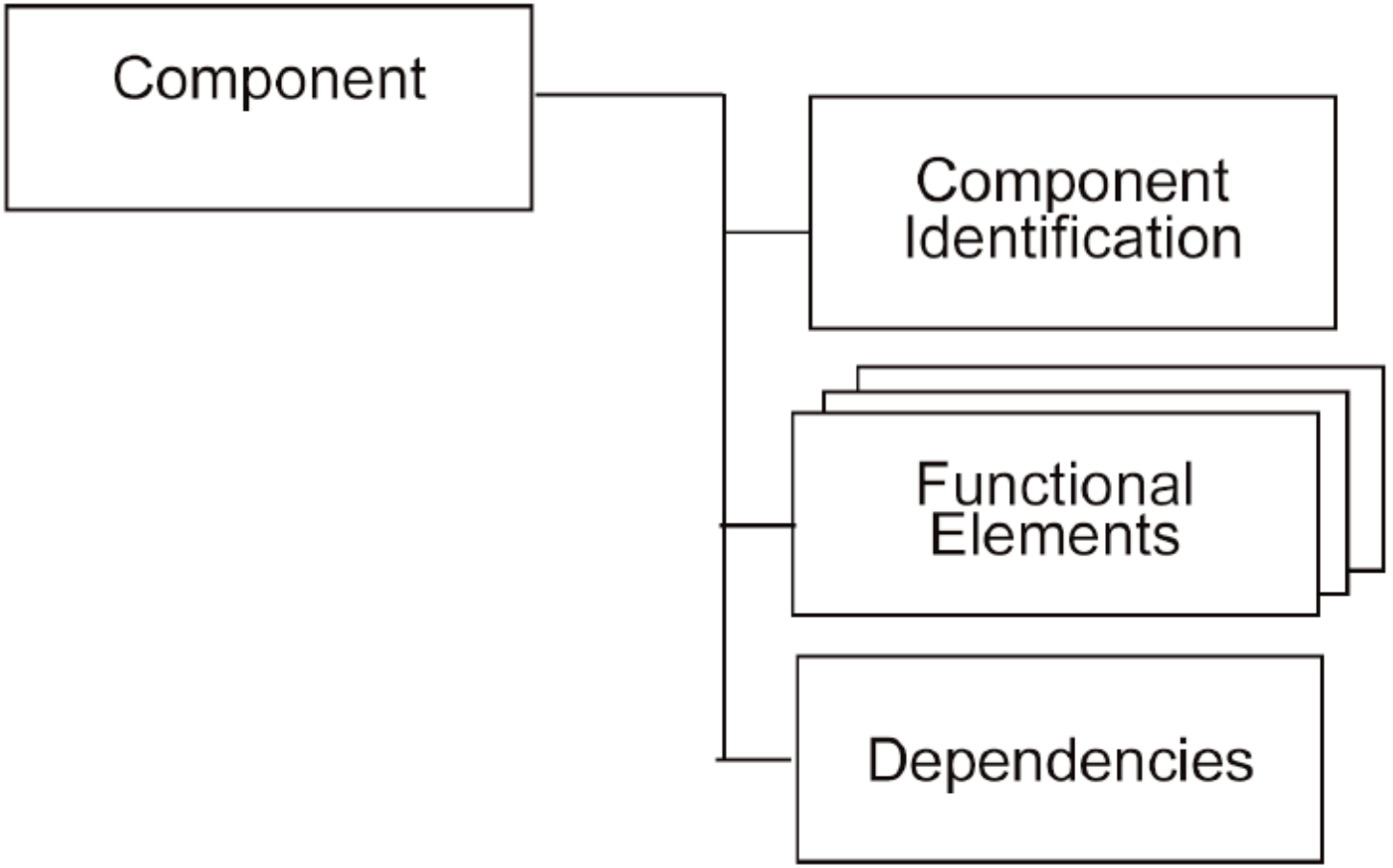
Tomado de : ISO/IEC 15408-1:2005

ISO/IEC 15408-2:2005



Tomado de : ISO/IEC 15408-1:2005

ISO/IEC 15408-2:2005



Tomado de : ISO/IEC 15408-1:2005

ISO/IEC 15408-2:2005

Clase FAU : Auditoria de Seguridad

- Esta familia define requerimientos para analizar de forma **automática** actividades del sistema y auditar datos para encontrar **posibles o reales** violaciones de seguridad
- Ejemplo

"The TSF shall be able to **maintain profiles of system usage, where an individual profile represents the historical patterns of usage performed by the member(s) of [assignment: *the profile target group].*"** ***[11]***

ISO/IEC 15408-2:2005

- FAU_ARP: Respuesta automática de auditoría de seguridad
  - 1. Alarmas de seguridad
- FAU_GEN: Generación de datos de auditoría de seguridad
  - 1. Define el nivel de los datos auditables
  - 2. Asociación de identidad del usuario
- FAU_SAA: Análisis de auditoría de seguridad
  - 1. Análisis de violación potencial
  - 2. Detección de anomalias con base en el perfil de usuarios meta
  - 3. Heurística de un ataque simple
  - 4. Heurística de un ataque complejo

ISO/IEC 15408-2:2005

- FAU_SAR: Revisión de la auditoría de seguridad
  - 1. Revisión de auditoría
  - 2. Revisión de auditoría restringida
  - 3. Revisión de auditoría seleccionable
- FAU_SEL: Selección de eventos de la auditoría de seguridad
  - 1. Auditoría selectiva
- FAU_STG: Almacenamiento de eventos de auditoría de seguridad
  - 1. Almacenamiento de indicios de auditoría
  - 2. Garantía de la disponibilidad de datos de auditoría
  - 3. Acción en caso de pérdida de datos de auditoría
  - 4. Prevención de pérdida de datos de auditoría

ISO/IEC 15408-2:2005

- **Clase FCO : Comunicación**
  - Provee dos familias para asegurar la identidad de un participante en un intercambio de datos
    - Non-repudiation of Origin
    - Non-repudiation of receipt
  - Ejemplo

"The TSF shall be able to generate evidence of receipt for received [assignment: *list of information types] at the request of the [selection: originator, recipient, [assignment: list of third parties]]."* [11]

ISO/IEC 15408-2:2005

- FCO_NRO: No repudio de origen
  - 1. Prueba de origen selectiva
  - 2. Prueba de origen obligatoria
- FCO_NRR: No repudio de recepción
  - 1. Prueba de recepción selectiva
  - 2. Prueba de selección obligatoria

ISO/IEC 15408-2:2005

- **Clase FCS : Soporte Criptográfico**
  - Soporte del ciclo de vida de las llaves criptográficas
    - Generación
    - Distribución
    - Acceso
    - Destrucción
  - Ejemplo

"The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *cryptographic key generation algorithm] and specified* cryptographic key sizes [assignment: *cryptographic key sizes] that meet the following: [assignment: list of standards].*" [11]

ISO/IEC 15408-2:2005

- FCS_CKM: Gestión de claves criptográficas
  - 1. Generación de claves criptográficas
  - 2. Distribución de claves criptográficas
  - 3. Acceso a las claves criptográficas
  - 4. Destrucción de las claves criptográficas
- FCS_COP: Operación criptográfica
  - 1. Una operación criptográfica se debe llevar a cabo de acuerdo a un algorítmo especificado

ISO/IEC 15408-2:2005

- **Clase FDP : Protección de los Datos de Usuario**
  - Esta familia especifica requerimientos para protección de datos
    - Control de Acceso
    - Autenticación de los Datos
    - Exportar fuera del control del TSF
    - Importar al TSF
    - Flujo de Información
    - Integridad de los datos almacenados
    - Transferencia segura de datos
  - Ejemplo

"The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received." [11]

ISO/IEC 15408-2:2005

- **FDP_ACC**: Política de control de acceso
- **FDP_ACF**: Funciones de control de acceso
- **FDP_DAU**: Autenticación de datos
- **FDP_ETC**: Exportación hacia fuera del control dela TSF
- **FDP_IFC**: Política de control de flujo de información
- **FDP_IFF**: Funciones de control de flujo de información
- **FDP_ITC**: Importación desde fuera del control de las TSF
- **FDP_ITT**: Transferencia interna en el TOE
- **FDP_RIP**: Protección de la información residual
- **FDP_ROL**: Rollback
- **FDP_SDI**: Integridad de los datos almacenados
- **FDP_UCT**: Protección de la confidencialidad de la transferencia de datos de usuario inter-TSF
- **FDP_UIT**: Protección de la integridad de la transferencia de datos de usuario inter-TSF

ISO/IEC 15408-2:2005

- **Clase FIA :Identificación y Autenticación**
  - Esta familia de requerimientos busca establecer y verificar la supuesta identidad de un usuario
    - Fallas de autenticación
    - Definición de atributos de usuario
    - Especificación de secretos
    - Autenticación de usuarios
    - Identificación de usuarios
  - Ejemplo

"The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received." [11]

ISO/IEC 15408-2:2005

- FIA_AFL: Fallas de autenticación
- FIA_ATD: Definición de atributos de usuario
- FIA_SOS: Especificación de secretos
- FIA_UAU: Autenticación de usuarios
- FIA_UID: Identificación de usuarios
- FIA_USB: Vínculo usuario-sujeto

- **Clase FMT : Manejo de la Seguridad**
  - Esta clase especifica el manejo de atributos de seguridad, datos y funciones
    - Manejo de atributos de seguridad
    - Revocación
    - Expiración
    - Roles
  - Ejemplo

"The TSF shall enforce the [assignment: *access control SFP, information flow control SFP] to restrict* the ability to [selection: *change_default, query, modify, delete,[assignment: other operations]] the* security attributes [assignment: *list of security attributes] to [assignment: the authorised identified roles].”* [11]

ISO/IEC 15408-2:2005

- FMT_MOF : Gestión de funciones en las TSF
- FMT_MSA: Gestión de atributos de seguridad
- FMT_MTB: Gestión de los datos de las TSF
- FMT_REV: Revocación
- FMT_SAE: Expiración de atributos de seguridad
- FMT_SMF: Especificación de funciones de gestión
- FMT_SMR: Roles de gestión de seguridad

ISO/IEC 15408-2:2005

Clase FPR: Privacidad

- Esta clase contiene requerimientos de privacidad para proveer protección al usuario contra descubrimiento y mal uso de su identidad por parte de otros usuarios
  - Anonimato
  - Pseudonimos
- Ejemplo

"The TSF shall ensure that [assignment: *set of users and/or subjects] are unable to determine the real* user name bound to [assignment: *list of subjects and/or operations and/or objects].*" [11]

ISO/IEC 15408-2:2005

- FPR_ANO: Anonimato
- FPR_PSE: Seudoanonimato
- FPR_UNL: Incapacidad para vincular
- FPR_UNO: Incapacidad para observar

ISO/IEC 15408-2:2005

- **Clase FRU: Utilización de Recursos**
  - Esta clase provee soporte a la disponibilidad de recursos requeridos (procesamiento/almacenamiento)
    - Tolerancia a Fallas
    - Prioridad del Servicio
    - Adjudicación de Recursos
  - Ejemplo

"The TSF shall ensure the operation of [assignment: *list of TOE capabilities] when the following* failures occur: [assignment: *list of type of failures].*" [11]

ISO/IEC 15408-2:2005

- FRU_FLT: Tolerancia ante fallas
  - 1. Tolerancia degrada ante fallas, exige que el TOE continúe la operación ante fallas identificadas
- FRU_PRS: Prioridad del servicio
- FRU_RSA: Asignación de recursos

ISO/IEC 15408-2:2005

Clase FTA: Acceso al TOE

- Esta familia especifica los requerimientos para controlar una sesión establecida con un usuario
  - Limitación de sesiones concurrentes
  - Sesiones con bloqueo
  - Historia de acceso
  - Establecimiento de una sesión
- Ejemplo

"The TSF shall require the following events to occur prior to unlocking the session: [assignment: *events to occur].*" [11]

ISO/IEC 15408-2:2005

- FTA_LSA: Limitación del alcance de los atributos seleccionados
- FTA_MCS: Limitación de sesiones simultáneas múltiples
- FTA_SSL: Bloqueo de sesión
- FTA_TAB: Mensaje de acceso del TOE
- FTA_TAH: Historia de acceso del TOE
- FTA_TSE: Establecimiento de sesión de TOE

ISO/IEC 15408-2:2005

- **Clase FTP: Canales/Caminos Confiables**
  - Esta clase provee requerimientos de canales de comunicaciones seguros entre el usuario y el TSF o entre el TSF y otros sistemas
    - Canales Seguros
    - Caminos Seguros
  - Ejemplo

"The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure." [11]

ISO/IEC 15408-2:2005

- FTP_ITC: Canal confiable inter TSF
- FTP_TRP: Ruta confiable

SQUARE

- **Security Quality Requirements Engineering (SQUARE)**
  - Desarrollado en Carnegie-Mellon University
  - Su objetivo es descubrir, categorizar y priorizar requerimientos de seguridad
  - Compuesto por 9 pasos
  - Se utilizan diferentes técnicas para descubrir y clasificar los requerimientos

SQUARE

- SQUARE
  - Paso 1. Unificar conceptos
  - Paso 2. Identificar objetivos de seguridad
  - Paso 3. Desarrollar artefactos para soportar las técnicas de descubrimiento
  - Paso 4. Realizar evaluación de riesgos
  - Paso 5. Seleccionar técnicas de descubrimiento
  - Paso 6. Descubrir requerimientos de seguridad
  - Paso 7. Categorizar requerimientos
  - Paso 8. Priorizar requerimientos
  - Paso 9. Inspeccionar Requerimientos

SQUARE

- **Paso 1. Unificar Conceptos**
  - Entradas
    - Definiciones tomadas de IEEE, Ontologías de Dominio, SWEBOK, ISO 15408, etc.
  - Técnicas
    - Entrevistas, Grupos Objetivos
  - Participantes
    - Analistas de Requerimientos, Usuarios
  - Salidas
    - Documento de Definiciones

SQUARE

Paso 1. Unificar Conceptos

- El objetivo es tener una definición común de los términos involucrados en la aplicación a desarrollar
- Alinear términos del Dominio
- Lenguajes de Dominio Específico
- Modelos de Dominio Específico
- MIT Process Handbook
- APQC Process Classification Framework

SQUARE

- **Paso 2. Identificar Objetivos de Seguridad**
  - Entradas
    - Definiciones, Motivadores de Negocio, Políticas y procedimientos
  - Técnicas
    - Entrevistas, Encuestas
  - Participantes
    - Analistas de requerimientos, Usuarios
  - Salidas
    - Objetivos

SQUARE

- **Paso 2. Identificar Objetivos de Seguridad**
  - Es posible que diferentes usuarios de la organización (stakeholders) tengan diferentes objetivos de seguridad en mente
    - Director de recursos humanos
    - Director de tecnología
    - Director Financiero

SQUARE

- **Paso 3. Desarrollar artefactos para soportar la definición de requerimientos de seguridad**
  - Entradas
    - **Casos de Abuso**
  - Técnicas
    - Sesiones de Trabajo
  - Participantes
    - Ingenieros de Requerimientos
  - Salidas
    - Artefactos requeridos, casos de abuso

SQUARE

- **Paso 3. Desarrollar artefactos para soportar la definición de requerimientos de seguridad**
  - Se elaboran los formatos necesarios para guardar y evaluar toda la información requerida
    - Casos de abuso
    - Requerimientos
    - Tablas de evaluación

SQUARE

- **Paso 4. Realizar Evaluación de Riesgos**
  - Entradas
    - Casos de Abuso, Escenarios, Objetivos de Seguridad
  - Técnicas
    - Modelaje de Riesgos
  - Participantes
    - Ingenieros de Requerimientos, Expertos en Seguridad, Usuarios
  - Salidas
    - Resultados de la evaluación de riesgos

SQUARE

- **Paso 4. Realizar Evaluación de Riesgos**
  - Participan expertos en riesgos con amplio conocimiento en la organización
  - Se utilizan mecanismos de evaluación
    - Matrices de Riesgos
    - Escenarios de Calidad
      - Fuente
      - Estimulo
      - Artefactos
      - Ambiente
      - Respuesta
      - Punto de Sensibilidad
      - Riesgo / no-riesgo

SQUARE

- **Paso 5. Seleccionar técnica de descubrimiento**
  - Entradas
    - Técnicas candidatas, objetivos de negocio, conocimiento de la organización, ISO 15408 (Componentes, Familias, Clases)
  - Técnicas
    - Sesiones de Trabajo
  - Participantes
    - Ingenieros de requerimientos
  - Salidas
    - Técnicas seleccionadas

SQUARE

- **Paso 5. Seleccionar técnica de descubrimiento**
  - Util cuando se tienen diferentes tipos de usuarios
  - Evitan problemas de comunicación

SQUARE

- **Paso 6. Descubrimiento de requerimientos de Seguridad**
  - Entradas
    - Artefactos, Resultados de análisis de riesgos, técnicas selecionadas, casos de abuso
  - Técnicas
    - Entrevistas, Encuestas, Listas de chequeo (ISO-15408-2:2005)
  - Participantes
    - Usuarios
  - Salidas
    - Requerimientos de seguridad iniciales

SQUARE

- **Paso 6. Descubrimiento de requerimientos de Seguridad**
  - Se utiliza la o las técnicas seleccionadas para descubrir los requerimientos de seguridad

SQUARE

- **Paso 7. Categorización de Requerimientos**
  - Entradas
    - Requerimientos Iniciales, Arquitectura, ISO15408
  - Técnicas
    - Sesiones de trabajo
  - Participantes
    - Ingenieros de Requerimientos
  - Salidas
    - Requerimientos Categorizados

SQUARE

- **Paso 7. Categorización de Requerimientos**
  - Se busca diferenciar los requerimientos escenciales de los deseables

SQUARE

- **Paso 8. Requerimientos Priorizados**
  - Entradas
    - Requerimientos Categorizados, Resultados de la evaluación de riesgos
  - Técnicas
    - Métodos de priorización: Triage
  - Participantes
    - Usuarios
  - Salidas
    - Requerimientos priorizados

SQUARE

- **Paso 8. Requerimientos Priorizados**
  - Priorización basada en análisis costo/ benficio y viabilidad técnica

SQUARE

- **Paso 9. Inspección de Requerimientos**
  - Entradas
    - Requerimientos Priorizados
  - Técnicas
    - Inspección de métodos: Revisión de Pares
  - Participantes
    - Equipo de Inspección
  - Salidas
    - Requerimientos Inspeccionados

SQUARE

- **Paso 9. Inspección de Requerimientos**
  - Se buscan defectos inyectados en esta fase
  - Apoyo de los Usuarios y expertos en seguridad

Agenda

- Introducción
- ISO/IEC 15408-2:2005
- SQUARE
- **Hoja de Trabajo**

Bibliografía

- [1] Gary McGraw. “Software Security – Building Security In” Addison-Wesley. 2005
- [2] Greg Hoglund, Gary McGraw, “Exploiting Software – How to Break Code” Addison-Wesley, 2004
- [11] ISO/IEC 15408-2:2005