

Tendencias de seguridad en tecnología para aplicaciones

Iván Arce - CTO

Core Security Technologies
Humboldt 1967 2do Piso
Buenos Aires, Argentina
Teléfono: (+54-11) 5556-2673
Email: ivan.arce@coresecurity.com

AGENDA

- **Prólogo, auto-bombo y otras excusas para hablar del tema**
- **Como modelar tecnología & seguridad ?**
- **Aplicación del modelo a 6 tecnologías específicas**
 - » Seguridad a nivel de sistemas operativos y aplicaciones, web 2.0 , verticales;
 - » Tecnología de virtualización
 - » Telefonía IP
 - » Infra-estructura de red.
 - » Dispositivos móviles
 - » SaaS – SOA/WS - Cloud computing
- ***Penetration Testing* y la visión del atacante**
- **Futurología: Desafíos y tendencias**

Presentación

- **CTO y co-fundador de Core Security Technologies**
<http://www.coresecurity.com>
 - Empresa de software y servicios de seguridad informática fundada en Argentina en 1996
- **ex-Director del equipo de consultoría: CORE Security Consulting Services (SCS)**
<http://www.coresecurity.com/content/services-overview-core-security-consulting-services>
 - Focalizado en servicios de Penetration Testing y auditoría de seguridad de software
- **Lidero la creación del equipo de CORE IMPACT**
<http://www.coresecurity.com/content/core-impact-overview>
 - El primer software comercial de penetration testing a nivel mundial
 - Lanzamiento de v1.0 en Abril del 2002
 - Lanzamiento de v8.0 en Dic. 2008
 - Más de 800 clientes en 40+ países alrededor del mundo.
- **Editor asociado de IEEE Security & Privacy magazine**
<http://www.computer.org/portal/security>
 - Co-editor de la sección New Vulnerabilities and Attack Trends (2003-2007)



Cúal es el propósito de esta charla?

LA CONSTRUCCION DE UN LENGUAJE COMUN

- **Presentar un marco de referencia para hablar de:**
 - Tecnologías emergentes
 - Tendencias de la industria y mercado
 - Tendencias y visibilidad de ataques
 - Estrategias para manejar riesgo y priorizar inversión en seguridad

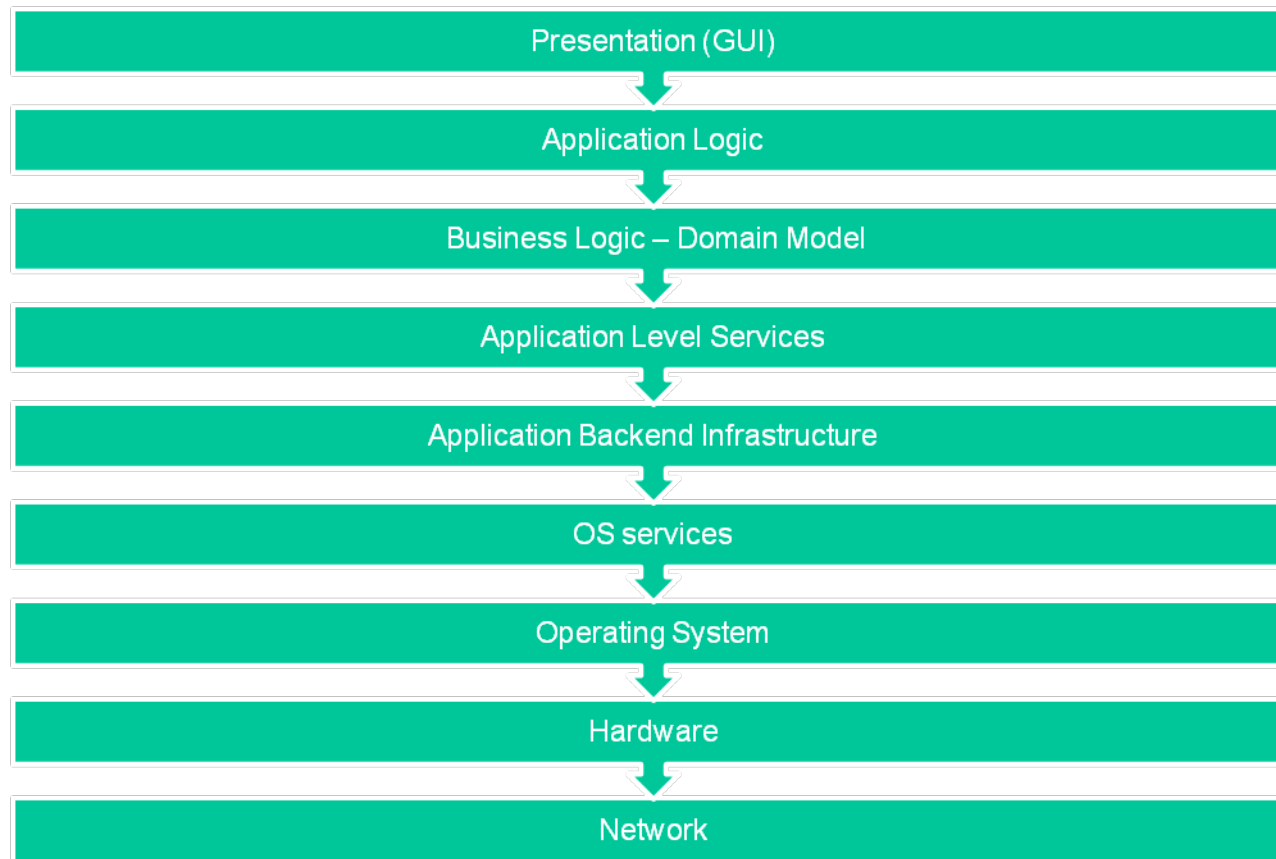
- **Describir nuestras experiencias abordando el problema desde el punto de vista del atacante**

- **Describir algunos desafíos técnicos y científicos venideros**

COMO MODELAR LA SEGURIDAD DE LA TECNOLOGIA PARA APLICACIONES?

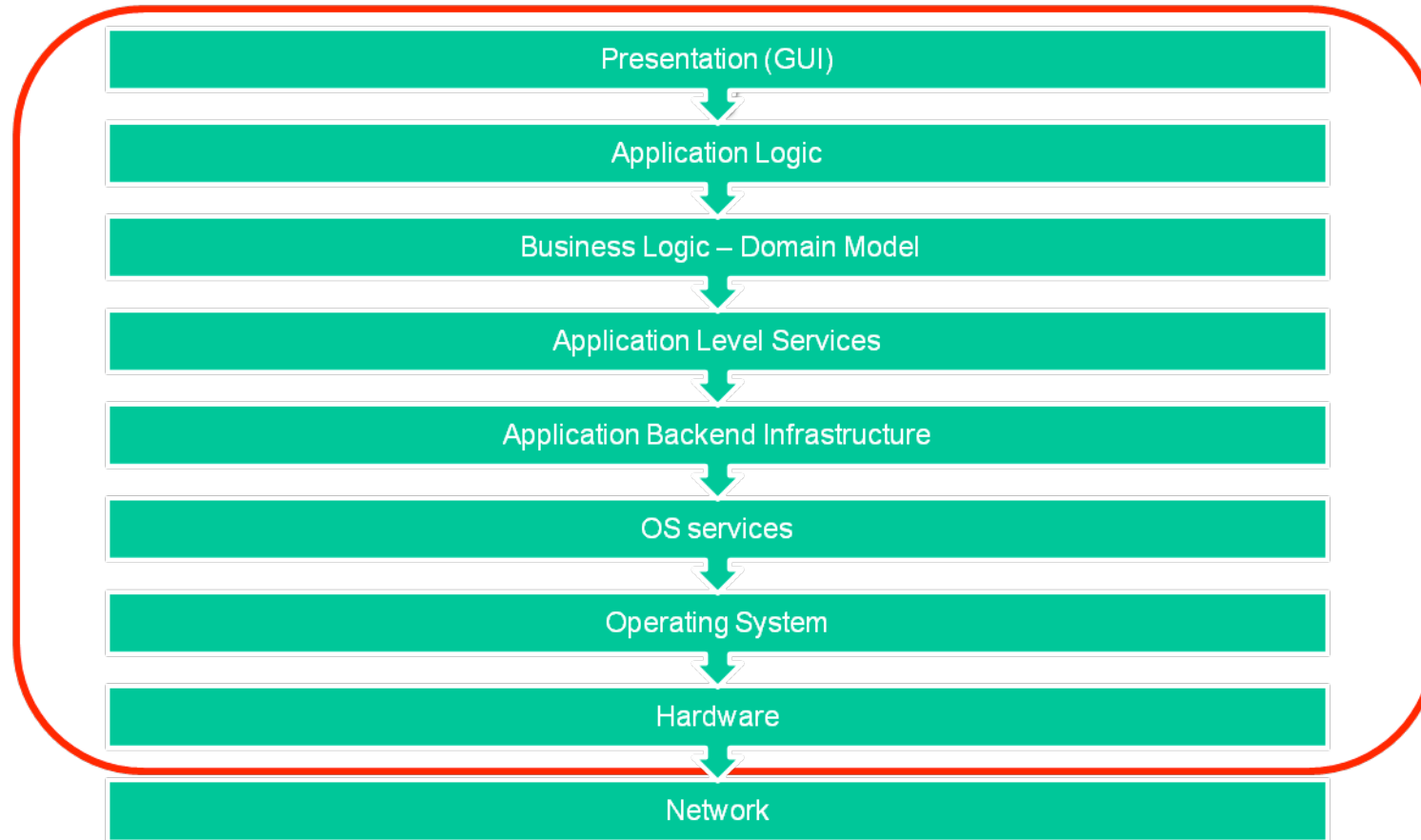
Modelo pseudo-OSI amigable para la gente de negocios

Visión de tecnología en capas



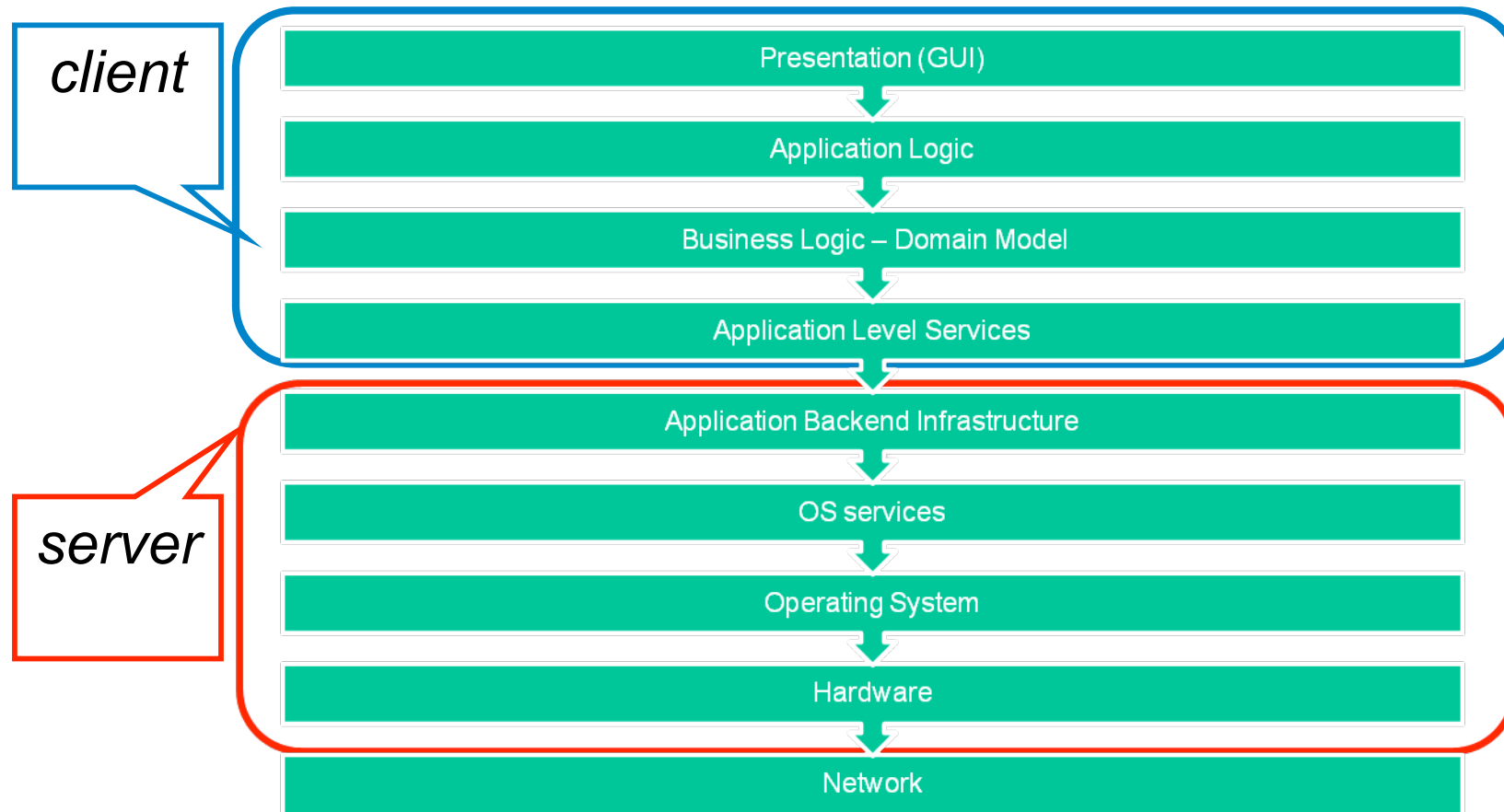
1960-1980: El paradigma Mainframe

El stack completo vive dentro de la maquina



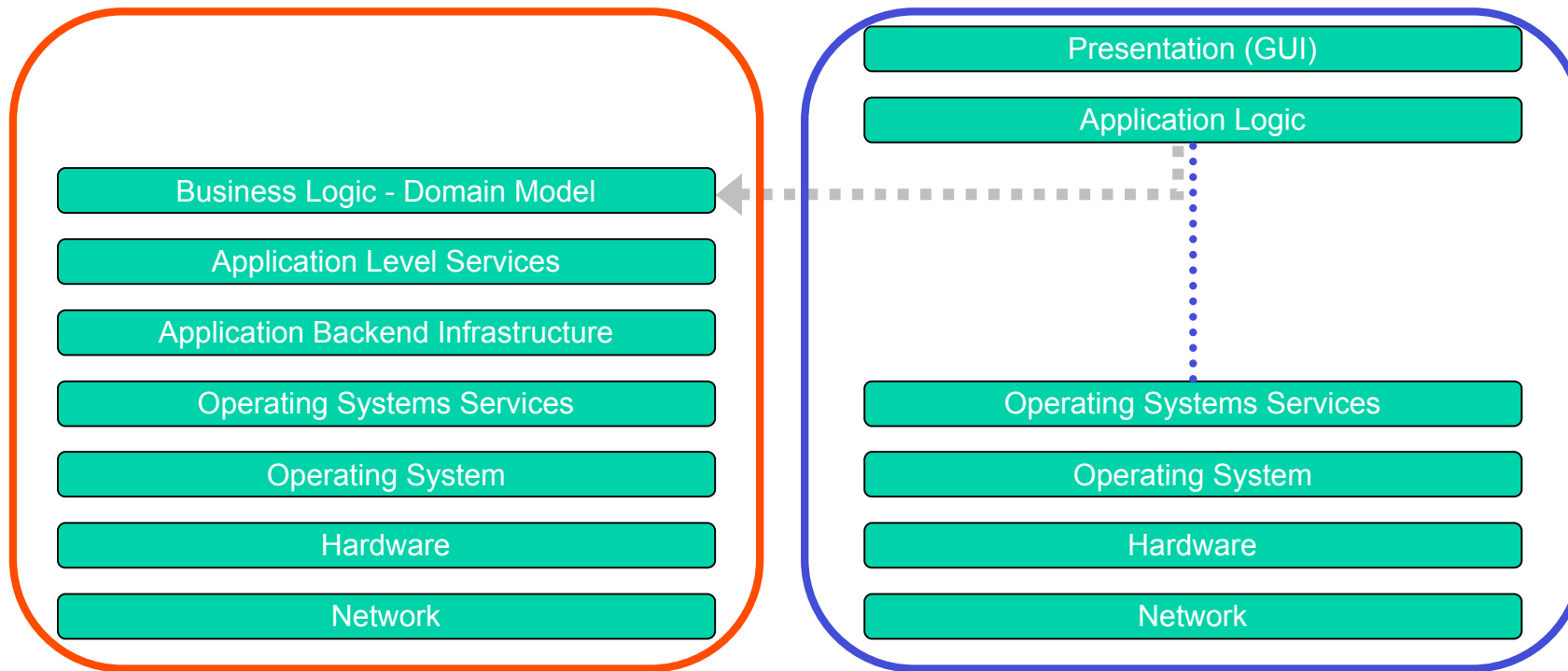
1980-1995: El paradigma Cliente-Servidor

Separemos las aplicaciones entre dos (o más) actores



1980-1995: Arquitectura cliente-servidor con 2 *tiers*

..... **Esta es la arquitectura más común para la mayoría de empresas**

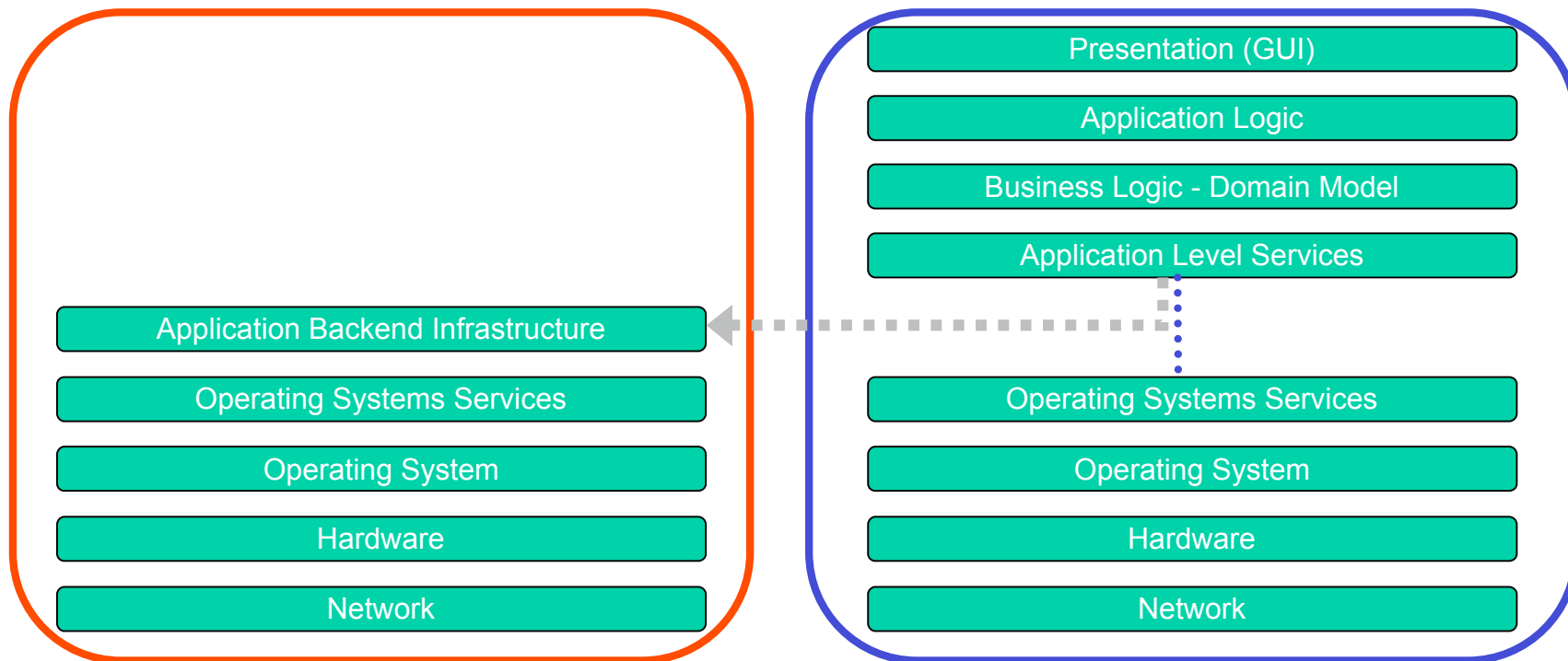


Servidores centralizan la lógica de negocios y el acceso a recursos críticos de la empresa y proveen servicio a múltiples clientes

Las aplicaciones clientes corriendo en computadoras de escritorio se las arreglan con el usuario. Integración via red TCP/IP (y otras)

1980-1995: 2-tier Cliente/Servidor con cliente gordo (“Fat Client”)

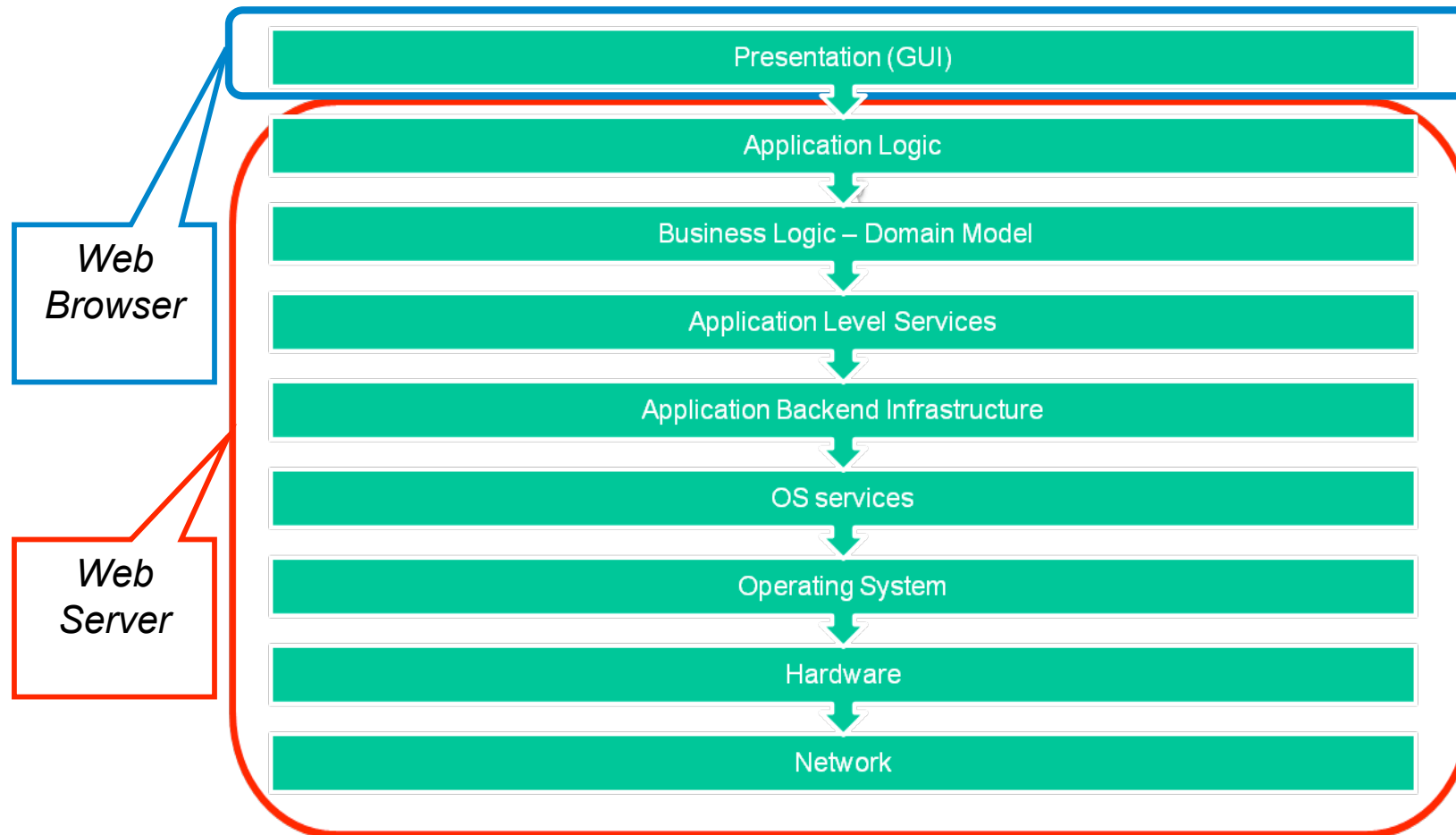
Se corre mucho más código en el cliente



La aplicaciones cliente hace mayor y mejor uso de los recursos de las PCs y reducen la carga de los servers... pero al mismo tiempo transfieren logica de negocios a un ambiente de ejecución que no controlan!

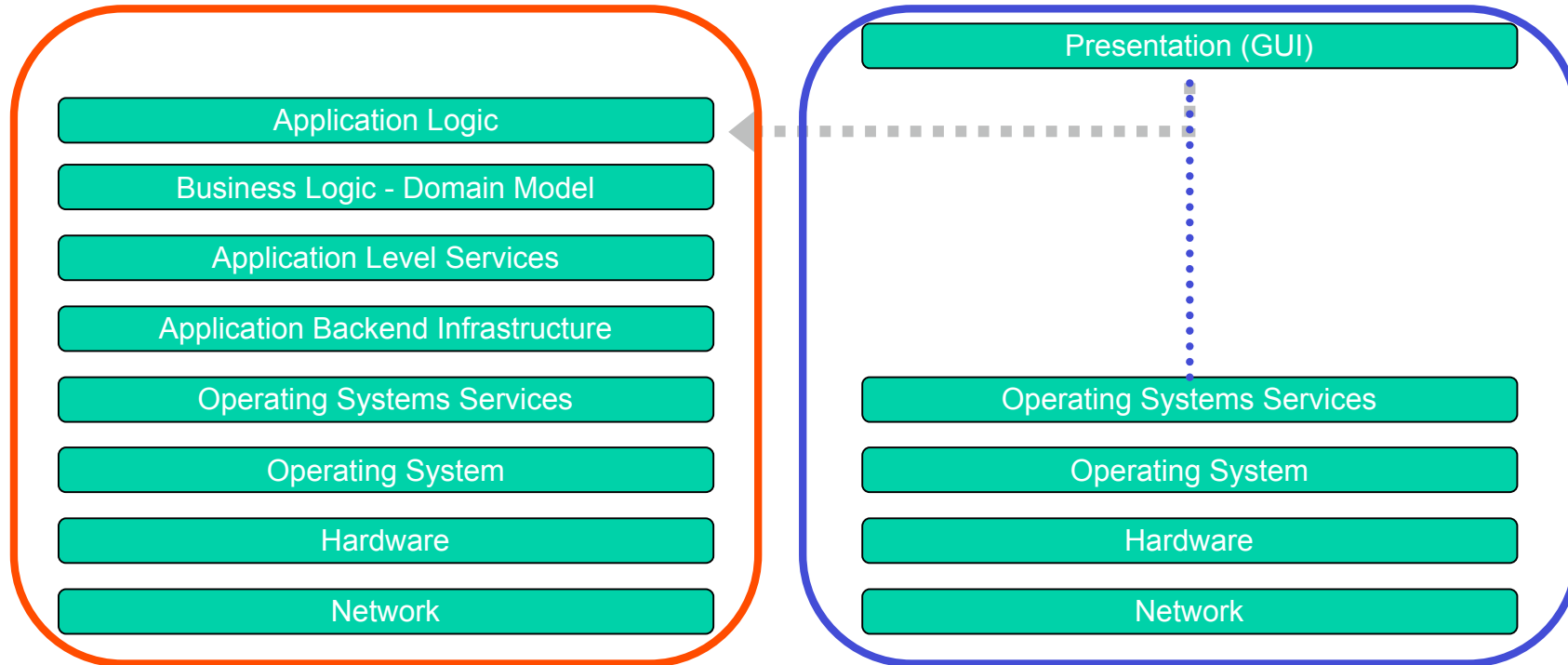
1995-2002: El paradigma Web (1.0)

Alguien se acuerda de “*the network is the computer*” ?



1995-2002: El paradigma Web (1.0)

La segunda forma mas común de tecnología en empresas



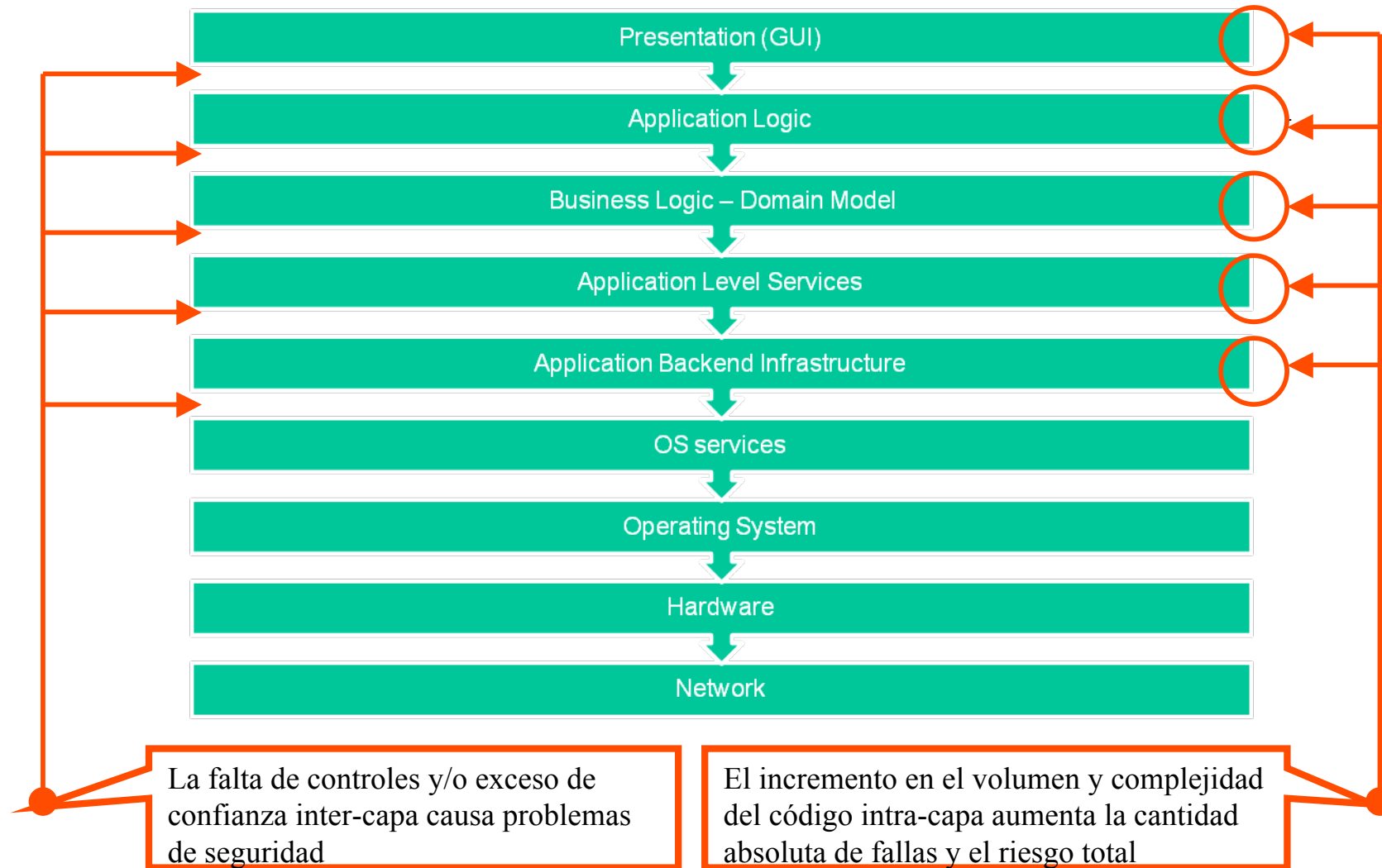
Servidores centralizan la lógica de negocios y el acceso a recursos críticos de la empresa y proveen servicio a multiples clientes

Cualquier web browser sirve de interfaz con los usuarios (GUI).
...Claro que se necesita procesar y presentar el documento HTML.
Integración sobre HTTP en una red TCP/IP

DE QUE TRATA LA SEGURIDAD DE APLICACIONES?

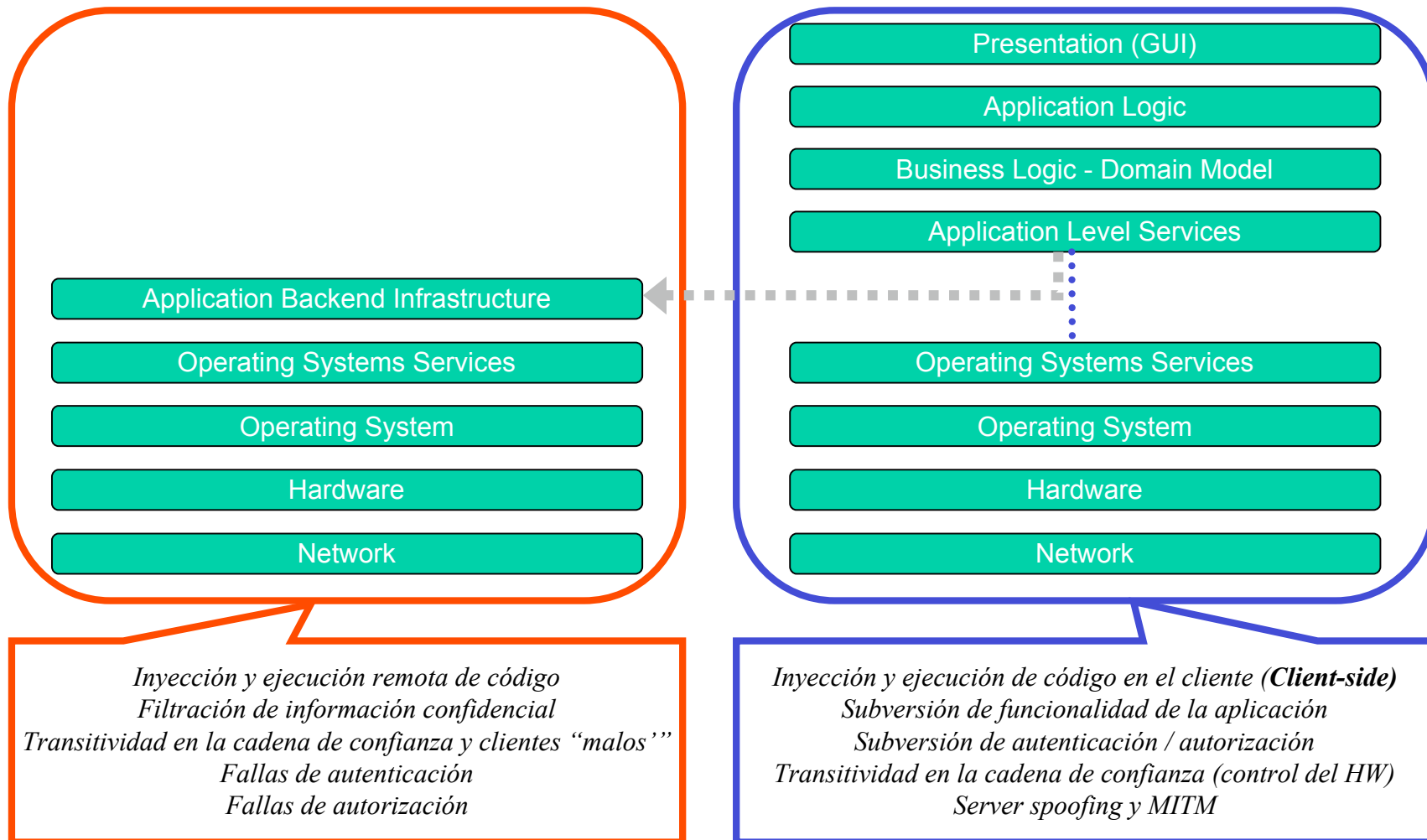
En definitiva , de que se trata la seguridad?

Superficies de ataque y fronteras de confianza



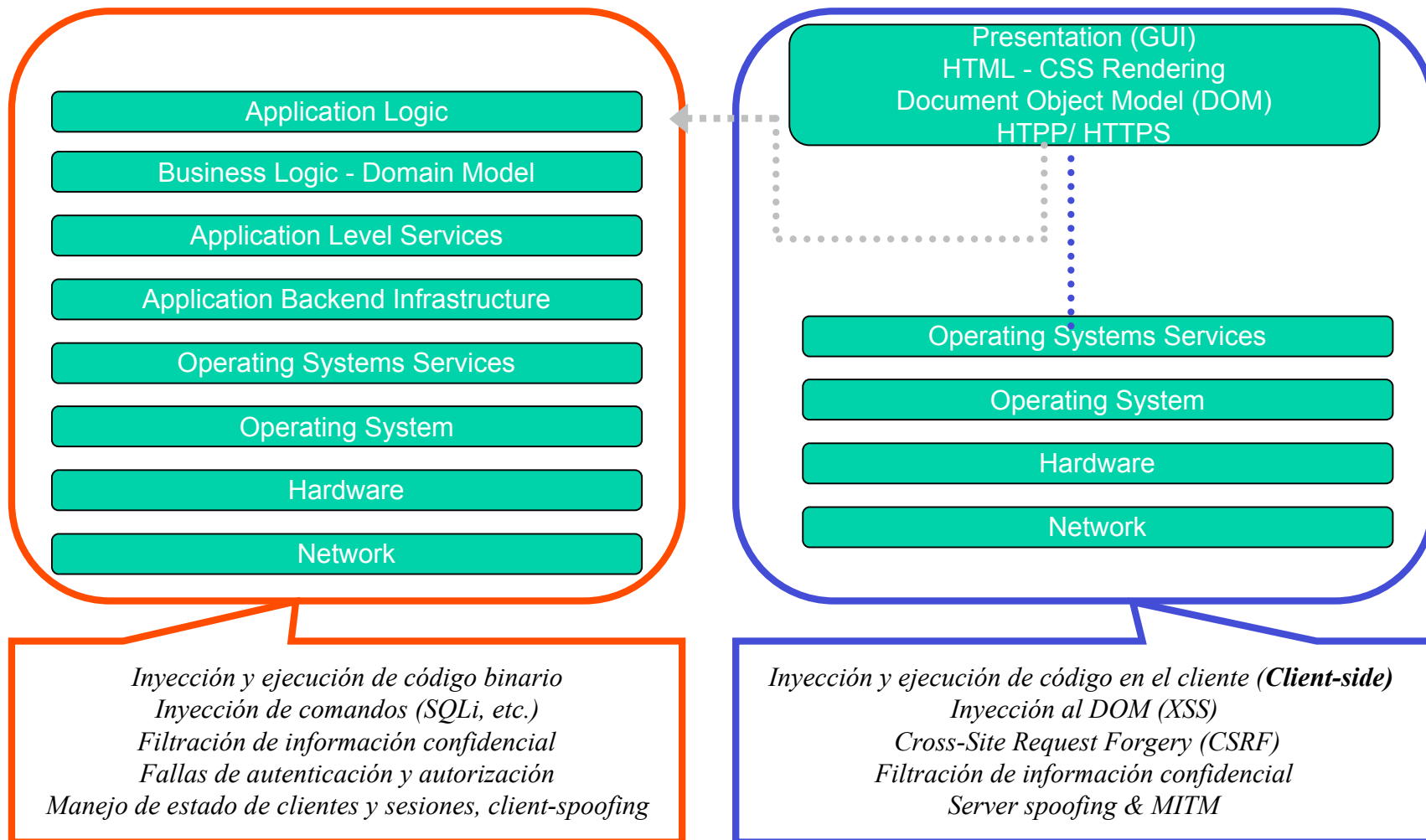
Problemas típicos del modelo Cliente/Servidor

..... Pocos servidores pero muy críticos, muchos clientes con MAYOR criticidad



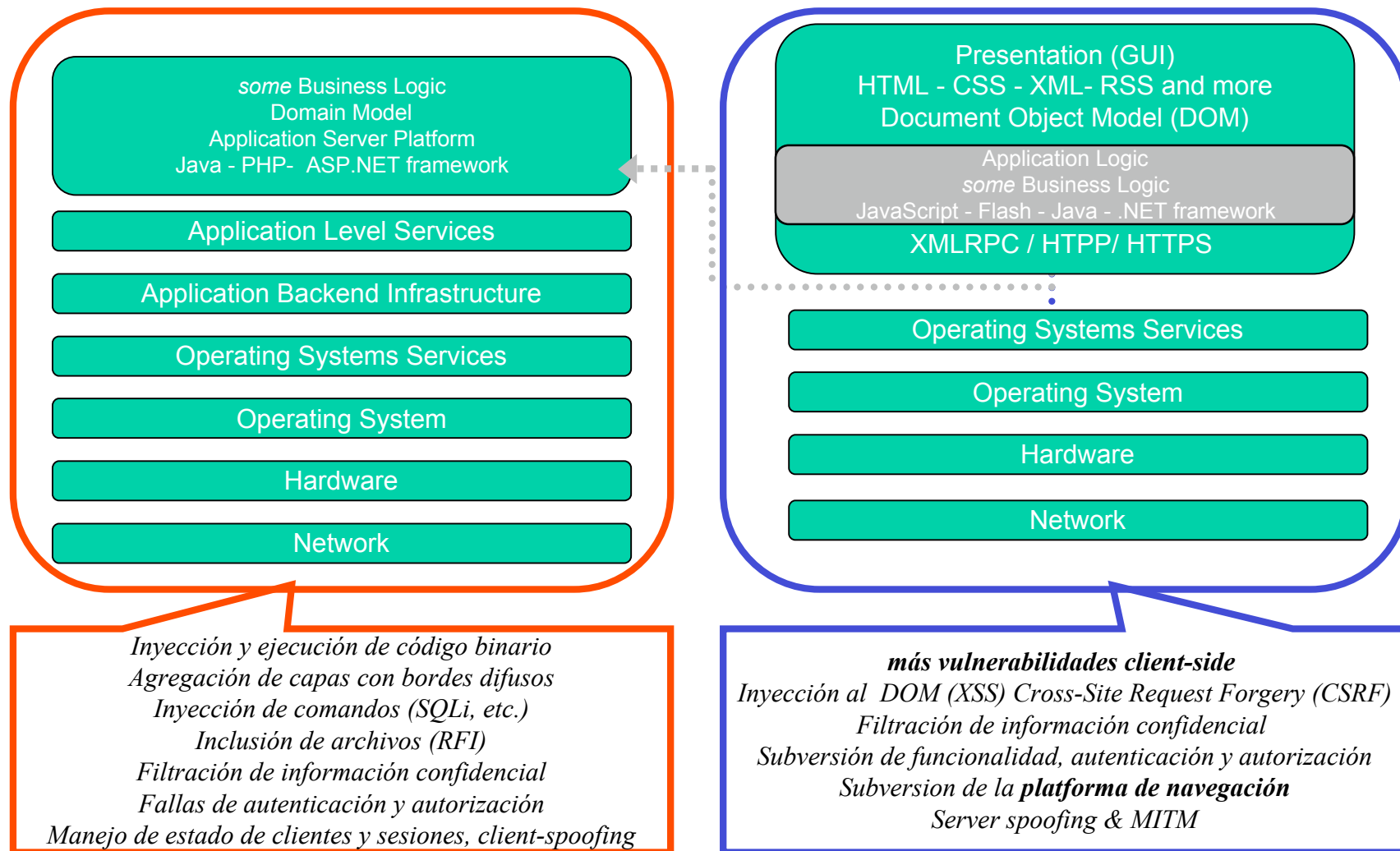
Bueno, y si hacemos que el cliente sea menos “pesado”?
... por ejemplo, si fuera “simplemente” un navegador Web?

El navegador es bastante mas complicado de lo que uno piensa



Que significa “Web 2.0” en este contexto?

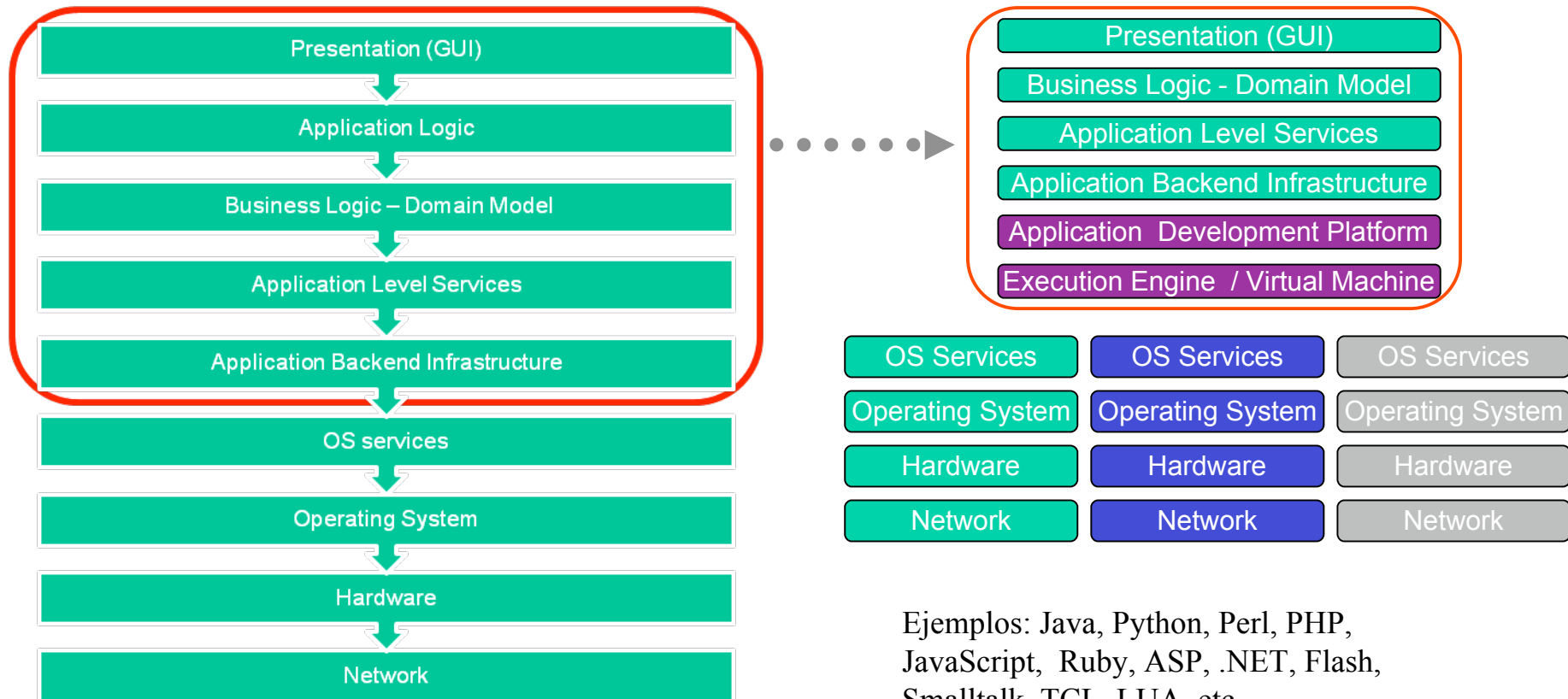
..... El “paradigma” Web 2.0 aumenta la superficie de ataque del browser



TECNOLOGIA DE VIRTUALIZACION

De que esta hablando este tipo?? Virtualización de aplicaciones?

Portabilidad de aplicaciones entre distintos sistemas operativos



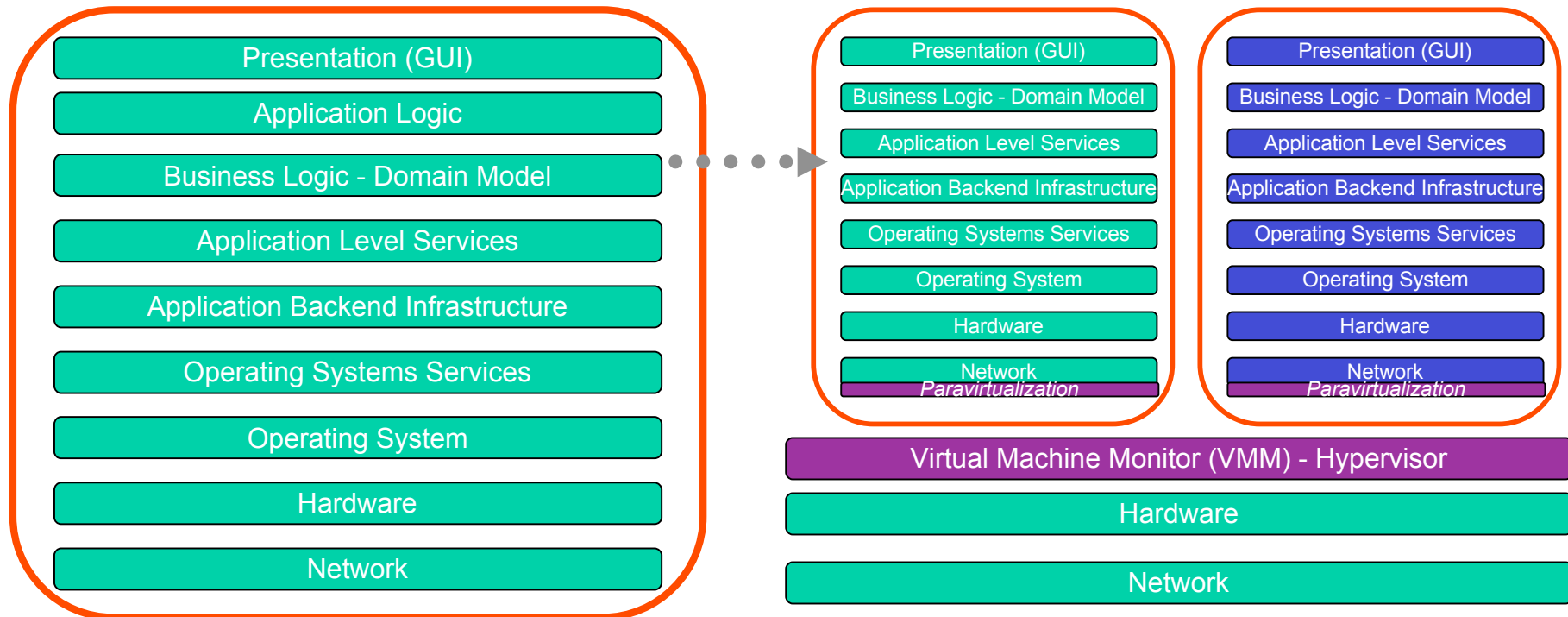
Ejemplos: Java, Python, Perl, PHP,
JavaScript, Ruby, ASP, .NET, Flash,
Smalltalk, TCL, LUA, etc.

Los navegadores tienen maquinas virtuales completas y poderosas y corren sobre sistemas operativos de proposito general o distintos tipos de dispositivos, los mecanismos de seguridad del S.O no tienen visibilidad dentro de la VM, una maquina virtual comprometida permite el control de las aplicaciones que corre independientemente del S.O., escapar de la VM permite controlar el S.O sobre el que corre el browser, “unmanaged code” cruza constantemente la frontera entre ambos, el entorno de ejecución comunicaciones es provisto por el S.O. Se mitigan las vulnerabilidades mas comunes pero aparecen otras.

Bueno, si esa no es papa la papa donde esta?

Virtualizar sistemas enteros! Sirve para bajar costos operativos y salvar al planeta.. Ahh si y para solucionar para siempre “el problema” de seguridad...

..... Multiples sistemas completos compartiendo recursos de HW



Virtualization de sistemas promete aislamiento pero agrega mas código y mayor complejidad. El aislamiento real es teóricamente imposible: canales encubiertos. Aún así, es posible comprometer la VM, escapar de una VM comprometida implica subvertir al VM M (Hypervisor). Subversion del VMM implica el compromiso de todas las otras VMs que maneja. Ataques inter-VM (VM to VM) , propagacion de ataques por persistencia y migración, El uso de tecnología de virtualización disminuye la visibilidad de la infraestructura de seguridad ya existente!

TELEFONIA IP & VOIP

1876-1990: En el esquema tradicional la PSTN era una “caja negra”

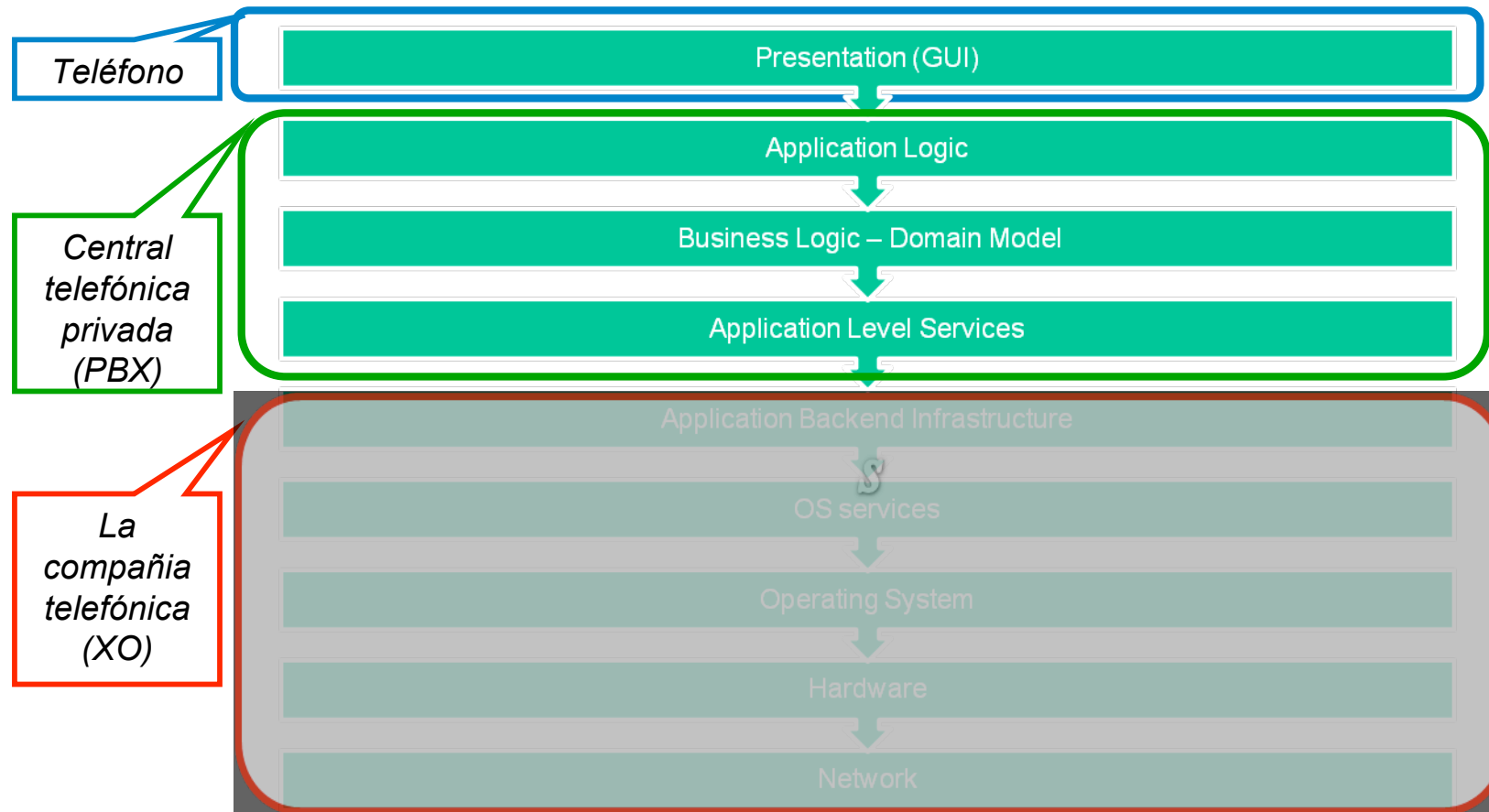
El teléfono es simplemente “la capa de presentación”



Una interfaz *mejorada* le permitió a los usuarios descubrir y manipular la funcionalidad de la PSTN: fraude telefónico, denegación de servicio, control de la red operativa, escuchas, MITM, spoofing, re-dirección, ruteo, etc. Señalización en-banda y cadena de confianza

1970-1990: The Private Branch Exchange (PBX)

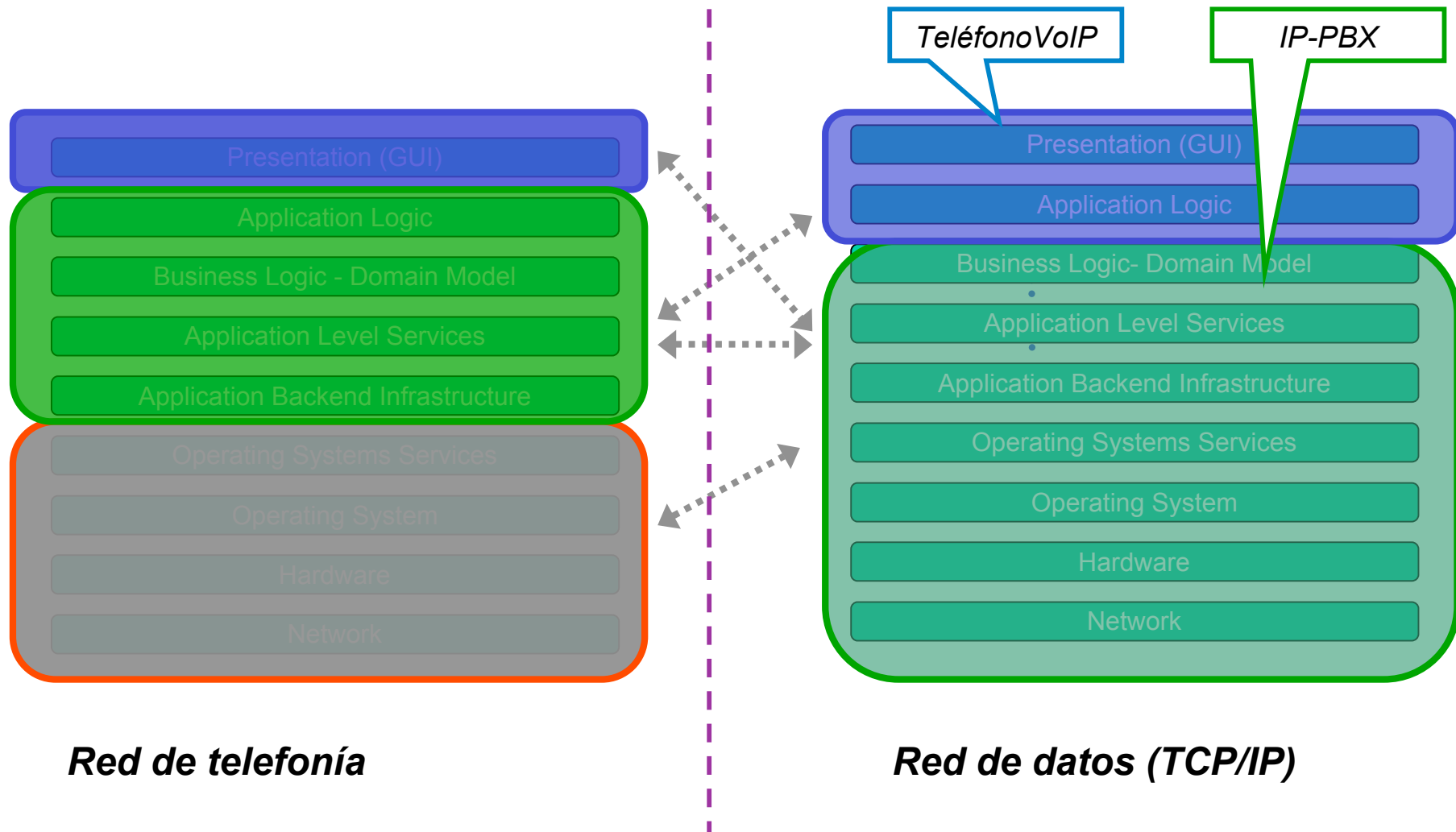
Equipamiento y aplicaciones de telefonía on-site



La PSTN ahora esta expuesta a manipulación de Customer Premise Equipment (CPE) y comparte confianza y responsabilidad con la empresa. Fraude telefonico y abuso de PSTN puede tener origen externo, la central privada puede ser re-programada maliciosamente. Es simplemente HW+SW en muchos casos gestionado remotamente vía modem!

1990-2008: Telefonía IP y VoIP combinan las amenazas de dos mundos

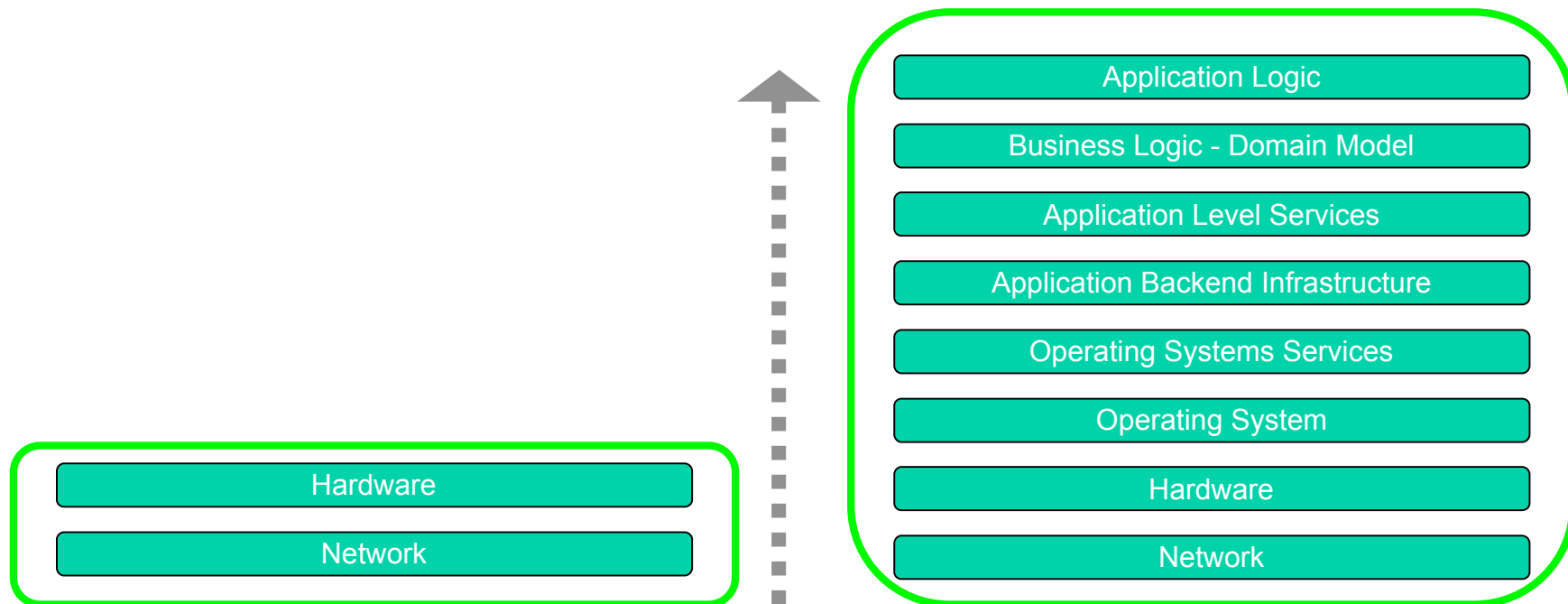
..... **Reducción de costos y mayor valor agregado motivan la convergencia de redes**



INFRASTRUCTURA PARA REDES CORPORATIVAS

1980-2005: 25 años de cambio significativo para los dispositivos de red

..... Las redes de datos de las empresas están ancladas a dispositivos muy complejos



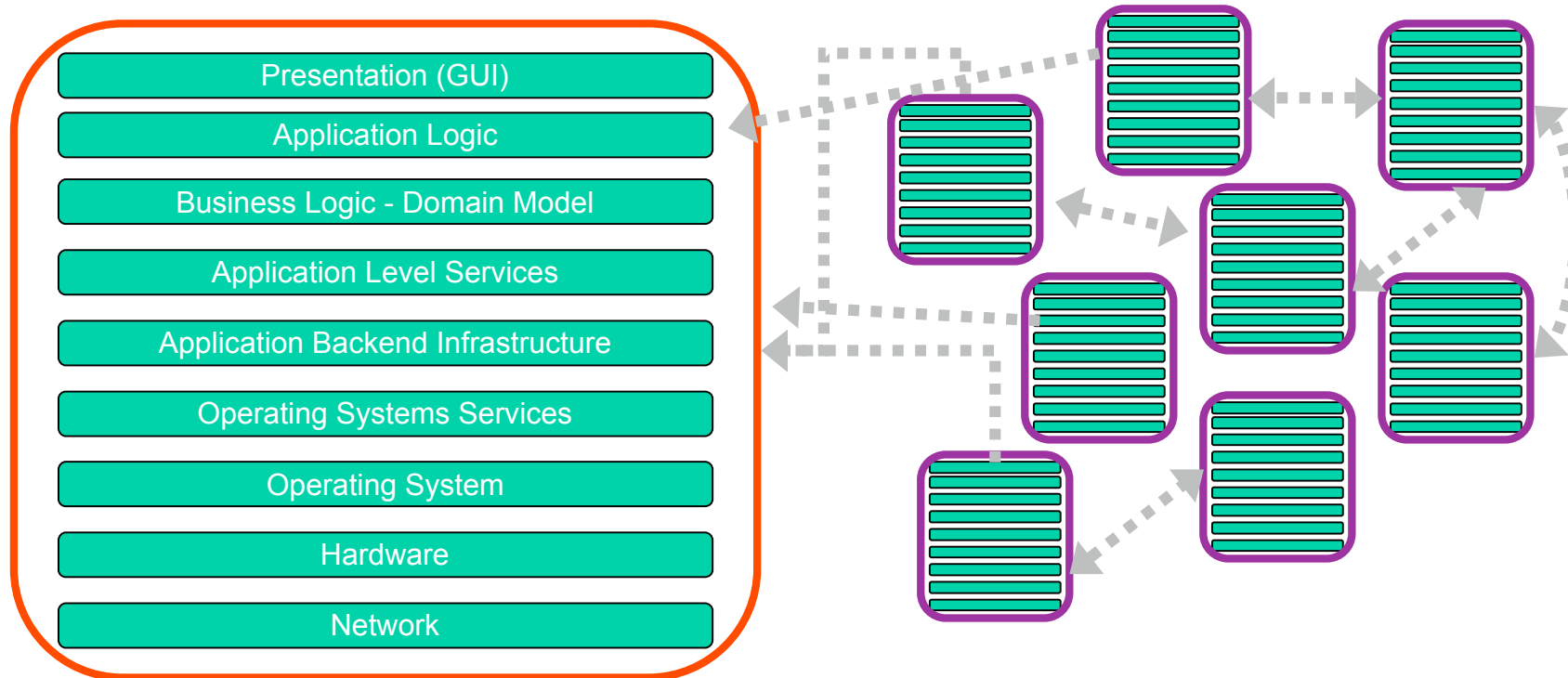
Hubs, switches, routers, firewalls, concentradores deVPN , IDS, balanceadores de carga y tráfico, SANs, impresoras & puntos de acceso inalámbrico se han convertido en sistemas de computo multi-proposito susceptibles al mismo tipo de amenazas a aquejan a los servers y máquinas de escritorio

Vulnerar la seguridad de estos dispositivos vulnera a toda la red de datos.

DISPOSITIVOS MOVILES

Por qué representan una amenaza?

Dispositivos con alto poder de cómputo

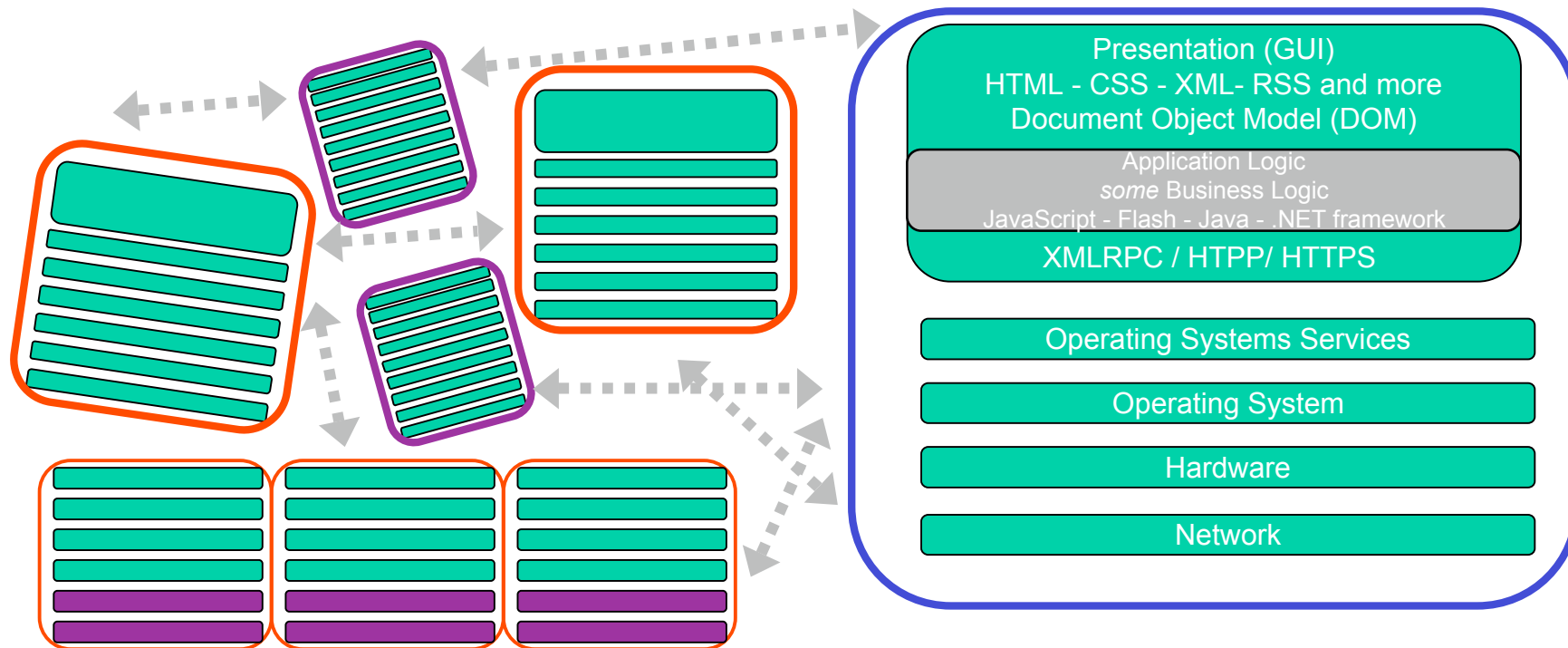


La mayoría de los dispositivos móviles usan aplicaciones y sistemas operativos con poca madurez en lo que respecta a su seguridad, pero con amplia funcionalidad tanto nativa como via VMs. Se conectan directamente a distintas redes de manera intermitente. No hay forma efectiva de aplicar y hacer cumplir políticas de control de acceso y manejo de recursos, conectividad P2P facilita la propagación de problemas, no tienen mecanismos adecuados de actualización y mantenimiento, la frontera entre lo privado y lo “propietario” se hace difusa

SaaS - MASH UPS – CLOUD COMPUTING

2005+ : Virtualización+Web Services+Web 2.0+Procesamiento distribuido

Se construye sobre la base de las tecnologías actuales



Servidores y servicios con
lógica de aplicación distribuida.
Modelo transaccional,
suscripción o *utility*

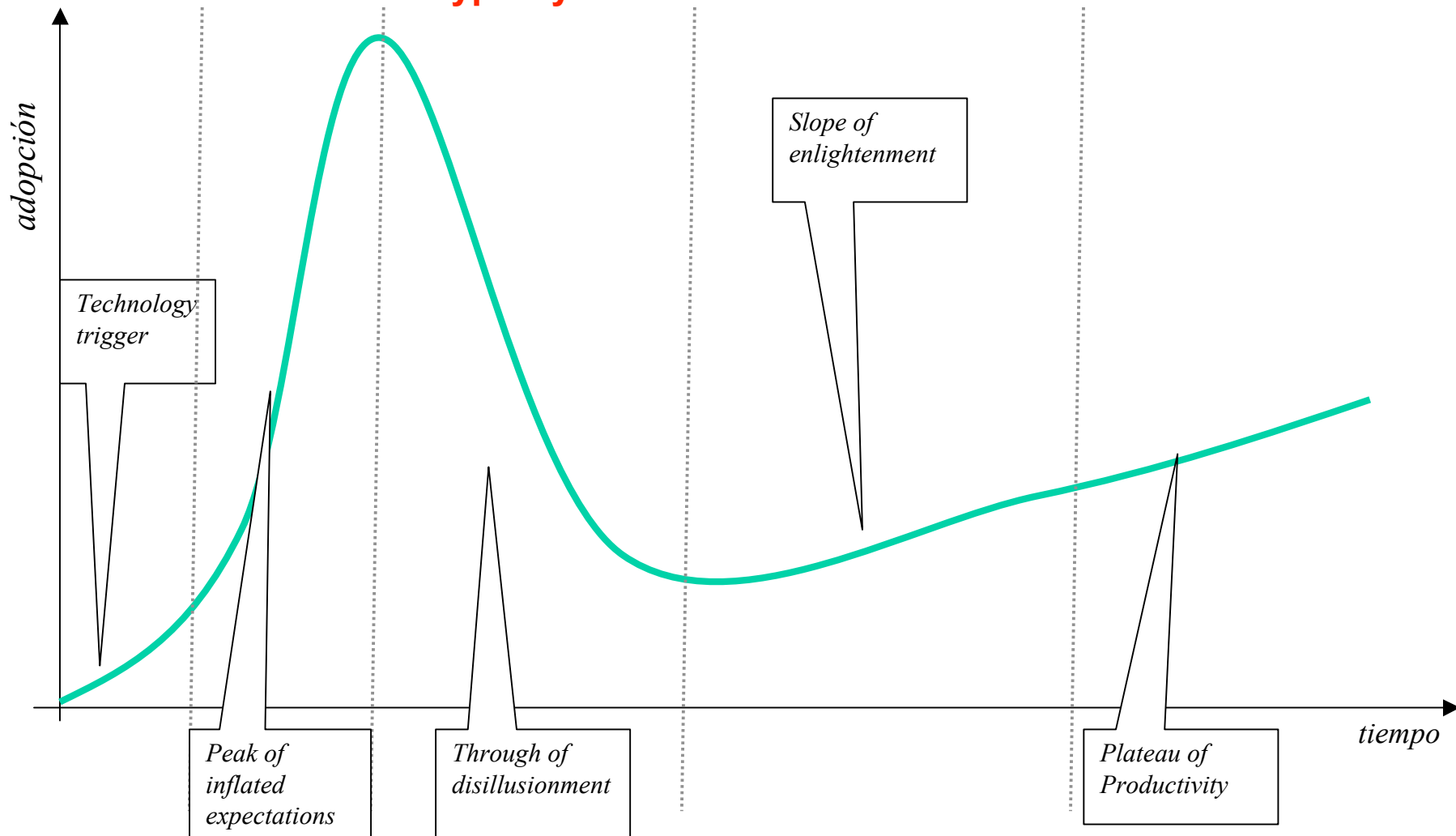
Un navegador Web corriendo sobre
cualquier plataforma adecuada para
interactuar con el usuario.

La lógica de negocios esta en el
navegador que utiliza colecciones de
servicios diversos. Integración vía
WS/HTTP sobre redes TCP/IP

COMO GESTIONAR MULTIPLES AMENAZAS DE MANERA SIMULTANEA?

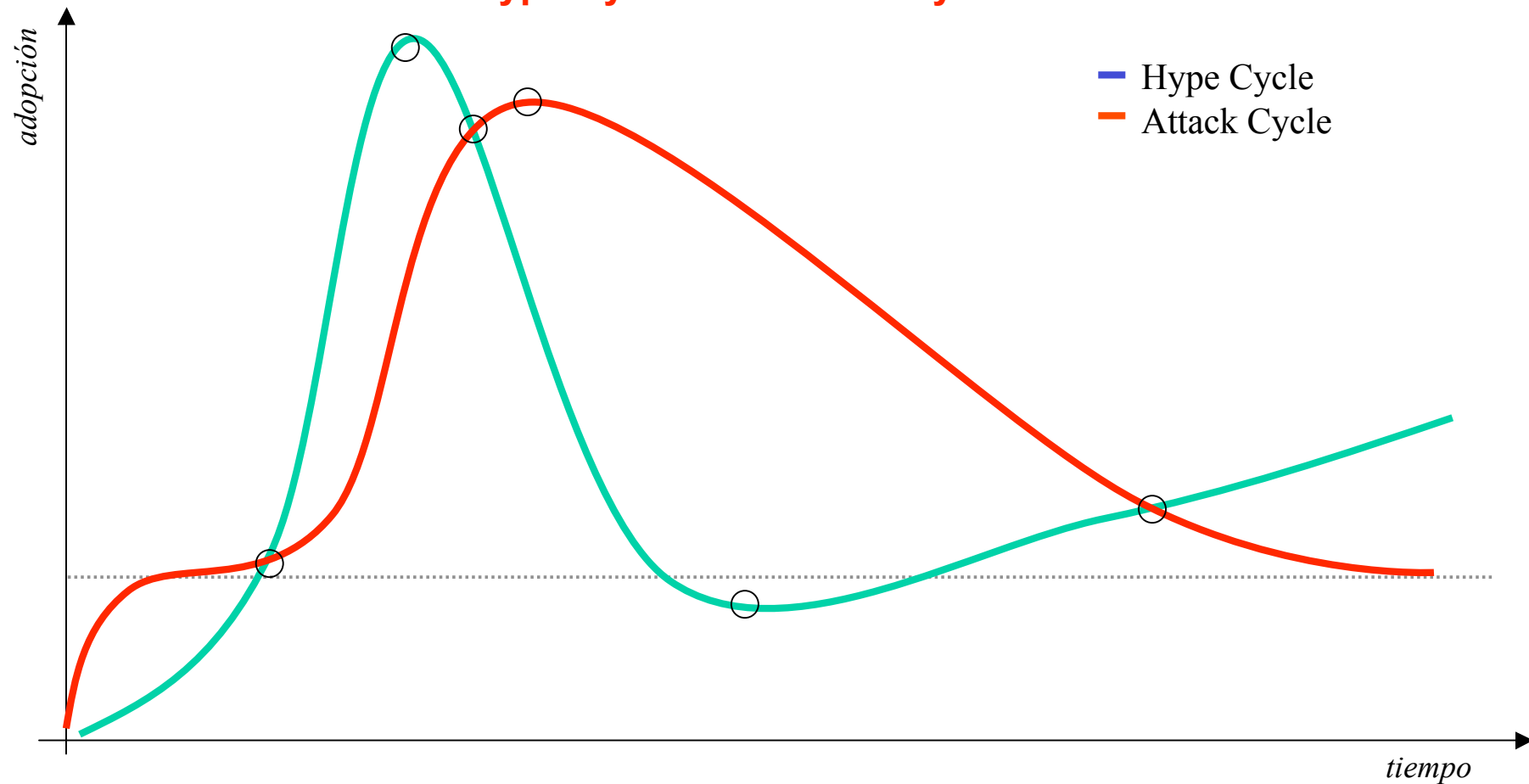
Es valido usar el “ruido del mercado” como un estimador del nivel de amenaza asociado?

El “Hype Cycle” de los analistas de la Industria



Y si nos inventamos un modelo propio?

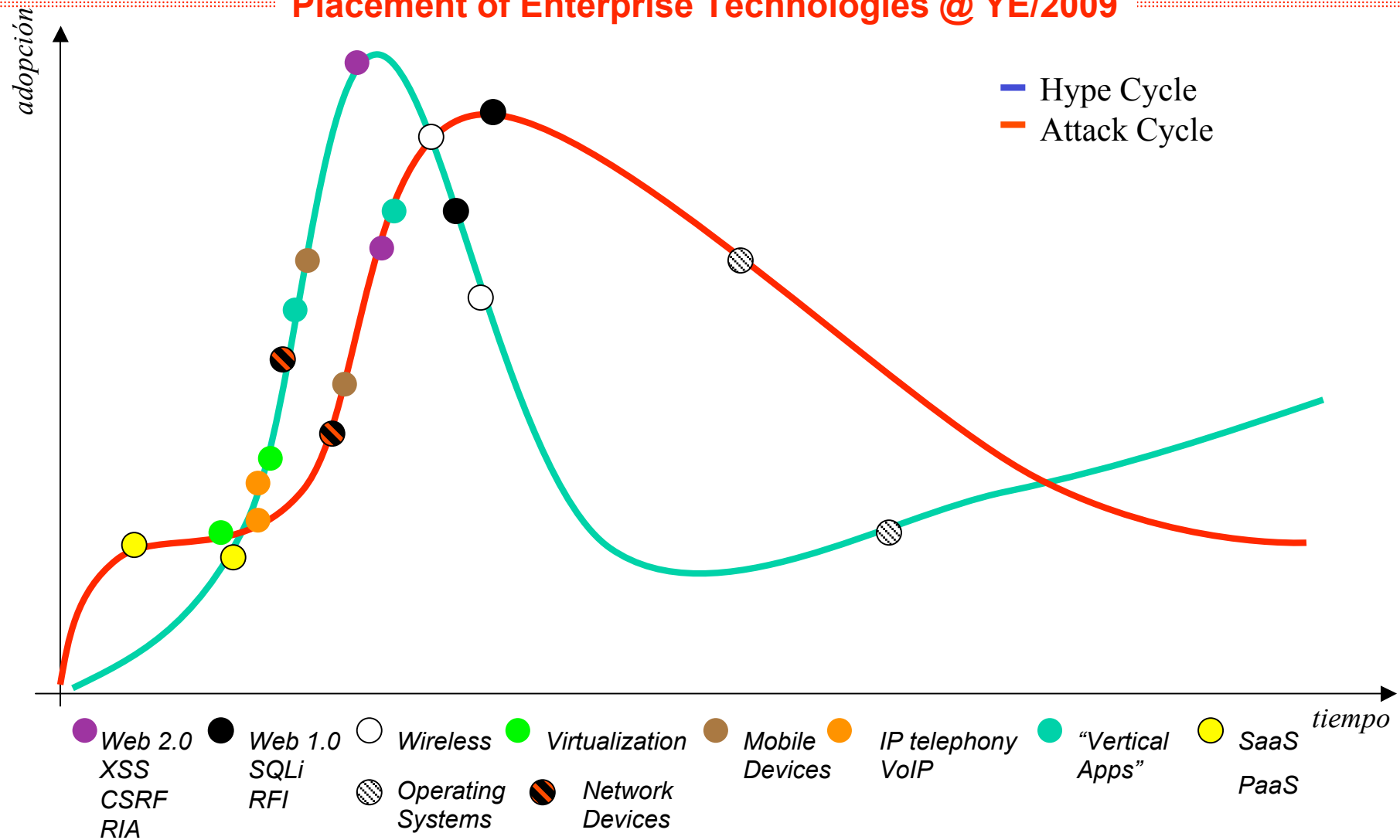
Hype Cycle vs. Attack Cycle de Core



Pronostico para fin del año 2009

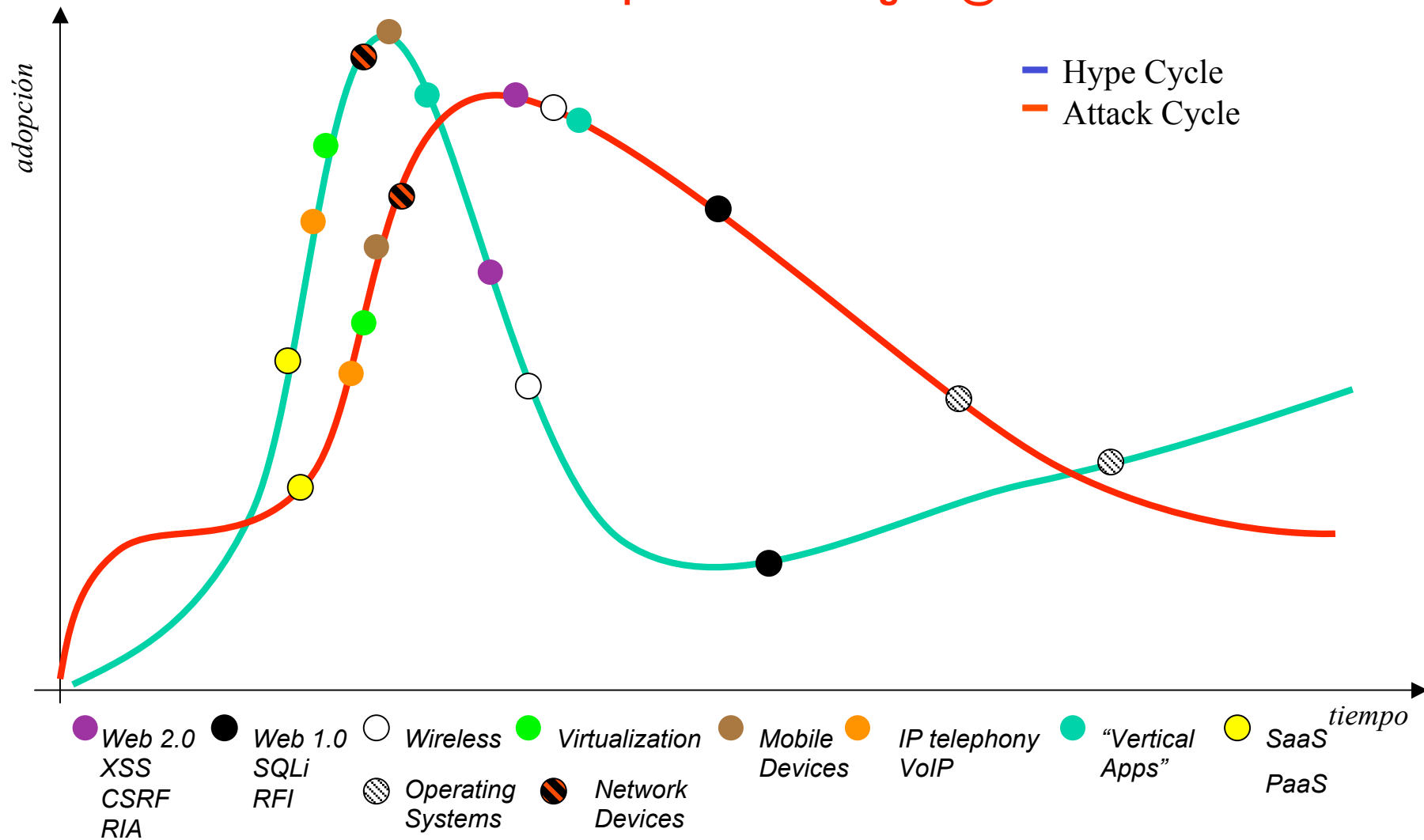
Estimado en Enero 2009

Placement of Enterprise Technologies @ YE/2009



Pronostico para fin del 2011

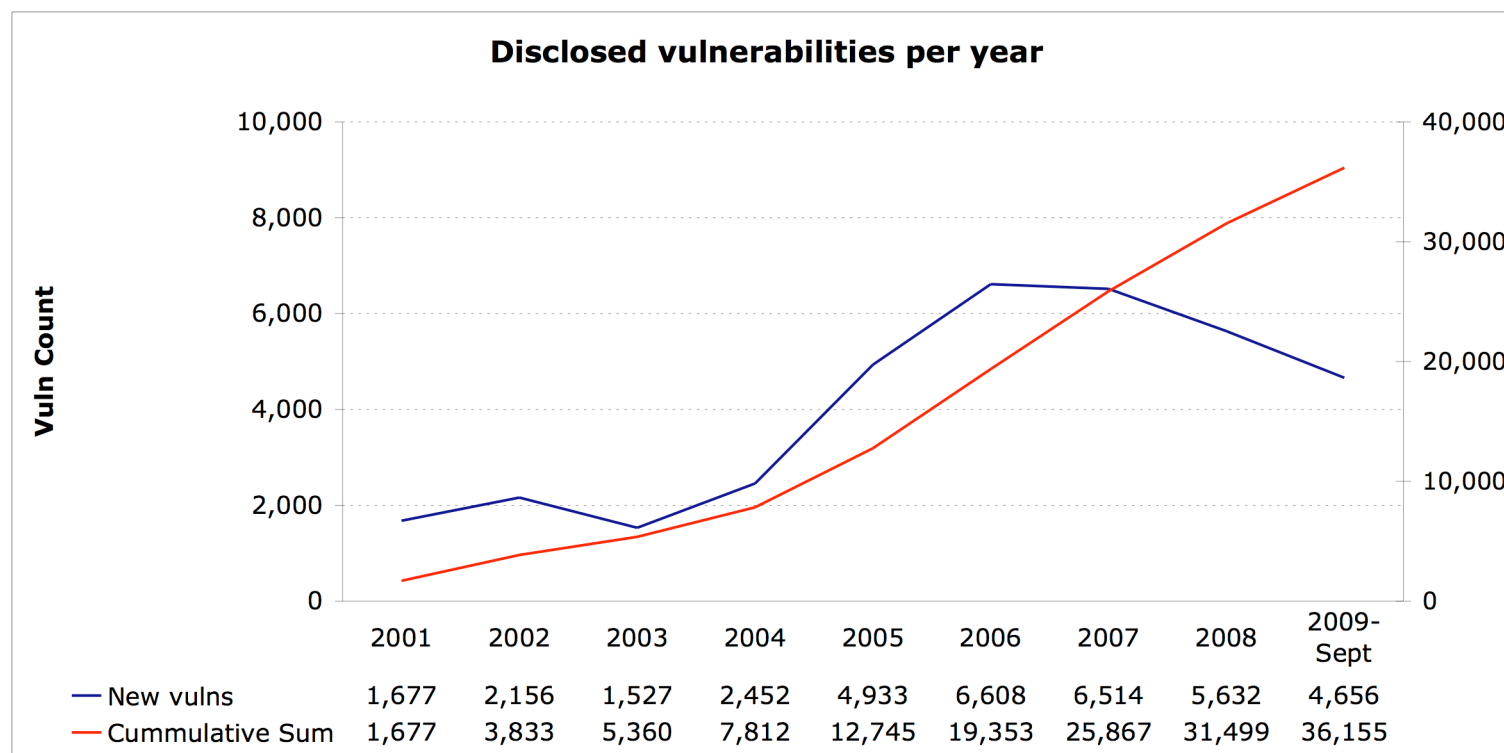
Placement of Enterprise Technologies @ YE/2011



LA EVOLUCION DE LOS ATAQUES

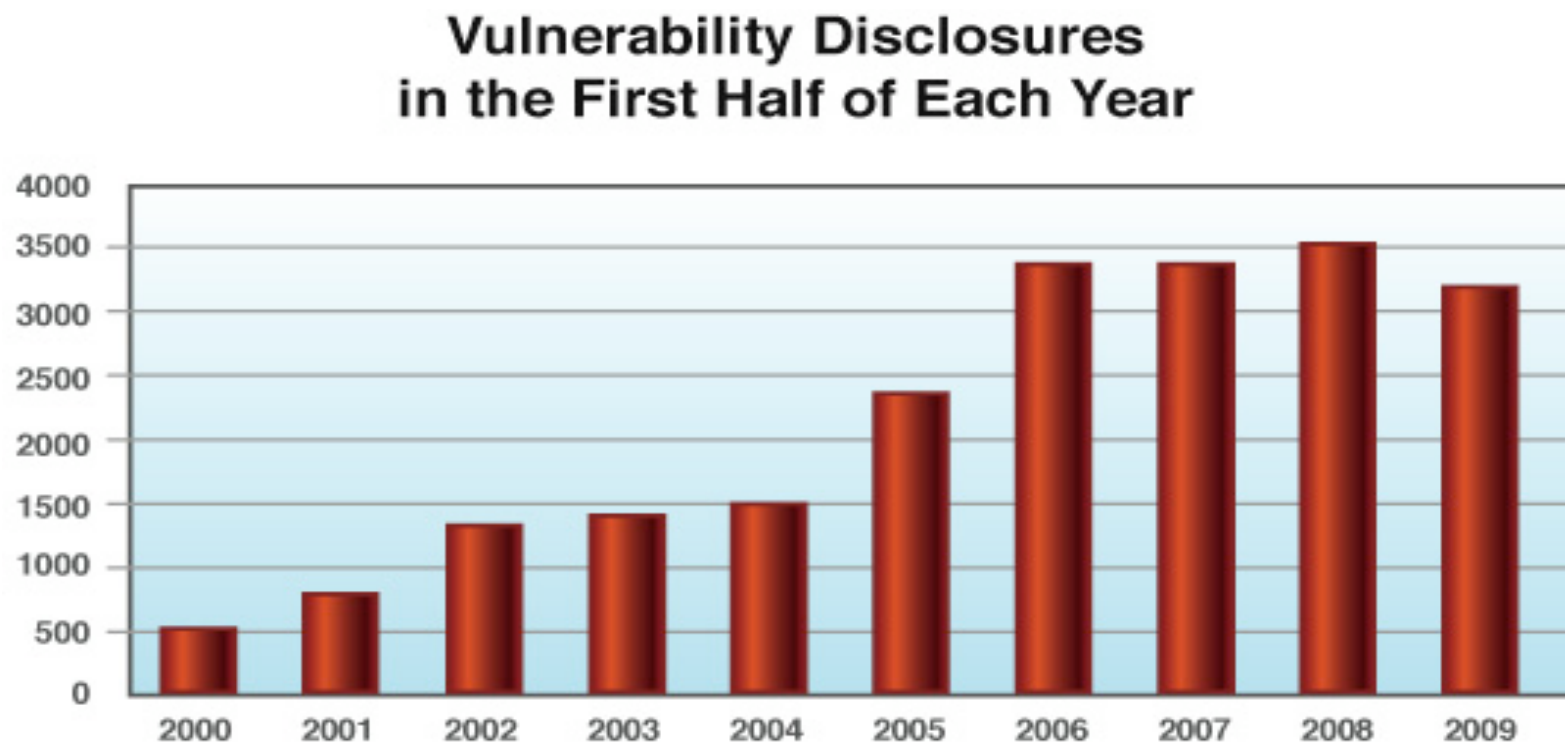
Cantidad de vulnerabilidades reportadas por año

- Más de 35,000 vulnerabilidades únicas (CVEs) en la National Vulnerability Database
- Más de 45,000 vulnerabilidades procesadas por CERT/CC desde 1995



Fuente: US National Institute of Standards and Technology (NIST) NVD
2009 actualizado al 30 Septiembre 2009 - <http://web.nvd.nist.gov>

Cantidad de vulnerabilidades reportadas por año #2



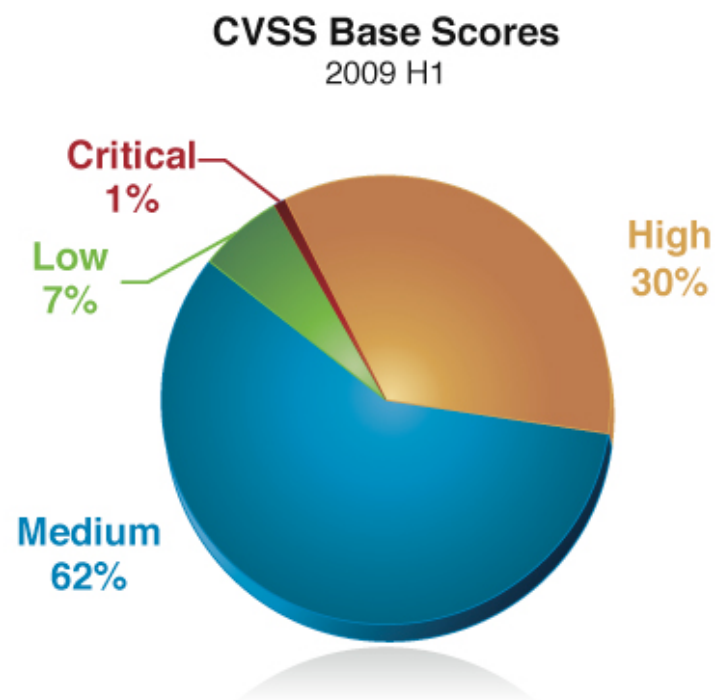
source: IBM X-Force®

Fuente: IBM/ISS X-Force 2009 Mid-Year Trend Statistics

<http://www-935.ibm.com/services/us/iss/xforce/trendreports/>

Si bueno, pero cuantas son realmente relevantes?

- Vulnerabilidades con CVSS ≥ 7.0 (High + Critical)



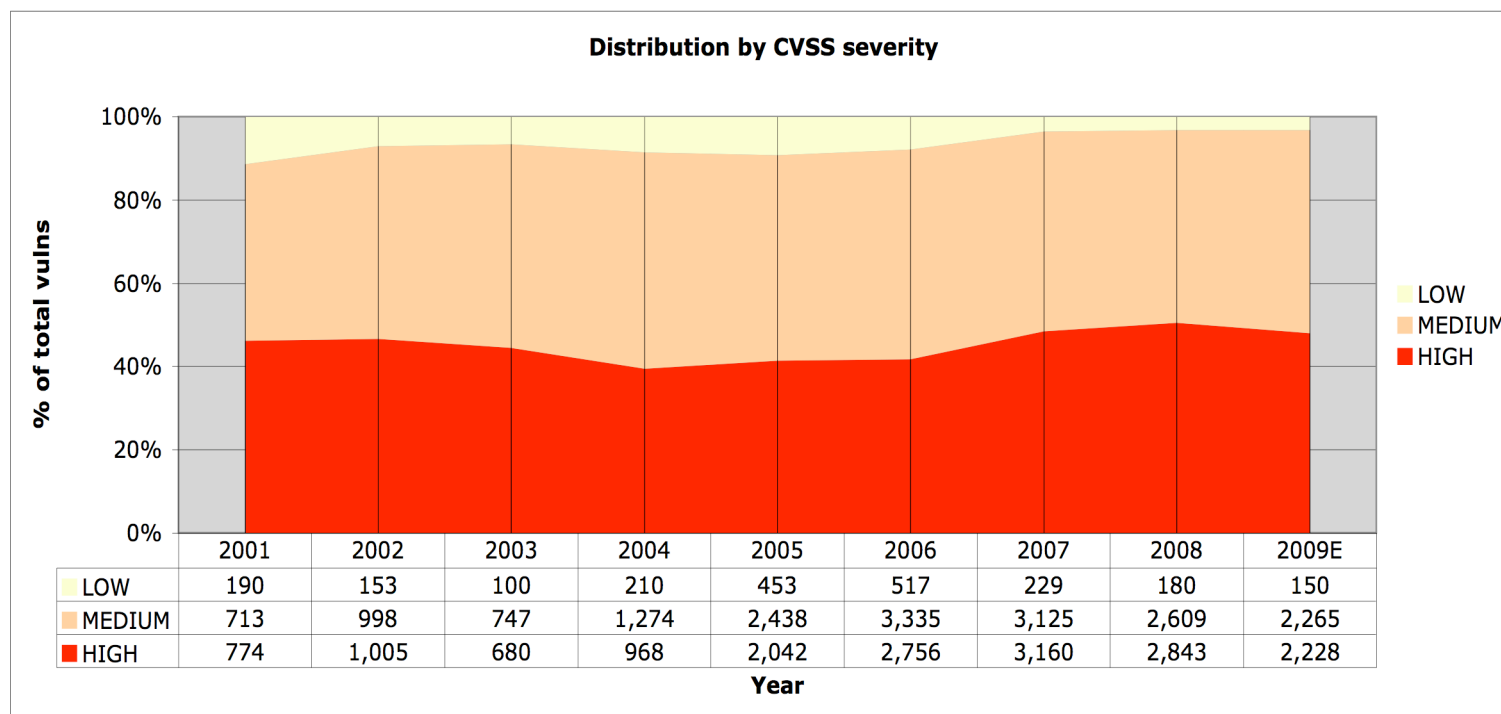
source: IBM X-Force®

Fuente: IBM/ISS X-Force 2009 Mid-Year Trend Statistics

<http://www-935.ibm.com/services/us/iss/xforce/trendreports/>

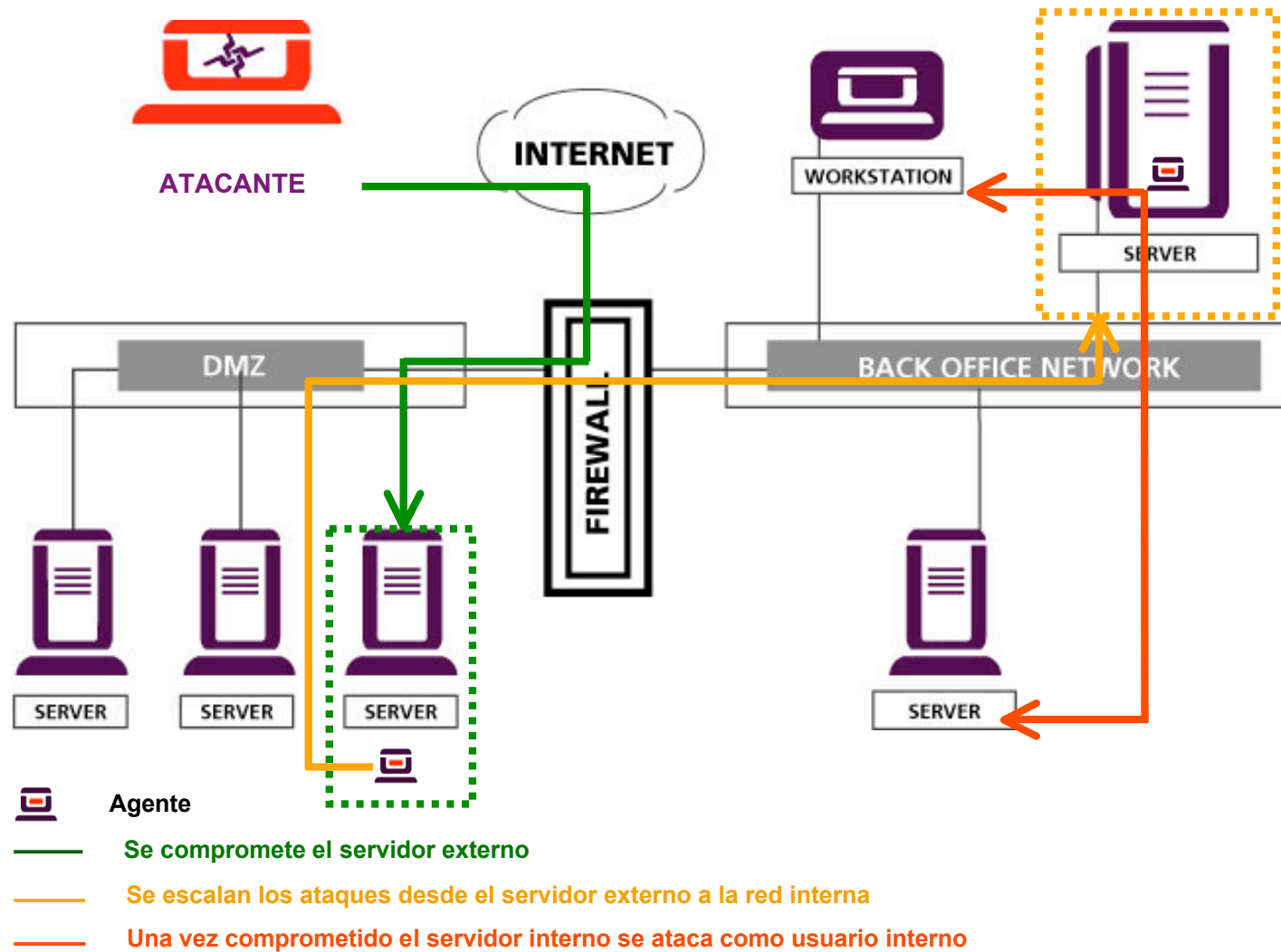
Cantidad anual de vulnerabilidades por severidad

- Un estimado conservador: 20%-25% de entre 6,000 y 7,000 anuales
- Un mínimo promedio de 23 vulnerabilidades nuevas por semana



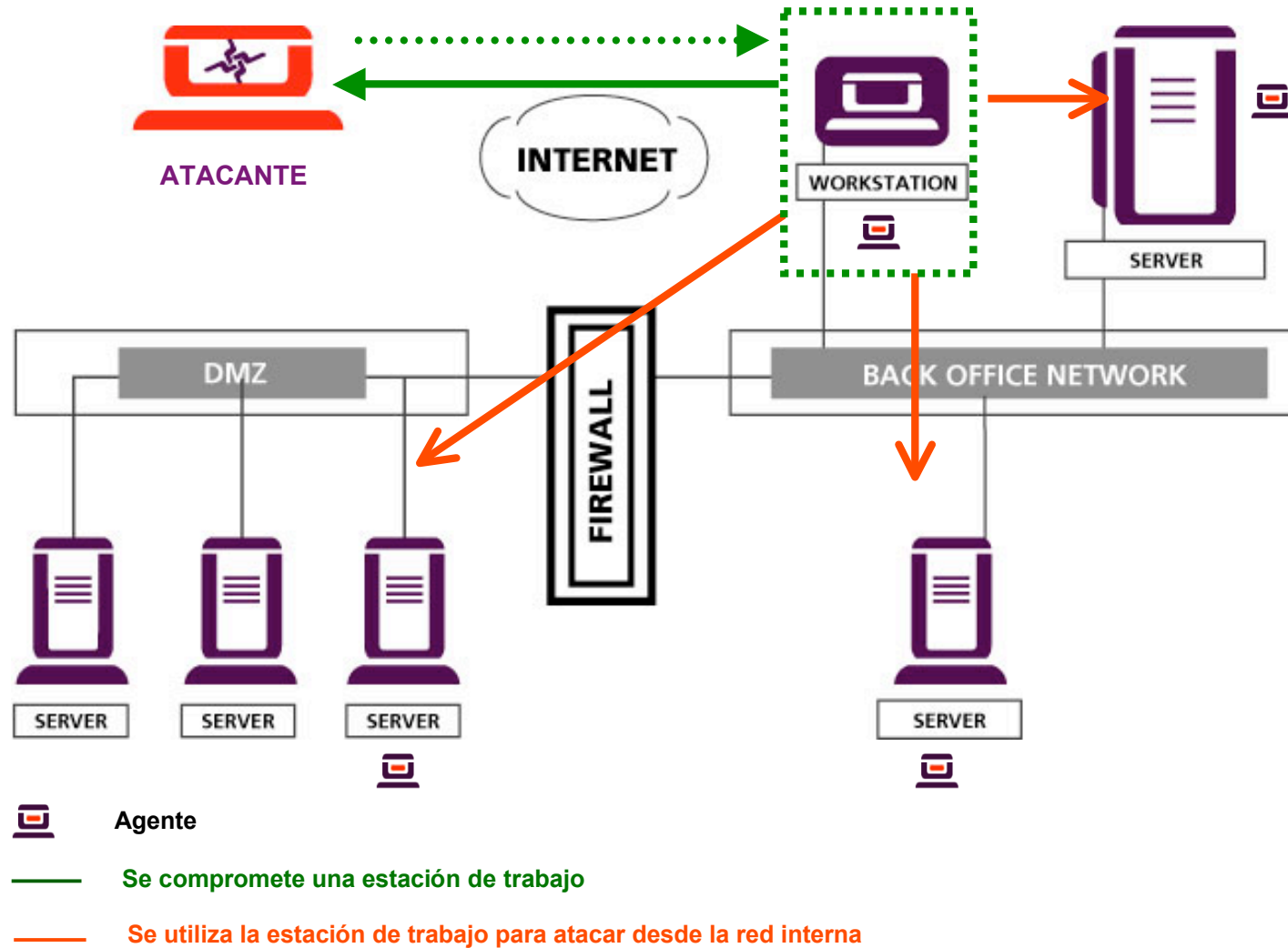
Fuente: US National Institute of Standards and Technology (NIST) NVD
2009 actualizado al 30 Septiembre 2009 - <http://web.nvd.nist.gov>

Anatomía del ataque clásico de los 90s (1990-2001)



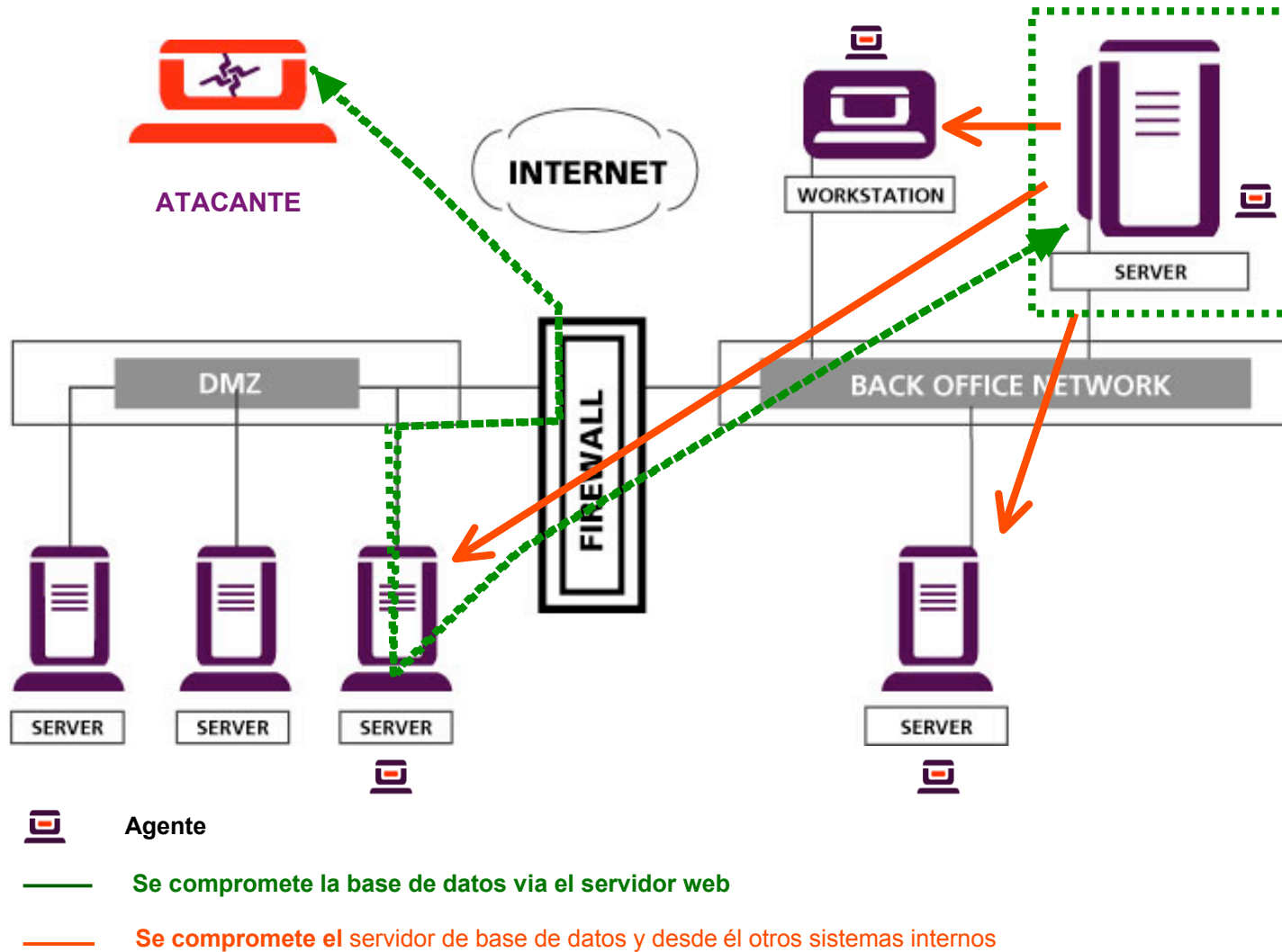
Ataques Client-Side (2001+)

ESCENARIO DE ATAQUE - CS



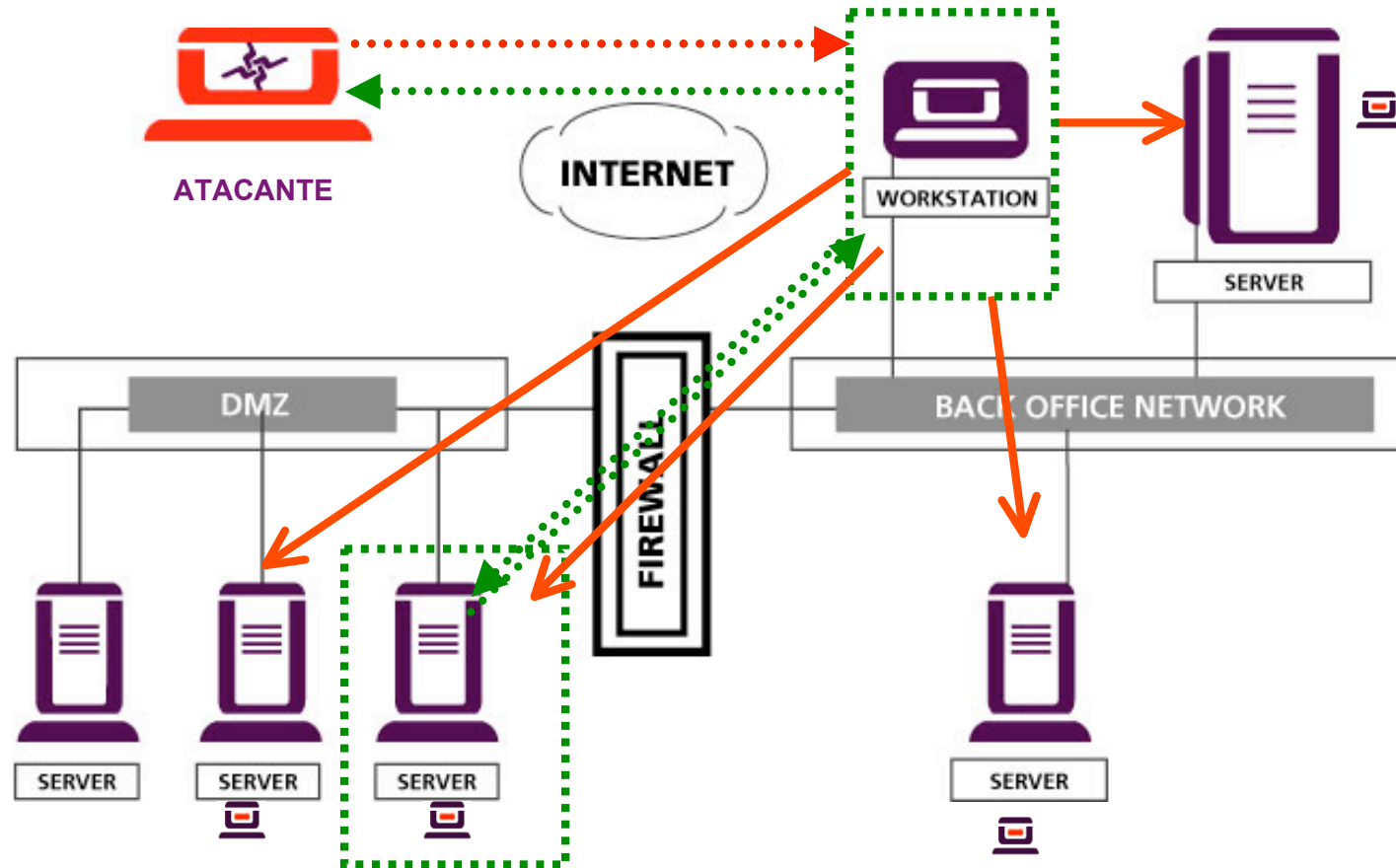
Ataque de Inyección de SQL (2000+)

ESCENARIO DE ATAQUE - SQLI



Ataques de Cross Site Scripting (2005+)

ESCENARIO DE ATAQUE - XSS



 Agente

— Se toma control del navegador de una estación de trabajo por medio de una vulnerabilidad en la aplicación web

— Se utiliza el navegador comprometido para acceder a otras aplicaciones y sistemas como usuario interno

Los desafíos del presente

- **En la actualidad los ataques comunes combinan distintos vectores y técnicas**
 - La multiplicidad de nuevos vectores de ataque tensiona el modelo de manejo de riesgo

- **Dada la cantidad creciente de vulnerabilidades que un atacante potencial podría explotar**
 - Como determinar cuales solucionar dado un conjunto finito de recursos?
 - Como determina cuales **implementar** dado un conjunto finito de recursos?
 - Decaimiento del valor del exploit en funcion del tiempo
 - Decaimiento del valor total del conjunto de exploits en funcion del tiempo
 - Es posible generar exploits programaticamente?
 - Como medir la calidad de un exploit?

- **Attack Paths & Attack Graphs**
 - Attack graph: Grafo dirigido (multiple y con loops). Targets y módulos.
 - Attack paths: Conjunto de caminos del attack graph
 - Determinar el conjunto mínimo de nodos a sacar para hacer el grafo no-conexo
 - Determinar el conjunto mínimo de aristas a sacar para hacer el grafo no-conexo
 - Determinar el conjunto mínimo de nodos a sacar que remuevan todos los caminos
 - Representación gráfica de grafos con miles de nodos y aristas

- **Crecimiento exponencial de la cantidad de nodos y aplicaciones en las redes**

Los potenciales desafíos del futuro

- **La ley de Moore también se aplica a la capacidad de los atacantes**
 - Poder de cómputo
 - Procesamiento distribuido
 - Cloud Computing
 - Costo de adquisición y mantenimiento de botnets
 - Desaparición del “perímetro” de red
 - Desaparición de la distinción entre datos en reposo o en tránsito
 - Protección de datos personales y privacidad
- **Y entonces como modelamos y emulamos efectivamente a un atacante?**
- **Agregación de niveles de abstracción**
 - Operativo
 - Táctico
 - Estratégico
- **Penetration Testing y Gestión de Riesgo**
 - Value at Risk (VaR), Annual Loss Expectancy (ALE)
 - Ausencia de datos sobre incidentes, valoración subjetiva de activos, activos intangibles
 - Concepción constructivista/reduccionista del riesgo
 - Riesgo como característica emergente
 - Economía, Ciencias Sociales, Biología, Física, Epistemología.
 - Teoría de Juegos, Dinámica Evolutiva, sistemas adaptativos complejos, Inteligencia Artificial, Aprendizaje
- **Como adquirir y transferir conocimiento de un conjunto de especialistas expertos?**

ES UTIL HACER *PENETRATION TESTING*?

Mi definición de “Penetration Testing”

“Un intento acotado y localizado en el tiempo de vulnerar la arquitectura de seguridad de una organización utilizando las técnicas de los atacantes”

Por qué es desable hacer Penetration Testing?

- **Modelar y gestionar riesgo con una estrategia puramente defensiva induce a error**
- **La percepción de valor y de riesgo de dos sujetos puede ser distinta**
- **Permite contrastar y corroborar hipótesis sobre la postura de seguridad**

Algunas cosas implícitas en nuestra definición

Se implica...

- Una definición de alcance en el espacio-tiempo
 - La existencia de un marco de referencia para modelar atacantes
 - La existencia de algún tipo de “arquitectura de seguridad” a probar
 - La aceptación del potencial disruptivo de vulneración de dicha arquitectura
 - La existencia de una *técnica (o...modus operandi)*
http://buscon.rae.es/drael/SrvltConsulta?TIPO_BUS=3&LEMA=t%E9cnica
 - 1. adj. Perteneciente o relativo a las aplicaciones de las ciencias y las artes.
 - 3. m. y f. Persona que posee los conocimientos especiales de una ciencia o arte.
 - 5. f. Conjunto de procedimientos y recursos de que se sirve una ciencia o un arte.
 - 6. f. Pericia o habilidad para usar de esos procedimientos y recursos.
 - 7. f. Habilidad para ejecutar cualquier cosa, o para conseguir algo.
 - Una sutil distinción entre “como un atacante” y “usando técnicas del atacante”
- => Se da a entender que hay un propósito u objetivo para el ejercicio

GRACIAS!