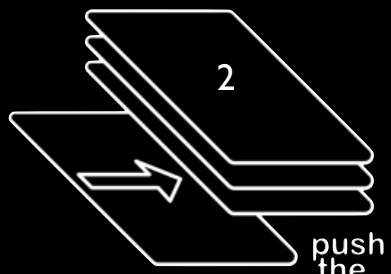
seguridad cuando nanosegundos son importantes

James Arlen, CISA
SecurityZone 2011
Cali, Colombia

renuncia

Soy empleado en la industria de Infosec, pero no autorizado para hablar en nombre de mi empleador o clientes.

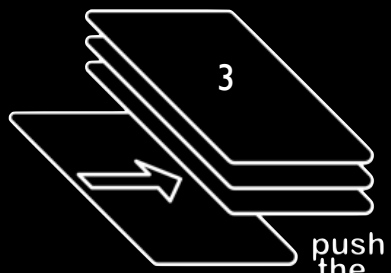
Todo lo que digo se puede culpar a las voces en SU cabeza.



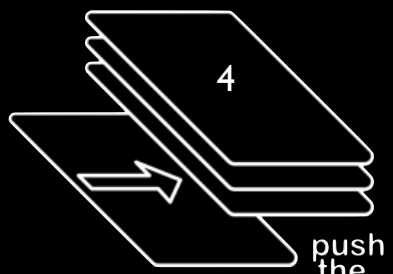
credenciales

- De 15+ años especialista en seguridad de la información
- personal de operaciones, consultor, auditor, el investigador
- servicios verticales (operaciones de la red, generación, distribución)
- financiera vertical (bancos, compañías de fideicomiso, el comercio)
- algunas cosas relacionadas con hackers (fundador de think|haus)

... todavía no es un experto en cualquier cosa.

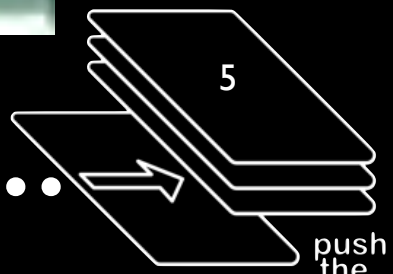


nanosegundos...



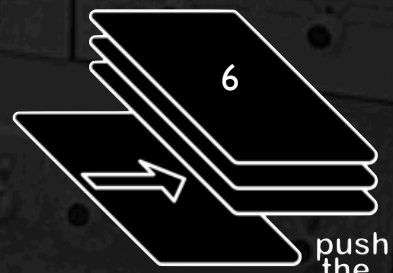
Admiral Hopper affirma...

From an interview segment by Morley Safer in 1982



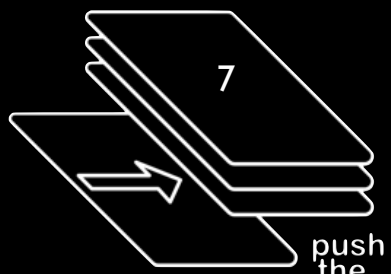
$=c (velocidad de la luz materia)

- distancia que la luz viaja en un:
  - milisegundo ~300km
  - microsegundo ~300m
  - nanosegundo ~30cm



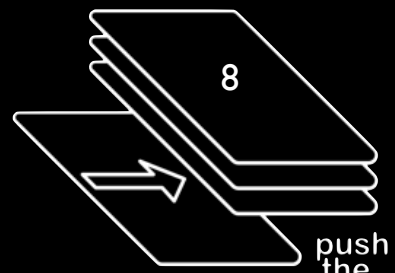
antes de preguntar ...

- Esta es una conversación... $$
- Yo no voy a mencionar ninguna de esas cosas en el término de moda de tarjetas de bingo:
  - SCADA
  - APT
  - PCI - DSS
  - wikileaks
  - (anti-|lulz)sec
  - hacktivism
  - ... insertar más aquí.



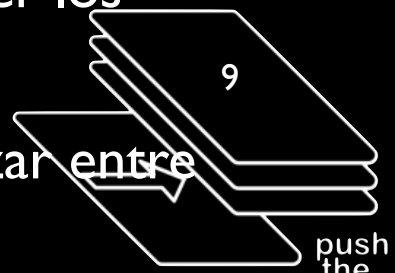
finanzas y la seguridad?

- Usted lo sabe!
- La mayoría de INFOSEC se acerca todas las técnicas ofensivas y defensivas y las tecnologías
- A veces, sabiendo que existe una vulnerabilidad de ser explotada ayuda acentrar la atención.
- A veces, la gente le gusta que le diga cosas que suenan completamente locos, pero tienen una historia de hacerse realidad.



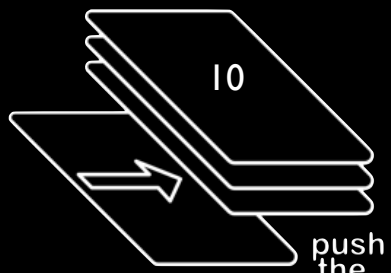
La historia de los mercados financieros

- 1200s - De los productos básicos y el comercio de la deuda
- 1500s - Inter-mercado de comercio
- 1600s - negociación de renta variable
- temprano 1800s - Reuters utiliza palomas mensajeras
- tarde 1800s - electrónica teletipo (Mercado de fuentes de datos) se generalizan
- mid 1900s - sistemas de cotización (precio al lado en vez de el último precio) se generalizan
- tarde 1900s - los ordenadores se utilizan para mantener los registros del intercambio
- temprano 2000s - las computadoras comienzan a cotizar entre sí sin intervención humana



definiciones

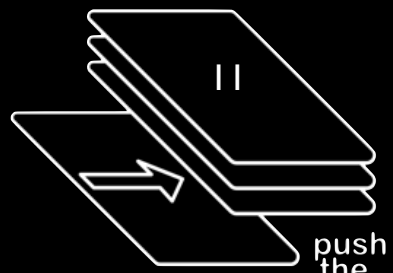
- de comercio de alta velocidad: la comisión negocia en una escala más rápida que las velocidades humanos interactivo
- algorítmica de comercio: comercio basado en el resultado matemático de la información recibida de fuentes externas (noticias, datos de mercado, etc)



arbitraje

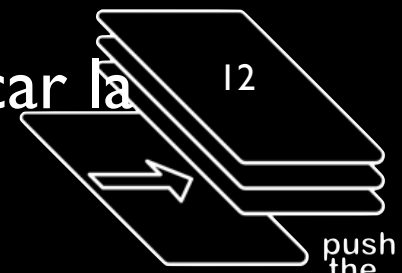
la práctica de tomar ventaja de una diferencia de precio entre dos o más mercados: lograr una combinación de ofertas de juego que capitalizar el desequilibrio, el beneficio es la diferencia entre los precios de mercado.

- en el espacio - entre dos mercados separados geográficamente
- en el tiempo - entre el momento está disponible la información y la información que actualmente se conoce ampliamente

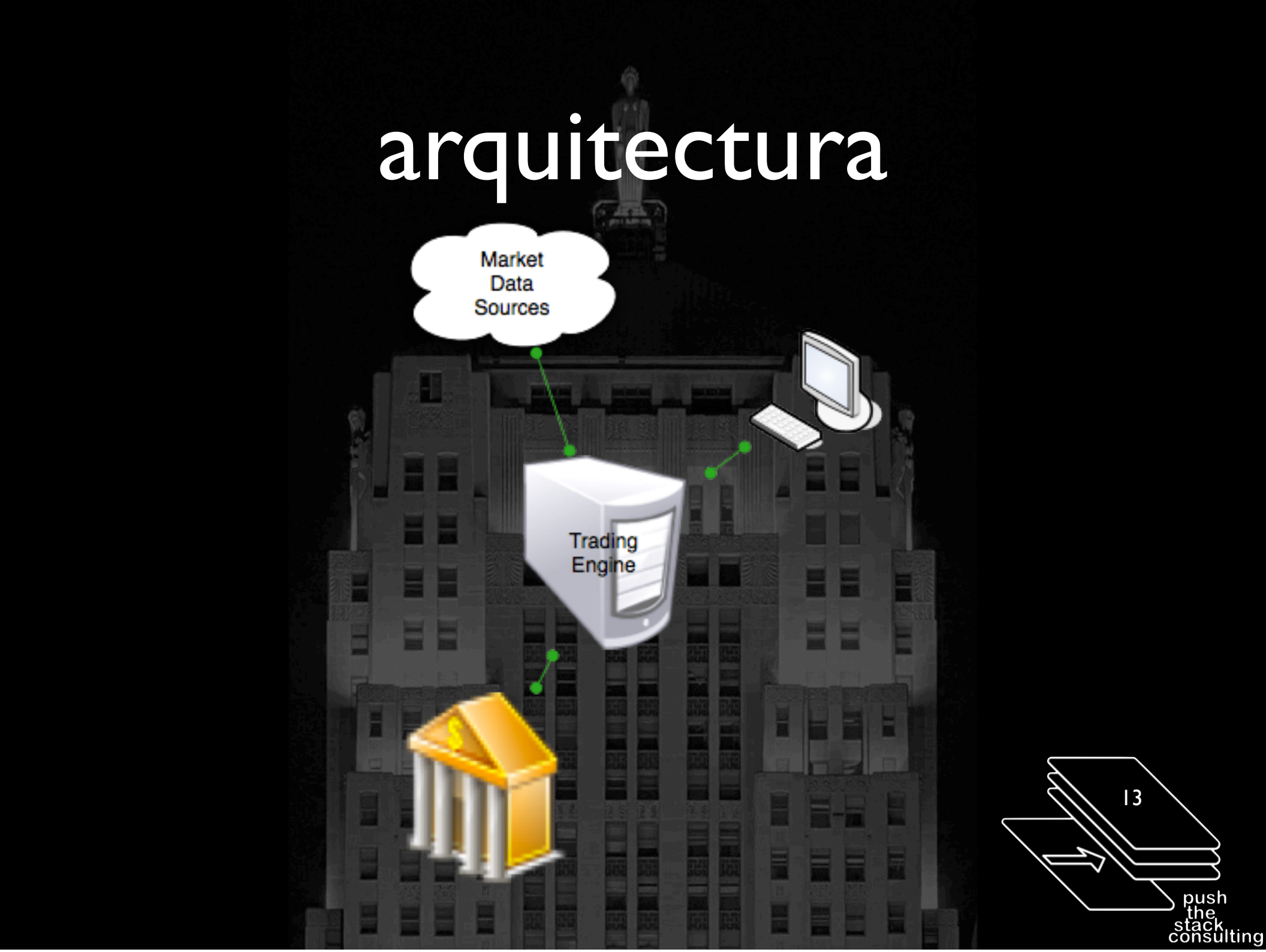


tiempo

- cuando los mercados eran nuevos (mediados del pasado milenio) veces el comercio se mide en una escala muy humana
- finales de 1800 llevó a los tiempos del comercio minutos
- 1900 trajo el comercio a veces segundos
- 2000 traerá tiempos el comercio de 100s de microsegundos
- Tiempos futuros y el comercio puede implicar la emisión de taquiones

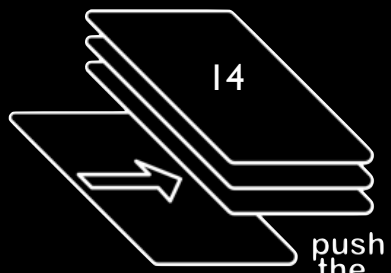


arquitectura



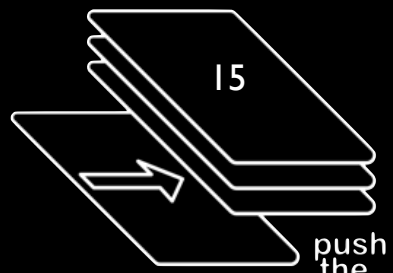
qué tan rápido es rápido?

- segundo: que no tienen una posición
- milisegundos: pierde casi cada vez que
- sub-milisegundo: los grandes jugadores que regularmente superar
- 100s de microsegundos: usted gana alguna vez y pierde poco
- 10s de microsegundos: usted por lo general gana



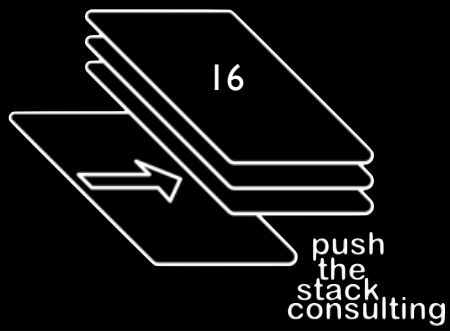
previsibilidad

- Casi tan importante como la velocidad pura es la velocidad predecible.
- Los enemigos son: inquietud, pérdida de paquetes, los protocolos ineficiente (TCP)
- Un paquete perdido es dinero perdido



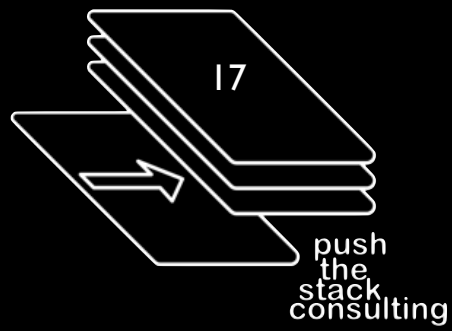
proximidad

- Proximidad alivia muchos de los efectos de velocidad / latencia / jitter
- Usted está en la LAN, no la MAN o la WAN

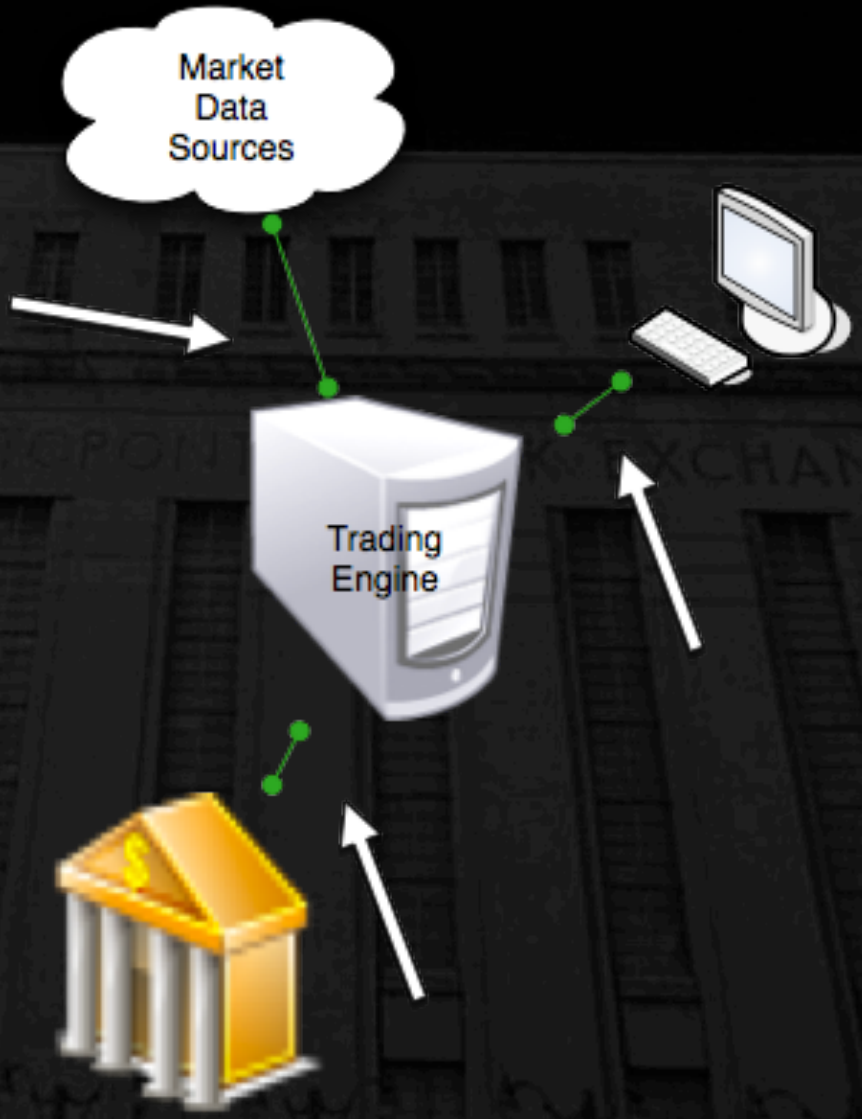


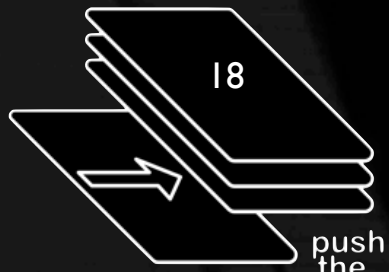
latencia cuesta $

- latencia tiene un costo de $ $ asociados a ella - medibles y por lo tanto,financiables



que falta?


Market
Data
Sources
Trading
Engine

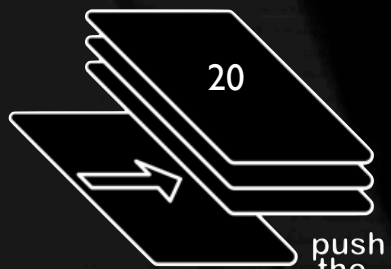

18
push
the
stack
consulting

oh mierda.


OTHER CUSTOMER
Market Data Sources
Trading Engine
OTHER CUSTOMER

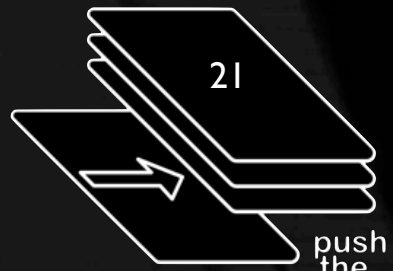
Colega, ¿dónde está mi firewall?

- ningún servidor de seguridad ...
- añaden latencia (un montón de latencia)
- latencia cuesta $
- riesgo <costo <ganancias



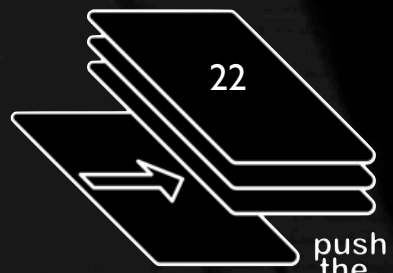
acl, por favor?

- no acls
- añaden latencia
- (la mayoría) los switches pierden velocida con ACLs



endurecer la ...

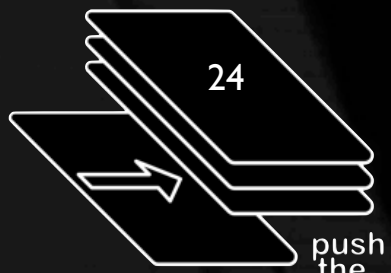
- no (con sentido) sistema de endurecimiento
- sistema de reducción de la carga (al desnudo)
- en gran parte del código de interfaz personalizado (Ethernet / InfiniBand / PCIe)
- y las quejas habituales de mantenimiento y resolución de problemas



Sistemas especializados

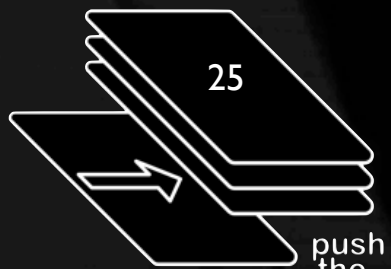
modelado de amenazas

- sabemos lo que falta en nuestro juego habitual de los controles
- ¿cómo lo describirías?
- ¿cómo podemos determinar qué es una amenaza razonable para construirmedidas de protección contra?



AMENAZA: vendedores

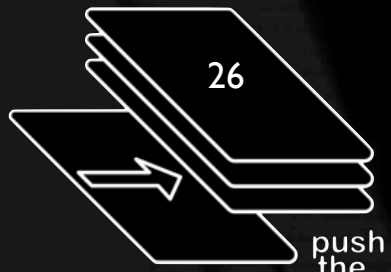
- Estás confiando en lo que dice mercadeo es verdat.
- Estás confiando en que no han contratado ningún malos.



LO MEJOR: los vendedores

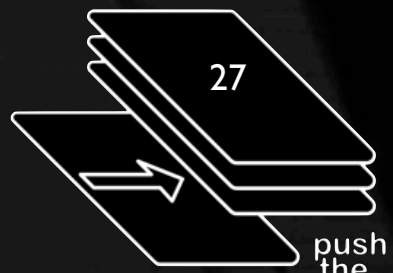
- ¿Qué tal un desarrollador vendedor que altera los parches que usted recibe por lo que el Precision Time Protocol (PTPv2 - 802.1AS) tiene un concepto diferente de un microsegundo de la que todos los demás están usando?

http://www.ieee802.org/1/pages/802.1as.html



AMENAZA: desarrolladores

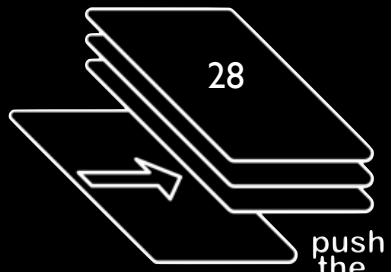
- En la mayoría de los algoritmos de comercio, el desarrollador no es tradicionalde desarrollo con todos los controles habituales SDLC
- El desarrollador es, probablemente, un comerciante o un subalternocomerciante que tiene acceso directo a la producción de motores y algoritmospuede hacer sobre la marcha los cambios



SÍ: Desarrolladores

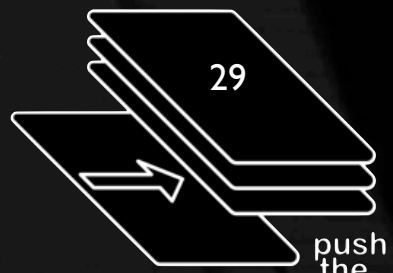
- Sergey Aleynikov
  July 3, 2009
  http://www.wired.com/threatlevel/2009/07/aleynikov/
  - 32 megabytes de código de Goldman Sachs
  - condenado a 97 meses de prisión (8 años 1 mes) y $ 12.500 fino

http://www.facebook.com/group.php?gid=12355051732O



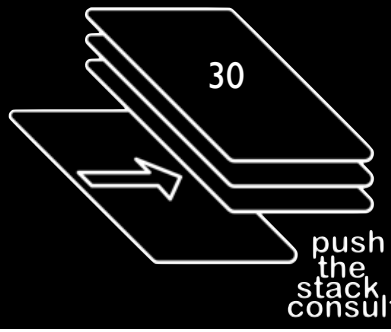
AMENAZA: la información privilegiada

- no que tipo de información privilegiada
- ¿Cómo lidiar con un operador (o administrador) que está utilizando el acceso a los datos del mercado de redes o redes de intercambio de causar efectos negativos sobre los demás participantes?



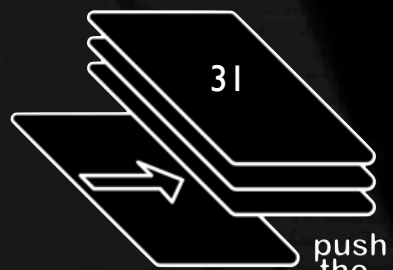
SI: Los comerciantes

- Samarth Agrawal
  April 16, 2010
  http://www.wired.com/threatlevel/2010/04/bankerarrested/
  - varios cientos de páginas de código de Societe Generale
  - condenado a 3 años de prisión y 2 años de libertad supervisada + deportación



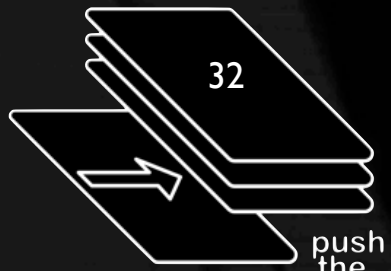
AMENAZA: el mercado

- Esta es una extraña amenaza técnico
- ¿Puede el mercado es causa de problemas con sus sistemas?
- mensajes mal formados
- escrutinio de transacciones de riesgo
- sistemas comprometidos



SÍ: Mercado

- 2010-05-06 - Dow Jones cae 900 puntos en cuestión de minutos - EL FLASH CRASH
- Informe de NANEX
  http://www.nanex.net/20100506/FlashCrashAnalysis_Part1-1.html



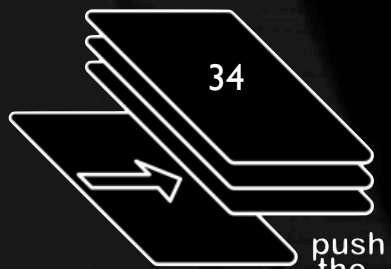
Sumario de Ed Felten

1. Algunos participantes del mercado envió un gran número de solicitudes de presupuesto para el New York Stock Exchange (NYSE) computadoras.
2. La Bolsa de Nueva York que normalmente pone comillas precio de salida en una cola antes de ser enviados. Debido a la alta tasa de solicitudes, esta cola de copia de seguridad, de modo que algunas citas tomó un tiempo(relativamente) de largo para ser enviado.
3. Una cita las listas de un precio y una hora. La Bolsa de Nueva York determinó el precio en el momento de poner la cita en la cola, y con fecha y hora de cada cita, en el momento en que salió de la cola. Cuando las colas de copia de seguridad, estas cotizaciones sería "obsoleto", en el sentido de que había un viejo, que ya no se precisa el precio --- pero sus marcas de tiempo hizo que se vean como las cotizaciones hasta al día.
4. Estas citas anómala confundir otros participantes del mercado, que falsamenteconcluyó que el precio de una acción en la Bolsa de Nueva York difiere de su precio en otras bolsas. Esta desinformación desestabilizado el mercado.
5. El precio de una acción más rápido que ha cambiado, más fuera de la Bolsa de Nueva York caótico cita sería. Por lo tanto la inestabilidad criados más inestabilidad, y el mercado se desplomaron.

https://freedom-to-tinker.com/blog/felten/stock-market-flash-crash-attack-bug-or-gamesmanship

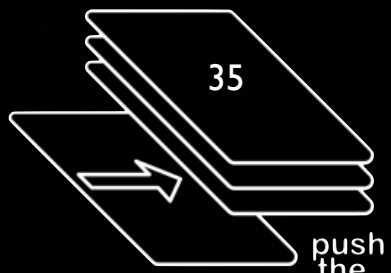
cuestionar la confianza

- ¿Es posible confiar en este marco?
- cómo asegurarse de que usted vigile las amenazas?



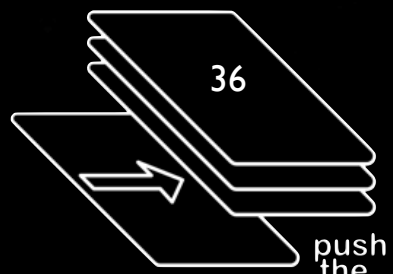
de seguridad tradicionales falla

- 100.000 veces demasiado lento
- dispuestos a aprender que éste es un mundo fundamentalmente diferente
- todavía se centra en cumplimiento



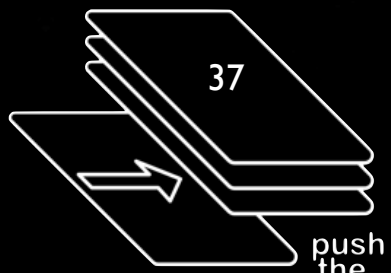
responder a la pregunta difícil - más tarde

- cómo asegurar que todo personalizado?
- cómo ser lo suficientemente rápido
- cómo hacer que el caso de que los esfuerzos de seguridad reducen el riesgo y evitar los desastres



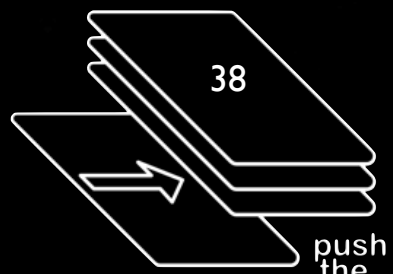
hacer algo!

- No estoy hablando de cosas duras como la revisión del código, la costumbrefirewalls a nivel de aplicación, cosas misteriosas FPGA ...
- El partido como si fuera 1999 - FUNDAMENTOS DE LA RED DE SEGURIDAD
- pon attencion capa 4

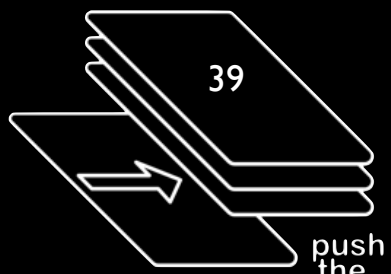


Seguridad de TI la nueva generación

- ¿dónde está la próxima generación que viene ...
- Juniper y Cisco son un buen comienzo ...
- cosas raras gravemente personalizado es un comienzo ...
- ¿por qué no estamos al día?

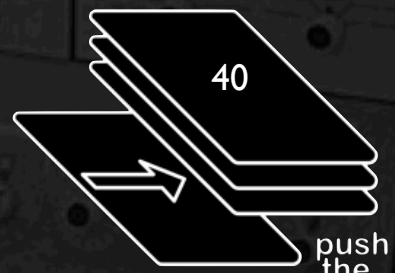


Bueno, gracias.
¿Y ahora qué?



HACER NADA

- en este punto - acelerar - cualquier cosa
- suena tan terrible decir esto, pero incluso el desarrollo de una comprensión dela arquitectura es mejor que nada
- hacer amigos e influenciar personas



HACER NADA

Most IT Security Pros Disabling Security Functions In Favor Of Network Speed

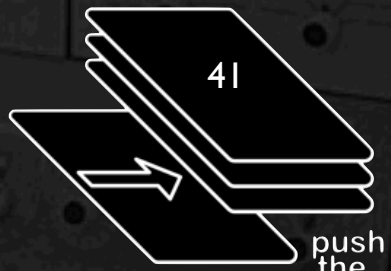
New survey shows dilemma faced by organizations over performance trade-offs with network security products

Jul 21, 2011 | 10:03 AM | 1 Comments

By Kelly Jackson Higgins
Dark Reading

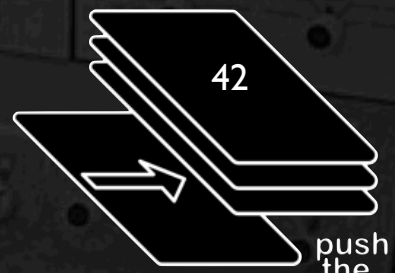
- usted está en el registro como decir que usted elegiría el rendimiento de la seguridad ...

http://www.darkreading.com/vulnerability-management/167901026/security/perimeter-security/231002280/most-it-security-pros-



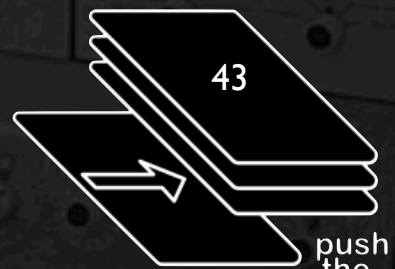
proveedores de productos ...

- tiempo de desafiar a sus proveedores
- desea más casillas de verificación
- hay otros mercados, además de cumplimiento de las tarjetas de crédito
- no hay dinero para gastar en cualquier cosa exótica que desea desarrollar



proveedores de productos ...

- Algunos proveedores de productos está recibiendo esta.
- La mayoría no lo son.
- Debido a que estamos "¿¡no preguntar por ella?!"

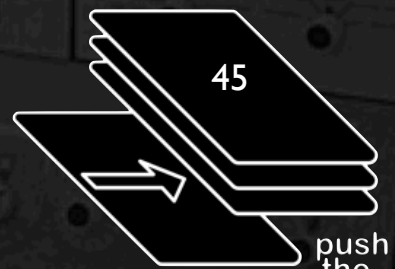


riesgo / proceso / policy / grc

- trabajar con la gente de su negocio
- que entiendan los riesgos - probablemente mejor que usted
- tienen diferente tolerancia al riesgo
- a entender cómo usar sus conocimientos para ayudarle a tomar buenas decisiones
- No seguir ciegamente las afirmaciones dogmáticas

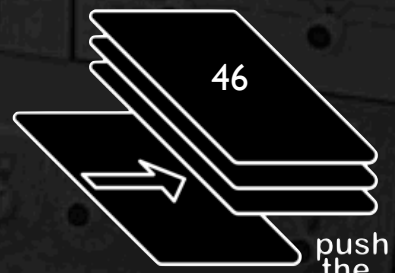
riesgo / proceso / policy / grc

- No vamos a ser capaces de cambiar de opinión sobre el costo de la latencia.
- Usted puede trabajar con ellos para cambiar su comprensión de cómo hacer las cosas.
- Sólo porque usted lo hizo de esa manera el año pasado no quiere decir quesigue siendo la mejor opción.



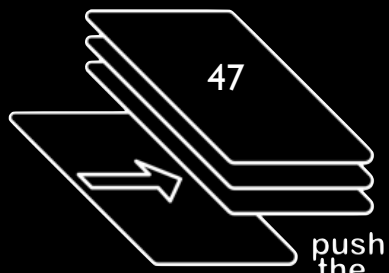
conformidad

- La gente de TI de cumplimiento, conocer a la gente el cumplimiento financiero -usted tiene cosas de que hablar.



conformidad

- La SEC está tomando un interés activo
- 26 de julio 2011 El anuncio de la Regla de información de grandes comerciantes (13h-1) http://sec.gov/news/press/2011/2011-154.htm
- Hay más por venir - otros reguladores están viendo.

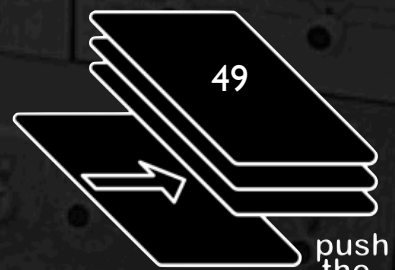


en las trincheras

INVESTIGACIÓN ORIGINAL

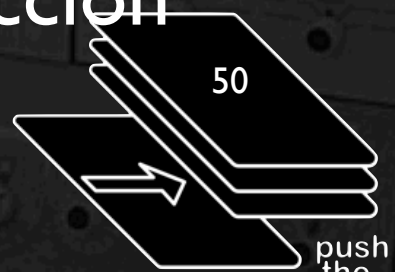
en las trincheras

- entender las necesidades de sus socios de negocios
- la búsqueda de soluciones
- construcción de plataformas de PoC para poner a prueba

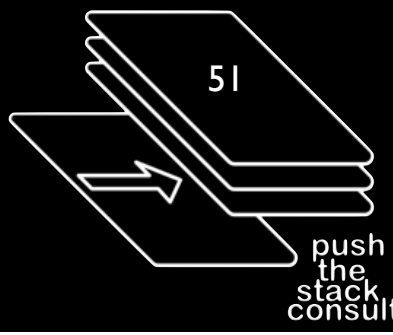


en las trincheras

- alentar a los proveedores para a hacer su trabajo
- pasar el tiempo mirando a las cosas realmente extrañas
- estar preparado para la continua presión sobre los tiempos de transacción

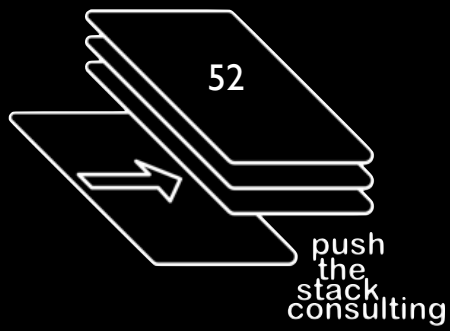


¡No se asuste!



Preguntas y Respuestas

twitter: @myrcurial
james.arlen@pushthestack.com



Créditos, Enlaces y Noticias

gracias: Todos ustedes, especialmente Ed Rojas, el pueblo de Colombia
Mis amigos, mi familia.

colofón: Twitter, wikipedia, la música rápida, la cafeína, a mi bella esposa y los niñoshackerish, luces Blinky, cosas brillantes, la angustia, el modafinil y el altruismo.

Me: http://myrcurial.com http://doinginfosecright.com
http://securosis.com http://liquidmatrix.org

créditos:
Chicago Board of Trade Image: Daniel Schwen
IBM Mainframe Image: ChineseJetPilot
New York Stock Exchange Image: Randy Le'Moine Photography
Toronto Stock Exchange Image: Jenny Lee Silver