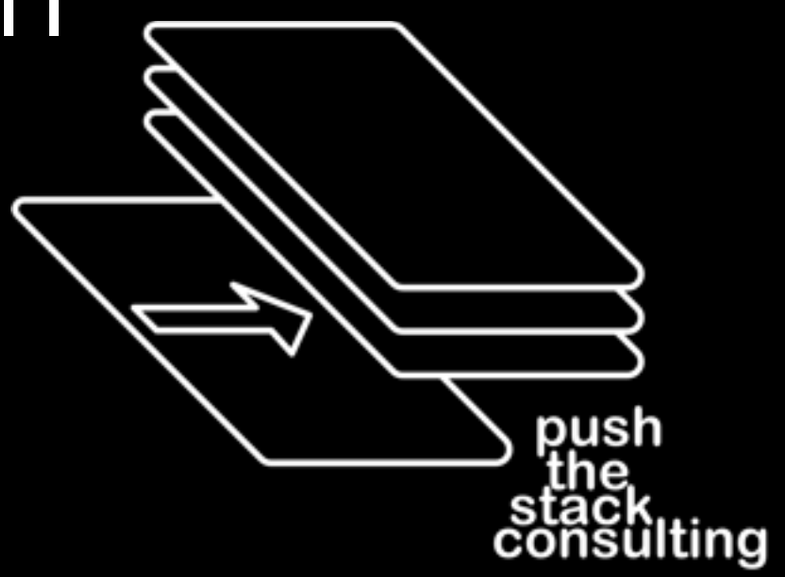
security when nanoseconds count

James Arlen, CISA

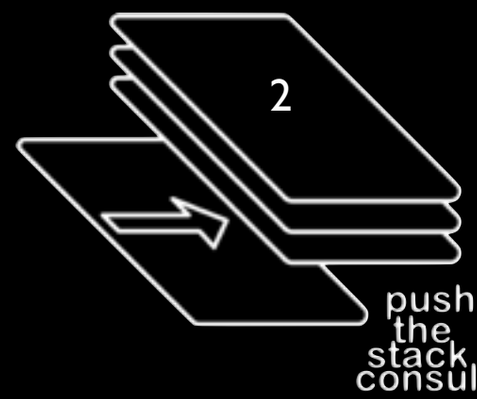
Blackhat USA - Briefings - 2011



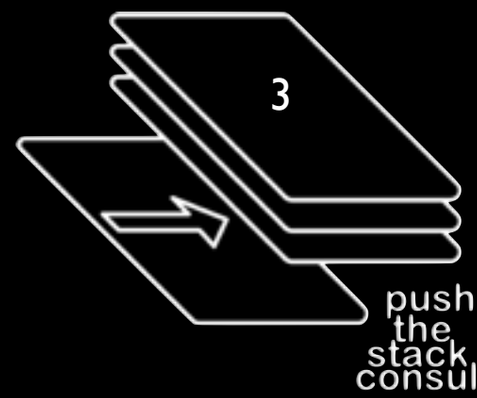
disclaimer

I am employed in the Infosec industry, but not authorized to speak on behalf of my employer or clients.

Everything I say can be blamed on the voices in *your* head.



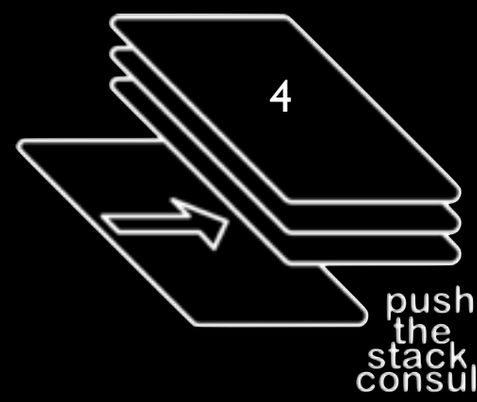
Please turn in your completed feedback form at the registration desk.



credentials

- 15+ years information security specialist
- staff operations, consultant, auditor, researcher
- utilities vertical (grid operations, generation, distribution)
- financial vertical (banks, trust companies, trading)
- some hacker related stuff (founder of think|haus)

...still not an expert at anything.



nanoseconds...

Admiral Hopper says...

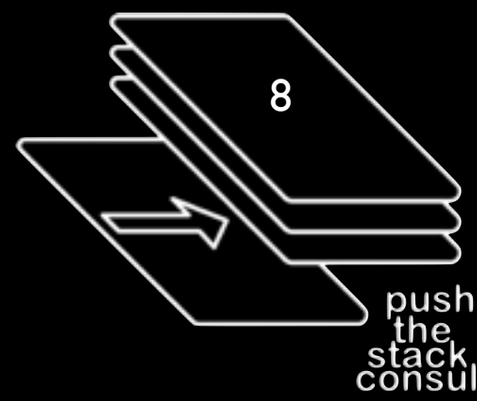
From an interview segment by Morley Safer in 1982

$=c (speed of light matters)

- distance light travels in a:
- millisecond ~300km (~186 miles)
- microsecond ~300m (~328 yards)
- nanosecond ~30cm (~1 foot)

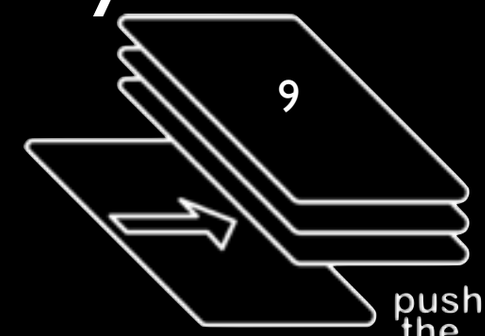
before you ask...

- This is a talk about... $$
- I'm not going to mention any of those things on your buzz-word bingo card:
  - SCADA
  - APT
  - PCI - DSS
  - wikileaks
  - (anti-|lulz)sec
  - hacktivism
  - ...insert more here.



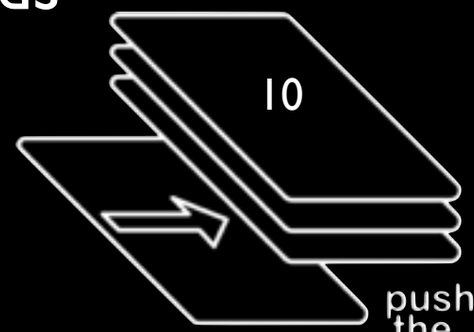
finance at blackhat?

- You know it!
- Blackhat is all about offensive and defensive techniques and technologies
- Sometimes, knowing that a vulnerability exists to be exploited helps to focus attention.
- Sometimes, people like me tell you things that sound completely crazy but have a history of coming true.



trading history

- 1200s - Commodity and Debt trading
- 1500s - Inter-market trading
- 1600s - Equity trading
- early 1800s - Reuters uses carrier pigeons
- late 1800s - electronic ticker tape (market data feeds) become widespread
- mid 1900s - quotation systems (next price rather than last price) become widespread
- late 1900s - computers are used to maintain the records of the exchange
- early 2000s - computers begin trading with each other without human intervention



definitions

- high speed trading: committing trades on a scale *faster* than human interactive speeds
- algorithmic trading: trades based on the mathematical result of incoming information from external sources (news, market data, etc.)

arbitrage

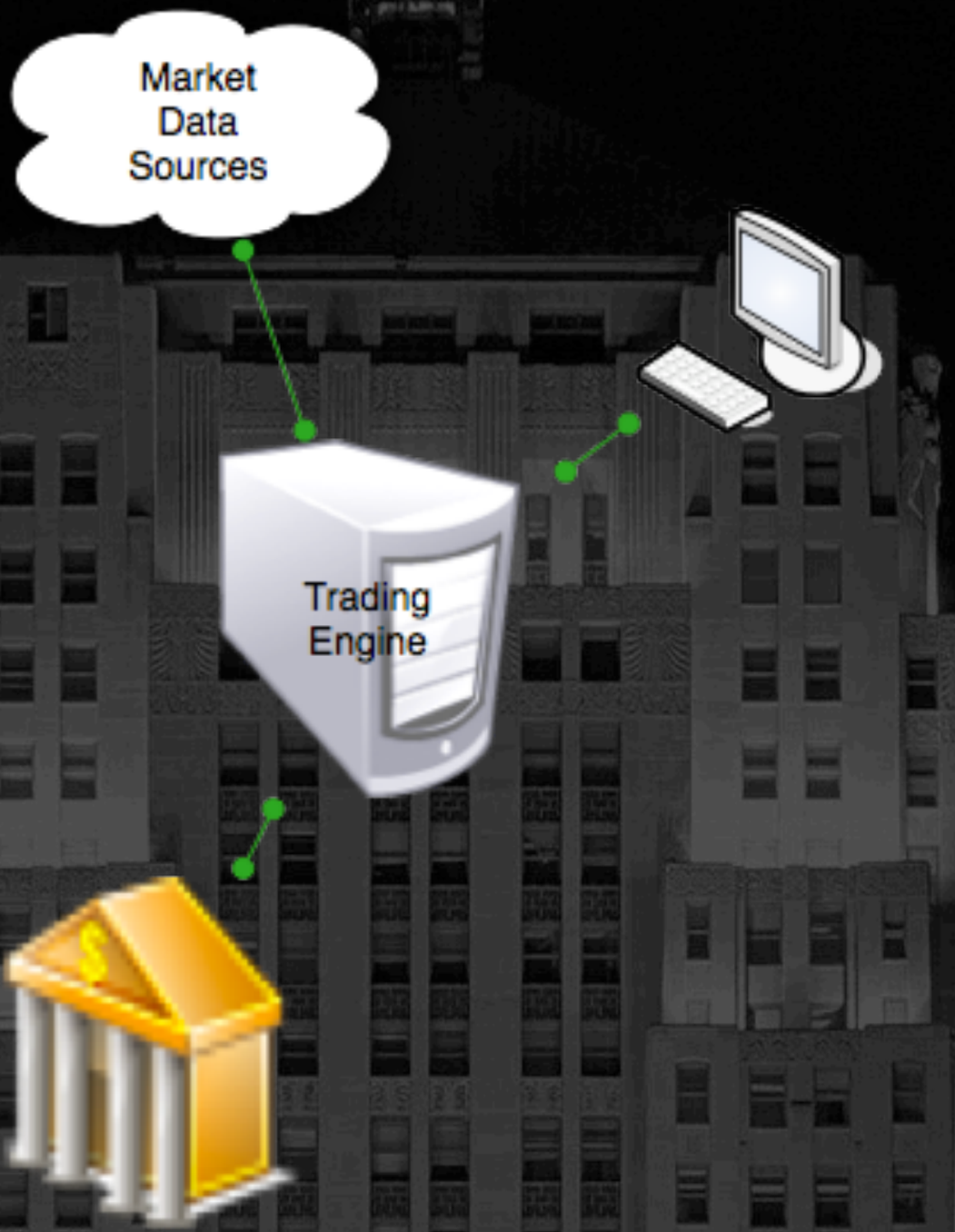
the practice of taking advantage of a price difference between two or more markets: striking a combination of matching deals that capitalize upon the imbalance, the profit being the difference between the market prices.

- in space - between two geographically separated markets
- in time - between the moment information is available and the moment information is widely known

time

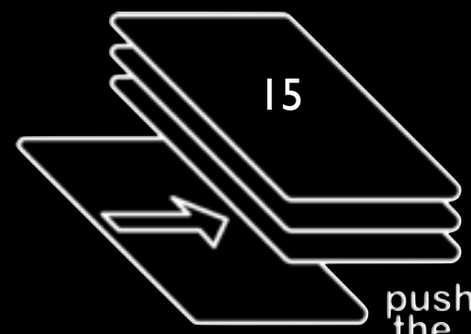
- when markets were new (middle of last millennium) trade times were measured at a very human scale
- late 1800s brought trade times to minutes
- 1900s brought trade times to seconds
- 2000s bring trade times in 100s of microseconds
- *Future trade times may well involve tachyon emissions*

architecture



how fast is fast?

- seconds: you have no position
- milliseconds: you lose nearly every time
- sub-millisecond: big players regularly beat you
- 100s of microseconds: you're a bit player and missing a lot
- 10s of microseconds: you're usually winning



predictability

- Almost as important as sheer speed is predictable speed.
- Enemies are: jitter, packet loss, inefficient protocols (tcp)
- Dropped packet is dropped cash

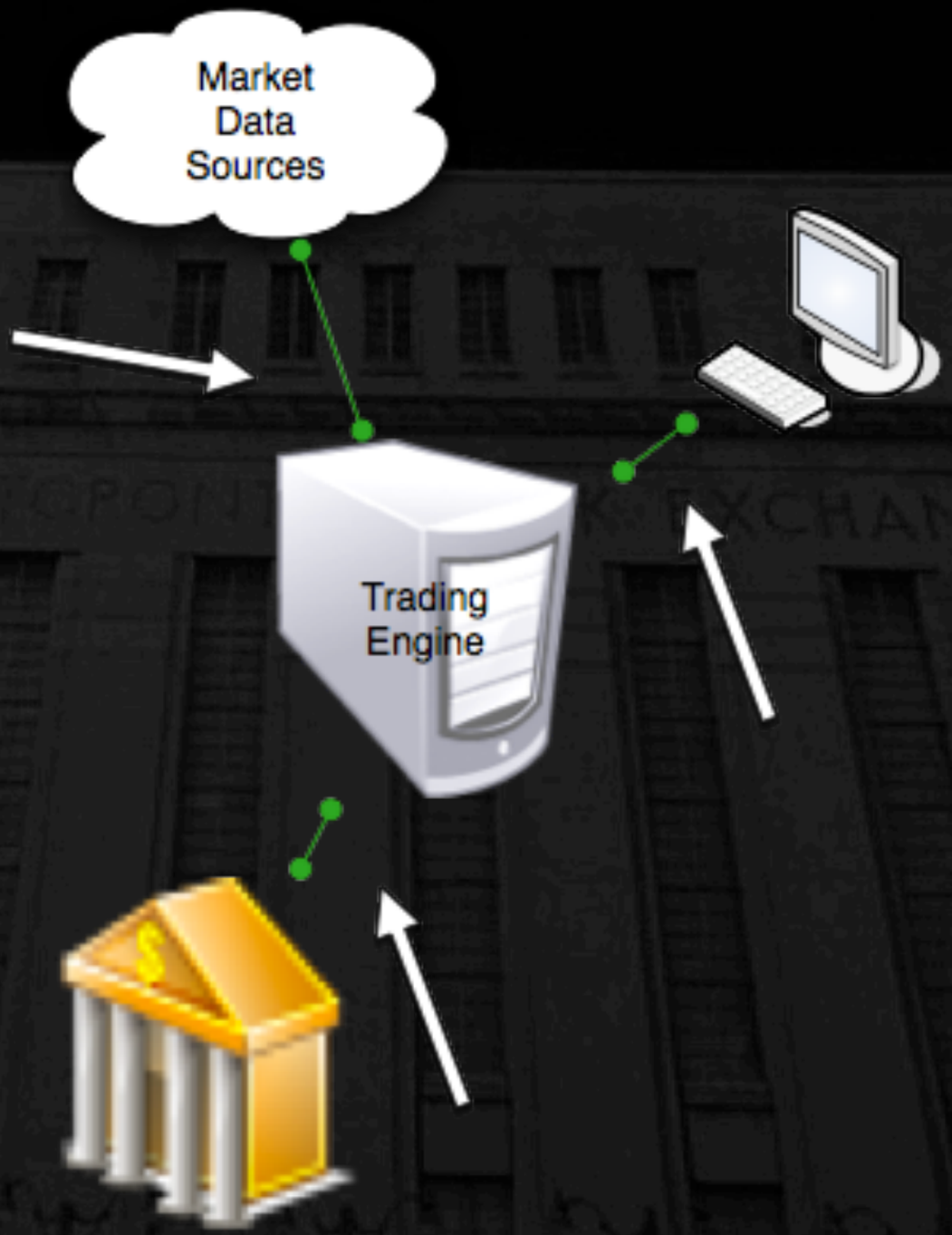
proximity

- Proximity relieves many of the speed/latency/ jitter effects
- You're on the LAN, not the MAN or the WAN

latency costs $

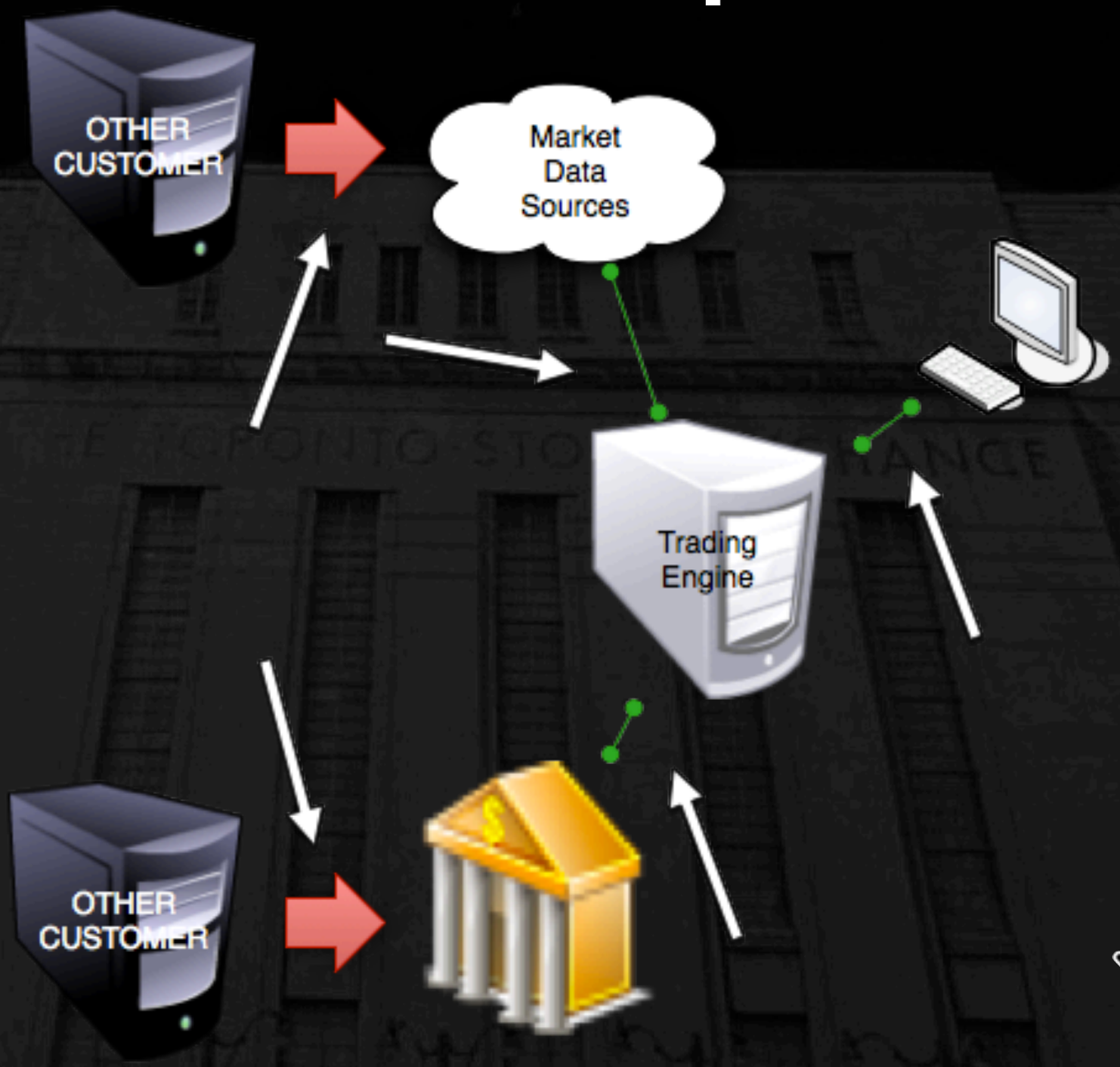
- latency has a $$cost associated with it - measurable and therefore fundable

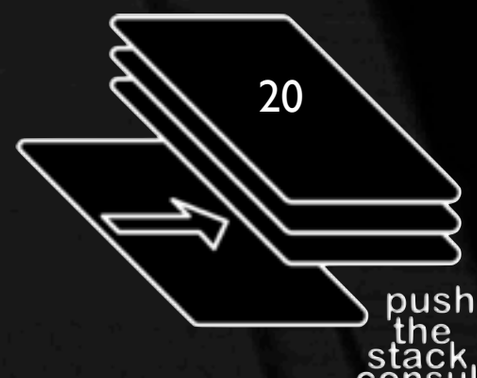
missing?



push the stack consulting

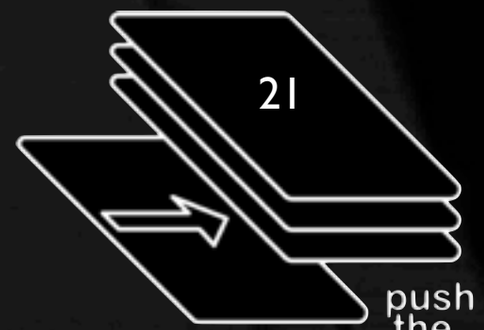
oh crap.


OTHER CUSTOMER
Market Data Sources
Trading Engine
OTHER CUSTOMER


20
push the stack
consulting

dude, where's my firewall?

- no firewalls...
- they add latency (a lot of latency)
- latency costs $
- risk < cost < profit



acl me please?

- no acls
- they add latency
- *(most)* switches can't cut through switch while acls are on
- risk < cost < profit

harden this...

- no *(meaningful)* system hardening
  - reduced system loading (stripped bare)
  - largely custom interfacing code (ethernet / infiniband / PCIe)
  - and the usual complaints about maintainability and problem resolution

Specialized Systems

Mellanox TECHNOLOGIES

RED KITE AMERICAS

SUNGARD

Extol

Corvil

B2BITS | <epam>

MACD

TradingScreen SIMPLIFYING GLOBAL MARKETS

FIXNETIX The ultimate trading advantage

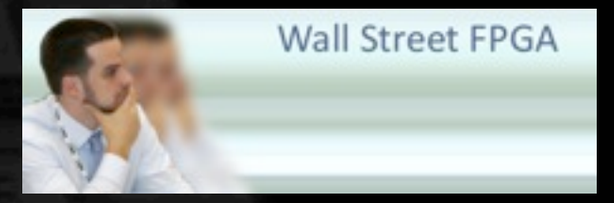
NYSE Euronext

ETNA SOFTWARE

ACTUARE SOFTWARE

JET·TEK FIX

abaxs



Fidessa Trade/Invest/Inform

abcmultiactive

PRIMARY SERVICES, SOLUTIONS AND TECHNOLOGY

activ FINANCIAL

EZX

Pravega Low Latency, Performance Driven

SNiXS.BIZ

CAMERON

Assimilate Technology

FIX Flyer™

koe

DEVEXPERTS

ats

PANTOR ENGINEERING

patsystems powers trades. builds exchanges. manages risk.

4SIGHT FINANCIAL SOFTWARE

ullink Connect. Trade.

FIRST FUTURES SOFTWARE

push the stack consulting

threat modelling

- we know what's missing in our usual suite of controls
- how do we describe it?
- how do we determine what is a reasonable threat to build protective measures against?

THREAT: vendors

- You're trusting that the marketing slick is what you'll get.
- You're trusting that they haven't hired any bad guys.

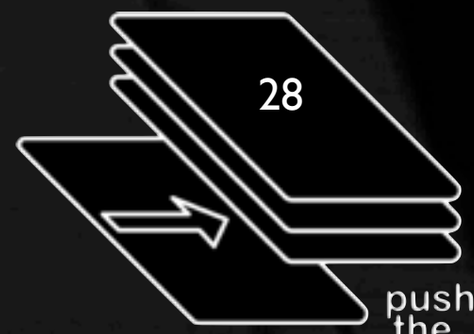
MAYBE: vendors

- How about a vendor developer who alters the patches you receive so that the Precision Time Protocol (PTPv2 - 802.1AS) has a different concept of a microsecond from the one everyone else is using?

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

THREAT: developers

- In most algo-trading, the developer isn't a traditional developer with all of the usual SDLC controls
- The developer is probably a trader or a trader underling who has live access to the production algo engine and can make on-the-fly changes



YES: Developers

- Sergey Aleynikov
  July 3, 2009
  http://www.wired.com/threatlevel/2009/07/aleynikov/

  - 32 MEGABYTES of code from Goldman Sachs

  - sentenced to 97 months in prison (8 years 1 month) and $12,500 fine

http://www.facebook.com/group.php?gid=123550517320

THREAT: the insider

- not *that* kind of insider
- how do you deal with a trader (or administrator) who is utilizing access to market data networks or exchange networks to cause negative effects on other participants?

YES: Traders

- Samarth Agrawal
  April 16, 2010
  http://www.wired.com/threatlevel/2010/04/bankerarrested/

- several hundred pages of code from Societe Generale

- sentenced to 3 years in prison + 2 years supervised release + deportation

THREAT: the market

- This is an odd kind of technical threat
- Can the market itself cause issues with your systems?
- malformed messages
- transaction risk scrutiny
- compromised systems

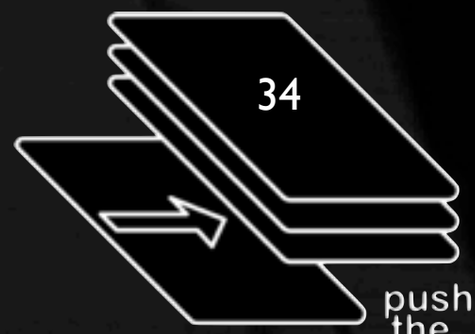
YES: Market

- 2010-05-06 - DJIA drops 900 points in minutes -- THE FLASH CRASH
- Report from Nanex
  http://www.nanex.net/20100506/FlashCrashAnalysis_Part1-1.html

Ed Felten's Summary

1. Some market participants sent a large number of quote requests to the New York Stock Exchange (NYSE) computers.
2. The NYSE normally puts outgoing price quotes into a queue before they are sent out. Because of the high rate of requests, this queue backed up, so that some quotes took a (relatively) long time to be sent out.
3. A quote lists a price and a time. The NYSE determined the price at the time the quote was put into the queue, and timestamped each quote at the time it left the queue. When the queues backed up, these quotes would be "stale", in the sense that they had an old, no-longer-accurate price --- but their timestamps made them look like up-to-date quotes.
4. These anomalous quotes confused other market participants, who falsely concluded that a stock's price on the NYSE differed from its price on other exchanges. This misinformation destabilized the market.
5. The faster a stock's price changed, the more out-of-kilter the NYSE quotes would be. So instability bred more instability, and the market dropped precipitously.

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



questioning trust

- is it even possible to trust within this framework?
- how to ensure that you monitor the threats?

traditional security fails

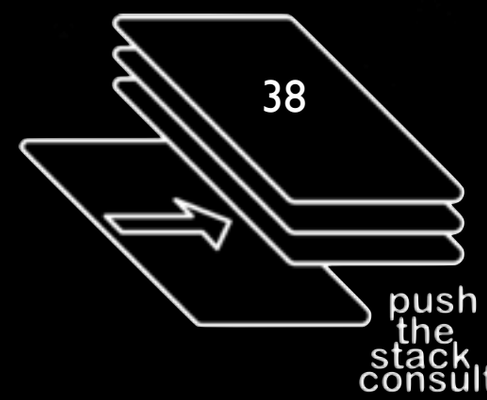
- 100,000 times too slow
- unwilling to learn that this is a fundamentally different world
- still focused on checkbox compliance

answer the hard one - later

- how to secure custom everything?
- how to be fast enough
- how to make the case that security efforts reduce risk and preclude disaster

do something!

- I'm not talking about hard stuff like code review, custom application level firewalls, mysterious FPGA stuff...
- Party like it's 1999 -- NETWORK SECURITY BASICS
- even a little bit of Layer 4 goodness would help

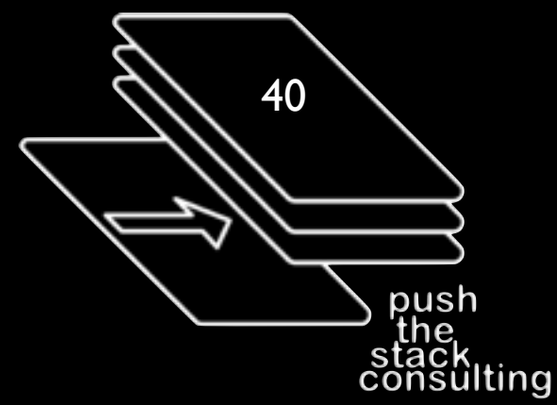


ITSecurity:TNG

- where's the next next generation...
- juniper and cisco are a start...
- weird severely custom stuff is a start...
- why aren't we aren't keeping up?

Well, thanks.

What now?



DO ANYTHING

- at this point - step up - do *anything*
- it sounds so terrible to say that but even developing an architectural understanding is better than nothing
- make friends and influence people

DO ANYTHING

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

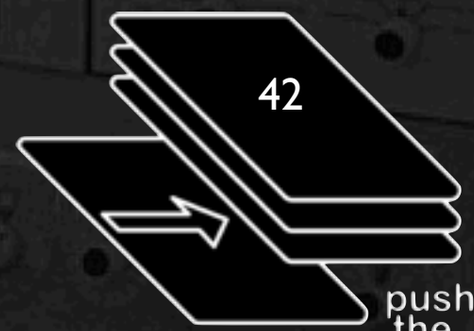
New survey shows dilemma faced by organizations over performance trade-offs with network security products

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

By Kelly Jackson Higgins
Dark Reading

- you're on the record as saying that you'd choose performance over security...

http://www.darkreading.com/vulnerability-management/167901026/security/perimeter-security/231002280/most-it-security-pros-disabling-security-functions-in-favor-of-network-speed.html (July 21, 2011)



product vendors...

- time to challenge your vendors
- you want more than checkboxes
- there are other markets besides credit card compliance
- there is money to spend on whatever exotic thing you want to develop

product vendors...

- Some product vendors are getting this.
- Most aren't.
- Because we're "not asking for it"!?!

risk / process / policy / grc

- work with your business folks
- they understand risk - probably better than you do
- they have a different tolerance for risk
- understand how to use their knowledge to help you make good decisions
- do not blindly follow dogmatic statements

risk / process / policy / grc

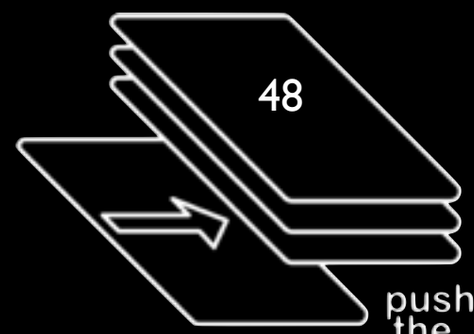
- You're not going to be able to change their minds about the cost of latency.
- You can work with them to change your understanding of how to do things.
- Just because you did it that way last year doesn't mean that's still the best option.

compliance

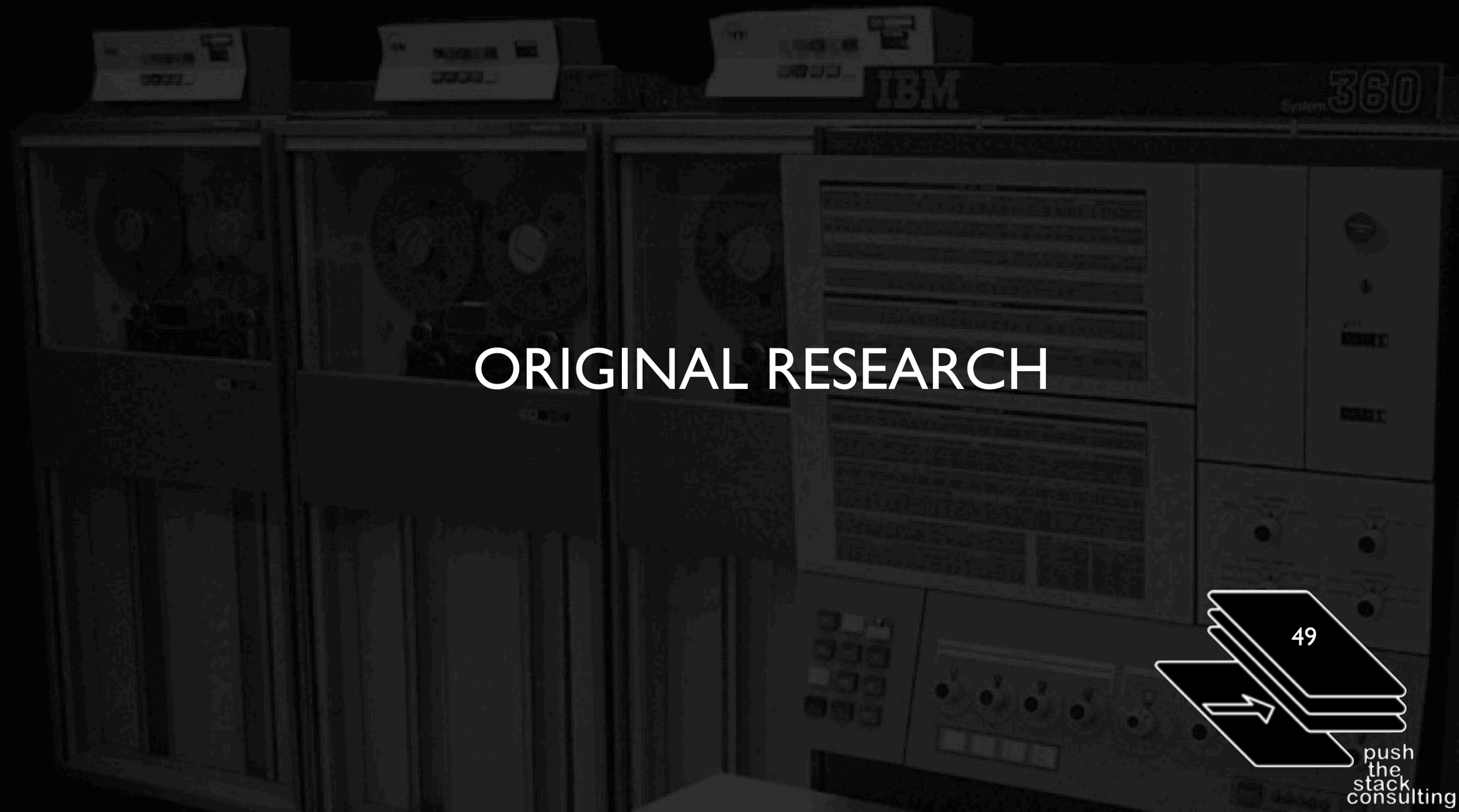
- IT compliance people, meet the financial compliance people - you have things to talk about.

compliance

- The SEC is taking an active interest
- July 26, 2011 announcement of the Large Trader Reporting Rule (13h-1)
  http://sec.gov/news/press/2011/2011-154.htm
- There is more to come - other regulators are watching.



in the trenches



ORIGINAL RESEARCH

push the stack consulting

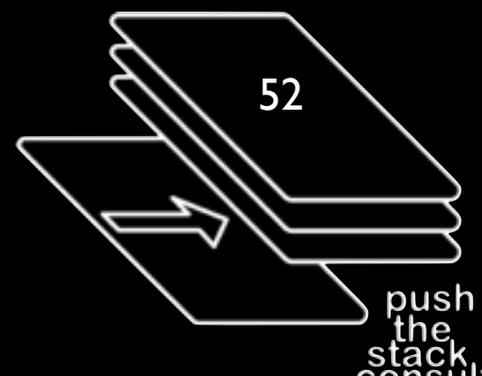
in the trenches

- understand your business partners' needs
- look for solutions
- build PoC rigs to test

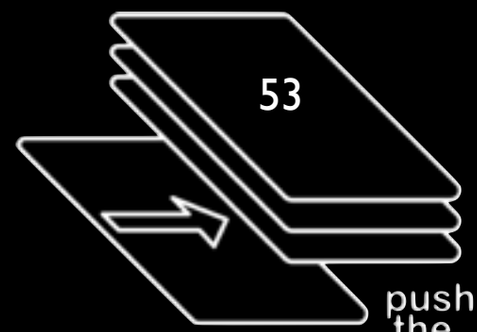
in the trenches

- encourage vendors to get with it
- spend time looking at the truly weird stuff
- be prepared for the continued downward pressure on transaction times

Don’t Panic

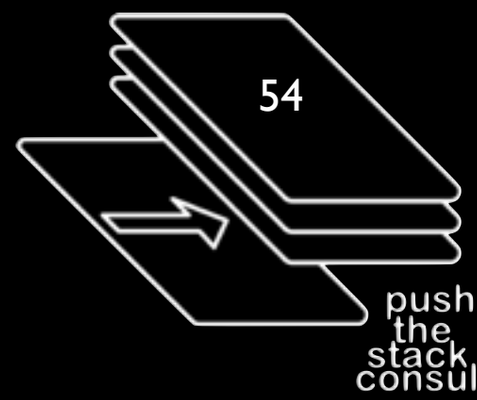


Please turn in your completed feedback form at the registration desk.



Q & A

twitter: @myrcurial
james.arlen@pushthestack.com



Credits, Links and Notices

Thanks: All of you, Jeff Moss & the Blackhat USA team, My Friends, My Family

Colophon: twitter, wikipedia, fast music, caffeine, my lovely wife and hackerish children, blinky lights, shiny things, angst, modafinil & altruism.

Me:

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

Credits:

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