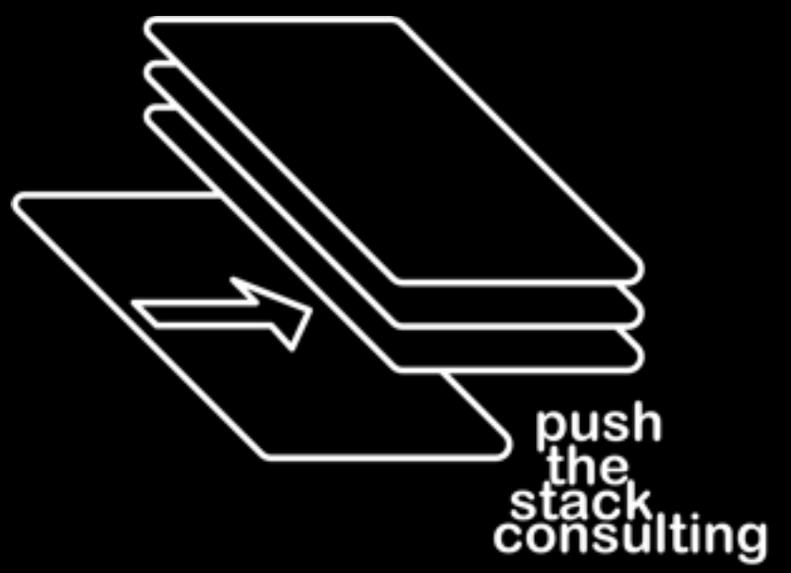
security when nanoseconds count

James Arlen, CISA

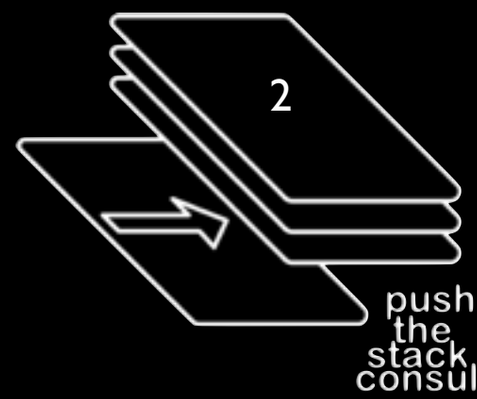
BH USA - Preview - 2011



disclaimer

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

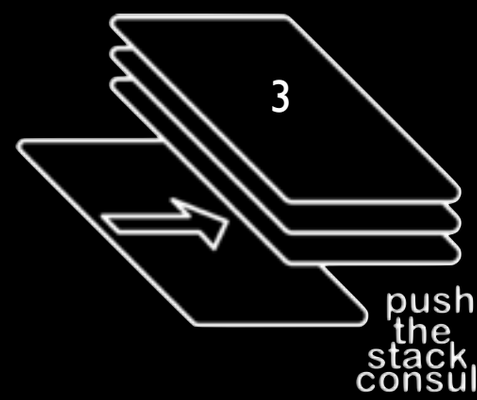
Everything I say can be blamed on the voices in *your* head.



credentials

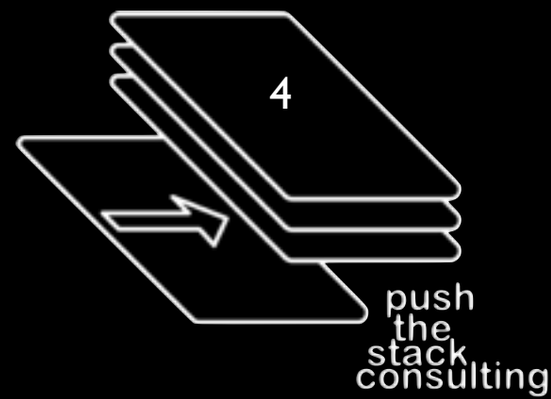
- 15+ years information security specialist
- staff operations, consultant, auditor, researcher
- utilities vertical (grid operations, generation, distribution)
- financial vertical (banks, trust companies, trading)
- some hacker related stuff (founder of think|haus)

...still not an expert at anything.



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

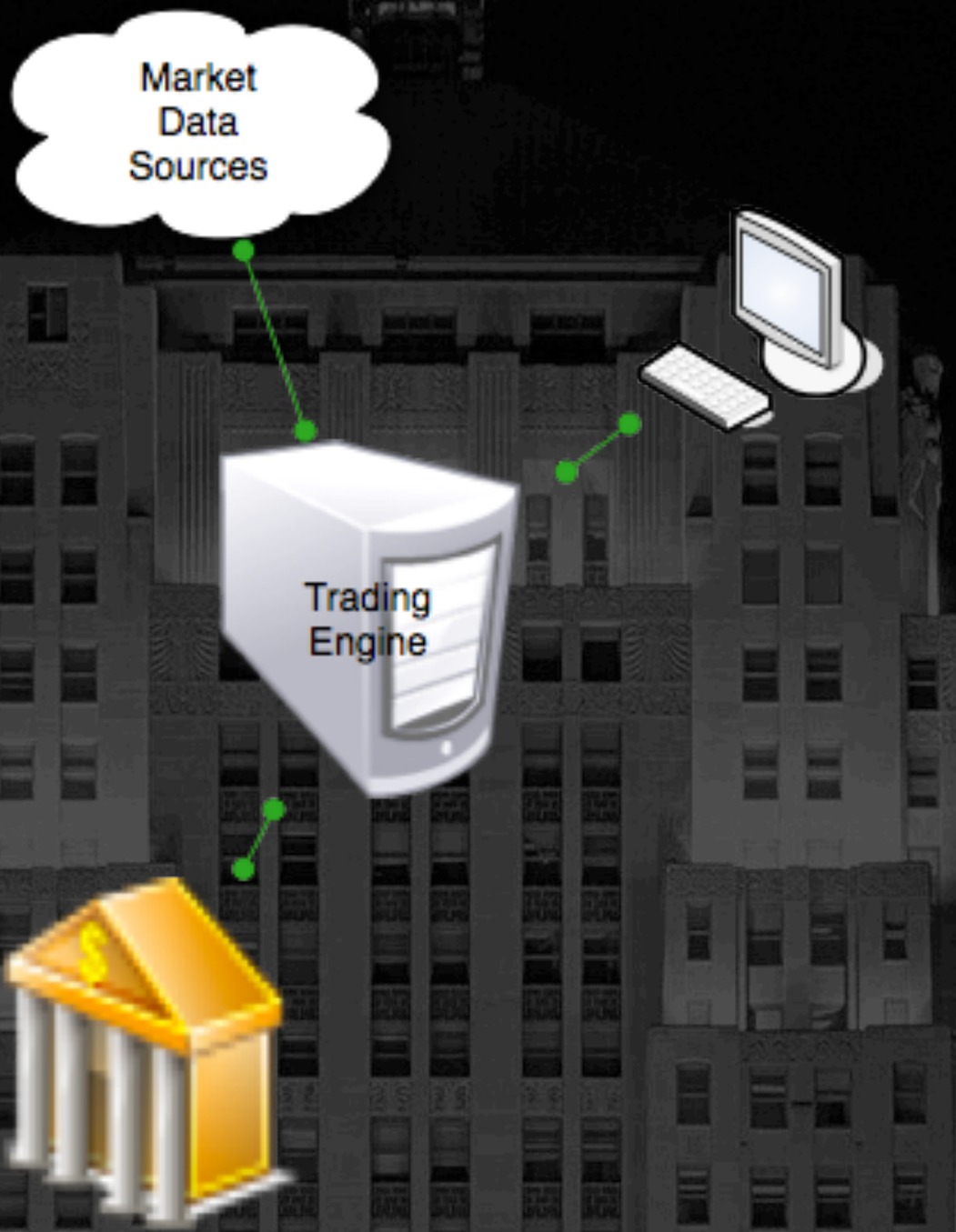
the practice of taking advantage of a price difference between two or more markets: striking a combination of matching deals that capitalize upon the imbalance, the profit being the difference between the market prices.

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

time

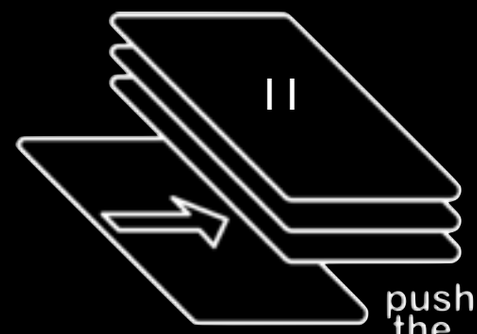
- when markets were new (middle of last millennium) trade times were measured at a very human scale
- late 1800s brought trade times to minutes
- 1900s brought trade times to seconds
- 2000s bring trade times in 100s of microseconds
- *Future trade times may well involve tachyon emissions*

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 $

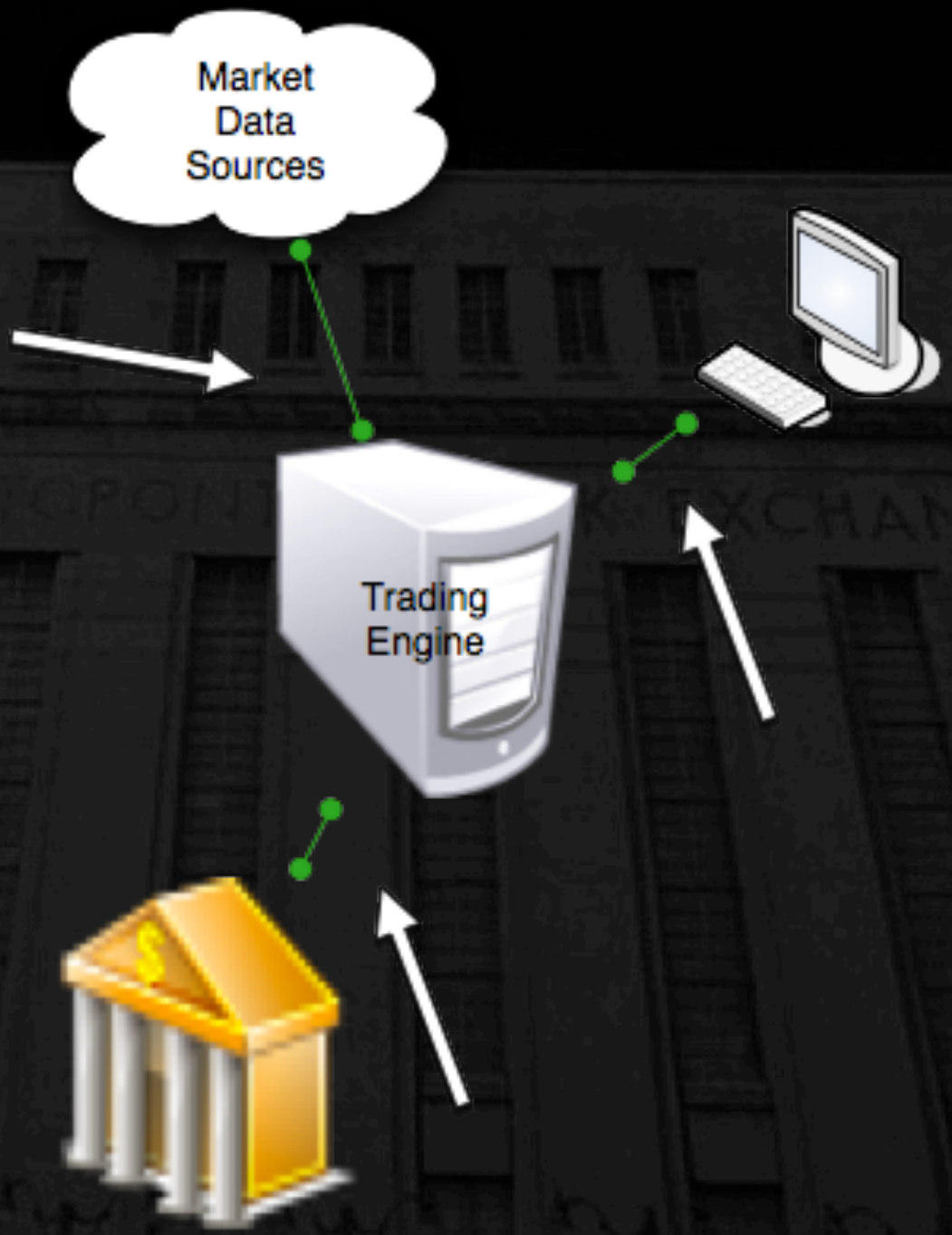
- latency has a $$cost associated with it - measurable and therefore fundable

$=c (speed of light matters)

distance light travels in a:

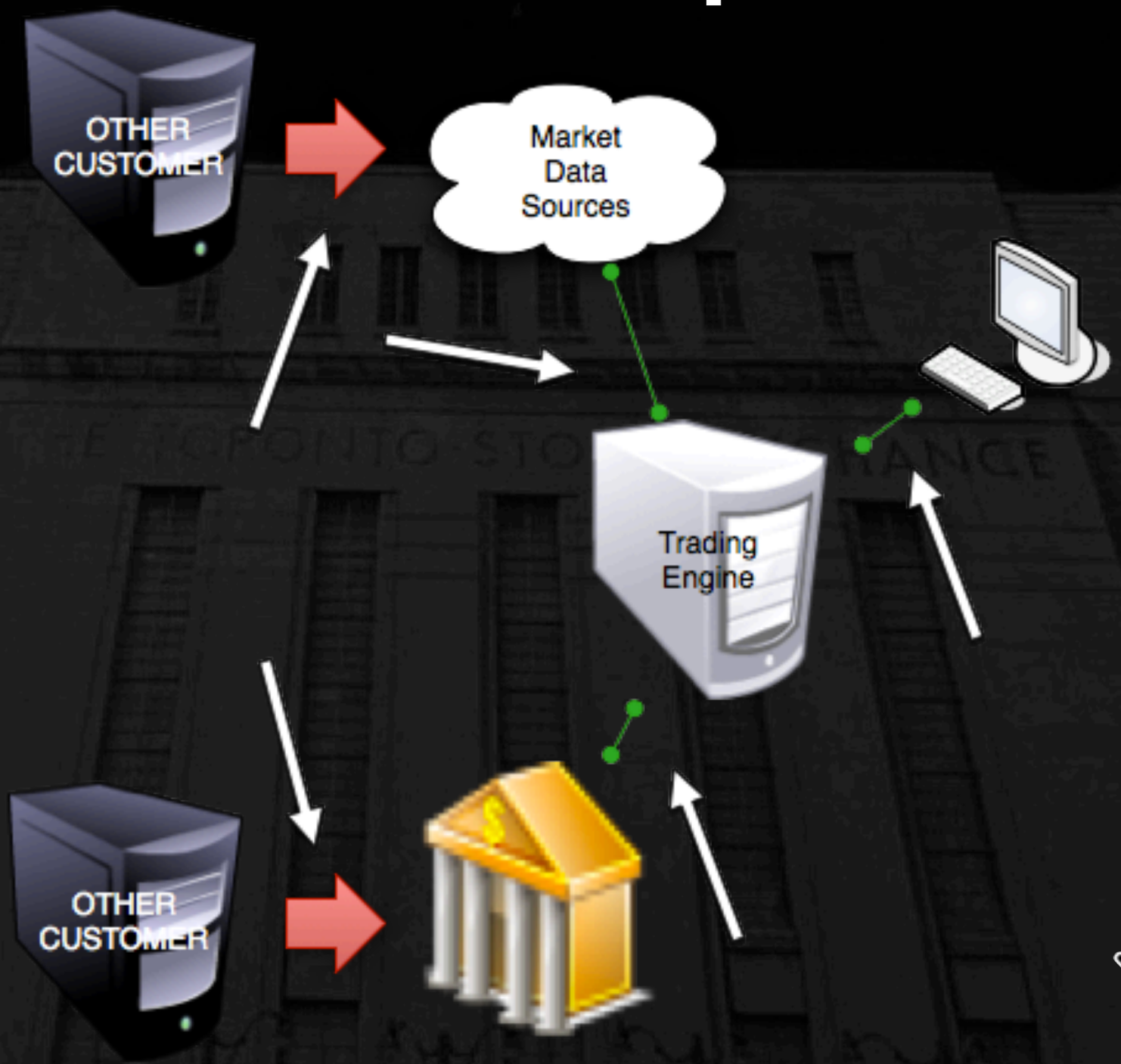
- millisecond ~300km (~186 miles)
- microsecond ~300m (~328 yards)
- nanosecond ~30cm (~1 foot)

missing?



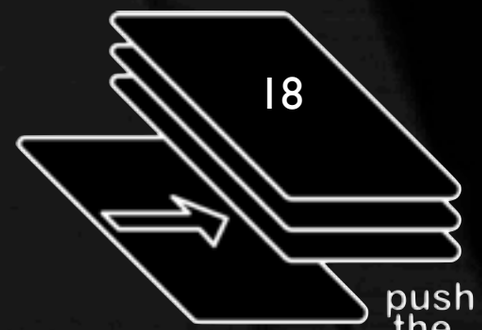
push the stack consulting

oh crap.


OTHER CUSTOMER
Market Data Sources
Trading Engine
OTHER CUSTOMER

dude, where's my firewall?

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

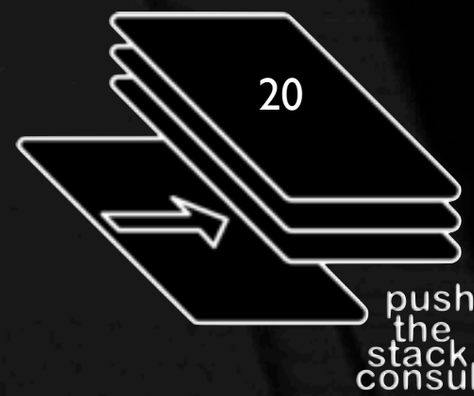


acl me please?

- 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



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: 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

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?

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

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

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

answer the hard one - later

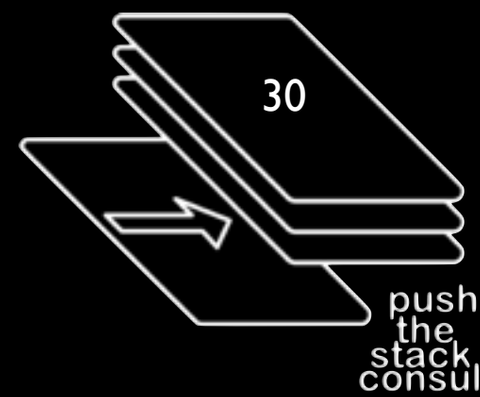
- how to secure custom everything?
- how to be fast enough
- how to make the case that security efforts reduce risk and preclude disaster

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?

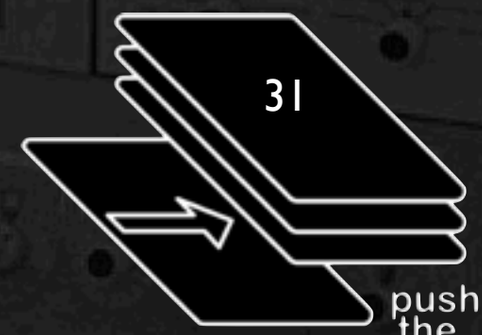
Well, thanks.

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



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

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

compliance

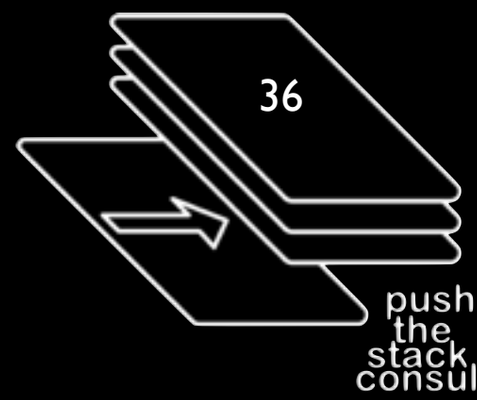
- IT compliance people, meet the financial compliance people - you have things to talk about.

in the trenches

- research everything
- understand your business partners' needs
- look for solutions
- build PoC rigs to test
- encourage vendors to get with it
- spend time looking at the truly weird stuff
- be prepared for the continued downward pressure on transaction times

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