The New York Stock Exchange's recently-completed primary data center in Mahwah, NJ is protected by guarded entrances and high fences, but the GPS antennas on the center's roof draw unsecured civil GPS signals directly into the core of the exchange.

GPS Spoofing and the Financial Sector

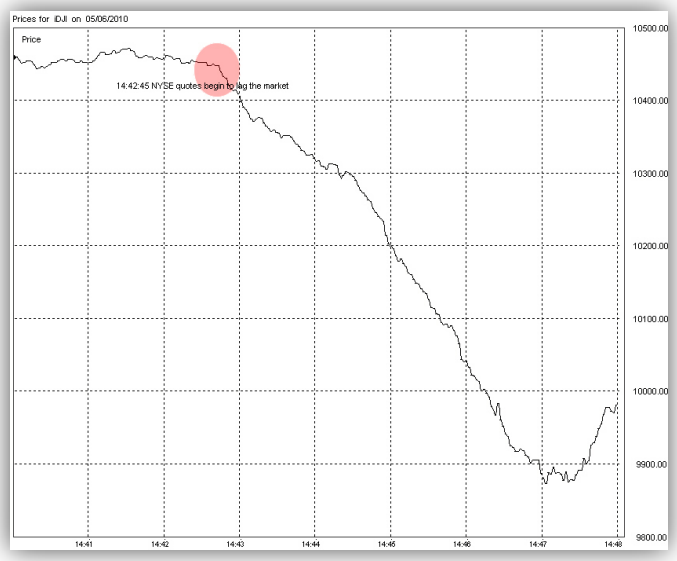
Todd Humphreys, The University of Texas at Austin, June 2011

All global financial exchanges, including the New York Stock Exchange (NYSE) and the Nasdaq, have gone digital. Large data centers hold the exchanges' matching engines—the modern-day equivalent of the historic trading floor—in racks of interconnected servers. The Department of Homeland Security considers these data centers critical national infrastructure. Private security personnel, tall fences, and the best network security money can buy protect the integrity of the thousands of high-stakes trades executed every second within these data centers.

But there is one input port that the network firewalls leave entirely unprotected. An unassuming set of antennas on the data center's roof carry unsecured civil GPS signals directly into the core of the matching engine network. Slaved to a once-per-second synchronization pulse from a GPS-locked timing card, the individual servers in the network apply time stamps to the trades they execute. A decade ago, a tenth of a second was an acceptable time stamp resolution. High frequency traders now demand nanoseconds.

What would happen if someone spoofed the civil GPS signals entering these data centers and manipulated the transaction time stamps? Three example scenarios are considered.

Timing and the Flash Crash



The red circle indicates when NYSE quotes began to lag the market just prior to the flash crash of May, 2010 (figure from Nanex).

On May 6, 2010, the Dow plummeted inexplicably in a 900-point "flash crash." Within minutes, the markets had almost completely recovered, but the episode sent chills through the financial world. What had gone wrong? Government and private teams pored over market data in an attempt to identify the trigger. The CFTC and the SEC produced a joint report in September of 2010 that faulted an overly aggressive automatic sell program which sold off $4.1 billion in contracts in just over 20 minutes. A liquidity crisis ensued and prices dropped. The report noted that there were some delays in market data dissemination, but concluded that these delays were more a symptom than a cause of the crash.

Other observers saw more significance in these delays. The private market data provider Nanex analyzed the flash crash and other similar "mini-crashes" and found a pattern. They noted that a sudden burst of buy or sell orders can cause the New York Stock Exchange's feed to the Consolidated Quote System (CQS) to saturate, which causes quote data to arrive at the CQS with a delay, sometimes milliseconds, sometimes seconds. But the quotes are time stamped as they leave the NYSE and not when the buy or sell actually takes place, so market participants have no way of knowing initially that the data are stale.

Nanex noted two consequences of stale quotes: crossed markets and market uncertainty.

Crossed Markets

When, for equivalent securities, one exchange bids higher than other exchanges are offering, or offers lower than others are bidding, it has "crossed" with the other markets. Exchanges assiduously avoid crossing each other because fast market participants will immediately punish them by buying at the lower ask price and selling at the higher bid price. Thus, under normal circumstances, it is rare to see markets crossed in stocks for more than a few milliseconds.

The Nanex analysis of the flash crash shows that the NYSE began to cross other markets just before the Dow began to plunge. Nanex pieced together the crash events and found that the NYSE quotes had crossed because they were stale, having been delayed in the NYSE feed to the CQS due to saturation of the feed. In other words, the NYSE was not actually crossed with other markets, but it appeared so because the CQS was comparing stale NYSE quotes to fresh quotes from the other exchanges. The result was increased sell pressure at the NYSE as traders bought from other exchanges and furiously attempted to sell at NYSE. But the sales were not executed at the delayed high bid quotes reported in the CQS; they were executed at the prompt lower quotes in the NYSE matching engines. The extreme sell pressure caused the NYSE's feed to the CQS to back up further still, eventually causing delays of up to 20 seconds for some symbols.

The lesson here is that improperly time-stamped quotes can cause markets to cross with each another, which in turn can lead to quote saturation and further delays in a nasty feedback effect. In the flash crash, it was a large sell order that initially triggered saturation in the NYSE's data queue and caused quote delays. But it appears quite possible that a GPS spoofing attack could trigger the same spurious market crossing by making one exchange's quote data appear late to the CQS. It would not be possible to introduce large (multiple-second) delays in an exchange's time stamps over a short time horizon, but it may nonetheless be possible to trigger a crossing that could lead to further delays as a burst in quote data builds up in an exchange's queues.

Market Uncertainty

High frequency traders (HFTs), whose automated transactions account for 50 to 70 percent of trading volume on major exchanges, don't like inexplicable market behavior; and, unlike old-fashioned traders who are obligated to stay in the market no matter its behavior, HFTs can pull the plug at any moment. In the aftermath of the flash crash, it was revealed that automatic data integrity checks in trading algorithms are often set to trigger on unusual latency in the exchanges' data feeds. In other words, if transaction time stamps don't look right, algorithmic traders flee the marketplace. A spoofing attack that aggressively manipulated an exchange's master clock would therefore cause a partial market vacuum – what traders call a loss of liquidity – with the result being increased price volatility and damage to market confidence.

Recognizing that time manipulation can scare away market participants, traders could use GPS spoofing as a weapon against each other. A trader could manipulate, via GPS spoofing, the timing of a competitor's trading engines, driving the competitor out of the marketplace during a crucial trading interval. After the attack, the rogue trader covers his tracks by bringing his competitor's timing back into proper alignment with true time. Such an attack would be extremely difficult to discover.

Skimming the Markets: Arbitrage via Time Manipulation

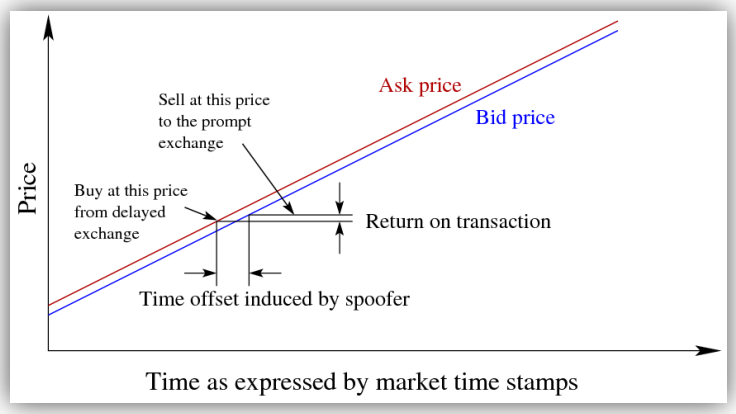


Illustration of a possible arbitrage scheme based on time stamp manipulation.

Some securities are jointly listed on multiple exchanges. Efficient markets tend to drive the price of these securities to equivalence, a condition called price parity. In other cases, securities listed at separate exchanges may not be exact substitutes but may be strongly correlated with one another. If the price of crude oil goes up at the NYSE, for example, so do gasoline futures on the Chicago board. Significant imbalance from price parity or from expected correlated security price movement opens up an opportunity to make a low-risk profit at zero cost. Traders call this arbitrage.

A decade ago, arbitrage opportunities were measured on time scales of days or weeks. With the emergence of high frequency trading, they are now measured in milliseconds. A nearly-straight fiber cable route was recently dug from Chicago to New York City at a cost of several hundred million dollars. The goal: shave 3 milliseconds off the previous route of lowest latency. In those 3 milliseconds, firms riding the new fiber route will complete arbitrage transactions ahead of their competitors. For arbitrage, timing is crucial.

Exploiting arbitrage opportunities requires a comparison of simultaneous prices. The fastest way to do this is to align the time stamps of the high-rate data feeds from separate exchanges. If price parity is maintained along time-aligned data feeds, then there are no arbitrage opportunities. Suppose, however, that a spoofer alters the time stamps at one of the exchanges. Then what appear to be time-aligned data feeds would actually be asynchronous by several milliseconds, concealing possible instantaneous prices mismatches. Presumably, no-one would be aware of this except those who initiated the spoofing attack; they alone could “skim the market” and profit by others’ ignorance of the actual price imbalance.

False Synchronicity: A Threat to Large Correlated Orders

Traders placing large correlated orders (e.g., a "buy" order for steel and timber for a new railway line) run the risk of pricing information being leaked to rival traders, increasing the chances that market prices will shift against them. In many cases, the large order must be broken up because the separate but correlated securities are best issued at different exchanges. To avoid price information from one part of the order from affecting another, traders time the placement of the orders so that they execute simultaneously at geographically separate exchanges. Traders estimate the latencies involved by sending out small advance orders and monitoring the time stamps applied to these orders as revealed in the exchanges' output data feeds.

A trader who mounts a spoofing attack could profit from large correlated orders by offsetting the timing of one exchange by several milliseconds—just enough time to register the receipt of the large order at the time-delayed exchange and buy or sell correlated securities at another exchange. The trader trying to achieve simultaneity at multiple exchanges will end up buying correlated securities at a higher price or selling them at a lower price than expected, with the difference going to the spoofer.

Further Reading

The full CFTC & SEC post-mortem report on the May, 2010 flash crash can be found here.

The Nanex flash crash summary report is here.

A discussion with high frequency traders on their decision to pull out of the market during the flash crash can be found here.

The Chicago-to-New York proprietary fiber run is discussed here.

The UT Radionavigation Laboratory website is: http://radionavlab.ae.utexas.edu