High Frequency Hacking

Some risks of the modern trading practices

Tadej Vodopivec, CISSP, CISA, CBCP
Information Security Consultant
ComTrade d.o.o.
ime.priimek AT see above d.o.o. DOT com

OWASP

September 15, 2011 - Ljubljana, Slovenia

The OWASP Foundation
http://www.owasp.org

Agenda

- The true story – Flash Crash of the May 6th, 2010
- High Frequecy Trading
- Known Issues
- Less Discussed Issues
- Not trading?
  Never mind, they trade on you...

May 6, 2010 - Flash Crash

Some links related to Flash Crash

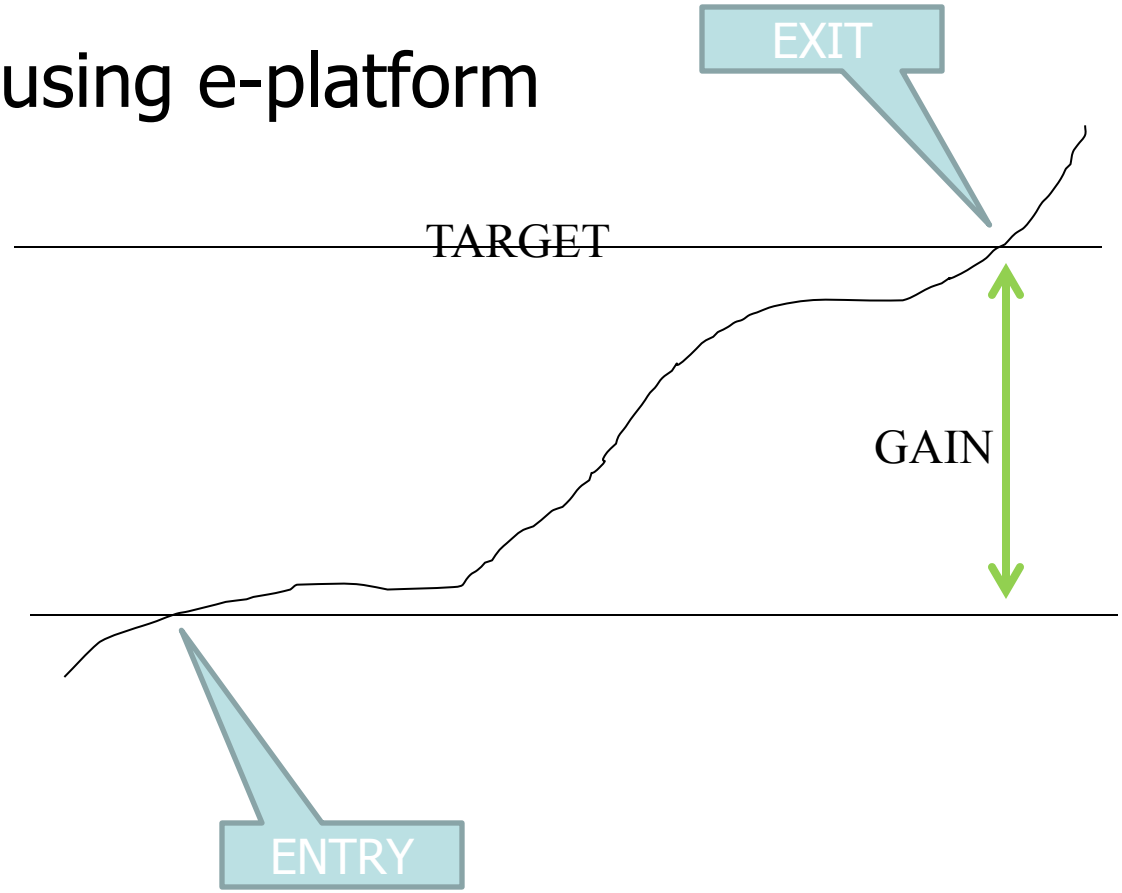
- CFTC-SEC report http://www.sec.gov/news/studies/2010/marketevents-report.pdf
- Nanex: http://www.nanex.net/FlashCrash/FlashCrashAnalysis.html
  - In contrast to CFTC-SEC, they focus on data analysis rather than interviews
  - incorrect data feeds were important (saturation – incorrect price)
  - Original 75k E-Mini sale was not a problem, but subsequent re-sales of the HFT parties that initially absorbed the selling presure

High Frequecy Trading

- The true story – Flash Crash of the May 6th, 2010
- **High Frequecy Trading**
- Known Issues
- Less Discussed Issues
- Not trading?
  Never mind, they trade on you...

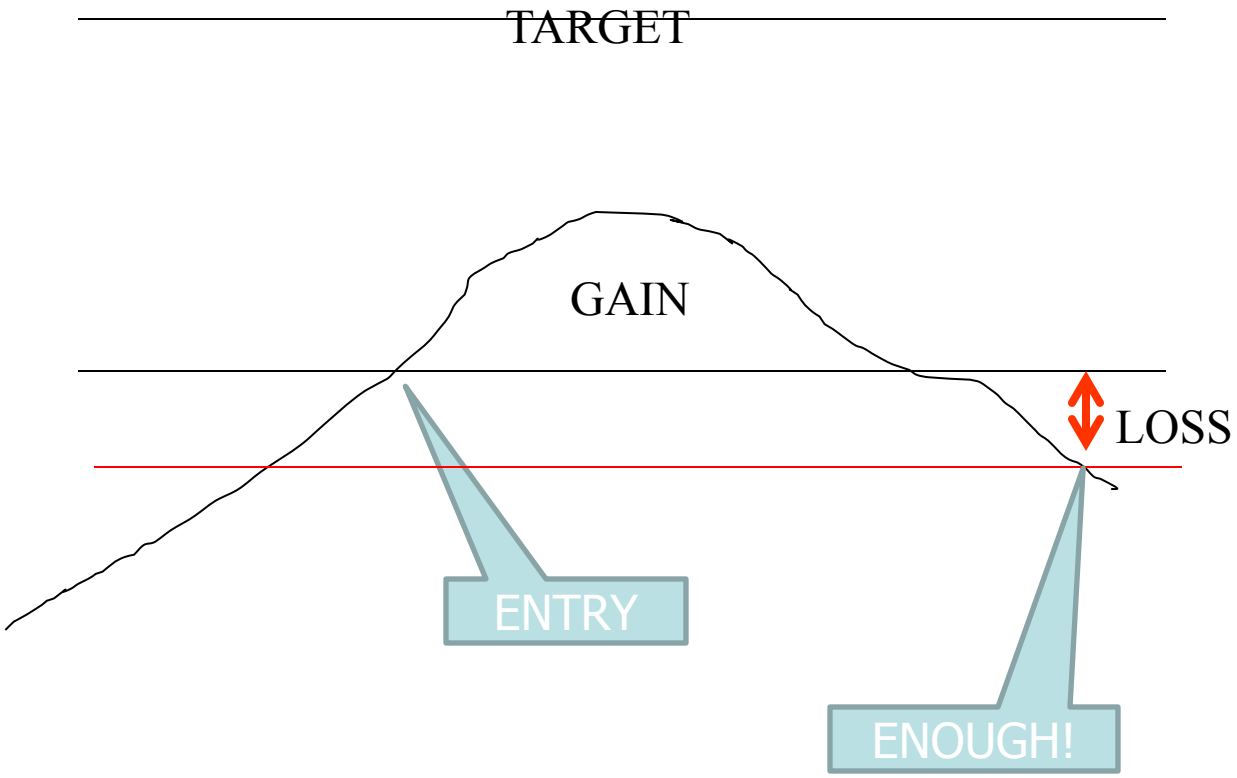
From trading to HFT

- Manual trading using e-platform
  - Limit
  - Stop Loss
- Shorting
- Leverage
- Derivatives
- Arbitrage



- High Speed
- Algorithmic

Stop Loss



Known Issues

- The true story – Flash Crash of the May 6th, 2010
- High Frequecy Trading
- **Known Issues**
- Less Discussed Issues
- Not trading?
  Never mind, they trade on you...

Known Issues

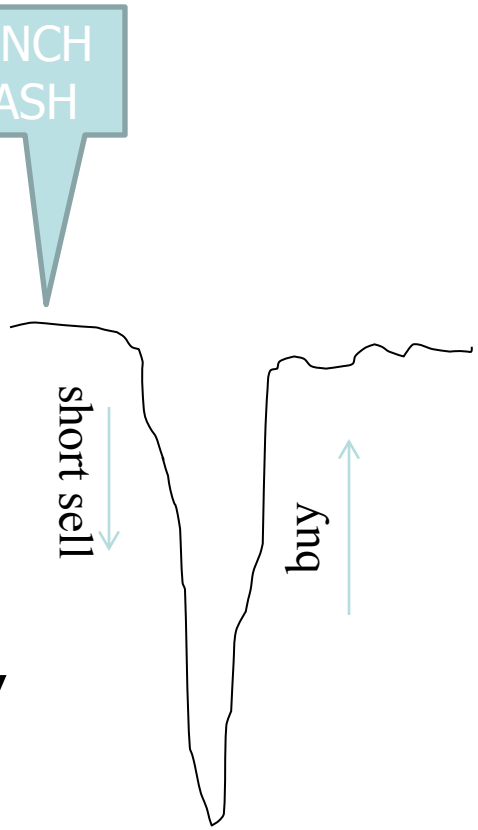
- May 6, 2010: Flash Crash happend
- Jan 2011: Rony Kay, cPacket Networks: Pragmatic Network Latency Engineering Fundamental Facts and Analysis – discusses HFT attacks by deliberately causing latency
  - http://www.cpacket.com/Introduction%20to%20Network%20Latency%20Engineering.pdf
- Black Hat USA and Defcon 2011, James Arlen
  - http://vimeo.com/28794878
  - Latency = direct financial loss in HFT
  - Traditional security (firewalls, AV, IDS...) implies latency
  - Therefore, traditional security countermeasures are non-existent in HFT
- Quote Stuffing
  - Lots of nonsense quotes, just to make other HFT busy -> latency

Less Discussed Issues

- The true story – Flash Crash of the May 6th, 2010
- High Frequecy Trading
- Known Issues
- **Less Discussed Issues**
- Not trading?
  Never mind, they trade on you...

Flash Crash Fraud Scenario

- DON'T DO THIS
- Induce flash crash of target instrument
  - Choose (in)apropriate moment
  - Sell large amount of target instrument
  - Saturate data feeds with quotes that do not make sense
- Short sell while riding down, buy back at pre set target, buy more while climbin up, sell at pre set target
  - Dont get too greedy



Intrusions everywhere in financial world

- No impact widely noticed so far – in several cases
- I remember a warning on a malware tageting certain trading platform in beginning of 2011
- Oct 2011, Nasdaq under attack – speculation about hackers getting to insider info http://www.bloomberg.com/news/2011-03-30/u-s-spy-agency-said-to-focus-its-decrypting-skills-on-nasdaq-cyber-attack.html
- Mar/Feb 2011, Morgan Stanley #1 – Aurora hackers attack – leaked via HBGary
- Jun 2011, IMF under attack http://www.bankinfosecurity.com/articles.php?art_id=3736
- Jun 2011, Bitcoin related attacks http://slo-tech.com/novice/t472678

Maybe some is just building a botnet? I mean a special one, targeting traders ....

Botnet of trader's computers would be useful for the attacker

- Perform coordinated actions from thousands of "owned" user accounts
  - e.g. starting a flash crash you need a substantial funding – this can be crowdsourced to owned accounts
    - or other "campains" to influence the price of something
  - DoS users; providers; stock exchanges
  - Stealth quote stuffing – poor man's (attacker's) compensation for HFT technology
  - Use your imagination for further use cases ...
  - Get info on the trading strategies that are not part of public order book – where is your stop loss set you said?
    - BTW Q for statistic freaks: what %/count is the representative sample for entire trading population?
- HFT – hi speed trading engines cannot be directly controlled by botnet due to technical limitations (botnet is on "standard" tech), but "control station" can

Less Discussed Issues

- DoS during big changes affects user
  - recent EUR/CHF 10% rise in minutes
- Stop loss effectiveness when under DoS
- Trading fraud vs. e-banking fraud
  - Hardly notified malicious intent
  - Probably because the traders are inherently malicious to each other
- Trading Flavour Salami attack
- Follow me to hell
- Reverse ingeneering trading algoritms, finding security vulnerabilities – is this actually market analysis? Evolution: fundamental, technical, algocentric

Not trading?

- The true story – Flash Crash of the May 6th, 2010
- High Frequecy Trading
- Known Issues
- Less Discussed Issues
- Not trading?
  Never mind, they trade on you…

They trade on you

- Index does not reflect the market anymore
  - index impacts the market – DJIA during the Flash Crash
  - ... and some suggest that solution against Flash Crash is introducing another tradable index (VPIN)
- Not trading? You are affected anyway
  - The probability of your countries public finance default is most likely subject to trade
  - Have debt in CHF? Wellcome to the club.
  - Is EUR, USD, <put your choice here> your currency? It's subject to trading with other currencies (FOREX)
  - Need oil for heating and mobility? Your next's years oil expenses are in large part subject to speculative financial markets.
  - Still not affected? Congratulations. Probably you are one of those not using mobile phone? Living on a bio-dinamic self-sufficient farm? OK, that makes sense...
  - BTW, IPV4 address space is subjet to trading - http://tradeipv4.com/

High Frequency Hacking

Some risks of the modern trading practices

Tadej Vodopivec, CISSP, CISA, CBCP
Information Security Consultant
ComTrade d.o.o.
ime.priimek AT see above d.o.o. DOT com

OWASP

September 15, 2011 - Ljubljana, Slovenia

The OWASP Foundation
http://www.owasp.org