MetaBreaking MetaTrader

Selected works on the state of security in proprietary trading platforms

Who are We?

@bppetrov

The Mad Scientist, did stints at CERN and IBM, all around troublemaker

@AlexBehar

Things just break in my presence, InfoSec veteran, founder of ECL-Labs

Intro to the FOREX market

- FOReign EXchange - currency trading
- Interbank vs Retail traders
- Use of leverage enhances profit (and loss) margins
- ~$2.8 Trillion of retail trading volume monthly (Forex Magnates, q3 2011)

Additional reading on currency trading and speculation:
http://www2.econ.iastate.edu/classes/econ355/choi/fex.htm

InfoSec intro to the FOREX market

- Low application diversity*
  - 4 trading platforms dominate 90% of the market
  - MetaTrader 4 executes 60%+ of retail trades
- Little research on the subject to date
  - Server daemons usually developed C++ and C
  - Semi-decentralized markets have plenty to lose from speculations exploiting the fact...

*No official stats exist, based on market feedback

MetaQuotes MetaTrader 4

MetaTrader 4 Ecosystem

- The Server
  - 32bit Windows application written in C++
  - Calls home frequently for updates, IP blacklists
  - MetaQuotes controls patching process
  - Outrageous licensing fee :)

- The Client
  - Branded terminal for every MetaQuotes customer
  - Executable signed by a Thawte code signing cert \o/
  - Binary packed with Themida
  - Connects to the server via a proprietary protocol with "custom encryption" on top of TCP

State of MT4 Security Research

- MetaQuotes is very diligent with reversers
  - Sued and successfully closed down Xogee, a mobile trading software vendor, for using their protocol
  - Constantly updates client and server with new security measures to thwart research

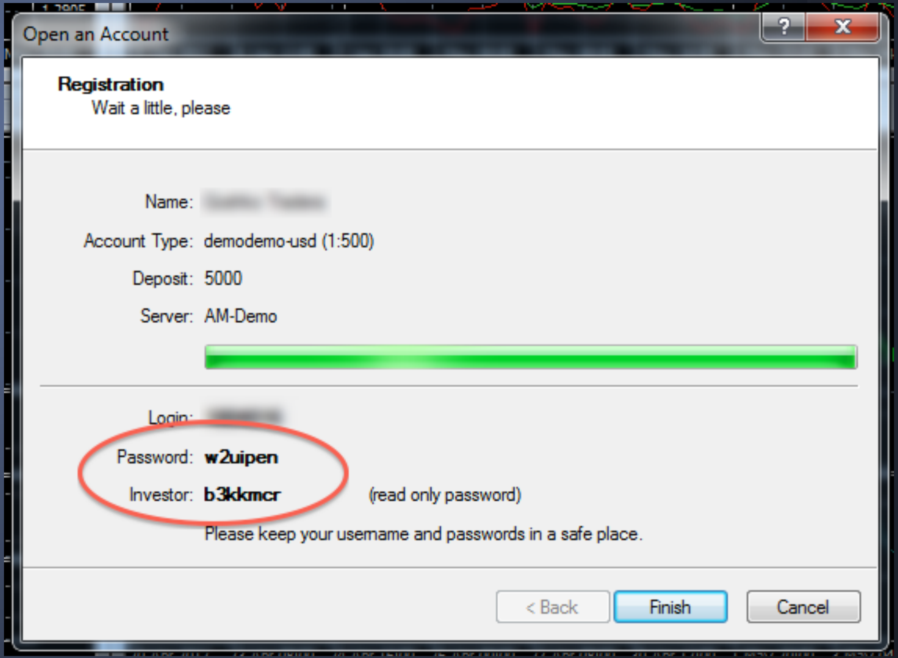
- Client-side extensions also prohibited
  - Several small vendors developing UI and analysis extensions were booted off the market over night

- So how much security was gained by locking everything down? Let’s find out...

Server-side password generation

MetaTrader 4 Server Passwords

- Server can generate passwords for both real and demo accounts alike
- Always 7 symbols
- Lower case & alphanumeric only
- Only basic measures of brute force resistance



Open an Account

Registration

Wait a little, please

Name: [redacted]

Account Type: demodemo-usd (1:500)

Deposit: 5000

Server: AM-Demo

Login: [redacted]

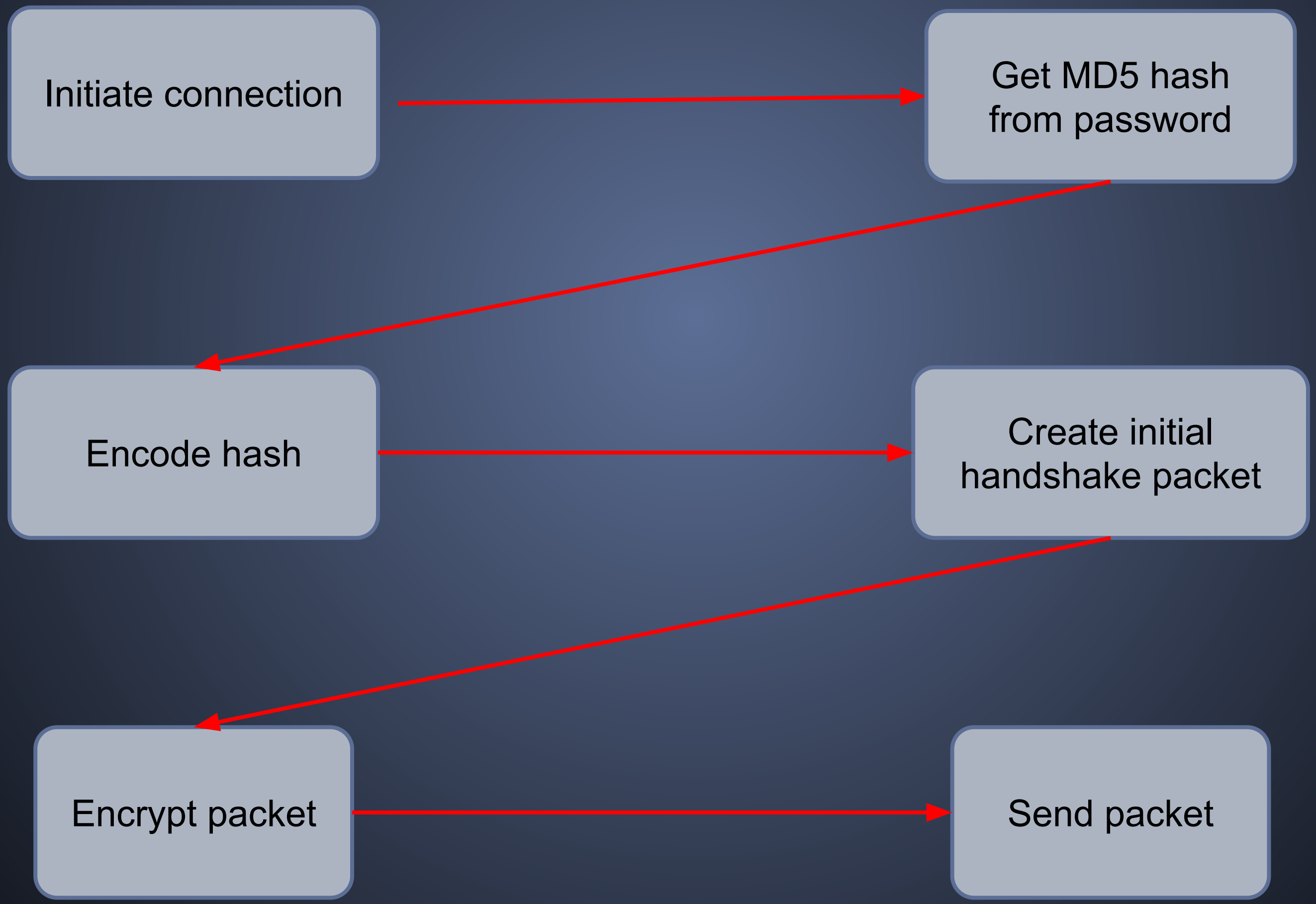
Password: **w2uipen**

Investor: **b3kkmcr** (read only password)

Please keep your username and passwords in a safe place.

MetaTrader 4 Protocol Fun

MT4 Protocol Handshake



MT4 Credential Transmission

- MD5 hashed password w/o salt
- MD5 custom transforms
  - Transforms performed post hashing
  - Does not increase security in any way
  - Reducing keyspace by a factor of 256
- No perfect forward secrecy (key exchange) during transmission
- Allows for MiTM and password recovery attacks

The MD5 text transform (“encoding”)

- “Encoding” it using simple bitshifts, bitwise operations
- Pseudocode:

```
prev = 0
for i from 0 to md5.size (16 bytes)
 encoded[i] = md5[i] ^ (prev + md5[i & 0xF])
 prev = md5[i]
```

Protocol Handshake Packet

- First and third bytes are 0 (?!)
- Insert “encoded” MD5 hash of user’s password at third byte
- Insert account number at byte 19
- Insert MT version and client build
- 28 bytes in total

“Encryption” stage

- Again trivial bitshifts/bitwise operations

Insecure MD5 usage - keyspace reduction

- From the code that encodes the MD5 hash:
    - prev = 0
    - encoded[i] = buf[i] ^ (prev + buf[i & 0xF])

- We can see that for i = 0 encoded[i] = 0 regardless of the value of buf[0]; so there is no way to reverse buf[0]
- This means that ANY value is ok and will make an MD5 hash that could be reversed into a valid password

In short...

- Critical mistakes in implementing MD5
- Performing transforms on top of armored hash
- Credentials are not encrypted, but rather scrambled
- Protocol vulnerable to MitM due to the lack of authentication

DEMO

(password recovery from packet capture)

Breaking the Bank

On liquidity and risk

- On broker connectivity to the outside world
  - Quote (ticker) streaming
  - Access to liquidity
  - Risk management (and STP)

- 32bit DLL plugins imported into the MT4 Server

- Provide connectivity to liquidity providers (banks)

On liquidity and risk

- Liquidity bridges clear orders with banks
- Assess risk of trades (!!!) and hedging
- Straight-Through Processing (STP) decisions
- Connectivity to several banks for high availability

Typical FX Broker Software Stack

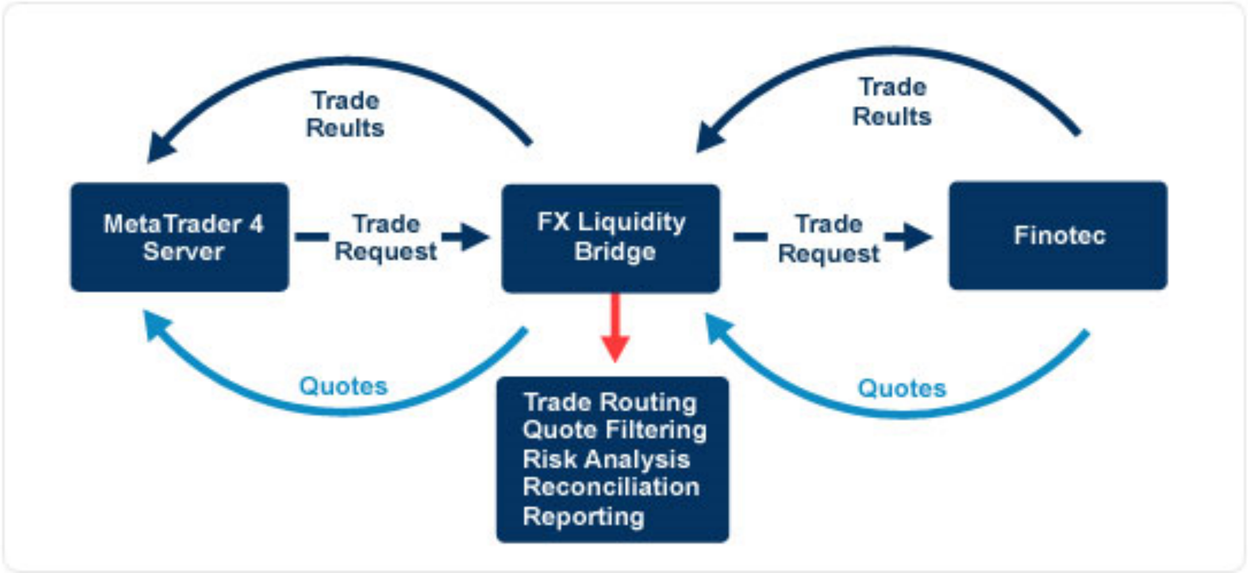
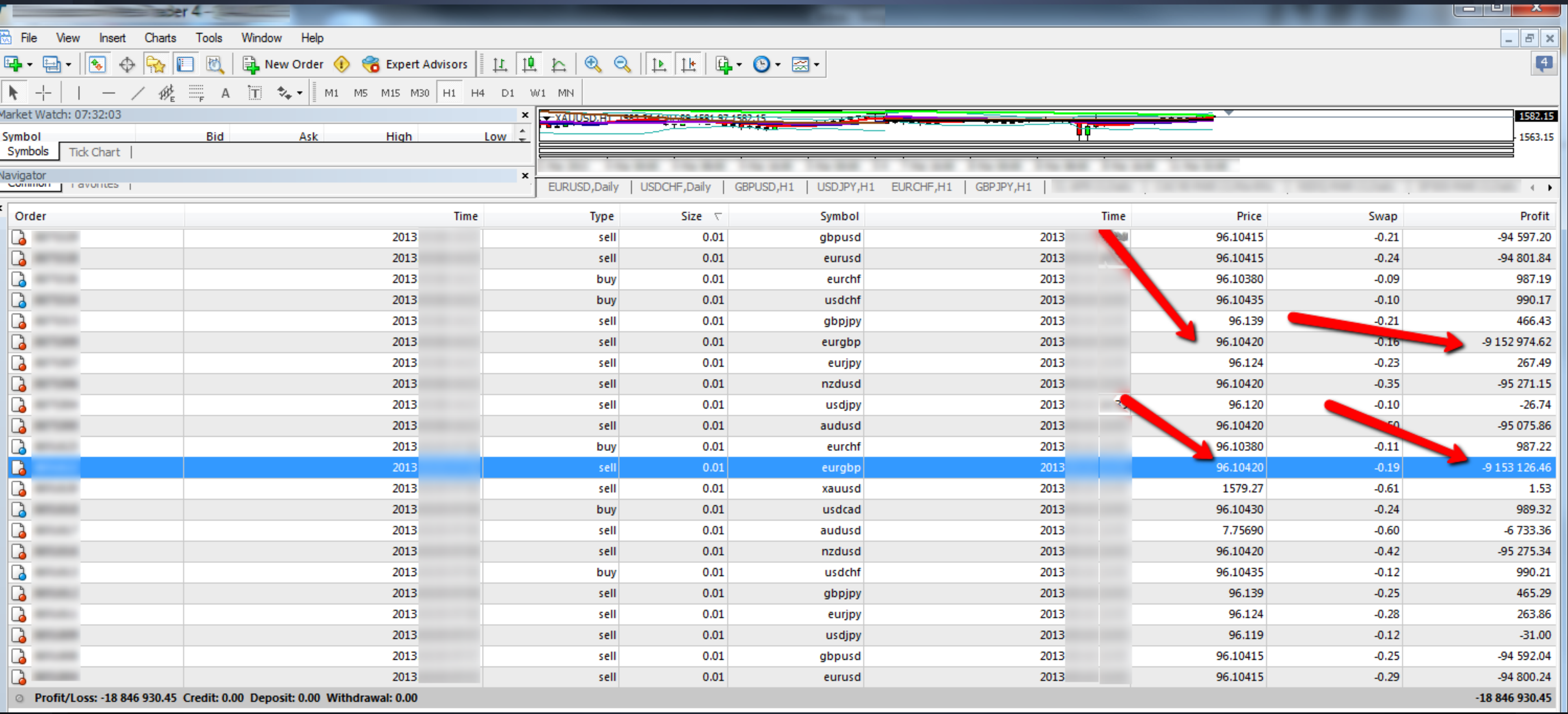


Image courtesy of Finotec Trading UK Ltd
http://www.finotec.com

Parameter Verification

- DoS-ing a liquidity bridge
  - No Margin Call issued for trades, even though account balance is zero



Order	Time	Type	Size	Symbol	Time	Price	Swap	Profit
[redacted]	2013 [redacted]	sell	0.01	gbpusd	2013 [redacted]	96.10415	-0.21	-94 597.20
[redacted]	2013 [redacted]	sell	0.01	eurusd	2013 [redacted]	96.10415	-0.24	-94 801.84
[redacted]	2013 [redacted]	buy	0.01	eurchf	2013 [redacted]	96.10380	-0.09	987.19
[redacted]	2013 [redacted]	buy	0.01	usdchf	2013 [redacted]	96.10435	-0.10	990.17
[redacted]	2013 [redacted]	sell	0.01	gbpjpy	2013 [redacted]	96.139	-0.21	466.43
[redacted]	2013 [redacted]	sell	0.01	eurgbp	2013 [redacted]	96.10420	-0.16	-9 152 974.62
[redacted]	2013 [redacted]	sell	0.01	eurjpy	2013 [redacted]	96.124	-0.23	267.49
[redacted]	2013 [redacted]	sell	0.01	nzdusd	2013 [redacted]	96.10420	-0.35	-95 271.15
[redacted]	2013 [redacted]	sell	0.01	usdjpy	2013 [redacted]	96.120	-0.10	-26.74
[redacted]	2013 [redacted]	sell	0.01	audusd	2013 [redacted]	96.10420	-0.50	-95 075.86
[redacted]	2013 [redacted]	buy	0.01	eurchf	2013 [redacted]	96.10380	-0.11	987.22
[redacted]	2013 [redacted]	sell	0.01	eurgbp	2013 [redacted]	96.10420	-0.19	-9 153 126.46
[redacted]	2013 [redacted]	sell	0.01	xauusd	2013 [redacted]	1579.27	-0.61	1.53
[redacted]	2013 [redacted]	buy	0.01	usdcad	2013 [redacted]	96.10430	-0.24	989.32
[redacted]	2013 [redacted]	sell	0.01	audusd	2013 [redacted]	7.75690	-0.60	-6 733.36
[redacted]	2013 [redacted]	sell	0.01	nzdusd	2013 [redacted]	96.10420	-0.42	-95 275.34
[redacted]	2013 [redacted]	buy	0.01	usdchf	2013 [redacted]	96.10435	-0.12	990.21
[redacted]	2013 [redacted]	sell	0.01	gbpjpy	2013 [redacted]	96.139	-0.25	465.29
[redacted]	2013 [redacted]	sell	0.01	eurjpy	2013 [redacted]	96.124	-0.28	263.86
[redacted]	2013 [redacted]	sell	0.01	usdjpy	2013 [redacted]	96.119	-0.12	-31.00
[redacted]	2013 [redacted]	sell	0.01	gbpusd	2013 [redacted]	96.10415	-0.25	-94 592.04
[redacted]	2013 [redacted]	sell	0.01	eurusd	2013 [redacted]	96.10415	-0.29	-94 800.24

Profit/Loss: -18 846 930.45 Credit: 0.00 Deposit: 0.00 Withdrawal: 0.00 -18 846 930.45

Parameter Verification

- MetaTrader 4 server fails to sanitize position closure parameters
- Attacker can send crafted “close position” parameters, causing closure with marginal difference between open and close prices
- This could lead to a hugely negative balance, lacking margin call, crashing liquidity providers and DoSing banks

Closing Remarks

“Wait a minute! Didn’t you promise pwnage in more platforms?”

We did!

FXCM Trading Station

SSL certificate verification (again!)

- FXCM Desktop and SDK connect to a schema server via HTTP
  - An attacker can trick it to connect to an arbitrary location and sniff credentials

- FXCM TradeStation does not verify SSL certificates correctly (or at all..)
  - Neither does the API SDK for **institutions**

SSL trust chain of fail!

It’s 2013 and people are still not getting it…

Closing Remarks

(for real this time)

Closing Remarks

- Please stop inventing proprietary protocols
  - And especially proprietary "encryption" schemes!

- Financial markets need open protocol stacks and specifications

- Financial Information eXchange (FIX) protocol adoption is still low in FOREX

Closing Remarks

- Security through obscurity (obviously) doesn't work

- Many other proprietary financial trading platforms in existence
  - FOREX, CFDs, Binary Options, Commodities...
  - A booming ecosystem of 3rd party plugin vendors

(and bugs)

Closing Remarks

- Got access to financial trading dev environments?
    - Let us know!
- Research into High Frequency Trading
    - Open protocols mean better, cheaper access to raw market data
    - Researchers can look for shenanigans (see @nanexllc)
- Lack of transparency == Lack of oversight

Thank you for your time!

Questions?