Reverse-Engineering Trust

Dr. Igor Muttik
Principal Research Architect, McAfee Labs

A quote
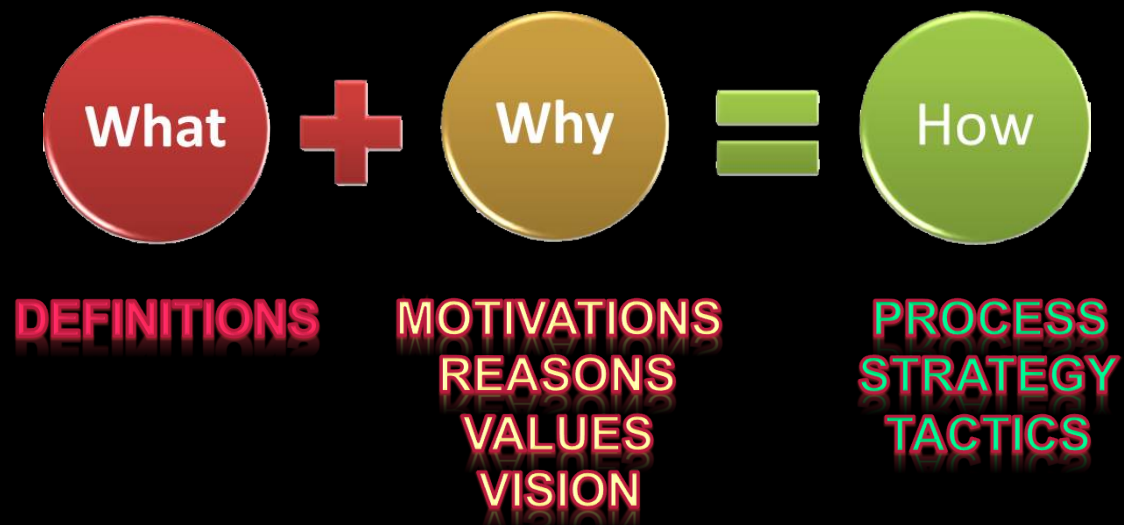
"There are known knowns – things we know that we know.

There are known unknowns – things that we now know we don't know.

But there are also unknown unknowns – things we do not know we don't know."

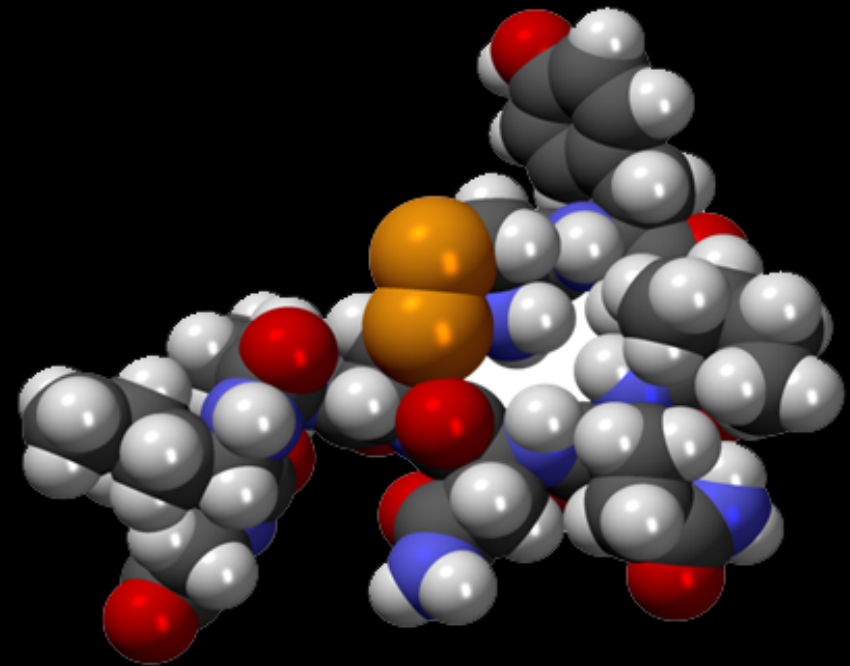—*United States Secretary of Defense, Donald Rumsfeld*

What Do We Know About Trust?

- Reflects "Trustor –Trustee" relationship

- Has strong group aspect (family, tribe, etc.)

- Its neurobiology is affected by oxytocin

- Humans (and the society) need trust as it drives confidence
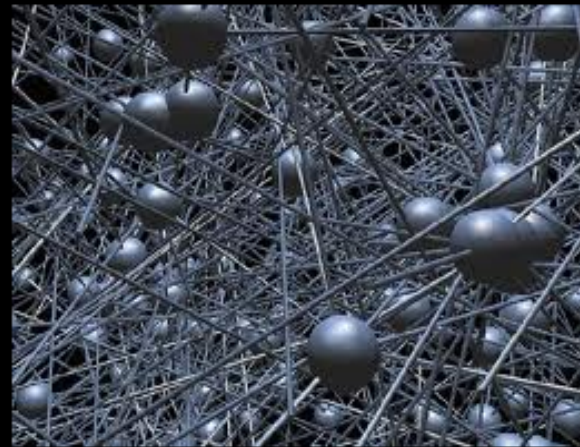
Trust History

- Human to a human (directly)

- Human to a computer

- Computer to a computer

- Human to a human (via computers)

- Computer = hardware
  + software
  + network
  + protocol
  + cloud
  + ecosystem
  + human!

Trust Attributes

- It is a measure of a risk in transactions

- Trust is contiguous - spectrum of reputations

- Temporal property

- Not mutual / symmetrical

- But mutual is nice!

Elements of Trust / Reputations

- Source

- History / Age

- Prevalence
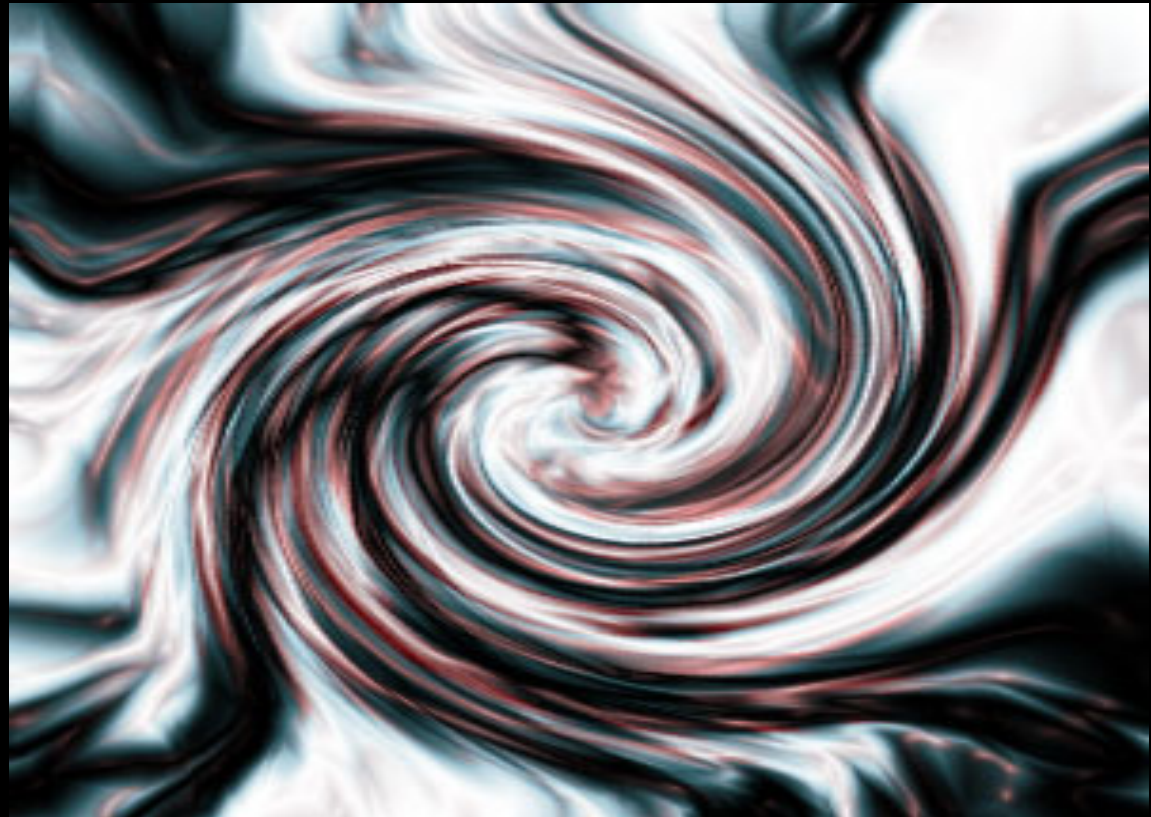
- Geography

- Documentation

- Opinions of others
  - Positive
  - Negative (feedback)

Computing Trust / Reputations

- Page rank

- "Inherited" trust

- "Fused" trust

- For all players
  - Humans
  - Computers
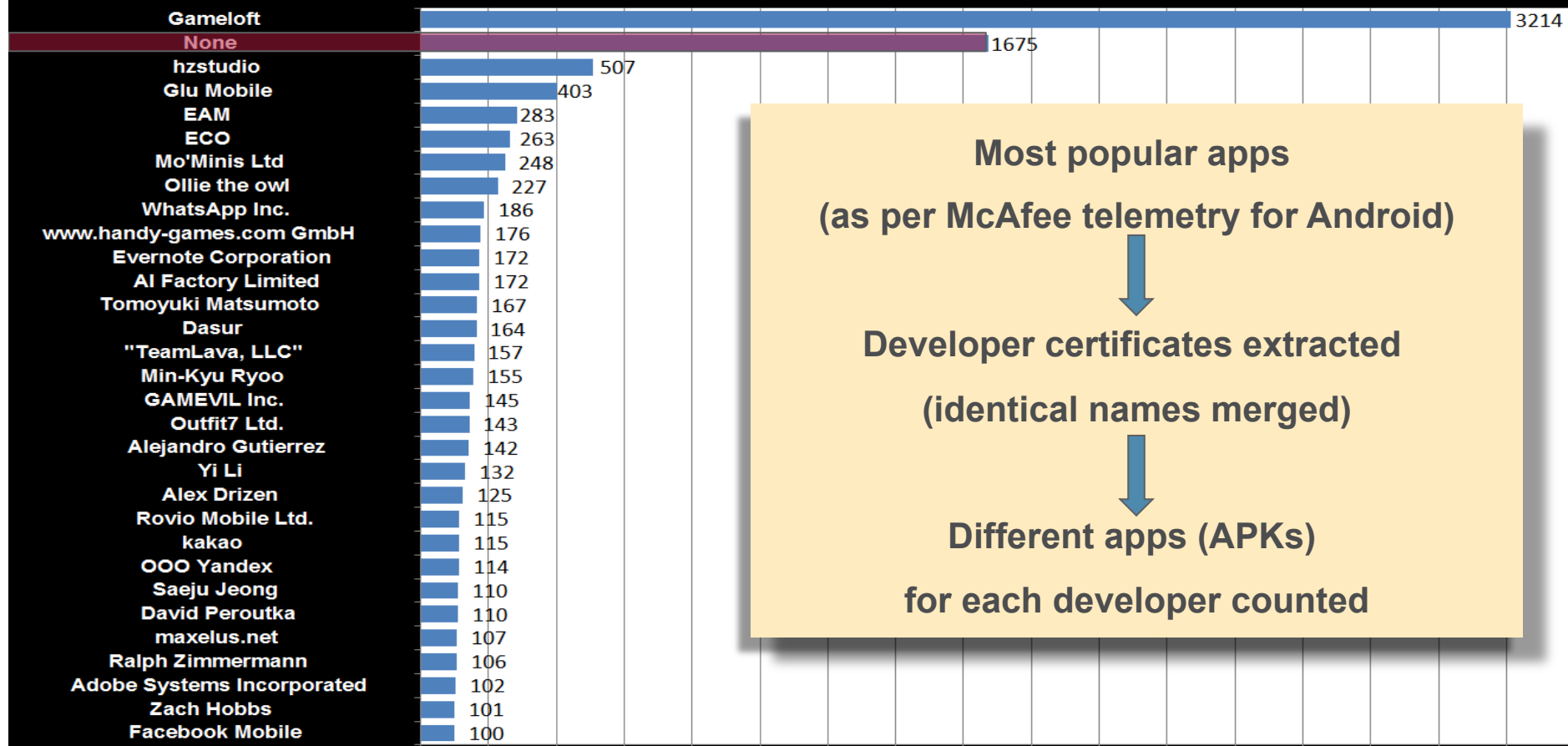 - Devices (IoT)
  - Networks
  - Protocols
  - Clouds

Abusing Trust

- Trust is now data (Big Data)

- MitM

- Commodity
  - Stolen
  - Forged

- Poisoning (e.g. Sybil attack)

Trusted Android Developers

Developer	Count
Gameloft	3214
None	1675
hzstudio	507
Glu Mobile	403
EAM	283
ECO	263
Mo'Minis Ltd	248
Ollie the owl	227
WhatsApp Inc.	186
www.handy-games.com GmbH	176
Evernote Corporation	172
AI Factory Limited	172
Tomoyuki Matsumoto	167
Dasur	164
"TeamLava, LLC"	157
Min-Kyu Ryoo	155
GAMEVIL Inc.	145
Outfit7 Ltd.	143
Alejandro Gutierrez	142
Yi Li	132
Alex Drizen	125
Rovio Mobile Ltd.	115
kakao	115
OOO Yandex	114
Saeju Jeong	110
David Peroutka	110
maxelus.net	107
Ralph Zimmermann	106
Adobe Systems Incorporated	102
Zach Hobbs	101
Facebook Mobile	100

Most popular apps

(as per McAfee telemetry for Android)

Developer certificates extracted

(identical names merged)

Different apps (APKs)

for each developer counted

Conclusions

- "Secrets don't destroy trust… But suspicions do…"

- "Trust everybody until they prove they aren't worthy of your trust."

- "In God we trust. Others must bring data!" *-Edward Deming*

3 errors