Trust in Computing Platforms

mi2g event: The Question of Trust, The Athenaeum, London, 18th July 2002

DK Matai, Chairman and CEO, mi2g

Trusting the quote

Most buying and selling decisions on the stock markets today are made via computer screens or automated price feeds. Let me ask you this – forget online graffiti, forget denial of service - think about a small manipulation of a specific share price on computer screens for an hour or so which goes unnoticed, and two types of large transactions take place.

Put options are exercised for Millions of Dollars and buy orders are placed at a lower price than the actual market. What is the actual profit and loss for the two transactions? Who gained from it and at whose expense?

There is no particular guarantee on the authenticity of most financial news screens available via the Internet, or the integrity of the data one is reading as being accurate in real time. Go to www.ft.com, www.wsj.com or finance.yahoo.com or any other financials site and you will see precisely what I mean.

In fact the recent case with USA Today, on 11th July, where their web site was hacked and genuine content was replaced with phoney articles is worth noting. USAToday.com is one of the Internet's most frequented news sites, with 9 million monthly visits. This breach of trust has caused major shock waves on the issue of trust associated with online content.

These sites that freely provide market data are not even protected by rudimentary Secure Socket Layer (SSL) encryption, which is deployed when making an online credit card purchase. Yet millions of investors around the globe assume that they are looking at accurate and near “real time” market indices and share price information and make actual investment decisions based on this “leap of faith” and judgement.

Trust in the digital world

Trust in the real world and digital world are very similar concepts. They sustain confidence. And there is a key difference as well, which is that the parties involved in any online interaction have very little knowledge about each other and cannot depend on time honoured trust building measures such as physical proximity, face to face and eye contact, handshakes and assimilating body-language.

Instead it is necessary to rely upon other trust building proxy measures such as the use of devices or biometrics for authentication; referencing through trusted third parties; wrapping confidentiality around messages and performing integrity checks; defining the limits of risk exposure; and clearly stipulating general safeguards against non-repudiation.

In the same way, the shareholders in a publicly listed company rely on trust by proxy. They cannot go and spend hours with the CEO and CFO of the public company so they rely on the auditors and regulatory authorities to do a good job of policing

confidentiality, integrity, authentication and non-repudiation of all transactions referenced in the annual report. But… what happens if the policeman cannot be trusted, as has happened in the case of Enron/Andersen?

Identity theft

Another problem arises on the issue of identity and authentication. Are you really who you claim to be? It is often assumed that the problem with supplying sensitive information to a bank is purely a matter of preventing interception by a third party during the transfer process and that once the necessary information for the transaction has been successfully exchanged it is safe and there is no further risk. Nothing could be further from the truth because of the possibility of identity theft. How can enough trust be established that the person making the request to withdraw funds via electronic means is indeed the person who he or she claims to be on each and every occasion? What needs to be carried by the user and what needs to be measured to authenticate and yet be non-replicable? Even fingerprints and key fobs can be usurped and duplicated.

In fact, there is no known method of establishing the identity of the user with complete certainty. The 3 components of identification – something you are, something you know and something you have – can all be compromised or simultaneously forged by a determined malicious user if used without coupling.

Overt digital attacks, loss of trust and correlation with identity theft

Many Heads of Security of banks say, “Yes, our website was defaced last year. They did not penetrate our systems. Not a big issue.” If violation of their brand name and the associated customer trust is a not a big issue, what is?

The trust that customers have in a company is effectively shattered as a direct consequence of a public attack. Even when banks and other corporations use third party hosting for their websites and only store important information on machines not accessible to the Internet, the general public still loses faith in them and can no longer be confident in the safety and integrity of information entrusted to those financial institutions or multinationals. After WorldCom and Enron is a consumer going to believe what the CEO, CIO and the auditors say about the integrity of their personal details and data surrendered online to their corporation?

In fact, if an online site is defaced it means that the security of the system hosting that website has been undermined and the data changed.

The Deceptive Duo, a US group that systematically defaced 11 US government sites and 6 military sites in April and May 2002, was able to access profiles of users on the systems they attacked; and they displayed them as part of their defacement in order to prove this to the world. They also targeted several banks and were able to access very sensitive customer account details, which were also made public. Identity theft is a key issue in the 21st Century.

Security on the Internet

The number of announced vulnerabilities in computing platforms has been rising exponentially and corporations failing to take them seriously face huge risks. In fact, the Internet was not conceived to be a secure network. Distributed – yes. Secure – no. From its inception, applying the Internet to business was problematic from a security perspective. Nonetheless, the Internet has been embraced as a global

information and communication backbone because of the expansive opportunities associated with this technology and a bull market fuelled by entrepreneurs, bankers and venture capitalists looking to cash in on the technology bubble. Time may prove the fallibility of the present Internet and the risk associated with it.

The reluctance of consumers to trust a company with their credit card details can effectively deprive that company from continuing and expanding business and it was only when a relatively secure and trusted mechanism for making electronic transactions was devised that Internet businesses began to see any degree of success. What is going to happen, however, when more incidents like CD Universe, in which users' credit card numbers were stolen and sold on the black market, continue to rise? The architectures which host credit card numbers are mostly not tranched or heavily encrypted because of the associated complexity and speed of response penalty. The rush to win market share and reduce the time to market has left the long-term issue of trust as secondary.

When trust fails the consequence is a "user strike" just as we are getting an equity investor strike at present. Do card companies and online vendors have the probability of such a strike plugged into their forward planning?

Focus on security

Bill Gates halted the work of thousands of engineers at Microsoft earlier this year with a view to focus on plugging security holes in his products and developing a trustworthy computing model. He went on to say that trustworthy computing is the crucial issue. This event has more significance than just helping to preserve the dominance of Microsoft in the desktop and networking market for the years to come. It is better regarded as an awareness-raising event for security so that it is no longer seen to be applied at the end stages of the product development cycle, but rather built into each and every product that will be brought to market at inception.

Trusting hardware

Trust is just as much an issue where hardware is concerned as with software. One of the main security vulnerabilities of computers is the fact that they are designed in such a way that the central processor will carry out whatever instructions it is given, with no way of knowing whether they are legitimate or not. There is no continuous authentication and authorisation system installed in the vast majority of digital processing systems available today. There are designs being put forward for the future mass user market that do just that.

However, an initiative by the Trusted Computing Platform Alliance (TCPA), formed by Intel, IBM, Microsoft and others, aims to develop a way of building secure computers and Microsoft itself has revealed details about a new project of its own called Palladium – a trusted form of Windows using the TCPA specification. It would use an authorisation process developed, managed and controlled by Microsoft.

Despite the fact that this could effectively mean an end to viruses, worms and spam, would the prospect of having a single company in control of files and programs that run on a computer not worry a lot of people?

Trusting peer-to-peer computing platforms

Which is the largest computer in the world? All the desktops and servers connected via the Internet to each other in a peer-to-peer fashion together are the world's largest computing system and information bank.

In global peer-to-peer networking, trust and security are essential and have become very significant issues as this interconnectivity has become commonplace on a 24/7 basis. Most computers at work are now always on or on stand-by and always connected. In the future, your house will be completely digitised via sometimes ubiquitous computers that will be always on and connected. Your bank records, your personal details, your family's photographs and where you holiday will all be available to a clever hacker or an organisation that chooses to access your information because you have not ticked the appropriate box. Have you wondered how many organisations and individuals hold your personal information and what use they are putting it to and with whom are they sharing it?

Conclusion

There is going to be a big issue of trust – confidentiality, integrity, authentication and non-repudiation - in the years to come around interconnected computing platforms.

As broad band networks proliferate and everybody will be connected 24/7 to each other, the amount of damage that could be brought about through a breach of trust is likely to be several orders of magnitude greater than originally calculated by the corporate or individual user or even understood.

Who is going to insure the risk and who is going to protect the online citizen in the big wide digital world? Which government and which regulatory body and over what jurisdiction?

So in conclusion, I would say that the 21st Century is going to be ever reliant on the pillars of trust between people who are interlinked across remote distances by computing and communications. Are the installed computing and communications platforms up to the job today? The answer is no. Will they be trustworthy some day? Yes, but only after a few major fires - like The Great Fire of London in September 1666 - have forced the vendors to adopt trustworthy computing architectures.