IX.5

# DISTRIBUTED MIDDLEWARE TOOLS FOR TRUSTED ELECTRONIC INTER-ACTIONS

**R Weber**

**Rapporteur:** Ian Welch

IX.7

# DISTRIBUTED MIDDLEWARE TOOLS FOR TRUSTED ELECTRONIC INTER-ACTIONS

**Robert Weber**
**Senior Vice President**
**Business and Technology Strategy**
**InterTrust Technologies Corporation**
**460 Oakmead Parkway**
**Sunnyvale, CA 94086**
**USA**

Founded in 1990, InterTrust Technologies Corporation provides middle-ware technology products that represent nearly a decade of R&D in how to make electronic commerce succeed. These technologies uniquely satisfy real commerce and security requirements for digital content distribution and protection businesses, as well as for businesses as diverse as electronic data interchange, electronic trading, and distributed process control.

Commerce traditions inherently reflect both human and organizational nature and time-proven efficiencies. A successful electronic commerce environment must therefore provide an automated extension of traditional processes. Such an environment must support rights protection in its broadest form, including the requirements of diverse societies (since electronic businesses can operate "virtually" in time and space) and media types ("bits are bits"). As a result, a commerce environment must be simple, transparent, optimally efficient, and equitable to use.

Commerce mechanisms inexorably move toward operations representing greatest efficiencies, rights protection, and transparency. Essential requirements for secure, trusted commerce interactions include efficient capabilities supporting persistent protection and automated chain of handling and control. Plural parties may contribute rules and usage consequences to and negotiate the parameters of electronic transactions, and so operate their own business models in cyberspace.

Efficient, transparent commerce interactions also require a trusted, general purpose, distributed, peer-to-peer architecture that is both modular and adaptive. InterTrust has invented such an architecture. It is comprised (in part) of DigiBox˙ secure containers, and distributed InterTrust Commerce Node middleware--which in multi-node combinations form peer-to-peer commerce environments.

Through the process of Chain of Handling and Control, rights holders including creators, publishers, aggregators, and repackagers can engage in value chain commerce in which content and commerce rules (price, permitted operations, use consequences, etc.) are distributed through individual user nodes. This process is automated by computerizing interactions, relationships, consequences, and the ability of rules to vary by jurisdiction, affiliation, and other identity-based rights.

Transposing traditional businesses into cyberspace requires letting rights holders associate rules with (rather that fix rules to) content, enabling such model flexibility as subscription renewals, pricing or rule updates, etc. Chain of handling and control capabilities also facilitate value chain participants deploying new business models, based both on superdistribution (turning pass-along from a copyright infringement problem into an opportunity), and on targeted merchandising and advertising (supporting intelligent marketing through the use of "information exhaust").

## DISCUSSION

**Rapporteur** : Ian Welch

### Lecture One

Dr Anderson asked whether InterTrust allowed technology to be customised per societal beliefs then would InterTrust fall foul of laws that forbid the export of technology that could be used for social repression. Dr Weber replied that he would look into it.

Another participant wondered if leaky information systems were in fact in the public interest making whistle-blowing impossible.

### Lecture Two

Professor Dobson asked Dr Weber what he meant by the term a "channel-less" world. Dr Weber replied that a channel existed between participants involved in a transaction. In the current business world these channels are fixed. In the new electronic business world these channels will not be fixed - they will dissolve and reform as required. This flexibility would allow new participants to be involved in financial transactions leading to a re-mediation of business relationships.

Professor Randell asked whether InterTrust saw security as an all or nothing option - essentially a binary value. Dr Weber replied that he believed that security was not a binary attribute, it could certainly be "good enough" for a financial transaction of a certain value and not "good enough" for a financial transaction of a higher value. The crucial factor is the cost of breaking the security and relating it to the secured goods. The protection offered by software-based security was seen as "good enough" for software packages worth $400 - $500.

Dr Anderson pointed out that in practice most security breaches are due to the discovery by laypeople of blunders made during the implementation of security. The clever hacker is a rare beast. He wondered if tamper-proofing the package buys you anything if a virus could be written that can steal the key to the package from browser, or subvert the device driver and steal transactions flowing between tamper-proof package and the browser. Professor Randell pointed out that it might be sufficient to assume that given enough time everyone can break the protection. If you start from this point then security can be viewed as an aspect of fault-tolerance and ideas from fault-tolerance could be used to make systems tamper-tolerant. Dr Weber agreed with this and suggested that intruder detection was one example of this approach.

A participant asked whether superdistribution already occurred. For instance, magazines often had "introduce a friend" offers that gave the reader a discount on the cost of the magazine if they introduced a friend as a subscriber. Dr Weber replied that in his view this was not superdistribution as the magazine scheme required active reselling on the part of the reader. With superdistribution it is simply a matter of giving a copy of the magazine to the friend and the friend reading the magazine that generates the revenue flow to the magazine publisher and lender. The flows are encoded as rules - a lender could add a rule that creates a revenue flow from the lendee to the lender.

Professor Turner asked whether this changes the nature of interpersonal relationships. Currently he didn't mind receiving unsolicited articles but if the mere fact of receiving it meant he was charged he would be less disposed to receive such articles in the future. This could reduce the sharing of information thereby poisoning current relationships. Dr Weber replied that InterTrust did provide an option for setting up chains of value that allowed people passing on articles to be paid by the recipients but there was no compulsion to use this option.

Professor Turner wondered if once the digibox is opened then he could just copy the contents thereby by-passing the security protection. Dr Weber replied that if right holders don't want to allow this behaviour then the right holder could add a rule enforcing persistent protection. This rule would force the recipient of the digibox to only play out the contents via an operating system extension that protects the output from copying.

One participant noted that it would be interesting if CD machines only accepted digiboxes. Dr Weber suggested that his company was discussing this with CD producers. Professor Turner pointed out that all people wanting to copy the CD would need to do would be add a device between the speakers and the trusted CD-player that copied the output. Dr Weber replied by pointing out that there are a lot of ways of infringing devices because at some point to be useful you need to expose the content. The aim was to make it harder to infringe copyright thereby reducing loss, not completely preventing. If the exposure could be reduced from 100% to single digit exposure it would be worth it. Perfect technology is snake oil. Obviously you wouldn't want to use this approach with military secrets where the exposure of any of the content is damaging, but for commercial purposes it is a reasonable approach.

A participant asked if he could make downstream rights less restrictive, i.e. I can photocopy an article and give it away without restriction. Dr Weber replied that he didn't want to be understood as suggesting that the purpose of technology to make free content priced - the point he was making was that people who have interests will negotiate for use. The same participant suggested that he hoped the control was not too rigorous - this could be a tyrannical way to distribute information. Dr Weber pointed out that in a profit-based world people would make trade-offs work in day to day business way. Common sense will prevail.

Professor Randell suggested that often responsibilities are talked about in relation to rights. Dr Weber suggested that the key responsibility of the consumer is not to destroy technology that ensures non-tamperability.

Professor Turner suggested that the InterTrust model of rights to protect copyright is flawed. Software patents are contentious. Only the USA recognises them and the majority of IT professionals believe that software patents shouldn't exist. Professor Turner is worried that putting the technology in place first is the wrong way around. Dr Weber suggested that it is not accurate that only the United States recognises software. It is controversial but he is aware that some European states are applying similar standards to the United States. Professor Turner suggested that copyright of software was still an unresolved issue in Europe and is yet to be fully worked through in the national courts. Professor Turner went on to say that his real worry was about what happens to the privacy of the individual in all this. Dr Weber replied that he believed privacy will become negotiable. In some circumstances individuals will waive their privacy in order to get a benefit such as a discount and in others their privacy will be jealously protected.

Another participant remarked that Dr Weber keeps talking about rights. The concept of what is a right is a slippery concept much argued about. Dr Weber replied that his view of rights was from a purely operational viewpoint as in what is a particular subject allowed to do to a particular object. The participant replied that this was perhaps too restrictive a viewpoint given the richness of commercial law and rights that arise from law.

Professor Randell asked what cooperation is required in order to install the InterTrust system, for example is there change to the operating system or a change to the infrastructure? Dr Weber replied that they are influencing the providers of infrastructures to support the InterTrust architecture for secure electronic commerce.