Panel: The InterTrust Commerce Architecture

Chair: **Willis Ware, RAND Corporation** **willis@conrad.rand.org**

Panelists

David Van Wie	**dvw@intertrust.com**
Olin Sibert	**osibert@intertrust.com**
James Horning	**horning@intertrust.com**

InterTrust Technologies Corporation
460 Oakmead Parkway
Sunnyvale, CA 94086
U.S.A.

408 222 6100 (voice), 408 222 6144 (fax)

Abstract

This panel introduces the InterTrust Commerce Architecture™, a system and architecture for trusted, distributed, global electronic commerce that has been developed by InterTrust Technologies Corporation. The panelists will address the overall system architecture and scope (Van Wie), describe the system's security architecture (Sibert), and discuss the focus areas of InterTrust's STAR Lab research organization (Horning). Each panelist's presentation will be followed by a discussion period.

The InterTrust Approach to Electronic Commerce
David Van Wie, Senior VP, Research

InterTrust has developed a system that automates existing commerce processes efficiently, and with a high degree of transparency. The system was designed from first principles to protect the diverse, interrelated rights of all participants in electronic interactions, including businesses, individuals, and governments. The new basic technologies incorporated into the InterTrust Commerce Architecture provide a fundamentally distributed trusted system that can utilize the existing global computing infrastructure to provide a platform for digital interaction, without conferring any inherent advantage to a particular society, commercial interest, or manner of conducting commerce.

Architectural Goals. InterTrust's system incorporates many new basic technologies that transparently and efficiently support corresponding core capabilities, such as distributed multiparty microtransactions and private auditing. The InterTrust system includes a complete set of secure components that support advertising, subscription, and ad hoc exchanges. These system capabilities are part of InterTrust's next-generation design for large scale commerce within the

scope of effective, and diverse, social context, and provide a system that supports many applications, including information commerce, electronic software distribution, multiparty trading systems, multilayered distribution chains, and enterprise document control and workflow management.

Components. The InterTrust architecture employs three principal components: the DigiBox™ secure container, the InterRights™ Point software, and the Transaction Authority infrastructure. The DigiBox container is a cryptographically protected storage environment for arbitrary information and business rules. The InterRights Point software provides Protected Processing Environment™ technology for manipulating information in DigiBox containers and for securely implementing business rules. The Transaction Authority infrastructure provides the end-to-end delivery of information generated as consequences of the business rules, and for carrying certain consequences, such as financial payment, to external systems.

InterTrust Functions and Processes. InterTrust's architecture assures that owners of information, stakeholders in transactions, and the user community can control their interactions using highly efficient and transparent models. The InterRights Point software at the heart of the architecture is provided to InterTrust's partners for no-cost distribution using InterTrust-supported management and administration software. The software transparently handles modularized underlying processes for the secure creation, storage, and exchange of any kind of information. Interactions proceed within the bounds of persistent rules for verifiable and controlled electronic actions over time in an occasionally-connected, peer-to-peer environment.

Default permissions and consequences for electronic events can reliably create accurate, auditable records of commercial interaction in the setting of diverse social requirements. Responsive distributed processes supported by the InterRights Point software can efficiently and traceably address common questions and disputes at low overheads, with excellent transparency. The software provides a platform that transparently manages certified distributed processes for authentication, nonrepudiation, and workflow validation.

Scope and Scaling. InterTrust reflects the diversity of commercial interactions. The architecture accommodates scaling to gargantuan system loads, as well as interactions from the elementary through highly detailed, independently managed, multiparty relationships. InterTrust supports interdependent horizontal and vertical multiparty relationships between independent actors in a dynamically reprogrammable, secure web. InterTrust can collect information, including highly aggregated information, about commercial actions in a distributed, auditable, and low overhead process. These distributed information flows are critical for fully automatic and trusted rules processing and other administrative needs.

In sum, the InterTrust system provides a general purpose, secure platform that ensures the substance of digital interactions is trusted and customizable. This distributed fabric for commerce efficiently supports simple transactions, with the power to describe—and automatically comply with—multilayered, multilateral, automated agreements.

The InterTrust Security Architecture
Olin Sibert, Director, Product Architecture

The InterTrust system provides a comprehensive solution to the security needs of global electronic commerce. This presentation assesses the relationship between commerce and trust, then describes how the InterTrust system fits into that picture. The InterTrust system uses cryptography and protected processing to associate information securely with the rules that govern its manipulation, and by doing so ensures that wherever the information is processed, the rules are followed. The InterTrust architecture is initially implemented in software, but will soon be incorporated into highly tamper-resistant hardware devices for a much higher level of security protection. The architecture provides for a true end-to-end solution for information management: a creator establishes the initial rules and associates them with the information; one or more subsequent distributors modify those rules (subject to conditions established by more senior parties), thus establishing a value chain; a consumer operates on the information; and the clearinghouse infrastructure returns information about the results of operations to members of the value chain as specified by the rules. The initial applications of the InterTrust architecture include content vending and electronic software distribution, but they are only two of the possible applications of the overall architecture. Unlike many approaches intended to solve specific problems, such as paying for Web content, the InterTrust architecture is general-purpose.

Commerce and Trust. Fundamentally, commerce is about trust: trust among the parties to an agreement, trust of societal and governmental institutions, trust of commercial enterprises, and so forth. However, trust is never absolute, and establishing trust has a cost. The trade-off between the cost of trust and the value of commerce is a fundamental aspect of commercial interactions. The InterTrust architecture uses a variety of security mechanisms to establish levels of trust appropriate to different situations. It is a trustworthy platform for all types of electronic commerce.

Technical Fundamentals. The fundamental technical innovation in the InterTrust architecture is the association of valued information with rules for manipulating it, and the guarantee that those rules will always be executed, in a trustworthy manner, when the information is manipulated. The information is protected by cryptography: its secrecy and integrity is guaranteed by key distribution. The rules are executed in the context of a Protected Processing Environment (PPE) mechanism which—depending on the level of trust required—may be implemented either in software or in a tamper-resistant hardware component. The cryptographic keys are protected inside PPE storage, and therefore are safe from disclosure.

To be processed by an InterTrust system, information and associated rules are packaged in a cryptographically secured structure called a DigiBox container. A DigiBox container can hold information with arbitrary size, format, and organization; in many ways, it is like a self-contained encrypted filesystem. The DigiBox container is a fundamental component of the InterTrust architecture: all information processed by an InterTrust system is stored in DigiBox containers whenever it is outside the protected environment.

A computer system incorporating this PPE mechanism is termed “InterTrust-enabled”; the software providing the PPE is called the InterRights Point. The InterRights Point software includes components that provide the client interface for applications (via a remote procedure call interface), tamper resistance and key management, execution of business rules, access to DigiBox containers, and cryptographically protected local storage of state, including transaction history and audit data. The InterRights Point software represents the components of the distributed Trusted Computing Base (TCB) in the InterTrust architecture.

Product Characteristics. The initial InterTrust product offering is a System Developer's Kit (SDK) that provides a protected environment in the context of Microsoft Windows 95 and Windows NT and that supports Transaction Authority functions on Windows NT and Solaris. These platforms provide a suitably secure base for using the InterTrust architecture to sell intellectual property, such as text, images, and software. However, there are applications where the security strength of such environments is not sufficient, so the long-term direction for InterTrust products is to run the InterRights Point software in a tamper-resistant hardware component called a Secure Processing Unit. The SPU incorporates a processor, cryptographic accelerator, volatile and non-volatile memory, and tamper-resistance features. It provides a strongly hardened environment for executing the InterTrust software, performing cryptography, and following the business rules.

System-Level Architecture. InterTrust-enabled systems can serve various functions: they can create new DigiBox containers and specify initial business rules (the *Creator* role); they can modify the rules and/or content in a container, subject to control of more senior rules (the *Distributor* role); they can release or otherwise manipulate information from a container as permitted by the rules (the *Consumer* role); and they can process the resulting consequence information to pass on to other InterTrust-enabled systems or to external financial systems (the *Clearinghouse* role, performed by a Transaction Authority system). There are also several other management and administration roles performed by Transaction Authority systems.

Relationship to Other Security Architectures. The InterTrust architecture is a distributed TCB made up of independent, distributed, decoupled InterTrust-enabled systems hosting the InterRights Point software. This degree of decoupling makes the InterTrust architecture fundamentally different from other distributed TCBs, and is achieved by packaging rules and control information and distributing them using the same mechanism as for content (DigiBox containers), rather than relying on communication with servers. Because it is based not only on cryptography, but on protected processing, it is fundamentally different from mechanisms such as S/MIME secure E-mail or the superficially similar IBM Cryptolopes; those mechanisms rely on conventional public key and secret key distribution schemes involving central servers. The InterTrust architecture has most in common with traditional capability-based systems such as PSOS, except that it uses cryptography and distributed protection to achieve security, rather than a centrally administered and physically protected host system.

InterTrust's Research Directions for Electronic Commerce
James Horning, Director, InterTrust STAR Laboratory

The Strategic Technologies and Architectural Research (STAR) Laboratory is responsible for ensuring that InterTrust has adequate technical options for trustworthy electronic commerce for the foreseeable future, and technical information needed to choose business strategies. STAR Lab will maintain a portfolio of investigations with various time scales and exploring various areas. Some of our early areas of interest are languages for electronic contracts—the translation between contractual terms meaningful to humans and securely executable rules for information handling; watermarking—applying unforgeable, unremoveable, secure marking to content to trace its origin; and tamper-resistance technology for hardware and software to prevent interference with secure operation.

Vision. The STAR Lab is a fundamental part of the InterTrust company vision. The nature of the problems InterTrust is addressing has led it to develop most of its own technology. STAR Lab was formed in early 1997 with the responsibility to ensure that InterTrust has adequate technical options two, five, and even ten years into the future, and adequate technical information to choose its business strategies. Because distributed general-purpose electronic commerce is such a diverse field, we cannot rely on universities, government labs, or large companies to develop the necessary technologies.

Mission. The Lab's mission is to maintain and increase the technological leadership of the InterTrust Commerce Architecture. A primary function of the Lab is to invent and discover technologies that create new business opportunities. The Lab is also responsible for a continuous effort to ensure that trustworthiness of InterTrust systems can be maintained, and to develop new security and tamper-resistance technologies to support that trust. The Lab tracks the external state-of-the-art and transfers technology, and Lab personnel consult with all parts of the company as well as communicating with technical and business communities.

The Lab's projects focus on areas where results have the potential to change the company's business strategy, one or more members have expertise and interest in the area, and there is a plausible idea to evaluate.

Commerce Control Language. The STAR Lab is researching languages that facilitate writing precise contracts that are readily understandable to contracting parties, yet can be translated into securely executable electronic form for use within a Protected Processing Environment. The fundamental problem is one of translating an unambiguous "language of contracts" into executable form; an additional challenge is to do so in a way that can be implemented with high-assurance, modular, secure components.

Watermarking. The STAR Lab is investigating robust technologies for watermarking or otherwise identifying content "in the clear," after it has been released from DigiBox containers in accordance with business rules. Such watermarks cannot readily be detected, removed, or altered by potential misusers of the content, and thus can assist in tracking contract violators and in

identifying the unauthorized release of protected information. The technical challenges for watermarking include data format independence, robustness, and validation.

Tamper Resistance. The initial implementations of the InterTrust architecture rely on software techniques for tamper-resistance; that is, ways of creating and structuring the software and data structures to make an attacker's job more difficult, and to ensure that an attack on one instance of the system does not translate easily into compromise of other instances. STAR Lab is developing techniques that increase the tamper resistance of software, as well as investigating methods for protecting hardware, including tamper-resistant packaging, tamper detection mechanisms, and secure hardware architecture. In addition, the Lab is working on system-wide fraud detection and analysis capabilities to assist InterTrust and partner organizations in detecting the inevitable tampering and tampering attempts that will occur.