Intel Security Initiative

Making PC interaction trustworthy for communications, commerce and content

The Intel Architecture Labs (IAL) Security initiative is made up of security researchers, designers and users from Intel's broad-based network of advanced research and development labs. Like its sister labs throughout Intel, IAL is commissioned to research and develop technologies that will add new users and new uses for personal computers.

This approach is consistent with Intel's strategy of pursuing market growth rather than just market segment share expansion. IAL's role in market growth is to research user needs and sponsor non-partisan, non-proprietary initiatives that will stimulate new products and applications for the PC, in turn attracting new users. The Security initiative is chartered to implement security technologies for the PC platform and for content distribution and commerce within the networked computing environment.

Key to IAL's work is its industry-wide advocacy for open architectural solutions, interoperability, and industry standards. This involves long-term IAL participation in industry standards groups and continuing cooperation with OEMs, operating system vendors, and application developers. Only when a new technology becomes widely accepted and used is IAL's work done.

The Many Facets of Security in the PC Environment

Both business and home users need to trust in the security of their connected PCs. Security takes on many meanings, each dependent upon the larger application:

- On-line shopping requires confidentiality for credit card numbers
- On-line banking, similarly, depends upon secure transactions using personal account numbers and ATM card information
- Business and personal video conferencing must be protected from eavesdropping and other security breaches
- Downloading of copyrighted material (movies, games, applications, etc.) requires protection from software and video piracy
- Remote PC management relies on secure networks

Figure 1 summarizes market needs for security technology Against this backdrop, the IAL Security initiative aims to make the networked PC trustworthy for communications, commerce and content. The applications presented in Figure 1, and many others, will thrive only when security issues are properly addressed.

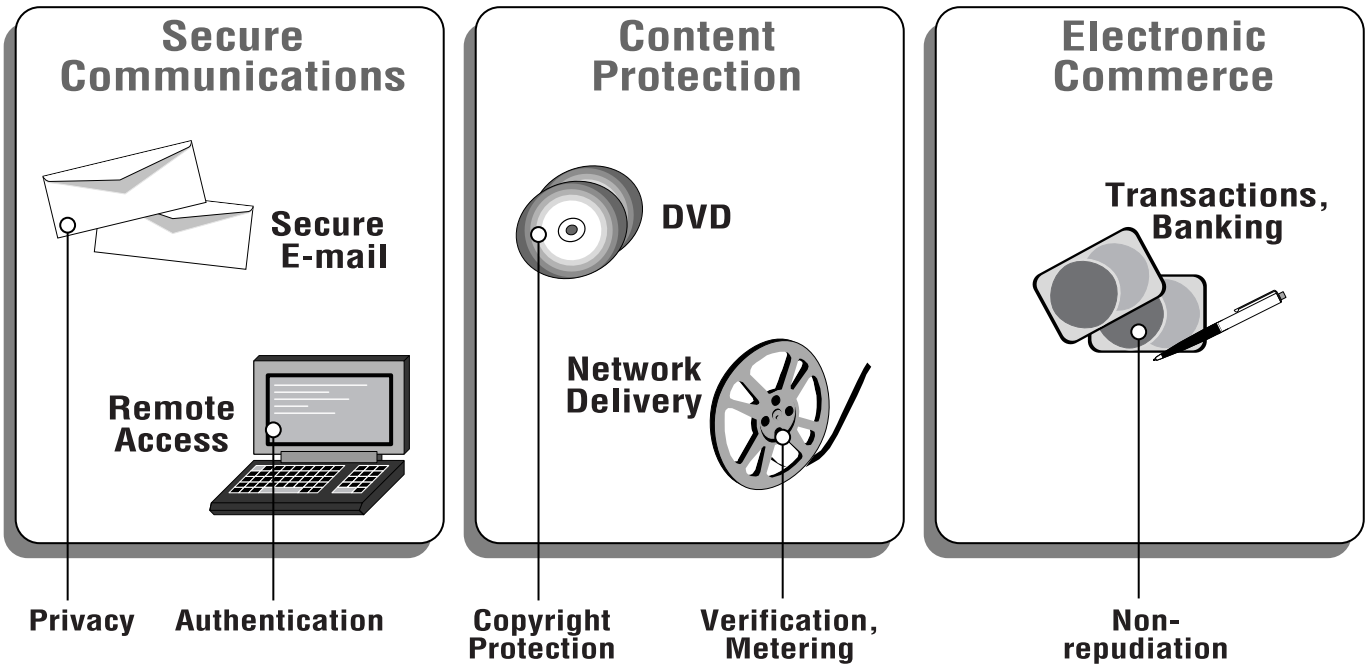

Figure 1. The Intel IALSecurity initiative aims to fulfill three basic categories of market needs for security technology.

Security Solutions

Four basic issues must be resolved to make any connected PC environment "secure." They are:

- ***Privacy*** **–** the network must be resistant to eavesdropping and intrusion
- ***Authentication*** **–** there must be a way to confirm the identity of the individual with whom one is conducting business
- ***Integrity*** **–** the content or data must be resistant to tampering and unauthorized access
- ***Non-repudiation*** **–** transactions, once concluded, must be binding; neither party involved can unilaterally disavow the transaction

The PC market is not lacking in security solutions. However, these are typically delivered as vertical solutions that work only within the narrow confines of one software tool or application. For example, an accounting software package might make it possible to secure personal financial information within the application, but the security mechanisms are "woven in" and are not usable outside that environment.

> A key goal of the IAL Security initiative is to make networked PC interaction trustworthy for communications, commerce and content.

Common Data Security Architecture (CDSA) is one concrete outcome of Intel's efforts in pursuit of that goal. Unique in the industry, CDSA specifies a security infrastructure that is operating-system independent and open. It takes into account the security requirements and solutions gathered from the PC industry as a whole. The specification is currently under evaluation by ranks of ISVs and has been accepted by many leading platform and application vendors. By defining a standard Applications Programming Interface (API) for security, CDSA will foster new PC applications and users by reducing time-to-market and engineering costs for developers of new applications requiring security.

Common Data Security Architecture (CDSA)

CDSA is designed as an overall infrastructure for data security on PCs, workstations, and servers. It is founded on two fundamental data security premises: digital certificates (a form of electronic identification which enables a hierarchy of trust, dependent on the identity of the user) and portable digital tokens which store cryptographic keys and perform cryptographic operations.

CDSA truly lives up to the term "infrastructure." It defines three layers, each building on the more fundamental services of the layer below it. The architecture is shown in block-diagram form in Figure 2. The bottom layer is made up of add-in security modules that start with basic components – cryptographic algorithms, base certificate manipulation facilities, and storage – and build up to secure, digital certificate-based transaction protocols in the uppermost layer (System Security Services). CDSA supports diverse programming environments, ranging from ANSI C to Java. The architecture is designed to be both modular and extensible. The extensible framework supports inserting domain-specific services like manipulation of IETF-standard X.509V3 certificates and digital "signaturing." Extensibility is important because it encourages ISVs to develop incremental functionality and performance improvements to remain competitive. Yet the basis for these developments is still the accepted, interoperable CDSA architecture.

Security Add-In Modules Layer

Four logical types of security add-ins (also known as plug-ins) integrate into the CDSA environment. These are:

- ***Cryptographic Service Providers (CSP)***

CSPs perform cryptographic operations such as bulk encrypting, digesting and signaturing; in addition, they store private keys. CSPs are the "lock and key" components of the CDSA structure.

- ***Trust Policy (TP) modules***

TPs implement policies are defined by authorities and institutions and set the level of trust required to carry out specific actions (such as issuing a check or access to confidential intellectual property). The modular concept permits TP add-ins to be associated with specific institutions' needs; a credit card issuer might have different trust policies than, say, a government agency.

- ***Certificate Library (CL) modules***

CLs provide syntactic manipulation of stored certificates and revocation lists, as well as access to remote signing capabilities known as Certification Authorities (CA).

- ***Data Storage Library modules (DL)***

DLs provide stable storage for security-related data objects – certificates, cryptographic keys, policy objects and more. The actual storage may be in a commercially-available database system, a native file system, a custom hardware device, etc. DLs are analogous to a "file cabinet" for security data.

Add-in modules may be provided by any number of independent software or hardware vendors; thus the CDSA emphasis on openness and interoperability. Applications directly or indirectly select the add-ins needed for specific security services. These add-ins may in turn invoke other add-ins to carry out portions of their task.

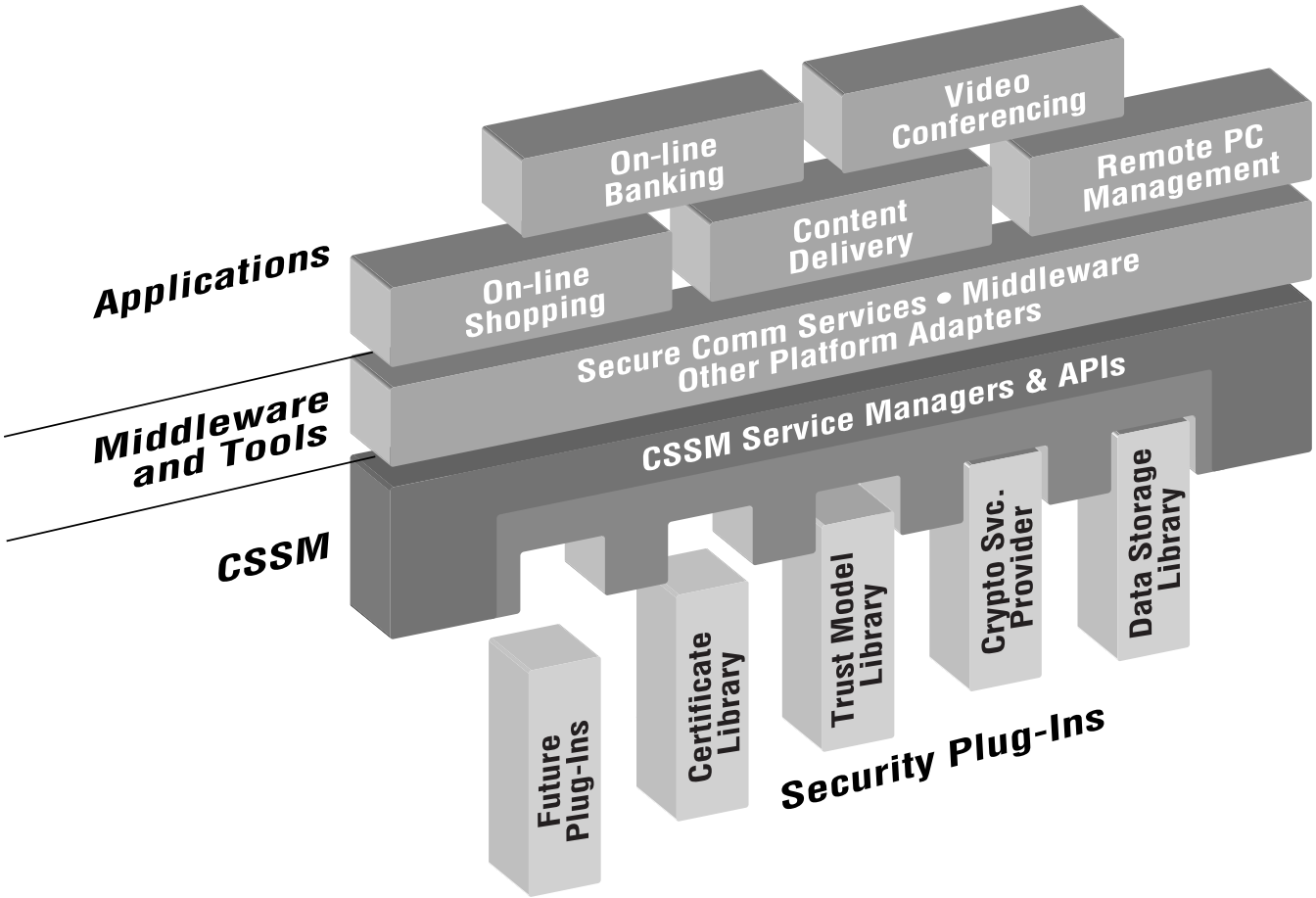

Figure 2. The Common Data Security Architecture (CDSA) consists of three, infrastructure layers: Each layer builds on the more basic underlying services positioned beneath it in the diagram.

Common Security Services Manager

The heart of CDSA is the Common Security Services Manager (CSSM), which accepts the software plug-ins and provides a path for both vertical and general-purpose security solutions. CSSM is an API with openly published specifications.

CSSM facilitates linking of digital certificates to cryptographic actions and trust protocols. It allows security-unaware applications to make high-level API calls for access to the security services. The actions that result from these calls include performing cryptographic operations, determining the trust level of a certificate holder, manipulating certificates, and accessing data storage media.

The add-in module types described earlier are mated to APIs and managers within CSSM. Thus, there is an API/manager pairing for each type of add-in: Cryptographic Services API and manager, Trust Policy API and manager, and so on.

The CSSM framework, including the high-level Security API that caps the CSSM layer, delivers important benefits to the CDSA architecture as a whole:

- It performs matchmaking between callers who need security services and providers of same
- It verifies the identity and integrity of components when they are dynamically added to the system
- It allows the dynamic addition of optional APIs for envisioned new categories of security services; APIs to support biometric devices performing recognition, for example

System Security Services Layer

The uppermost layer of CDSA is the System Security Services layer. This layer makes CSSM security services available to applications; it provides tools to manage the security infrastructure; and it provides transparent security services for file systems and private communications.

An Emerging Industry Convention

CDSA is fast establishing itself as a contender for broad industry adoption. The Open Group, a worldwide standards body dedicated to the advancement of multivendor standards for information systems, has approved a draft proposal for CDSA. Final approval is expected before the end of 1997. Equally important, CDSA supports and is interoperable with industry security standards that focus on specific aspects of security; for example, SSL, X.509V3, and PKCS 11.

Intel has taken a step beyond the usual sharing of APIs to encourage the use of CDSA, and the CDSA “installed base” is expanding quickly. Netscape,* to name one prominent user, plans to implement CDSA as the security API for future products. Implementations like this will benefit from the rapid time-to-market and reduced development costs that come with choosing CDSA.

Intel’s own LANDesk® family of network management products includes a Configuration Manager, a virus protection program, and more – and uses CDSA technology throughout. Intel LANDesk products permit remote PC management over LANs, and rely on CDSA tools to provide security within this “wired for management” application. Exacting security procedures are especially important in such an environment, where risks can range from eavesdropping to malicious tampering. The Intel LANDesk application uses CDSA to provide authenticated connections when performing remote system management services.

Intel maintains a world wide web home page devoted to security technology, and CDSA in particular. The URL for the site is http://developer.intel.com/ial/security/. More information about the Open Group is available at http://www.opengroup.org/.

Other Security Work at Intel Architecture Labs

While CDSA is Intel's best-known security deliverable, it is not the company's only security effort. As a co-developer of the open Internet telephony standard known as H.323, Intel has joined its industry partners in extensive efforts to ensure that H.323-compliant communications can pass through institutional "firewalls." The effort involved the design of an H.323 proxy that works with firewalls to pass legitimate H.323 traffic. An implementation of the proxy for the Windows* 95 and Windows NT* platforms was developed and tested. In addition, Intel worked with leading firewall vendors to include H.323 support in their products, providing consultation and testing (for Cisco Systems and Checkpoint) or licensing the source code outright (for Trusted Information Systems and Raptor).

Many enterprises want to use the Internet for business communication among branch offices, remote users, partners, suppliers and customers. IPSEC and ISAKMP very likely will be the foundation of secure communication as the Internet matures, and IPSEC implementations are expected to be available on all PCs shortly. Therefore, Intel has focused on building implementations of ISAKMP and related components to enable integration into other products. Like the H.323 program mentioned earlier, Intel developed technology that was integrated into a broader set of products. For additional information, check out RFCs 1825-1829, and draft-ietf-ipsec,-* available at ftp://ds.internic.net.

Another area of Intel security work relates to content protection for Digital Versatile Disks (DVD). First-generation DVDs lack true copy protection in the digital domain. This problem is impeding the acceptance of the medium by content providers – the motion picture industry in particular. Intel has been closely involved with DVD industry groups to propose a more secure software-based playback scheme.

Conclusion

Connected (networked) PCs are now the norm, where just a few years ago they were the exception. The networked PC environment has made security a major concern for businesses and consumers alike. It is now clear that applications such as on-line transactions, Internet telephony, and content delivery cannot prosper unless networks are made secure. The mission of the IAL Security initiative is to address these concerns: to make networked PC interaction trustworthy for communications, commerce and content. IAL has provided industry leadership with open, interoperable security solutions – notably the Common Data Security Architecture – that clear the path for PC market growth.