Client Security Solutions

Clain Anderson
Program Director, Client Security

IBM Personal Computing Division
February 12, 2003

Security Environment

- 591,000 mobile computers stolen in US. in 2001
  - *"I know of some thefts of executives laptops that would make your blood curdle, especially if you were investing in their companies..." - Ravi Hariprasad, CEO of Lucira Technologies, a laptop security provider. **
- Corporate spending on security is up 100% over 1999 and is estimated to grow tenfold over the next decade
- Corporate implementation of PKI/encryption is accelerating at 61% CAGR from $281 in 1999 to 3 billion in 2004 **
- Dramatic increase in Virtual Private Network (VPN) spending
- Share Survey (top IBM accounts) shows security #1 issue (#5 in 2000)

** USA Today, 4/10/2002*

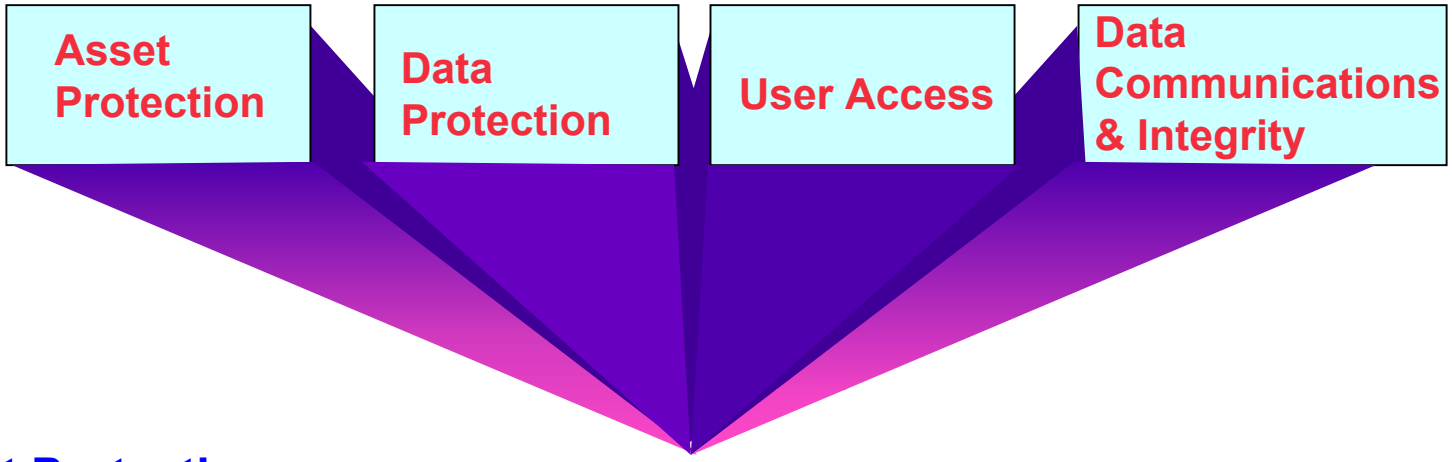
** IDC study

The security threat is real and growing

- By any measure, the security threat
  - *is large*
  - *it is growing*
  - *and it is expensive*

Computer Security Institute "Computer Crime and Security Survey"

What Customer Needs are Driving Client Security?



Asset Protection

- If my asset is stolen or damaged...how can it be replaced?
- If my asset is stolen...how can I recover it?
- How can I track the present location of my assets?
- How can I inventory my asset upon purchase?

User Access & Authentication

- How can I protect my PC assets from unauthorized use?
- How can I protect sensitive data from wrongful access?
- How can I administer a uniform security policy in my company to control access to critical data?
- How can I reduce the cost of password administration and still allow access to only those who need it?

Data Protection

- How can I protect sensitive data from wrongful access?
- If my Thinkpad is stolen, how can I protect the data from being accessed?
- If my data is lost, stolen, or damaged, how can I recover it?

Data Communications & Integrity

- Can I use Wireless LAN without exposing confidential data?
- How do I know that the data I just received wasn't read in by someone on the internet, such as my competitors?
- How do I know data received was not tampered with in transit?
- Do I have to buy extra software to begin using encrypted email?

TCPA – A new PC Standard for Platform Security

Trusted Computing Platform Alliance

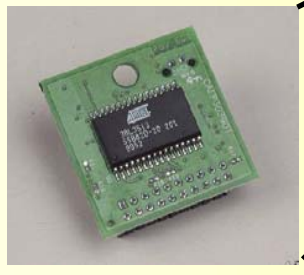
- Cross-industry standards group founded by IBM, Microsoft, Intel, HP, and Compaq
- Founded in 1999
- Now includes 190+ members

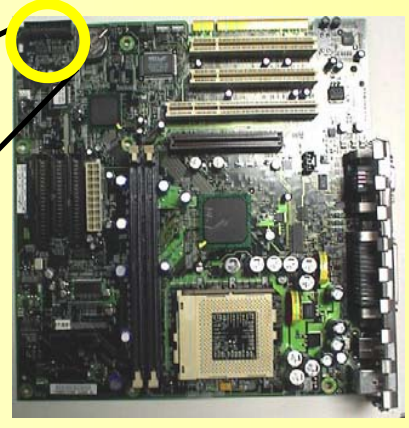
IBM Thinkpads and NetVistas (ThinkCentre) are the world's first TCPA 1.1 Compliant PCs

- On-chip key generation
- Up to 2048-bit keys supported
- Pre-boot BIOS checks to insure system integrity
- NOT yet Common Criteria or FIPS-140 Certified (both early 2003)
- All major new Thinkpad and NetVista platform announcements from this point forward will be TCPA-compliant

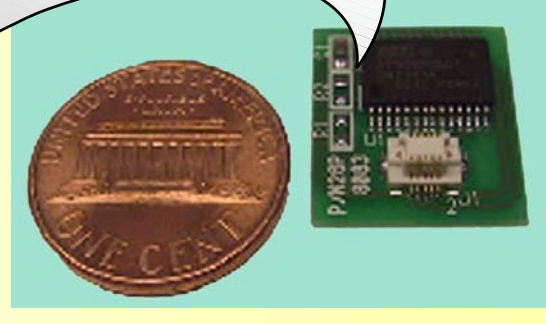
The Security Chip – First shipped in September 1999

NetVista Security Chip



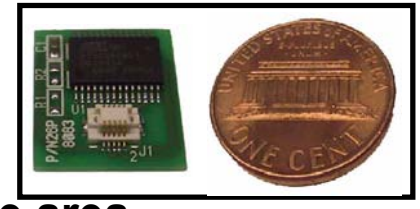


ThinkPad Security Chip



TCPA Embedded Security Subsystem - What is it?

Security Chip on the MainBoard of the PC

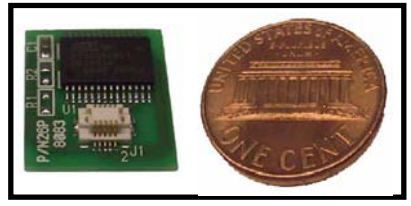


- Inert when shipped from factory
- Contains an encryption engine and secure storage area
- Base keys are generated on the chip and stored on the chip
  - ✓Keys never exposed in memory or on hard drive
- Price $25 list price, unit quantity 1

Client Security Software & Drivers

- IBM version includes free including future upgrades
- Communicates with outside software through PKCS#11 and MSCAPI
  - ✓Works w/Outlook, Internet Explorer, Netscape, etc.
- Free aplets available for On-the-fly file Encryption and Password Manager

Embedded Security Subsystem - What does it do? - 1



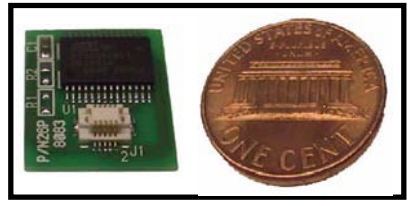
Hardware Token Replacement

- Hardware tokens can be emulated to simplify application of security policy
  - ✓RSA SecurID token is highly secure – perhaps the best hardware token and can be emulated with RSA Software used with ESS
  - ✓Authentication tools can be applied to control token access
  - ✓ROI is positive
  - ✓Convenience and administration is improved

Enhanced Wireless Security

- ESS can securely store wireless certificates / credentials
- Transport Layer Services (TLS) under 802.1X works effortlessly and can provide a substantial security gain
- LEAP can be enhanced by ESS storage of digital credentials

Embedded Security Subsystem - What does it do? - 2



File and folder Encryption

- Supported by the ESS encryption engine
- On-the-fly encryption available now

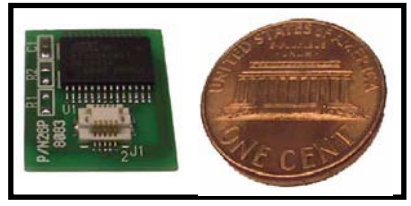
Secure Storage of Keys, Certificates, Passwords

- The essentials of your identity can be protected
- Password Manager gives full protection for passwords and "single sign-on"
  - ✓All passwords, logon IDs, and other data is encrypted and stored on your PC

Certificate Creation

- Microsoft NT Certificate Authority (CA) product works through MSCAPI

Embedded Security Subsystem - What does it do? - 3



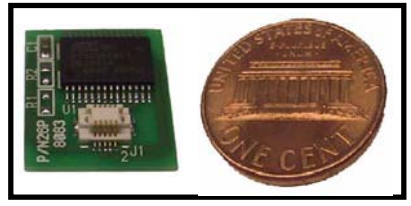
E-mail Encryption

- MS Outlook and Outlook Express are designed to work with the Embedded Security Subsystem through the MSCAPI interface
- All you need is a certificate and to check the "encrypt mail" box

Support for Popular Applications, including encryption software Suites

- Entrust
- Baltimore
- Many others that use MSCAPI and PKCS#11

Embedded Security Subsystem - What does it do? - 4



Stronger Authentication

- Platform Authentication can be added to user authentication to provide much stronger access protection - through a machine certificate tied to ESS
- ESS can perform a gate-keeper function and easily be tied to a variety of stronger authentication tools
- Authentication can be tied to specific events on the PC, including Windows logon, file encryption, applying digital signatures, password changes, etc.
- Authentication tools can include external smart cards, biometrics, proximity badges, passphrases, and more...
- ESS-controlled protection is offered for Lotus Notes logon and Entrust logon

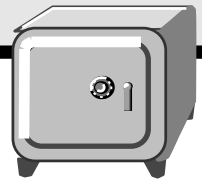
ESS-The Perfect Complement to Smart Cards

What can you do with ESS AND Smart Cards?

- Secure Client Roaming - Authenticate the user to the PC, then authenticate the PC to the network
- Multifactor authentication - Smart Cards as ESS authentication token along with biometrics, proximity badges, passphrases, and any new authentication tool
- Division of tasks – use ESS for secure on-board crypto operations, use smart card for authentication, building access, stored value functions, and more
- The combination is more secure than either used alone

PC Client Security Issues and Solutions

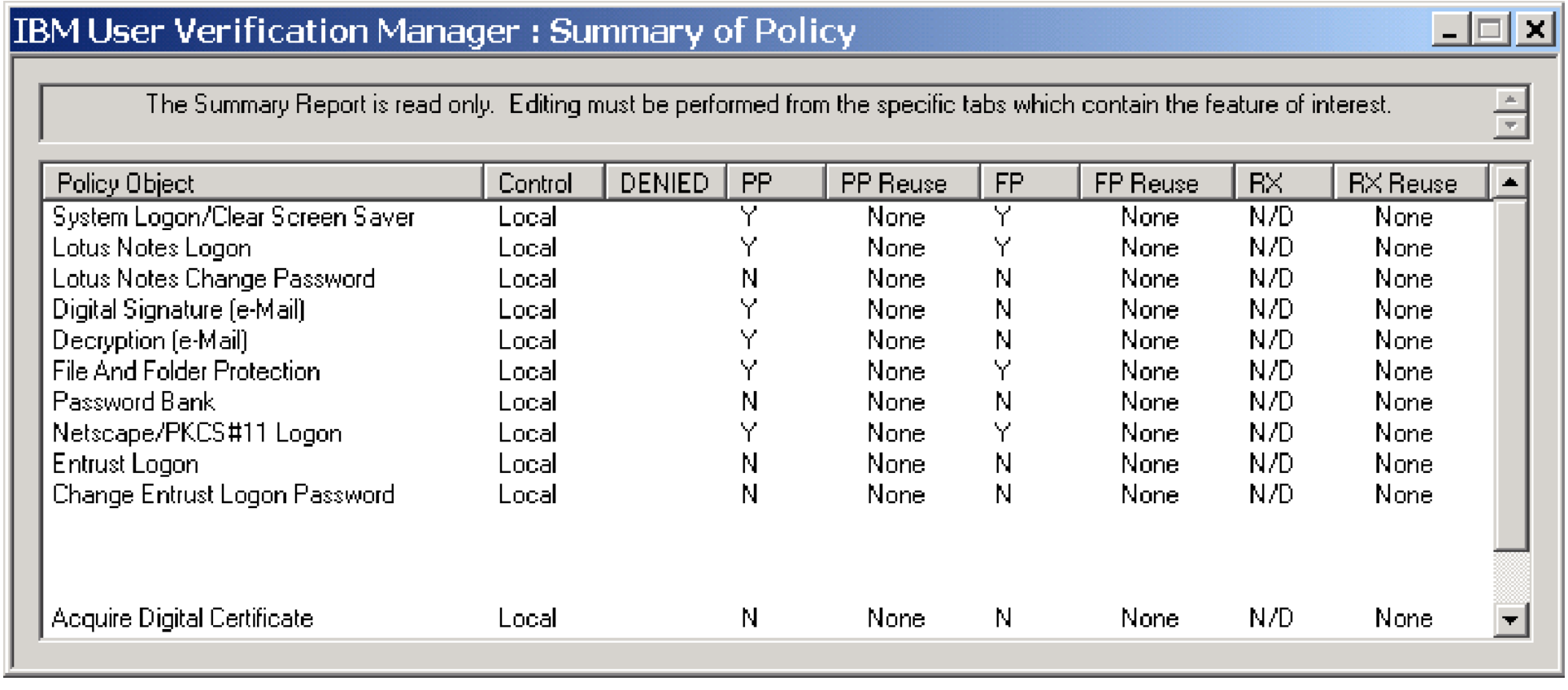
Asset protection	User authorization and access	Data protection	Data communications and integrity
Issue: PCs may be lost or stolen	**Issue:** Access of unauthorized users must be restricted	**Issue:** Data resident on hard drives is at risk of compromise	**Issue:** Communications via e-mail, cable/DSL, and wireless are at risk
IBM solutions: ➢Assurant Comprehensive PC Protection ➢Absolute SW PC Tracking and loss control (Computrace PC Theft Tracing)	**IBM solutions:** ➢**User Verification Manager (UVM)** ➢**Embedded Security Subsystem (ESS) allows user-selectable combinations of supplements pass-phrases, biometrics, and proximity badges**	**IBM solutions:** ➢IBM ESS Security Subsystem encrypts digital IDs ➢IBM ESS supports encryption of HD files and folders ➢IBM ESS supports both RSA SecurID and Entrust SW	**IBM solutions:** ➢IBM ESS secures wireless communication -Supports VPN technology -Uses 802.1x transport layer services (TLS) ➢IBM ESS supports MS Outlook and Outlook Express e-mail encryption
Customer Benefits: ➢Financial protection against damage or loss of Thinkpad ➢Increased likelihood of recovery of stolen PCs	**Customer Benefits:** ➢Strongest available policy control over key PC events, including sytem logon, email encryption and decryption, file encryption / decryption, and more	**Customer Benefits:** ➢Best available protection of hard drive files, digital keys and certificates, ➢Lower cost replacement of smart cards and other hard tokens	**Customer Benefits:** ➢Best available protection of wireless LAN credentials under 802.1X ➢Strong protection of email utilizing standard MS mail packages



Client Security Software – Platform Policy control

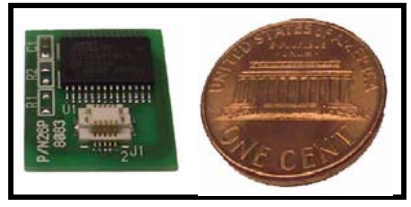
IBM User Verification Manager (UVM)

Policy Summary



Policy Object	Control	DENIED	PP	PP Reuse	FP	FP Reuse	RX	RX Reuse
System Logon/Clear Screen Saver	Local		Y	None	Y	None	N/D	None
Lotus Notes Logon	Local		Y	None	Y	None	N/D	None
Lotus Notes Change Password	Local		N	None	N	None	N/D	None
Digital Signature (e-Mail)	Local		Y	None	N	None	N/D	None
Decryption (e-Mail)	Local		Y	None	N	None	N/D	None
File And Folder Protection	Local		Y	None	Y	None	N/D	None
Password Bank	Local		N	None	N	None	N/D	None
Netscape/PKCS#11 Logon	Local		Y	None	Y	None	N/D	None
Entrust Logon	Local		N	None	N	None	N/D	None
Change Entrust Logon Password	Local		N	None	N	None	N/D	None
Acquire Digital Certificate	Local		N	None	N	None	N/D	None

Customers using Client Security Solutions



Large Pharmaceutical Company

- Rolling out tens of thousands of units
- Primary usage points:
  - ✓ Stronger security for wireless LAN (using XP/802.1X)
  - ✓ Stronger user authentication (using RSA SecureID)
  - ✓ File encryption
  - ✓ E-mail encryption is planned

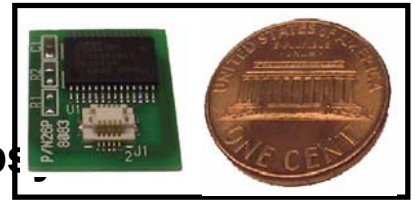
Large Manufacturing Company

- Has deployed tens of thousands of units
- Decided to implement security features in 2002
- Primary usage points:
  - ✓Certificate-based VPN
  - ✓File encryption

Regional Banks (2)

- Evaluated and adopted the ESS solution
- Deploying approx. 1-2000 units each
- Primary usage points:
  - ✓Stronger authentication
  - ✓File encryption
  - ✓E-mail encryption

Why IBM for Client Security?



Client Hardware Leadership

- First in the industry with Embedded Security Subs
- Lower cost than equivalent solutions (per Gartner Cost Model)
- First to develop ties to a spectrum of solution elements
  - ✓RSA, Entrust, Ensure, Targus, Checkpoint, Tivoli, etc.
- First to obtain Common Criteria Certification

Client Software Leadership

- IBM licensing security middleware to enable the industry
- Client Security Software 5th generation available October 25

Services Leadership

- Largest security services team on earth
  - ✓Assessment, integration, implementation

Where to find more info...

- www.trustedcomputing.org
- www.ibm.com/security
- www.pc.ibm.com/ww/ibmpc/security