 wave[®] Secure Electronic Commerce and Content Distribution Services

Trusted Input Devices Distributed Strong Authentication

States Security Research Workshop
Carnegie Mellon University
March 28, 2002
Lark M. Allen / Wave Systems
Lallen@wavesys.com

Authentication Challenges

- ❑ Personal computers are *untrusted* devices
 - Input, processing, and output cannot be protected or hidden from interception, observation, and hacking
- ❑ Centralized authentication approaches have major issues
 - Broadly available national biometric databases for fingerprints, facial prints, iris scans, and other personally identifiable information are unlikely due to privacy issues
 - Inadequate scalability and long response times for most applications
- ❑ Identity is context related (businesses, organizations, states) with little or no interoperability
- ❑ No indemnification for authentication 'mistakes'

3/30/02 2

Authentication and Privacy wave

- Privacy is growing social issue, even post 9/11
- EU, Canada and others with tough Data Protection laws
- Authentication and Privacy must find acceptable 'balance'
- Where authentication is done will affect privacy concerns
- Users will 'opt-in' for benefits, i.e. faster airport security


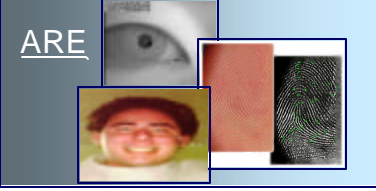


Location of Authentication

Privacy Concerns

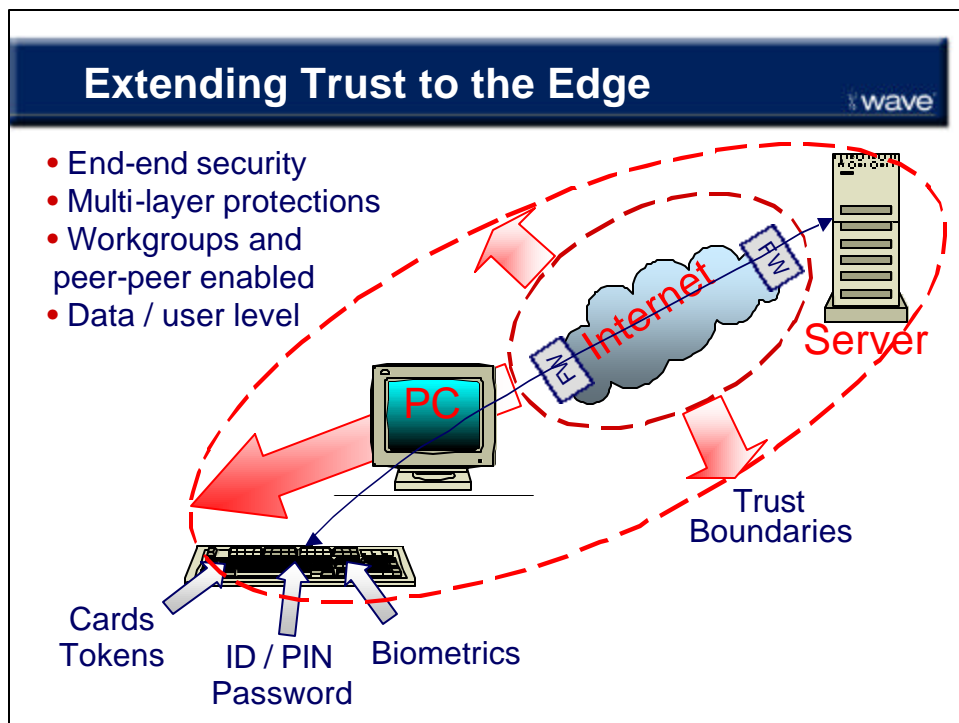
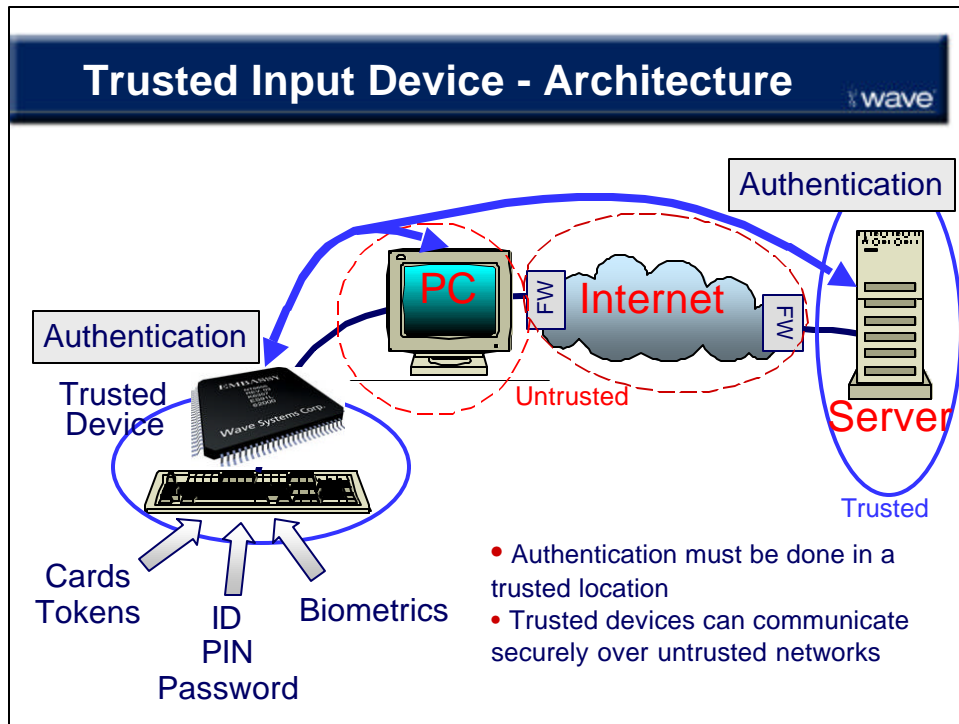
User

'Near' User Local Regional National Intrnl.

Authentication –Trusted? wave

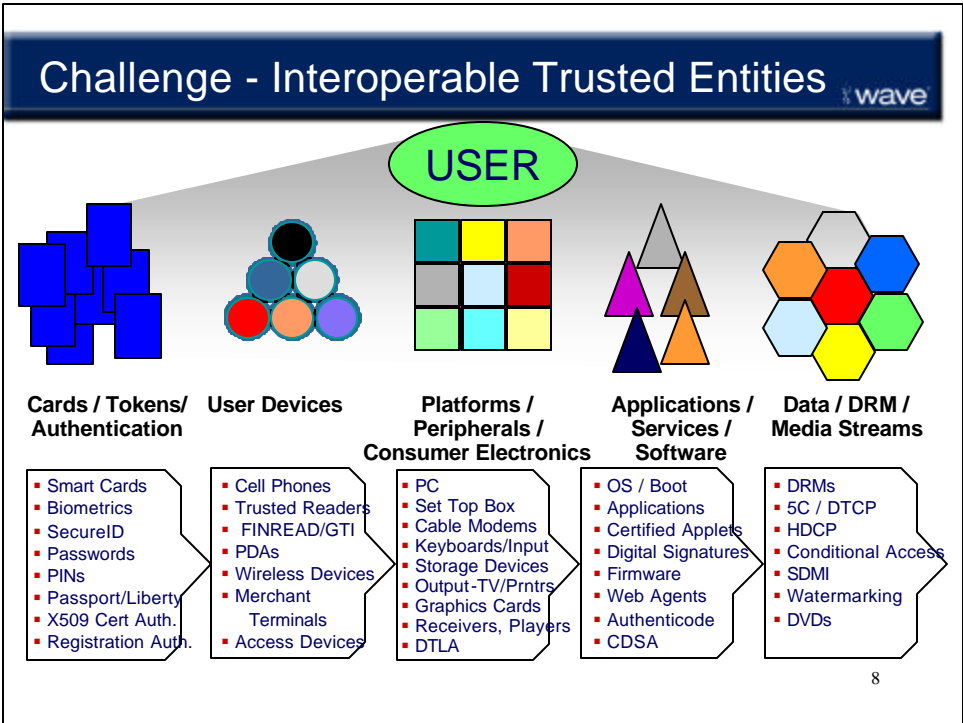
Identity	Authentication
<p>HAVE</p>  <p>KNOW</p> <ul style="list-style-type: none"> • Password • User ID • PIN <p>ARE</p> 	<p style="text-align: center;"><u>Trusted</u></p>  <p style="text-align: center;"><u>Untrusted</u></p> 

Access




Infrastructure Security Requirements wave

- Dynamic and broad range of security needs
 - ◆ Platform, File, and Application Security
 - ◆ Strong Authentication
 - ◆ Content and Services Protection
 - ◆ Privacy Solutions
 - ◆ E-Commerce
 - ◆ VPNs, Communications
 - ◆ Digital Signatures
- Security of hardware, flexibility of software, future-proof
- Internet must deploy new trusted layer – every component and device must have ‘trusted’ mode

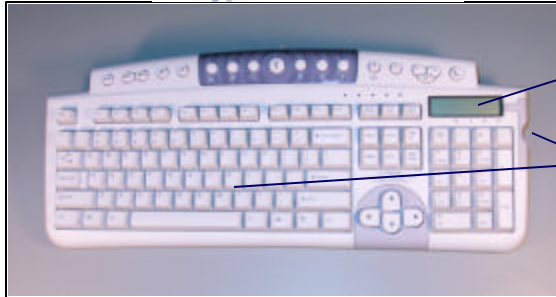


Trusted Input Device - Components wave

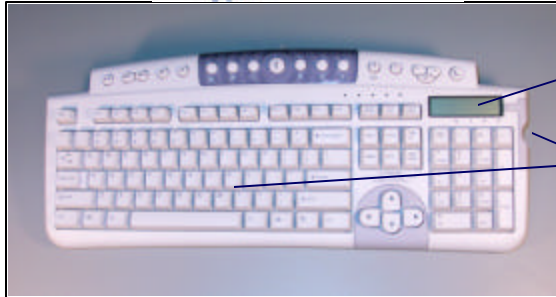
**EMBASSY
Trusted
Client
Platform**



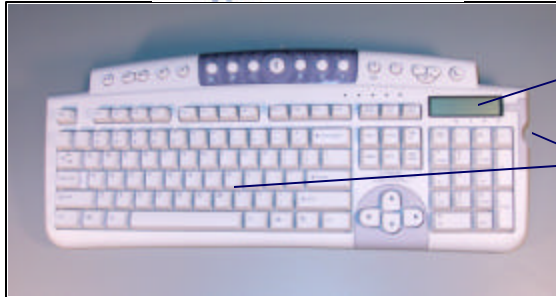
Strong
Cryptography



Secure
Processing
• Storage
• Time



Secure
Display



Secure
Input

Trusted Input Devices - Applications wave

- Finance Industry
 - FinRead – European Union Spec for Trusted Financial Readers
 - ‘Card Holder Present’ E-Commerce Transactions
- Strong Authentication
 - Network and System Access
 - Digital Signature
 - Physical Access
- On-Line Gaming
 - Financial, GPS, Biometric, Smart Card, Password Authentication
- Entertainment
 - Age-Based Access

