Securing Next-generation Mobile Platforms: The User-to-Device Authentication Issue



MPSoC (August 2006)

Srivaths Ravi (Email: sravi@nec-labs.com) NEC Laboratories America Princeton, NJ **Security Requirements of Mobile Appliances**





A Case for Biometrics

- Conventional solutions (E.g., passwords, Tokens)
 - Easy-to-break: Most commonly used password is "password"
 - Cumbersome: 30% of system-admin help desk calls are reset requests
- Cost of insecurity is very high
 - 3.3 million identity thefts in U.S.(2002)
 - 6.7 million victims of credit card fraud
 - US\$ 10 billion loss per year due to identity theft (Gartner, 2002)
- Solution: Use of biometrics
- Physiological traits that are unique to an individual & easily quantifiable
 - Fingerprint
 - Voice
 - Face
 - Iris
 - Hand geometry





Voice recognition



Fingerprint





How does Biometric Authentication Work? (An Example: Fingerprint)







- Current solutions
 - Using better sensors: MORE COST
 - Dedicated chip for biometric authentication: MORE COST
 - Trade-off between performance and accuracy
 - E.g., skip image enhancement steps
 - LOWER ACCURACY

Srivaths Ravi

NEC Labs America



	Test	Test Parameter	False Reject Rate	False Accept Rate
Fingerprint	FVC [2004]	20 years (average age)	2%	2%
Face	FRVT [2002]	Varied Lighting (outdoor/ind oor)	10%	1%
Voice	NI ST [2000]	Text independent	10-20%	2-5%

(Courtesy: Anil Jain, MSU)

- × High inaccuracies for uni-modal biometric technologies
 - × Can deny legal user entry
 - × Can provide unauthorized user access
- × Poor User Experience
- × Low Security

Srivaths Ravi

NEC Labs America



Summary of Challenges



- Performance Gap
 - Computational workload of biometric authentication algorithms can overwhelm embedded processor capabilities
- Accuracy
 - Biometric authentication accuracy (false accept/reject) needs to be significantly improved
- Attack Resistance
 - Protect the authentication process from implementation attacks (physical, SW,..)

Srivaths Ravi

NEC Labs America

HW/SW Multimodal Biometric Platform



Multi-modal biometric manager SW

Higher security by combining biometrics
Multi-threaded for efficient utilization of multi-processor platforms
Mobile biometric processor

Custom instruction set accelerates biometric algorithms

Over 10X speedup

Low overheads

Attack resistance

Several elements including boot-time verification, runtime protection using access control monitors, etc.



Benefits: Faster Authentication



Benefits: Improved Accuracy



