

Identity Crisis: The Day My PC Mistook Me For A Hat*

GOPI KURUP



August 2010

* With apologies to Oliver Sacks

Extol MSC

- **Extol Corp**
 - 25th year in business
 - Grown from a general PC and IT trading house to a leading ICT Security solution provider
- **R&D successes**
 - ARMOUR 1st Malaysian AV software – bi-directional technology transfer to Norman (1994), 1.5M copies bought by U.S. Dept of Defense, Dept of Energy, official AV for Kuala Lumpur XVI Commonwealth Games (1998)
 - OpenVoice – voice attendant & mail module bundled with Toshiba PABX systems (1997)
 - 1st Malaysian RACE ADSL modem – developed by subsidiary, Cronos Systems (2001)

Extol MSC

- Human capital
 - Staff strength ~ 70
 - ~ 75% with technical background
 - ~ 25% full-time R&D staff (inc mathematicians, physicists and engineers), contract staff from global talent pool
 - CMMI L3 compliant, ISO27001:2005, ISO9001:2000, CDP Software Testing Capability
- Selected products
 - Managed Security Services, AI-Authentication Systems, Mobile Applications, Professional Services

Landscape Snapshot



Global Threats



Insider Threats



Exploiting Vulnerabilities



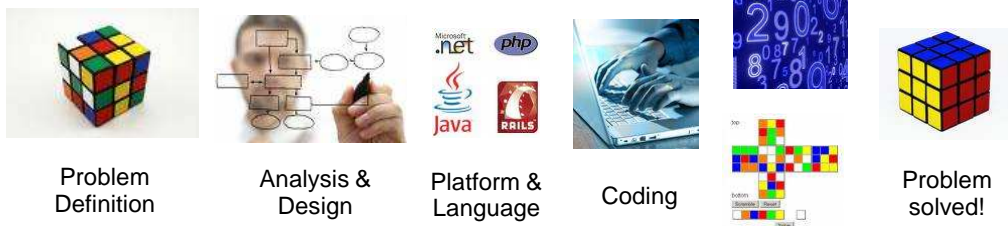
Emerging Threats

General Trends

- Attackers are proactive
- Defenders are reactive
- Attack mechanisms getting cheaper
- Defense mechanisms getting more expensive
- Attacks can be measured; defense mechanisms?

- Limitations of rule-based solutions
- Revisiting self learning mechanisms
- Scalable solutions

Current Solutions



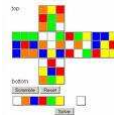
Problem Statement



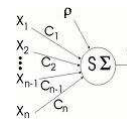
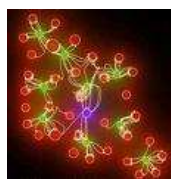
??



Give Me A Break!



Artificial Intelligence Systems



Mathematical Models → **Software Systems**
Solves Complex, Dynamic & Non-linear Problems

Can be applied to...



Face Recognition



Signature Verification



Computer Virus Detection



Surveillance Platforms



Business Intelligence



Biological Virus Identification

and many more applications..

Existing AI Solutions

- AI technologies & techniques
 - Tightly coupled to vertical applications
 - Face Recognition AI API cannot be reused for Virus Detection although they may share many similar underlying mechanisms
 - not scalable, flexible
 - Delayed software prototyping process
 - developers lack AI knowledge/skills (mathematical problem, not IT)
 - current NN training process inefficient for commercial applications
 - new data preprocessing and algorithms for each application (not reusable)

Existing AI Solutions

- Limited commercial Application Programming Interfaces (APIs)
 - expensive
 - not comprehensive for a multitude of applications
 - protected for military applications (technology export/sale restrictions)

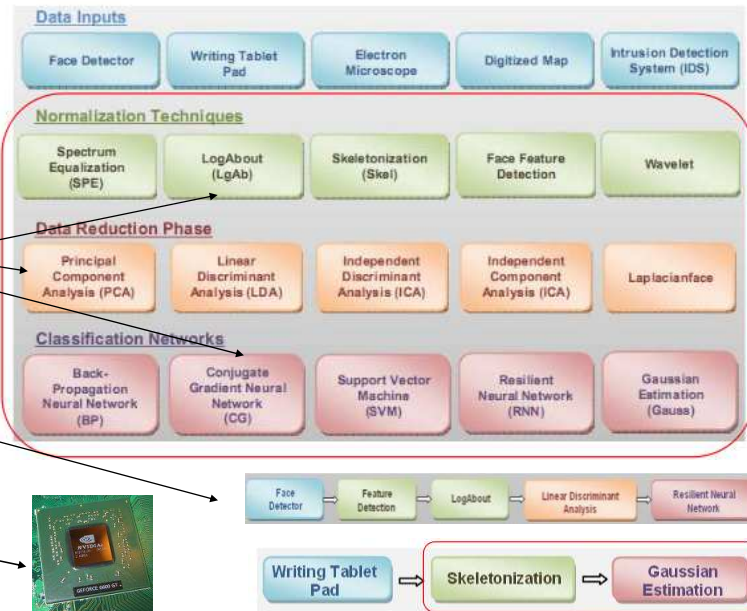
Research Areas

Comprehensive AI framework & techniques within each layer

Algorithm design for specific techniques to suit applications

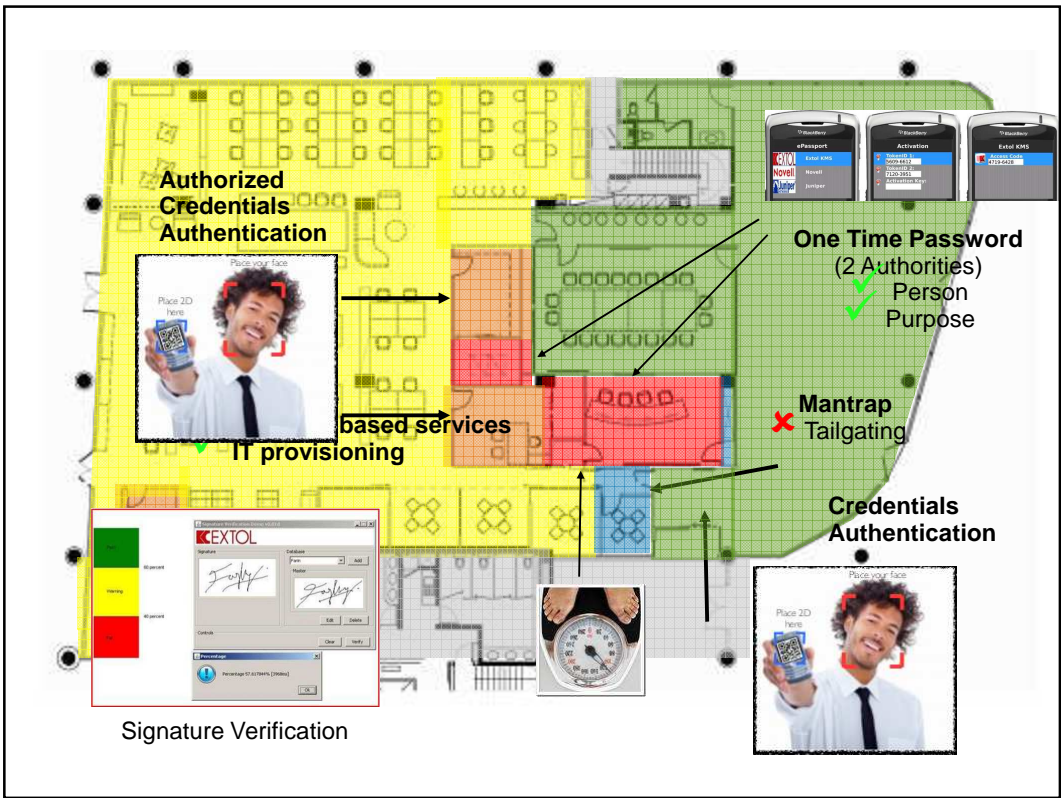
Optimization for individual AI-APIs

Maximize AI training capability and efficiency



Making Sense

- Data collection
 - Physical or geo-spatial
 - Trusted and untrusted domains
 - Location specific encryption
 - Biometric information
 - Electronic
- Correlation
- Heuristics



Thank You

Research

Cryptography



Authentication



Integrity



Training &
Awareness

Audits, Risk
Analysis &
Security Policies