Overview of SCRUB
Research Thrusts

Thin intermediation layer

Mobile security

Security analytics

Data-centric security

SCRUB
Secure Thin Intermediation Layer

Applications
- CloudTerminal
- Verifiable Resource Accounting

Primitives
- Attested Execution Tracing
- Control-flow Integrity

Verification
- PokeEMU
- S2W

Infrastructure
- Robot AppStore
- fileProxy
- PPD
  w/ Data-Centric
Mobile Security Thrust

MOBILE PLATFORMS
- Permission systems
- Understand users
- Secure mobile OS

APP ANALYSIS
- TaintDroid

→ Secure app ecosystem, secure mobile devices
Security Analytics Thrust

Anthony D. Joseph (UCB)
Rachel Greenstadt (Drexel), Ling Huang (Intel), Dawn Song (UCB), Doug Tygar (UCB)
Security Analytics Goals

- Collaborate with Intel and McAfee to identify applications and datasets
  - In addition to analyzing data from other ISTC thrusts

- Develop robust security metrics and analytics
  - Developing tools combining machine learning and program analysis to automatically extract features and build models
  - Improving users’ experiences by translating the reasoning behind security decisions into human understandable concepts
  - Designing robust algorithms for large-scale machine-learning in the presence of adversarial manipulation
Large-scale Machine Learning for Security

(Distributed) data sources // The Digital & Physical World

- Human Biosignals (EEG, vision tracking)
- Social Media (comments, stylometry)
- Program analysis (apps, malwares)
- Logs (Network, system, Malware traces)

Heterogeneous (noisy & adversarial) data

Knowledge extraction

- Feature extraction and selection
- Feature representations
- Machine learning (ML) and modeling

Refined information & models

Security applications

- User authentication
- User ID
- Anomaly/Spam detection
- Decision support
- Forensic/Risk analysis
- Activity recognition
Update

- Built suite of security analytics tools
  - Stylometry – authorship recognition at large-scale
  - Detect adversaries in text and comments
  - Detect human biosignals – EEG, vision tracking
  - Privacy preserving data analysis

- Working with McAfee to mine Global Threat Intelligence databases
  - Develop tools to sanitize data by removing identifying information
  - Detecting stealthy attacks (APTs and TPTs)
  - Applying stylometry to attacker identification
Summary – Security Analytics Thrust

Security Analytics and Metrics

- Decision Model
- Adversarial ML
- Large-scale ML
- Biometrics Collectors
- Text Analysis
- Decision Analysis
- Code Analysis
- Log Analysis

McAfee GTI DB

Metrics, Alerts

App Store
Data-Centric Security Thrust

Dawn Song
Petros Maniatis, Adrian Perrig, Scott Shenker
Main Security Problem: Security of Data

• Users, enterprise, governments
  – More and more digital assets & private data
  – Big Data, cloud => security of data?
We Need Stronger Capabilities

• Where is your data?
• Who can access the data?
• What has happened to your data?
• How to securely access your data even when your machine may be compromised?
• What properties can you ensure about your data even when service providers may not be trusted?
Vision

• Imagine if ...
  – Users/trusted third-parties could audit what has happened to their data and control how their data will be used
  – Programmers could easily develop privacy-aware apps/systems in distributed environments
  – Security does not rely on complete trust of service providers
Specific Goals

• Trust and privacy evidence for data
• Enable simple data management
  – Location, backup, delete, audit
• Easy development of rich privacy-aware applications
• Backward compatibility with legacy systems
• Ease of deployment
• General architecture for broad applicability
• Practical performance & usability
Realizing the Vision

• Novel security abstractions & primitives
  – Cloud terminal for trusted path
  – Secure data capsules
• Novel programming framework
  – PPD: Platform for private data
  – GUPT: Privacy-preserving data analysis framework
• New eco-system
Data-Centric Security Thrust

• Novel security abstractions & primitives
  – Cloud terminal for trusted path
  – Secure data capsules

• Novel programming framework
  – PPD: Platform for private data
  – GUPT: Privacy-preserving data analysis framework
Secure Thin Intermediation Layer

Applications: CloudTerminal, Verifiable Resource Accounting
Primitives: Attested Execution Tracing, Control-flow Integrity, PokeEMU, S2W
Verification: Robot AppStore, fileProxy, PPD

Mobile Security Thrust

- Permission systems
- Understand users
- Secure mobile OS
- TaintDroid

MOBILE PLATFORMS + APP ANALYSIS → Secure app ecosystem, secure mobile devices

Security Analytics Thrust

Security Analytics and Metrics
- Decision Model
- Adversarial Machine Learning
- Biometrics Collectors
- Text Analysis
- Log Analysis
- Code Analysis
- Decision Analysis

Data-Centric Security Thrust

- Novel security abstractions & primitives
  - Cloud terminal for trusted path
  - Secure data capsules
- Novel programming framework
  - PPD: Platform for private data
  - GUPT: Privacy-preserving data analysis framework