Panel: Research Agenda for Data and Application Security

Moderator: **X. Sean Wang (NSF & University of Vermont)**

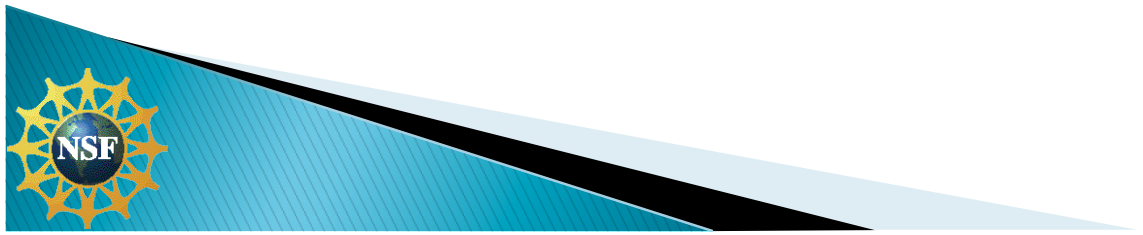
Panelists: **Mauro Conti *(Vrije Universiteit, Amsterdam)***
Calton Pu *(Georgia Tech)*
Ravi Sandhu *(UTSA)*
Dan Thomsen *(Sandia)*
Bhavani Thuraisingham *(UTDallas)*

CODASPY 2011

The views expressed herein do not necessarily reflect the views of NSF, the US Government or my employer UVM .

From CODASPY 2011 homepage

- Security concerns have rapidly *moved up* the software stack as the Internet and web have matured. The security, privacy, functionality, cost and usability tradeoffs necessary in any practical system *can* ***only*** be effectively achieved at the data and application layers.



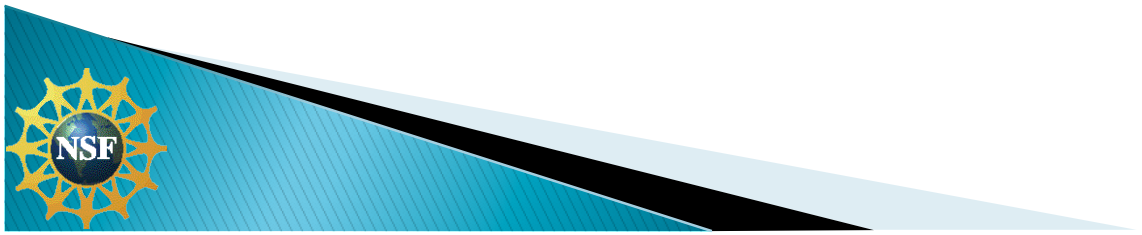
Topic uniqueness vs "traditional security"?

- Application layer security policies
- Authorization/Access Control for Applications
- Authorization/Access Control for Databases
- Data dissemination controls
- Data forensics
- Enforcement layer security policies
- Privacy preserving techniques
- Private information retrieval
- Search on protected/encrypted data
- Secure knowledge management
- Secure multiparty computations
- Secure auditing
- Secure collaboration
- Secure data provenance
- Secure electronic commerce
- Secure information sharing
- Secure software development
- ***Securing data/apps on untrusted platforms***
- Securing the semantic web
- Security and Privacy in GIS/Spatial Data
- Security and Privacy in Healthcare
- Security policies for databases
- Social computing security and privacy
- Social networking security and privacy
- Trust metrics for application, data and user
- Web application security

Most red you may generalize with "systems" or "network"… So app/data security is just a specialization of "general security"?

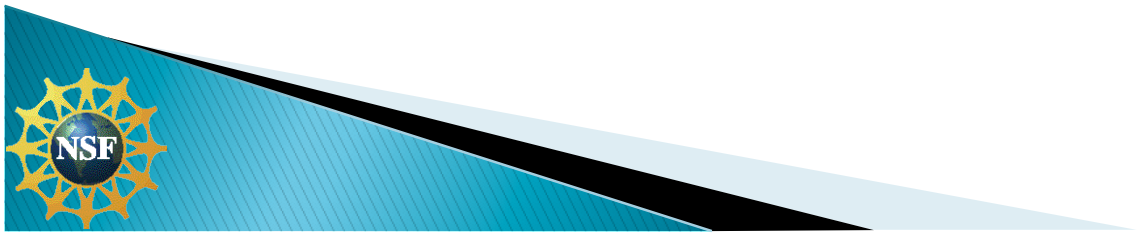
Oakland 2011 Topics

- Access control
- Accountability
- Anonymity
- Application security
- Attacks and defenses
- Authentication
- Censorship and censorship-resistance
- Distributed systems security
- Embedded systems security
- Forensics
- Hardware security
- Intrusion detection
- Language-based security
- Malware
- Metrics
- Network security
- Privacy-preserving systems
- Protocol security
- Secure information flow
- Security and privacy policies
- Security architectures
- System security
- Usability and security
- Web security



US federal cyber security and information assurance strategy (leap-ahead)

- Three research themes:
  - Tailored space
  - Moving targets
  - Cyber-economics
- Plus: Science of (Cyber) Security
- Are they relevant to app/data security? If yes, how?



Questions to the panelists

- General directions? Hardest problems? *Ravi*
- Interface with system security? *Dan*
- Is there a "science of data and application security"? *Bhavani*
- How are the federal research themes relevant to the data and application security? *Mauro*
- What about human factors and usability in data and application security? *Calton*
- How to evaluate research results in this area? *All*