Security

Thomas Ristenpart

Computer security

- Breaking computing systems
- Building computing systems --- to resist those who break things

> Studying the behavior of computing systems in the presence of malicious agents

- Confidentiality
- Availability
- Integrity
- Privacy

Computer security

- Functionality, efficiency, etc.
  - easy to specify goals
  - (usually) easy to know when met
- Security
  - easy to specify goals
  - not easy to know when met
  - Preclude all (even unforeseen) damaging attacks

Some research flavors

- Operating systems
- Network security
- Distributed systems (Byzantine fault tolerance)
- Applied cryptography
- Programming languages & software engineering (static/dynamic analysis)
- Privacy
- Usability

Recent topics of interest

- Privacy for genomic studies
- Cloud computing
- Video game anti-cheating
- Web, browser security
- Applications of trusted computing
- Malware, botnets
- Electronic voting
- Power grid security

- Security + (computer science topic x)
- Security + (technology Y)

Recent best papers

- Native client (Google) --- Oakland 2009
- Medical device security (UW, UMass) --- Oakland 2008
- Vanish (UW) --- Usenix 2009
- Cold-boot attacks (Princeton) --- Usenix 2008
- Highly-predictive blacklisting (SRI/Sans) --- Usenix ‘08

Top tier conferences

- IEEE Symposium on Security & Privacy
  - Oakland
- Network and Distributed System Security
  - NDSS
- USENIX Security
  - Security
- Computer and Communications Security
  - CCS

Where's hot?

- Stanford, Berkeley, CMU have strong groups
- UNC, UCSD, GeorgiaTech, UCSB, Princeton, JHU, UW, …
- MSR, IBM Research

Here at UCSD:

Stefan Savage (IP traceback, OS security)
Hovav Shacham (Return-oriented programming)
Geoff Voelker (URL classification)

What does UCSD do?

- Break stuff

vmware

- Economics behind e-crime

- Build secure systems

Adeona
PRIVATE, RELIABLE, OPEN SOURCE

- Security tools

Botnet Judo