PANEL 5: SECURITY AND PRIVACY OF INFORMATION SYSTEMS

KEN KLINGENSTEIN,
EHAB AL-SHAER,
ALPTEKIN KUPCU,
ALBERT LEVI,
DI MA
&
GENE TSUDIK

Security and Privacy (S&P)

- Throughout 70-s and early 80-s
  - Mainly within government/military + contractors
  - Some industry
  - Thinly represented in academic research
- Late 80-s, early 90-s
  - More industry involvement
  - Initial research funding availability
- Late 90-s
  - Lots of industry interest
  - Gradually earns academic “respect”
  - More funding (e.g., DARPA, NSA, DOE, NIST)
- Last decade
  - Much more funding (NSF, DHS, IARPA enter the game)
  - Many faculty positions & much more academic research
  - Less industry research due to worsening economy

S&P Maturity

- Secure & Trusted Computing (SATC) program at NSF
- Even the ACM now treats S&P as a first-class object in its classification update effort (on-going)
- Numerous conferences of widely varying quality
  - About 8-10 with reasonable reputations
  - Many collaborations form at these venues
  - NOTE: few ME researchers attend!
- A few reputable journals, e.g., ACM TISSEC, JoC, JCS, IEEE TDSC & TIFS

Security Research in General

- Reactive
  1. Identify existing security problems
  2. Propose techniques to address/mitigate them

  OR:

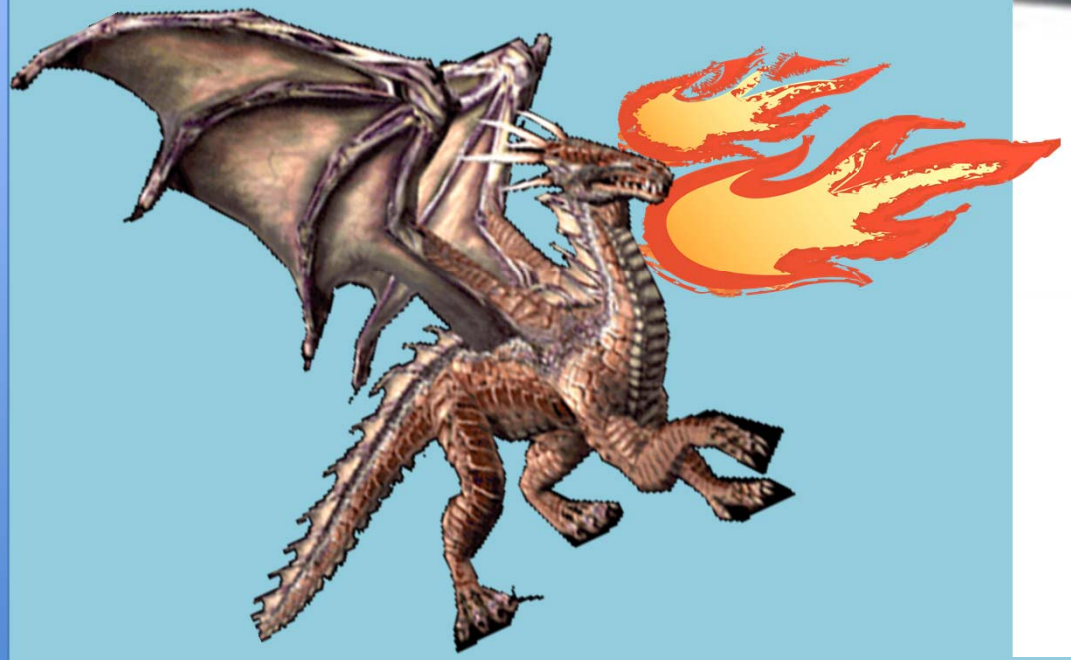
  1. Spot problems in current security methods
  2. Expose and, optionally, patch them

- Proactive: a 4-step process…

Step 1: Invent plausible, credible and very scary new adversary

Step 2: Postulate new exciting (and viable) habitat for scary new adversary

Step 3: Develop credible, effective and <u>practical</u> weapons against scary adversary



Step 4: Market and popularize your "fairy tale"

Which way?

- Reactive research gets attention & immediate appreciation
- Proactive is much riskier, but stimulates the intellect more
- Plenty of motivation for either/both in US-ME collaboration

SPROUT

Security & **P**rivacy
Research **Out**fit

http://sprout.ics.uci.edu

Current Research Interests & Directions

- Privacy-agile cryptographic protocols
  - Signing, authentication with privacy
  - Private set operations, leading to:
    - private database querying, genomic, social networking & participatory sensing applications
- Secure Embedded Systems
  - Minimal malware-resilient architectures, smart metering applications (privacy)
  - RFID applications, e.g., supply-chain tracking, malicious reader mitigation
- Candidate future Internet architectures → Named Data Networking (NDN)
  - Lots of interesting security/privacy issues stemming from named, signed content
- WSN-s and MANET-s
  - Resilient autonomous/unattended operation with mobile adversary
  - Privacy-agile mobility + routing
- Usability in/of S&P
  - Device association, security configuration
  - Privacy interfaces, RFID applications

Sample Tentative Collaboration Topics

- Anonymous low-latency communication
- Censorship mitigation
- Privacy in OSNs, micro-blogging
- S&P in Emerging Internet Architectures
- CPS security, e.g., malware resistance/detection


The End