SaTC 2029

Amit Sahai

Director of

Center *for* Encrypted Functionalities

An NSF Frontier Center

and

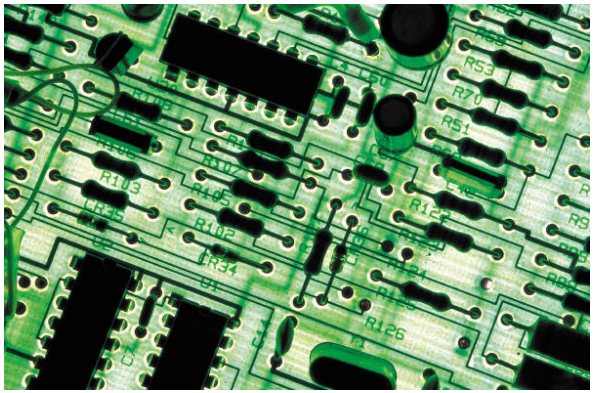
Professor, UCLA

Cat and Mouse game?

- Must security be a cat-and-mouse game between attacker and defender?
- Unfortunately, Yes…
- This is true of any adversarial human activity: war, crime, etc.

The hope for 2029…

- Move from:



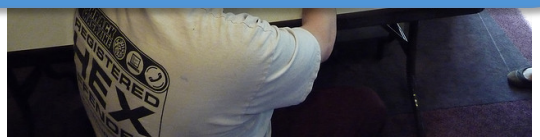
vs.

Specific System

Hacker

The hope for 2029…

- Goal:
  Security vs. large classes of attacks



Security Model
+ proof of security/
risk quantification

Hacker/
Researcher

Better Abstractions

- Bad abstractions are problematic… but we cannot realistically design systems at the level of quarks and electrons.
  - The role of science is to build better models, that more closely approximate reality, but which remain tractable
- We are still **far** from this for trusted computing, but we are getting better.
  - examples: *NSF CEF*: **mathematical program obfuscation** (full access to program), protocol concurrency, insider threats (e.g. ABE), side-channel attacks, physical tampering, …
- Won't attackers always be able to find holes in the model, assumptions?
  - Sure, but we can expect that this will cause attacks to become qualitatively/quantitatively more difficult, more costly.

Predictions for 2029 ?

- Main prediction:

  xmY4uWEvVf0pHI8H1VpuM6yOwJoVZGD29NiOXG93aIQ3qHiLPK
  2H2QI7qvoCv4iPMMCwSzx8qa7cVvlwoj70UUZJ3j20ikqsglgO
  h8F4HXJMkAFDRJBCRTKn1TGMOTgSV7WUraiYHqW8qPHuqllj2V
  vmPew84KDbi11bsZTJwJ7rDnjlDTw9tFDOvbKTIcT00A2nvBgu
  Drw9LFR8LqIwrW6f4ULsaHm4yI6QyIGWUbuGgmIJ4mlA2l9ERN
  iq0xaS5IbNi2waWVuIYExtNKJkorXm45OQnpnraDFElLuRmSaR
  pAZCSusK5ADzTCGIfoGltO86sWGE3r1emMhKkx8RNM4SKomKpk
  a7IYHicltaAmngTnYJCgXxAYI5cMW0uako0RyQYwvanYArA1WD
  gCbZfwmiz2T5lDox9nKSDHmACXBtI51bUuxYzZtoTN0TlctPE4
  GqffSFu9R9cZ0HPsRToC5eJOfnu64jRqLMiewzD4CDismMwEz6

- Of course, prediction is in encrypted form.
- Will open in 2029 to see if I was right…
  (using a one-time pad key to be revealed later)

Predictions for 2029 ?

- NSF will continue to sponsor great security research
- More security systems based on mathematical hardness.
- Cryptographic innovations (e.g. secure computation protocols, zero-knowledge attestation, mathematical obfuscation) more widely used, at least for high-security scenarios.
- More use of physical assumptions to prevent purely remote digital attacks.
- Password-only authentication extinct (?)
- Pushback vs. SaTC due to major terrorist attack where strong encryption prevented detection.
- Many new attack targets:
  - Stealing cryptocurrency keys,
  - Cyborg devices: hacking enhanced perception of reality

Predictions for 2029 ?

- **Basic Problem: Can we make castles out of excrement?**
  - Real world: poor quality software, human limitations, interoperability concerns & lack of consensus
  - E.g. for many startups, security is usually not the top priority. Software written with duct tape will continue until (?)
  - Hope: Incentive changes: Smart regulation?
    - Perhaps mandatory insurance vs. hacks
    - Govt. re-insurance to mitigate lack of actuarial data
    - Insurance companies will demand **real** (vs. buzzword-based) best practices for lower premiums (?)
  - Hope: security as a service: Paypal, authentication, …
    - Security without stifling pace of innovation (?)
  - Hope: Better engagement between SaTC Pis and policymakers

Extra slides

Center *for* Encrypted Functionalities

An NSF Frontier Center

The mind-reading adversary

- Suppose you want to keep a secret.
  But there is an adversary that:
  - Captures your entire brain
  - Reads and tampers with the activity of **every** neuron in brain
  - *While you are thinking about your secret*.

- Computing-analog of this scenario is common:
  - Can a computer program keep a secret, even if adversary captures the entire program?
  - **No trusted hardware, no interaction.**
  - Just an ordinary program with ordinary inputs and outputs.
  - Running on a *single* ordinary computer.

Earlier concepts

Secure Multi-Party Computation (80s-)
& Homomorphic Encryption (2009-)

Previous concepts required some portion of computation to be ***completely hidden*** from Adversary.

Obfuscated Software:
No part of computation is hidden.