CSE 484 / CSE M 584 (Autumn 2011)

Last class

Daniel Halperin
Tadayoshi Kohno

Thanks to Dan Boneh, Dieter Gollmann, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...

Class updates

- Extra office hours
  - Today @4:30ish (I have a talk to see @3:30)
  - Generally, by appointment
- In class final
  - Here next Tuesday @2:30
- Optional Lab 3
  - Next Wednesday evening @midnight [11:59:59pm]

Today

- **Review?**
  - No one sent me any questions related to material covered in class so far
- **The future of security**
  - What is the (academic) research community doing today to think about tomorrow?

Current Research I

- **New frontiers for security**
  - Really, new[ish] places we have computers
  - Key factor: added functionality, e.g., *networking*, *sensors*, *storage*, *actuation*.
  - **Implantable medical devices**
  - **Automobiles**

Current Research II

- **New cryptographic primitives**
  - E.g., ***fully homomorphic cryptography***
    - You can compute things on encrypted data without revealing the data

Current Research III

- **Practical systems using new cryptography**
  - E.g., **CryptDB**
    - How do I store data in a database without giving the DB admin access to all of it?

Current Research IV

- **Attacks on modern “secure” systems**
  - E.g., **“Hooked on Phonics”**
    - How can I tell what you’re saying if you’re talking over an encrypted Skype connection?

Current research summary

- **Disclaimer:** I've listed only 4 categories; there are many more!
- That said, ***which do you want to hear about today?***
    - Medical devices
    - Fully homomorphic encryption
    - CryptDB
    - "Hooked on Phonics"

Current Research V

- (Yoshi added in class)
- **Measurements about what the bad guys are doing**
  - Spam, selling fake products, etc.
  - Botnets, malware, SearchSpam
  - and more!