COLLEGE OF SOCIAL & BEHAVIORAL SCIENCES
School of Information

Layer 8+ Privacy II

Information Privacy with Applications

David Sidi (dsidi@email.arizona.edu)

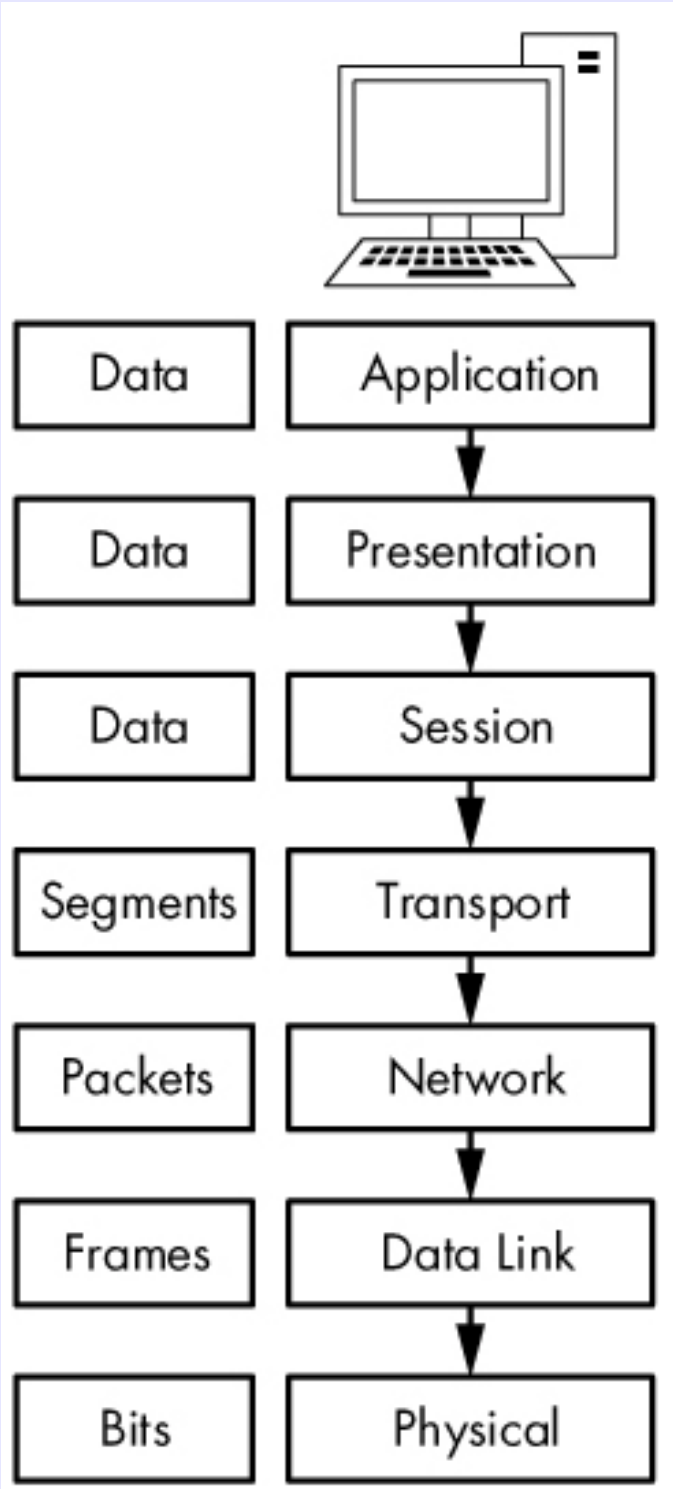
Warm-up

- Summarize some part of what Dan Geer said in Identity as Privacy

Small mention of interesting things

- Assignment 1
- ISO rejects NSA crypto (link)

The Seven-Layer OSI Model classifies protocols by function



Trust with 8+ layers

- Jeanette Wing (video) @ 10:37-12:15, 55:19 - 60:00
- “What is a theory of trust in these networks of humans and computers?”

People can be hacked

- Social Engineering
  - Laura’s presentation
  - The Art of Deception

People can be hacked

- Social Engineering
  - Laura’s presentation
  - The Art of Deception
- Contract law

People can be hacked

- Social Engineering
  - Laura’s presentation
  - The Art of Deception
- Contract law
- Compulsion

- Incentives, costs, benefits, ...

Philip Zimmerman on trust

- “When examining a cryptographic software package, the question always remains, why should you trust this product? Even if you examined the source code yourself, not everyone has the cryptographic experience to judge the security. Even if you are an experienced cryptographer, subtle weaknesses in the algorithms could still elude you.”

“In some ways, cryptography is like pharmaceuticals. Its integrity may be absolutely crucial. Bad penicillin looks the same as good penicillin. You can tell if your spreadsheet software is wrong, but how do you tell if your cryptography package is weak? The ciphertext produced by a weak encryption algorithm looks as good as ciphertext produced by a strong encryption algorithm. There's a lot of snake oil out there. A lot of quack cures.”

“I'm not as certain about the security of PGP as I once was about my brilliant encryption software from college. If I were, that would be a bad sign. But I'm pretty sure that PGP does not contain any glaring weaknesses (although it may contain bugs). The crypto algorithms were developed by people at high levels of civilian cryptographic academia, and have been individually subject to extensive peer review. Source code is available to facilitate peer review of PGP and to help dispel the fears of some users. It's reasonably well researched, and has been years in the making. And I don't work for the NSA. I hope it doesn't require too large a "leap of faith" to trust the security of PGP.”

- Credentials (“high levels of cryptographic academia”)
- Peer review
- Open source code
- Test of time (“It's reasonably well researched, and has been years in the making”)
- No conflict of interest (“I don’t work for the NSA”)

Credentials

- Phil Zimmerman’s own email service, Hushmail turned over plaintext email in response to government warrant in a steroid drug dealing case
  - https://www.wired.com/images_blogs/threatlevel/files/hush_klp.pdf
- Ladar Levinson and Lavabit

Peer review

- Even if a protocol itself is reviewed, there is a gap between theory and implementation (often by different parties)
- Implementations are usually not audited, even if open source

Open Source

- Example: Signal protocol
  - Signal is GPL’d, but many products get to say they “use Signal protocol” while remaining closed source
  - WhatsApp, Allo, Facebook Messenger

Test of Time

- Attacks may be classified
- “After World War II, the US sold German Enigma ciphering machines to third world governments. But they didn't tell them that the Allies cracked the Enigma code during the war, a fact that remained classified for many years.”
- See: Snowden disclosures
- Good candidate for “test of time”: Tor?

Test of Time

- Attacks may be classified
- “After World War II, the US sold German Enigma ciphering machines to third world governments. But they didn't tell them that the Allies cracked the Enigma code during the war, a fact that remained classified for many years.”
- See: Snowden disclosures
- Good candidate for “test of time”: Tor?
  - Also: https://netzpolitik.org/2017/secret-documents-reveal-german-foreign-spy-agency-bnd-attacks-the-anonymity-network-tor-and-advises-not-to-use-it/

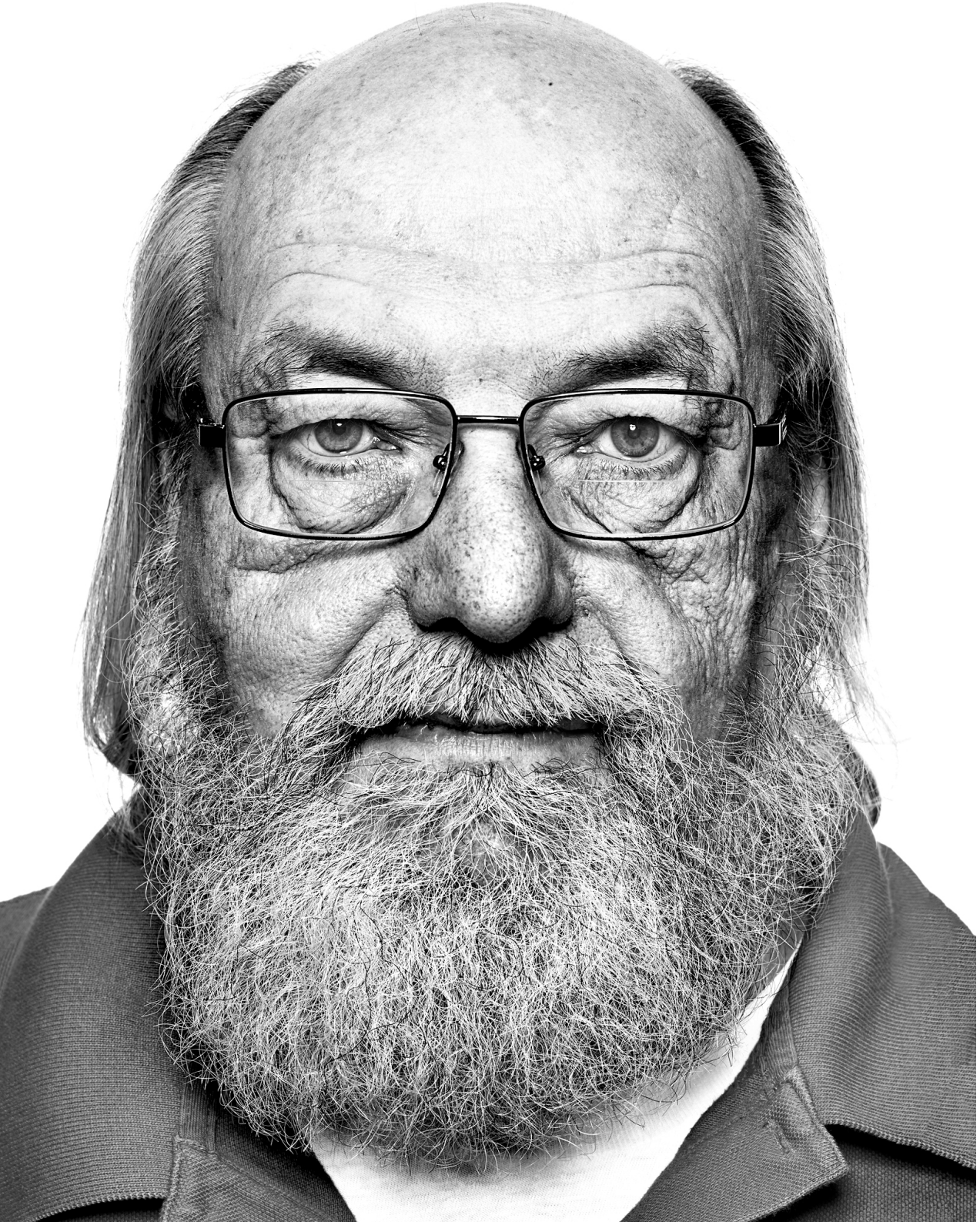
Sidenote: About Enigma

- Even today many Unix systems worldwide use the Enigma cipher for file encryption, in part because the Government has created legal obstacles against using better algorithms. They even tried to prevent the initial publication of the RSA algorithm in 1977. And they have squashed essentially all commercial efforts to develop effective secure telephones for the general public.
- man -S1 crypt (for example)

No conflict of interest

- Based on personal assurances
- There are many interests involved in research, with a lot of money to spend
  - sponsors of Usenix SOUPS: Facebook, Google
  - sponsors of the Future of Privacy Institute Workshop: Acxiom, Palantir, Facebook, Google, Euclid, ... (link)

Trust: Counsel of Despair?



The moral is obvious. You can't trust code that you did not totally create yourself. (Especially code from companies that employ people like me). No amount of source-level verification or scrutiny will protect you from using untrusted code.

Ken Thompson, ACM Turing Award Speech, “Reflections on Trusting Trust”

Is Ken Thompson right? (2 min)

Example Technologies at layer 8

- PGP web of trust
- Ceremonies for verifying keys in instant messengers
- biometrics countermeasures
- shoulder surfing countermeasures
- reputation systems

What can happen if you don’t use the PGP web of trust?

- https://stallman.org/gpg.html
- (Ian Goldberg’s shadow attack)