OTR paper thoughts...

Why assign a paper full of terminology we haven’t covered?

- Creates a “need-to-know”

Terminology basics we'll be covering...

- Secure hash function
- Symmetric crypto (block or stream)
- MAC and HMAC

ABSTRACT

Quite often on the Internet, cryptography is used to protect private, personal communications. However, most commonly, systems such as PGP are used, which use long-lived encryption keys (subject to compromise) for confidentiality, and digital signatures (which provide strong, and in some jurisdictions, legal, proof of authorship) for authenticity.

In this paper, we argue that most social communications online should have just the opposite of the above two properties; namely, they should have *perfect forward secrecy* and *repudiability*. We present a protocol for secure online communication, called "off-the-record messaging", which has properties better-suited for casual conversation than do systems like PGP or S/MIME. We also present an implementation of off-the-record messaging as a plugin to the Linux GAIM instant messaging client. Finally, we discuss how to achieve similar privacy for high-latency communications such as email.

terminology

Why is email harder?

More terms in the paper...

- Malleable encryption
- Repudiability
- Perfect forward secrecy
- Others?

Historical context

- Paper is from 2004
  - “...Internet has grown over the last decade…”
- Today Signal and chat programs using Signal’s protocol (like WhatsApp and Viber) are more common
  - If you’re really nerdy, you can run OTR 3 on XMPP

Why stream (or OTP) *vs.* block?

- OTP == one-time-pad
- Speed
- Malleability – can be good or bad