Some notes for InfoSec30006

Vanessa Teague, Aug 2017

Review of basic ways to agree on a shared secret

- El Gamal
  - Usually used with a new key each time
  - Susceptible to man-in-the-middle attacks
- RSA
  - If the public key is compromised, so are all past communications
- Both options are possible in SSL/TLS

What’s that first verification code?

- When you add a new contact
- Actually it’s complicated to understand exactly what it is, but you’re
  - Learning the other person’s public key g^a
  - Establishing a shared secret for later use

Desirable properties for secret messages

- Resistance to man-in-the middle attacks
  - Even from an attacker who can read, write and delete messages
- “Forward Secrecy”
  - Even if the attacker compromises your key now, your past communications stay secure
- “Future Secrecy”
  - When you’re using a new key each time (“ephemeral” keys)
  - Even if the attacker compromises your key now, your future communications stay secure

“Ratcheting” protocol

- Combines the ephemeral Diffie-Hellman exchange with longer-term memory of the public key exchanged when the contact was first met
- Details at https://whispersystems.org/blog/advanced-ratcheting/

In summary

- Verify identity/public key
- Establish a shared secret
- Use that secret each time to generate a new (“ephemeral”) encryption key
- It’s
  - Forward secure, and
  - Future secure