Security Talk
Pretty Good Privacy (PGP/GNUpg)

Brian Epstein <bepstein@ias.edu>

Security Talk: PGP/GNUpg

- AIC triad – PGP/GNUpg
- History of PGP/GNUpg/OpenPGP
- Shared Key Cryptography
- Public Key Cryptography
- Cryptographic Hashing
- Web of Trust

Security Talk: PGP/GNUpg

- Main Principles in Security
  - Availability
  - Integrity
  - Confidentiality

- PGP/GNUpg covers Integrity and Confidentiality

History of Pretty Good Privacy

- Pretty Good Privacy (PGP) created in 1991 by Phil Zimmermann
- OpenPGP rfc2440 created in 1998
- GNU Privacy Guard (GNUpg or GPG) created in 1999
- Commercial PGP changed hands twice in the past decade

Shared Key Cryptography

- Also known as symmetric key, single-key or private key cryptography
- Analogous to a regular door key
  - Cereal box decoder ring
  - ZIP file encryption
  - Excel Spreadsheet encryption

Shared Key Cryptography

- Strengths
  - Easy to use
  - Quick to understand
  - Keeps data confidentiality
- Weaknesses
  - Vulnerable key exchange
  - Number of keys required is n(n – 1)/2
  - No integrity checking available (we don't know who encrypted)

Public Key Cryptography

- Also known as asymmetric key or split key cryptography
- Each person has two keys
  - Public key to share with the world
  - Private key to keep very secret.

Public Key Cryptography

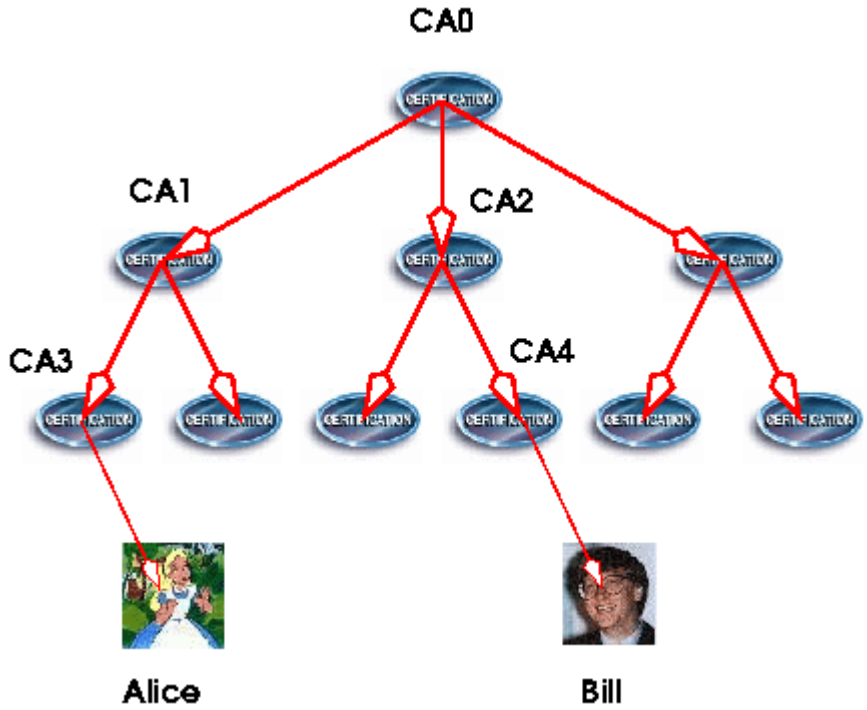
- Public key
  - Data encrypted by this key can only be opened by its Private Key
  - Encrypting with public key ensures confidentiality
  - Alice encrypts with Bob's public key so that only Bob can read
- Private key
  - Data encrypted by this key can only be opened by its Public Key
  - Encrypting with private key ensures integrity
  - Alice encrypts with her private key to prove to Bob that she authored the email

Public Key Cryptography

- Strengths
  - Number of keys required is n*2
  - Keeps data integrity
  - Keeps data confidentiality
- Weaknesses
  - Vulnerable key exchange
  - Key trust (PKI or Web of Trust)
  - More difficult to manage

PKI versus Web of Trust

- Public Key Infrastructure (PKI) has a trust tree



PKI versus Web of Trust

- PKI Strengths
  - Single point of trust
- PKI Weaknesses
  - Must have a shared point of trust
  - Verisign, Thawte, RSA certificates
  - Must spend money

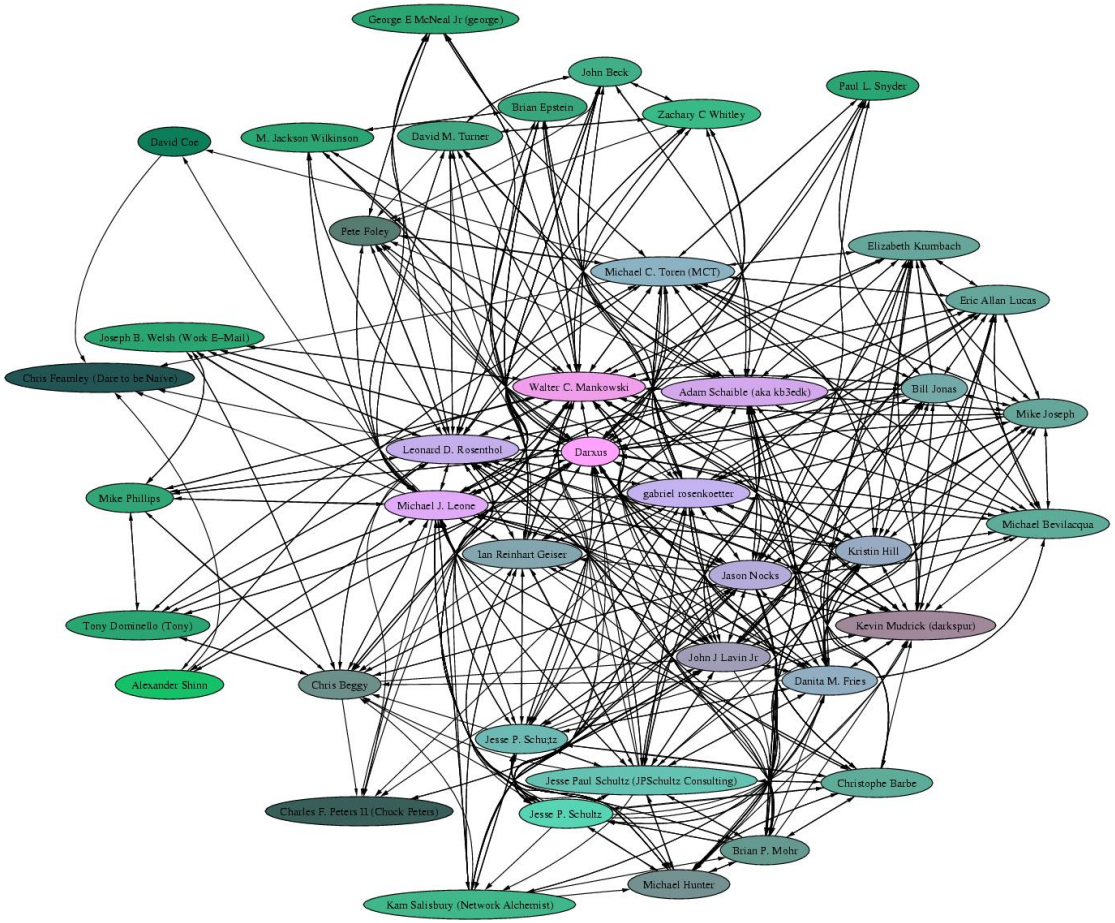
PKI versus Web of Trust

- Web of Trust Strengths
  - No single point of trust
  - Mesh network of trust
  - Usually free
- Web of Trust Weaknesses
  - Requires more work to setup consistently
  - How much do you trust your web?

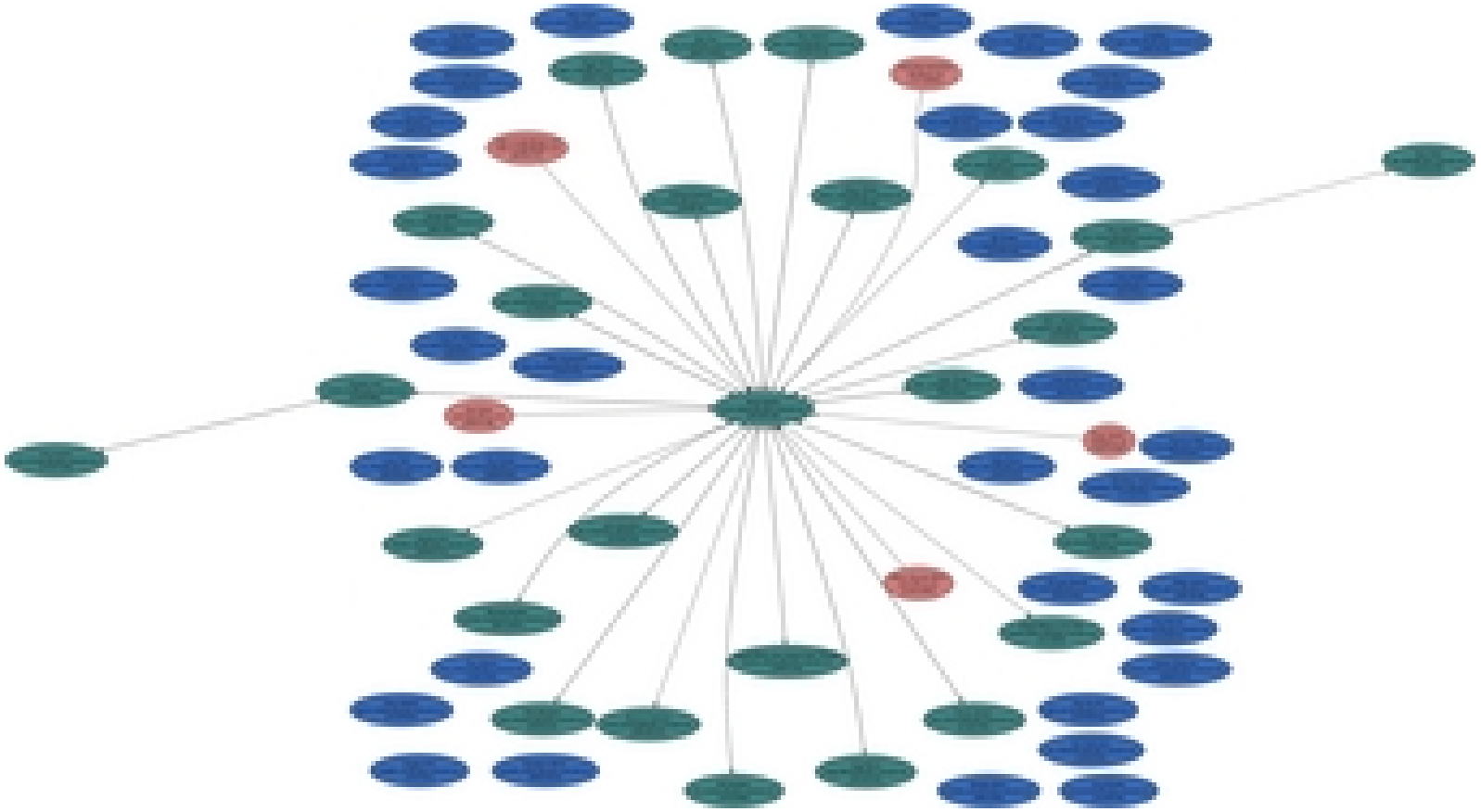
Web of Trust

- Should not be spoke and wheel
- Should look like a web

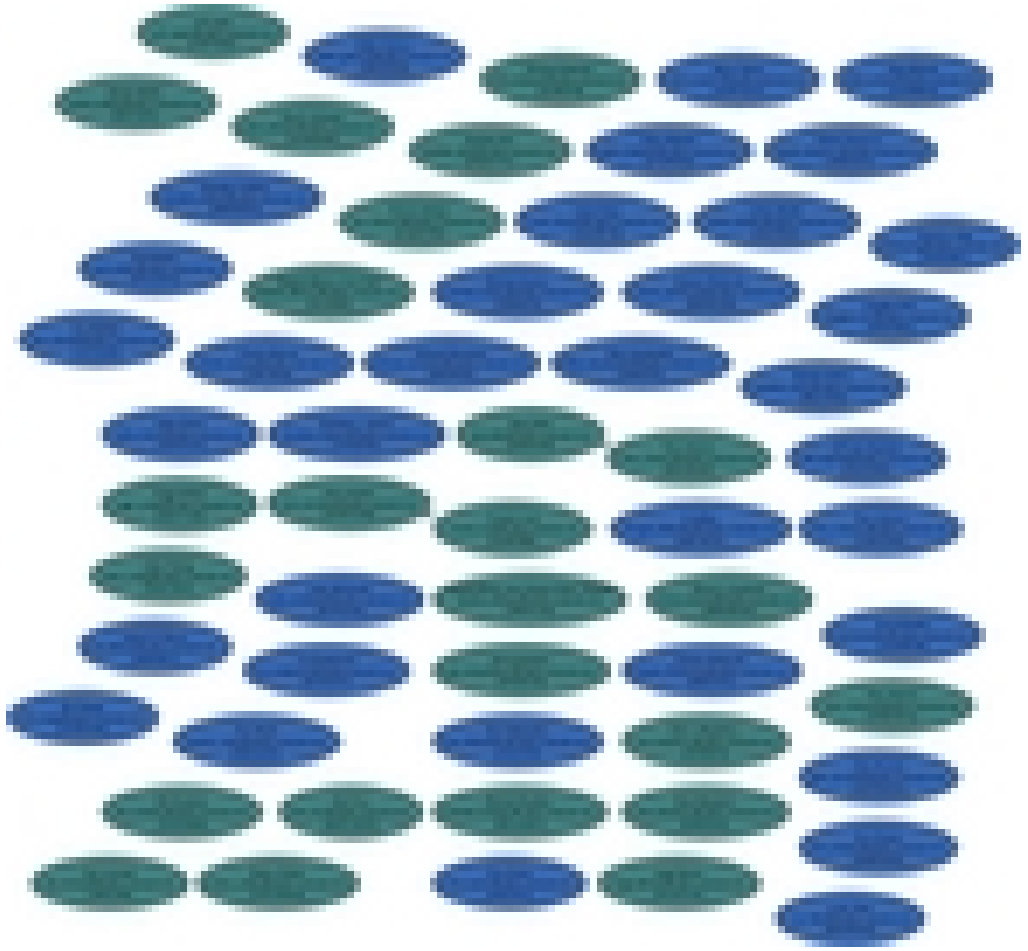
- Good Web of Trust



- Spoke and Wheel



- Broken Spoke and Wheel



IAS Web of Trust

Demo

Questions?

Thanks, time to party!

Security Talk
Pretty Good Privacy (PGP/GNUpg)

Brian Epstein <bepstein@ias.edu>

- AIC triad – PGP/GNUpg
- History of PGP/GNUpg/OpenPGP
- Shared Key Cryptography
- Public Key Cryptography
- Cryptographic Hashing
- Web of Trust

- Main Principles in Security
  - Availability
  - Integrity
  - Confidentiality

- PGP/GNUpg covers Integrity and Confidentiality

History of Pretty Good Privacy

- Pretty Good Privacy (PGP) created in 1991 by Phil Zimmermann
- OpenPGP rfc2440 created in 1998
- GNU Privacy Guard (GNUpg or GPG) created in 1999
- Commercial PGP changed hands twice in the past decade

Phil Zimmermann was the target of a criminal investigation for US export restrictions. Case was dropped in 1996, and PGP, Inc. was founded.

Network Associates Inc (NAI) acquired PGP Inc. in 1997.

PGP Corp acquired PGP from NAI in 2002.

GNUpg was first released in 1999. It follows the OpenPGP standard, RFC2440, released in 1998.

Shared Key Cryptography

- Also known as symmetric key, single-key or private key cryptography
- Analogous to a regular door key
  - Cereal box decoder ring
  - ZIP file encryption
  - Excel Spreadsheet encryption

Shared Key Cryptography

- Strengths
  - Easy to use
  - Quick to understand
  - Keeps data confidentiality
- Weaknesses
  - Vulnerable key exchange
  - Number of keys required is n(n – 1)/2
  - No integrity checking available (we don't know who encrypted)

Public Key Cryptography

- Also known as asymmetric key or split key cryptography
- Each person has two keys
  - Public key to share with the world
  - Private key to keep very secret.

Public Key Cryptography

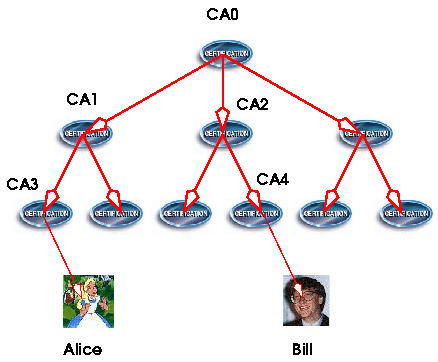
- Public key
  - Data encrypted by this key can only be opened by its Private Key
  - Encrypting with public key ensures confidentiality
  - Alice encrypts with Bob's public key so that only Bob can read
- Private key
  - Data encrypted by this key can only be opened by its Public Key
  - Encrypting with private key ensures integrity
  - Alice encrypts with her private key to prove to Bob that she authored the email

Public Key Cryptography

- Strengths
  - Number of keys required is n*2
  - Keeps data integrity
  - Keeps data confidentiality
- Weaknesses
  - Vulnerable key exchange
  - Key trust (PKI or Web of Trust)
  - More difficult to manage

PKI versus Web of Trust

- Public Key Infrastructure (PKI) has a trust tree



PKI versus Web of Trust

- PKI Strengths
  - Single point of trust
- PKI Weaknesses
  - Must have a shared point of trust
  - Verisign, Thawte, RSA certificates
  - Must spend money

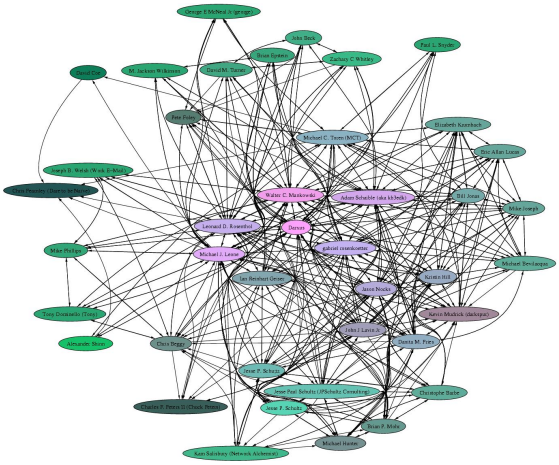
PKI versus Web of Trust

- Web of Trust Strengths
  - No single point of trust
  - Mesh network of trust
  - Usually free
- Web of Trust Weaknesses
  - Requires more work to setup consistently
  - How much do you trust your web?

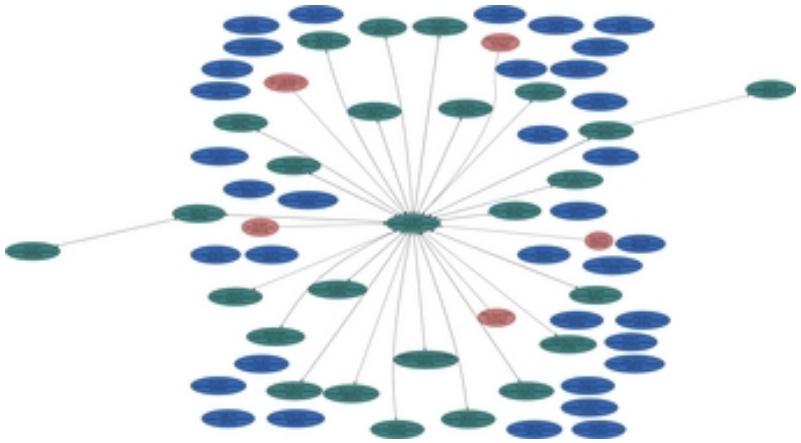
Web of Trust

- Should not be spoke and wheel
- Should look like a web

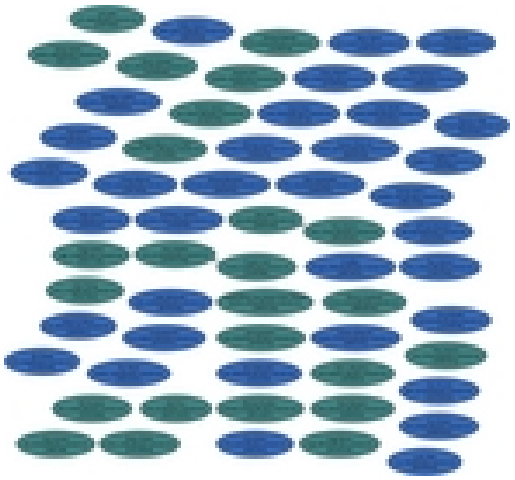
- Good Web of Trust



- Spoke and Wheel



- Broken Spoke and Wheel



IAS Web of Trust

Demo

Questions?

Thanks, time to party!