Anonymous communications and systems

A short introduction

George Danezis
Computer Security Group
Computer Laboratory

Introducing Hiding

- Two strategies to safeguard assets:
  - protect (guards, walls, safes, hardcore crypto)
  - hide (dig, evade, useful when out gunned)
- Fields in information hiding:
  - **Anonymity, traffic analysis**, steganography, steganalysis, low probability of intercept, watermarking, computer forensics, censorship resistance.
- Anonymity: hiding links between actions and identities of agents.

Roadmap

- Requirements and environments where anonymity is useful.
- Extract assets & threat models.
- Technical issues:
  - Measuring anonymity.
  - Anonymous credentials.
  - Anonymous communications.
- Where to go next.

Privacy

- Protect sensitive information about individuals. (PET: Privacy Enhancing Technologies)
- Examples:
  - Marketing and price discrimination (Odlyzko)
  - Health care & medical privacy (see BMA model)
  - Political & Trade Union activity and membership
- Statutory requirements imposed by DPA'98
  - Only collect what is necessary, time constraints, deleting personal data, ...

Freedom from Compulsion

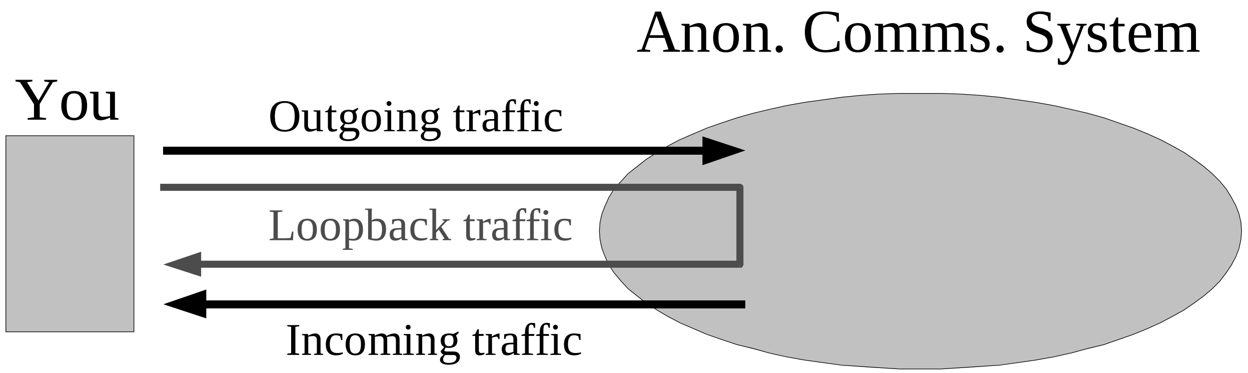
- If identity of actor is not known they cannot be intimidated into doing a particular action.
  - Double edged sword: freedom from accountability.
- Example 1 – Election protocols
  - Additional requirement is *receipt freeness*
- Example 2 – Censorship resistance
  - Protect resources, publishers, distributors, readers by hiding them.

Evading Surveillance

- **Traffic Analysis** can leak a lot of information.
  - Origins: navy with advent of radio comms.
  - Friendship trees in investigations.
  - Accurate target selection reduces cost of further action.
- Anonymity & Covert Channels (Moskowitz, NRL)
  - Combines multi level security with anonymity.
  - Anon. comms. reduces the potential for covert channels.

Selective Denial of Service

- The brutal end of compulsion attacks.
  - Unless very close to the target an adversary cannot easily select what to signal to jam or wire to cut.
  - Choice between DoS (more easy to detect?) or allow the communication through.
- Example 1: How can you tell you are connected to the outside world?



Other uses...

- Identity Theft?
  - Expose less information?
  - Rely less on “identity information” to grant access?
- Spam?
  - But pseudonyms will receive spam.
- Dissent/Liberation in repressive regimes?
  - Not a joke! (Safeweb, Anonymizer)
  - Need more than technology.

Properties & assets

- Link between action and identity.
  - Anonymity, Sender & Receiver anonymity (comms): cannot link an identified actor to an action.
  - Unobservability: Cannot tell if an actor has performed any action of interest.
- Link between different actions as having been performed by the same actor.
  - Unlinkability: linking actions is not possible.
  - Pseudonymity: Allows different actions to be linked to the same actor whose identity is protected.

Philosophical dimensions of identity I

- What is identity (after all this is what the attacker wants!)
- Biometric identity
  - Something reliably linking to a human being.
  - Photographs, fingerprints, DNA, voice, ...
- Administrative & Social identity
  - Widely used identifier linking to a human.
  - Name, address, NI number, NHS number, record, IP address, ...

Philosophical dimensions of identity II

- Network identity (Social network analysis)
  - You are who you know (and very little otherwise)
  - Position in social network, connections, role, capabilities, access to resources.
- Intrinsic identity
  (L'homme n'est que la somme de ses actes – Sartre)
  - Things that are virtual but you cannot change.
  - Writing style, use of language, typing patterns, ...
  - Can allow linking of actions through profiling.

Adversaries

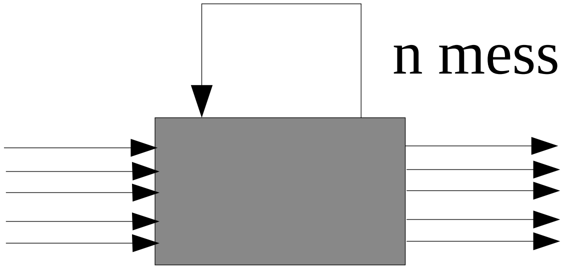
- Traditional:
  - Passive: can see everything on links (global)
  - Active: can change anything it sees.
  - % Corrupt Nodes: completely controls some nodes.
- Compulsion:
  - Can force honest actors to perform some actions.
  - E.g. Collect traffic data, decrypt particular ciphertexts, surrender keys.
  - Note that the coerced nodes can lie if they not not risk being found out.

How anonymous are you?

- Qualitative (Crowds):
  - “absolute privacy”, “beyond suspicion”, “probable innocence”, “possible innocence”, “exposed”, “provably exposed”
- Anonymity sets:
  - Create the set of all people who *could* have been the sought actor.
  - Measure anonymity as the cardinality of the set.

Information theoretic measure

- Problem with sets: the Pool mix (infinite size?)



n messages stay in the pool each round

N inputs

N outputs

Each round choose N messages out of (N+n) and output them

- Solution:
  - Assign probabilities to each actor.
  - Use the entropy of the distribution as a measure.
- “How many yes/no questions the adversary has to ask to uniquely identify an actor?”

Principles of Anonymity Systems

- Bitwise unlinkability:
  - The bit patterns that can be extracted by an adversary and associated with different actions and actors must be independent or unlinkable.
  - Don't be dressed in red when others are in black.
- Dynamic aspect:
  - The actions of enough actors must be confused together. (Noise must exist and be sufficient)
  - Even if you dress in black it won't help if you are alone.

Intro to Anonymous Credentials

- Both ACLs and Capabilities assume authentication as a first stage!
  - Not a very good model for the "cinema ticket", let alone physical cash.
- Using credentials you can prove that you are authorised to do something without revealing any bit string that links you to a previous transaction.
- Can be used for login, elections, cash...
  - On line they require anonymous communications, but have many uses off line (electronic wallets)

The “IB” credential protocol

- Initial (named) key exchange

  A->T: $E_{encT}\{E_{sigA}\{T\}\}$

  T->A: $E_{encA}\{E_{sigT}\{K1\}\}$

  Anonymous key exchange

  A_{-Z}?->*: $E_{encA}\{K2,K3\}$ = TA_{-Z}

  T?->*: $E_{sigT}\{TA,TB,...,TZ\}$ = T

  Accreditation (when all partis have replied)

  A_{-Z}->T: $E_{encT}\{E_{sigA}\{T,K1\}\}$

  T?->*: $E_{sigT}\{E_{KT3}\{E_{sigT}\{KT2\}\}\}$

- Highlights principles, but inefficient

RSA based credentials

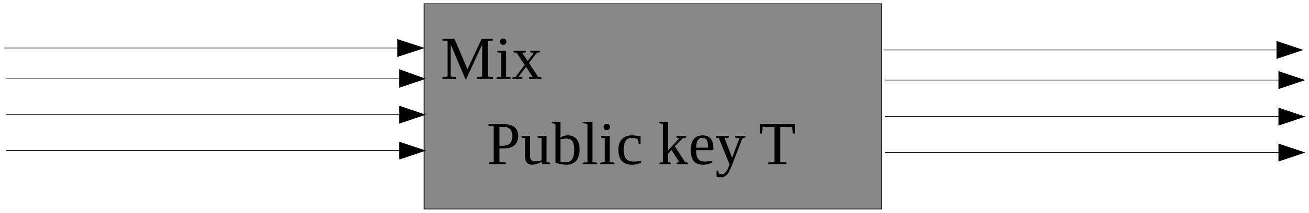
- mechanism called “blind signatures”
- The third party has an accreditation key *d* that can be verified with key *v*.
- Alice wants to accredit the string I and sends:
  `A->T: (B^vI) mod N`
- The third party sends back by raising to *d*
  `T->A: BI^v mod N`
- Alice can divide by the blinding factor B and get:
  `I^v mod N` which is T signature on I.

Notes on credentials

- RSA based protocols does not require any anonymous comms. to issue the credential.
- First protocol makes it explicit that more than one person needs to participate to archive anonymity.
- Beyond the toy examples:
  - credentials with many attributes embedded into them
  - Show any logic formula on these attributes without revealing anything else (Brands).

Anonymous communications

- Introducing the Mix:
  "A message relay that hides the correspondences between its inputs and outputs"



Mix

Public key T

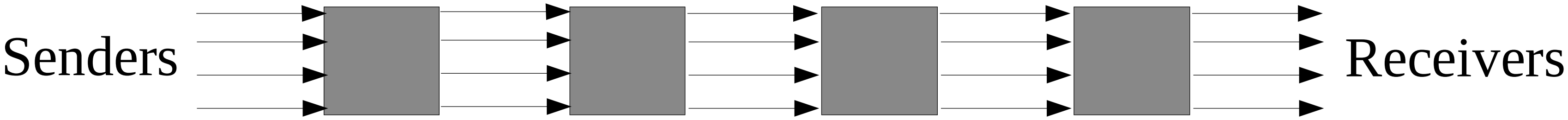
A->T: $E_{enc_T}\{B, Message_i, J_i\}$

T->B: $Message_i$

- Encryption is used to provide bitwise unlinkability
- Batching and padding is used to provide mixing.

Mix Cascades and Networks

- Mixes need to be trusted, so we reply on many.



- Arbitrary topologies can be used, but one has to assess how much uncertainty about the origin or destination they introduce.
- Need to hide the route length, path, the position on the path, need to distribute and chose information about the network securely.
- Complex distributed systems! And they fail.

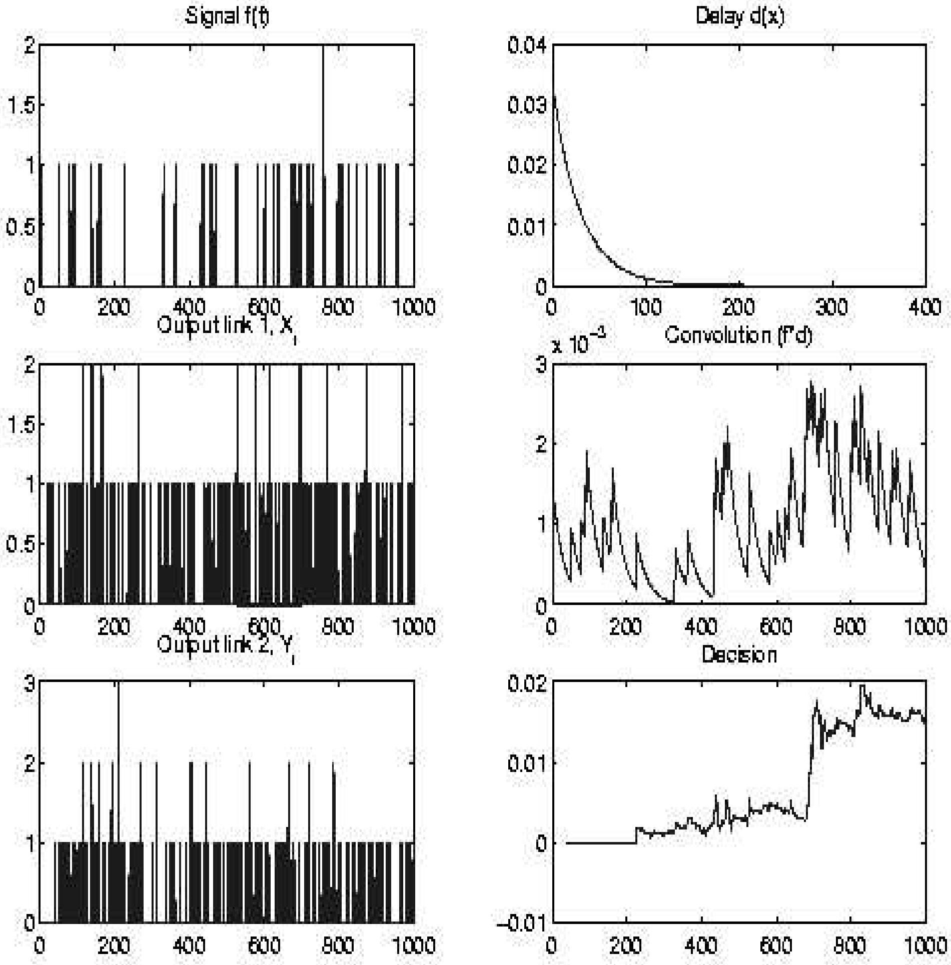
Deployed systems

- Email:
  - *Anon.penet.fi* (legal attack)
  - *Cypherpunk* and *Mixmaster*
  - *Mixminion*: anonymous replies, and secure against active attacks.
- Academic and amateur run systems.

- Web browsing:
  - *Anonymizer*.com (commercial)
  - *Onion Routing* (US Navy)
  - *Freedom* Network (failed commercial)
- Too expensive to run just for fun!

Attacks

- Failures in the bitwise unlinkability are not uncommon (messages leak information)
- Active attacks introduce glitches that ripple through the anonymity systems.
- Traffic analysis is still new to the open academic community.



Anonymity in the Real World

- Bad guys do not need to use anonymity systems to hide their identity. Dirty tricks are sufficient.
  - Share with others a hotmail account and use HTTPs to communicate through using “Draft” messages.
  - Hack other machines or PBXs to mail and phone anonymosly.
  - Steal a mobile phone when you need to make a call!
  - Use pay as you go and internet cafes for short periods of time.
- This is an arms race and techniques are not invented but evolve.

Where to go next?

- If you are interested in anonymity and traceability the resident experts are:
  R. Clayton (rnc1), G. Danezis (gd216), A. Serjantov (aas23)
- Most papers on anonymity can be found at:
  `http://www.freehaven.net/anonbib/`
- **`Mixminion.net`**
- Credentials: “Rethinking Public Key Infrastructures and Digital Certificates” (Brands)