Privacy Enhancing Technologies 2003

An Analysis of GNUnet and the Implications for Anonymous, Censorship-Resistant Networks

Dennis Kügler
Federal Office for Information Security, Germany

Dennis.Kuegler@bsi.bund.de

Anonymous, Censorship-Resistant Networks

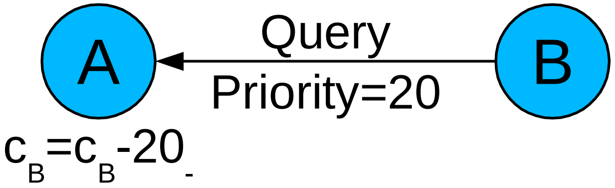
- Anonymous Peer-to-Peer Networks
  - Gnutella
    - Searching is relatively anonymous
    - Downloading is not anonymous
- Censorship-Resistant Networks
  - Eternity Service
    - Distributed storage medium
    - Attack resistant
- Anonymous, Censorship-Resistant Networks
  - Freenet
  - GNUnet

GNUnet: Obfuscated, Distributed Filesystem

- Content Hash Key: $[H(B),H(E_{H(B)}(B))]$
  - Content encryption: $H(B)$
  - Unambiguous filename: $H(E_{H(B)}(B))$
- Content replication
  - Caching while delivering
  - Based on unambiguous filename
- Searchability
  - Keywords

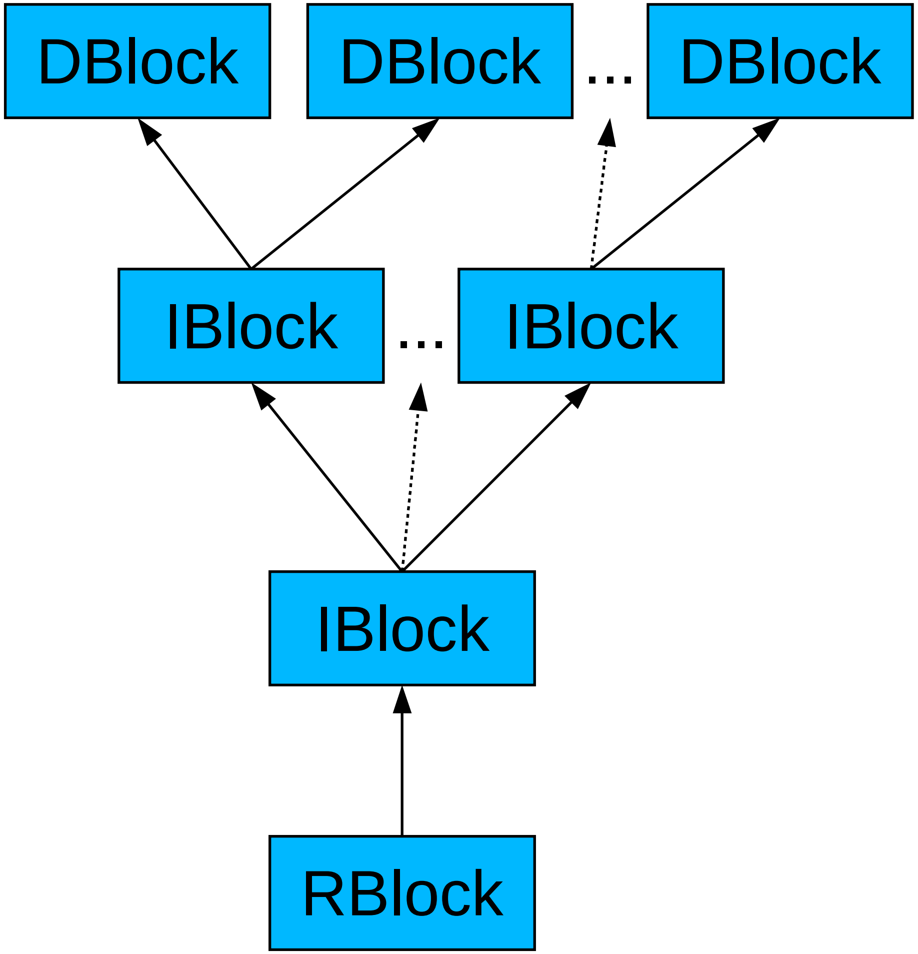
GNUnet: Peer-to-Peer MIX Network

- Initiating node
  - Downloads content
- Supplying nodes
  - Store content unencrypted
- Intermediary nodes
  - Forward and cache encrypted content
  - Plausible deniability due to encryption
- Economic model
  - Based on credit
  - Charge for queries
  - Pay for responses



GNUnet Encoding

- DBlocks
  - 1KB of the content
  - Content hash encrypted
- IBlocks
  - CHKs of 25 DBlocks
  - Organized as tree
  - Content hash encrypted
- RBlock
  - Description of the content
  - CHK of the root IBlock
  - Keyword encrypted



The Attacker Model

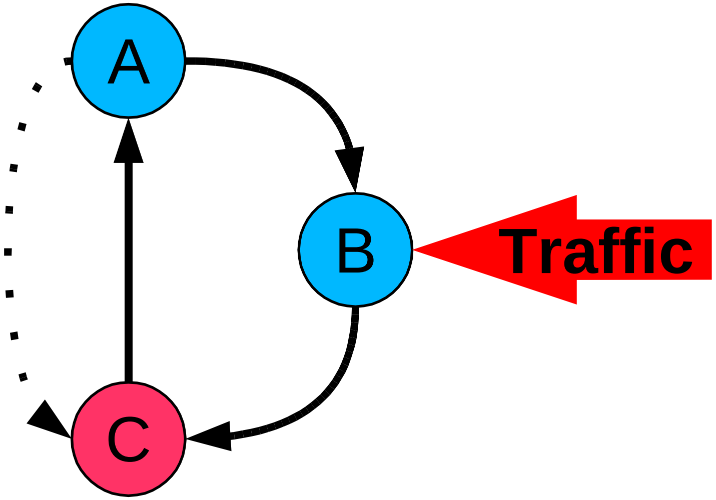
- Attacker
  - Controls malicious nodes that behave correctly
  - Prepares dictionary of interesting keywords
  - Observes queries and responses
    - Queries for known keywords
    - Queries for known IBlocks and DBlocks
    - Responses containing known IBlocks and DBlocks
- Goals
  - Uncover initiating node
  - Uncover supplying node(s): Censorship

Classical Attacks

- Intersection Attack
  - Not all nodes participate in every (MIX) batch
  - Remove nodes not involved in routing linkable traffic
- Predecessor Attack
  - Log identity of preceding node
  - All nodes are logged with equal probability
  - Initiator is logged more often
- **Both attacks are not discussed in GNUnet**

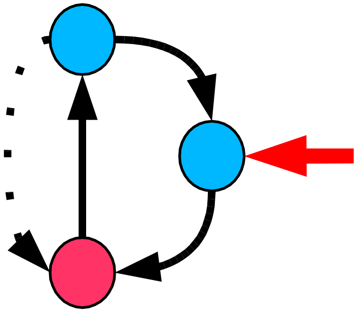
The Shortcut Attack

- Shortcuts do not hurt anonymity?
  - Remove nodes from anonymity set
- Simplification
  - Guess preceding node
  - Verify guess afterwards
  - No flooding required



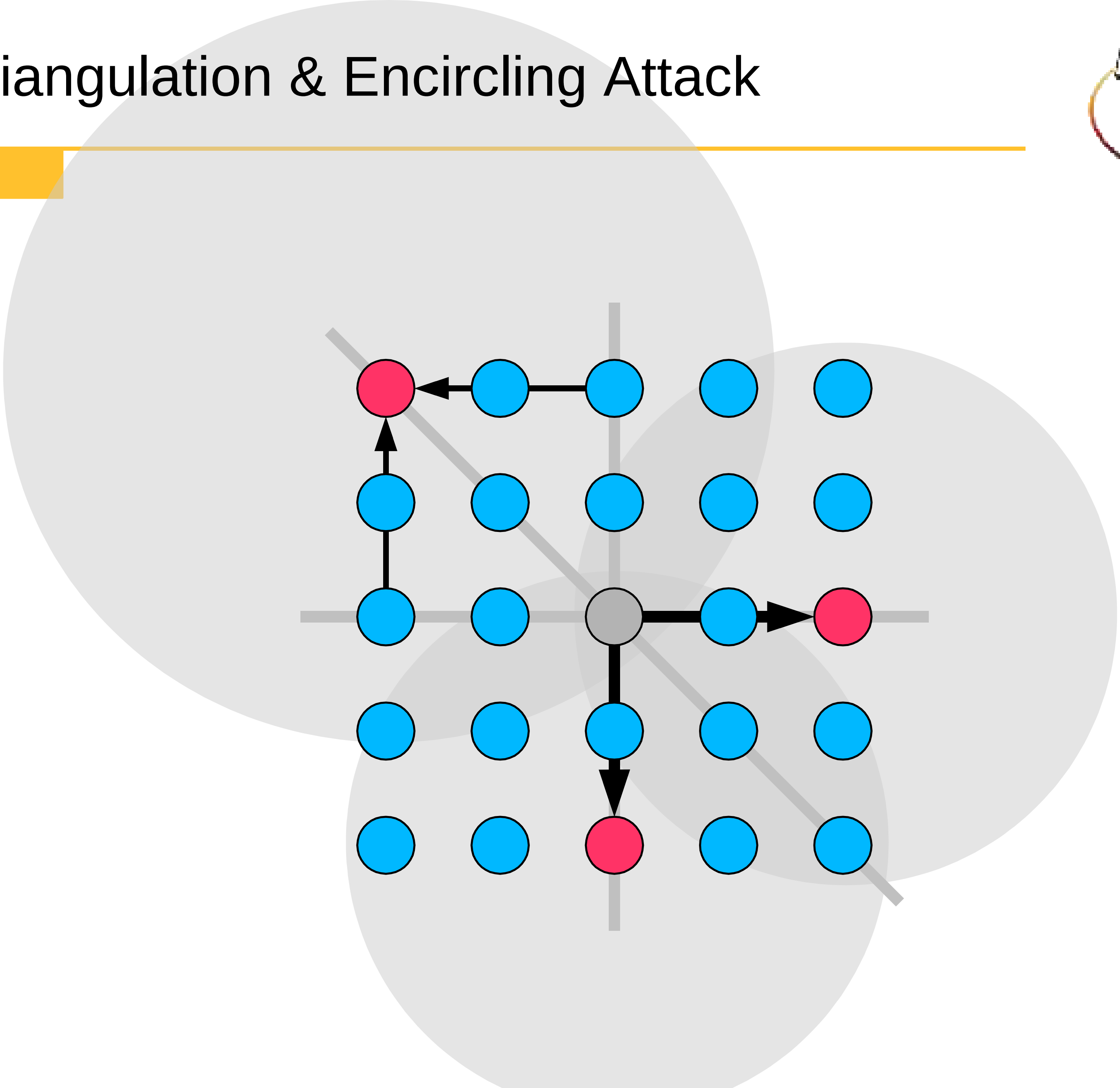
Comments from the GNUnet Team

- ***Only <u>outbound</u> traffic is considered for indirection!***
  - Flooding requires credit
    - Shortcut attack may become even more powerful
    - Improved attack does not require flooding at all
  - Introduces additional intersection attack: DDoS



- ***GNUnet doesn't setup static paths!***
  - Every query is routed individually (with preference)
    - Route queries to nodes that have responded recently
    - Further queries are likely to use the shortcut
  - Attacks are more likely *without* static paths
    - Predecessor Attack
    - Triangulation & Encircling Attack

Triangulation & Encircling Attack



Censoring GNUnet

- Rubber Hose Cryptanalysis
  - Censor infrequently requested content
  - Force nodes to remove content
- Content Filtering
  - Censor frequently requested content
  - Legally enforced by law

Rubber Hose Cryptanalysis

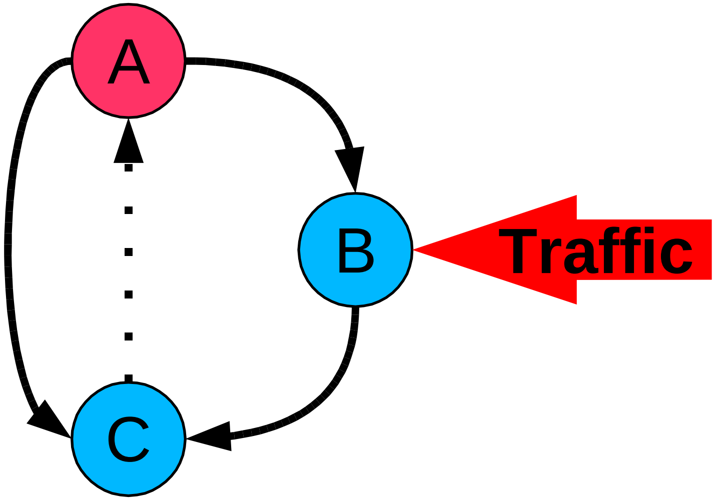
- Distance Attack
  - Determine nodes providing illegal content
  - Use low, increasing TTL to query nodes
- ***GNUnet uses a different notion of TTLs***
  - Relative Time: TTL
  - Absolute Time: TTL + T_{node}

Routing Queries and Responses

- Routing Table
  - Order entries by absolute time
  - Fixed number of entries
    - Discard only overstocked entries
    - Relative TTL may become negative!
- Responses
  - Only after entry has been allocated long enough
  - Probably received response from another node
- Intersection Attack
  - Linkability reduces deniability

Reverse Shortcut Attack

- Reverse Shortcut Attack
  - Remove nodes from anonymity set
- Simplification
  - Guess following node
  - Verify guess afterwards
  - No flooding required



Content Filtering

- Every block is unique identified by $H(E_{H(B)}(B))$
- Censoring with licenses
  - Search for illegal content
  - Issue ***negative licenses*** for indexed content
    - Prohibits delivering the block
  - Issue ***positive license*** upon request otherwise
    - Allows delivering the block
    - Time restricted
    - Need not check content
  - Licenses are cached in GNUnet

Conclusion

- We have presented some attacks on GNUnet
  - Linkability should be prevented at all costs
  - Setup paths as static as possible
  - Shortcut Attacks cannot be fixed easily
    - Economic model cannot replace trust
    - PGP Web of Trust?
  - Unique identifiers enable content filtering
    - Content filtering perhaps won't be realized
    - ...but it shows weaknesses in the concept
- So, is GNUnet a sound approach?