CISC859: Topics in Advanced Networks & Distributed Computing: Network & Distributed System Security

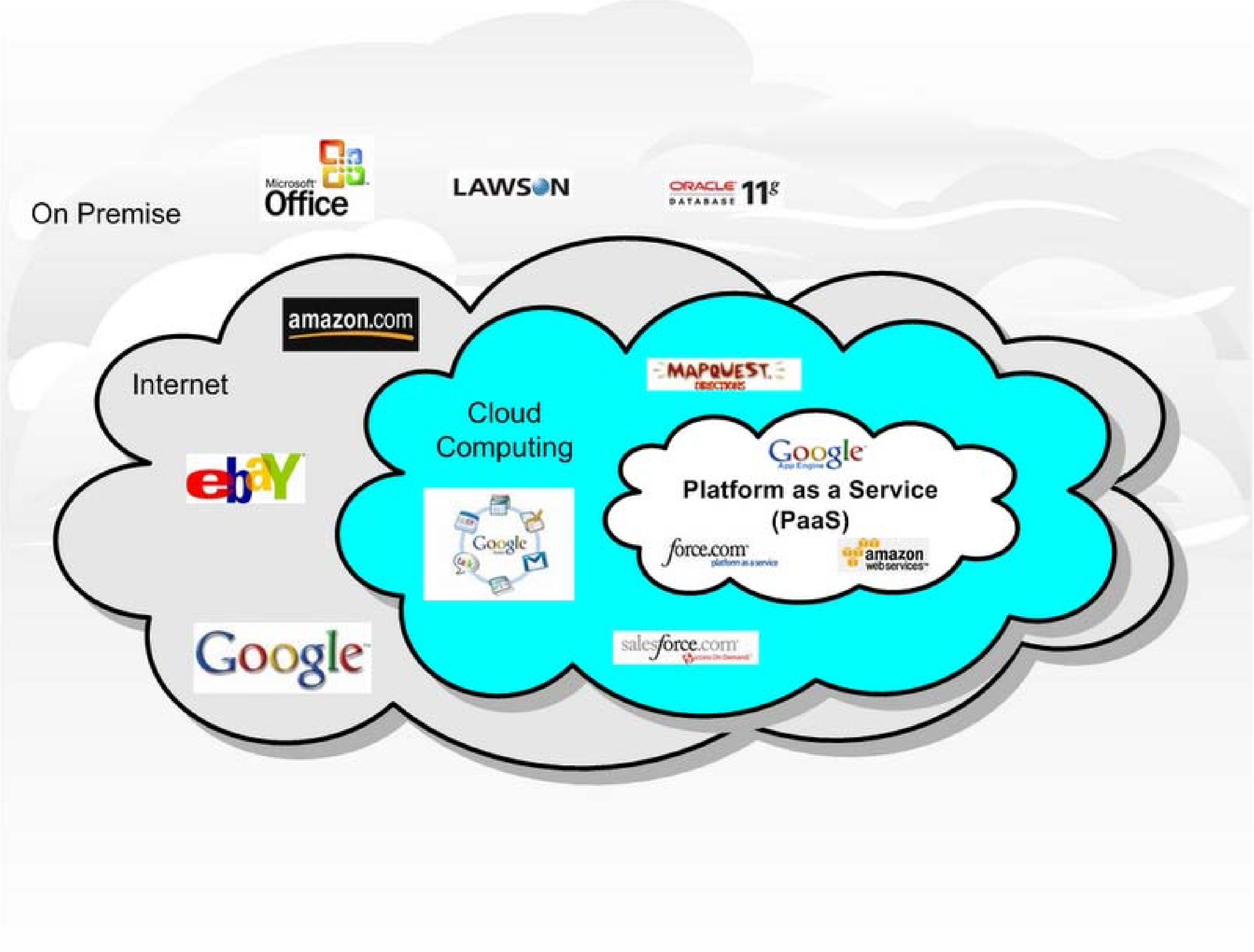
A Brief Overview of Security & Privacy Issues

Topics to Be Covered

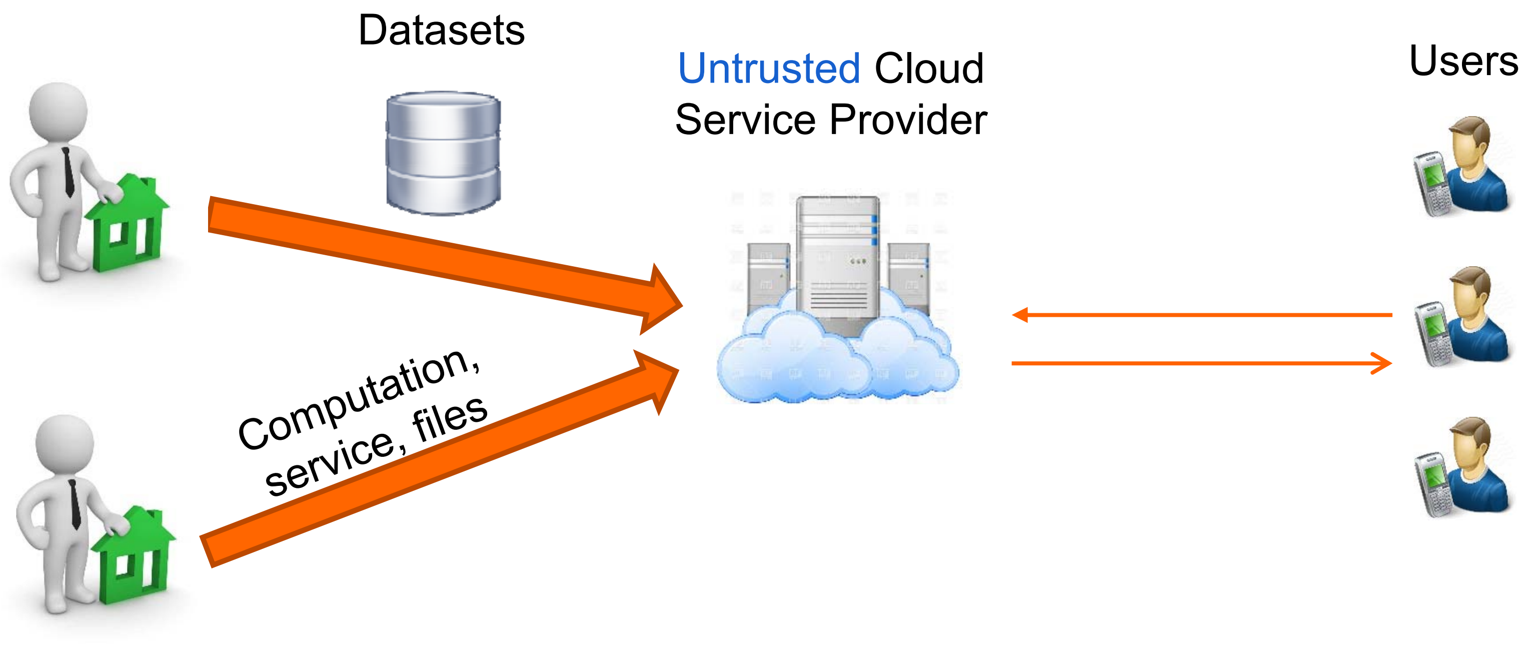
- Cloud computing
- RFID systems
- Bitcoin
- Anonymous comm.
- Social networks
- Sybil attacks

- Location privacy
- Mobile crowdsourcing
- Telecom networks
- Internet of Things
- Cognitive radios
- Anything interesting

Cloud Computing



Typical Scenarios



Security and privacy issues

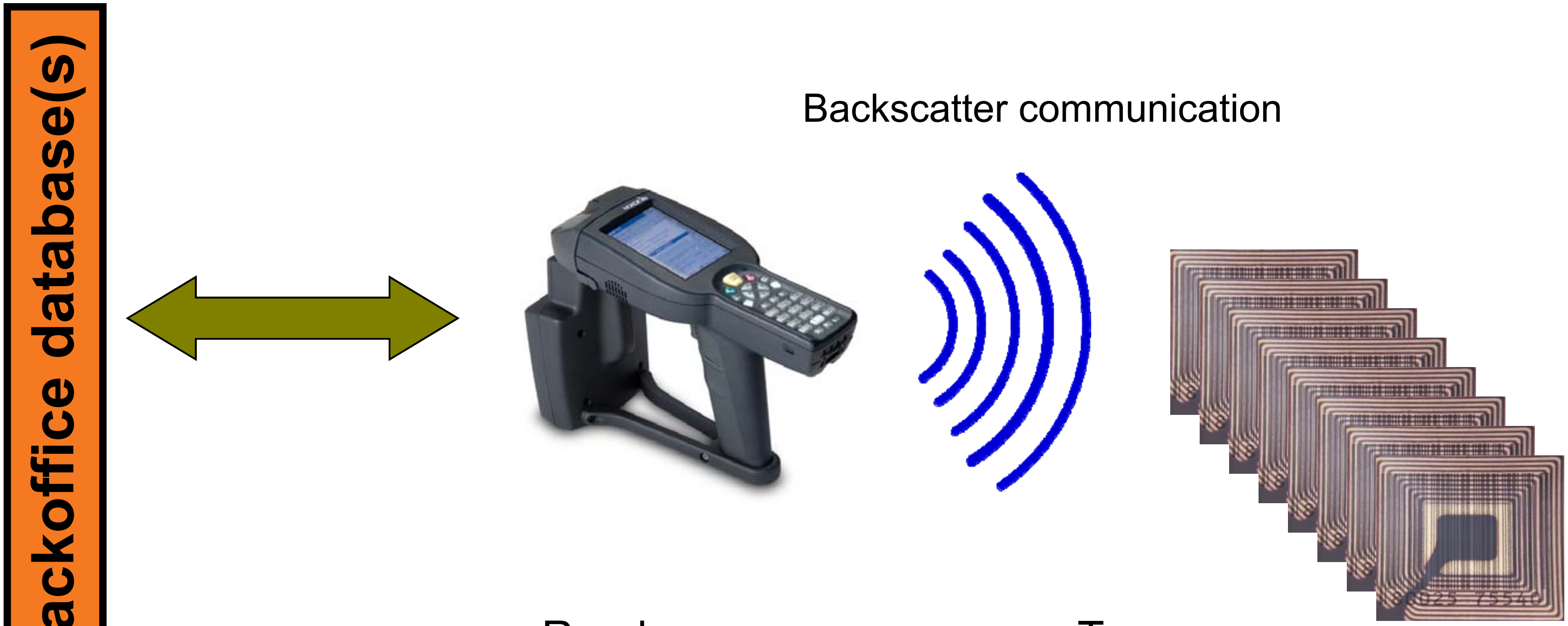
- How to verify the computation/query results returned by CSPs?
- How to process queries over encrypted datasets?
- How to deduplicate files encrypted under different keys?
- How to verify that my uploaded files are retrievable?

RFID System

http://www.youtube.com/watch?v=_xNhL39uD7I

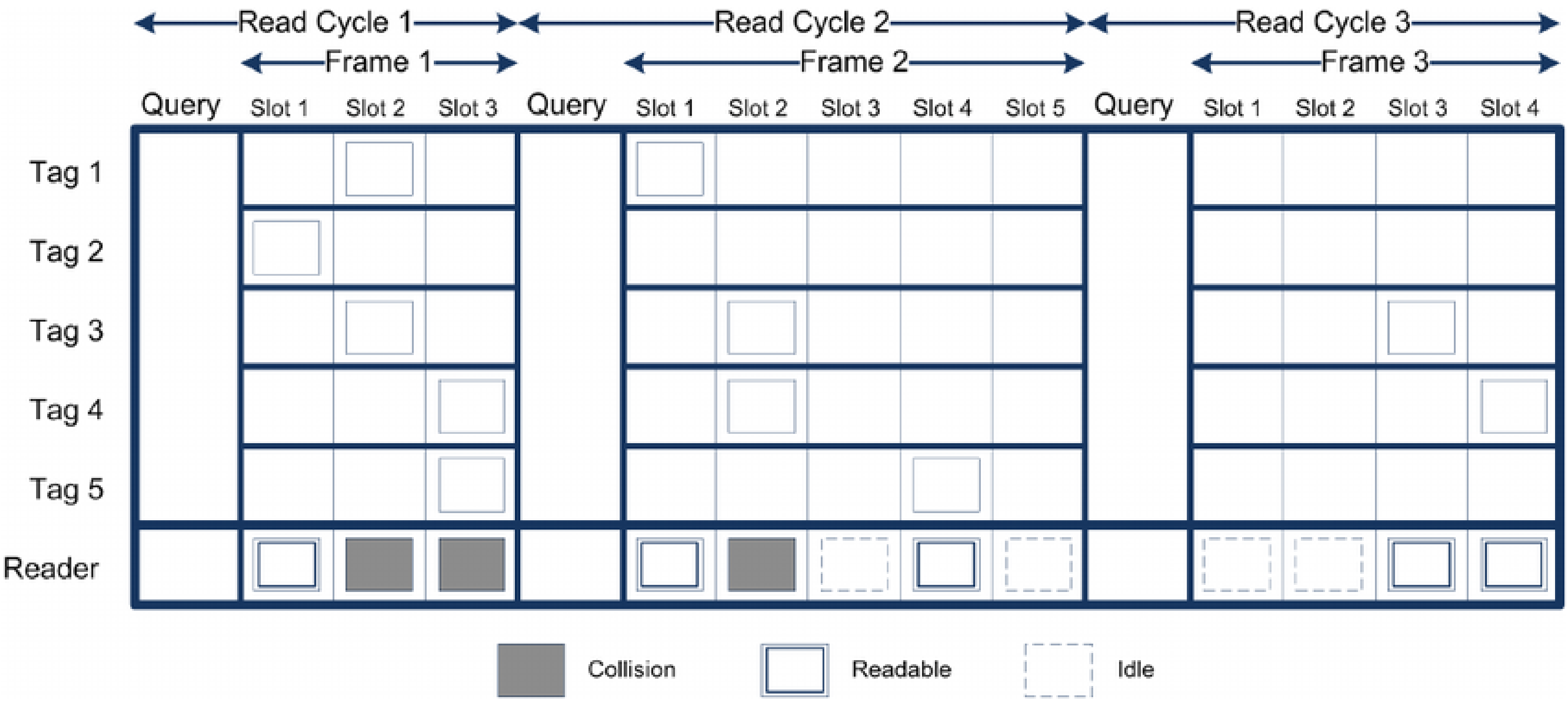
- RFID = Radio Frequency IDentification.
- An ADC (Automated Data Collection) technology that:
  - Uses radio-frequency waves to transfer data between a reader and a movable item to identify, categorize, track..
  - Is fast and does not require physical sight or contact between reader/scanner and the tagged item.
  - Performs the operation using low cost components.
  - Attempts to provide unique identification and backend integration that allows for wide range of applications.
- Other ADC technologies: Bar codes, OCR.

A typical RFID system



- Reader
  - LF / UHF
  - Communication range
  - Coupling
- Tag
  - active / passive
  - 1 bit – 64 kB (EEPROM/SRAM)
  - controller / CPU
  - read-only / read-write

Frame Slotted Aloha Protocol



Current RFID Systems Unsafe

- No authentication
  - No friend/foe distinction
- No access control
  - Rogue reader can link to tag
  - Rogue tag can mess up reader
- No encryption
  - Eavesdropping possible
- Predictable responses
  - Traffic analysis, linkability
- No GUI…
  - … and “distance” not enforced by tag

Security & Privacy Issues

- Privacy-preserving tag identification/authentication/counting
- Missing tag detection/identification
- Batch tag authentication
- Clone/counterfeit detection
- etc.

Bitcoin & Blockchain

- A nice introductory video on bitcoin
  - Youtube, search “How Bitcoin Works Under the Hood”

- A decentralized digital ledger that records transactions such that the registered transactions cannot be altered retroactively

- Important concepts: transactions, blocks, mining, mining pools, etc.

- Cryptographic techniques: cryptographic hash and digital signature

Research issues

- Double spending
- Proof-of-work
- Stability
- Consensus protocol
- Payment verification
- Key management
- etc.

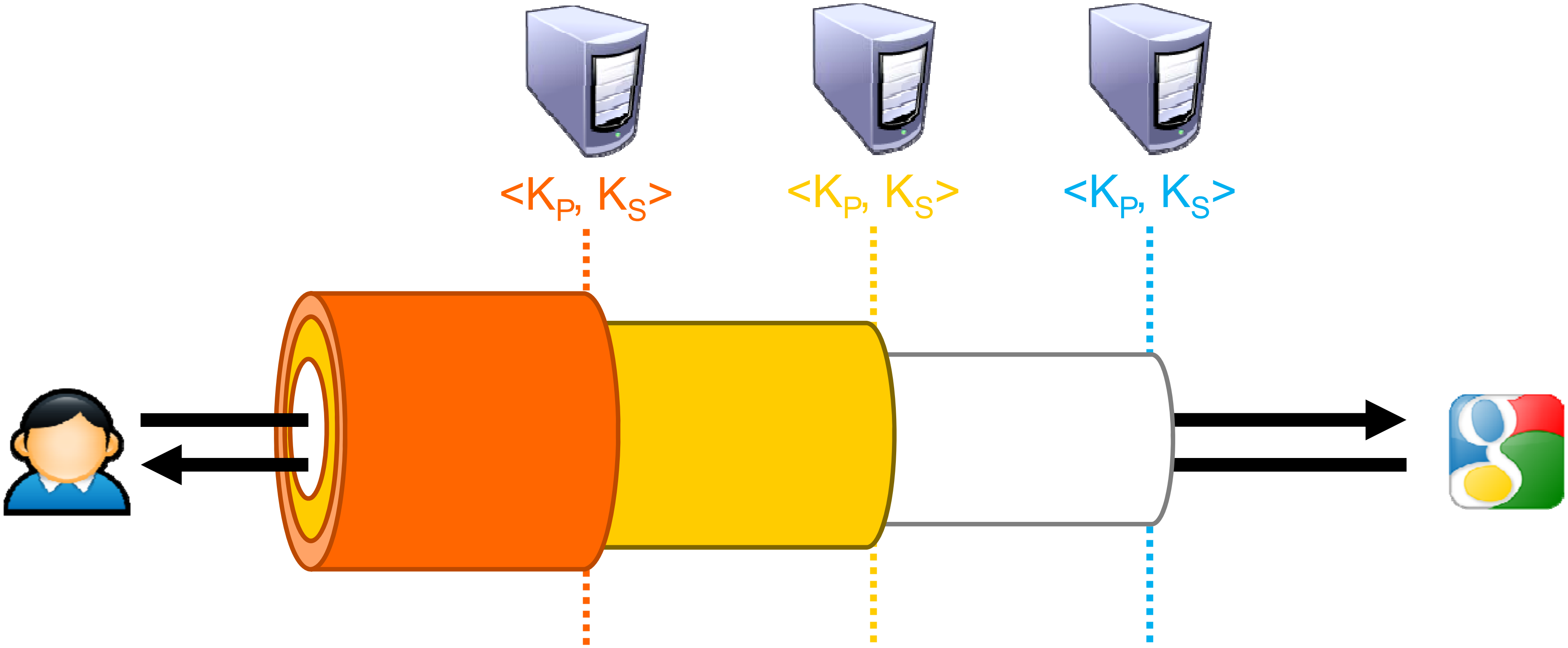
- Additional reading: “SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies” IEEE S&P 2015

Anonymous communication

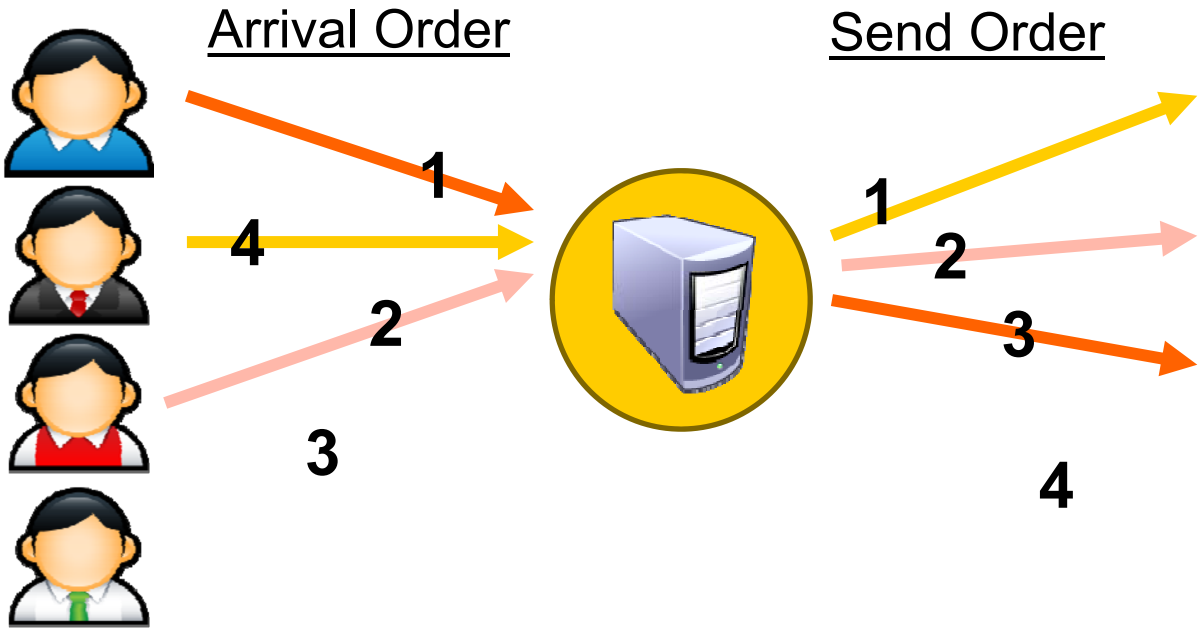
- Hiding the identitie(s) of the parties involved in digital communications from each other, or from third-parties

- Types of Anonymity
  - Sender anonymity
  - Receiver anonymity
  - Sender-Receiver (a.k.a. relationship) anonymity

Mix Proxies and Onion Routing

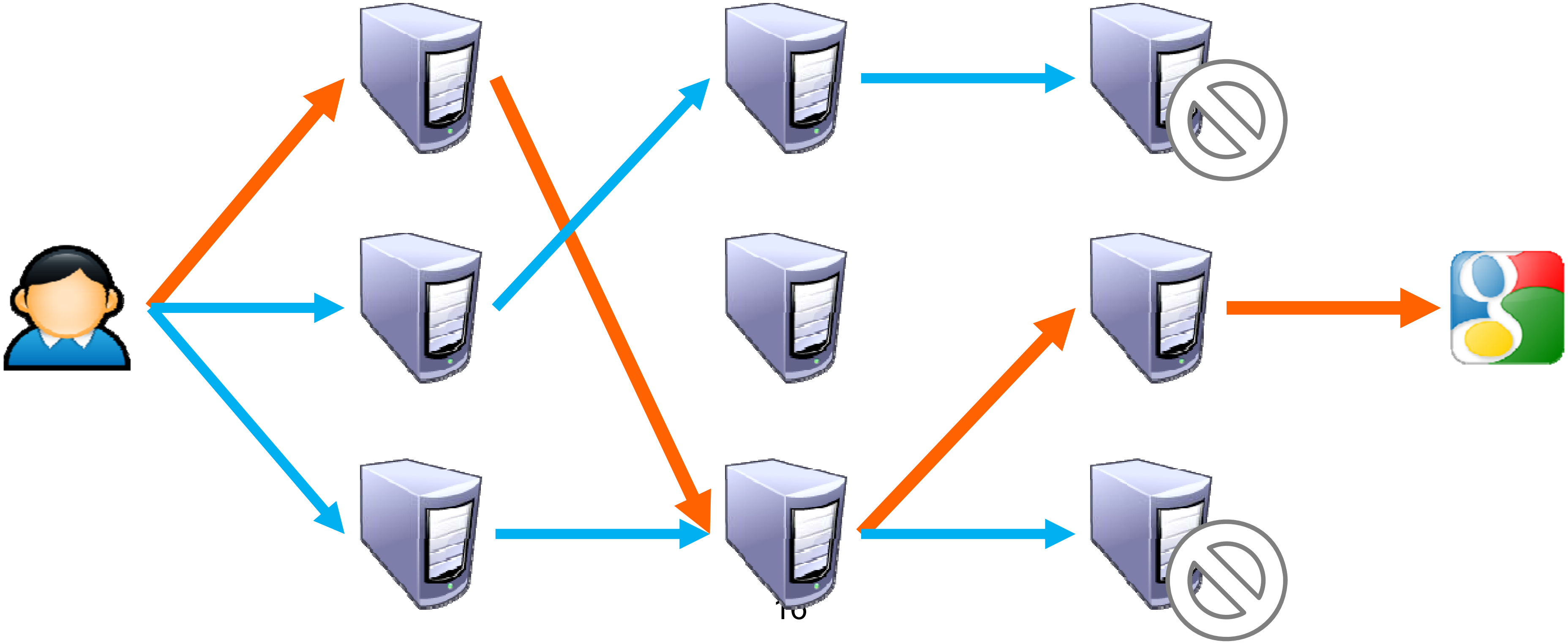


Traffic Mixing



Dummy / Cover Traffic

- Simple idea:
  - Send useless traffic to help obfuscate real traffic



Tor

- Largest, most well deployed anonymity preserving service on the Internet
  - Publicly available since 2002
  - Continues to be developed and improved
- Currently, ~5000 Tor relays around the world
  - All relays are run by volunteers
  - It is suspected that some are controlled by intelligence agencies
- 500K – 900K daily users
  - Numbers are likely larger now, thanks to Snowden
- Additional reading: Tor: The Second-Generation Onion Router, Usenix Security 2004

Research Issues

- Novel anonymous communication systems
- Attacks on existing anonymous communication systems, e.g., Tor
- Improvement for Tor
- etc.

Social Networks

Sybil Attack

- Definition: an individual entity masquerades as multiple simultaneous identities
  - Why named "Sybil" attack
- Severe impact on many distributed applications and everyday services
  - Commonly assume that every participating entity controls exactly one identity
- Examples of the Sybil attack
  - Rig Internet polls by using multiple IP addresses to submit votes
  - Gain advantage in any results of a chain letter
  - A well-known major problem in real-world selections
  - Increase the Google PageRank ratings of customers' pages

Sybil Attack

- Examples of the Sybil attack (cont'd)
  - A common attack on social networking websites, e.g., Facebook, Twitter
  - A common attack on real-world reputation systems like Ebay
  - Obtain multiple accounts on free-email systems by spammers
  - Cause P2P computing systems which use voting to verify correct answers, such as SETI@home, to accept false solutions from a Sybil attacker
  - Reveal the initiator of a connection in a system that provides anonymous communications between peers, like Tor
  - Out-votes honest users in other collaborative tasks such as resource allocation, voting, …

Defenses against Sybil Attack

- Using a trusted central authority
  - Tie identities to actual human beings
- Not always desirable
  - Can be hard to find such authority
  - Sensitive info may scare away users
  - Potential bottleneck and target of attack
- Without a trusted central authority
  - Impossible unless using special assumptions [Douceur'02]
  - Resource challenges not sufficient -- adversary can have much more resources than a typical user

Research Issues

- Detect fake/malicious accounts in social networks

- Explore social networks to thwart Sybil attacks
  - Additional reading: “Using Social Networks to Overcome Sybil Attacks”, Distributed Computing 2011.