Matsuura Lab.

[Attacks and Countermeasures of Privacy Protection Technologies on the Internet]

Department of Informatics and Electronics, IIS

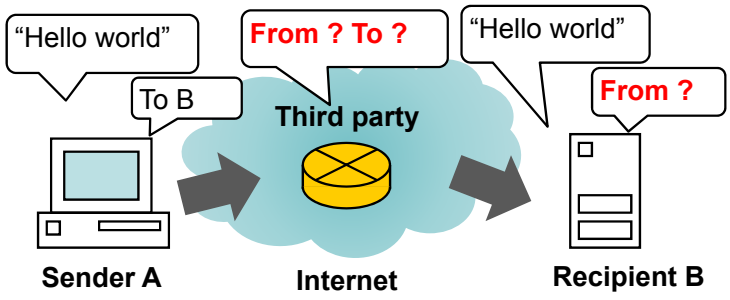
Graduate School of
Information Science and Technology
Department of
Information & Communication Engineering

http://kmlab.iis.u-tokyo.ac.jp/

Information Security

Internet Privacy Protection

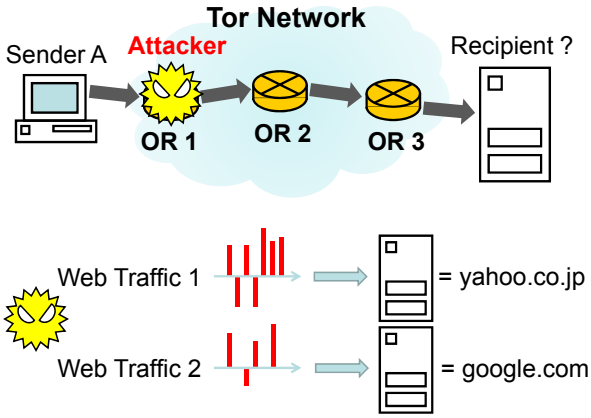
In recent years the Internet is now available for various purposes due to its rapid spread. However, unlike other means of communication such as postal mail and telephone, the privacy protection for Internet is not sufficient. For example, it is possible for someone who is not familiar with IT to easily monitor others' behaviors by generally distributed tools. Encrypted communications can conceal its contents but not the route of communication. As a result, many anonymous communication technologies have been devised in order to conceal the route of communication, and the implementations of these technologies are already prevalent in the world.



✓ Conceptual diagram of anonymous communication system. It conceals the link between communicating parties (who is communicating with whom), instead of the communication contents.

- Applications
  - Privacy protection for web browsing
  - Anonymous voting service, anonymous bulletin board, etc.

Vulnerability Assessment of Anonymous Communication Systems



Even the currently most popular anonymous communication system's anonymity is not perfect.

Several means of attacks to degrade the anonymity have already been found. Among these attacks, fingerprinting attacks that only observe the traffic passing through the entry node of a path, have been attracting attentions, because the amount of required resources is small and it can be a real threat compared to others.

The left figure is a conceptual diagram of fingerprinting attacks. Under the experiment environment of our laboratory, it has been confirmed that the link between communicating parties can be identified with a probability of 70-80% by fingerprinting attacks.