「研究と実務融合による高度情報セキュリティ人材育成プログラム（ISS square）」参加

松浦研究室

情報セキュリティ・暗号研究の成果を展示中。

［Tor 匿名システムへのフィンガープリント攻撃］

Fingerprinting Attack on the Tor Anonymity System

生産技術研究所　情報・エレクトロニクス系部門
Department of Informatics and Electronics, IIS
http://kmlab.iis.u-tokyo.ac.jp
情報理工学系研究科
電子情報学専攻

専門分野：　情報セキュリティ

Webページの閲覧と個人情報保護

Web Browsing and Privacy Preservation

インターネットを介した通信は、他人に容易に覗き見られてしまう。そのため、誰が、何時、どのようなWebページを閲覧したかという個人情報は、閲覧者本人や閲覧されたWebサイトの管理者以外でも収集できる。

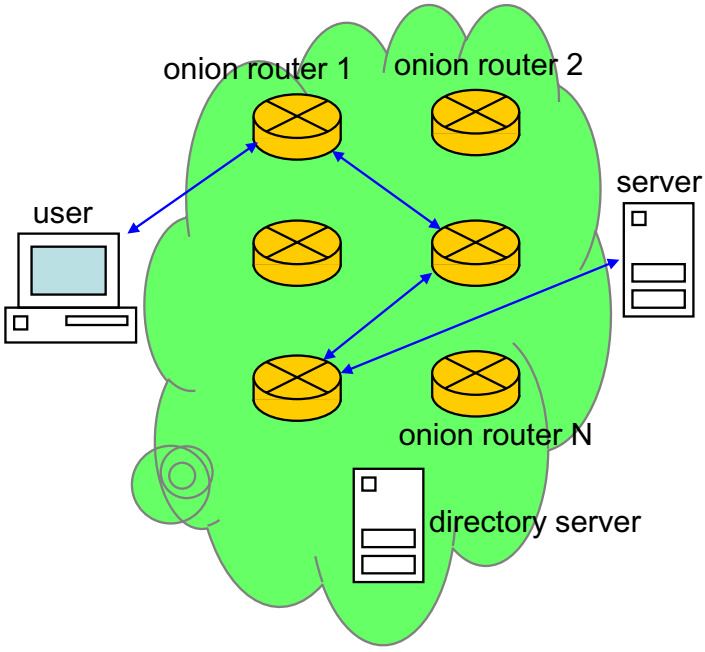
※通信の暗号化だけでは、通信内容を秘匿できても、通信相手は隠せない。

- 保安活動（対テロ活動、など）。
- ✓ 深刻なプライバシー侵害
  - 例：「かつらメーカーのWebサイトを頻繁に閲覧している」との情報、など。

Tor 匿名ネットワーク通信システム

Tor Anonymity System

- Tor：onion routerを使い、インターネット上でのTCP/IP通信に匿名性を持たせる、匿名ネットワークシステム。
- 構成要素
  - user (client)：Torのサービスを使って、serverへアクセスする。
  - server：userの接続先。TCPでのサービスを提供する。
  - onion router：匿名通信を実現するために、途中で経由するルータ。
    □暗号化・カプセル化されたパケット
  - directory server：Tor内のルータ情報を持ち、Torのサービス使用者に提供する。



フィンガープリント攻撃

Finger Printing Attack

- ■ Torへの入り口のrouterとuserの間の通信を傍受。
- ■ 各Webページのファイルの数と大きさ
  →フィンガープリント（区別の指標）
  - パケット数、転送時間、
  - 「interval」：inflowパケットの連続
- ■ 作成しておいたフィンガープリントと比較。

松浦研究室の貢献

- ◆フィンガープリント攻撃を実用的な方法でTor匿名システムへ適用。
- ◆ Tor匿名システムへの現実的な脅威モデルを作成。
- ◆それに基づいた攻撃の成功率の見積り。
- ◆その攻撃への対策の提案。