BÀI 8.
ẨN DANH

Bùi Trọng Tùng,
Viện Công nghệ thông tin và Truyền thông,
Đại học Bách khoa Hà Nội

Nội dung

- Truyền tin ẩn danh
- Bài toán nhà mật mã học ăn tối
- Mạng ẩn danh Tor

1. ẨN DANH LÀ GÌ?

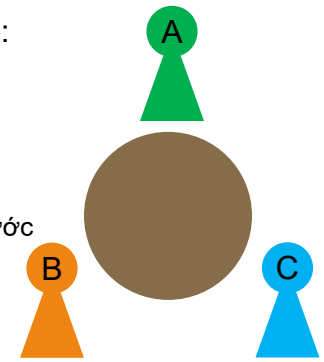
Bùi Trọng Tùng,
Viện Công nghệ thông tin và Truyền thông,
Đại học Bách khoa Hà Nội

Ẩn danh là gì?

- Ẩn danh(Anonymity): che giấu danh tính của chủ thể
- Truyền thông ẩn danh (Anonymous Communication):
  - Ẩn danh người nhận: Không xác định được ai là người đã gửi thông tin trong một tập những người có khả năng
  - Ẩn danh người gửi
  - Ẩn danh người gửi-người nhận: không xác định được cặp giao tiếp trong các cặp có thể
- Mức độ ẩn danh được đánh giá qua lực lượng tập người gửi/người nhận:
  - Tập càng lớn, mức độ ẩn danh càng cao

Bài toán nhà mật mã học ăn tối

- Có 3 nhà mật mã học ăn tối cùng nhau:
  - Một người trong số họ muốn tiết lộ thông tin nhưng không muốn lộ danh tính
  - Giả sử, bản tin là 1 bit, cách thực hiện?
- Trao đổi khóa:
  - Mỗi người trao đổi bí mật 1 khóa có kích thước 1 bit với người bên cạnh
  - Mỗi người sẽ có 2 khóa k_{left} và k_{right}
- Công bố thông tin:
  - Nếu có thông tin m, công bố: $m \oplus k_{left} \oplus kright$
  - Nếu không, công bố: $k_{left} \oplus kright$



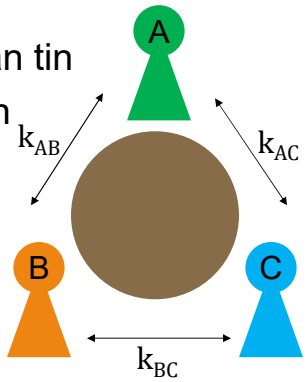
5

5

Bài toán nhà mật mã học ăn tối

- Nhận thông tin: XOR tất cả các bản tin
- Giải thích: Giả sử A tiết lộ thông tin
  - A: $m_A = m \oplus k_{AC} \oplus kAB$
  - B: $m_B = k_{AB} \oplus kBC$
  - C: $m_C = k_{BC} \oplus kAC$
  - Kết quả:

$$m_A \oplus m_B \oplus m_C =$$
$$(m \oplus k_{AC} \oplus kAB) \oplus$$
$$(k_{AB} \oplus kBC) \oplus$$
$$(k_{BC} \oplus kAC) = m$$



6

6

Kết quả thực hiện giao thức

- Tất cả đều biết:
  - Khóa của họ trao đổi với người bên cạnh
  - Nội dung thông tin
- Không ai biết giá trị bit còn lại
- Không ai biết người đã công bố thông tin
- Ví dụ

7

7

Bài toán nhà mật mã học ăn tối

- Chứng minh tính đúng đắn: David Chaum, *The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability*
- Ưu điểm:
  - Giao thức đơn giản
  - Các bên không cần tương tác theo cặp sau khi chia sẻ khóa
  - Rất khó để gian lận: tất cả những người còn lại hiệp sức mới có thể biết ai là người công bố thông tin → số người càng lớn, độ an toàn của giao thức càng cao
- Hạn chế:
  - Tình trạng đụng độ: giao thức không hoạt động nếu có >1 người cùng công bố
  - Bất kỳ ai trong nhóm cũng có thể phá hoại giao thức
  - Khóa không thể dùng lại

8

8

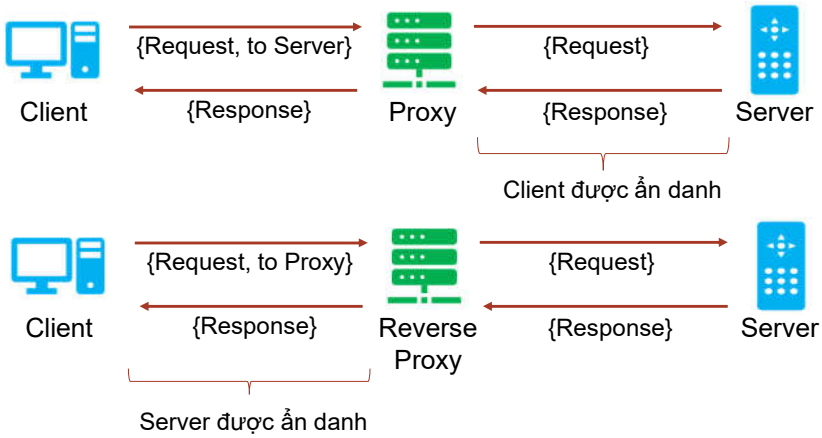
2. MẠNG TOR

Bùi Trọng Tùng,
Viện Công nghệ thông tin và Truyền thông,
Đại học Bách khoa Hà Nội

9

Làm thể nào để truyền tin ẩn danh

- Sử dụng dịch vụ proxy

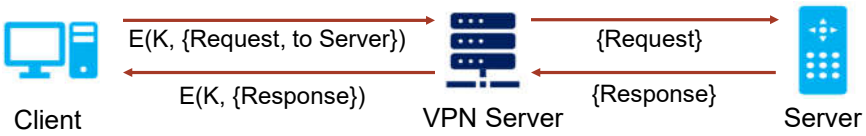


Tuy nhiên, proxy vẫn biết được danh tính 2 bên

10

Làm thế nào để truyền tin ẩn danh

- Sử dụng VPN(Virtual Private Network)



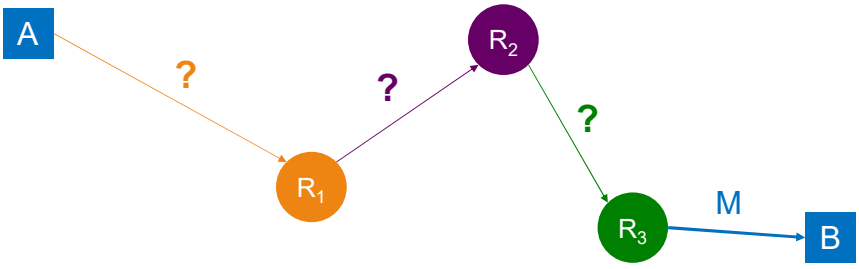
- Ẩn danh được bên gửi và bên nhận
- Tuy nhiên, VPN Server vẫn biết được danh tính 2 bên
- Cách thực hiện tốt hơn?

11

11

Định tuyến củ hành – Onion Routing

- Ý tưởng: Sử dụng một số lượng các nút tùy ý trung gian để chuyển dữ liệu
- Nguyên tắc: Không nút nào được biết đồng thời danh tính của cả 2 bên
- Thảo luận: Thiết lập như thế nào?



12

12

Tấn công vào Onion Routing

- Khai thác thông tin từ nhân viên điều hành các nút
- Chiếm quyền điều khiển một số lượng đủ lớn các nút
- Tấn công kênh bên: phân tích thời gian bên gửi phát dữ liệu và bên nhận thu được dữ liệu

13

13

Tor Project

- Tor network: cung cấp kết nối ẩn danh, chuyển tiếp dữ liệu thông qua hệ thống Onion Router
- Tor browser: phát triển từ trình duyệt Mozzila Firefox với các tính năng bảo vệ quyền riêng tư(privacy), sử dụng Tor network để kết nối tới Web server
- Tor Onion Service: cung cấp cơ chế cho các dịch vụ chỉ có thể truy cập thông qua Tor network
  - Ví dụ: Dark Web
- Tor bridge: cơ chế đóng gói dữ liệu truyền tới Tor network để tránh kiểm duyệt

14

14

Tor network

- Bao gồm hàng nghìn Onion Router, gọi là Tor node
  - Mỗi node có cặp khóa bất đối xứng
  - Giao tiếp với các node khác thông qua kết nối TLS (Transport Layer Security)
- Vanilla Tor: thiết lập một kênh truyền (Tor circuit) giữa nguồn và đích:
  - Bao gồm một số lượng ngẫu nhiên các Tor node
- Dữ liệu trên kênh truyền được bên gửi mã hóa theo nhiều lớp:
  - Số lớp bằng với số chặng
  - Qua mỗi một chặng sẽ giải mã 1 lớp

15

15

Thiết lập khóa cho kênh truyền

Sử dụng sơ đồ trao đổi khóa Diffie-Hellman

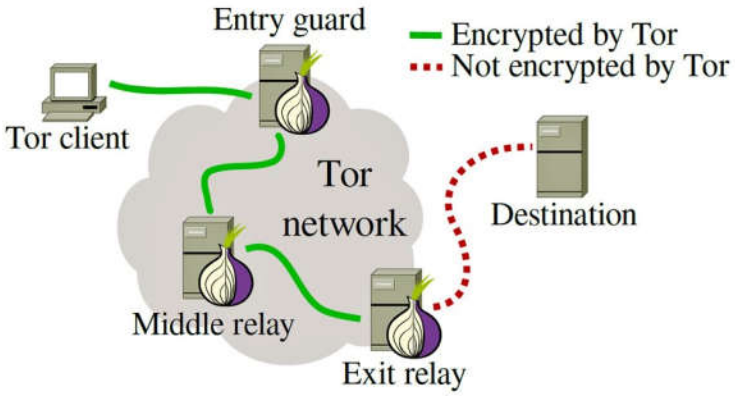
1) Bên gửi thiết lập khóa với nút thứ nhất (OR1)
   - Nút đầu tiên được gọi là nút canh giữ (guard node)
2) Bên gửi báo cho OR1 mở rộng kênh tới nút thứ 2 (OR2)
   - Thiết lập khóa với OR2 (bí mật với OR1)
   - OR2 không biết danh tính của bên gửi
3) Bên gửi báo cho OR2 mở rộng kênh tới nút thứ 3 (OR3)
   - Thiết lập khóa với OR3
   - OR3 không biết danh tính bên gửi
   - OR1 không biết kênh được mở rộng tới OR3
4) Tới nút cuối cùng gọi là nút ra (exit nodeexit relay), kênh được hoàn thành

16

16

Tor network

- Kênh phải có tối thiểu có 3 nút
  - Tại sao?
- Encryption stack: $E(K_{OR1},E(K_{OR2}(E(K_{OR3}, M \,||\, B)||OR3)||OR2)$



17

17

Tor Onion Service

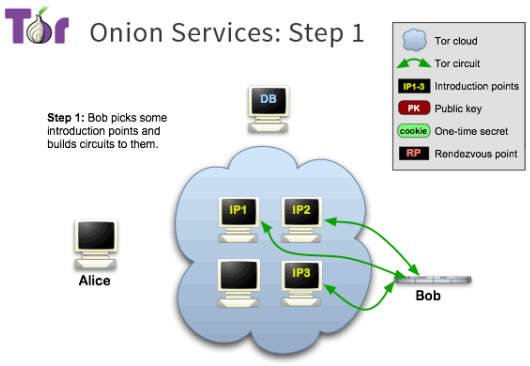
- Với Vanilla Tor và Tor Browser, danh tính client đã được che dấu
- Làm cách nào để cung cấp một dịch vụ mà máy chủ được ẩn danh?
- Tor Onion Service cho phép cung cấp 1 dịch vụ trên Tor network mà không để lộ tên miền và địa chỉ IP của máy chủ
  - Tên miền dạng *.onion
  - Khóa công khai của dịch vụ được băm để tạo ID cho dịch vụ
  - Ví dụ, chợ đen AlphaBay: http://pwoah7foa6au2pul.onion

18

18

Thiết lập Tor Onion Service

- B1: Chọn một số Tor node ngẫu nhiên để thiết lập kênh. Những nút này được gọi là điểm giới thiệu dịch vụ (introduction point)

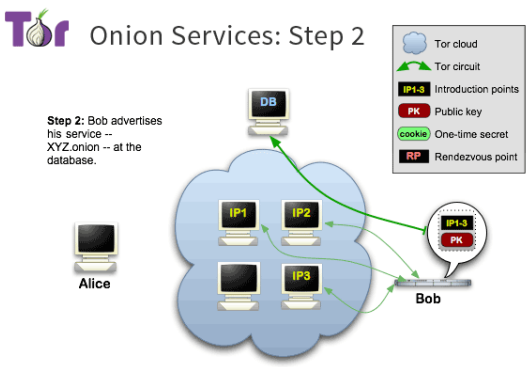


19

19

Thiết lập Tor Onion Service

- B2: Tạo bản mô tả dịch vụ bao gồm khóa công khai và danh sách các điểm giới thiệu dịch vụ. Bản mô tả được ký bằng khóa riêng. Lưu bản mô tả bằng CSDL với ID của dịch vụ là mã băm(16 byte) của khóa công khai.

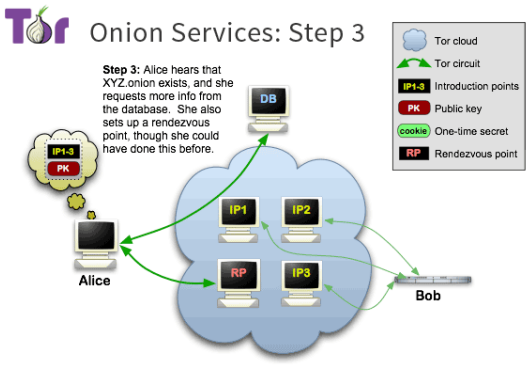


20

20

Kết nối Tor Onion Service

- B3: Client thiết lập kênh ẩn danh và yêu cầu 1 nút ngẫu nhiên là điểm hẹn(rendezvous point)

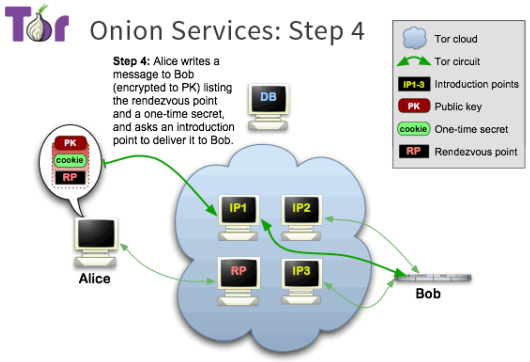


21

21

Kết nối Tor Onion Service

- B4: Client gửi yêu cầu kết nối tới một trong các điểm giới thiệu dịch vụ. Yêu cầu này được mã hóa bởi khóa công khai của dịch vụ, nội dung bao gồm địa chỉ điểm hẹn, giá trị bí mật cookie

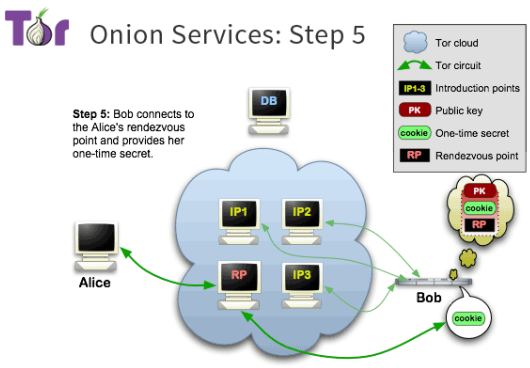


22

22

Kết nối Tor Onion Service

- B5: Máy chủ dịch vụ kết nối tới điểm hẹn và gửi đi giá trị ngẫu nhiên

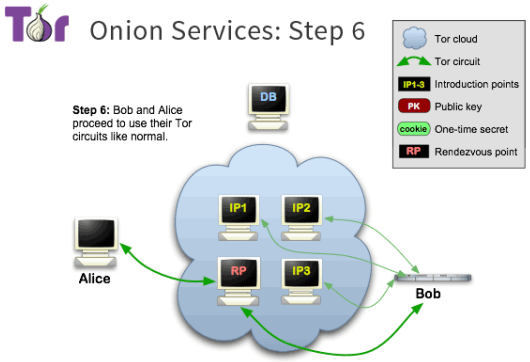


23

23

Kết nối Tor Onion Service

- B6: Nút điểm hẹn gửi thông báo tới client đã thiết lập được kết nối tới dịch vụ.



24

24

Các vấn đề của Tor Onion Service

- Máy chủ phải sử dụng nút canh giữ (guard node) tin cậy trong một thời gian dài để thiết lập kênh truyền
- Điểm giới thiệu dịch vụ và điểm hẹn phải là các nút khác nhau
- Tốc độ rất chậm:
  - Số chặng mỗi kết nối: 6+

25

25

Tor có thực sự giúp ẩn danh?

- Các cơ chế ẩn danh chỉ hiệu quả khi nó được sử dụng trong một đám đông:
  - Bạn không khác biệt với những người khác
- Mặc định, rất dễ để chỉ ra rằng "Ai đang truy cập vào Tor network"
- Ví dụ:

6

26

Tor brigde

- Truyền tin ẩn danh cần phải thực hiện 2 yêu cầu:
  - Ẩn danh tính các bên
  - Chống lại các cơ chế kiểm duyệt
- Vanilla Tor chỉ đáp ứng tốt yêu cầu đầu tiên
- Tor bridge cung cấp cơ chế để đóng gói dữ liệu của mạng Tor bằng các giao thức khác:
  - obs3
  - Meek

27

27

Truy nguyên Tor Onion Service

- Thu thập thông tin từ dịch vụ
  - Công cụ: onion scan
- Tấn công dịch vụ
- Truy nguyên client truy cập
  - FBI sử dụng các kỹ thuật Network Investigatory Technique khai thác lỗ hổng của Tor Browser
- Đưa các nút kiểm soát vào mạng Tor
  - Hiện nay Tor project rất thận trọng cấp phép cho một nút mới

28

28