Walking Onions: Scaling Anonymity Networks while Protecting Users

Chelsea H. Komlo¹, Nick Mathewson², Ian Goldberg¹

¹ University of Waterloo          ² The Tor Project

USENIX Security Symposium, 13 August 2020

CrySP
Cryptography, Security, and Privacy
— Research Group @ uWaterloo —
Tor is a privacy-enhancing tool to use the Internet privately and circumvent censorship.
Current Tor Path Selection and Circuit Extension

Current Consensus

Create

$R_1 \rightarrow R_2 \rightarrow R_3 \rightarrow R_4 \rightarrow R_5 \rightarrow R_6$

Chelsea Komlo, Nick Mathewson, Ian Goldberg
Walking Onions
13 August 2020
Current Tor Path Selection and Circuit Extension

Current Consensus

1

R1

R2

R3

R4

R5

R6

Chelsea Komlo, Nick Mathewson, Ian Goldberg

Walking Onions

13 August 2020
Current Tor Path Selection and Circuit Extension

Current Consensus

Extend $R_5$

$R_1, R_2, R_3, R_4, R_5, R_6$
Current Tor Path Selection and Circuit Extension
Current Tor Path Selection and Circuit Extension

Current Consensus

R1 → R2 → R5

R1 → R3

R1 → R4 → R6
Current Tor Path Selection and Circuit Extension

Current Consensus

R1
R2
R3
R4
R5
R6

Chelsea Komlo, Nick Mathewson, Ian Goldberg
Walking Onions
13 August 2020 3 / 17
Current Tor Path Selection and Circuit Extension

Current Consensus

Extend $R_6$

$R_1 \rightarrow R_2 \rightarrow R_5$

$R_3 \rightarrow R_4 \rightarrow R_6$
Current Tor Path Selection and Circuit Extension

Current Consensus

Extend $R_6$
Current Tor Path Selection and Circuit Extension
Current Tor Path Selection and Circuit Extension

Current Consensus
Current Tor Path Selection and Circuit Extension

Current Consensus

- $R_1$
- $R_2$
- $R_3$
- $R_4$
- $R_5$
- $R_6$
Current Tor Path Selection and Circuit Extension

Current Consensus

R1

R2

R3

R4

R5

R6

6
Current Tor Path Selection and Circuit Extension

Current Consensus
Epistemic Attacks: Users with different views of the network can be distinguished by their relay selection.
Tor Security Model: Security over Scalability

- **Epistemic Attacks**: Users with different views of the network can be distinguished by their relay selection.

  **Tor’s Protection**: All clients to maintain an up-to-date consensus copy.
Tor Security Model: Security over Scalability

- **Epistemic Attacks**: Users with different views of the network can be distinguished by their relay selection.

  **Tor’s Protection**: All clients to maintain an up-to-date consensus copy.

- **Route-Capture Attacks**: When an adversary can influence users’ relay selection.
Tor Security Model: Security over Scalability

- **Epistemic Attacks**: Users with different views of the network can be distinguished by their relay selection.

**Tor’s Protection**: All clients to maintain an up-to-date consensus copy.

- **Route-Capture Attacks**: When an adversary can influence users’ relay selection.

**Tor’s Protection**: Clients verify relay responses using signing keys in the consensus.
What Contributions Does Walking Onions Make?

- **Constant-Size Client Overhead.** Client bandwidth overhead remains constant even as new relays join (or at worst logarithmic).
What Contributions Does Walking Onions Make?

- **Constant-Size Client Overhead.** Client bandwidth overhead remains constant even as new relays join (or at worst logarithmic).

- **Maintains Tor’s Existing Security Model.** One variant has no change, the other a slight loosening of forward secrecy (for path selection, not content).
What Contributions Does Walking Onions Make?

- **Constant-Size Client Overhead.** Client bandwidth overhead remains constant even as new relays join (or at worst logarithmic).

- **Maintains Tor’s Existing Security Model.** One variant has no change, the other a slight loosening of forward secrecy (for path selection, not content).

- **Immediate Performance Improvements.** Demonstrates improvements at networks the size of Tor today.
What Contributions Does Walking Onions Make?

- **Constant-Size Client Overhead.** Client bandwidth overhead remains constant even as new relays join (or at worst logarithmic).

- **Maintains Tor’s Existing Security Model.** One variant has no change, the other a slight loosening of forward secrecy (for path selection, not content).

- **Immediate Performance Improvements.** Demonstrates improvements at networks the size of Tor today.

- **Generally Applicable.** Aspects of Walking Onions apply to network designs beyond Tor.
What Improvements Does Walking Onions Make?

- How to represent relay information to enable oblivious selection and individual verification?
What Improvements Does Walking Onions Make?

- How to represent relay information to enable oblivious selection and individual verification?
- How to build paths using oblivious relay selection?
What Improvements Does Walking Onions Make?

- How to represent relay information to enable oblivious selection and individual verification?
- How to build paths using oblivious relay selection?
- How to perform more efficient circuit construction?
What improvements does Walking Onions make?

- How to represent relay information to enable oblivious selection and individual verification?
New Data Structure: Separable Network Index Proof (SNIP)

Current Consensus

- Network Parameters
- Relay Entries
New Data Structure: Separable Network Index

Current Consensus

[5284,5716)
New Data Structure: Separable Network Index Proof (SNIP)

Current Consensus

SNIPs
ENDIVE: Efficient Network Directory with Independently Verifiable Entries

Current Consensus

SNIPs

ENDIVE
ENDIVE: Efficient Network Directory with Independently Verifiable Entries
What improvements does Walking Onions make?

- How to represent relay information to enable oblivious selection and individual verification?
- How to build paths using oblivious relay selection?
Telescoping Walking Onions

$R_1 \rightarrow R_4$

$R_2$

$R_3$

$R_5$

$R_6$
Telescoping Walking Onions
Telescoping Walking Onions
Telescoping Walking Onions

$R_1$ → $R_2$ → $R_5$ → $R_3$
Telescoping Walking Onions

- $R_1$
- $R_2$
- $R_3$
- $R_4$
- $R_5$
- $R_6$
Telescoping Walking Onions

R₁

R₂

R₃

R₄

R₅

R₆
Telescopings Walking Onions

Diagram showing relationships between various parts labeled as $R_1$, $R_2$, $R_3$, $R_4$, $R_5$, and $R_6$. Connections and keys are indicated in the diagram.
Telescoping Walking Onions

\[ R_1 \rightarrow R_2 \rightarrow R_5 \rightarrow R_3 \]

\[ \text{Key: } 3 \]

Chelsea Komlo, Nick Mathewson, Ian Goldberg

Walking Onions

13 August 2020 11 / 17
Telescoping Walking Onions

$R_1$, $R_2$, $R_3$, $R_4$, $R_5$, $R_6$
Telescoping Walking Onions

Diagram showing the connections between $R_1$, $R_2$, $R_3$, $R_4$, $R_5$, and $R_6$. The diagram illustrates the telescoping effect in Walking Onions.
Telescoping Walking Onions

R_1 \rightarrow R_2 \rightarrow R_3 \rightarrow R_4 \rightarrow R_5 \rightarrow R_6

Chelsea Komlo, Nick Mathewson, Ian Goldberg

13 August 2020
Telescoping Walking Onions
What improvements does Walking Onions make?

- How to represent relay information to enable oblivious selection and individual verification?
- How to build paths using oblivious relay selection?
- How to perform more efficient circuit construction?
Single-Pass Walking Onions

\[ R_4 \]

\[ R_2 \]

\[ R_5 \]

\[ R_3 \]

\[ R_6 \]

1, 1
Single-Pass Walking Onions

\[ k \leftarrow DH(r_{\overline{5}}, \overline{s}_{\overline{5}}) \]

\[ r \leftarrow VRF_{\overline{5}}(DH(r_{\overline{5}}, \overline{s}_{\overline{5}})) \]
Single-Pass Walking Onions

\[ k' \leftarrow DH(\cdot, \cdot_3) \]
\[ r' \leftarrow VRF_{\cdot_3}(DH(\cdot', \cdot_3)) \]
Single-Pass Walking Onions
Single-Pass Walking Onions

$R_4$

$R_2$

$R_3$

$R_5$

$R_6$
Single-Pass Walking Onions
Performance Evaluation
Walking Onions requires 4–6 times less bandwidth than Vanilla Onion Routing at a network the size of Tor today. Improvement of 25–40 times less bandwidth at a network 10 times the size of Tor.

Chelsea Komlo, Nick Mathewson, Ian Goldberg
Walking Onions requires 4–6 times less bandwidth than Vanilla Onion Routing at a network the size of Tor today.

Improvement of 25–40 times less bandwidth at a network 10 times the size of Tor.
Walking Onions requires 4–6 times less bandwidth than Vanilla Onion Routing at a network the size of Tor today.

Improvement of 25–40 times less bandwidth at a network 10 times the size of Tor.
Bandwidth Results for Tor Clients

Clients in Walking Onions save 10–15 times the bandwidth over Vanilla Onion Routing in a network the size of Tor today.

In a network 10 times the size of Tor, Walking Onions saves clients 90–150 times the bandwidth over Vanilla.
Clients in Walking Onions save 10–15 times the bandwidth over Vanilla Onion Routing in a network the size of Tor today.
Clients in Walking Onions save 10–15 times the bandwidth over Vanilla Onion Routing in a network the size of Tor today.

In a network 10 times the size of Tor, Walking Onions saves clients 90–150 times the bandwidth over Vanilla.
Takeaways

- The design of Tor today imposes impractical overheads to clients as the network scales.

Find our paper and artifact at https://crysp.uwaterloo.ca/software/walkingonions
Takeaways

- The design of Tor today imposes impractical overheads to clients as the network scales.

- Walking Onions:

Find our paper and artifact at https://crysp.uwaterloo.ca/software/walkingonions
Takeaways

- The design of Tor today imposes impractical overheads to clients as the network scales.

- Walking Onions:
  - Removes the per-relay bandwidth and storage cost to clients

Find our paper and artifact at https://crysp.uwaterloo.ca/software/walkingonions
The design of Tor today imposes impractical overheads to clients as the network scales.

Walking Onions:
- Removes the per-relay bandwidth and storage cost to clients
- Offers the same security protections against epistemic and route capture attacks as prior designs that required a globally consistent view.

Find our paper and artifact at https://crysp.uwaterloo.ca/software/walkingonions
Takeaways

- The design of Tor today imposes impractical overheads to clients as the network scales.

- Walking Onions:
  - Removes the per-relay bandwidth and storage cost to clients
  - Offers the same security protections against epistemic and route capture attacks as prior designs that required a globally consistent view.

- Tor has already begun the specification work to integrate Walking Onions into the Tor protocol.

Find our paper and artifact at https://crysp.uwaterloo.ca/software/walkingonions