One Cell is Enough to Break Tor's Anonymity

Xinwen Fu
University of Massachusetts Lowell
Team members
Zhen Ling, Southeast University
Junzhou Luo, Southeast University
Wei Yu, Cisco Systems Inc.
Weijia Jia, City Univ. of Hong Kong
Wei Zhao, Univ. of Macau

University of Massachusetts Lowell
UMASS Lowell

nis University of Massachusetts Lowell Center for Network and Inforamtion Security

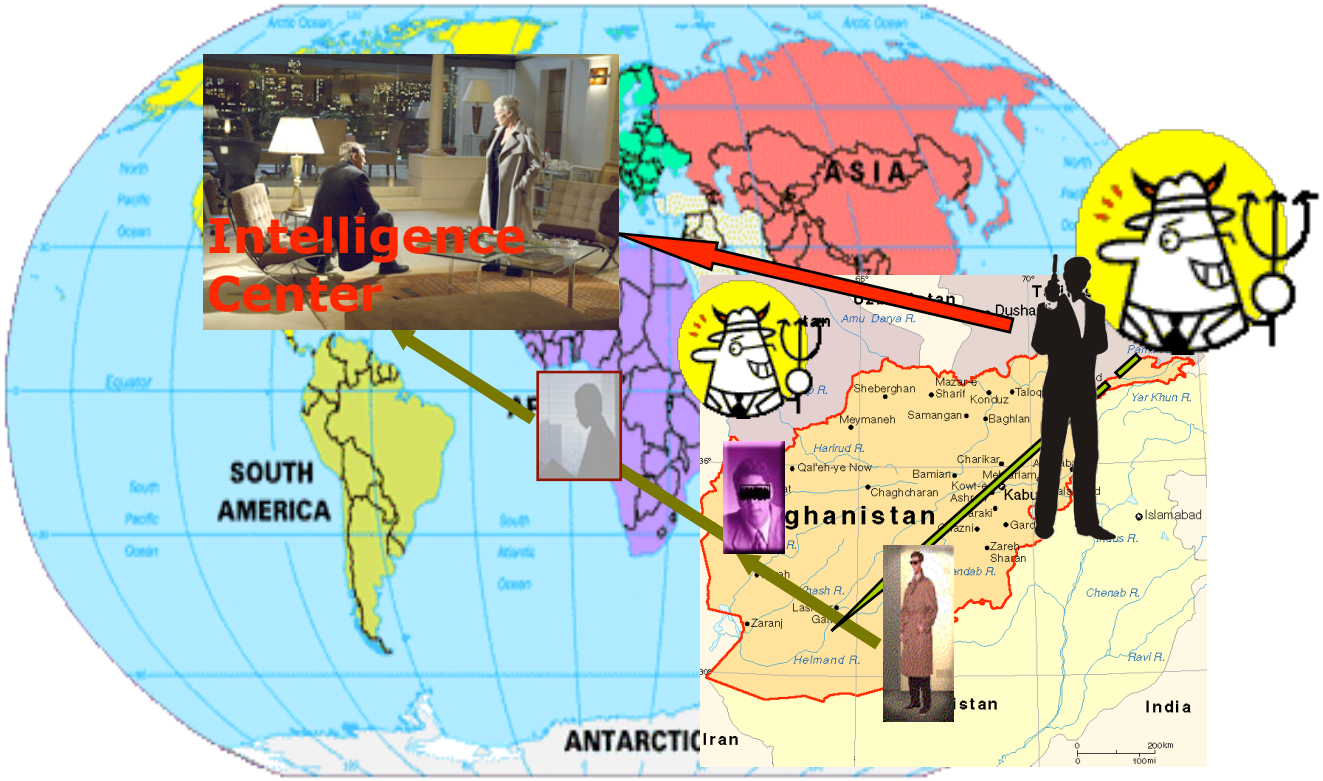
Outline

- Introduction
- Basic components and operation of Tor
- Protocol-level attacks
- Impact of protocol-level attacks
- Guideline of countermeasures
- Related work
- Summary

Internet Security

- Internet has brought convenience to our everyday lives
- Internet has many design vulnerabilities
  - Malicious codes (worm and viruses) caused $13.2 billions in financial losses worldwide in 2001
- We need to understand these attacks and design corresponding countermeasures
- We present our research on a new type of attack against anonymous communication systems

Traditional Spy Network



- Indirectly send secret to Intelligence headquarter through a number of intermediate agents
- Protect the intelligence agent (i.e., source of secret) from being identified

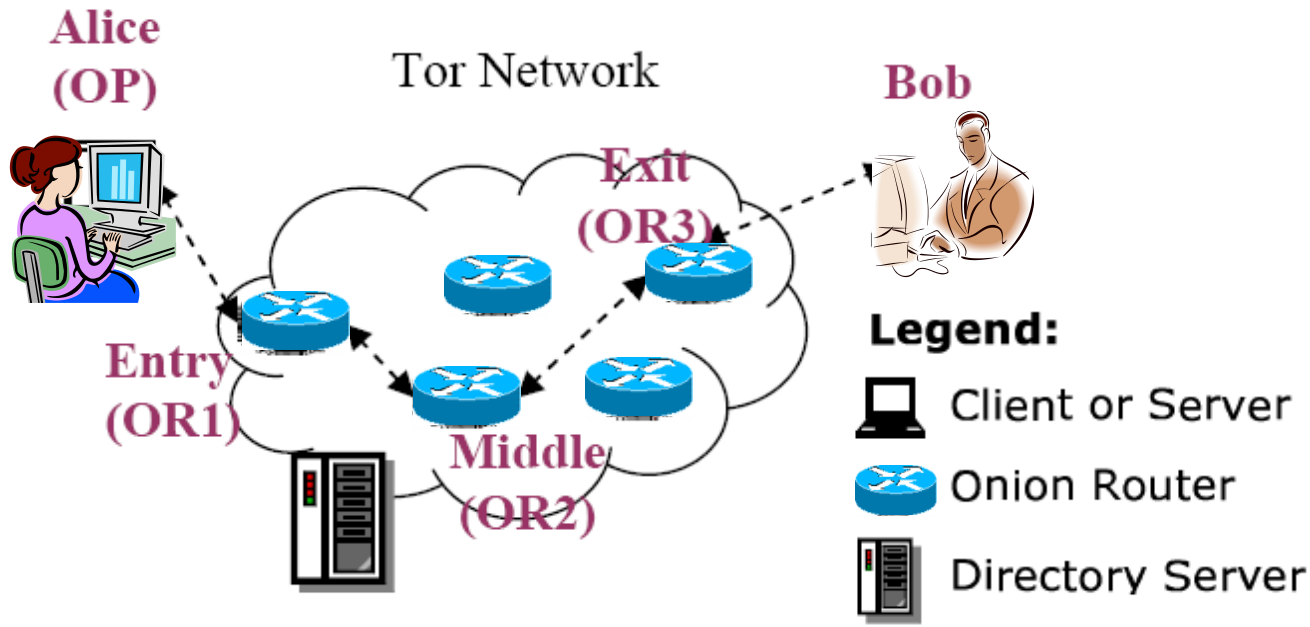
Outline

- Introduction
- Basic components and operation of Tor
- Protocol-level attacks
- Impact of protocol-level attacks
- Guideline of countermeasures
- Related work
- Summary

Tor

- A great Internet anonymous communication network
- Volunteer operation model
  - Volunteers around the world donate their computers and network bandwidth
  - Those donated computers form the Tor network based on the Tor protocol
  - Those computers in the Tor network relay user messages down to the destination
- Users of Tor
  - Human rights workers
  - Many others: refer to Tor website https://www.torproject.org/torusers.html.en/

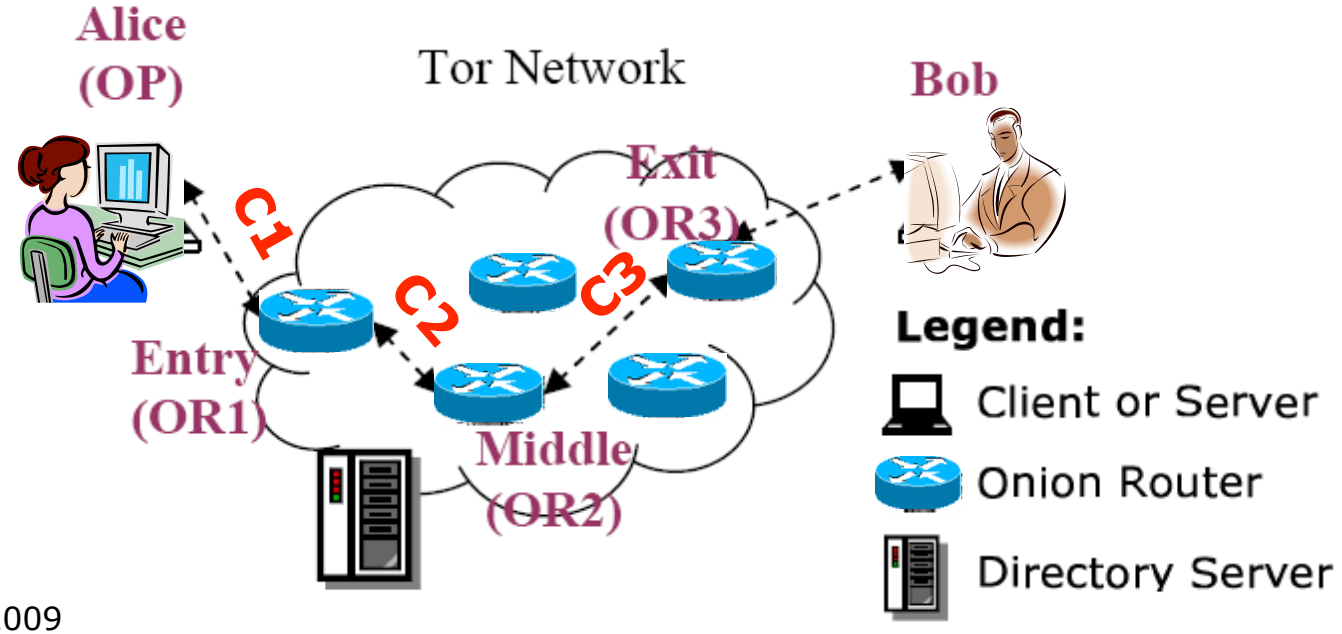
Components of Tor



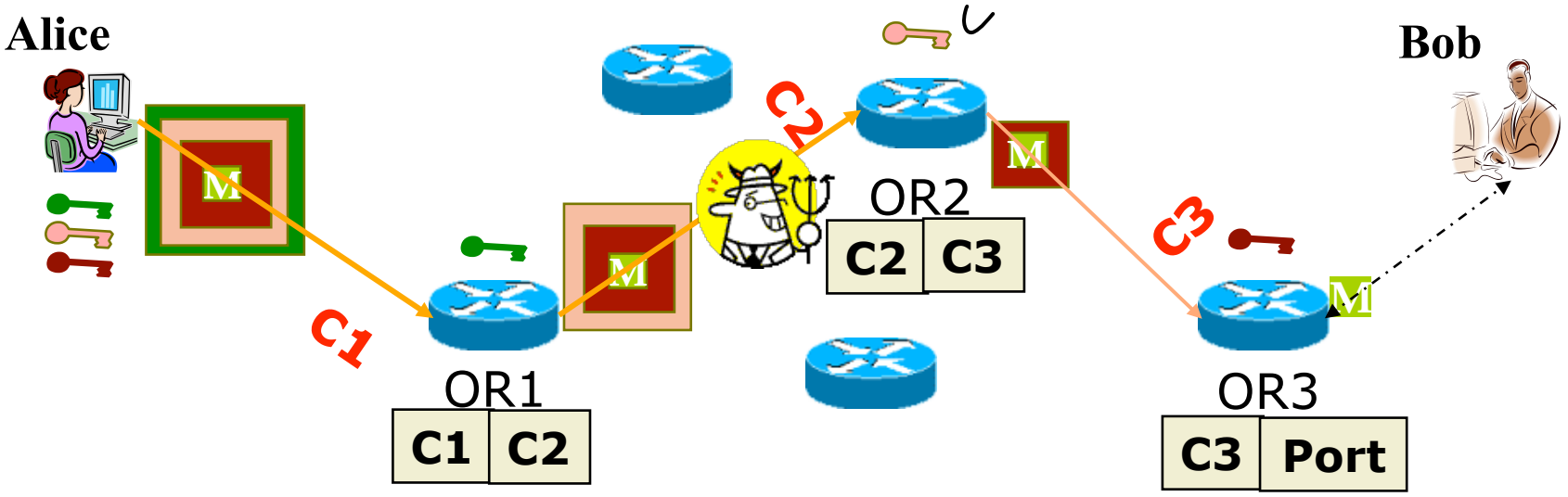
- **Client**: the user of the Tor network
- **Server**: the target TCP applications such as web servers
- **Tor (onion) router**: the special proxy relays the application data
- **Directory server**: servers holding Tor router information

How Tor Works? --- Circuits

- Alice herself chooses the relay routers and creates circuits through the relay routers
  - Circuit --- communication tunnel from Alice to Bob
  - These circuits are dedicated for Alice
- Can the routers along the circuit or a third party find communication relationship by checking the packet header?



How Tor Works? --- Onion Routing



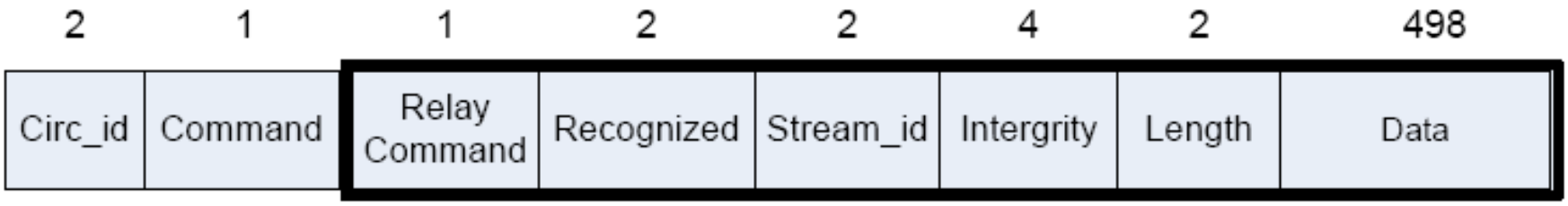
- A circuit is built incrementally one hop by one hop
- Onion-like encryption
  - Alice negotiates an AES key with each router
  - Messages are divided into equal sized cells
  - Each router knows only its predecessor and successor
  - Only the Exit router (OR3) can see the message, however it does not know where the message is from

Detailed Circuit Setup Steps: One-Hop Circuit

Alice (OP) | **Entry OR (OR1)** | **Middle OR (OR2)** | **Exit OR (OR3)** | **Bob**

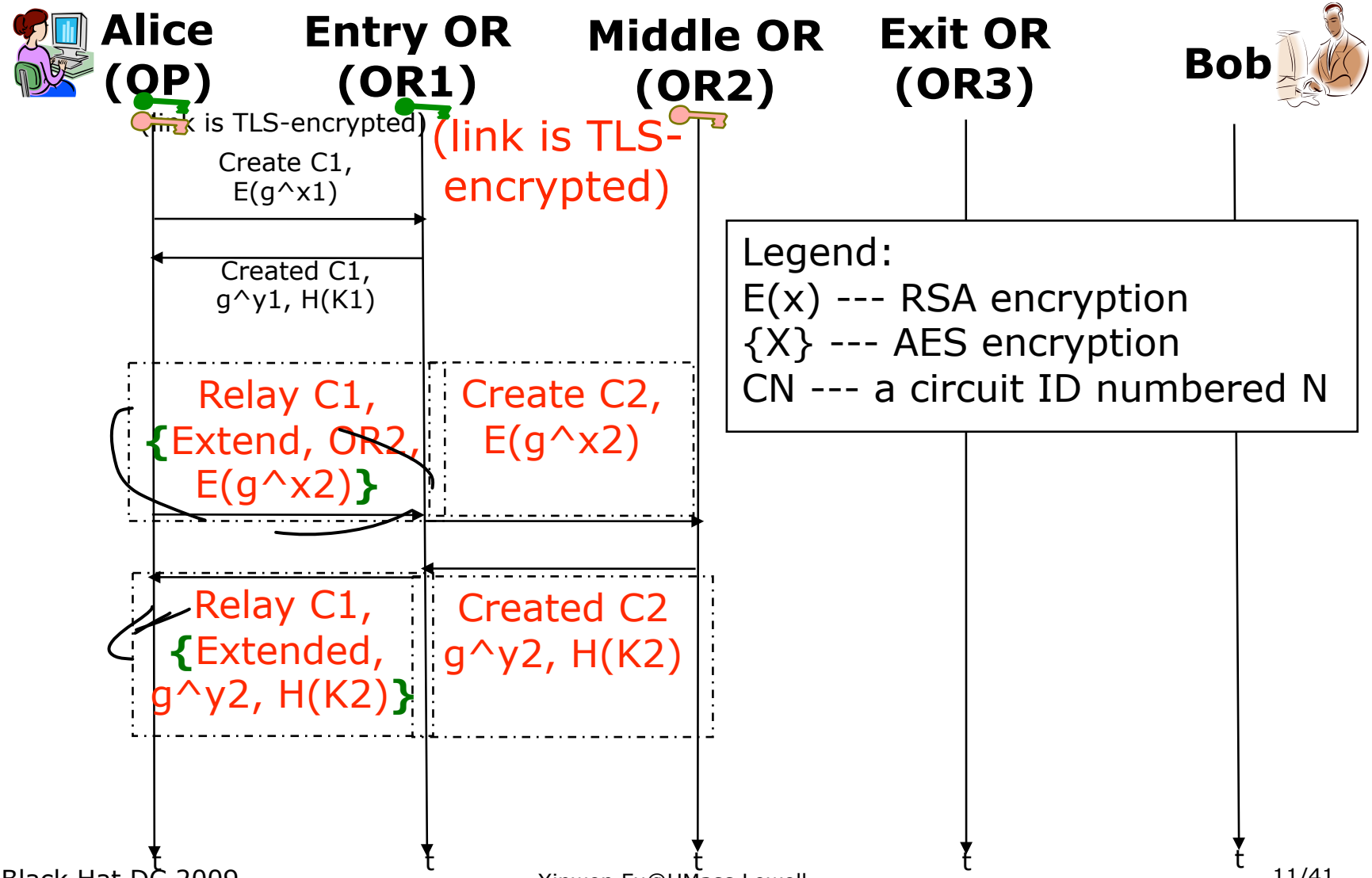
(link is TLS-encrypted)

(a) Tor Cell Format

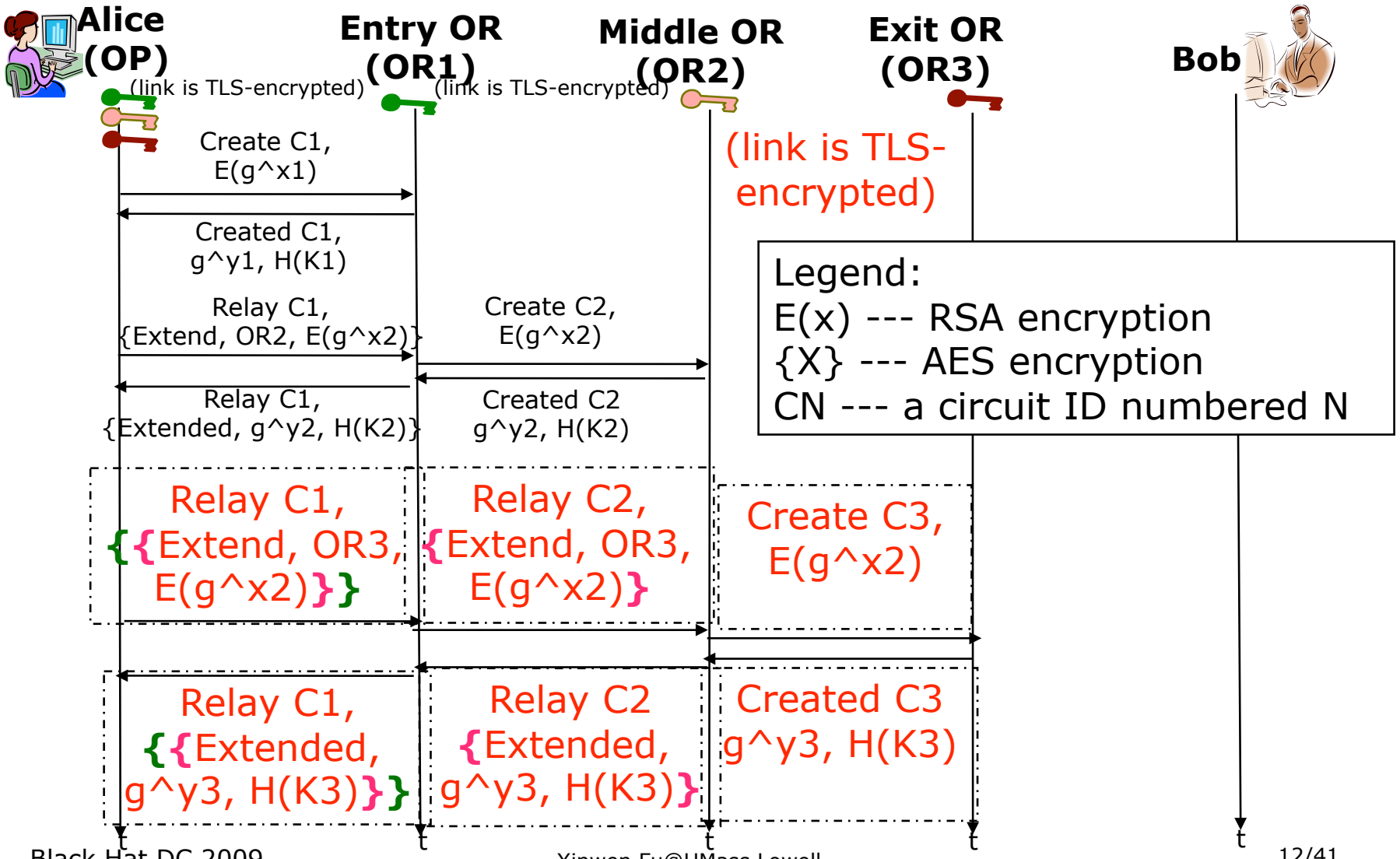


(b) Tor Realy Cell Format

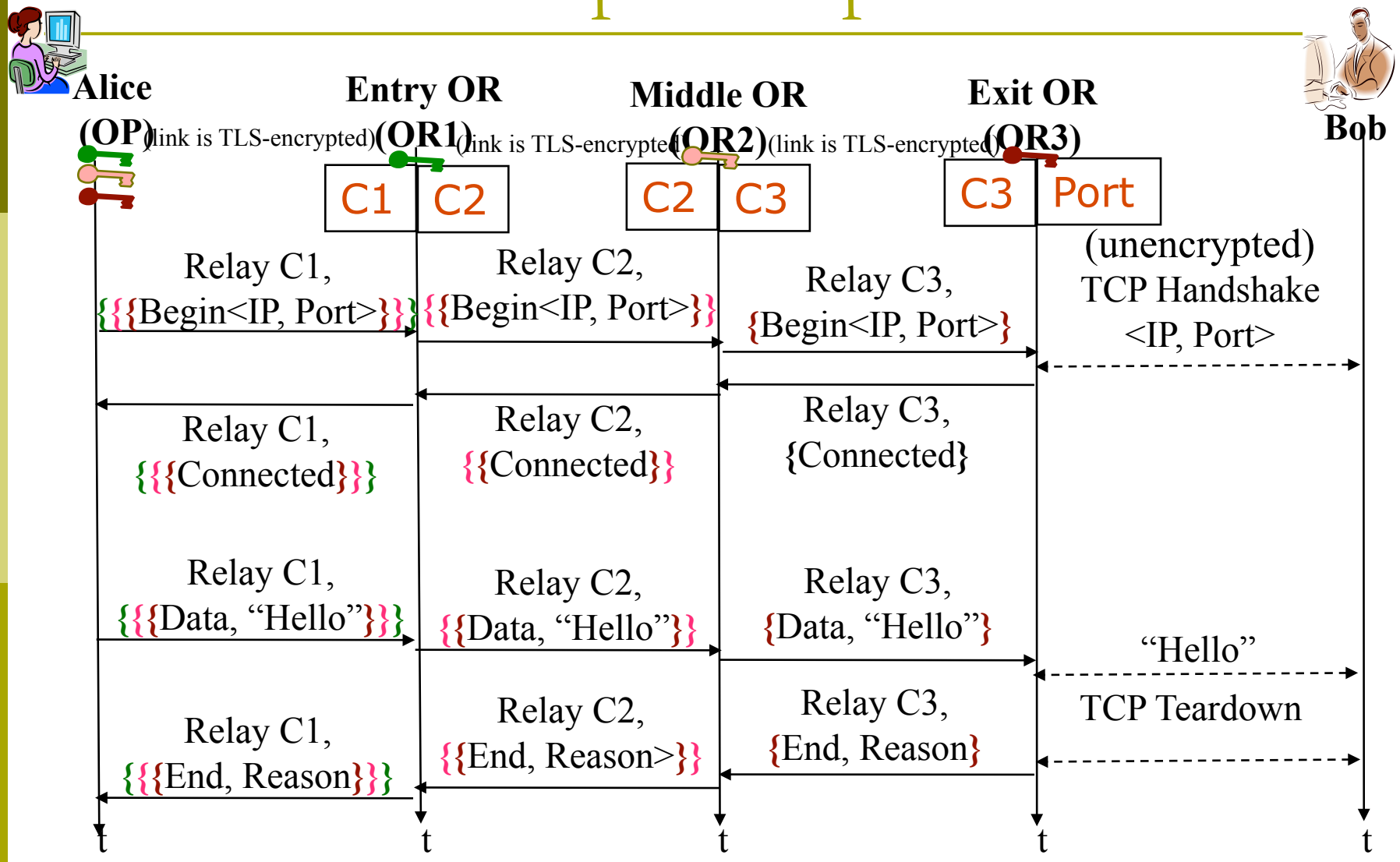
Two-Hop Circuit



Three-Hop Circuit



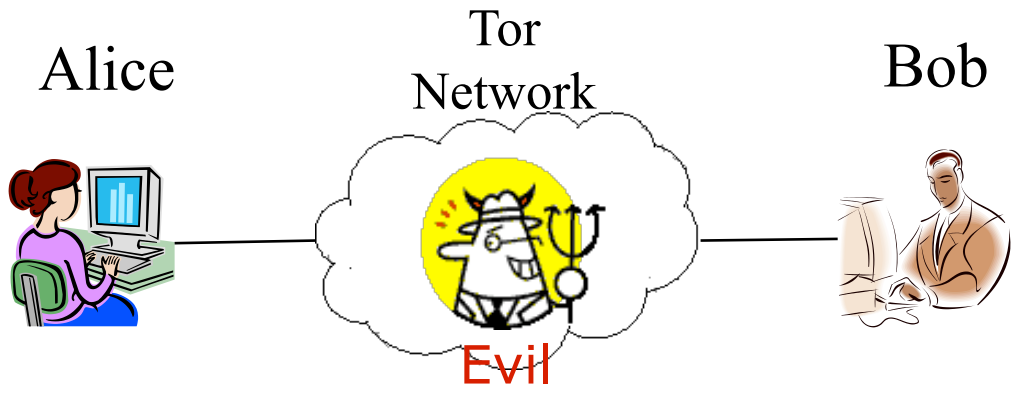
Connection Setup Example



Outline

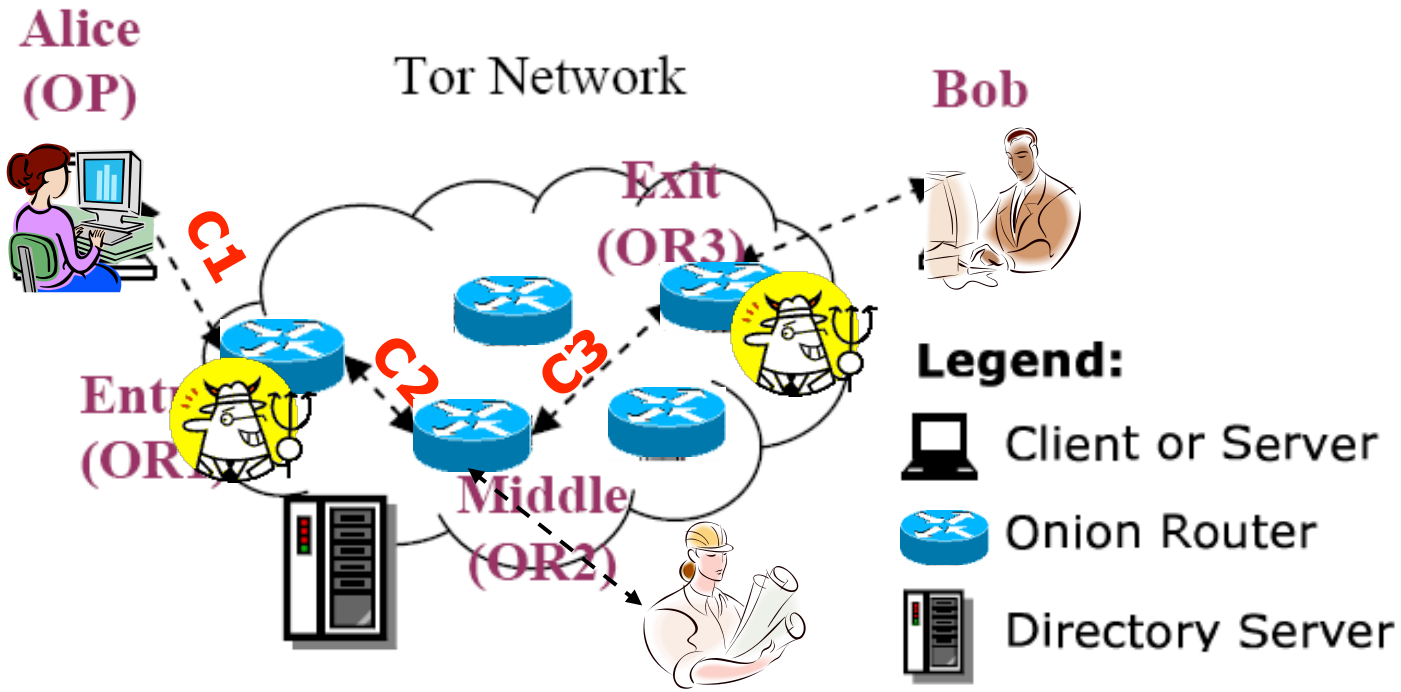
- Introduction
- Basic components and operation of Tor
- Protocol-level attacks
- Impact of protocol-level attacks
- Guideline of countermeasures
- Related work
- Summary

Problem Definition of Attacks against Tor



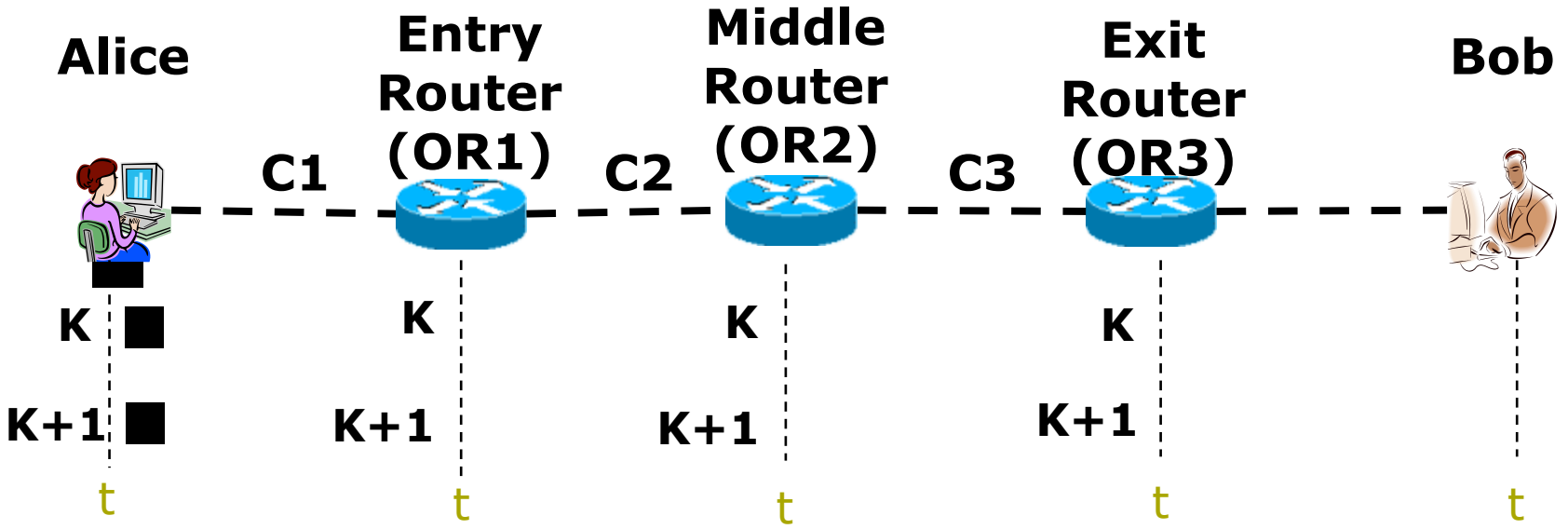
- Alice is sending messages to Bob through an encrypted and anonymous circuit, how can Evil confirm the communication relationship between Alice and Bob?

Attack Methodology



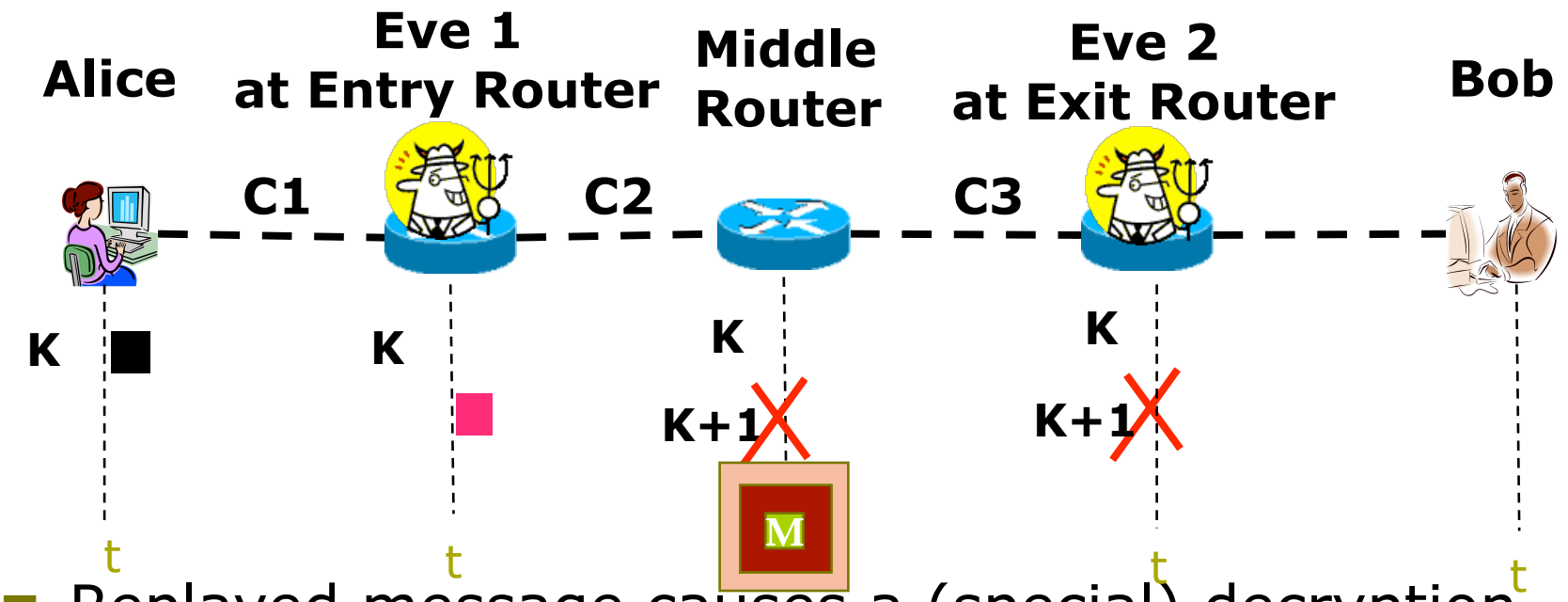
- If the attacker can determine circuit segments C1 and C3 belong to the same circuit, the attacker confirms the communication relationship for sure
  - Entry knows where the packet comes from and Exit knows where the packet goes

AES Counter – Normal Case



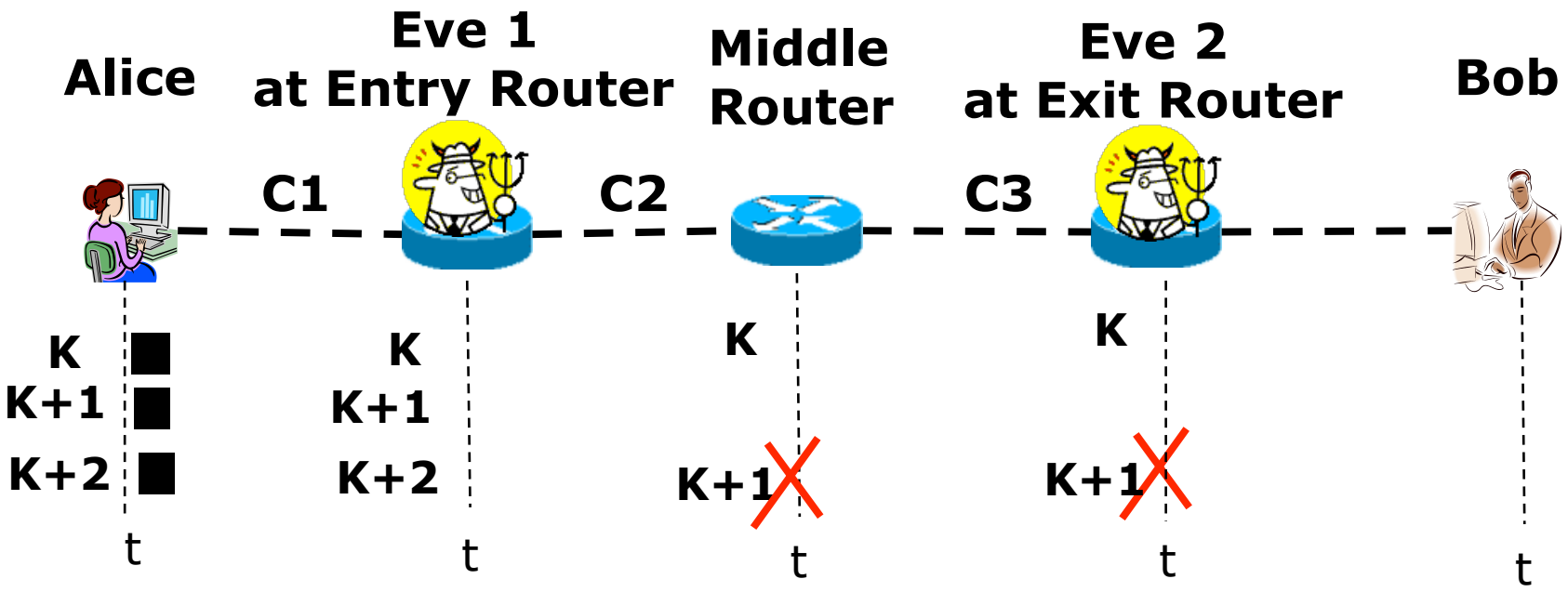
- A message comes from Alice through Circuit Segment C1, and goes to Bob after Circuit Segment C3
- An AES counter is synchronized through the circuit

AES Counter – Replay Attack Case



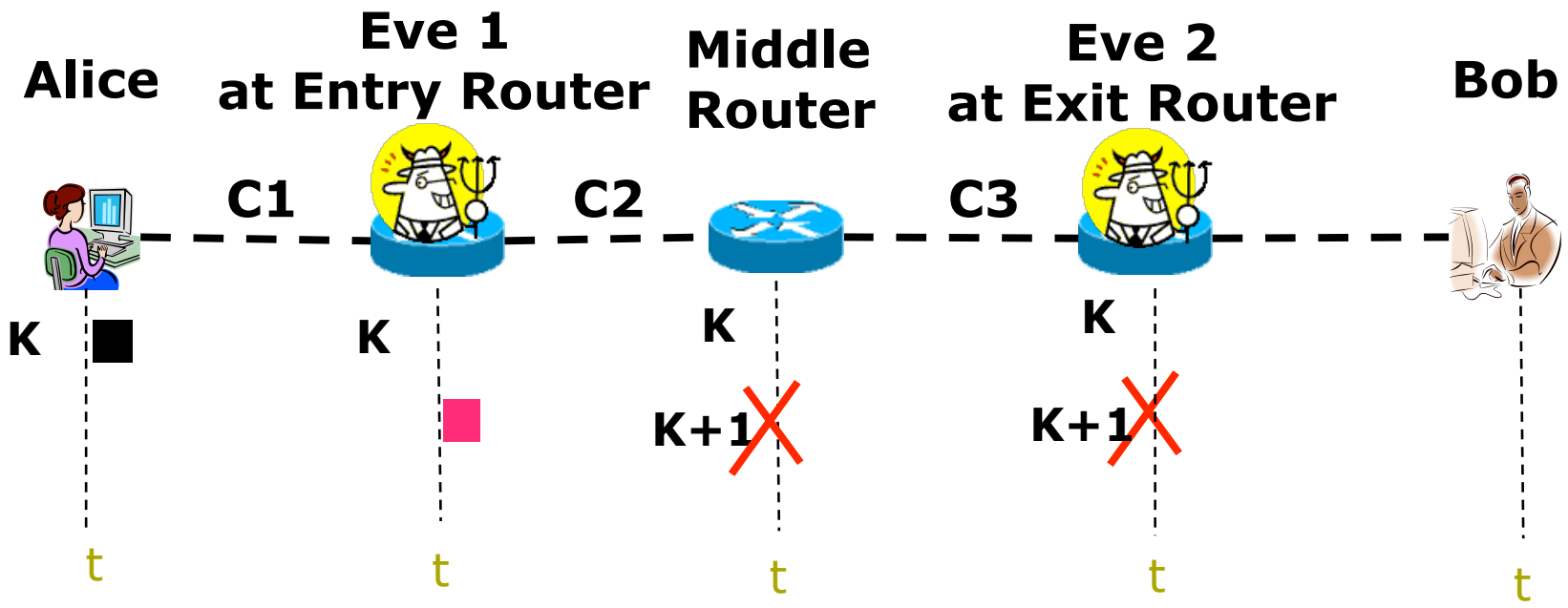
- Replayed message causes a (special) decryption error at the end of circuit C3 at Eve 2
  - The duplicated message disrupts the counter
- Therefore, Circuits C1 and C3 are created by Alice
- Claim: Alice is communicating with Bob

AES Counter – Deletion Attack Case



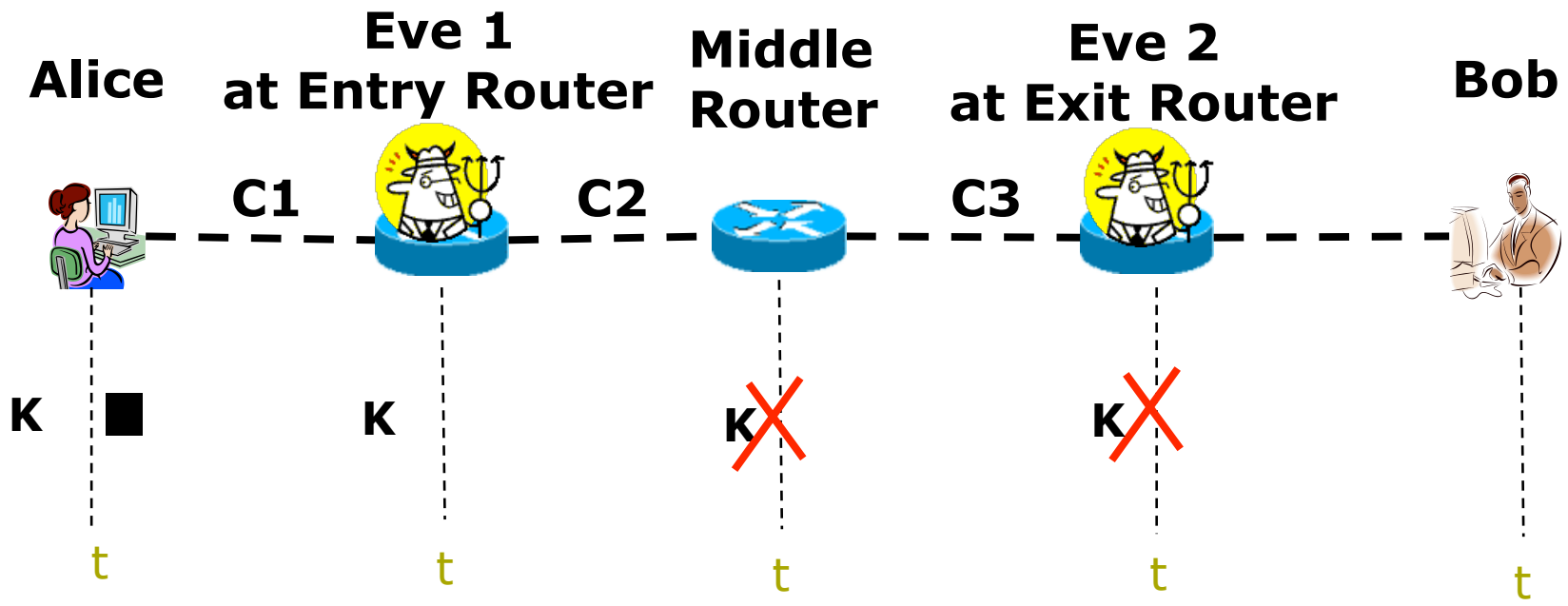
- The cell after the deleted cell causes decryption error

AES Counter – Insert Attack Case



- The inserted cell causes decryption error

AES Counter – Modify Attack Case

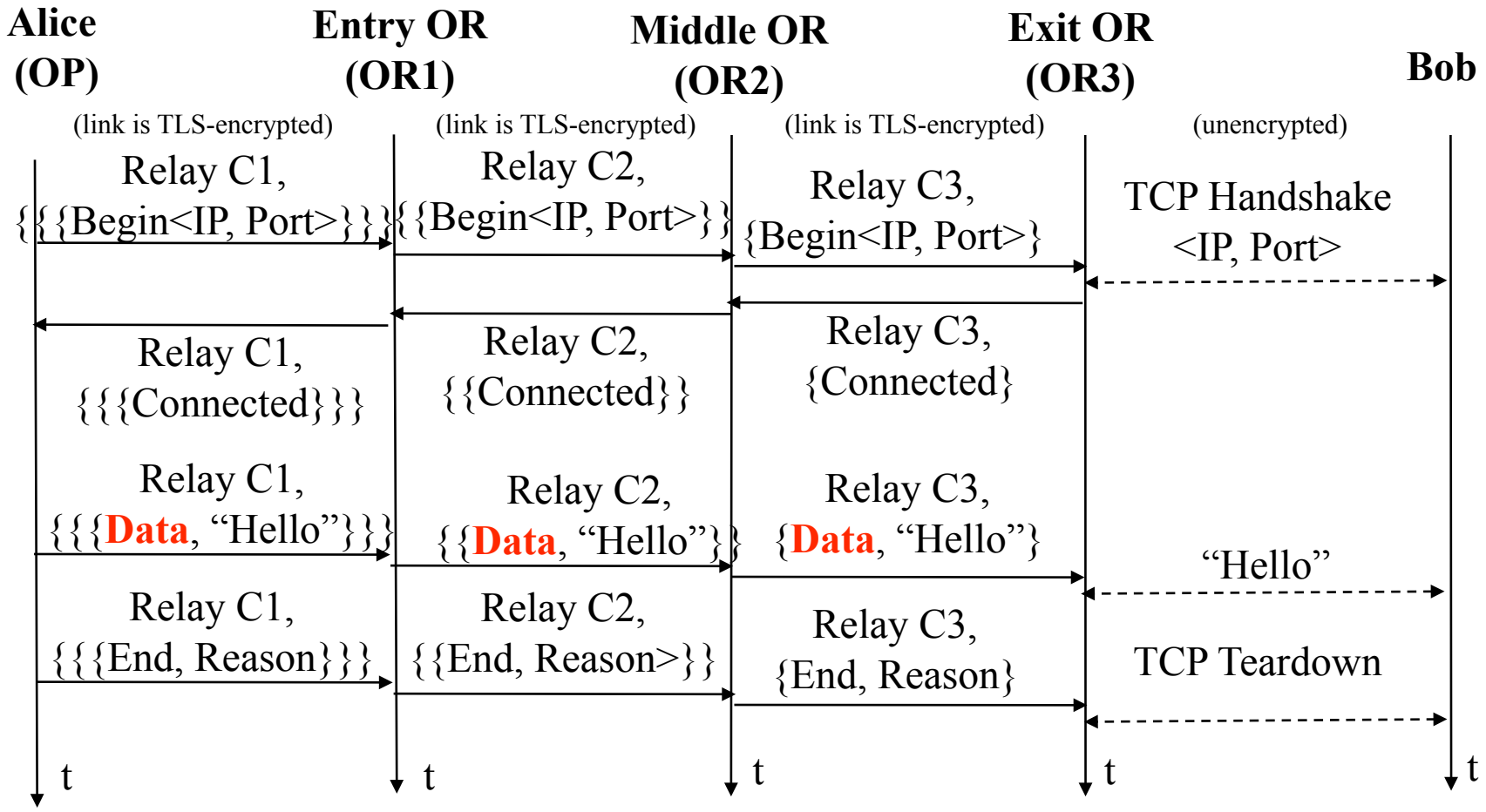


- The modified cell causes decryption error

Issues in Attacks Above

- Which cells and when to manipulate
  - The circuit is torn down when there is decryption error
- How to make attack stealthy
  - Broken circuits may render Alice's attention

Which Cells and When to Manipulate

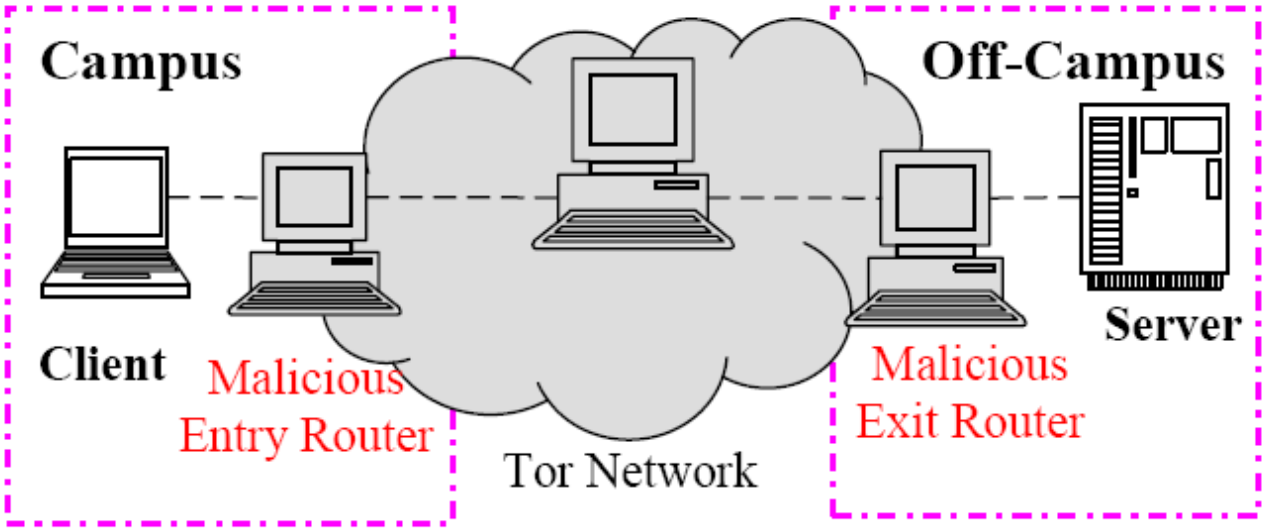


- Target data cells after the circuit is built
- Identify protocol status by counting cells

How to Make Attack Stealthy

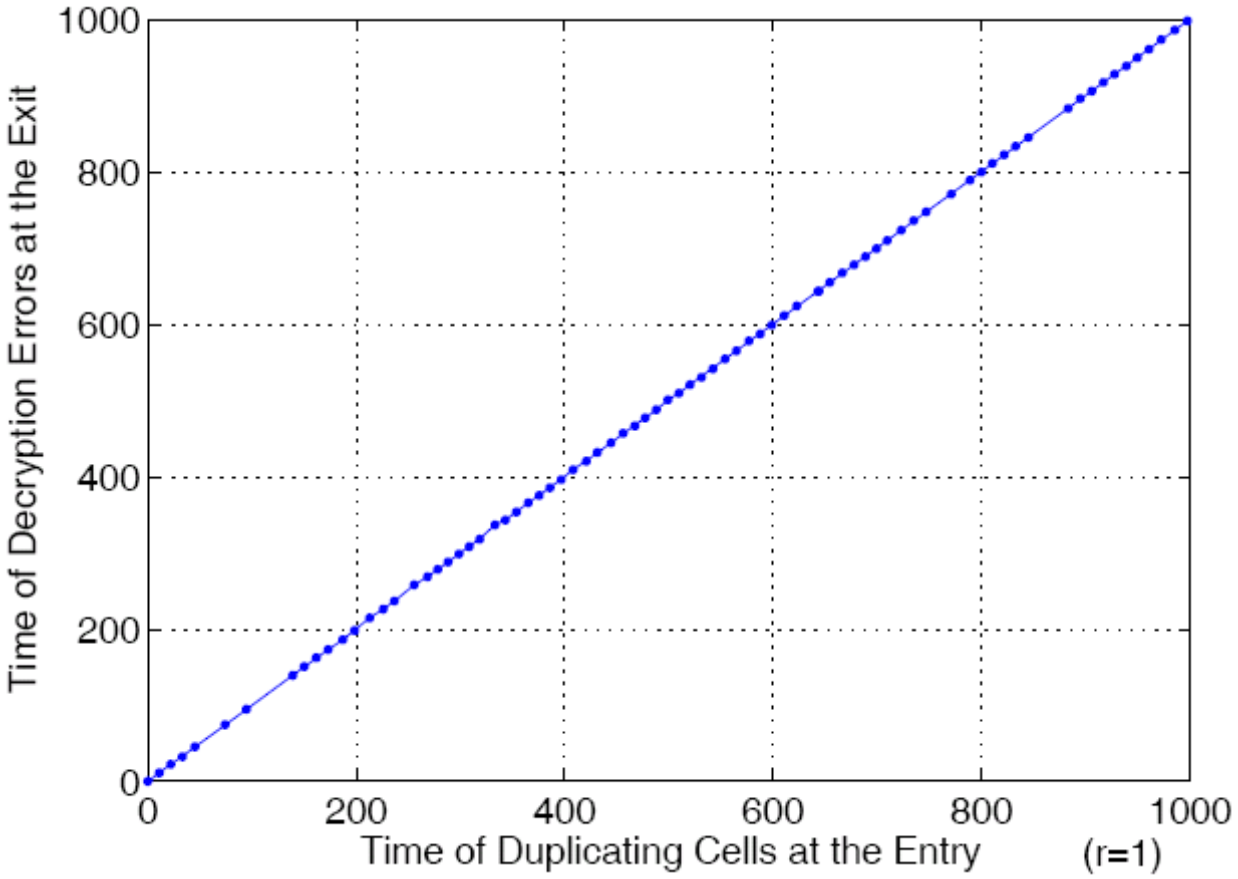
- Insert and replay attacks are very flexible and can be made stealthy can be applied freely
- When there is no traffic and a circuit is idle (the circuit already carried target traffic)
- At the end of the lifetime of a circuit
  - Default lifetime is 10 minutes
  - Before teardown
  - While holding teardown commands

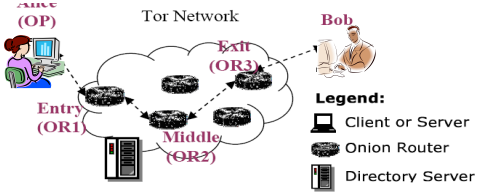
Experiment Setup



- One computer was setup as an exit router
- It takes two days for our second computer to become an entry router

Decryption Error Time v.s. Duplication Time





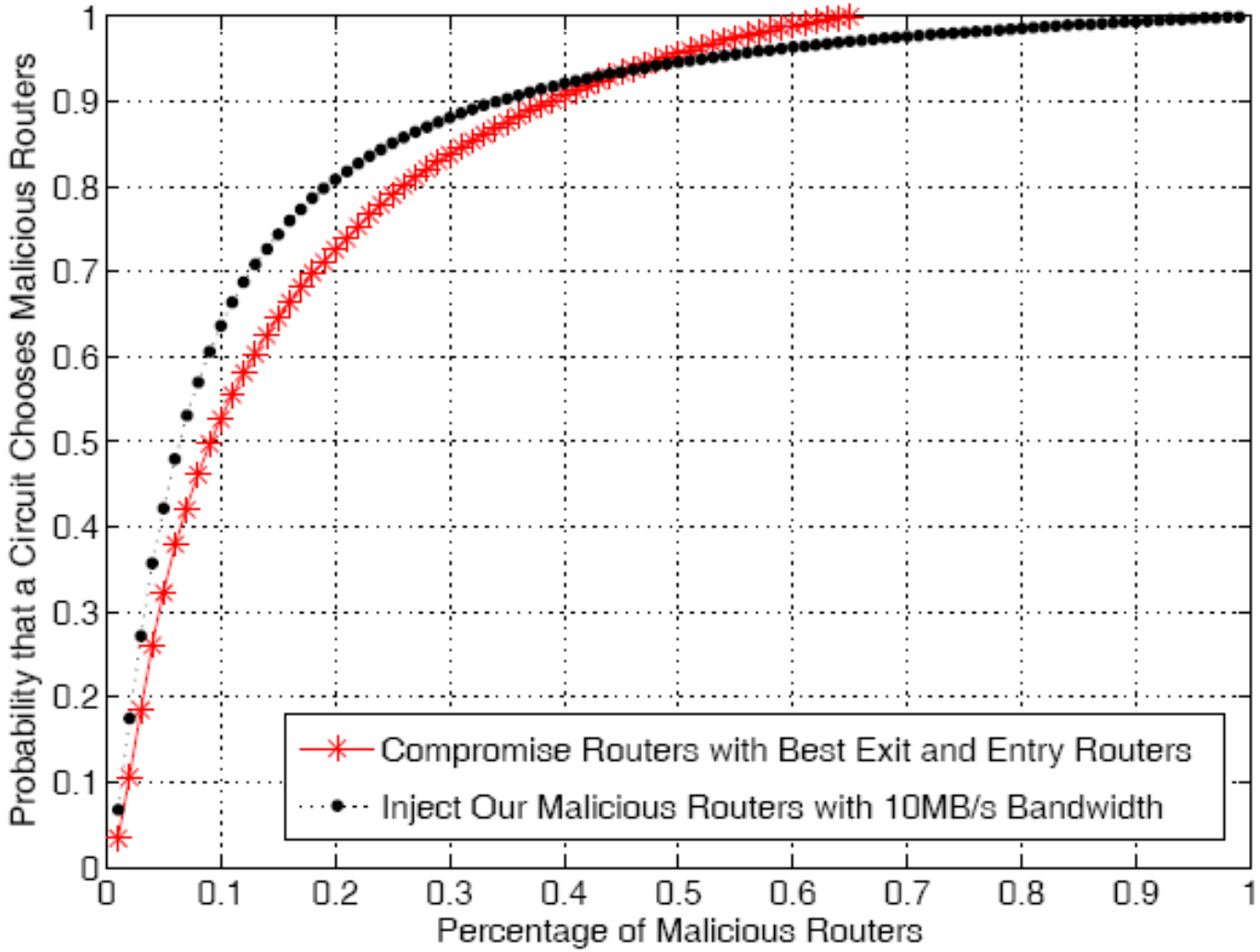
Outline

- Introduction
- Basic components and operation of Tor
- Protocol-level attacks
- Impact of protocol-level attacks
- Guideline of countermeasures
- Related work
- Summary

Impact

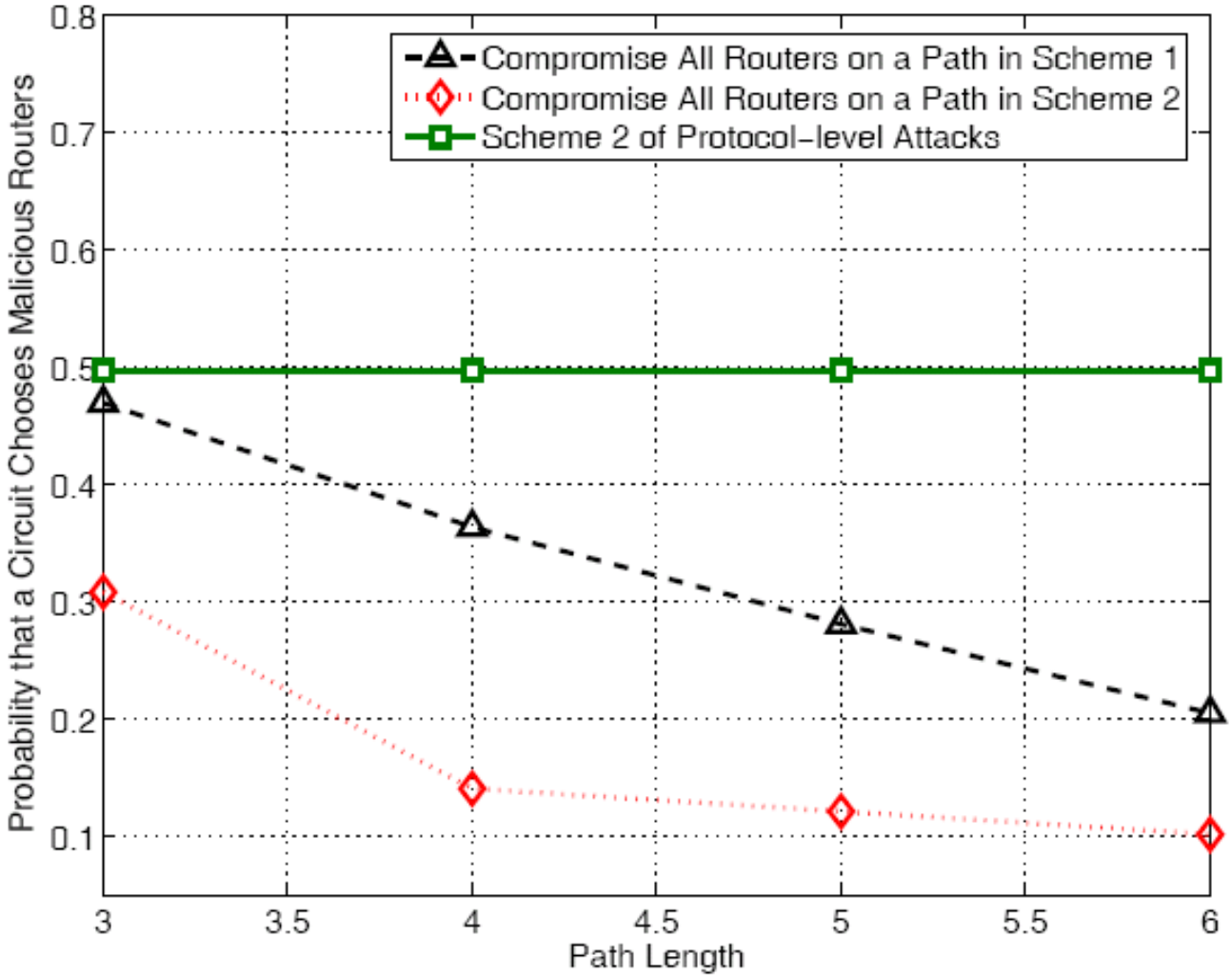
- Metrics: probability that a circuit chooses malicious Tor routers
  - A circuit chooses a malicious entry and exit, it is done
- Attackers can do the following in order to increase the probability
  - Scheme 1: Inject (donate) high-bandwidth routers into the Tor network
  - Scheme 2: Compromise high-bandwidth Tor routers into the Tor network

Big Impact: 9% v.s. 60%



Protocol-level Attack v.s. Brute Force Attack

- Brute force attack: attackers occupy all routers on a circuit



Outline

- Introduction
- Basic components and operation of Tor
- Protocol-level attacks
- Impact of protocol-level attacks
- Guideline of countermeasures
- Related work
- Summary

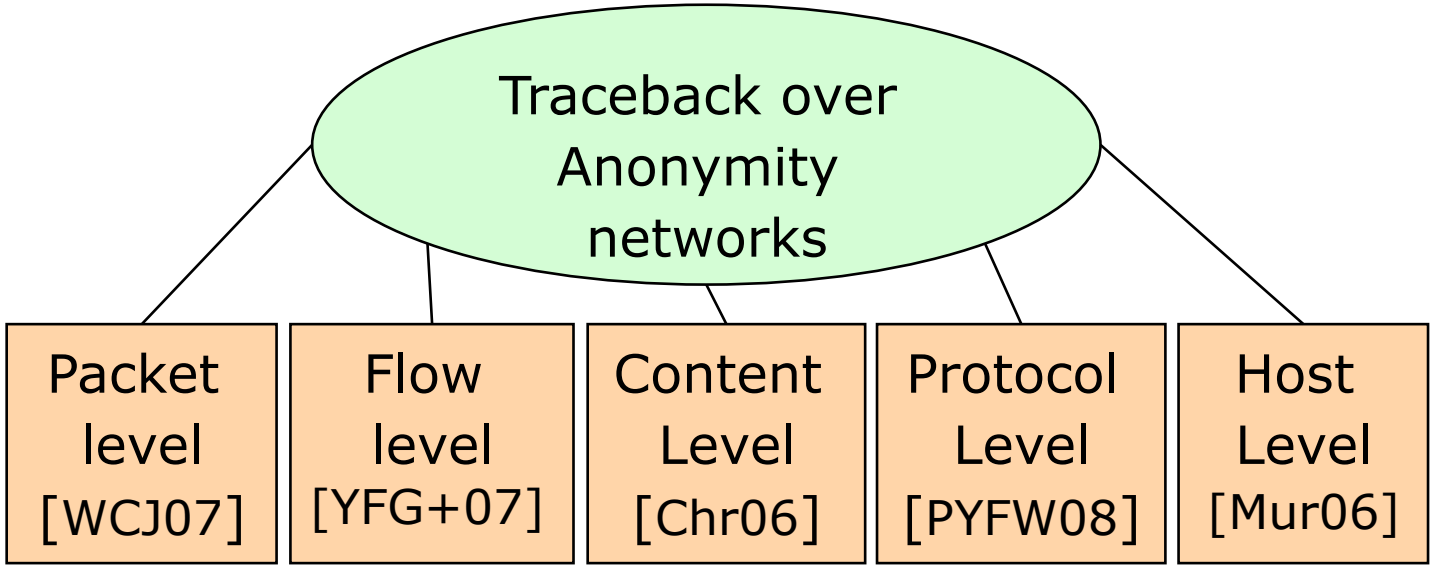
Hard to Defend

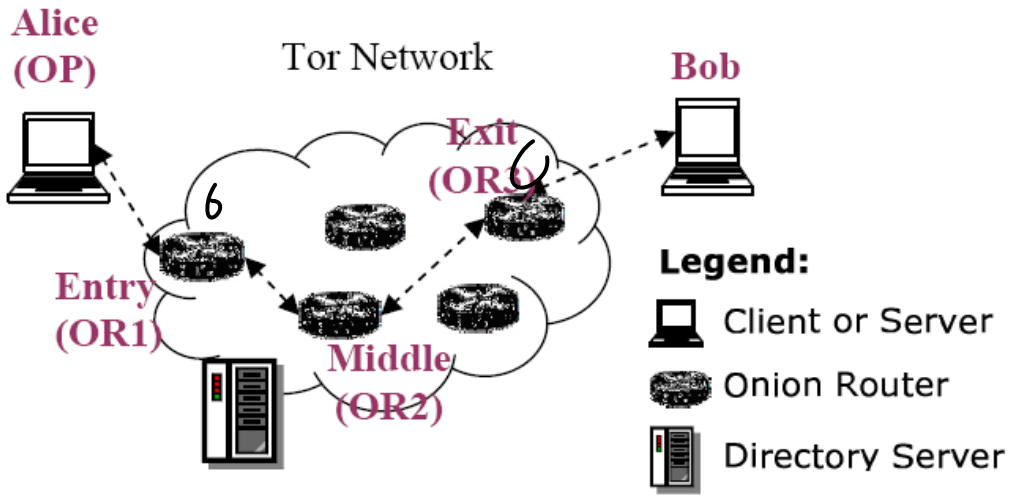
- No easy way to defend against replay, insert, delete and modify attacks because of the anonymity maintained here
  - The attacks are flexible can be deployed at any moment during the life time of a connection
  - What if attackers just attack for DoS?
- Careful routing protocols
  - Choose routers in different countries or regions in order to prevent a single organization from deploying the attack

Outline

- Introduction
- Basic components and operation of Tor
- Protocol-level attacks
- Impact of protocol-level attacks
- Guideline of countermeasures
- Related work
- Summary

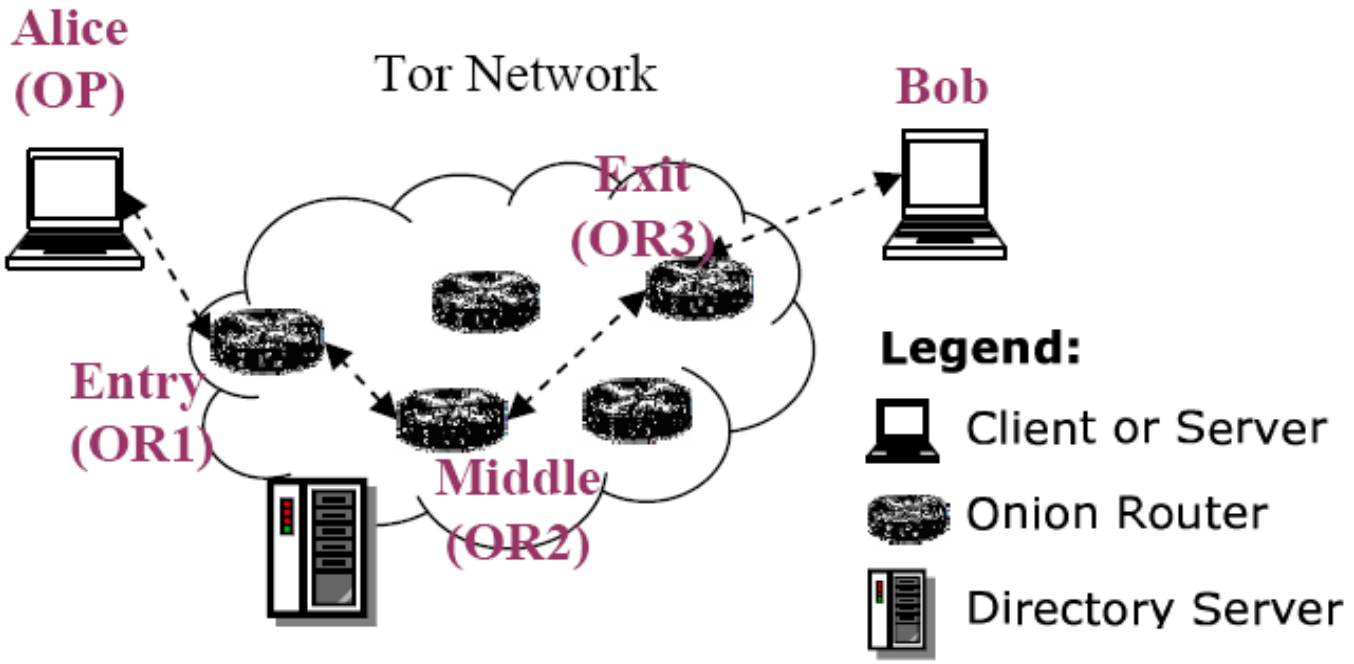
Many Attacks





Tagging Attacks

- Outside attackers mark attacks: use TLS to guarantee integrity
- Protocol-level attacks are by inside attackers



Outline

- Introduction
- Basic components and operation of Tor
- Protocol-level attacks
- Impact of protocol-level attacks
- Guideline of countermeasures
- Related work
- Summary

Summary

- We identified a class of new attack, protocol-level attack, against anonymous communication network Tor
  - Need only one cell to confirm the communication relationship
  - One attack can confirm multiple connections using the same circuit
  - Confirmation is a sure thing (100%)
- Our experiments validate the feasibility and effectiveness of all attacks
- The impact is huge
  - Given 9% percent of Tor routers are malicious, over 60% of the connections can be compromised

Future Work

- Develop countermeasure against the protocol-level attack
  - Tor is a pioneer software for on-line privacy
- Fight the abuse of Tor (forensic traceback)
  - Anonymous networks may be abused
  - Government has resource and donates high-performance routers and bandwidth to Tor in exchange of necessary surveillance
  - The abuse of Tor threatens Tor

Acknowledgment

- Tor developers
- Other Tor researchers

References

[Chr06] A. Christensen, Practical Onion Hacking: finding the real address of Tor clients, http://packetstormsecurity.org/0610-advisories/Practical_Onion_Hacking.pdf, Oct. 2006

[DMP04] R. Dingledine, N. Mathewson, and P. Syverson, Tor: The second-generation onion router, in Proceedings of the 13th USENIX Security Symposium, 2004

[Mur06] Steven J. Murdoch, Hot or Not: Revealing Hidden Services by their Clock Skew, In *Proceedings of ACM CCS*, 2006

[PNR05] P. Peng, P. Ning, and D. S. Reeves, On the secrecy of timing-based active watermarking trace-back techniques, in Proceedings of the IEEE Security and Privacy Symposium (S&P), 2006

[PYFW08] Ryan Pries, W. Yu, Xinwen Fu and W. Zhao, A New Replay Attack Against Anonymous Communication Networks, In Proceedings of the IEEE International Conference on Communications (ICC), China, May 19-23, 2008 (Best paper award)

[WCJ07] X. Wang, S. Chen , and S. Jajodia, Network flow watermarking attack on low-latency anonymous communication systems, in *Proceedings of the IEEE Security and Privacy Symposium* (*S&P*), 2007

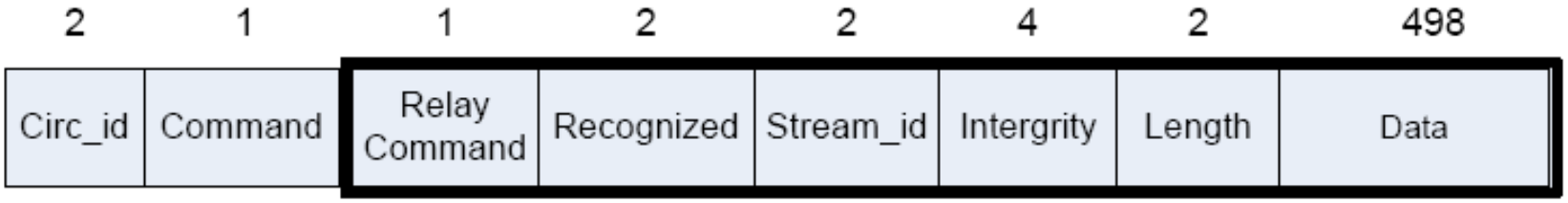
[YFG+07] W. Yu, Xinwen Fu, S. Graham, Dong Xuan, and W. Zhao, DSSS-based flow marking technique for invisible traceback, in *Proceedings of the IEEE Security and Privacy Symposium* (*S&P*), 2007

Thank you!

Xinwen Fu

Cell Format in Tor

(a) Tor Cell Format



(b) Tor Realy Cell Format