CSE 484 / CSE M 584: Computer Security and Privacy

Anonymity and Secure Messaging

Fall 2016

Ada (Adam) Lerner
lerner@cs.washington.edu

Thanks to Franzi Roesner, Dan Boneh, Dieter Gollmann, Dan Halperin, Yoshi Kohno, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...

Tor

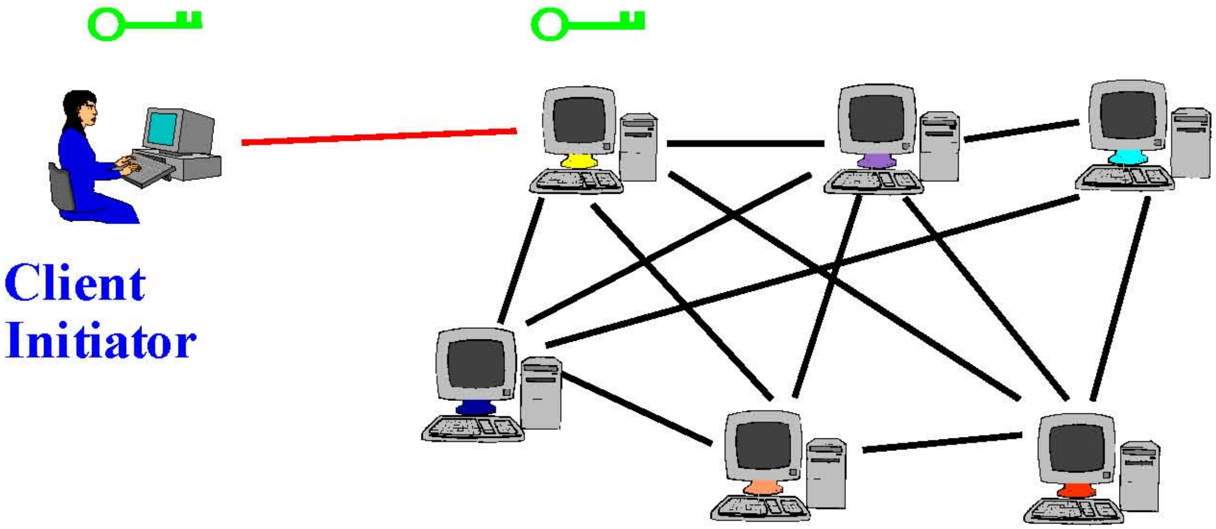
- Second-generation onion routing network
  - https://www.torproject.org/
  - Now a large open source project with a non-profit organization behind it
  - Specifically designed for low-latency anonymous Internet communications
- Running since October 2003
- “Easy-to-use” client proxy
  - Freely available, can use it for anonymous browsing

Tor Browser Bundle

- A single, downloadable browser app which does the right thing.

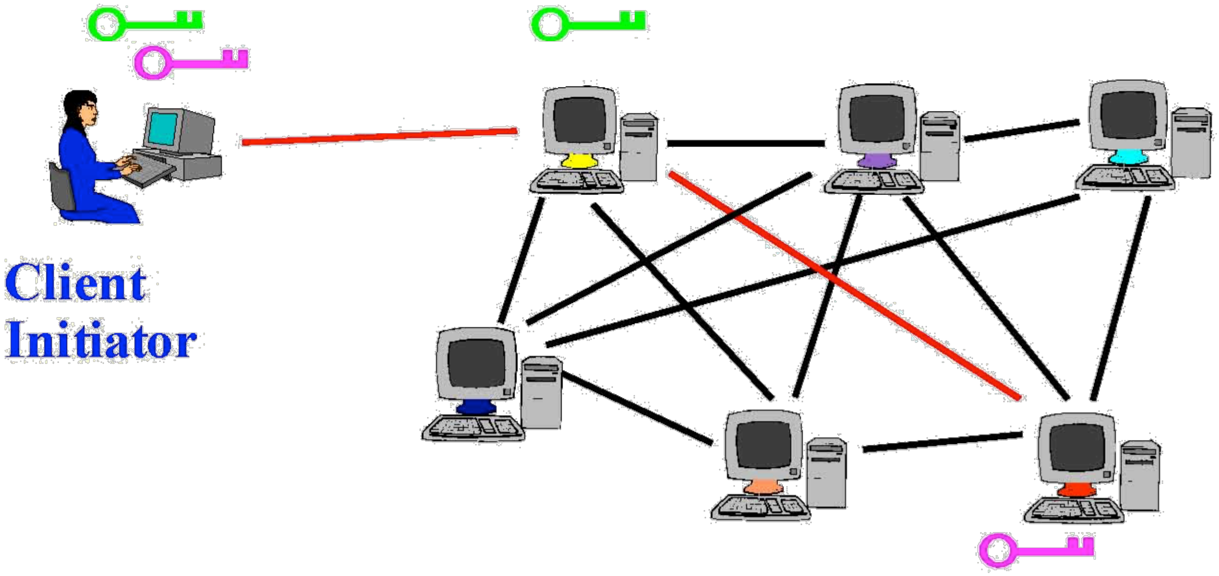
Tor Circuit Setup (1)

- Client proxy establishes a symmetric session key and circuit with Onion Router #1



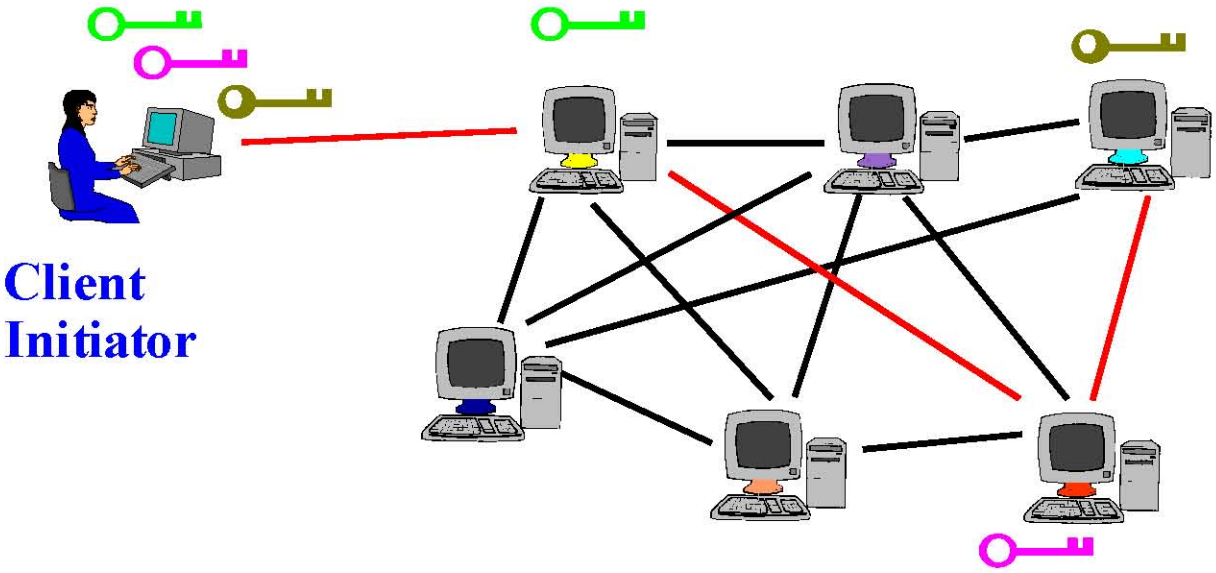
Tor Circuit Setup (2)

- Client proxy extends the circuit by establishing a symmetric session key with Onion Router #2
    - Tunnel through Onion Router #1



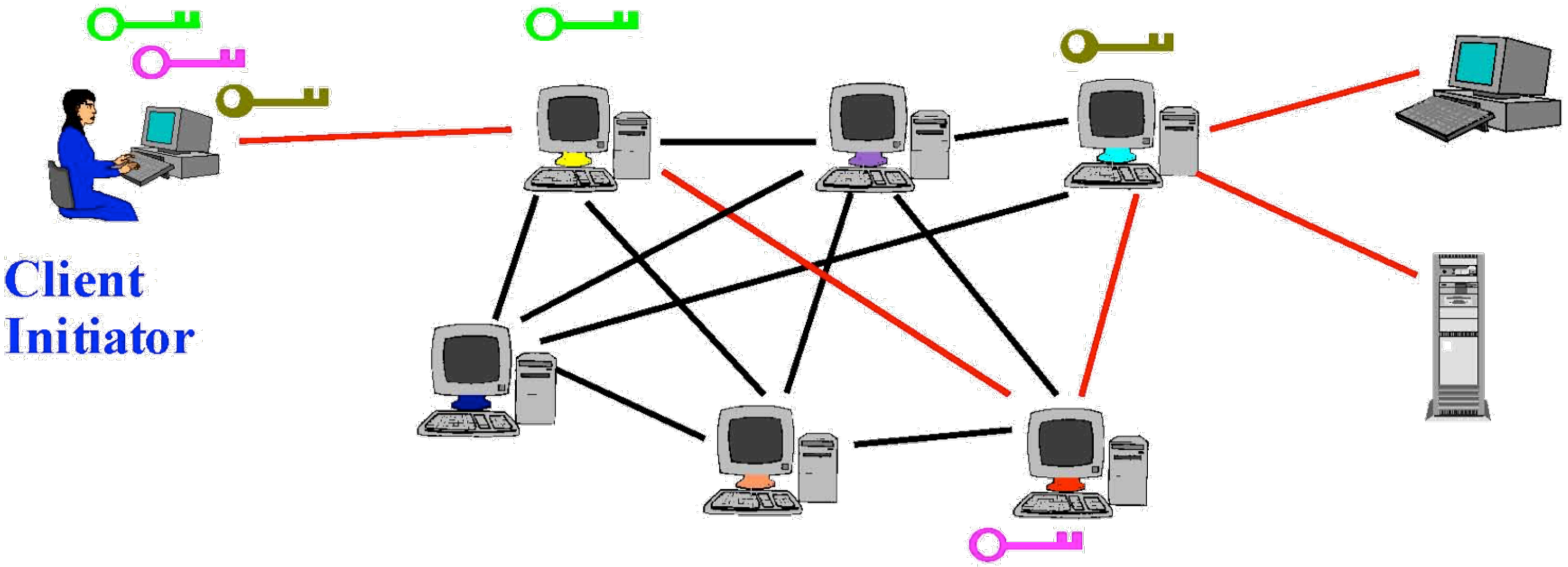
Tor Circuit Setup (3)

- Client proxy extends the circuit by establishing a symmetric session key with Onion Router #3
  - Tunnel through Onion Routers #1 and #2



Using a Tor Circuit

- Client applications connect and communicate over the established Tor circuit.



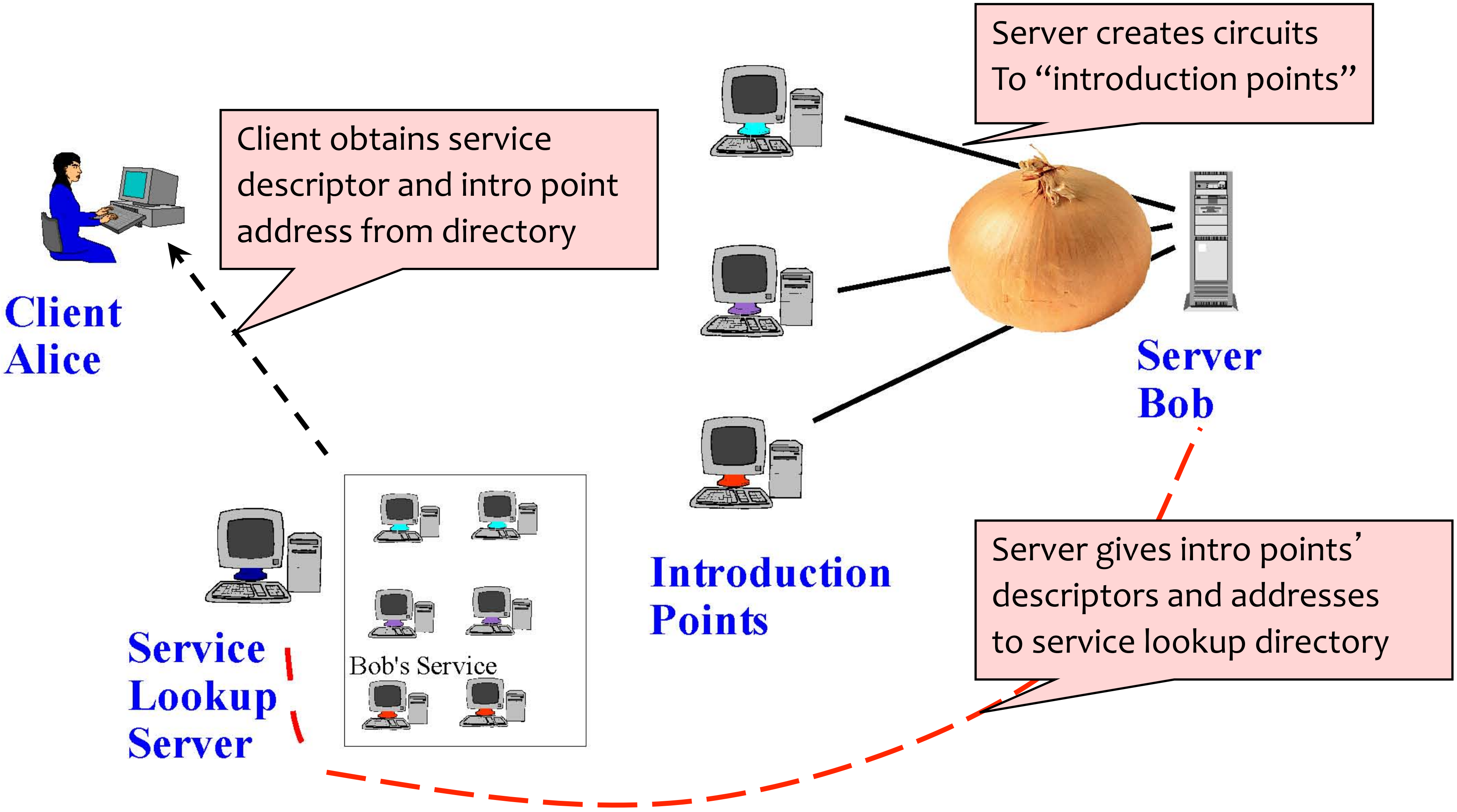
Tor Management Issues

- Many applications can share one circuit
  - Multiple TCP streams over one anonymous connection
- Tor router doesn’t need root privileges
  - Encourages people to set up their own routers
  - More participants = better anonymity for everyone
- Directory servers
  - Maintain lists of active onion routers, their locations, current public keys, etc.
  - Control how new routers join the network
    - “Sybil attack”: attacker creates a large number of routers
  - Directory servers’ keys ship with Tor code

Location Hidden Service

- **Goal:** deploy a server on the Internet that anyone can connect to without knowing where it is or who runs it
- Accessible from anywhere
- Resistant to censorship
- Can survive a full-blown DoS attack
- Resistant to physical attack
  - Can't find the physical server!

Creating a Location Hidden Server



Server creates circuits
To "introduction points"

Client obtains service
descriptor and intro point
address from directory

Server gives intro points'
descriptors and addresses
to service lookup directory

Client
Alice

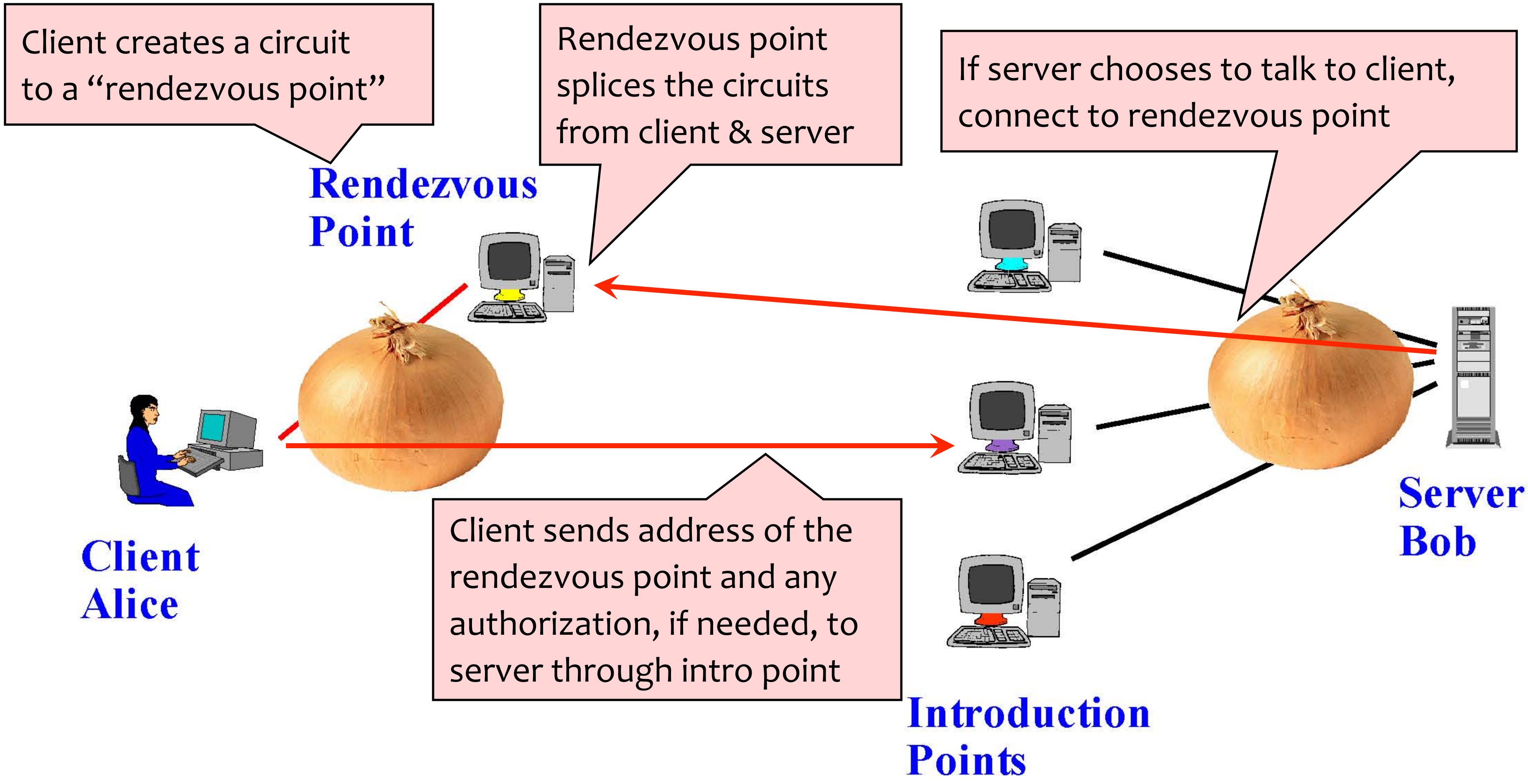
Server
Bob

Introduction
Points

Service
Lookup
Server

Bob's Service

Using a Location Hidden Server



Client creates a circuit to a "rendezvous point"

Rendezvous point splices the circuits from client & server

If server chooses to talk to client, connect to rendezvous point

Client sends address of the rendezvous point and any authorization, if needed, to server through intro point

Attacks on Anonymity

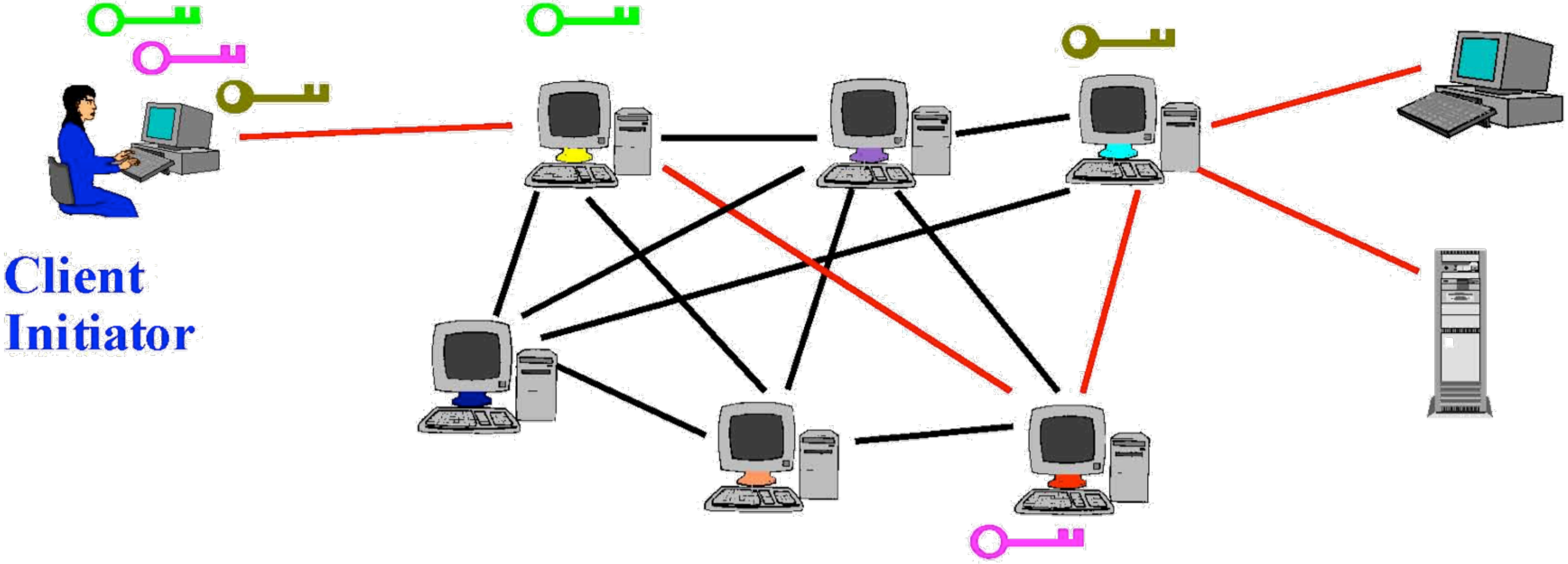
- Passive traffic analysis
  - Infer from network traffic who is talking to whom
  - To hide your traffic, must carry other people's traffic!
- Active traffic analysis
  - Inject packets or put a timing signature on packet flow
- Compromise of network nodes
  - Attacker may compromise some routers
  - It is not obvious which nodes have been compromised
    - Attacker may be passively logging traffic
  - Better not to trust any individual router
    - Assume that some fraction of routers is good, don't know which

Deployed Anonymity Systems

- Tor (http://tor.eff.org)
  - Overlay circuit-based anonymity network
  - Best for low-latency applications such as anonymous Web browsing
- Mixminion (http://www.mixminion.net)
  - Network of mixes
  - Best for high-latency applications such as anonymous email
- Not: YikYak ☺

Some Caution

- Tor isn't completely effective by itself
  - Tracking cookies, fingerprinting, etc.
  - Exit nodes can see everything!



Identifying Web Pages: Traffic Analysis

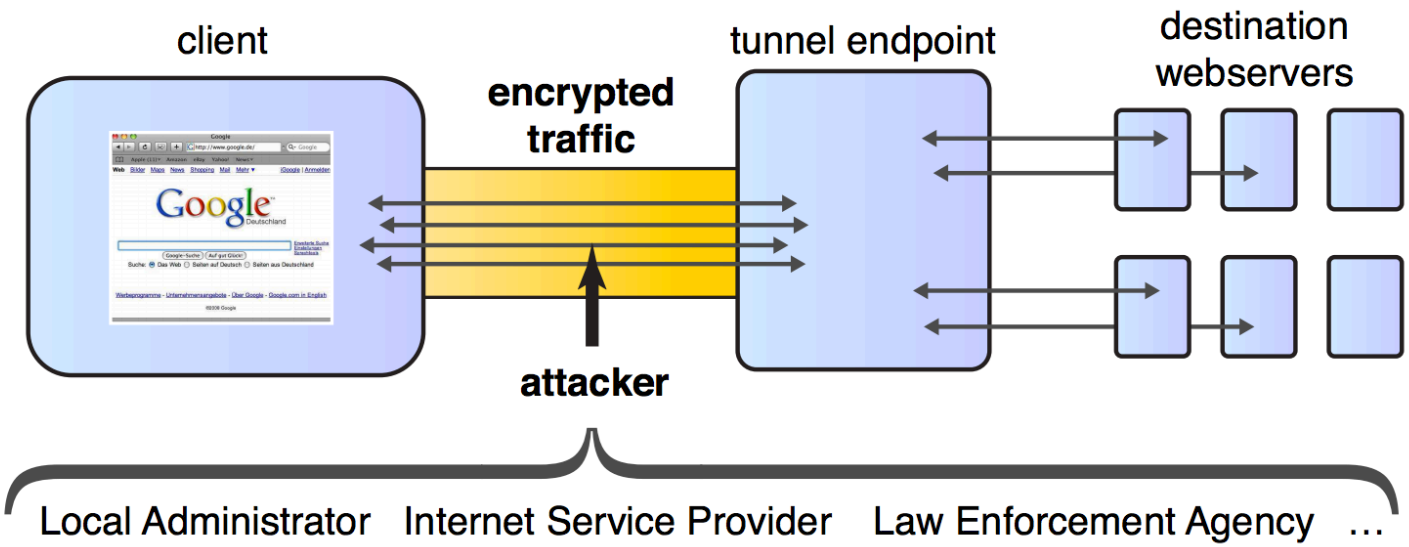


Figure 1: Website fingerprinting scenario and conceivable attackers

Herrmann et al. "Website Fingerprinting: Attacking Popular Privacy Enhancing Technologies with the Multinomial Naïve-Bayes Classifier" CCSW 2009

OTR AND SECURE MESSAGING

OTR – "Off The Record"

- Protocol for end-to-end encrypted instant messaging

- End-to-end: Only the endpoints can read messages.
  - PGP, iMessage, WhatsApp, and a variety of other services provide some form of end-to-end encryption today.

(Borisov, Goldberg, Brewer 2014)

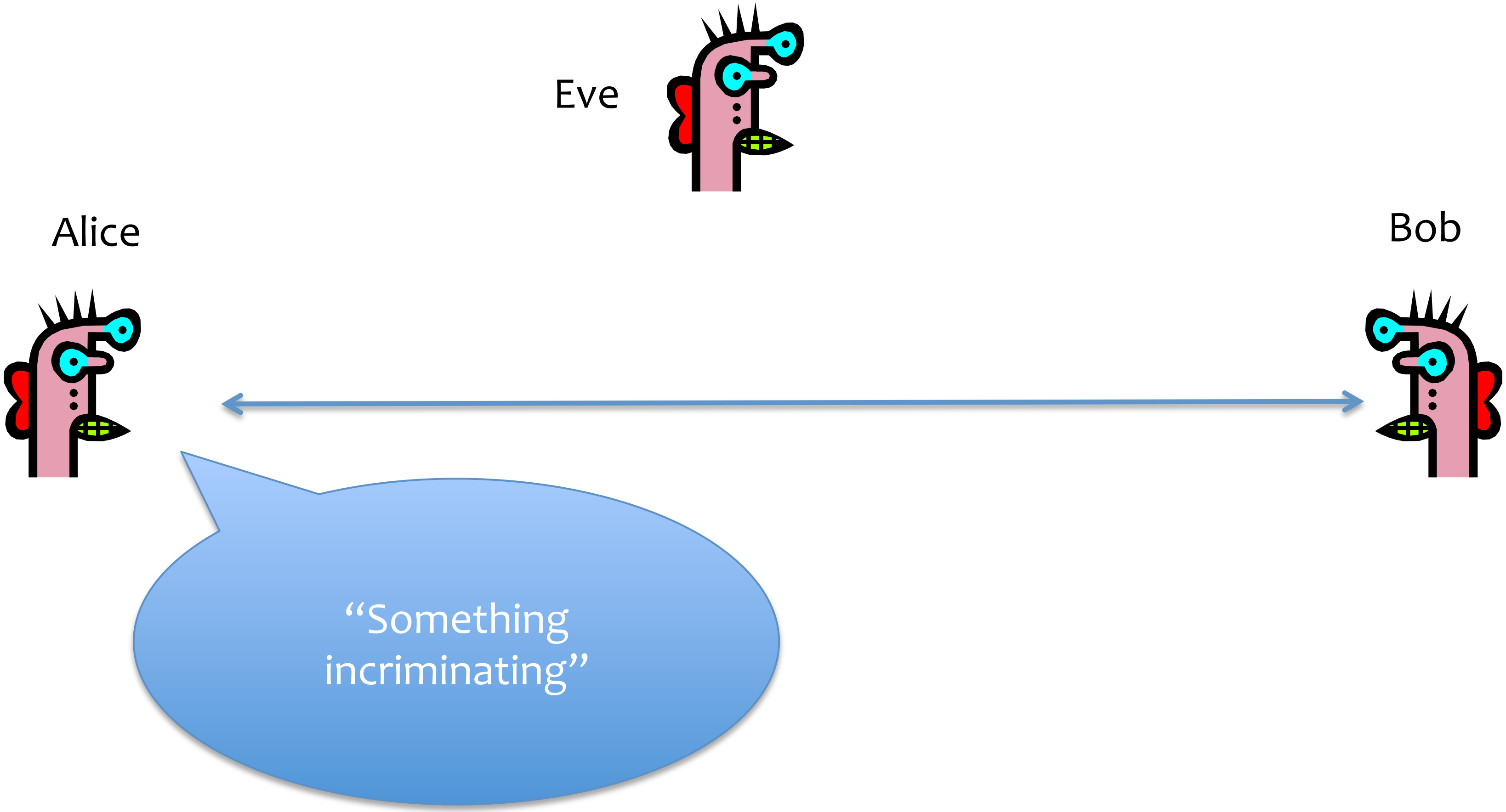
OTR – “Off The Record”

- **End-to-end encryption**
- **Authentication**
- Deniability, *after* the fact
- Perfect Forward Secrecy

OTR – "Off The Record"

- End-to-end encryption
- Authentication
- **Deniability/Repudability, *after* the fact**
- **Perfect Forward Secrecy**

OTR: Deniability/Repudability



Eve

Alice

Bob

“Something incriminating”

OTR: Deniability/Repudability

- During a conversation session, messages are authenticated and unmodified.

- Authentication happens using a MAC derived from a shared secret.

OTR: Deniability/Repudability

- During a conversation session, messages are authenticated and unmodified.
- Authentication happens using a MAC derived from a shared secret.
- Q1

OTR: Deniability/Repudability

- Can’t prove the other person sent the message, because you also could have computed the MAC!

OTR: Deniability/Repudability

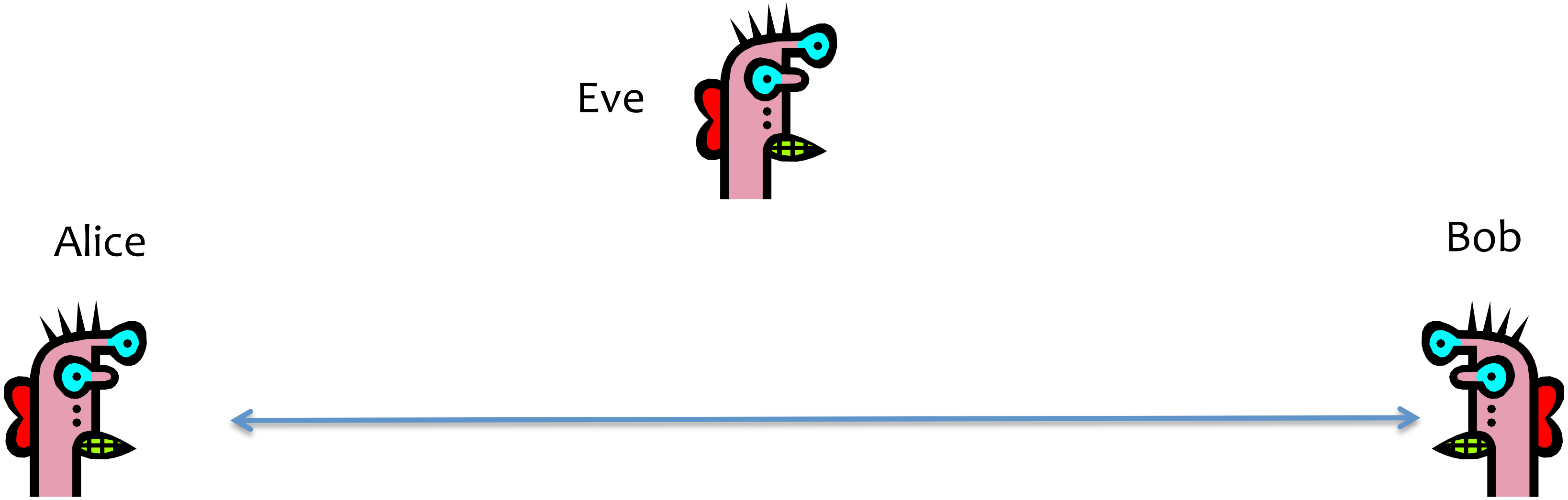
- Can't prove the other person sent the message, because you also could have computed the MAC!

- OTR takes this one step farther: After a messaging session is over, Alice and Bob send the MAC key publicly over the wire!

OTR: Deniability/Repudability

- Eve now knows the MAC key, so technically speaking, she also has the ability to forge messages from Alice or Bob.

Perfect Forward Secrecy

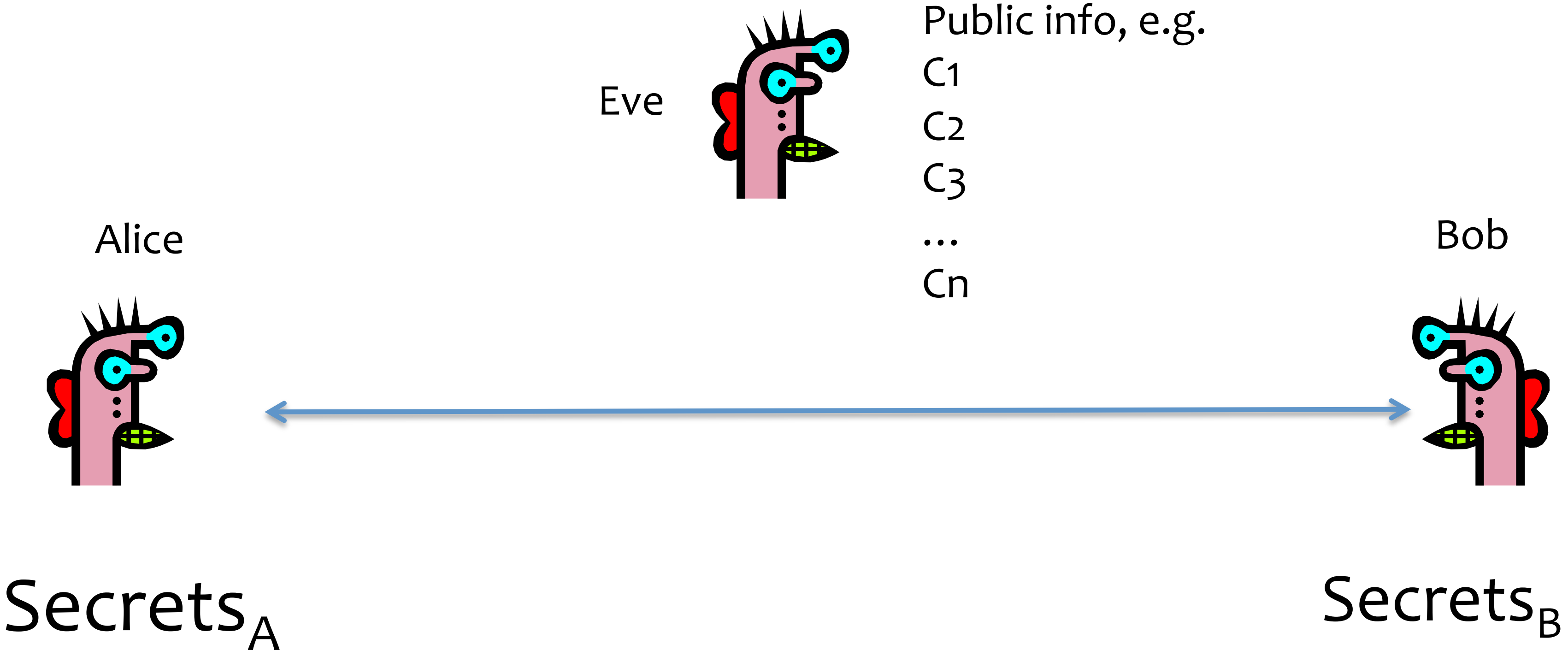


Eve

Alice

Bob

Perfect Forward Secrecy



Eve

Public info, e.g.
C1
C2
C3
…
Cn

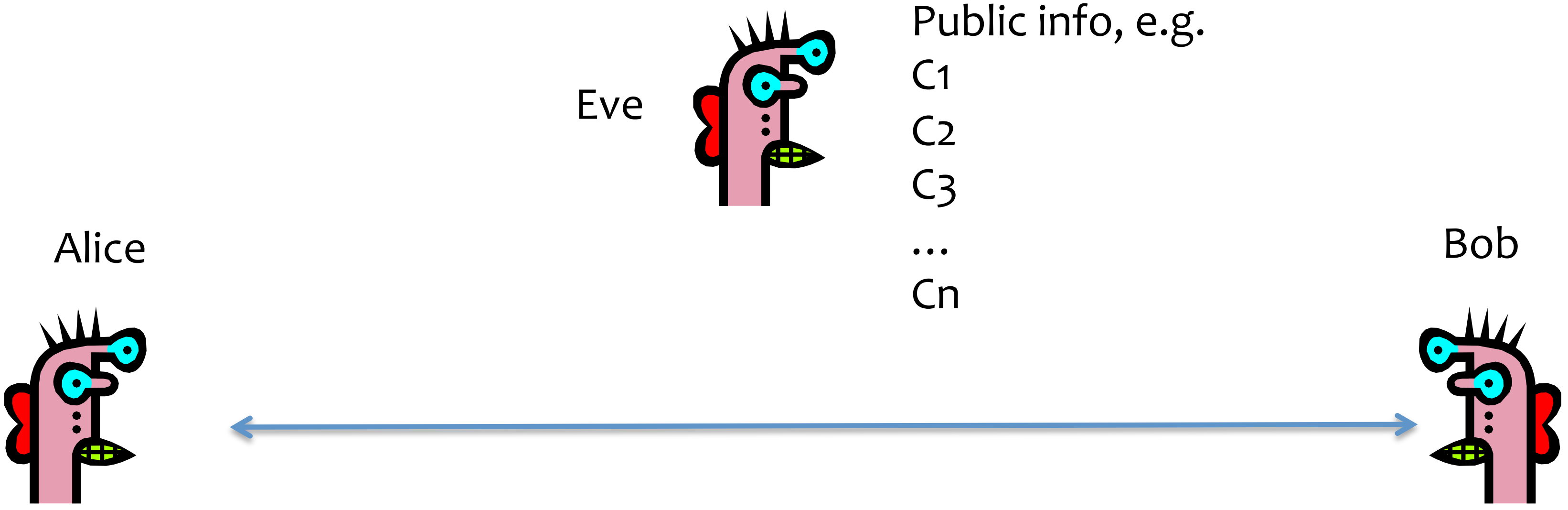
Alice

Bob

Secrets_A

Secrets_B

Perfect Forward Secrecy



Eve

Public info, e.g.
C1
C2
C3
…
Cn

Alice

Bob

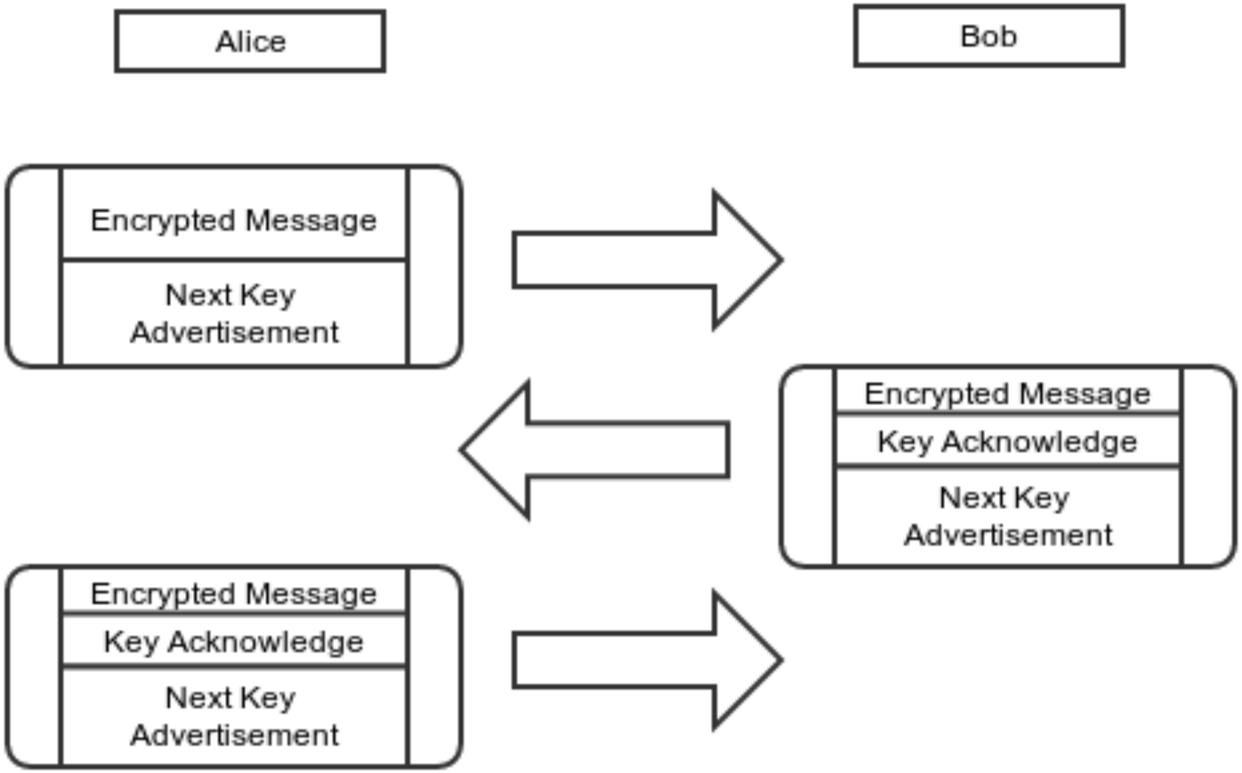
Secrets_A

If Eve compromises Alice or Bob's computers at a later date, we would like to prevent her from being able to learn what M1, M2, M3, etc. correspond to C1, C2, C3, etc.

Secrets_B

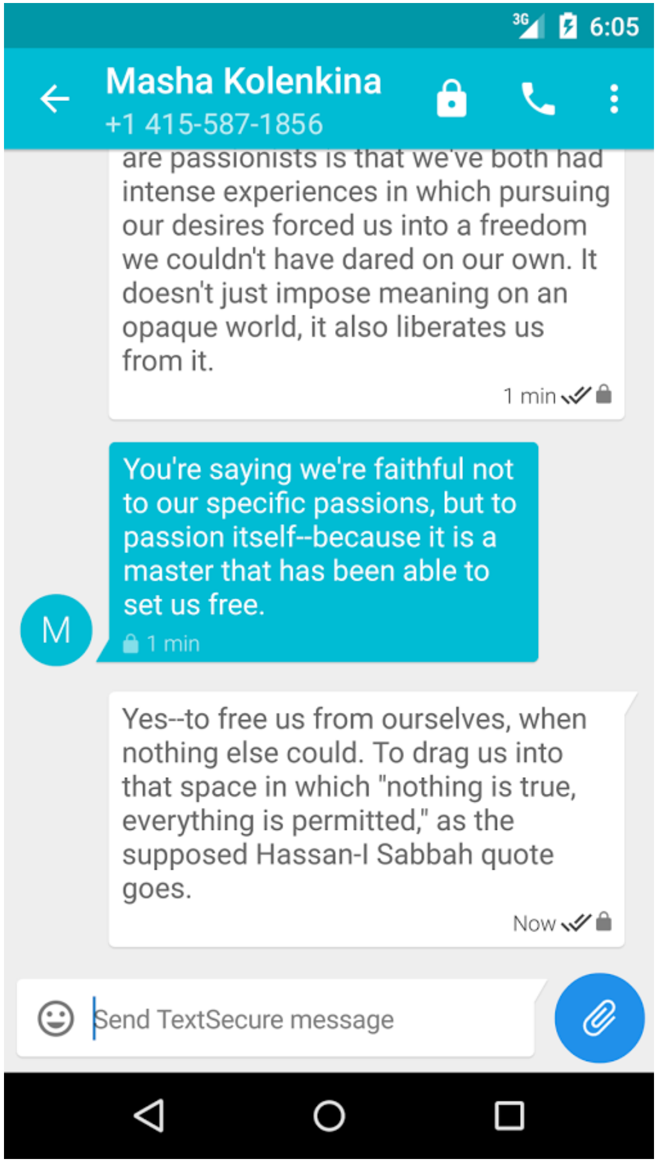
OTR: Ratcheting

- Idea: Use a new key for every session/ message/time period.



Signal

- End-to-end encrypted chat/IM based on OTR
- Provides variations on ratcheting, deniability, etc.
- Widely used, public code, audited.



Masha Kolenkina
+1 415-587-1856

are passionists is that we've both had intense experiences in which pursuing our desires forced us into a freedom we couldn't have dared on our own. It doesn't just impose meaning on an opaque world, it also liberates us from it.
1 min

M

You're saying we're faithful not to our specific passions, but to passion itself--because it is a master that has been able to set us free.
1 min

Yes--to free us from ourselves, when nothing else could. To drag us into that space in which "nothing is true, everything is permitted," as the supposed Hassan-I Sabbah quote goes.
Now

Send TextSecure message