Lecture 10: Authentication Protocols

CS 181S

Spring 2024

Aspects of Security

- **Authentication:** mechanisms that bind principals to actions

- **Authorization:** mechanisms that govern whether actions are permitted

- **Audit:** mechanisms that record and review actions

Aspects of Security

- **Authentication:** mechanisms that bind principals to actions

- **Authorization:** mechanisms that govern whether actions are permitted

- **Audit:** mechanisms that record and review actions

... Gold Standard [Lampson 2000]

Classes of Principals

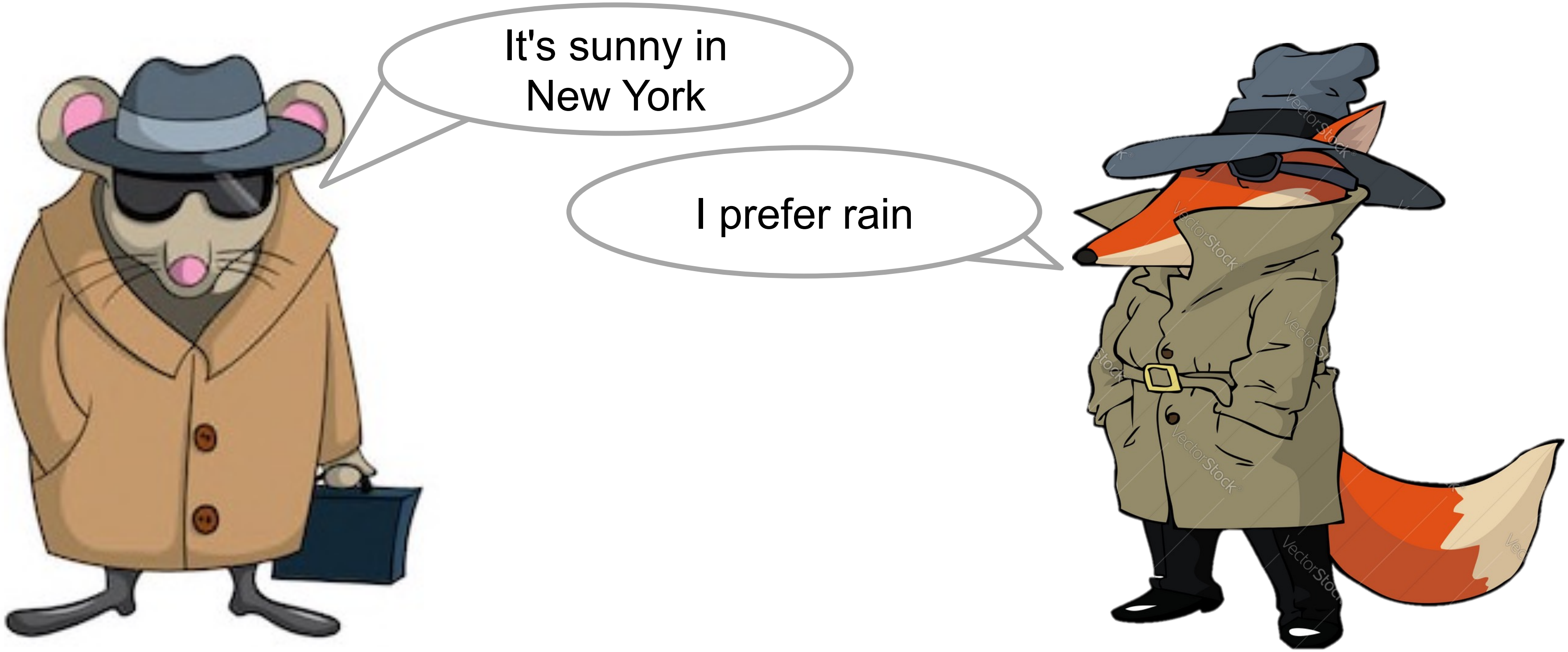
- **Authentication:** mechanisms that bind principals to actions
  - Authenticating Machines
  - Authenticating Programs
  - Authenticating Humans

Authentication

- **Threat:** attacker who controls the network
  - Dolev-Yao model: attacker can read, modify, delete messages
- **Vulnerability:** communication channel between sender and receiver can be controlled by other principals
- **Harm:** attacker can pretend to have attributes they don't actually have (violating security goals)
- **Countermeasure:** authentication protocols

Authentication Protocols

- An **authentication protocol** allows a principal receiving a message to verify the identity of the principal that sent that message



Assumptions

- Assume Alice and Bob have a shared secret key k
- Assume that symmetric-key crypto works

Protocol 1

1. B -> A: B
2. A -> B: A, k

Defining Authentication

- A **strong authentication protocol** demonstrates knowledge of the secret without revealing the secret itself

Protocol 2

1. B -> A: B
2. A -> B: A, H(k)

Threat Model

- Dolev-Yao attacker
  - controls the network, can read, modify, create packets

- A **replay attack** occurs when an adversary repeats (fragments of) a previous protocol run

1. `B -> A: B`
2. `A -> B: A, H(k)`
   1) `B -> T: B`
   2) `T -> B: A, H(k)`

Exercise: Replay Attacks

- Consider the following authentication protocol. Either demonstrate a replay attack against it or make an informal argument as to why it is secure against replay attacks.

1. B -> A: B
2. A -> B: A, Enc(A^B; k)

Protocol 3

Idea: require Alice to authenticate with a different message every time

1. `B -> A: B, r`
2. `A -> B: A, Enc(r;k)`

Threat Model

- Dolev-Yao attacker
  - controls the network, can read, modify, create packets

- A **reflection attack** occurs when an adversary sends messages from an ongoing protocol back to the originator

```
1. B -> T: B, r
   1)  T -> B: A, r
   2)  B -> T: B, Enc(r;k)
2. T -> B: A, Enc(r;k)
```

Exercise: Reflection Attacks

- Consider the following authentication protocol. Is this protocol vulnerable to a reflection attack? In each case, exhibit an attack or explain why it is not possible

1. B -> A: B, r
2. A -> B: A, Enc(A*B+r; k)

Exercise: Reflection Attacks

Replay Attacks

Reflection Attacks

Protocol 4: Multiple Keys

- Idea: have two different keys k_AB and k_BA for authenticating in the different directions

```
1. B -> A: B, r
2. A -> B: A, Enc(r;k_AB)
```

Protocol 5: Included Identity

- Idea: include the identity of the sender in the encrypted ciphertext

1. `B -> A: B, r`
2. `A -> B: A, Enc(A, r; k)`

Foiling Reflection Attacks

Multiple Keys

```
1. B->T: B, r
   1)  T->B: A, r
   2)  B->T: B, Enc(r;k_BA)
2.  T->B: A, Enc(r;k_BA)
```

☒

Included Identity

```
1. B->T: B, r
   1)  T->B: A, r
   2)  B->T: B, Enc(B, r; k)
2.  T->B: A, Enc(B, r; k)
```

☒

Exercise: Authentication Protocols

- Consider the following authentication protocols. For each: Is it vulnerable to a replay attack? Is this protocol vulnerable to a reflection attack? In each case, exhibit an attack or explain why it is not possible
- Protocol 1:
  1. B -> A: B, r
  2. A -> B: A, Enc($A \oplus B$; k)
- Protocol 2:
  1. B -> A: B, r
  2. A -> B: A, Enc($A \oplus B$ + r; k)
- Protocol 3:
  1. B -> A: B, r
  2. A -> B: A, Enc(A^B + r; k)

Threat Model

- Dolev-Yao attacker
  - controls the network, can read, modify, create packets

- A **man-in-the-middle attack** occurs when an adversary secretly relays (and potentially changes) communications between two principals who believe they are communicating directly with eachother

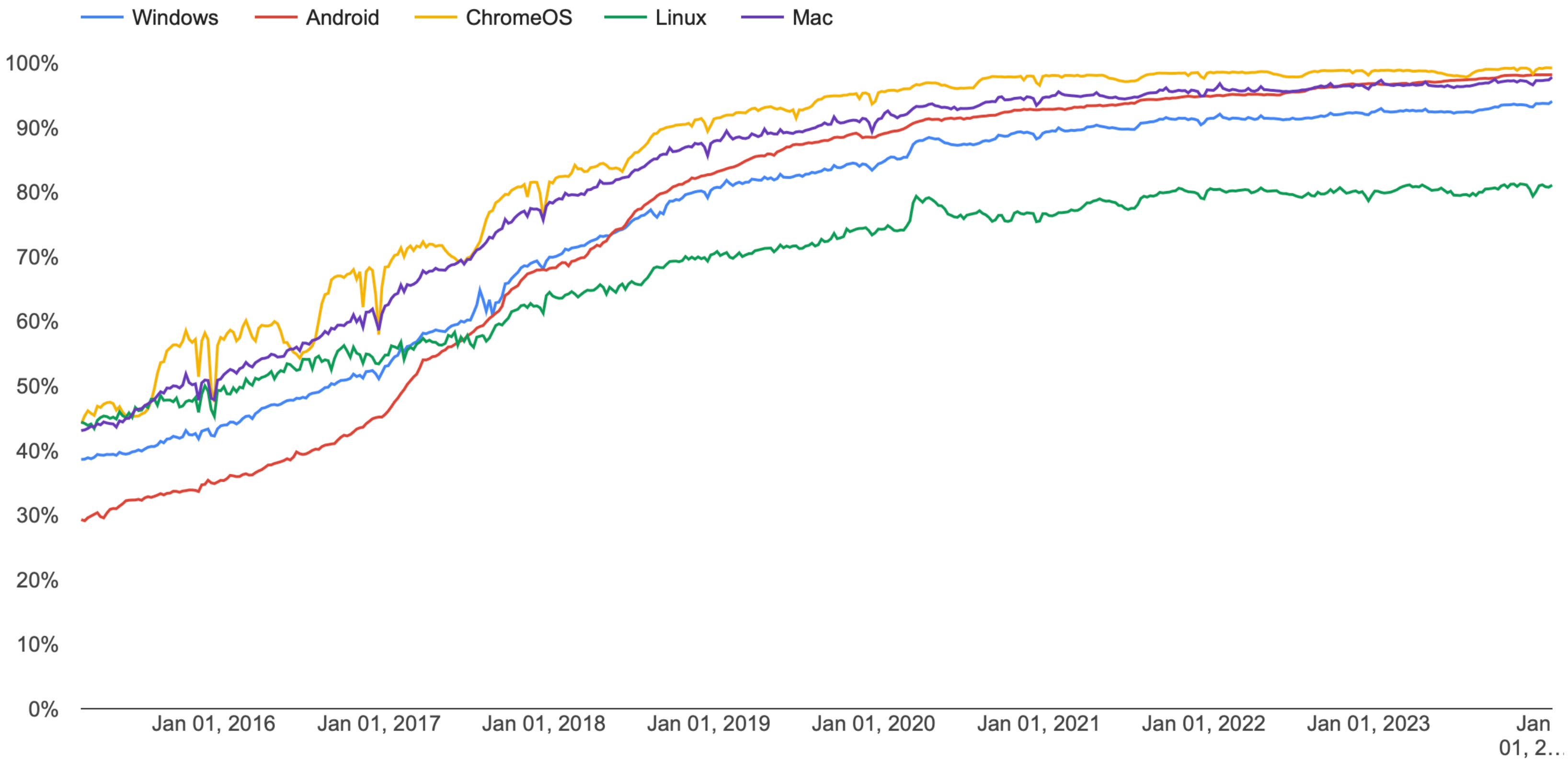
1. B -> T: B, r
   1) T -> A: B, r
   2) A -> T: A, Enc(A, r; k)
2. T -> B: A, Enc(A, r;k)

Authentication

- **Threat:** attacker who controls the network
  - Dolev-Yao model: attacker can read, modify, delete messages
- **Vulnerability:** communication channel between sender and receiver can be controlled by other principals
- **Harm:** attacker can pretend to have attributes they don't actually have (violating security goals)
- **Countermeasure:** authentication protocols

Solution: Encrypt Everything

Percentage of pages loaded over HTTPS in Chrome by platform


Windows
Android
ChromeOS
Linux
Mac
Jan 01, 2016
Jan 01, 2017
Jan 01, 2018
Jan 01, 2019
Jan 01, 2020
Jan 01, 2021
Jan 01, 2022
Jan 01, 2023
Jan 01, 2…