Challenge-Response Authentication

Prof. Ravi Sandhu
Executive Director and Endowed Chair
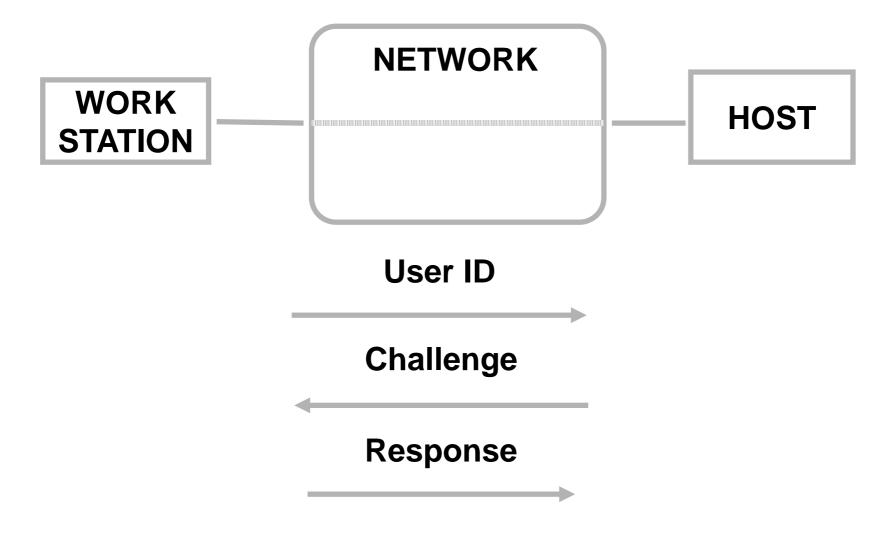
Lecture 5

ravi.utsa@gmail.com
www.profsandhu.com

World-Leading Research with Real-World Impact!
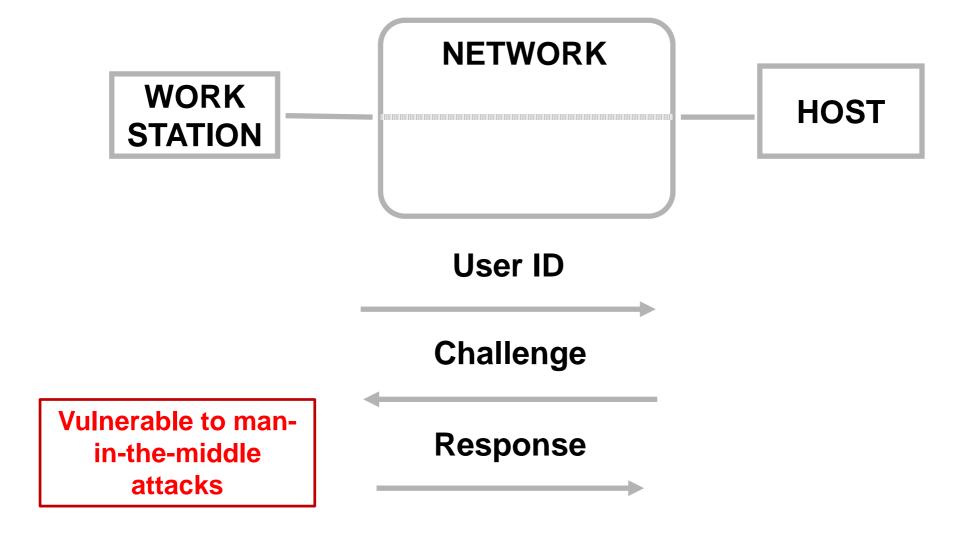
WORK STATION

NETWORK

HOST

User ID

Challenge

Response

World-Leading Research with Real-World Impact!

NETWORK

WORK STATION

HOST

User ID

Challenge

Response

Vulnerable to man-in-the-middle attacks

NETWORK

WORK STATION

HOST

User ID

→

Challenge = Time

←

Response

→ **One Time Password**

World-Leading Research with Real-World Impact!

Symmetric Key

Encrypt

Challenge

Response

Symmetric Key

Time

Encrypt

Response

Implicit challenge = Time

One-Time Password

Symmetric Key

MAC

Challenge

Response

World-Leading Research with Real-World Impact!