Challenge-Response Authentication

Prof. Ravi Sandhu
Executive Director and Endowed Chair

Lecture 5

ravi.utsa@gmail.com
www.profsandhu.com
Challenge-Response Authentication

WORK STATION $\rightarrow$ NETWORK $\rightarrow$ HOST

User ID

Challenge

Response

Vulnerable to man-in-the-middle attacks
Time Synchronized

WORK STATION \[\rightarrow\] NETWORK \[\rightarrow\] HOST

User ID

Challenge = Time

Response \[\rightarrow\] One Time Password
Symmetric Key Based

Symmetric Key

Encrypt

Challenge

Response
Time Synchronized

Symmetric Key

Encrypt

Time

Implicit challenge = Time

Response

One-Time Password
Symmetric Key Based

Symmetric Key

MAC

Challenge

Response
Asymmetric Key Based

Private Key

Sign

Challenge

Response