

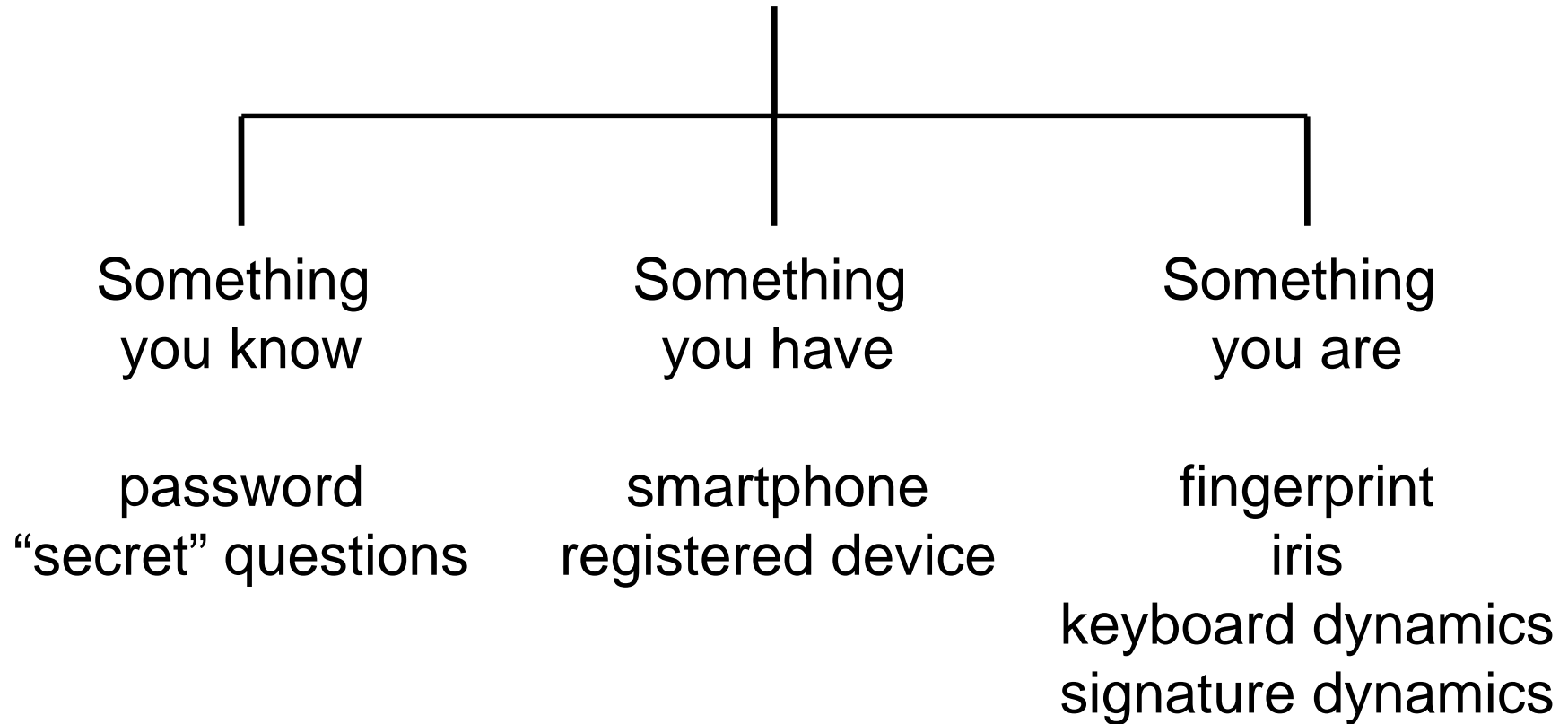
# Authentication by Passwords

Prof. Ravi Sandhu  
Executive Director and Endowed Chair

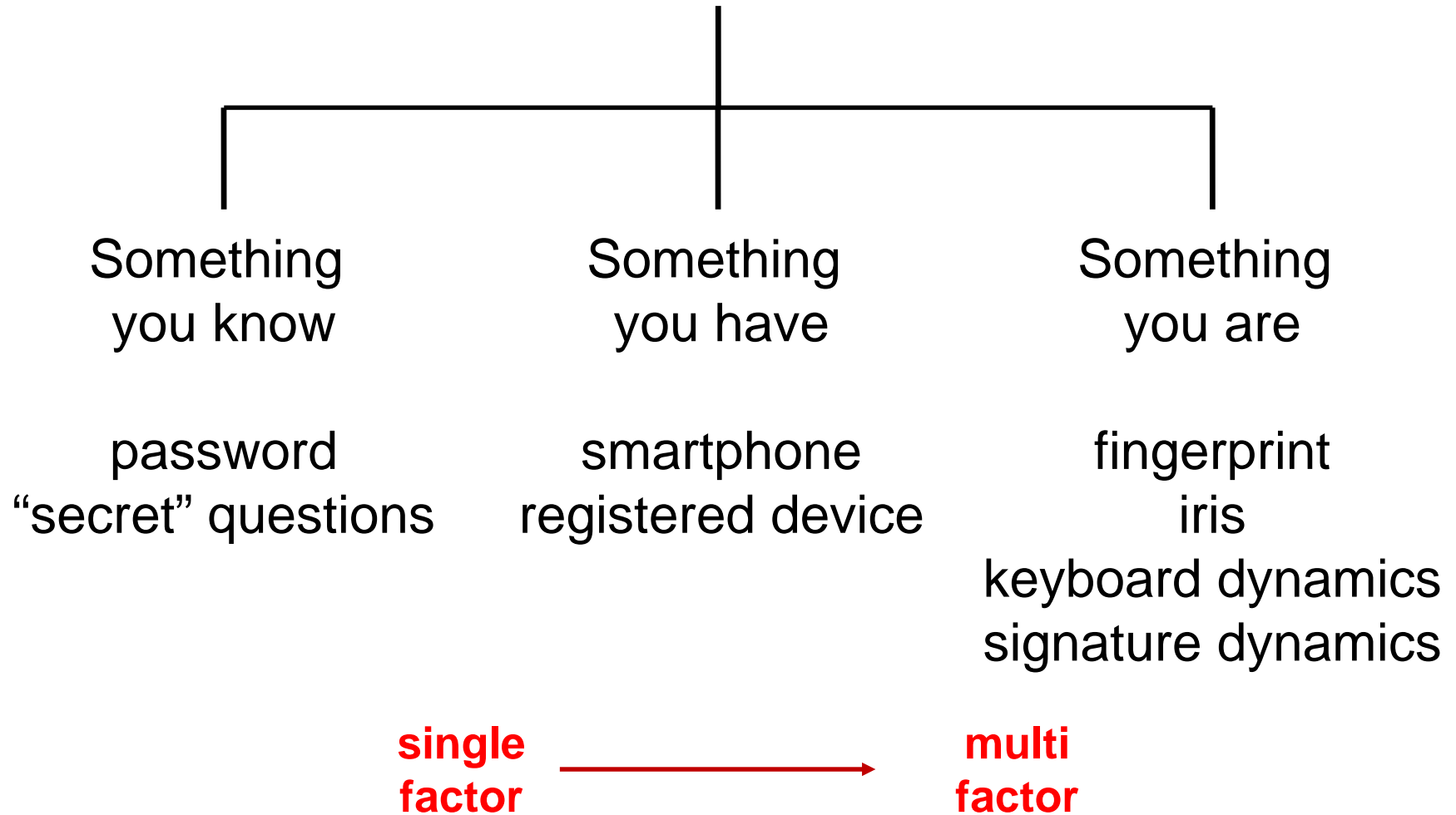
Lecture 16

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

## Authentication

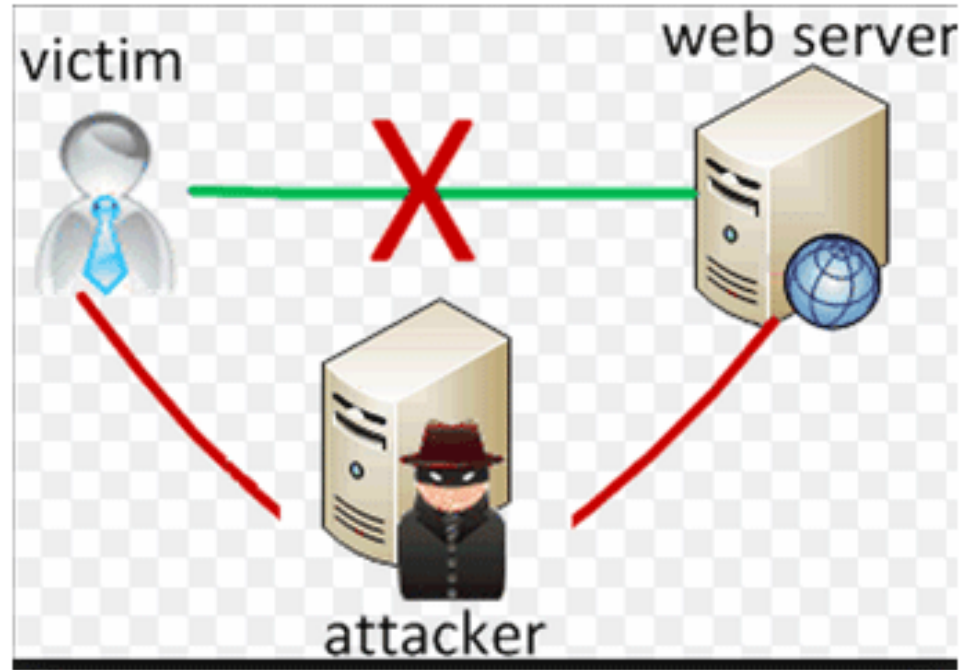


## Authentication

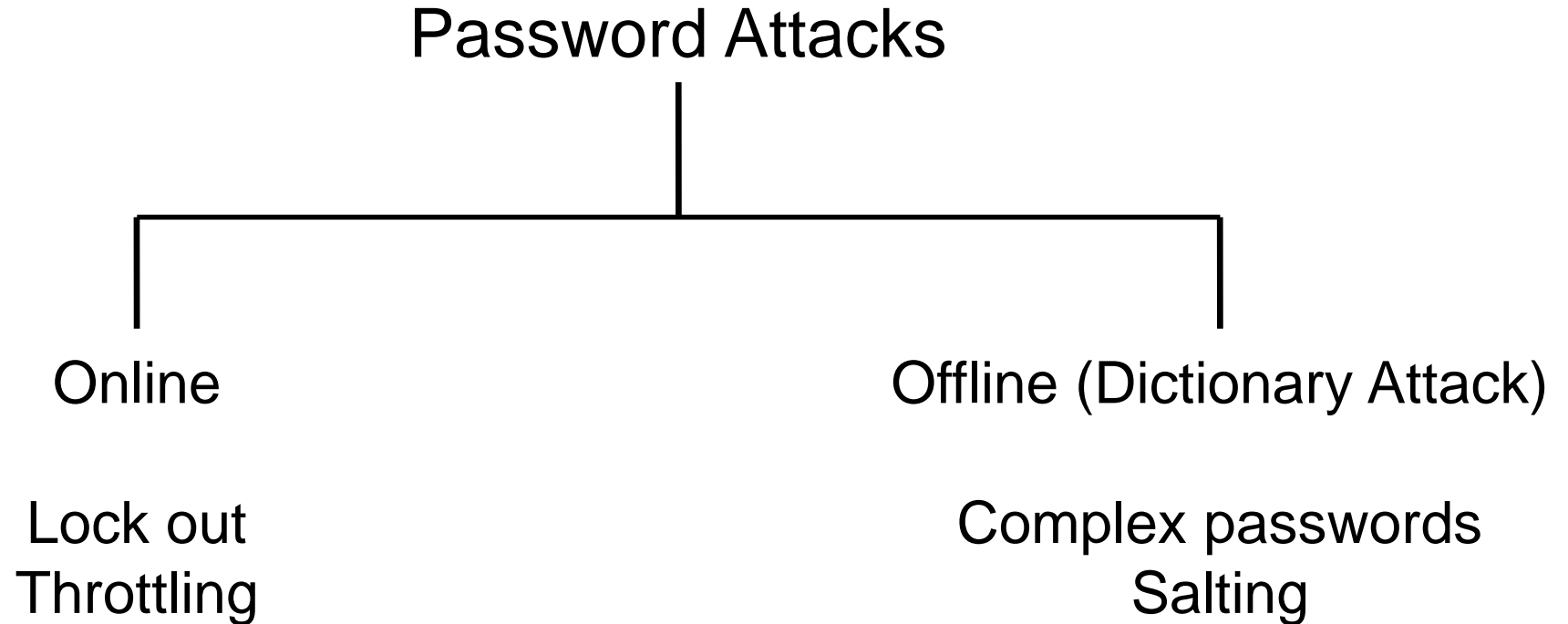




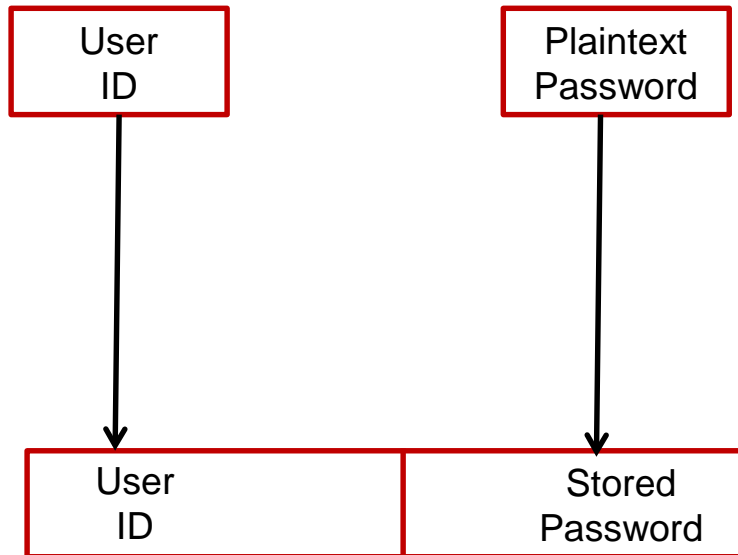
Personalized image to authenticate webserver to user



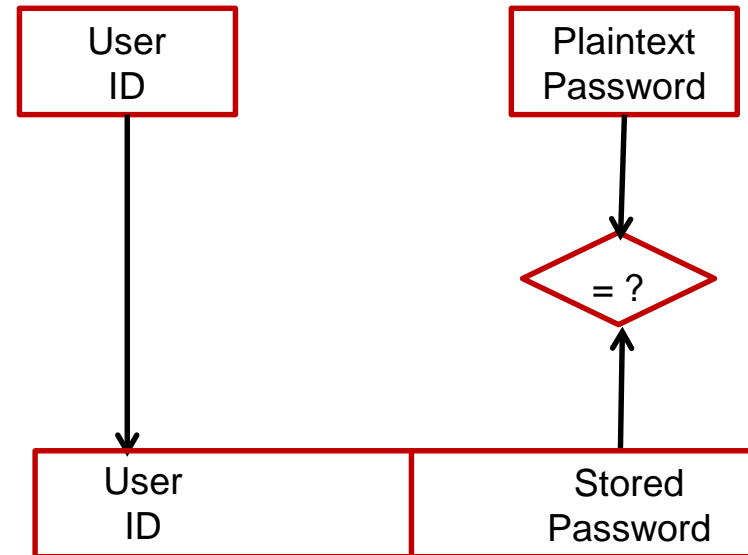
Personalized image passed through



## Password Storage

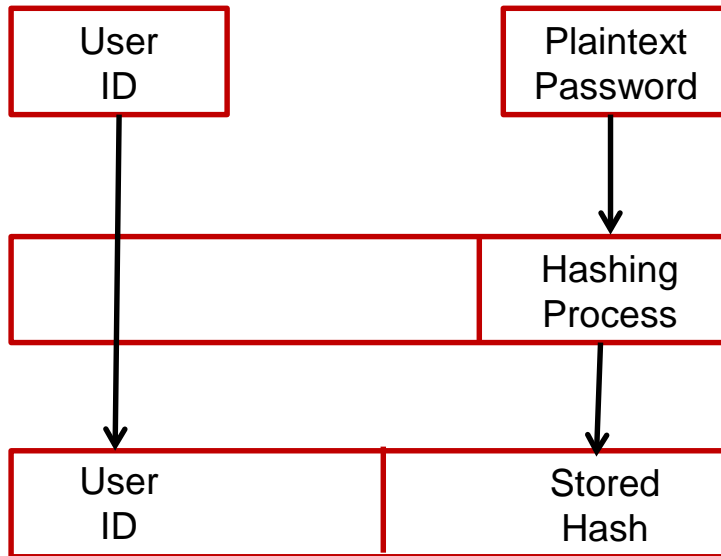


## Password Verification



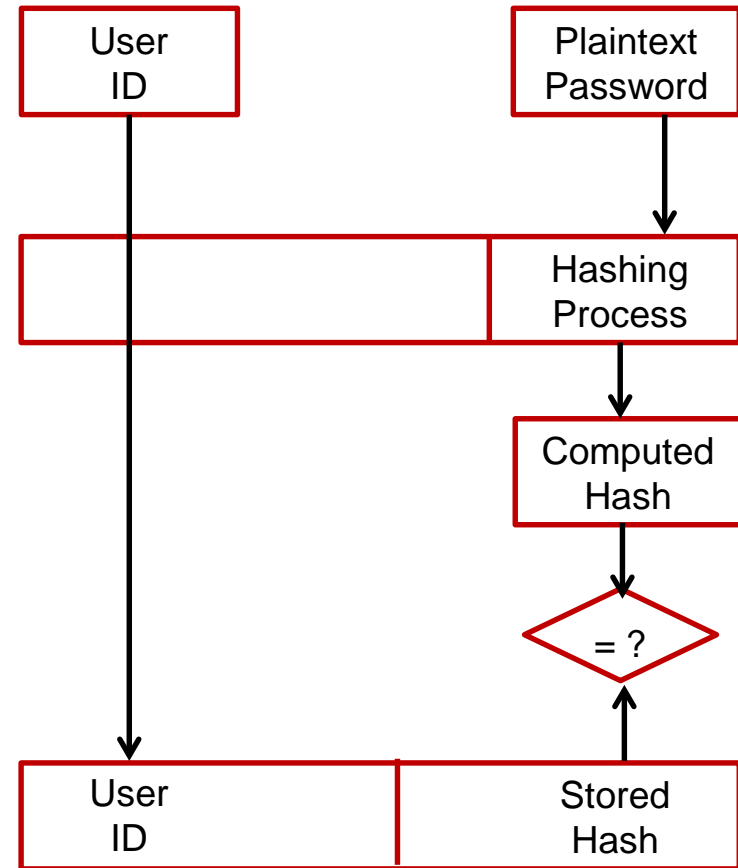
Loss of stored passwords =  
Catastrophic failure

## Password Storage



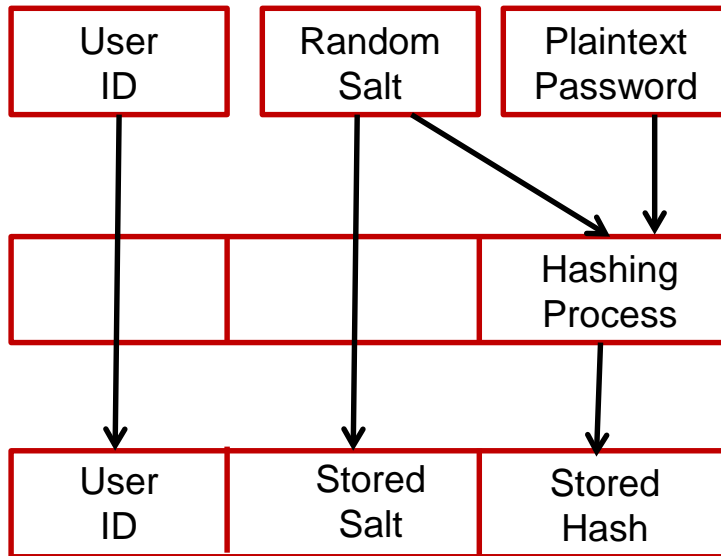
Loss of stored hashes =  
Attack by single dictionary

## Password Verification





## Password Storage



Loss of stored hashes =  
Attack by different dictionary  
for each salt value

## Password Verification

