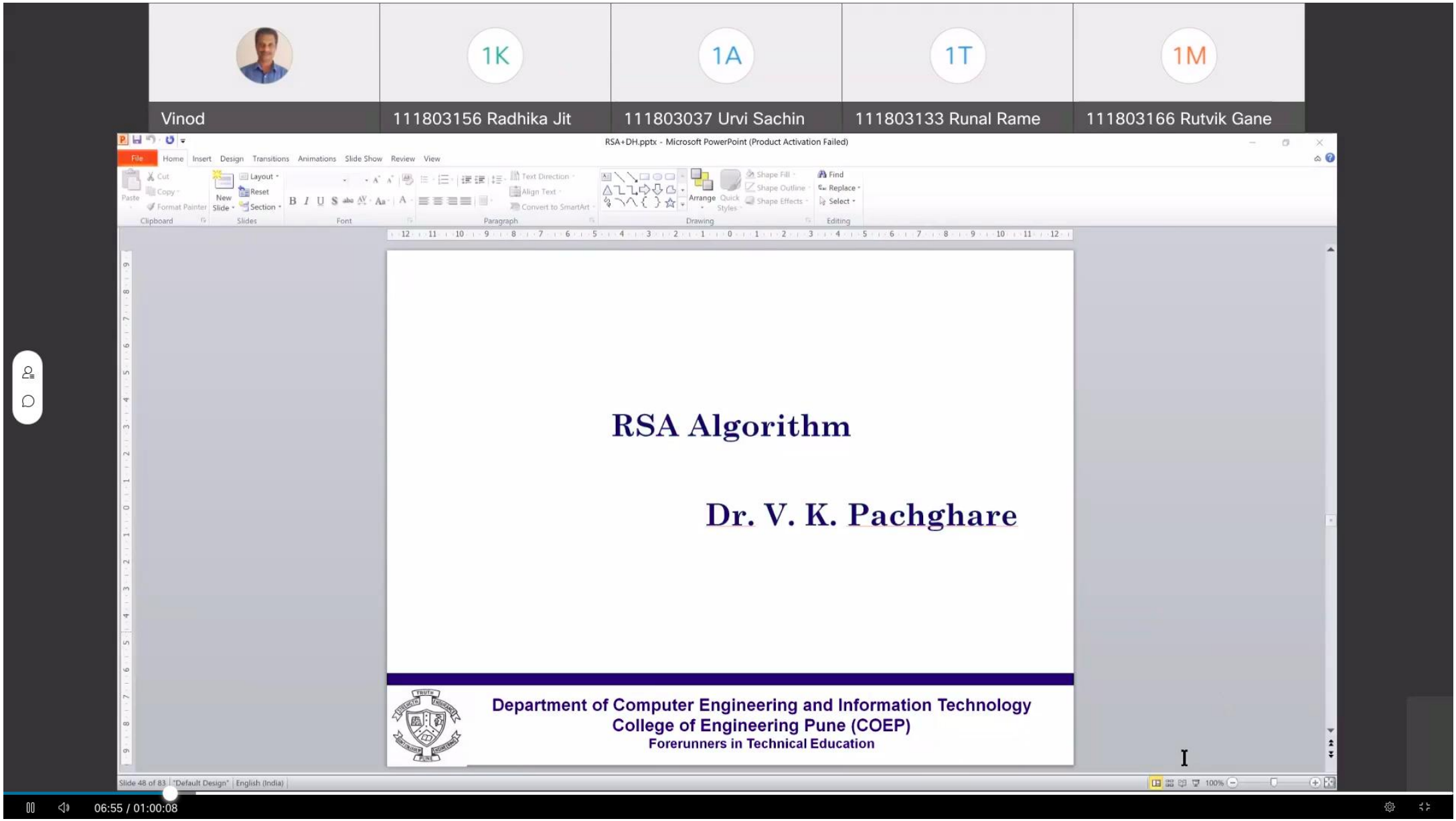

Vinod
1K
111803156 Radhika Jit
1A
111803037 Urvi Sachin
1T
111803133 Runal Rame
1M
111803166 Rutvik Gane
RSA+DH.pptx - Microsoft PowerPoint (Product Activation Failed)
RSA Algorithm
Dr. V. K. Pachghare
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
06:55 / 01:00:08

1N

Press Esc to exit full screen

1T

1M

Vinod | 111811052 Anup Sures | 111803037 Urvi Sachin | 111803133 Runal Rame | 111803166 Rutvik Gane

RSA+DH.pptx - Microsoft PowerPoint (Product Activation Failed)

File Home Insert Design Transitions Animations Slide Show Review View

Cut Copy Format Painter Paste Clipboard

New Slide Layout Reset Section Slides

Font Paragraph Drawing Editing

Text Direction Align Text Convert to SmartArt

Arrange Quick Styles Shape Fill Shape Outline Shape Effects

Find Replace Select

RSA Public Key Cryptosystem
Key Generation Algorithm

Step 1: Choose two random large prime numbers p and q
For maximum security, choose p and q are of about equal length, e.g. 512-1024 bits each.

Step 2: Compute the product n = p·q

Step 3: Choose a random integer e < m [Where $m = \Phi(n) = (p-1)(q-1)$]
The numbers e and (p-1)(q-1) must be relatively prime, i.e. they should not share common prime factors. GCD(e, m) = 1

Step 4: Compute the unique inverse $d = e^{-1} \bmod m$
The equation $d \cdot e \bmod m = 1$
can be solved using the Euclidian algorithm

Step 5: $C = P^e \bmod n$

Step 6: $P = C^d \bmod n$

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Slide 49 of 83 | "Default Design" | English (India)

100%

+48

Encryption

p = 3, q = 11

n = p ·q = 33

m = Totient function Φ(n) = (p-1) ·(q-1)

= 2 · 10 = 20

The public exponent 'e' must be relatively prime to 20,

i.e. e = 3, 7, 9, 11, 13, 17, 19

here we select e =3

Plaintext x: 9

$y = x^3 \bmod 33$

Ciphertext: 3

1N	1A	1T	1M
Vinod	111811052 Anup Sures	111803037 Urvi Sachin	111803133 Runal Rame	111803166 Rutvik Gane

RSA+DH.pptx - Microsoft PowerPoint (Product Activation Failed)

File Home Insert Design Transitions Animations Slide Show Review View

Decryption

$d = e^{-1} \bmod m$

$d = 3^{-1} \bmod 20$

$d \cdot e \bmod 20 = 1$

So, for e = 3, d = 7

Ciphertext y: 3

$x = y^7 \bmod 33$

Plaintext: 9

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Slide 52 of 83 "Default Design" English (India)

+65

1N

Press Esc to exit full screen

1D

1M

Vinod | 111811052 Anup Sures | 111803037 Urvi Sachin | 111803110 Amey Maka | 111803166 Rutvik Gane

RSA+DH.pptx - Microsoft PowerPoint (Product Activation Failed)

File Home Insert Design Transitions Animations Slide Show Review View

Clipboard Slides Font Paragraph Drawing Editing

Click to add title

p = 7, q = 19, M= 6

Find out the minimum value for e and corresponding value for d.

Encrypt the message M = 6 using above e.

Also decrypt using above d to get M= 6

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Slide 54 of 83 | "Default Design" | English (India)

+66

1N	1A	1D	1M
Vinod	111811052 Anup Sures	111803037 Urvi Sachin	111803110 Amey Maka	111803166 Rutvik Gane

RSA+DH.pptx - Microsoft PowerPoint (Product Activation Failed)

File Home Insert Design Transitions Animations Slide Show Review View

Paste Cut Copy Format Painter | New Slide Layout Reset Section | Clipboard Slides Font Paragraph Drawing Editing

Click to add title

p = 7, q = 19, M= 6

Find out the minimum value for e and corresponding value for d.

Encrypt the message M = 6 using above e.

Also decrypt using above d to get M= 6

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Slide 54 of 83 | "Default Design" | English (India) | 100%

34:07 / 01:00:08

1N	1A	1D	1M
Vinod	111811052 Anup Sures	111803037 Urvi Sachin	111803110 Amey Maka	111803166 Rutvik Gane

RSA+DH.pptx - Microsoft PowerPoint (Product Activation Failed)

File Home Insert Design Transitions Animations Slide Show Review View

Click to add title

We compute 'd' using Euclids algorithm

We get d = 65 for e = 5

Public Key: (5, 133)

Private Key: (65, 133)

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Slide 57 of 83 | "Default Design" | English (India)

35:08 / 01:00:08

1N	1A	1D	1M
Vinod	111811052 Anup Sures	111803037 Urvi Sachin	111803110 Amey Maka	111803166 Rutvik Gane

RSA+DH.pptx - Microsoft PowerPoint (Product Activation Failed)

File Home Insert Design Transitions Animations Slide Show Review View

Clipboard Slides Font Paragraph Drawing Editing

Click to add title

Use RSA algorithm to encrypt the message M = 123. The parameters given are: p = 61, q = 53, e = 17. Also find out the value of d and decrypt the message to get M = 123.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Slide 61 of 83 "Custom Design" English (India)

36:39 / 01:00:08

1N	1A	1D	1M
Vinod	111811052 Anup Sures	111803037 Urvi Sachin	111803110 Amey Maka	111803166 Rutvik Gane

RSA+DH.pptx - Microsoft PowerPoint (Product Activation Failed)

File Home Insert Design Transitions Animations Slide Show Review View

$\mathbf{3120 = 17(183) + 9}$	$9 = 3120 - 17\,(183)$
$\mathbf{17 = 9\,(1) + 8}$	$8 = 17 - 9(1)$
$\mathbf{9 = 8\,(1) + 1}$	$1 = 9 - 8(1)$
$\mathbf{8 = 1(8)}$	

$$
\begin{aligned}
1 &= 9 - 8(1) \\
&= 9 - [17 - 9(1)](1) \\
&= 9(2) - 17 \\
&= [3120 - 17\,(183)](2) - 17 \\
&= 3120\,(2) - 17(367) \\
&= 3120\,(2) + 17\,(-367)
\end{aligned}
$$

so the inverse of 17 mod 3120 = -367 = 2753

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Slide 63 of 83 | "Custom Design" | English (India)

Speed 1x

javascript:void(0);

5:48 / 01:00:08

1N	1A	1D	1M
Vinod	111811052 Anup Sures	111803037 Urvi Sachin	111803110 Amey Maka	111803166 Rutvik Gane

RSA+DH.pptx - Microsoft PowerPoint (Product Activation Failed)

File Home Insert Design Transitions Animations Slide Show Review View

Paste Cut Copy Format Painter | New Slide Layout Reset Section | Clipboard Slides Font Paragraph Drawing Editing

Click to add title

Use RSA algorithm to encrypt the message M = 123. The parameters given are: p = 61, q = 53, e = 17. Also find out the value of d and decrypt the message to get M = 123.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Slide 61 of 83 | "Custom Design" | English (India)

+66

1N	1A	1D	1M
Vinod	111811052 Anup Sures	111803037 Urvi Sachin	111803110 Amey Maka	111803166 Rutvik Gane

RSA+DH.pptx - Microsoft PowerPoint (Product Activation Failed)

File Home Insert Design Transitions Animations Slide Show Review View

Paste Cut Copy Format Painter | New Slide Layout Reset Section | Clipboard Slides Font Paragraph Drawing Editing

Decryption:

Ciphertext = 855 and the private key is (2753, 3233)

The decryption function is:

$$\text{decrypt}(c) = c^d \bmod n = c^{2753} \bmod 3233$$

where c is the ciphertext.

To decrypt the ciphertext value 855, we calculate

$$\text{decrypt}(855) = 855^{2753} \bmod 3233 = 123$$

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Slide 64 of 83 | "Custom Design" | English (India) | 100%

+66

1N	1A	1D	1M
Vinod	111811052 Anup Sures	111803037 Urvi Sachin	111803110 Amey Maka	111803166 Rutvik Gane

RSA+DH.pptx - Microsoft PowerPoint (Product Activation Failed)

Example - 4

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Slide 66 of 83 | "Custom Design" | English (India)

+66

1N	1A	1D	1M
Vinod	111811052 Anup Sures	111803037 Urvi Sachin	111803110 Amey Maka	111803166 Rutvik Gane

RSA+DH.pptx - Microsoft PowerPoint (Product Activation Failed)

File Home Insert Design Transitions Animations Slide Show Review View

$1 = 7 - 3(2)$

$1 = 7 - 3(9-7) = 4(7) - 3(9)$

$1 = 4(214-9(23))-3(9) = 4(214) - 95(9)$

$1 = 4(214) - 95(223 - 214) = 99(214) - 95(223)$

$1 = 99(660 - 2(223))-95(223)$

$1 = 99(660)-293(223)$

so the inverse of 223 mod 660 = -293 = 367

Therefore

Private Key = (367, 713)

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Slide 70 of 83 | "Custom Design" | English (India)

+66

RSA+DH.pptx - Microsoft PowerPoint (Product Activation Failed)

Decryption

The ciphertext is 284

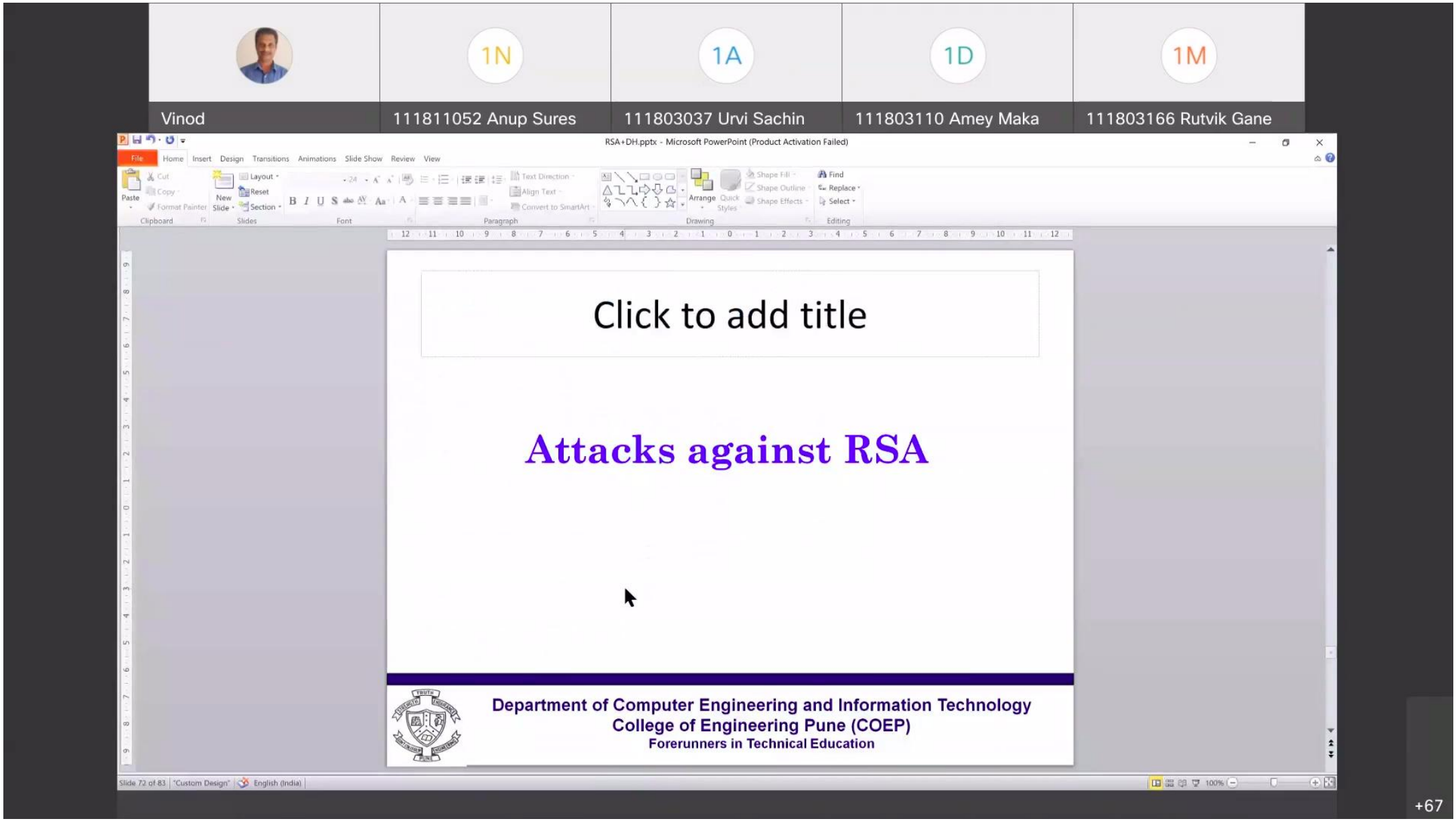
Plaintext $P = C^d \bmod n$

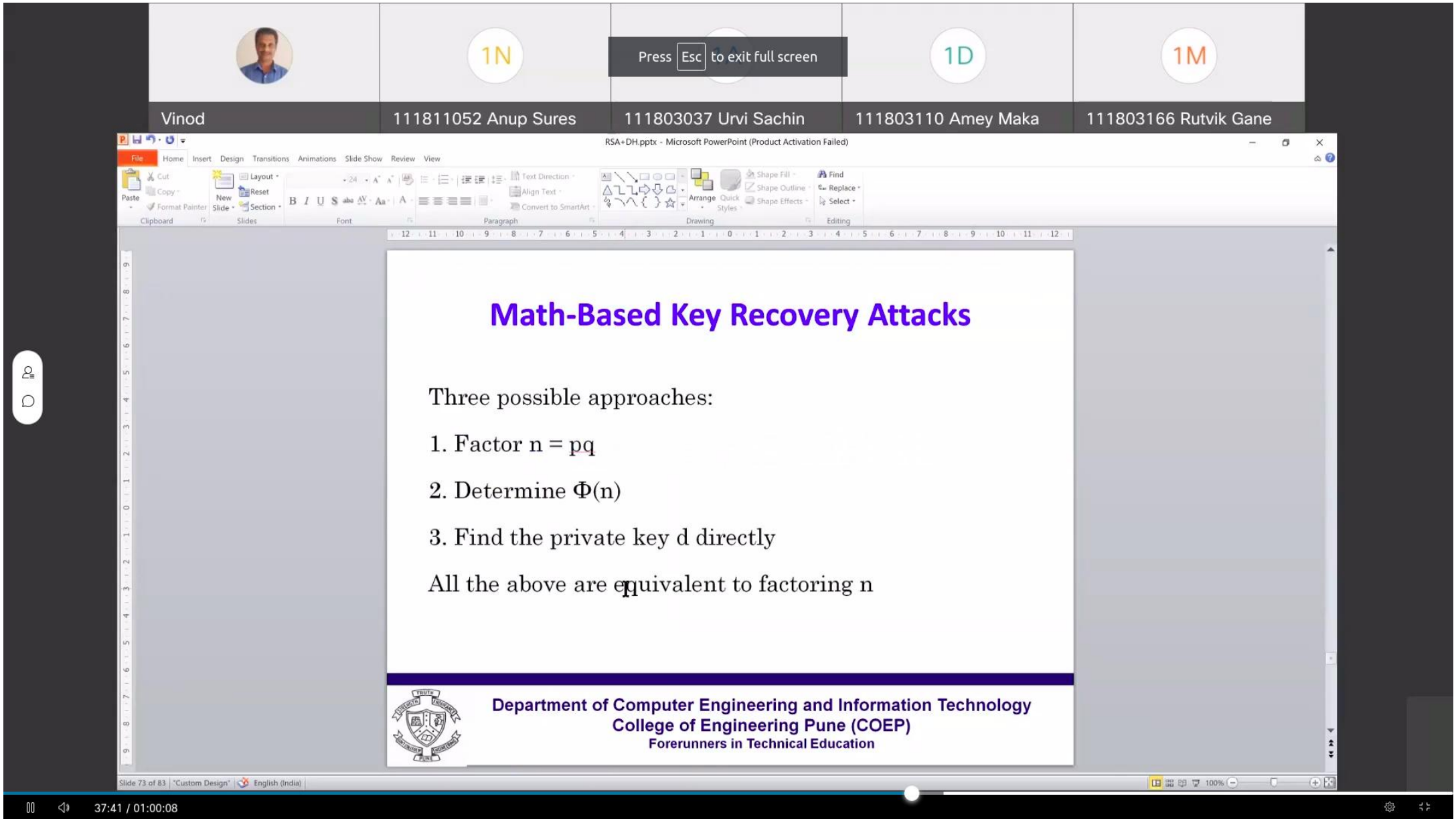
$P = 284^{367} \bmod 713 = 439$

Use modulo arithmetic to compute the value of P

Message $M = P = 439$

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education


Vinod
1N
111811052 Anup Sures
1A
111803037 Urvi Sachin
1D
111803110 Amey Maka
1M
111803166 Rutvik Gane
RSA+DH.pptx - Microsoft PowerPoint (Product Activation Failed)
Click to add title
Attacks against RSA
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
+67


Vinod
1N
111811052 Anup Sures
Press Esc to exit full screen
111803037 Urvi Sachin
1D
111803110 Amey Maka
1M
111803166 Rutvik Gane
RSA+DH.pptx - Microsoft PowerPoint (Product Activation Failed)
Math-Based Key Recovery Attacks
Three possible approaches:
1. Factor n = pq
2. Determine Φ(n)
3. Find the private key d directly
All the above are equivalent to factoring n
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
Slide 73 of 83
37:41 / 01:00:08

1N	1A	1D	1M
Vinod	111811052 Anup Sures	111803037 Urvi Sachin	111803110 Amey Maka	111803166 Rutvik Gane

RSA+DH.pptx - Microsoft PowerPoint (Product Activation Failed)

File Home Insert Design Transitions Animations Slide Show Review View

Paste Cut Copy Format Painter | New Slide Layout Reset Section | Clipboard Slides Font Paragraph Drawing Editing

Knowing Φ(n) Implies Factorization

- If a cryptanalyst can learn the value of Φ(n), then he can factor n and break the system.
- Computing Φ(n) is no easier than factoring n.
- In fact, knowing both n and Φ(n), one knows n = pq
- Therefore q = n/p

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Slide 74 of 83 | "Custom Design" | English (India)

+65

1N

Press Esc to exit full screen

1D

1M

Vinod | 111811052 Anup Sures | 111803037 Urvi Sachin | 111803110 Amey Maka | 111803166 Rutvik Gane

RSA+DH.pptx - Microsoft PowerPoint (Product Activation Failed)

$\Phi(n) = (p-1)(q-1) = pq - p - q + 1$

(Substitute $pq = n$ and $q = n/p$)

$= n - p - n/p + 1$

$p\Phi(n) = np - p^2 - n + p$

shift RHS terms to LHA

$p^2 - np + \Phi(n)p - p + n = 0$

$p^2 - (n - \Phi(n) + 1)\, p + n = 0$ = p^2 – 12 p +12

There are two solutions of p in the above equation.

Both p and q are solutions.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Slide 75 of 83 | "Custom Design" | English (U.S.)

+66

1N

1A

1D

1M

Vinod | 111811052 Anup Sures | 111803037 Urvi Sachin | 111803110 Amey Maka | 111803166 Rutvik Gane

RSA+DH.pptx - Microsoft PowerPoint (Product Activation Failed)

File Home Insert Design Transitions Animations Slide Show Review View

Paste Cut Copy Format Painter | New Slide Layout Reset Section | Clipboard Slides Font Paragraph Drawing Editing

Knowing Φ(n) Implies Factorization

- If a cryptanalyst can learn the value of Φ(n), then he can factor n and break the system.
- Computing Φ(n) is no easier than factoring n.
- In fact, knowing both n and Φ(n), one knows n = pq
- Therefore q = n/p

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Slide 74 of 83 | "Custom Design" | English (India) | 100%

44:45 / 01:00:08

1N

1A

1D

1M

Vinod | 111811052 Anup Sures | 111803037 Urvi Sachin | 111803110 Amey Maka | 111803166 Rutvik Gane

RSA+DH.pptx - Microsoft PowerPoint (Product Activation Failed)

Suppose the cryptanalyst has learned that n = 33 and $\Phi(n)=20$. Find out the two factors of n.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Slide 76 of 83 | "Custom Design" | English (India)

+66

1N

Press Esc to exit full screen

1D

1M

Vinod | 111811052 Anup Sures | 111803037 Urvi Sachin | 111803110 Amey Maka | 111803166 Rutvik Gane

RSA+DH.pptx - Microsoft PowerPoint (Product Activation Failed)

File Home Insert Design Transitions Animations Slide Show Review View

Paste Cut Copy Format Painter | New Slide Layout Reset Section | Clipboard Slides Font Paragraph Drawing Editing

Click to add title

Solution:

$p^2 - (n - \Phi(n) + 1)\, p + n = 0$

$p^2 - (33 - 20 + 1)\, p + 33 = 0$

$p^2 - (14)\, p + 33 = 0$

$p = 11$ and 3

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Slide 77 of 83 | "Custom Design" | English (India) | 100%

+66

1N	1A	1D	1M
Vinod	111811052 Anup Sures	111803037 Urvi Sachin	111803110 Amey Maka	111803166 Rutvik Gane

RSA+DH.pptx - Microsoft PowerPoint (Product Activation Failed)

Suppose the cryptanalyst has learned that n = 84773093 and Φ(n)=84754668.

Find out the two factors of n.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Slide 77 of 83 | "Custom Design" | English (U.S.)

javascript:void(0);

:14 / 01:00:08

1P	1A	1J	1M
Vinod	111803089 Muskan De	111803037 Urvi Sachin	111809044 Aniket Jaya	111803166 Rutvik Gane

RSA+DH.pptx - Microsoft PowerPoint (Product Activation Failed)

File Home Insert Design Transitions Animations Slide Show Review View

Paste Cut Copy Format Painter | New Slide Layout Reset Section | Clipboard Slides Font Paragraph Drawing Editing

Decryption attacks on RSA

RSA Problem:

Given a positive integer n (that is a product of two distinct large primes p and q), a positive integer e (Public Key exponent) such that gcd(e, (p-1)(q-1))=1, and an integer c (Ciphertext), find an integer m (plaintext) such that $m^e \equiv c \pmod{n}$ – widely believed that the RSA problem is computationally equivalent to integer factorization; however, no proof is known.

The security of RSA encryption's scheme depends on the hardness of the RSA problem.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Slide 80 of 83 | "Custom Design" | English (India) | 100%

javascript:void(0); 3:56 / 01:00:08

1P

1A

1J

1M

Vinod | 111803089 Muskan De | 111803037 Urvi Sachin | 111809044 Aniket Jaya | 111803166 Rutvik Gane

RSA+DH.pptx - Microsoft PowerPoint (Product Activation Failed)

Finding d: Timing Attacks

Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems (1996), Paul C. Kocher

By measuring the time required to perform decryption (exponentiation with the private key as exponent), an attacker can figure out the private key

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Slide 81 of 83 | "Custom Design" | English (India)

+62

1P	1A	1J	1M
Vinod	111803089 Muskan De	111803037 Urvi Sachin	111809044 Aniket Jaya	111803166 Rutvik Gane

RSA+DH.pptx - Microsoft PowerPoint (Product Activation Failed)

File Home Insert Design Transitions Animations Slide Show Review View

Paste Cut Copy Format Painter | New Slide Layout Reset Section | Clipboard Slides Font Paragraph Drawing Editing

Click to add title

- Possible countermeasures: –
  - use constant exponentiation time
  - add random delays
  - blind values used in calculations

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Slide 82 of 83 | "Custom Design" | English (India)

+62

1P	1J	1M
Vinod	111803089 Muskan De	111803037 Urvi Sachin	111809044 Aniket Jaya	111803166 Rutvik Gane

Press Esc to exit full screen

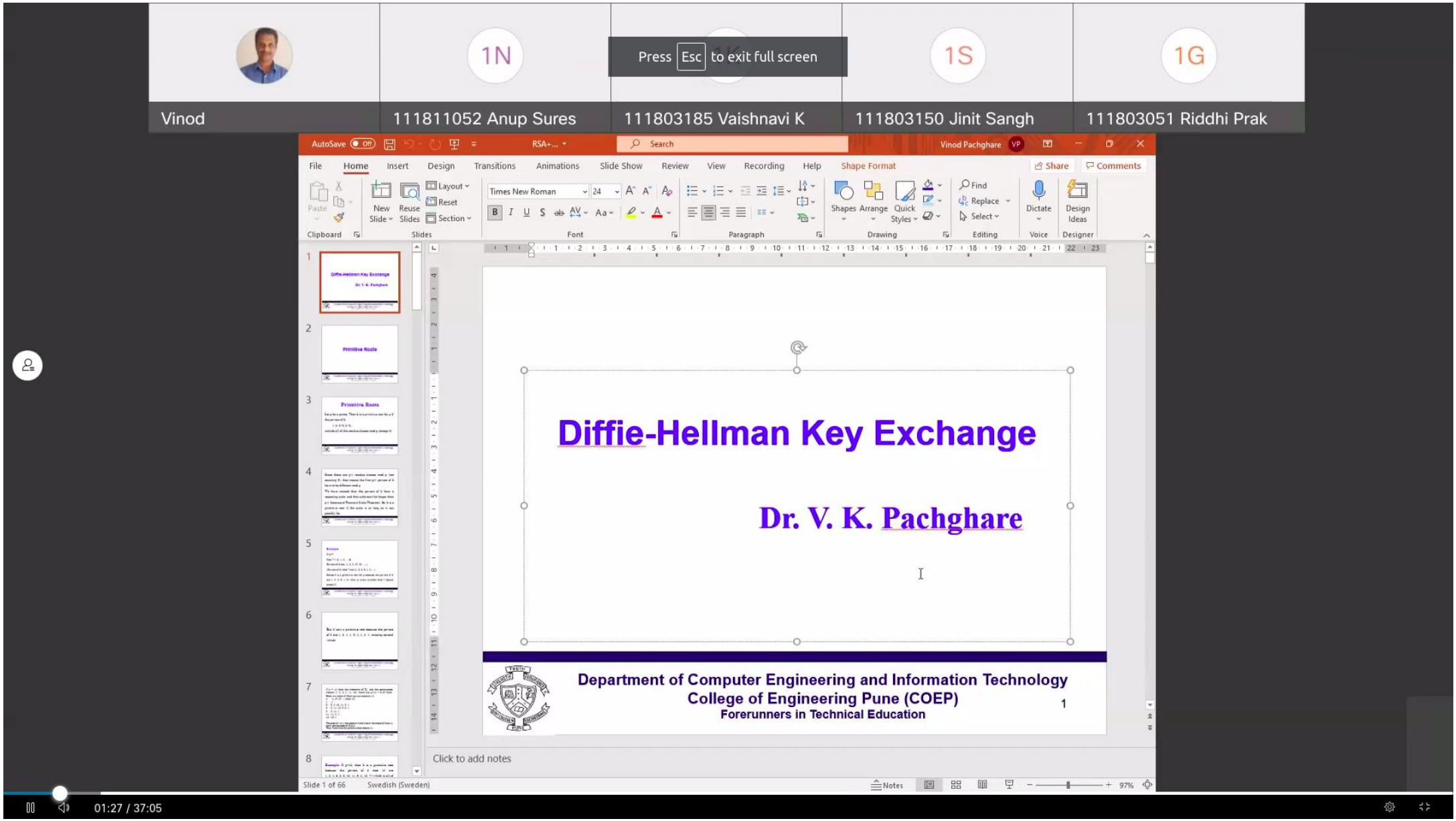
RSA+DH.pptx - Microsoft PowerPoint (Product Activation Failed)

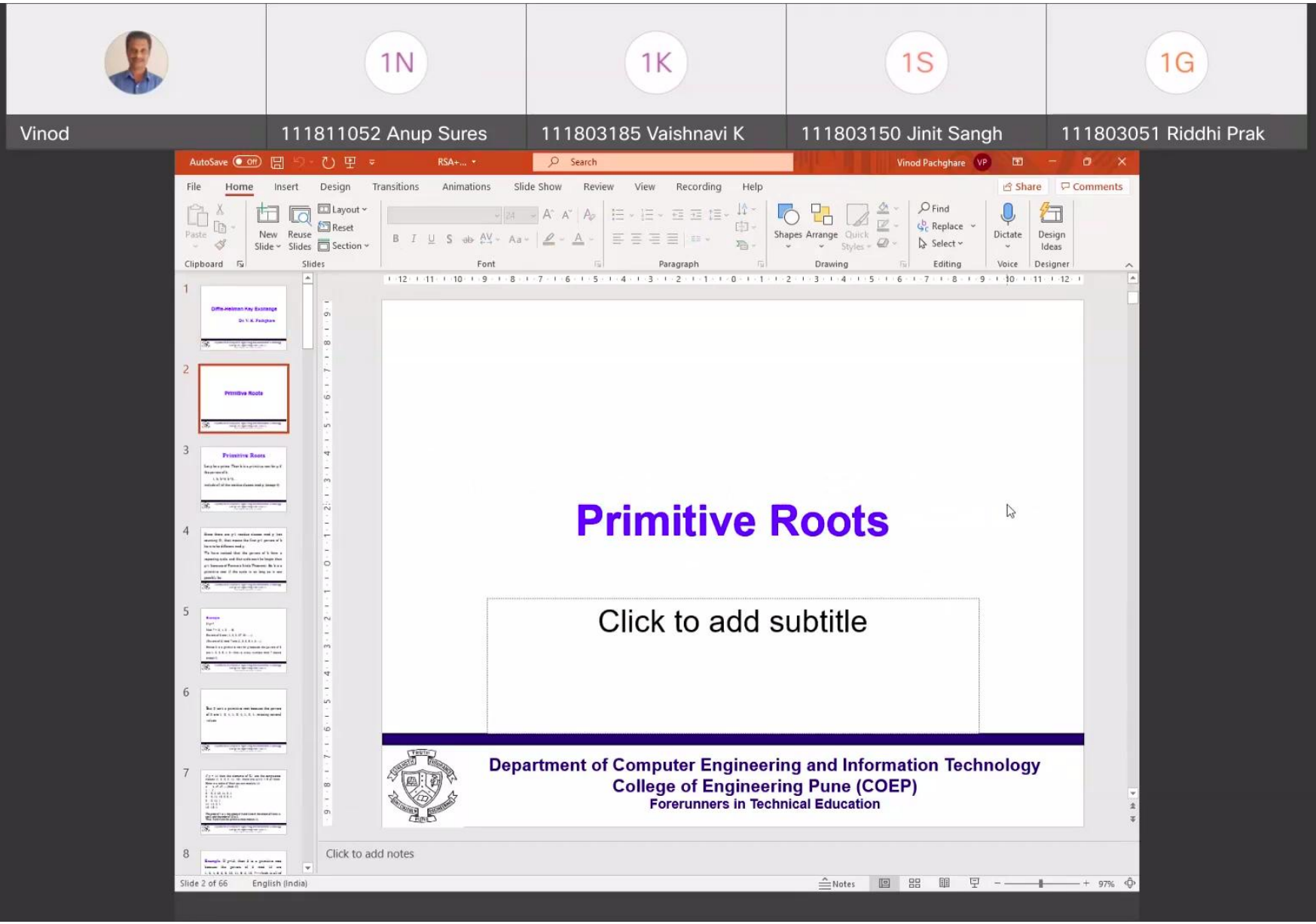
- Researchers have discovered a timing attack on RSA keys, to which OpenSSL is generally vulnerable, unless RSA blinding has been turned on.
- RSA blinding: the decryption time is no longer correlated to the value of the input ciphertext
- Instead of computing c^d mod n, choose a secret random value r and compute $(r^2c)^d$ mod n.
- A new value of r is chosen for each ciphertext

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Slide 83 of 83 | "Custom Design" | English (India)

+61


Press Esc to exit full screen
Vinod
111811052 Anup Sures
111803185 Vaishnavi K
111803150 Jinit Sangh
111803051 Riddhi Prak
Diffie-Hellman Key Exchange
Dr. V. K. Pachghare
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
1
Click to add notes
01:27 / 37:05


Vinod
1N
111811052 Anup Sures
1K
111803185 Vaishnavi K
1S
111803150 Jinit Sangh
1G
111803051 Riddhi Prak
Primitive Roots
Click to add subtitle
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
Click to add notes
Slide 2 of 66
English (India)
+67

Vinod | 111811052 Anup Sures | 111803185 Vaishnavi K | 111803150 Jinit Sangh | 111803051 Riddhi Prak

AutoSave Off | RSA+... | Search | Vinod Pachghare VP

File Home Insert Design Transitions Animations Slide Show Review View Recording Help | Share | Comments

Paste | New Slide | Reuse Slides | Layout | Reset | Section | Clipboard | Slides | Font | Paragraph | Shapes | Arrange | Quick Styles | Find | Replace | Select | Editing | Dictate | Voice | Design Ideas | Designer

1 Diffie-Hellman Key Exchange
2 Primitive Roots
3 Primitive Roots
4
5
6
7
8

Primitive Roots

Let p be a prime. Then b is a *primitive root* for p if the powers of b,

1, b, b^2, b^3, ...

include all of the residue classes mod p (except 0).

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Click to add notes

Slide 3 of 66 | English (India) | Notes | 97%

02:11 / 37:05

Vinod | 111811052 Anup Sures | 111803185 Vaishnavi K | 111803150 Jinit Sangh | 111803051 Riddhi Prak

AutoSave Off | RSA+... | Search | Vinod Pachghare VP

File Home Insert Design Transitions Animations Slide Show Review View Recording Help | Share | Comments

Clipboard | Slides | Font | Paragraph | Drawing | Editing | Voice | Designer

1 Diffie-Hellman Key Exchange
Dr V. K. Pachghare

2 Primitive Roots

3 Primitive Roots

4

5

6

7

8

Since there are p-1 residue classes mod p (not counting 0), that means the first p-1 powers of b have to be different mod p.

We have noticed that the powers of b form a repeating cycle, and that cycle can't be longer than p-1 (because of Fermat's Little Theorem). So, b is a primitive root if the cycle is as long as it can possibly be.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Click to add notes

Slide 4 of 66 | English (India) | Notes | 97%

+82

Vinod | 111811052 Anup Sures | 111803185 Vaishnavi K | 111803150 Jinit Sangh | 111803051 Riddhi Prak

AutoSave Off | RSA+... | Search | Vinod Pachghare VP

File Home Insert Design Transitions Animations Slide Show Review View Recording Help | Share | Comments

Paste | New Slide | Reuse Slides | Layout | Reset | Section | Clipboard | Slides | Font | Paragraph | Shapes | Arrange | Quick Styles | Find | Replace | Select | Editing | Dictate | Voice | Design Ideas | Designer

1 Diffie-Hellman Key Exchange
Dr. V. K. Pachghare

2 Primitive Roots

3 Primitive Roots

4

5

6

7

8

Example:

If p=7,

Mod 7 = {0, 1, 2, ….6}

Powers of 3 are { 1, 3, 9, 27, 81 …..}

(Powers of 3) mod 7 are {1, 3, 2, 6, 4, 5…..}

Hence 3 is a primitive root for p because the powers of 3 are 1, 3, 2, 6, 4, 5---that is, every number mod 7 occurs except 0.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Click to add notes

Slide 5 of 66 | English (India) | Notes | 97%

+83

Vinod | 111811052 Anup Sures | 111803185 Vaishnavi K | 111803150 Jinit Sangh | 111803051 Riddhi Prak

AutoSave Off | RSA+... | Search | Vinod Pachghare VP

File Home Insert Design Transitions Animations Slide Show Review View Recording Help | Share | Comments

Paste | New Slide | Reuse Slides | Layout | Reset | Section | Clipboard | Slides | Font | Paragraph | Shapes | Arrange | Quick Styles | Find | Replace | Select | Editing | Dictate | Voice | Design Ideas | Designer

1 Diffie-Hellman Key Exchange
Dr V. K. Pachghare

2 Primitive Roots

3 Primitive Roots

4

5

6

7

8

Click to add title

But 2 isn't a primitive root because the powers of 2 are 1, 2, 4, 1, 2, 4, 1, 2, 4...missing several values.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Click to add notes

Slide 6 of 66 | English (India) | Notes | 97%

javascript:void(0); 5:32 / 37:05

Vinod | 111811052 Anup Sures | 111803185 Vaishnavi K | 111803150 Jinit Sangh | 111803051 Riddhi Prak

AutoSave Off | RSA+... | Search | Vinod Pachghare VP

File Home Insert Design Transitions Animations Slide Show Review View Recording Help Shape Format | Share | Comments

Clipboard | Slides | Font | Paragraph | Drawing | Editing | Voice | Designer

1 Diffie-Hellman Key Exchange
2 Primitive Roots
3 Primitive Roots
4
5
6
7
8

if $p = 14$ then the elements of $\mathbf{Z}_n^\times$ are the congruence classes {1, 3, 5, 9, 11, 13}; there are $\varphi(14) = 6$ of them. Here is a table of their powers modulo 14:

x x, x^2, x^3, ... (mod 14)

1 : 1
3 : 3, 9, 13, 11, 5, 1
5 : 5, 11, 13, 9, 3, 1
9 : 9, 11, 1
11 : 11, 9, 1
13 : 13, 1

The order of 1 is 1, the orders of 3 and 5 are 6, the orders of 9 and 11 are 3, and the order of 13 is 2.
Thus, 3 and 5 are the primitive roots modulo 14.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

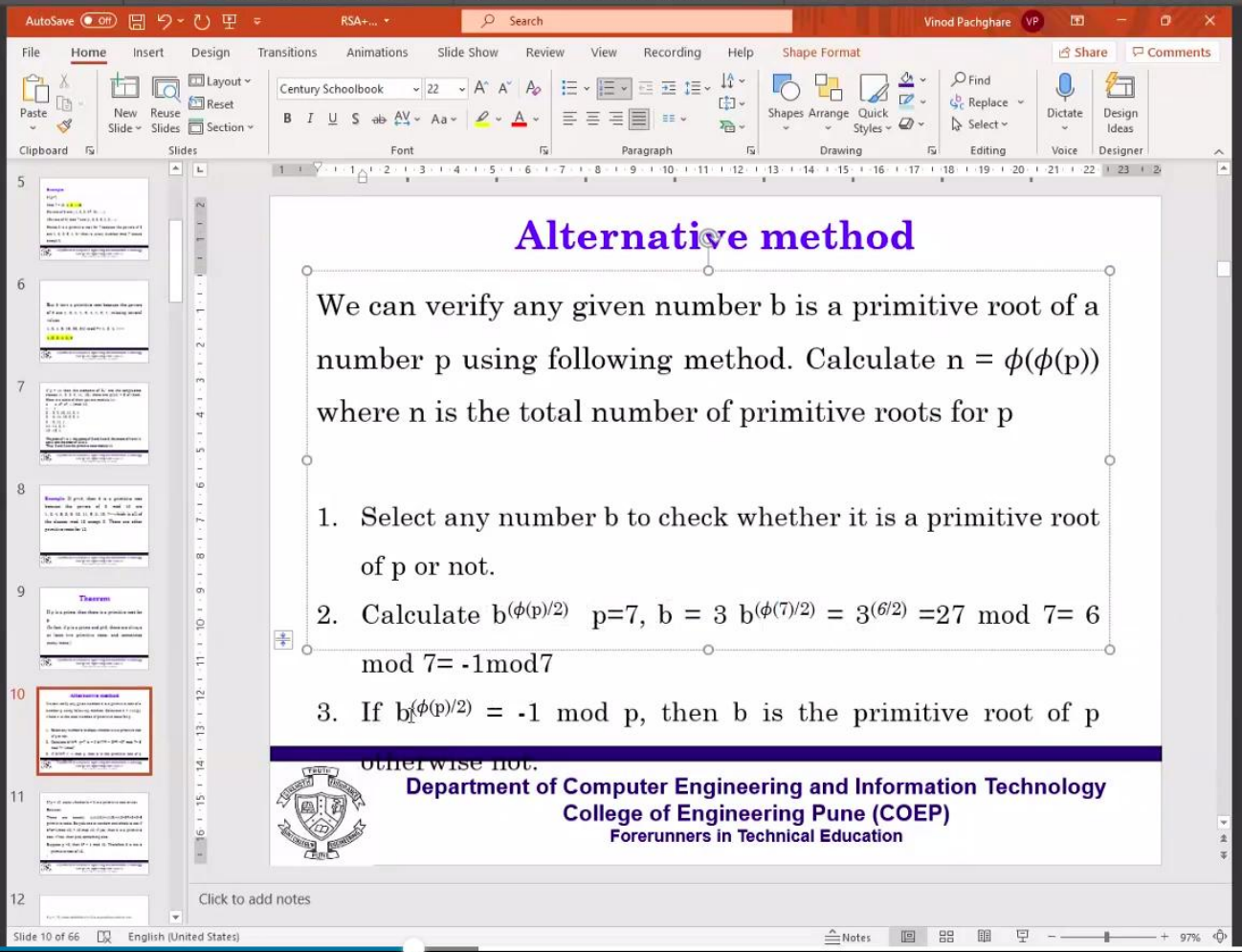
Click to add notes

Slide 7 of 66 | English (United States) | Notes | 97%

+93

1N	1K	1N	1G
Vinod	111811052 Anup Sures	111803185 Vaishnavi K	111803141 Rushikesh	111803051 Riddhi Prak

Example: If p=13, then 2 is a primitive root because the powers of 2 mod 13 are 1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7---which is all of the classes mod 13 except 0. There are other primitive roots for 13.



14:50 / 37:05

If p = 19, state whether b = 5 is a primitive root or not.

Solution:

There are exactly $\phi(\phi(19))=\phi(18)=\phi(2\times3^2)=2\times3=6$ primitive roots. So pick one at random and check to see if $b^9 \equiv -1 \pmod{19} = 18 \bmod 10$; if yes, then b is a primitive root; if not, then pick something else.

Suppose p =5; then $5^9 = 1 \bmod 19$. Therefore 5 is not a primitive root of 19.

•

Vinod | 111811052 Anup Sures | 111803185 Vaishnavi K | 111803141 Rushikesh | 111803051 Riddhi Prak

Diffie-Hellman Key Exchange

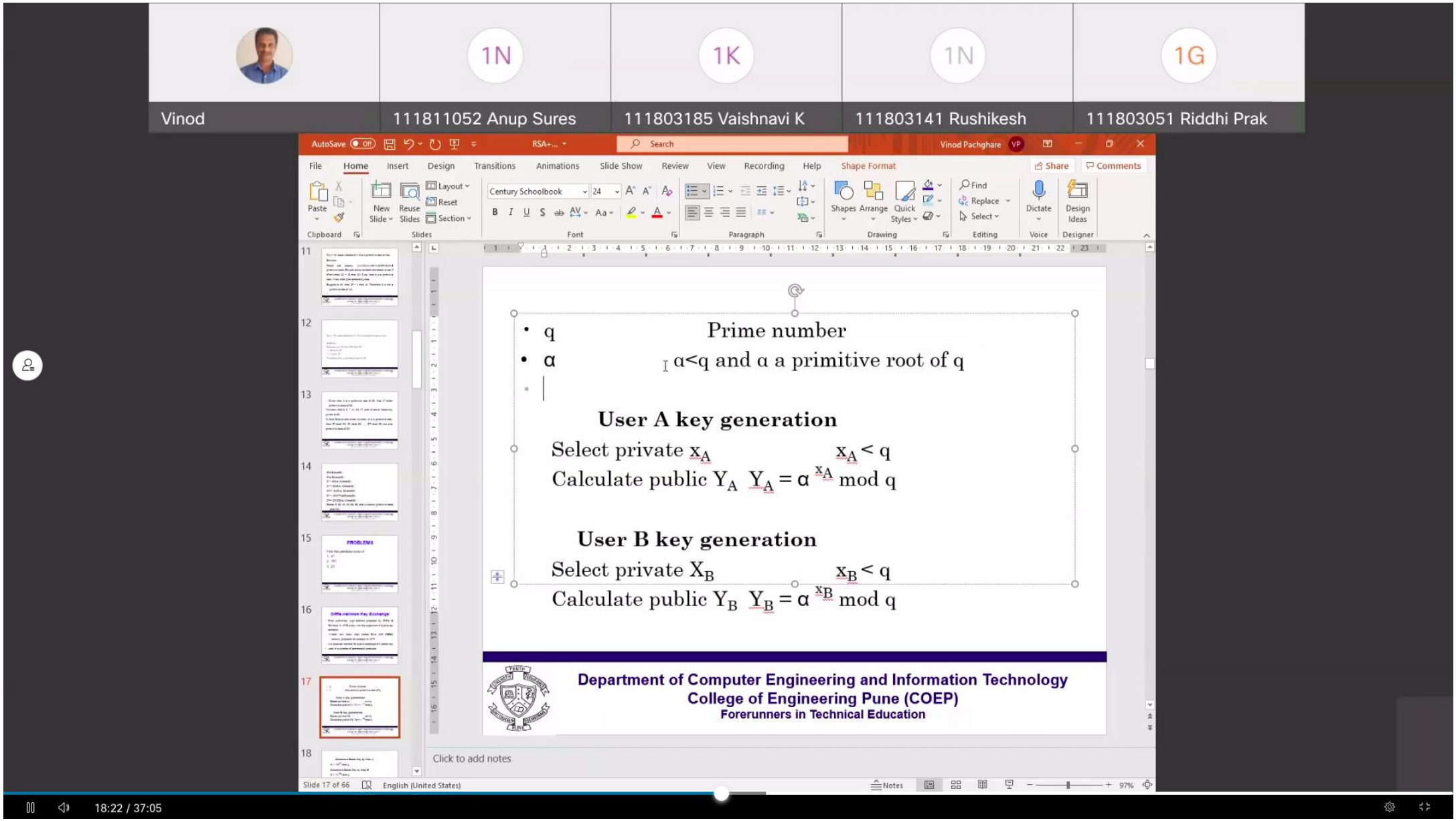
- First public-key type scheme proposed by Diffie & Hellman in 1976 along with the exposition of public key concepts
  - note: now know that James Ellis (UK CESG) secretly proposed the concept in 1970
- is a practical method for public exchange of a secret key
- used in a number of commercial products

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

The idea of public key schemes, and the first practical scheme, which was for key distribution only, was published in 1977 by Diffie & Hellman. The concept had been previously described in a classified report in 1970 by James Ellis (UK CESG) - and subsequently declassified in 1987. See History of Non-secret Encryption (at

Slide 16 of 66 English (India)

17:53 / 37:05


Vinod
111811052 Anup Sures
111803185 Vaishnavi K
111803141 Rushikesh
111803051 Riddhi Prak
Vinod Pachghare
File Home Insert Design Transitions Animations Slide Show Review View Recording Help Shape Format
Share Comments
Century Schoolbook 24
Paste New Slide Reuse Slides Layout Reset Section
Clipboard Slides Font Paragraph Drawing Editing Voice Designer
Shapes Arrange Quick Styles Find Replace Select Dictate Design Ideas
• q Prime number
• α α<q and α a primitive root of q
User A key generation
Select private x_A $x_A < q$
Calculate public Y_A $Y_A = \alpha^{x_A} \bmod q$
User B key generation
Select private X_B $x_B < q$
Calculate public Y_B $Y_B = \alpha^{x_B} \bmod q$
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
Click to add notes
Slide 17 of 66
English (United States)
Notes
97%
18:22 / 37:05

Vinod | 111811052 Anup Sures | 111803185 Vaishnavi K | 111803141 Rushikesh | 111803051 Riddhi Prak

Generate a Secret Key by User A

$K = Y_B^{X_A} \bmod q$

Generate a Secret Key by User B

$K = Y_A^{X_B} \bmod q$

Both calculations produce identical results.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Click to add notes

Slide 18 of 66 English (India)

+109

prime q = 23 and α = 5

select random secret keys:

A chooses X_A= 6

B chooses X_B=15

Compute the Shared session key

$$Y_A = 5^6 \bmod 23 = 8$$

$$Y_B = 5^{15} \bmod 23 = 19$$

$$K = 19^6 \bmod 23 = 2$$

$$K = 8^{15} \bmod 23 = 2$$

1N	1K	1N	1G
Vinod	111811052 Anup Sures	111803185 Vaishnavi K	111803141 Rushikesh	111803051 Riddhi Prak

Users A and B use the Diffie–Hellman key exchange technique with a common prime $q = 71$ and a primitive root $a = 7$.

(a) If user A has private key $X_A = 5$, what is A's public key Y_A?

(b) If user B has private key $X_B = 12$, what is B's public Y_B?

(c) What is the shared secret key?

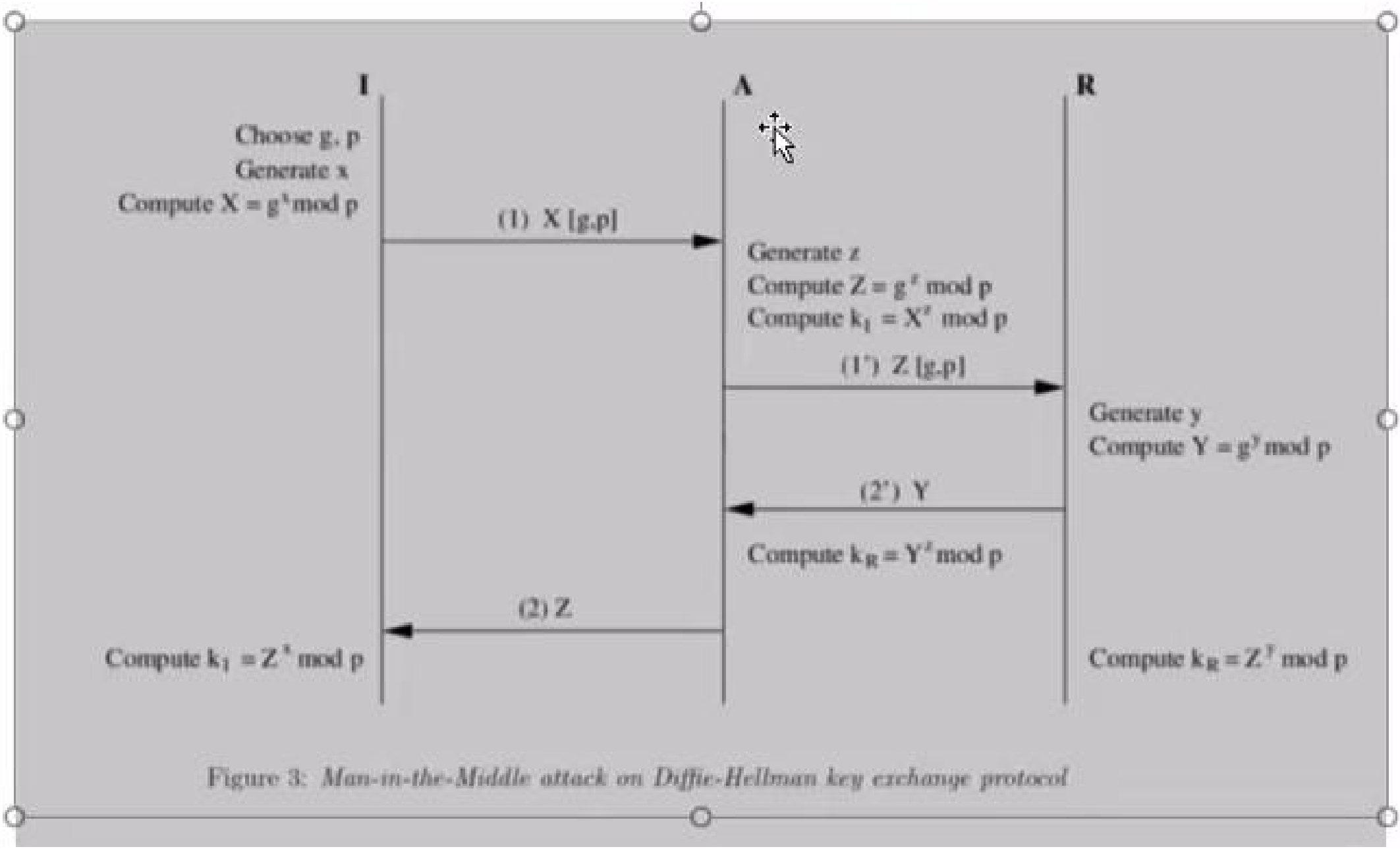


Figure 3: *Man-in-the-Middle attack on Diffie-Hellman key exchange protocol*

Vinod	141903010 Kajal Naray	111803166 Rutvik Gane	111803064 Onkar Datta	141903005 Kajol Vijay

Firewall - Microsoft PowerPoint

Home Insert Design Animations Slide Show Review View

You are sharing your entire screen. Stop Sharing

Slides Outline

1 Cryptography and Network Security
Unit-VI
Date: 13 Oct 2021
Dr. V. K. Pachghare

2 Firewalls
V. K. Pachghare

3 Introduction
- Plays an important and major role to protect the system.
- Prevents unauthorized access to and from the network.
- Protect the network from the attackers.
- Allow the internal users to access the outside network via Internet and WAN.

4 Functions
- It blocks unauthorized traffic.
- It forward the incoming traffic to more reliable internal computer systems.
- It hides internal computers or network which are vulnerable.
- It hides the information about internal network such as names of the computer system, network topology used, types of network device, etc.

5
- It provides strong user authentication.
- It can serve as a platform for IPSec.

Firewalls

V. K. Pachghare

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

2

Click to add notes

Slide 2 of 39 'Default Design' English (United States) 110%

00:03 / 35:42

1K	1M	1K	1G
Vinod	141903010 Kajal Naray	111803166 Rutvik Gane	111803064 Onkar Datta	141903005 Kajol Vijay

Firewall - Microsoft PowerPoint

Home Insert Design Animations Slide Show Review View

You are sharing your entire screen. Stop Sharing

Slides Outline

1 Cryptography and Network Security
Unit-VI
Date: 13 Oct 2021
Dr. V. K. Pachghare

2 Firewalls
V. K. Pachghare

3 Introduction
- Plays an important and major role to protect the system.
- Prevents unauthorized access to and from the network.
- Protect the network from the attackers.
- Allow the internal users to access the outside network via Internet and WAN.

4 Functions
- It blocks unauthorized traffic
- It forward the incoming traffic to more reliable internal computer systems
- It hides internal computers or network which are vulnerable
- It hides the information about internal network such as names of the computer system, network topology used, types of network device, etc.

5
- It provides strong user authentication
- It can serve as a platform for IPSec

Introduction

- Plays an important and major role to protect the system.
- Prevents unauthorized access to and from the network.
- Protect the network from the attackers.
- Allow the internal users to access the outside network via Internet and WAN.

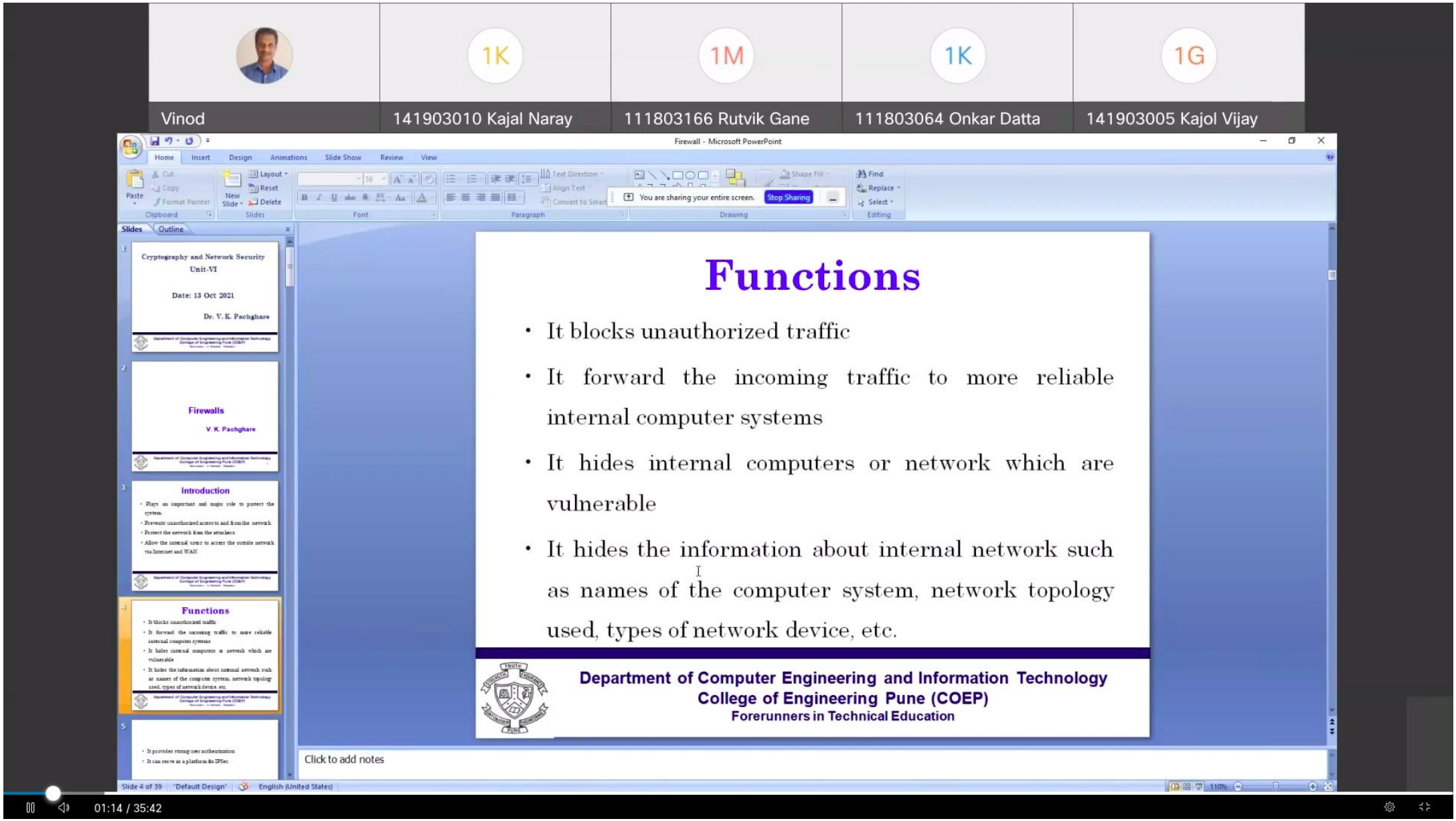
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

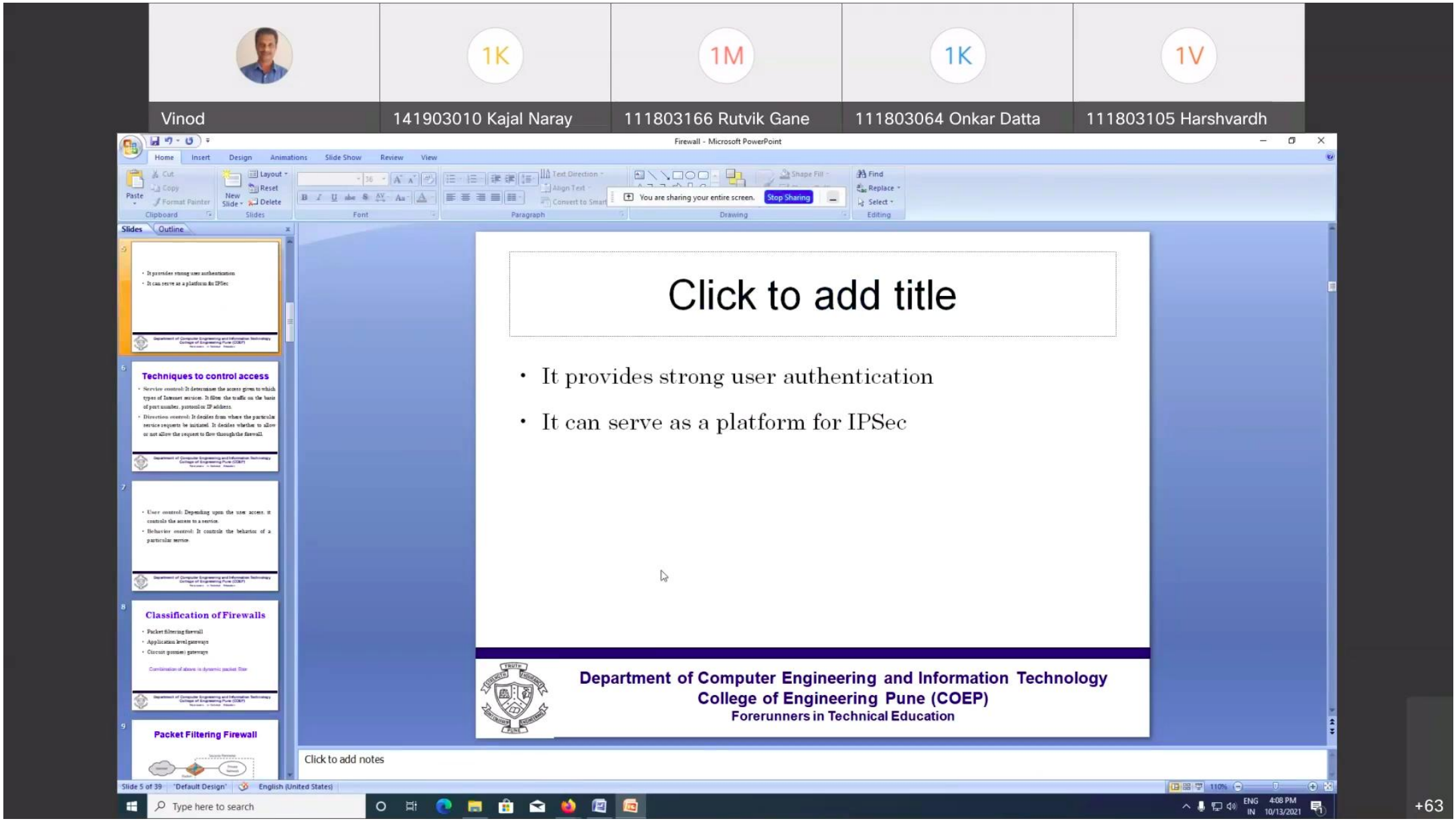
The idea of public key schemes, and the first practical scheme, which was for key distribution only, was published in 1977 by Diffie & Hellman. The concept had been previously described in a classified report in 1970 by James

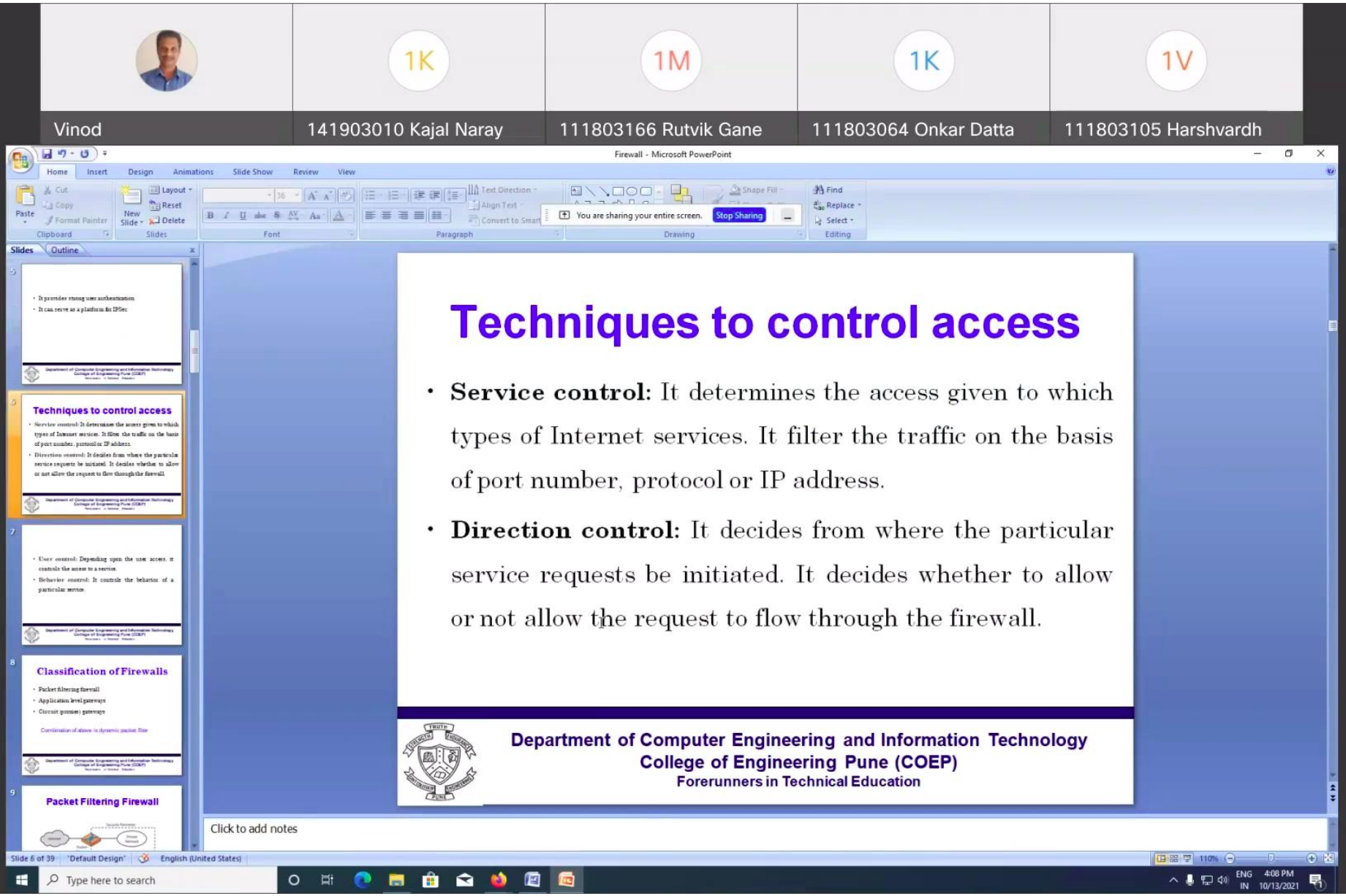
Slide 3 of 39 'Default Design' English (United States) 110%

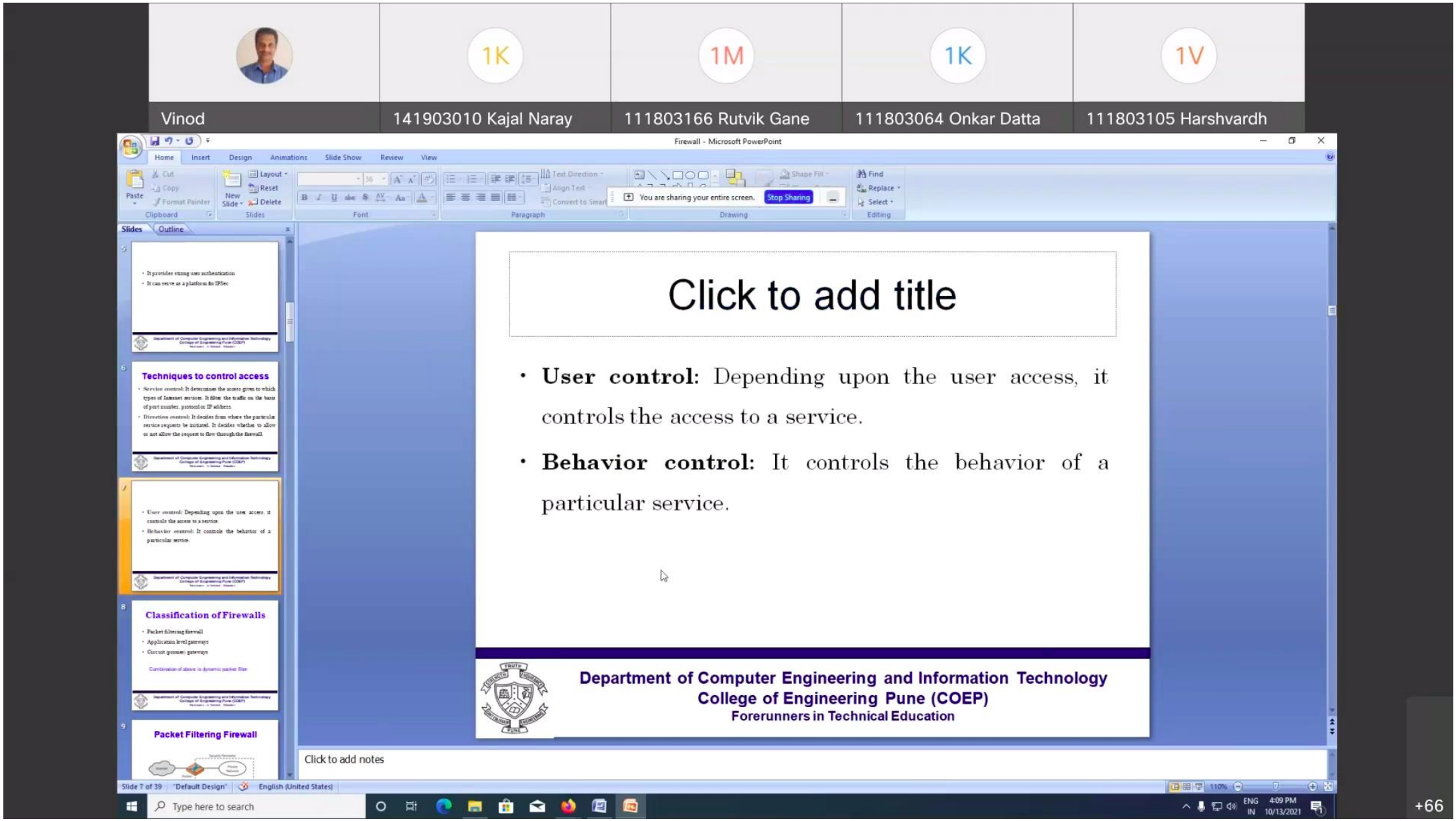
Type here to search ENG IN 4:05 PM 10/13/2021

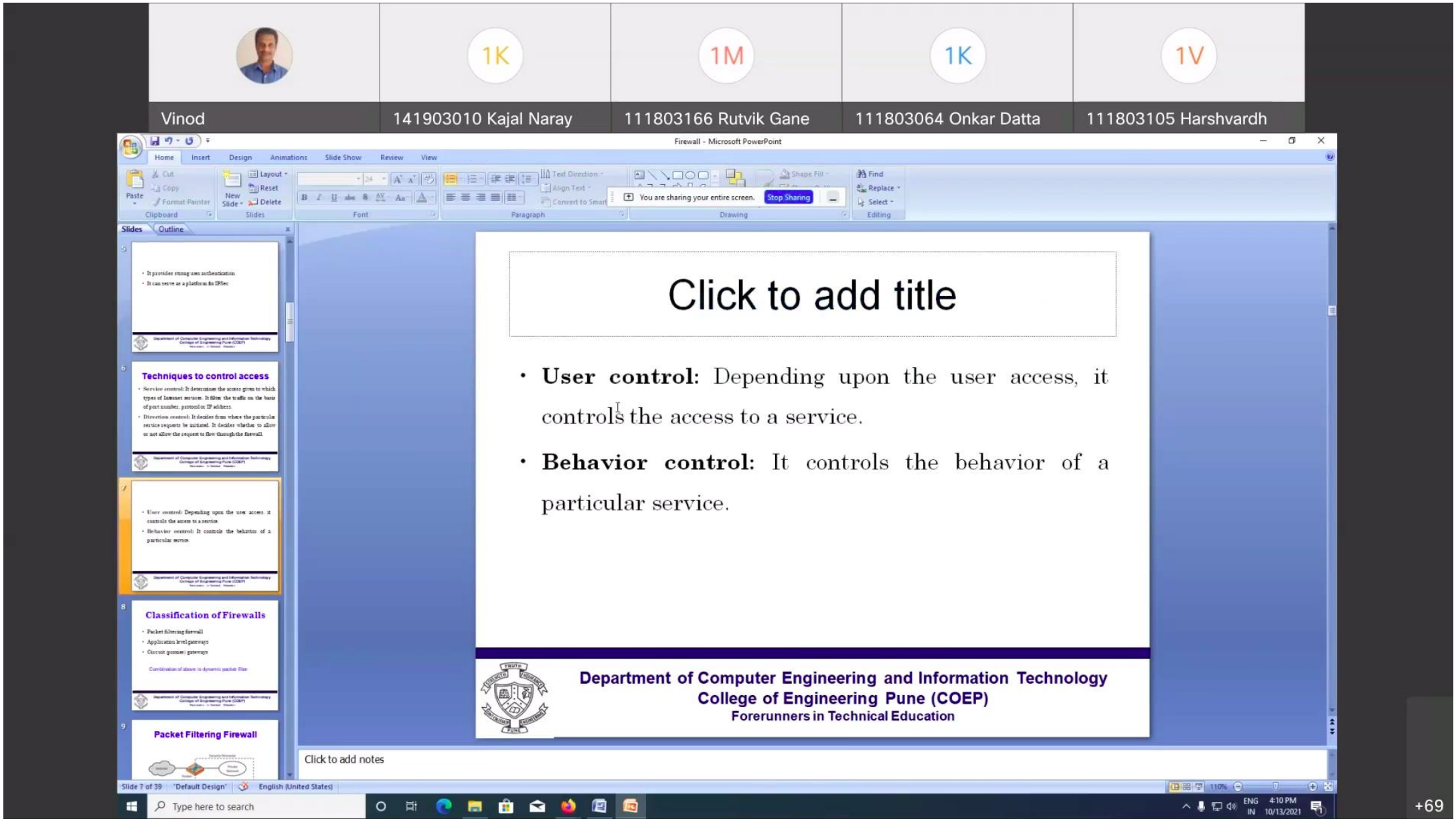
+48

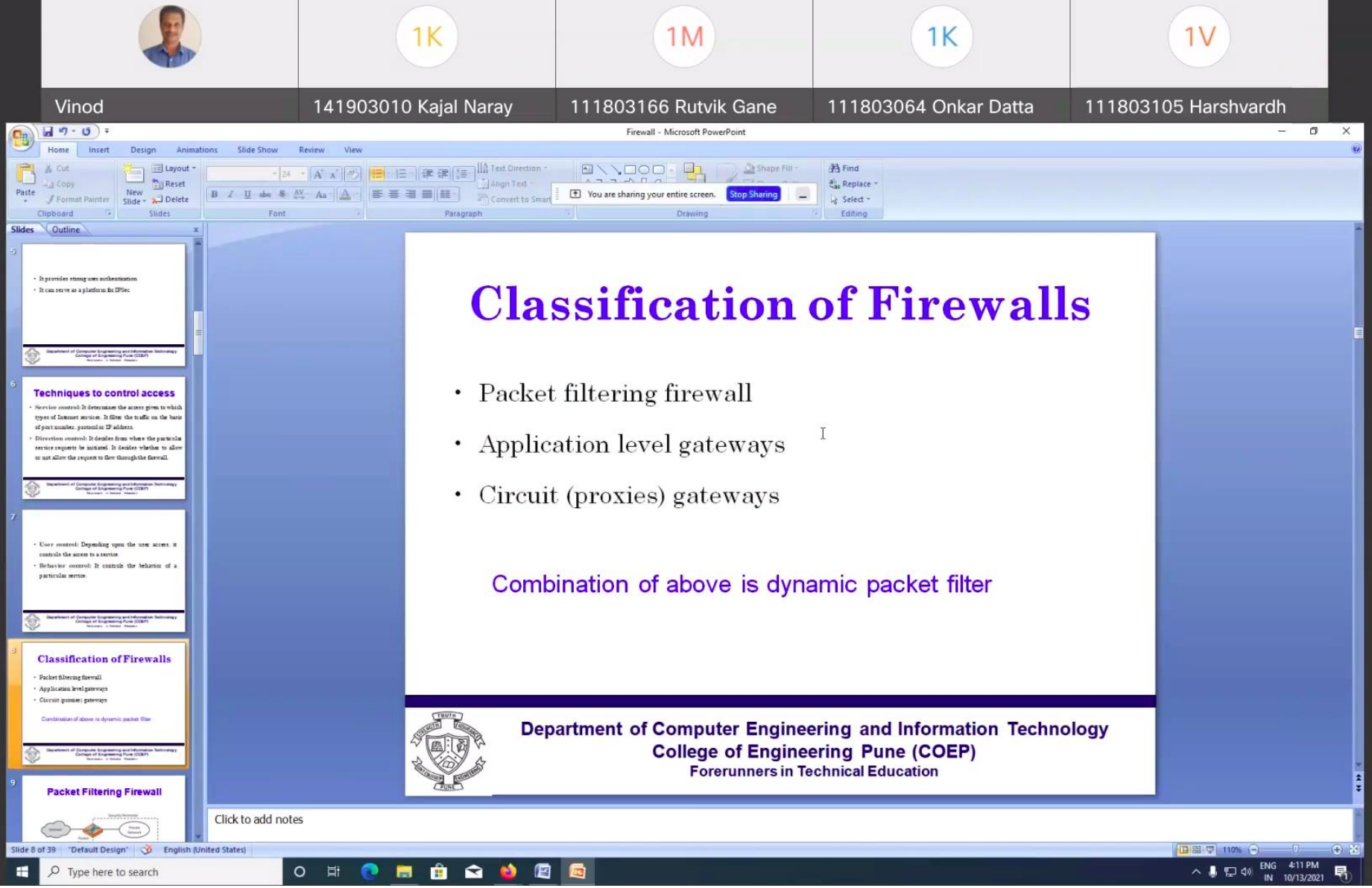

Vinod
141903010 Kajal Naray
111803166 Rutvik Gane
111803064 Onkar Datta
141903005 Kajol Vijay
Firewall - Microsoft PowerPoint
You are sharing your entire screen.
Stop Sharing
Functions
It blocks unauthorized traffic
It forward the incoming traffic to more reliable internal computer systems
It hides internal computers or network which are vulnerable
It hides the information about internal network such as names of the computer system, network topology used, types of network device, etc.
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
Click to add notes
01:14 / 35:42


Vinod
141903010 Kajal Naray
111803166 Rutvik Gane
111803064 Onkar Datta
111803105 Harshvardh
Firewall - Microsoft PowerPoint
You are sharing your entire screen.
Stop Sharing
Click to add title
It provides strong user authentication
It can serve as a platform for IPSec
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
Click to add notes
Techniques to control access
Classification of Firewalls
Packet Filtering Firewall
Slide 5 of 39
Type here to search
+63


Vinod
141903010 Kajal Naray
111803166 Rutvik Gane
111803064 Onkar Datta
111803105 Harshvardh
Firewall - Microsoft PowerPoint
You are sharing your entire screen.
Stop Sharing
Techniques to control access
Service control: It determines the access given to which types of Internet services. It filter the traffic on the basis of port number, protocol or IP address.
Direction control: It decides from where the particular service requests be initiated. It decides whether to allow or not allow the request to flow through the firewall.
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
Click to add notes
Classification of Firewalls
Packet Filtering Firewall
Slide 6 of 39
'Default Design'
English (United States)
Type here to search
ENG
IN
4:08 PM
10/13/2021
+65


Vinod
141903010 Kajal Naray
111803166 Rutvik Gane
111803064 Onkar Datta
111803105 Harshvardh
Firewall - Microsoft PowerPoint
You are sharing your entire screen.
Stop Sharing
Click to add title
User control: Depending upon the user access, it controls the access to a service.
Behavior control: It controls the behavior of a particular service.
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
Click to add notes
Techniques to control access
Classification of Firewalls
Packet Filtering Firewall
Type here to search
+66

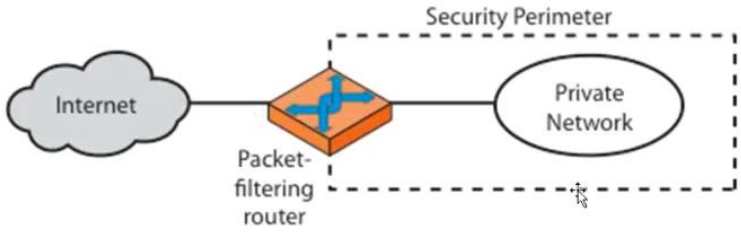

Vinod
141903010 Kajal Naray
111803166 Rutvik Gane
111803064 Onkar Datta
111803105 Harshvardh
Firewall - Microsoft PowerPoint
You are sharing your entire screen.
Stop Sharing
Click to add title
User control: Depending upon the user access, it controls the access to a service.
Behavior control: It controls the behavior of a particular service.
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
Click to add notes
Techniques to control access
Classification of Firewalls
Packet Filtering Firewall
Slide 7 of 39
Type here to search
+69


Vinod
141903010 Kajal Naray
111803166 Rutvik Gane
111803064 Onkar Datta
111803105 Harshvardh
Firewall - Microsoft PowerPoint
You are sharing your entire screen.
Stop Sharing
Classification of Firewalls
Packet filtering firewall
Application level gateways
Circuit (proxies) gateways
Combination of above is dynamic packet filter
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
Click to add notes
Slide 8 of 39
Type here to search
+69

Vinod | 141903010 Kajal Naray | 111803166 Rutvik Gane | 111803064 Onkar Datta | 111803105 Harshvardh

Firewall - Microsoft PowerPoint

Packet Filtering Firewall



(a) Packet-filtering router

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Click to add notes

Slide 9 of 39 'Default Design' English (United States)

+72

1K	1M	1K	1V
Vinod	141903010 Kajal Naray	111803166 Rutvik Gane	111803064 Onkar Datta	111803105 Harshvardh

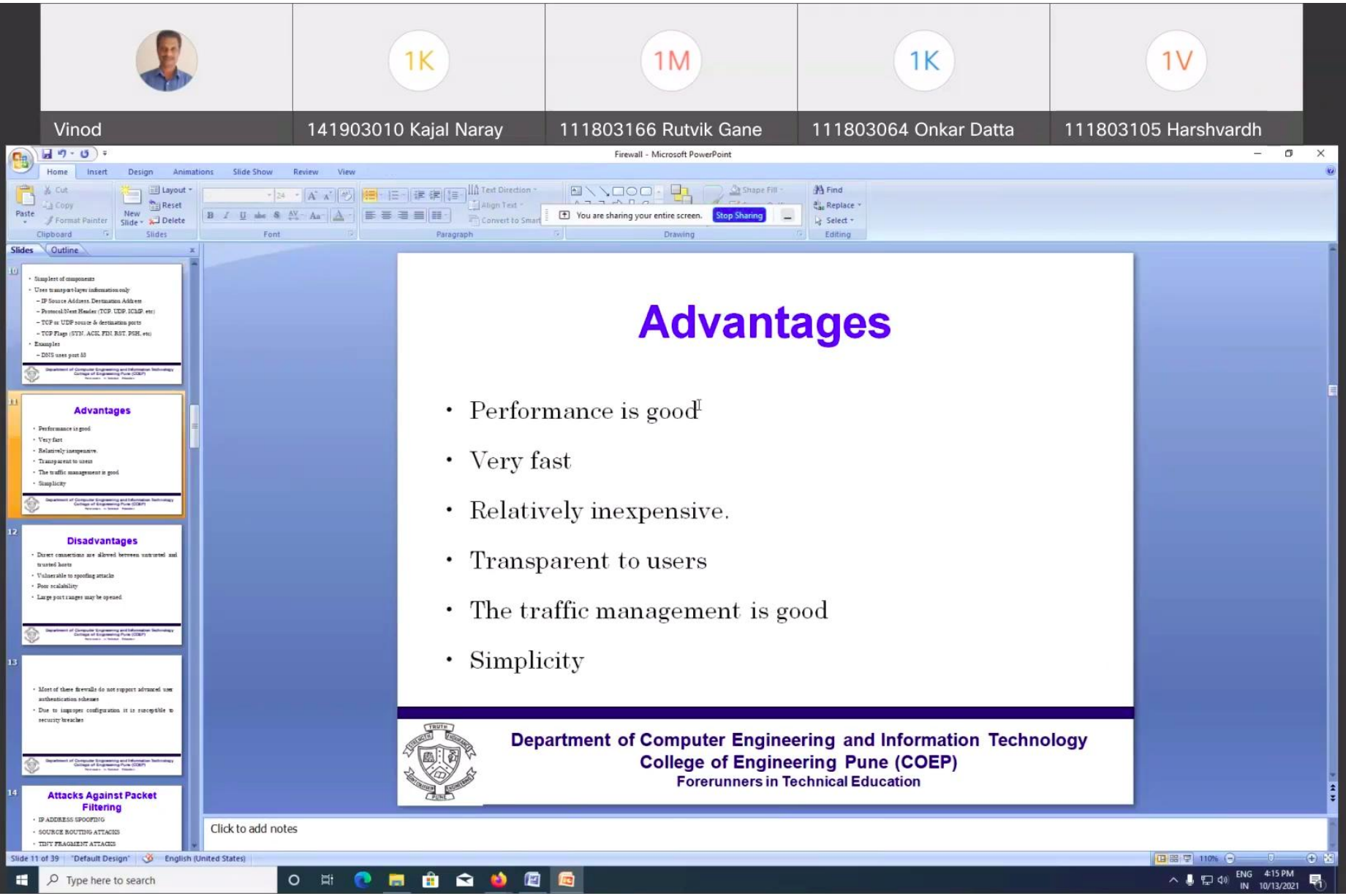
Firewall - Microsoft PowerPoint

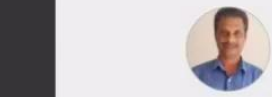
- Simplest of components
- Uses transport-layer information only
  - IP Source Address, Destination Address
  - Protocol/Next Header (TCP, UDP, ICMP, etc)
  - TCP or UDP source & destination ports
  - TCP Flags (SYN, ACK, FIN, RST, PSH, etc)
- Examples
  - DNS uses port 53

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Click to add notes

+78


Vinod
141903010 Kajal Naray
111803166 Rutvik Gane
111803064 Onkar Datta
111803105 Harshvardh
Firewall - Microsoft PowerPoint
You are sharing your entire screen.
Stop Sharing
Advantages
Performance is good
Very fast
Relatively inexpensive.
Transparent to users
The traffic management is good
Simplicity
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
Click to add notes
Slide 11 of 39
Type here to search
+79



1K	1M	1K	1V
Vinod	141903010 Kajal Naray	111803166 Rutvik Gane	111803064 Onkar Datta	111803105 Harshvardh

Firewall - Microsoft PowerPoint

Home Insert Design Animations Slide Show Review View

You are sharing your entire screen. Stop Sharing

Slides Outline

10 • Simplest of components
• Uses transport-layer information only
– IP Source Address, Destination Address
– Protocol/Next Header (TCP, UDP, ICMP, etc)
– TCP or UDP source & destination ports
– TCP Flags (SYN, ACK, FIN, RST, PSH, etc)
• Examples
– DNS uses port 53

11 **Advantages**
• Performance is good
• Very fast
• Relatively inexpensive
• Transparent to users
• The traffic management is good
• Simplicity

12 **Disadvantages**
• Direct connections are allowed between untrusted and trusted hosts
• Vulnerable to spoofing attacks
• Poor scalability
• Large port ranges may be opened

13 • Most of these firewalls do not support advanced user authentication schemes
• Due to improper configuration it is susceptible to security breaches

14 **Attacks Against Packet Filtering**
• IP ADDRESS SPOOFING
• SOURCE ROUTING ATTACKS
• TINY FRAGMENT ATTACKS

Disadvantages

- Direct connections are allowed between untrusted and trusted hosts
- Vulnerable to spoofing attacks
- Poor scalability
- Large port ranges may be opened

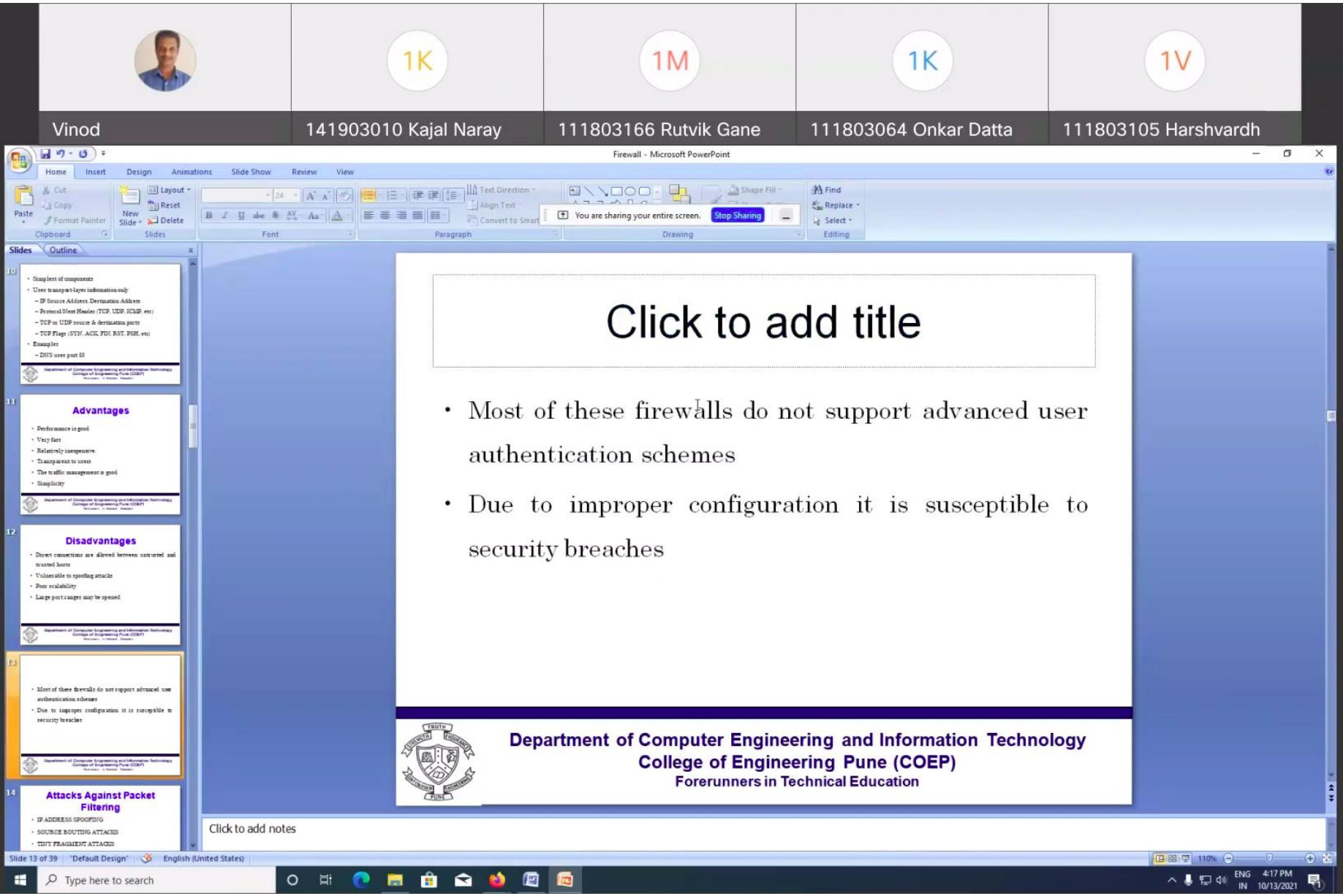
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Click to add notes

Slide 12 of 39 "Default Design" English (United States) 110%

Type here to search ENG IN 4:16 PM 10/13/2021

+79


Vinod
1K
141903010 Kajal Naray
1M
111803166 Rutvik Gane
1K
111803064 Onkar Datta
1V
111803105 Harshvardh
Firewall - Microsoft PowerPoint
You are sharing your entire screen.
Stop Sharing
Click to add title
Most of these firewalls do not support advanced user authentication schemes
Due to improper configuration it is susceptible to security breaches
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
Click to add notes
Advantages
Performance is good
Very fast
Relatively inexpensive
Transparent to users
The traffic management is good
Simplicity
Disadvantages
Direct connections are allowed between untrusted and trusted hosts
Vulnerable to spoofing attacks
Poor scalability
Large port ranges may be opened
Attacks Against Packet Filtering
IP ADDRESS SPOOFING
SOURCE ROUTING ATTACKS
TINY FRAGMENT ATTACKS
Slide 13 of 39
"Default Design"
English (United States)
Type here to search
ENG IN
4:17 PM
10/13/2021
+78

1K	1M	1K	1V
Vinod	141903010 Kajal Naray	111803166 Rutvik Gane	111803064 Onkar Datta	111803105 Harshvardh

Firewall - Microsoft PowerPoint

Home Insert Design Animations Slide Show Review View

You are sharing your entire screen. Stop Sharing

Slides Outline

13 Attacks Against Packet Filtering
- IP ADDRESS SPOOFING
- SOURCE ROUTING ATTACKS
- TINY FRAGMENT ATTACKS

15 IP Address Spoofing
- The attackers put the internal address as a source address
- He believes that due to this spoof address, the firewall assumes that this packet is from trusted internal host and allow to pass that packet.

16 Countermeasure
- If the packet coming from outside and has the IP address of the internal host, then discard such packet. This is implemented at the router which is external to the firewall.

17 Source Routing Attacks
- Attacks assume that the source routing information is not analyzed so the route of a packet across the Internet is specifies by the source

18 Countermeasure
- Discard the packets which use this option

Attacks Against Packet Filtering

- IP ADDRESS SPOOFING
- SOURCE ROUTING ATTACKS
- TINY FRAGMENT ATTACKS

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

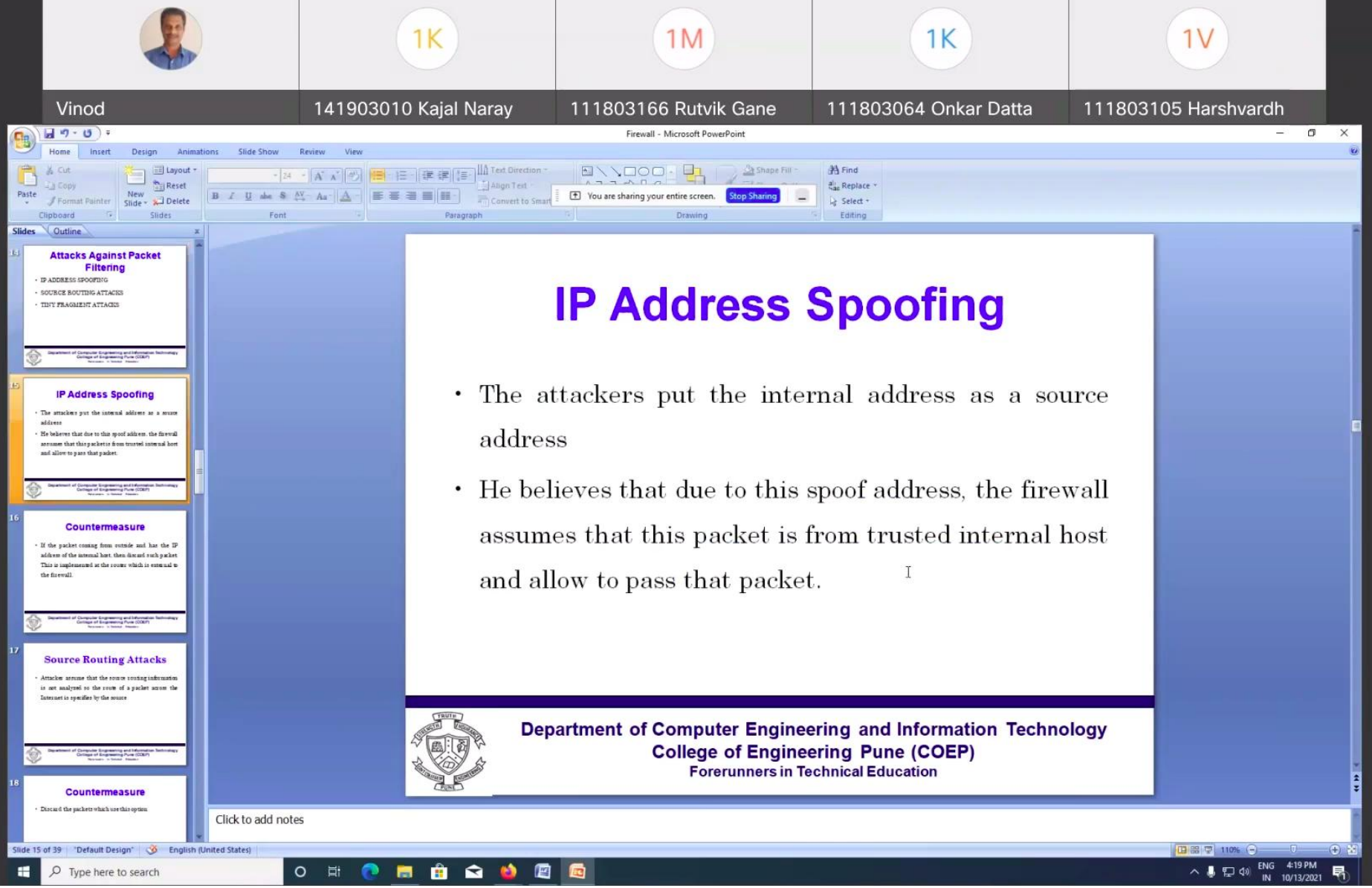
Click to add notes

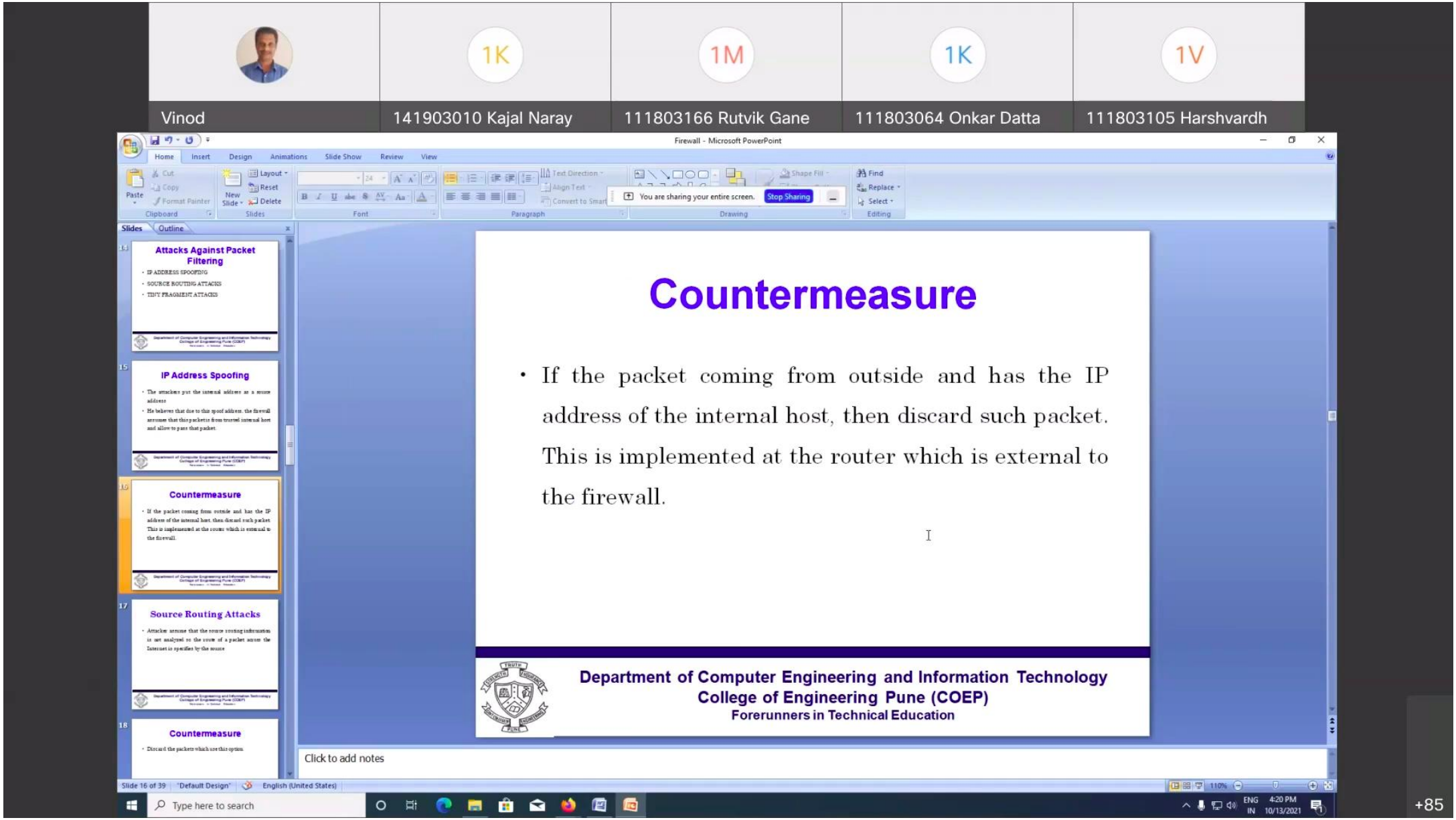
Slide 14 of 39 "Default Design" English (United States) 110%

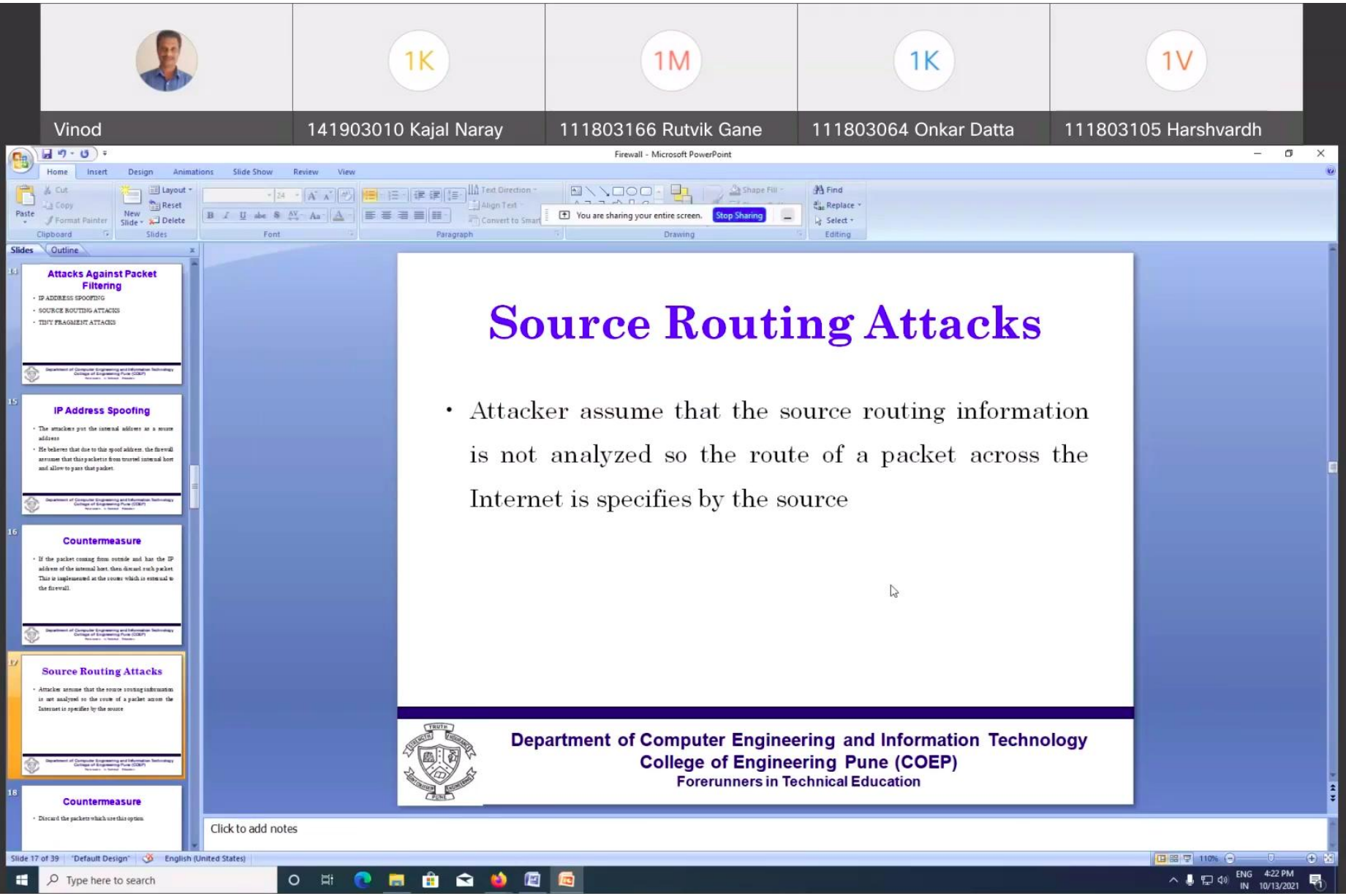
Type here to search

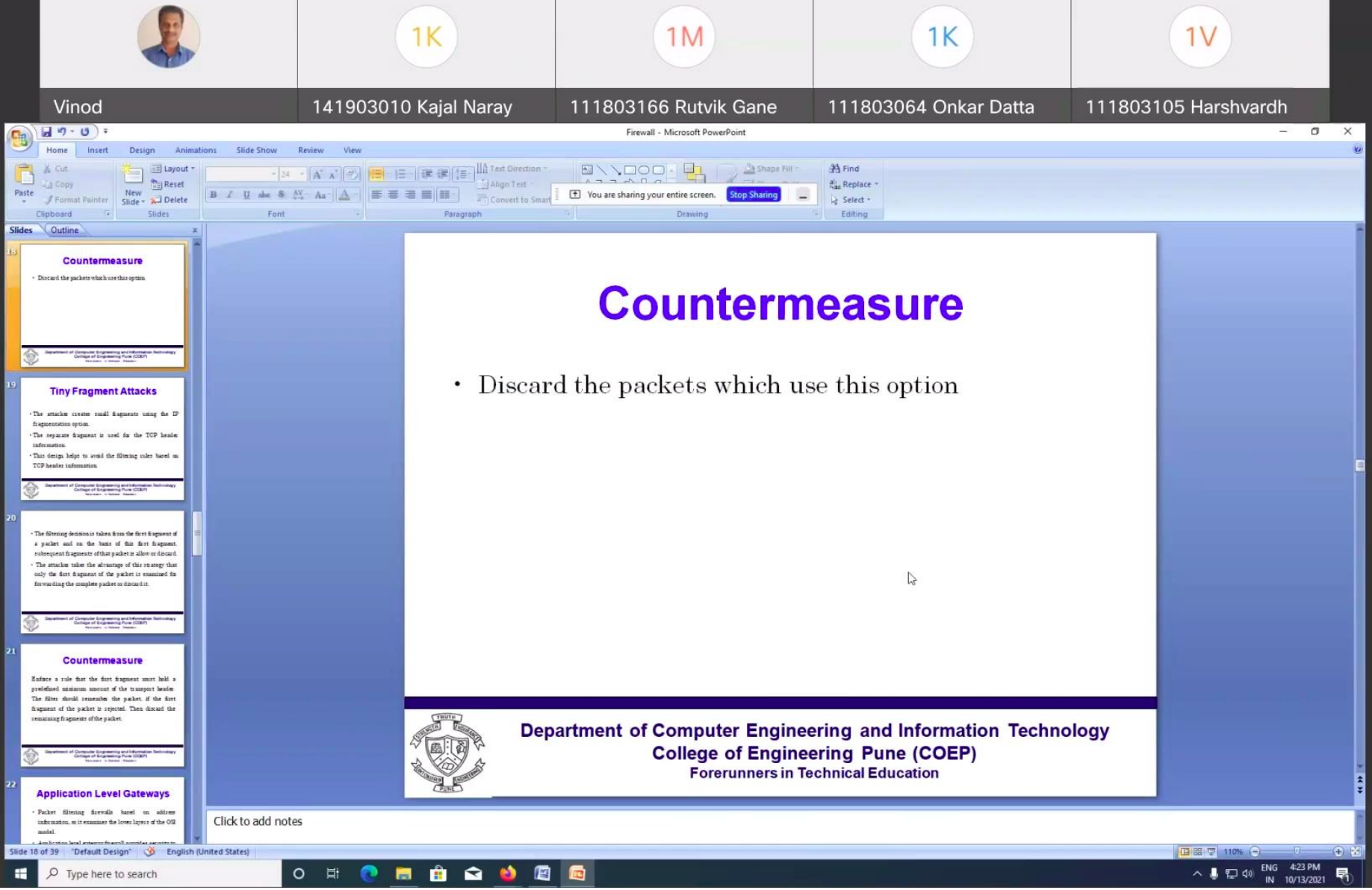
ENG IN 4:18 PM 10/13/2021

+79


Vinod
141903010 Kajal Naray
111803166 Rutvik Gane
111803064 Onkar Datta
111803105 Harshvardh
Firewall - Microsoft PowerPoint
You are sharing your entire screen.
Stop Sharing
Attacks Against Packet Filtering
IP ADDRESS SPOOFING
SOURCE ROUTING ATTACKS
TINY FRAGMENT ATTACKS
IP Address Spoofing
Countermeasure
Source Routing Attacks
Countermeasure
IP Address Spoofing
The attackers put the internal address as a source address
He believes that due to this spoof address, the firewall assumes that this packet is from trusted internal host and allow to pass that packet.
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
Click to add notes
Slide 15 of 39
"Default Design"
English (United States)
Type here to search
+79


Vinod
141903010 Kajal Naray
111803166 Rutvik Gane
111803064 Onkar Datta
111803105 Harshvardh
Firewall - Microsoft PowerPoint
You are sharing your entire screen.
Stop Sharing
Slides
Outline
Attacks Against Packet Filtering
IP ADDRESS SPOOFING
SOURCE ROUTING ATTACKS
TINY FRAGMENT ATTACKS
IP Address Spoofing
Countermeasure
Source Routing Attacks
Countermeasure
Discard the packets which use this option
Countermeasure
If the packet coming from outside and has the IP address of the internal host, then discard such packet. This is implemented at the router which is external to the firewall.
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
Click to add notes
Slide 16 of 39
"Default Design"
English (United States)
Type here to search
ENG
IN
4:20 PM
10/13/2021
+85


Vinod
141903010 Kajal Naray
111803166 Rutvik Gane
111803064 Onkar Datta
111803105 Harshvardh
Firewall - Microsoft PowerPoint
You are sharing your entire screen.
Stop Sharing
Slides
Outline
Attacks Against Packet Filtering
IP ADDRESS SPOOFING
SOURCE ROUTING ATTACKS
TINY FRAGMENT ATTACKS
IP Address Spoofing
Countermeasure
Source Routing Attacks
Countermeasure
Discard the packets which use this option
Source Routing Attacks
Attacker assume that the source routing information is not analyzed so the route of a packet across the Internet is specifies by the source
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
Click to add notes
Slide 17 of 39
"Default Design"
English (United States)
Type here to search
ENG
IN
4:22 PM
10/13/2021
+85


Vinod
141903010 Kajal Naray
111803166 Rutvik Gane
111803064 Onkar Datta
111803105 Harshvardh
Firewall - Microsoft PowerPoint
You are sharing your entire screen.
Stop Sharing
Countermeasure
Discard the packets which use this option
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
Tiny Fragment Attacks
Application Level Gateways
Click to add notes
Slide 18 of 39
English (United States)
Type here to search
+88

1K	1M	1K	1V
Vinod	141903010 Kajal Naray	111803166 Rutvik Gane	111803064 Onkar Datta	111803105 Harshvardh

Firewall - Microsoft PowerPoint

Home Insert Design Animations Slide Show Review View

You are sharing your entire screen. Stop Sharing

Slides Outline

15 **Countermeasure**

- Discard the packets which use this option.

17 **Tiny Fragment Attacks**

- The attacker creates small fragments using the IP fragmentation option.
- The separate fragment is used for the TCP header information.
- This design helps to avoid the filtering rules based on TCP header information.

20

- The filtering decision is taken from the first fragment of a packet and on the basis of this first fragment, subsequent fragments of that packet is allow or discard.
- The attacker takes the advantage of this strategy that only the first fragment of the packet is examined for forwarding the complete packet or discard it.

21 **Countermeasure**

Enforce a rule that the first fragment must hold a predefined minimum amount of the transport header. The filter should remember the packet, if the first fragment of the packet is rejected. Then discard the remaining fragments of the packet.

22 **Application Level Gateways**

- Packet filtering firewalls based on address information, so it examines the lower layers of the OSI model.

Tiny Fragment Attacks

- The attacker creates small fragments using the IP fragmentation option.
- The separate fragment is used for the TCP header information.
- This design helps to avoid the filtering rules based on TCP header information.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

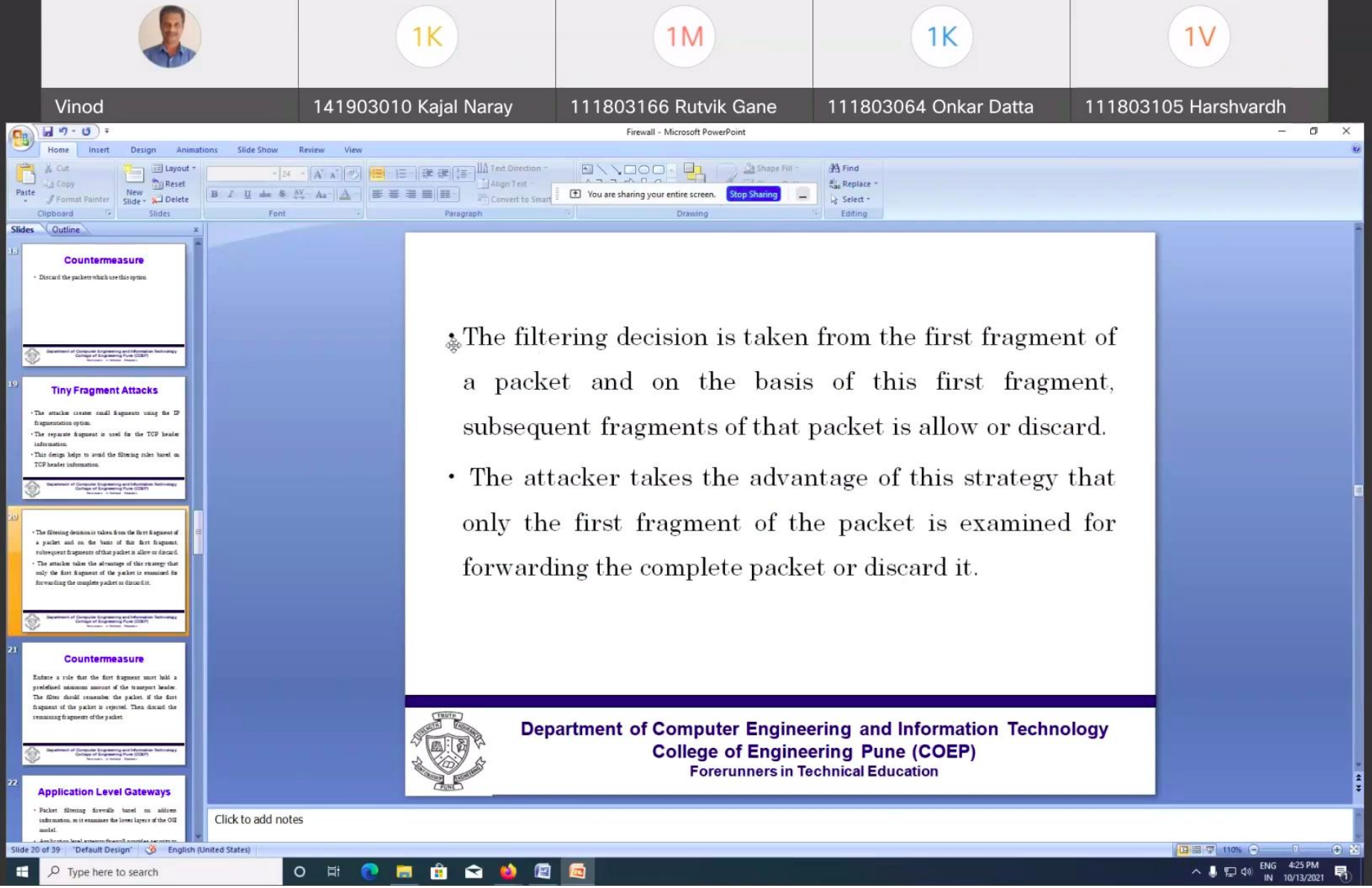
Click to add notes

Slide 19 of 39 "Default Design" English (United States) 110%

Type here to search

ENG IN 4:23 PM 10/13/2021

+88


Vinod
1K
141903010 Kajal Naray
1M
111803166 Rutvik Gane
1K
111803064 Onkar Datta
1V
111803105 Harshvardh
Firewall - Microsoft PowerPoint
You are sharing your entire screen.
Stop Sharing
Countermeasure
Discard the packets which use this option
Tiny Fragment Attacks
The attacker creates small fragments using the IP fragmentation option.
The separate fragment is used for the TCP header information.
This design helps to avoid the filtering rules based on TCP header information.
The filtering decision is taken from the first fragment of a packet and on the basis of this first fragment, subsequent fragments of that packet is allow or discard.
The attacker takes the advantage of this strategy that only the first fragment of the packet is examined for forwarding the complete packet or discard it.
Countermeasure
Enforce a rule that the first fragment must hold a predefined minimum amount of the transport header. The filter should remember the packet, if the first fragment of the packet is rejected. Then discard the remaining fragments of the packet.
Application Level Gateways
Packet filtering firewalls based on address information, so it examines the lower layers of the OSI model.
The filtering decision is taken from the first fragment of a packet and on the basis of this first fragment, subsequent fragments of that packet is allow or discard.
The attacker takes the advantage of this strategy that only the first fragment of the packet is examined for forwarding the complete packet or discard it.
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
Click to add notes
Slide 20 of 39
"Default Design"
English (United States)
Type here to search
ENG
IN
4:25 PM
10/13/2021
+90

1K	1M	1K	1V
Vinod	141903010 Kajal Naray	111803166 Rutvik Gane	111803064 Onkar Datta	111803105 Harshvardh

Firewall - Microsoft PowerPoint

Home Insert Design Animations Slide Show Review View

You are sharing your entire screen. Stop Sharing

Slides Outline

18 **Countermeasure**
- Discard the packets which use this option

19 **Tiny Fragment Attacks**
- The attacker creates small fragments using the IP fragmentation option.
- The separate fragment is used for the TCP header information.
- This design helps to avoid the filtering rules based on TCP header information.

20
- The filtering decision is taken from the first fragment of a packet and on the basis of this first fragment, subsequent fragments of that packet is allow or discard.
- The attacker takes the advantage of this strategy that only the first fragment of the packet is examined for forwarding the complete packet or discard it.

21 **Countermeasure**
Enforce a rule that the first fragment must hold a predefined minimum amount of the transport header. The filter should remember the packet, if the first fragment of the packet is rejected. Then discard the remaining fragments of the packet.

22 **Application Level Gateways**
- Packet filtering firewalls based on address information, so it examines the lower layers of the OSI model.

Countermeasure

Enforce a rule that the first fragment must hold a predefined minimum amount of the transport header. The filter should remember the packet, if the first fragment of the packet is rejected. Then discard the remaining fragments of the packet.

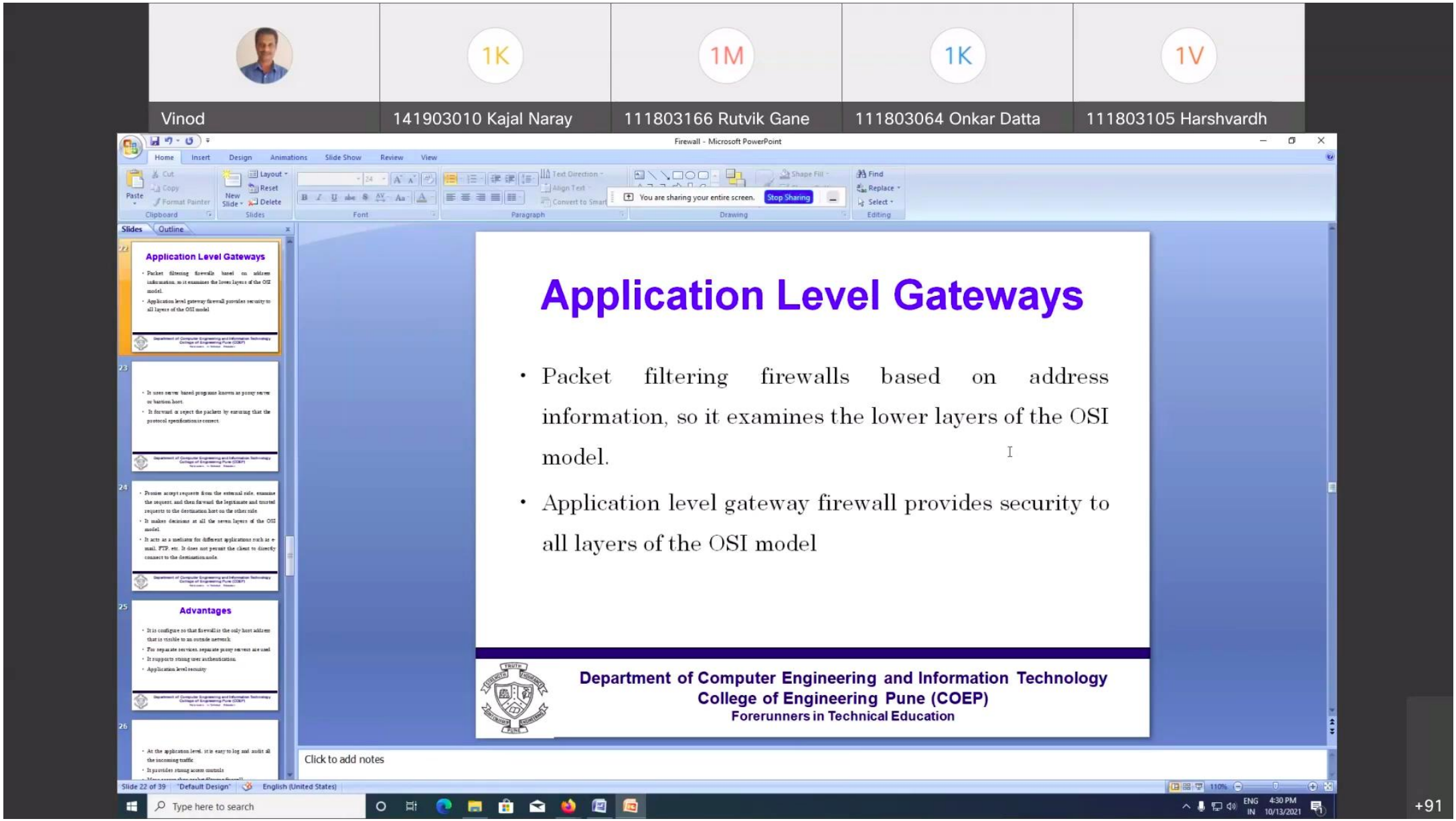
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

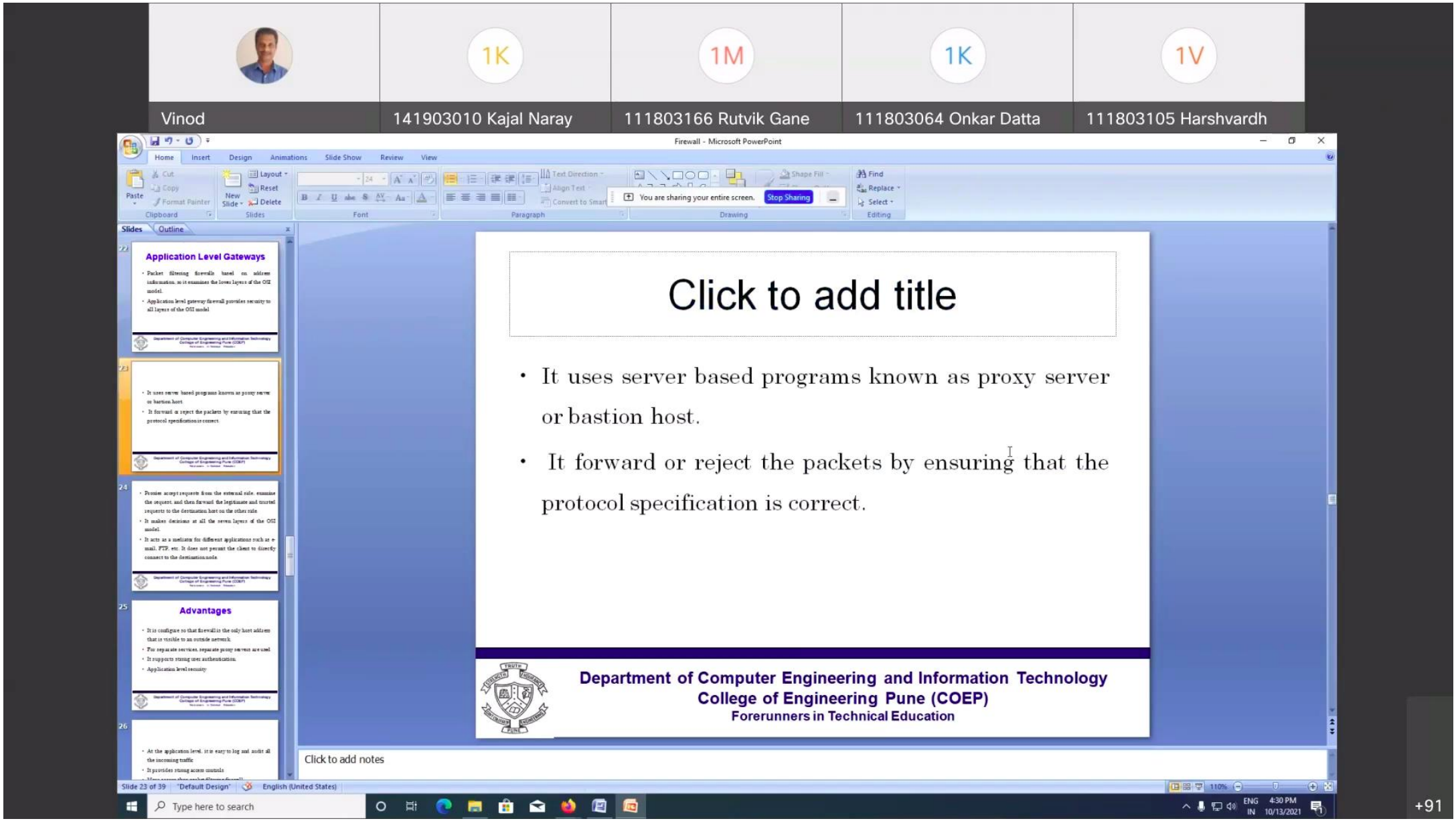
Click to add notes

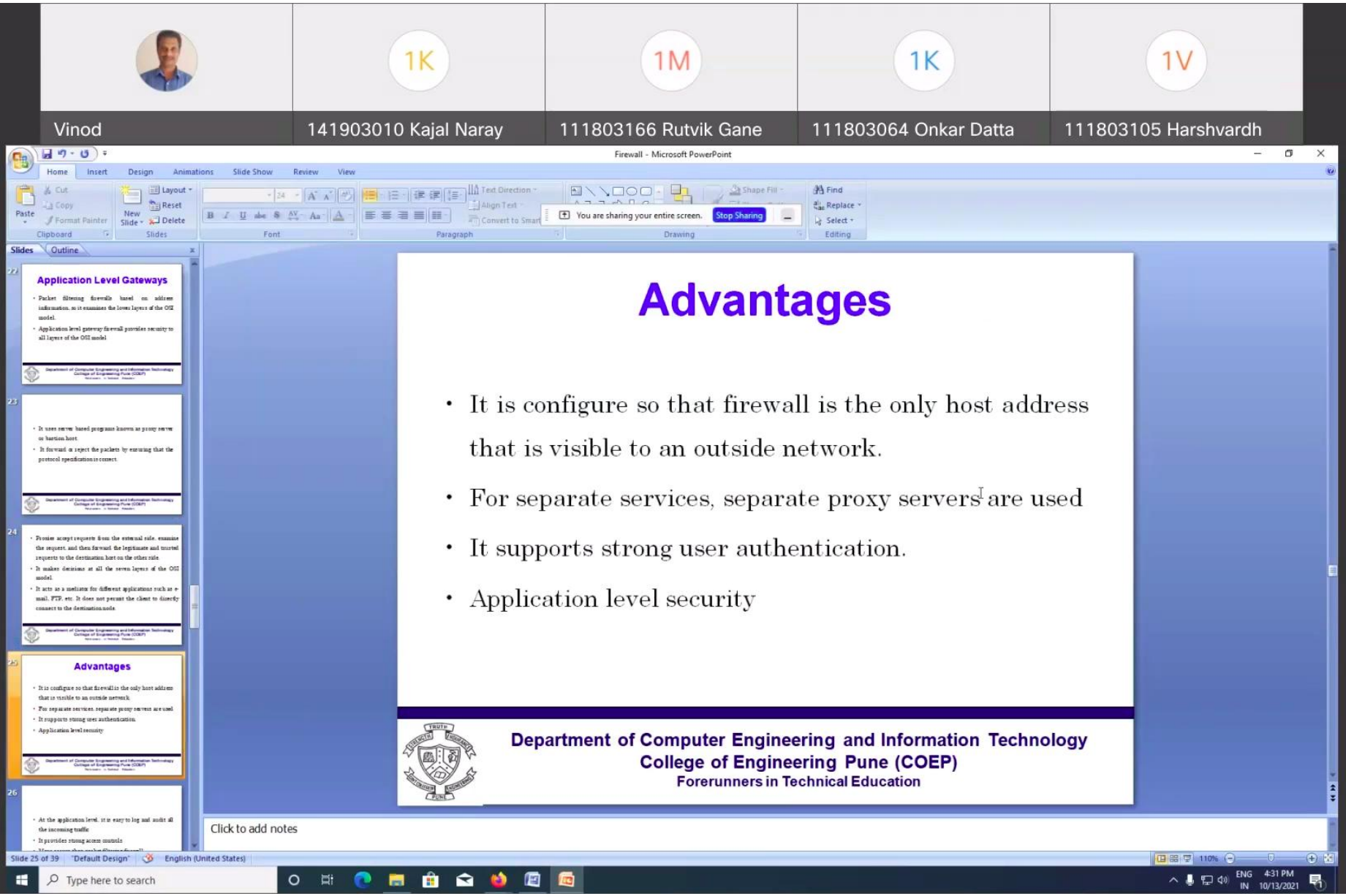
Slide 21 of 39 "Default Design" English (United States) 110%

Type here to search ENG IN 4:26 PM 10/13/2021

+91


Vinod
141903010 Kajal Naray
111803166 Rutvik Gane
111803064 Onkar Datta
111803105 Harshvardh
Firewall - Microsoft PowerPoint
You are sharing your entire screen.
Stop Sharing
Application Level Gateways
Packet filtering firewalls based on address information, so it examines the lower layers of the OSI model.
Application level gateway firewall provides security to all layers of the OSI model
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
Click to add notes
Slide 22 of 39
Type here to search
+91


Vinod
141903010 Kajal Naray
111803166 Rutvik Gane
111803064 Onkar Datta
111803105 Harshvardh
Firewall - Microsoft PowerPoint
You are sharing your entire screen.
Stop Sharing
Slides
Outline
Application Level Gateways
Advantages
Click to add title
It uses server based programs known as proxy server or bastion host.
It forward or reject the packets by ensuring that the protocol specification is correct.
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
Click to add notes
Slide 23 of 39
"Default Design"
English (United States)
Type here to search
+91


Vinod
141903010 Kajal Naray
111803166 Rutvik Gane
111803064 Onkar Datta
111803105 Harshvardh
Firewall - Microsoft PowerPoint
You are sharing your entire screen.
Stop Sharing
Slides
Outline
Application Level Gateways
Advantages
Advantages
It is configure so that firewall is the only host address that is visible to an outside network.
For separate services, separate proxy servers are used
It supports strong user authentication.
Application level security
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
Click to add notes
Slide 25 of 39
"Default Design"
English (United States)
Type here to search
+89

1K	1M	1K	1V
Vinod	141903010 Kajal Naray	111803166 Rutvik Gane	111803064 Onkar Datta	111803105 Harshvardh

Firewall - Microsoft PowerPoint

Home Insert Design Animations Slide Show Review View

You are sharing your entire screen. Stop Sharing

Slides Outline

26
- At the application level, it is easy to log and audit all the incoming traffic
- It provides strong access controls
- More secure than packet filtering firewall

27 **Disadvantages**
- For each application special proxy is required
- Performance is slow
- On each connection there is an additional processing overhead
- Sometimes it is inconvenient faced by the users
- There is lack of transparency

28 **DMZ (Demilitarized Zone)**
- Two types of firewall
  - Internal firewall
  - external firewall

Internal firewalls protect the entire network of an organization.

The external firewall provides basic security to the entire network. An external firewall is installed at the boundary of local or organization network.

29
- It is located inside the boundary router. This region between two firewalls is called demilitarized zone or DMZ.
- Many network devices are located between these two firewalls.
- It includes devices which are allowed to access from external networks.
- These devices can be accessed externally but protected from vulnerability.

30
- The internal firewall provides two-way protection.
- Initially it protects the entire internal network from attacks launched from DMZ systems originate from worms, bots or other malicious software.
- Then the internal firewall protects system located at

Click to add title

- At the application level, it is easy to log and audit all the incoming traffic
- It provides strong access controls
- More secure than packet filtering firewall

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

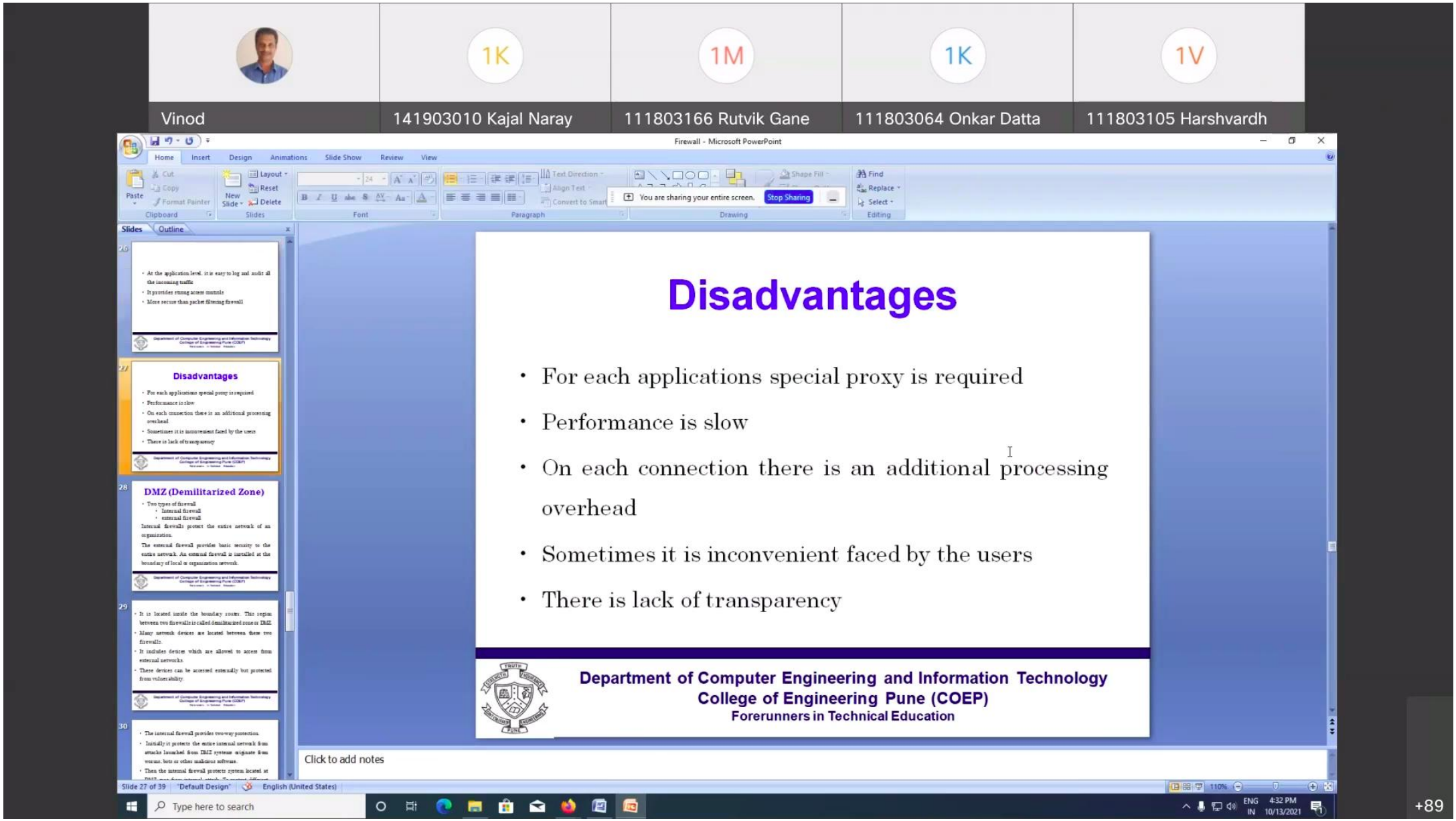
Click to add notes

Slide 26 of 39 "Default Design" English (United States) 110%

Type here to search

ENG IN 4:32 PM 10/13/2021

+89


Vinod
141903010 Kajal Naray
111803166 Rutvik Gane
111803064 Onkar Datta
111803105 Harshvardh
Firewall - Microsoft PowerPoint
You are sharing your entire screen.
Stop Sharing
Disadvantages
For each applications special proxy is required
Performance is slow
On each connection there is an additional processing overhead
Sometimes it is inconvenient faced by the users
There is lack of transparency
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
Click to add notes
Slide 27 of 39
"Default Design"
English (United States)
Type here to search
+89

1K	1M	1K	1V
Vinod	141903010 Kajal Naray	111803166 Rutvik Gane	111803064 Onkar Datta	111803105 Harshvardh

Firewall - Microsoft PowerPoint

Home Insert Design Animations Slide Show Review View

You are sharing your entire screen. Stop Sharing

Slides Outline

26
- At the application level, it is easy to log and audit all the incoming traffic
- It provides strong access controls
- More secure than packet filtering firewall

27 **Disadvantages**
- For each applications special proxy is required
- Performance is slow
- On each connection there is an additional processing overhead
- Sometimes it is inconvenient faced by the users
- There is lack of transparency

28 **DMZ (Demilitarized Zone)**
- Two types of firewall
  - Internal firewall
  - external firewall

Internal firewalls protect the entire network of an organization.

The external firewall provides basic security to the entire network. An external firewall is installed at the boundary of local or organization network.

29
- It is located inside the boundary router. This region between two firewalls is called demilitarized zone or DMZ.
- Many network devices are located between these two firewalls.
- It includes devices which are allowed to access from external networks.
- These devices can be accessed externally but protected from vulnerability.

30
- The internal firewall provides two-way protection.
- Initially it protects the entire internal network from attacks launched from DMZ systems originate from worms, bots or other malicious software.
- Then the internal firewall protects system located at

DMZ (Demilitarized Zone)

- Two types of firewall
  - Internal firewall
  - external firewall

Internal firewalls protect the entire network of an organization.

The external firewall provides basic security to the entire network. An external firewall is installed at the boundary of local or organization network.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Click to add notes

Slide 28 of 39 "Default Design" English (United States) 110%

Type here to search ENG IN 4:33 PM 10/13/2021

+91

1K	1M	1K	1V
Vinod	141903010 Kajal Naray	111803166 Rutvik Gane	111803064 Onkar Datta	111803105 Harshvardh

Firewall - Microsoft PowerPoint

Home Insert Design Animations Slide Show Review View

You are sharing your entire screen. Stop Sharing

Slides Outline

26 · At the application level, it is easy to log and audit all the incoming traffic
· It provides strong access controls
· More secure than packet filtering firewall

27 **Disadvantages**
· For each application special proxy is required
· Performance is slow
· On each connection there is an additional processing overhead
· Sometimes it is inconvenient faced by the users
· There is lack of transparency

28 **DMZ (Demilitarized Zone)**
· Two types of firewall
  · Internal firewall
  · external firewall
Internal firewalls protect the entire network of an organization.
The external firewall provides basic security to the entire network. An external firewall is installed at the boundary of local or organization network

29 · It is located inside the boundary router. This region between two firewalls is called demilitarized zone or DMZ.
· Many network devices are located between these two firewalls.
· It includes devices which are allowed to access from external networks.
· These devices can be accessed externally but protected from vulnerability.

30 · The internal firewall provides two-way protection.
· Initially it protects the entire internal network from attacks launched from DMZ systems originate from worms, bots or other malicious software.
· Then the internal firewall protects system located at

- It is located inside the boundary router. This region between two firewalls is called demilitarized zone or DMZ.
- Many network devices are located between these two firewalls.
- It includes devices which are allowed to access from external networks.
- These devices can be accessed externally but protected from vulnerability.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Click to add notes

Slide 29 of 39 "Default Design" English (United States) 110%

Type here to search ENG IN 4:34 PM 10/13/2021

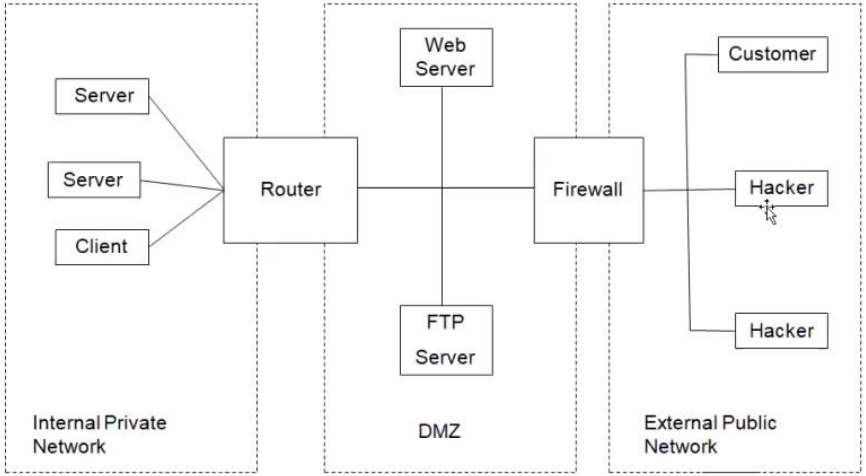
+92

Vinod	141903010 Kajal Naray	111803166 Rutvik Gane	111803064 Onkar Datta	111803155 VIREN RAJE

Firewall - Microsoft PowerPoint

You are sharing your entire screen. Stop Sharing

DMZ



Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Click to add notes

Slide 31 of 39 "Default Design" English (United States)

Type here to search

ENG IN 4:36 PM 10/13/2021

+92

1K	1M	1K	1P
Vinod	141903010 Kajal Naray	111803166 Rutvik Gane	111803064 Onkar Datta	111803155 VIREN RAJE

Firewall - Microsoft PowerPoint

Home Insert Design Animations Slide Show Review View

You are sharing your entire screen. Stop Sharing

Slides Outline

30

- The internal firewall provides two-way protection.
- Initially it protects the entire internal network from attacks launched from DMZ systems originate from worms, bots or other malicious software.
- Then the internal firewall protects system located at DMZ area from internal attack. To protect different portions of the large network from each other, multiple internal firewalls are used.

31

DMZ

32

Circuit Level Gateways

- Stand-alone system
- It validates connections and then allows the data to be exchanged.
- They also work as per defined rules similar to packet filter.
- Circuit level gateways cannot route the packets.

33

- The connections are allowed or discard based on these rules. So circuit level gateways establishes the connections between the source and the destinations. It focuses on the TCP/IP layer.
- This firewall is installed between the router and the external network such as Internet. The actual address is hidden from the external users because only the address of the proxy is transmitted.

34

Circuit Level Gateways

- Stand-alone system
- It validates connections and then allows the data to be exchanged.
- They also work as per defined rules similar to packet filter.
- Circuit level gateways cannot route the packets.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Click to add notes

Slide 32 of 39 "Default Design" English (United States) 110%

Type here to search ENG IN 4:37 PM 10/13/2021

+94

1K	1M	1K	1P
Vinod	141903010 Kajal Naray	111803166 Rutvik Gane	111803064 Onkar Datta	111803155 VIREN RAJE

Firewall - Microsoft PowerPoint

Home Insert Design Animations Slide Show Review View

You are sharing your entire screen. Stop Sharing

Slides Outline

30

- The internal firewall provides two-way protection.
- Initially it protects the entire internal network from attacks launched from DMZ systems originate from worms, bots or other malicious software.
- Then the internal firewall protects system located at DMZ area from internal attack. To protect different portions of the large network from each other, multiple internal firewalls are used.

31

DMZ

32

Circuit Level Gateways

- Stand-alone system
- It validates connections and then allows the data to be exchanged.
- They also work as per defined rules similar to packet filter.
- Circuit level gateways cannot route the packets.

33

- The connections are allowed or discard based on these rules. So circuit level gateways establishes the connections between the source and the destinations. It focuses on the TCP/IP layer.
- This firewall is installed between the router and the external network such as Internet. The actual address is hidden from the external users because only the address of the proxy is transmitted.

34

- The connections are allowed or discard based on these rules. So circuit level gateways establishes the connections between the source and the destinations. It focuses on the TCP/IP layer.
- This firewall is installed between the router and the external network such as Internet. The actual address is hidden from the external users because only the address of the proxy is transmitted.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Click to add notes

Slide 33 of 39 "Default Design" English (United States) 110%

32:04 / 35:42

	1K	1M	1K	1P
Vinod	141903010 Kajal Naray	111803166 Rutvik Gane	111803064 Onkar Datta	111803155 VIREN RAJE

+94

1K	1M	1K	1P
Vinod	141903010 Kajal Naray	111803166 Rutvik Gane	111803064 Onkar Datta	111803155 VIREN RAJE

Firewall - Microsoft PowerPoint

Advantages

- Transparent to users
- Excellent for relaying outbound traffic

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Click to add notes

Slide 35 of 39 "Default Design" English (United States)

+94

Vinod	141903010 Kajal Naray	111803166 Rutvik Gane	111803064 Onkar Datta	111803155 VIREN RAJE

Firewall - Microsoft PowerPoint

Home Insert Design Animations Slide Show Review View

You are sharing your entire screen. Stop Sharing

Slides Outline

34

35 **Advantages**

- Transparent to users
- Excellent for relaying outbound traffic

36 **Disadvantages**

- Slower than packet filtering firewall
- Inbound traffic is risky

37 **Benefits of a Firewall**

- Increased ability to enforce network security standards/policies
- Centralization of intra-network audit capability (audit of in/out-bound traffic)

38 **Limitations of a Firewall**

- It cannot protect those attacks that bypass the firewall.
- It cannot protect the network against the internal

Disadvantages

- Slower than packet filtering firewall
- Inbound traffic is risky

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Click to add notes

Slide 36 of 39 "Default Design" English (United States) 110%

Type here to search ENG IN 4:38 PM 10/13/2021

+94

1K	1M	1K	1P
Vinod	141903010 Kajal Naray	111803166 Rutvik Gane	111803064 Onkar Datta	111803155 VIREN RAJE

Firewall - Microsoft PowerPoint

Home Insert Design Animations Slide Show Review View

You are sharing your entire screen. Stop Sharing

Slides Outline

34

35 **Advantages**

- Transparent to users
- Excellent for relaying outbound traffic

36 **Disadvantages**

- Slower than packet filtering firewall
- Inbound traffic is risky

37 **Benefits of a Firewall**

- Increased ability to enforce network security standards/policies
- Centralization of inter-network audit capability (audit of in/out-bound traffic)

38 **Limitations of a Firewall**

- It cannot protect those attacks that bypass the firewall.
- It cannot protect the network against the internal

Benefits of a Firewall

- Increased ability to enforce network security standards/policies
- Centralization of inter-network audit capability (audit of in/out-bound traffic)

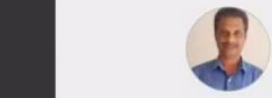
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Click to add notes

Slide 37 of 39 "Default Design" English (United States) 110%

Type here to search ENG IN 4:38 PM 10/13/2021

+94



1K	1M	1K	1P
Vinod	141903010 Kajal Naray	111803166 Rutvik Gane	111803064 Onkar Datta	111803155 VIREN RAJE

Firewall - Microsoft PowerPoint

Home Insert Design Animations Slide Show Review View

You are sharing your entire screen. Stop Sharing

Slides Outline

36 **Disadvantages**
- Slower than packet filtering firewall
- Inbound traffic is risky

37 **Benefits of a Firewall**
- Increased ability to enforce network security standards/policies
- Centralization of inter-network audit capability (audit of in/out-bound traffic)

38 **Limitations of a Firewall**
- It cannot protect those attacks that bypass the firewall.
- It cannot protect the network against the internal attacks.

39
- An internal firewall that separates the different parts of an network cannot protect against wireless communications among local computer systems on different sides of the internal firewall.
- Different devices such as laptop or portable storage device may be used and infected outside the network, and then used internally.

Limitations of a Firewall

- It cannot protect those attacks that bypass the firewall.
- It cannot protect the network against the internal attacks.

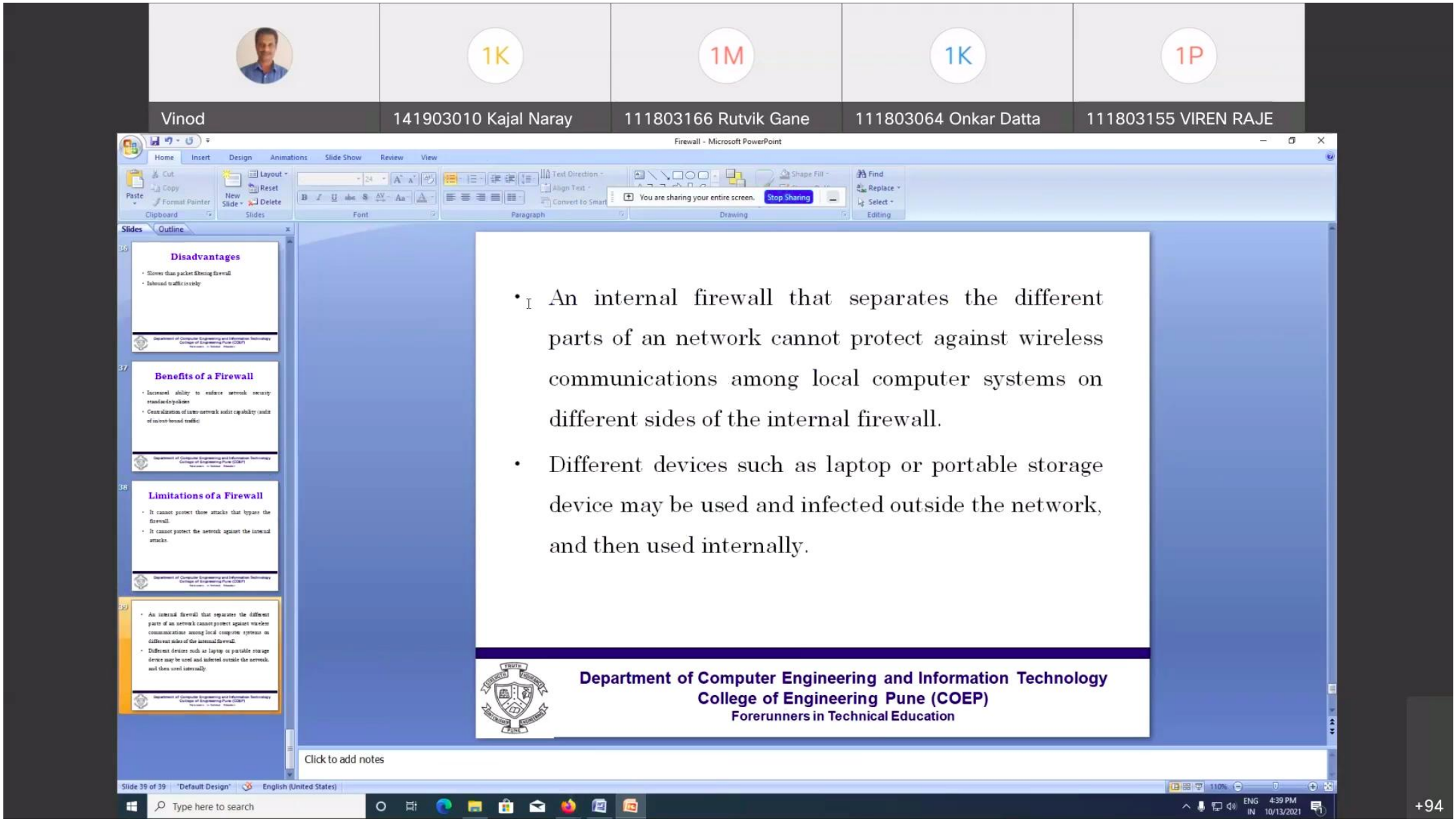
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Click to add notes

Slide 38 of 39 "Default Design" English (United States) 110%

Type here to search ENG IN 4:38 PM 10/13/2021

+94


Vinod
141903010 Kajal Naray
111803166 Rutvik Gane
111803064 Onkar Datta
111803155 VIREN RAJE
Firewall - Microsoft PowerPoint
You are sharing your entire screen.
Stop Sharing
Slides
Outline
Disadvantages
Benefits of a Firewall
Limitations of a Firewall
An internal firewall that separates the different parts of an network cannot protect against wireless communications among local computer systems on different sides of the internal firewall.
Different devices such as laptop or portable storage device may be used and infected outside the network, and then used internally.
Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education
Click to add notes
Slide 39 of 39
"Default Design"
English (United States)
Type here to search
+94

Vinod | 1C | 111803068 Kush Vijay | 1T | 111803133 Runal Rame | 1D | 111803111 Atharva Kail | 1N | 111803141 Rushikesh

IDS.pdf - Adobe Acrobat Reader DC (64-bit)

File Edit View Sign Window Help

Home Tools IDS.pdf TCP-IP-Attacks.pdf Sign In

2 / 21 111%

Intrusion

- An intrusion is a deliberate, unauthorized attempt to access or manipulate information or system and to render them unreliable or unusable.
- Intruders may be from outside the network or legitimate users of the network.
- Intrusion can be a physical, system or remote intrusion.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Search 'Insert Page'

Export PDF

Adobe Export PDF

Convert PDF Files to Word or Excel Online

Select PDF File

IDS.pdf

Convert to

Microsoft Word (*.docx)

Document Language: English (U.S.) Change

Convert

Edit PDF

Create PDF

Comment

Combine Files

Organize Pages

Compress PDF

Create, edit, and e-sign PDF forms & agreements

Free 7-Day Trial

+45

Vinod | 1C | 111803068 Kush Vijay | 1T | 111803133 Runal Rame | 1D | 111803111 Atharva Kail | 1N | 111803141 Rushikesh

IDS.pdf - Adobe Acrobat Reader DC (64-bit)

File Edit View Sign Window Help

Home Tools IDS.pdf TCP-IP-Attacks.pdf Sign In

3 / 21 111%

Intruders

- Significant issue for networked systems is hostile or unwanted access
- either via network or local
- can identify classes of intruders:
  - **Masquerader-** An individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account

+50

Vinod | 1C | 111803068 Kush Vijay | 1T | 111803133 Runal Rame | 1D | 111803111 Atharva Kail | 1N | 111803141 Rushikesh

IDS.pdf - Adobe Acrobat Reader DC (64-bit)

File Edit View Sign Window Help

Home Tools IDS.pdf TCP-IP-Attacks.pdf Sign In

4 / 21 111%

– **Misfeasor**: A legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuse his/her privileges.

– **clandestine user**: An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection.

+56

Vinod | 1C | 111803068 Kush Vijay | 1T | 111803133 Runal Rame | 1D | 111803111 Atharva Kail | 1N | 111803141 Rushikesh

IDS.pdf - Adobe Acrobat Reader DC (64-bit)

File Edit View Sign Window Help

Home Tools IDS.pdf TCP-IP-Attacks.pdf Sign In

5 / 21 111%

Jargon Related to IDS

- False Negative:

  False negatives are any alert that should have happened but didn't. Attack ->Normal

- False Positive:

  False positive is any normal or expected behavior that is identified as anomalous or malicious

  Normal->Attack

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Search 'Insert Page'

Export PDF

Adobe Export PDF

Convert PDF Files to Word or Excel Online

Select PDF File

IDS.pdf

Convert to

Microsoft Word (*.docx)

Document Language: English (U.S.) Change

Convert

Edit PDF

Create PDF

Comment

Combine Files

Organize Pages

Compress PDF

Create, edit, and e-sign PDF forms & agreements

Free 7-Day Trial

12:41 / 59:59

Vinod | 1C | 111803068 Kush Vijay | 1T | 111803133 Runal Rame | 1D | 111803111 Atharva Kail | 1N | 111803141 Rushikesh

IDS.pdf - Adobe Acrobat Reader DC (64-bit)

File Edit View Sign Window Help

Home Tools IDS.pdf TCP-IP-Attacks.pdf Sign In

6 / 21 111%

Intrusion Detection Systems (IDS)

Intrusion Detection Systems look for attack signatures, which are specific patterns that usually indicate malicious or suspicious intent.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Search 'Insert Page'

Export PDF

Adobe Export PDF

Convert PDF Files to Word or Excel Online

Select PDF File

IDS.pdf

Convert to

Microsoft Word (*.docx)

Document Language: English (U.S.) Change

Convert

Edit PDF

Create PDF

Comment

Combine Files

Organize Pages

Compress PDF

Create, edit, and e-sign PDF forms & agreements

Free 7-Day Trial

+74

Vinod | 1C | 111803068 Kush Vijay | 1T | 111803133 Runal Rame | 1D | 111803111 Atharva Kail | 1N | 111803141 Rushikesh

IDS.pdf - Adobe Acrobat Reader DC (64-bit)

File Edit View Sign Window Help

Home Tools IDS.pdf TCP-IP-Attacks.pdf Sign In

7 / 21 111%

Types of IDS

- Anomaly detection
- Signature based (misuse)
- Host based
- Network based

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Search 'Insert Page'

Export PDF

Adobe Export PDF

Convert PDF Files to Word or Excel Online

Select PDF File

IDS.pdf

Convert to

Microsoft Word (*.docx)

Document Language: English (U.S.) Change

Convert

Edit PDF

Create PDF

Comment

Combine Files

Organize Pages

Compress PDF

Create, edit, and e-sign PDF forms & agreements

Free 7-Day Trial

18:01 / 59:59

Vinod | 1C | 111803068 Kush Vijay | 1T | 111803133 Runal Rame | 1D | 111803111 Atharva Kail | 1N | 111803141 Rushikesh

IDS.pdf - Adobe Acrobat Reader DC (64-bit)

File Edit View Sign Window Help

Home Tools IDS.pdf TCP-IP-Attacks.pdf Sign In

8 / 21 111%

Anomaly based IDS

- Anomaly-Based IDS examines ongoing traffic, activity, transactions and behavior in order to identify intrusions by detecting anomalies.
- This IDS models the normal usage of the network as a noise characterization.
- Anything distinct from the noise is assumed to be an intrusion activity. E.g flooding a host with lots of packet.
- The primary strength is its ability to recognize novel attacks.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Search 'Insert Page'

Export PDF

Adobe Export PDF

Convert PDF Files to Word or Excel Online

Select PDF File

IDS.pdf

Convert to

Microsoft Word (*.docx)

Document Language: English (U.S.) Change

Convert

Edit PDF

Create PDF

Comment

Combine Files

Organize Pages

Compress PDF

Create, edit, and e-sign PDF forms & agreements

Free 7-Day Trial

+82

Vinod | 1C | 111803068 Kush Vijay | 1T | 111803133 Runal Rame | 1D | 111803111 Atharva Kail | 1N | 111803141 Rushikesh

IDS.pdf - Adobe Acrobat Reader DC (64-bit)

File Edit View Sign Window Help

Home Tools IDS.pdf TCP-IP-Attacks.pdf Sign In

9 / 21 111%

Drawbacks

- Assumes that intrusions will be accompanied by manifestations that are sufficiently unusual so as to permit detection.
- These generate many false alarms and hence compromise the effectiveness of the IDS.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Search 'Insert Page'

Export PDF

Adobe Export PDF

Convert PDF Files to Word or Excel Online

Select PDF File

IDS.pdf

Convert to

Microsoft Word (*.docx)

Document Language: English (U.S.) Change

Convert

Edit PDF

Create PDF

Comment

Combine Files

Organize Pages

Compress PDF

Create, edit, and e-sign PDF forms & agreements

Free 7-Day Trial

22:23 / 59:59

Vinod | 1C | 111803068 Kush Vijay | 1T | 111803133 Runal Rame | 1D | 111803111 Atharva Kail | 1N | 111803141 Rushikesh

IDS.pdf - Adobe Acrobat Reader DC (64-bit)

File Edit View Sign Window Help

Home Tools IDS.pdf TCP-IP-Attacks.pdf Sign In

10 / 21 111%

Signature based IDS

- Signature-Based IDS use a rule set to identify intrusions by watching for patterns of events specific to known and documented attacks.
- It is typically connected to a large database which houses attack signatures.
- It compares the information it gathers against those attack signatures to detect a match.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Search 'Insert Page'

Export PDF

Adobe Export PDF

Convert PDF Files to Word or Excel Online

Select PDF File

IDS.pdf

Convert to

Microsoft Word (*.docx)

Document Language: English (U.S.) Change

Convert

Edit PDF

Create PDF

Comment

Combine Files

Organize Pages

Compress PDF

Create, edit, and e-sign PDF forms & agreements

Free 7-Day Trial

23:23 / 59:59

Vinod | 1C | 111803068 Kush Vijay | 1T | 111803133 Runal Rame | 1D | 111803111 Atharva Kail | 1N | 111803141 Rushikesh

IDS.pdf - Adobe Acrobat Reader DC (64-bit)

File Edit View Sign Window Help

Home Tools IDS.pdf TCP-IP-Attacks.pdf Sign In

11 / 21 111%

Signature based IDS

- These IDS are normally presumed to be able to detect only attacks "known" to its database.
- Thus, if the database is not updated with regularity, new attacks could slip through.
- It can, however, detect new attacks that share characteristics with old attacks,
- In cases of new, uncataloged attacks, this technique is pretty porous.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Search 'Insert Page'

Export PDF

Adobe Export PDF

Convert PDF Files to Word or Excel Online

Select PDF File

IDS.pdf

Convert to

Microsoft Word (*.docx)

Document Language: English (U.S.) Change

Convert

Edit PDF

Create PDF

Comment

Combine Files

Organize Pages

Compress PDF

Create, edit, and e-sign PDF forms & agreements

Free 7-Day Trial

25:21 / 59:59

Vinod | 1C | 111803068 Kush Vijay | 1T | 111803133 Runal Rame | 1D | 111803111 Atharva Kail | 1N | 111803141 Rushikesh

IDS.pdf - Adobe Acrobat Reader DC (64-bit)

File Edit View Sign Window Help

Home Tools IDS.pdf TCP-IP-Attacks.pdf Sign In

12 / 21 111%

Drawbacks of Signature based IDS

- They are unable to detect novel attacks.
- Suffer from false alarms
- Have to programmed again for every new pattern to be detected.
- Also, it may affect performance in cases when intrusion patterns match several attack signatures

Search 'Insert Page'

Export PDF

Adobe Export PDF

Convert PDF Files to Word or Excel Online

Select PDF File

IDS.pdf

Convert to

Microsoft Word (*.docx)

Document Language: English (U.S.) Change

Convert

Edit PDF

Create PDF

Comment

Combine Files

Organize Pages

Compress PDF

Create, edit, and e-sign PDF forms & agreements

Free 7-Day Trial

+92

Vinod | 1C | 111803068 Kush Vijay | 1T | 111803133 Runal Rame | 1D | 111803111 Atharva Kail | 1N | 111803141 Rushikesh

IDS.pdf - Adobe Acrobat Reader DC (64-bit)

File Edit View Sign Window Help

Home Tools IDS.pdf TCP-IP-Attacks.pdf Sign In

13 / 21 111%

Host based IDS

- IDS is installed on a host in the network.
- It collects and analyzes the traffic that is originated or is intended to that host.
- HIDS leverages their privileged access to monitor specific components of a host that are not readily accessible to other systems.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Search 'Insert Page'

Export PDF

Adobe Export PDF

Convert PDF Files to Word or Excel Online

Select PDF File

IDS.pdf

Convert to

Microsoft Word (*.docx)

Document Language: English (U.S.) Change

Convert

Edit PDF

Create PDF

Comment

Combine Files

Organize Pages

Compress PDF

Create, edit, and e-sign PDF forms & agreements

Free 7-Day Trial

28:23 / 59:59

Vinod | 1C | 111803068 Kush Vijay | 1T | 111803133 Runal Rame | 1D | 111803111 Atharva Kail | 1N | 111803141 Rushikesh

IDS.pdf - Adobe Acrobat Reader DC (64-bit)

File Edit View Sign Window Help

Home Tools IDS.pdf TCP-IP-Attacks.pdf Sign In

14 / 21 111%

- These audit information includes events like the use of identification and authentication mechanisms (logins etc.), file opens and program executions, admin activities etc.
- This audit is then analyzed to detect trails of intrusion.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Search 'Insert Page'

Export PDF

Adobe Export PDF

Convert PDF Files to Word or Excel Online

Select PDF File

IDS.pdf

Convert to

Microsoft Word (*.docx)

Document Language: English (U.S.) Change

Convert

Edit PDF

Create PDF

Comment

Combine Files

Organize Pages

Compress PDF

Create, edit, and e-sign PDF forms & agreements

Free 7-Day Trial

+94

Vinod | 1C | 111803068 Kush Vijay | 1T | 111803133 Runal Rame | 1D | 111803111 Atharva Kail | 1N | 111803141 Rushikesh

IDS.pdf - Adobe Acrobat Reader DC (64-bit)

File Edit View Sign Window Help

Home Tools IDS.pdf TCP-IP-Attacks.pdf Sign In

15 / 21 111%

Strengths of the host based IDS

- Attack verification
- System specific activity
- Encrypted and switch environments
- Monitoring key components
- Near Real-Time detection and response.
- No additional hardware

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Search 'Insert Page'

Export PDF

Adobe Export PDF

Convert PDF Files to Word or Excel Online

Select PDF File

IDS.pdf

Convert to

Microsoft Word (*.docx)

Document Language: English (U.S.) Change

Convert

Edit PDF

Create PDF

Comment

Combine Files

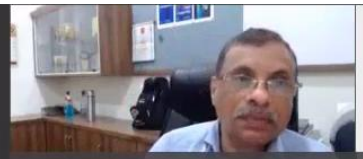
Organize Pages

Compress PDF

Create, edit, and e-sign PDF forms & agreements

Free 7-Day Trial

29:00 / 59:59



Vinod | 1C | 111803068 Kush Vijay | 1T | 111803133 Runal Rame | 1D | 111803111 Atharva Kail | 1N | 111803141 Rushikesh

IDS.pdf - Adobe Acrobat Reader DC (64-bit)

File Edit View Sign Window Help

Home Tools IDS.pdf TCP-IP-Attacks.pdf Sign In

16 / 21 111%

Drawbacks

- Can not see all network activities
- Running audit mechanisms adds overload to system, performance may be an issue
- Audit trails can take lots of storage
- OS vulnerabilities can undermine the effectiveness of agents
- Escalation of false positive
- Greater deployment and maintenance cost

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Search 'Insert Page'

Export PDF

Adobe Export PDF

Convert PDF Files to Word or Excel Online

Select PDF File

IDS.pdf

Convert to

Microsoft Word (*.docx)

Document Language: English (U.S.) Change

Convert

Edit PDF

Create PDF

Comment

Combine Files

Organize Pages

Compress PDF

Create, edit, and e-sign PDF forms & agreements

Free 7-Day Trial

30:11 / 59:59

Vinod | 1C | 111803068 Kush Vijay | 1T | 111803133 Runal Rame | 1D | 111803111 Atharva Kail | 1N | 111803141 Rushikesh

IDS.pdf - Adobe Acrobat Reader DC (64-bit)

File Edit View Sign Window Help

Home Tools IDS.pdf TCP-IP-Attacks.pdf Sign In

17 / 21 111%

Network based IDS

- Network IDSs (NIDS) are placed in key areas of network infrastructure and monitors the traffic as it flows to other host.
- Unlike HIDS, NIDS have the capability of monitoring the network and detecting the malicious activities intended for that network.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Search 'Insert Page'

Export PDF

Adobe Export PDF

Convert PDF Files to Word or Excel Online

Select PDF File

IDS.pdf

Convert to

Microsoft Word (*.docx)

Document Language: English (U.S.) Change

Convert

Edit PDF

Create PDF

Comment

Combine Files

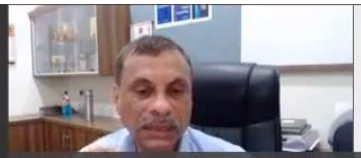
Organize Pages

Compress PDF

Create, edit, and e-sign PDF forms & agreements

Free 7-Day Trial

+94



Vinod | 1C | 111803068 Kush Vijay | 1T | 111803133 Runal Rame | 1D | 111803111 Atharva Kail | 1N | 111803141 Rushikesh

IDS.pdf - Adobe Acrobat Reader DC (64-bit)

File Edit View Sign Window Help

Home Tools IDS.pdf TCP-IP-Attacks.pdf Sign In

18 / 21 111%

Network based IDS

- This IDS looks for attack signatures in network traffic via a promiscuous interface.
- A filter is usually applied to determine which traffic will be discarded or passed on to an attack recognition module. This helps to filter out known un-malicious traffic.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Search 'Insert Page'

Export PDF

Adobe Export PDF

Convert PDF Files to Word or Excel Online

Select PDF File

IDS.pdf

Convert to

Microsoft Word (*.docx)

Document Language: English (U.S.) Change

Convert

Edit PDF

Create PDF

Comment

Combine Files

Organize Pages

Compress PDF

Create, edit, and e-sign PDF forms & agreements

Free 7-Day Trial

32:03 / 59:59

Vinod | 1C | 111803068 Kush Vijay | 1T | 111803133 Runal Rame | 1D | 111803111 Atharva Kail | 1N | 111803141 Rushikesh

IDS.pdf - Adobe Acrobat Reader DC (64-bit)

File Edit View Sign Window Help

Home Tools IDS.pdf TCP-IP-Attacks.pdf Sign In

19 / 21 111%

Strengths

- Can get information quickly without any reconfiguration of computers or need to redirect logging mechanisms
- Does not affect network or data sources
- Monitor and detects in real time networks attacks or misuses
- Does not create system overhead

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Search 'Insert Page'

Export PDF

Adobe Export PDF

Convert PDF Files to Word or Excel Online

Select PDF File

IDS.pdf

Convert to

Microsoft Word (*.docx)

Document Language: English (U.S.) Change

Convert

Edit PDF

Create PDF

Comment

Combine Files

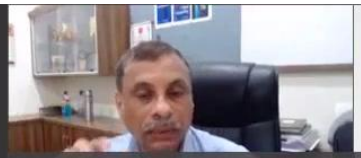
Organize Pages

Compress PDF

Create, edit, and e-sign PDF forms & agreements

Free 7-Day Trial

+93



Vinod | 1C | 111803068 Kush Vijay | 1T | 111803133 Runal Rame | 1D | 111803111 Atharva Kail | 1N | 111803141 Rushikesh

IDS.pdf - Adobe Acrobat Reader DC (64-bit)

File Edit View Sign Window Help

Home Tools IDS.pdf TCP-IP-Attacks.pdf Sign In

20 / 21 111%

Disavantages

- Cannot scan protocols if the data is encrypted
- Can infer from network traffic what is happening on host but cannot tell the outcome
- Hard to implement on fully switched networks
- Has difficulties sustaining network with a very large bandwidth

Vinod | 1C | 111803068 Kush Vijay | 1T | 111803133 Runal Rame | 1D | 111803111 Atharva Kail | 1N | 111803141 Rushikesh

IDS.pdf - Adobe Acrobat Reader DC (64-bit)

File Edit View Sign Window Help

Home Tools IDS.pdf TCP-IP-Attacks.pdf Sign In

21 / 21 111%

Commercial ID Systems

- ISS – Real Secure from Internet Security Systems:
  - Real time IDS.
  - Contains both host and network based IDS.
- Tripwire – File integrity assessment tool.
- Bro and Snort – open source public-domain system.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Search 'Insert Page'

Export PDF

Adobe Export PDF

Convert PDF Files to Word or Excel Online

Select PDF File

IDS.pdf

Convert to

Microsoft Word (*.docx)

Document Language: English (U.S.) Change

Convert

Edit PDF

Create PDF

Comment

Combine Files

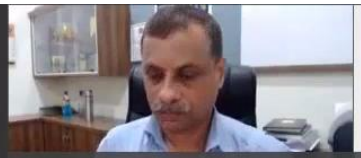
Organize Pages

Compress PDF

Create, edit, and e-sign PDF forms & agreements

Free 7-Day Trial

+94



Vinod | 1N | 111803083 Varun Ajit N | 1Y | 111803147 Aayush Kali | 1C | 141903003 Shravani Sh | 1B | 111803041 Mugdha Pra

TCP-IP-Attacks.pdf - Adobe Acrobat Reader DC (64-bit)

File Edit View Sign Window Help

Home Tools TCP-IP-Attacks.pdf Sign In

Vulnerabilities in TCP/IP model

Dr. V. K. Pachghare

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

1

Export PDF

Adobe Export PDF

Convert PDF Files to Word or Excel Online

Select PDF File

TCP-IP-Attacks.pdf

Convert to

Microsoft Word (*.docx)

Document Language: English (U.S.) Change

Convert

Edit PDF

Create PDF

Comment

Combine Files

Organize Pages

Compress PDF

Create, edit, and e-sign PDF forms & agreements

35:52 / 59:59

Vinod | 1N | 111803083 Varun Ajit N | 1Y | 111803147 Aayush Kali | 1C | 141903003 Shravani Sh | 1B | 111803041 Mugdha Pra

TCP-IP-Attacks.pdf - Adobe Acrobat Reader DC (64-bit)

File Edit View Sign Window Help

Home Tools TCP-IP-Attacks.pdf Sign In

Introduction

- The TCP/IP protocol suite was created
  - as an internetworking solution (with little or no regard to security aspects.)
  - The development of TCP/IP protocol suite was focused on creating a communication protocol standard that can interoperate between different hardware devices and software independently.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Export PDF

Adobe Export PDF

Convert PDF Files to Word or Excel Online

Select PDF File

TCP-IP-Attacks.pdf

Convert to

Microsoft Word (*.docx)

Document Language: English (U.S.) Change

Convert

Edit PDF

Create PDF

Comment

Combine Files

Organize Pages

Compress PDF

Create, edit, and e-sign PDF forms & agreements

35:54 / 59:59

Vinod | 1N | 111803083 Varun Ajit N | 1Y | 111803147 Aayush Kali | 1C | 141903003 Shravani Sh | 1B | 111803041 Mugdha Pra

TCP-IP-Attacks.pdf - Adobe Acrobat Reader DC (64-bit)

File Edit View Sign Window Help

Home Tools TCP-IP-Attacks.pdf Sign In

- Other major goals included:
  - failure recovery and the ability to handle high error rates,
  - efficient protocol with low overhead, routable data
  - the ability to add new networks to an already existing network without disrupting the existing network

Its main emphasis was providing a suite not the security

Hence, by default, TCP/IP has security flaws at both the protocol level and implementation.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Search 'Insert Page'

Export PDF

Adobe Export PDF

Convert PDF Files to Word or Excel Online

Select PDF File

TCP-IP-Attacks.pdf

Convert to

Microsoft Word (*.docx)

Document Language: English (U.S.) Change

Convert

Edit PDF

Create PDF

Comment

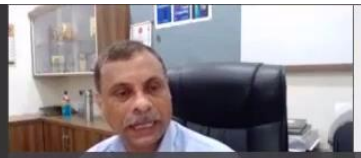
Combine Files

Organize Pages

Compress PDF

Create, edit, and e-sign PDF forms & agreements

41:05 / 59:59



Vinod | 1N | 111803083 Varun Ajit N | 1Y | 111803147 Aayush Kali | 1C | 141903003 Shravani Sh | 1B | 111803041 Mugdha Pra

TCP-IP-Attacks.pdf - Adobe Acrobat Reader DC (64-bit)

File Edit View Sign Window Help

Home Tools TCP-IP-Attacks.pdf × Sign In

4 / 85 111%

TCP/IP Protocol Model

- **Four Layers**
  - Application
  - Transport
  - Internetwork
  - Network access

At each layer, there are some security weaknesses that can be exploited by attackers

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Search 'Insert Page'

Export PDF

Adobe Export PDF

Convert PDF Files to Word or Excel Online

Select PDF File

TCP-IP-Attacks.pdf

Convert to

Microsoft Word (*.docx)

Document Language: English (U.S.) Change

Convert

Edit PDF

Create PDF

Comment

Combine Files

Organize Pages

Compress PDF

Create, edit, and e-sign PDF forms & agreements

+95

Vinod | 1N | 111803083 Varun Ajit N | 1Y | 111803147 Aayush Kali | 1C | 141903003 Shravani Sh | 1B | 111803041 Mugdha Pra

TCP-IP-Attacks.pdf - Adobe Acrobat Reader DC (64-bit)

File Edit View Sign Window Help

Home Tools TCP-IP-Attacks.pdf × Sign In

5 / 85 111%

APPLICATION LAYER

Some of application layer protocols are:

- Web Application and Browser Security Vulnerabilities
- Domain Name System (DNS)
- Dynamic Host Control Protocol (DHCP)

Each of these protocols has vulnerabilities.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Search 'Insert Page'

Export PDF

Adobe Export PDF

Convert PDF Files to Word or Excel Online

Select PDF File

TCP-IP-Attacks.pdf

Convert to

Microsoft Word (*.docx)

Document Language: English (U.S.) Change

Convert

Edit PDF

Create PDF

Comment

Combine Files

Organize Pages

Compress PDF

Create, edit, and e-sign PDF forms & agreements

41:31 / 59:59

Vinod | 1N | 111803083 Varun Ajit N | 1Y | 111803147 Aayush Kali | 1C | 141903003 Shravani Sh | 1B | 111803041 Mugdha Pra

TCP-IP-Attacks.pdf - Adobe Acrobat Reader DC (64-bit)

File Edit View Sign Window Help

Home Tools TCP-IP-Attacks.pdf × Sign In

7 / 85 111%

Caching

- Web browsers perform caching of the web pages
- The contents in the cache are saved temporarily
- The cache can contain images, passwords and user names.
- If the user's computer was compromised, an attacker can view all the contents and the user's browsing habits without any need of being authenticated and thus can be a privacy concern

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Search 'Insert Page'

Export PDF

Adobe Export PDF

Convert PDF Files to Word or Excel Online

Select PDF File

TCP-IP-Attacks.pdf

Convert to

Microsoft Word (*.docx)

Document Language: English (U.S.) Change

Convert

Edit PDF

Create PDF

Comment

Combine Files

Organize Pages

Compress PDF

Create, edit, and e-sign PDF forms & agreements

42:16 / 59:59

Vinod | 1N | 111803083 Varun Ajit N | 1Y | 111803147 Aayush Kali | 1C | 141903003 Shravani Sh | 1B | 111803041 Mugdha Pra

TCP-IP-Attacks.pdf - Adobe Acrobat Reader DC (64-bit)

File Edit View Sign Window Help

Home Tools TCP-IP-Attacks.pdf × Sign In

8 / 85 111%

Counter-measure

- It is important to clear the cache once in a while
- Disable the auto saving feature in the browser of passwords and user names in the cache

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Search 'Insert Page'

Export PDF

Adobe Export PDF

Convert PDF Files to Word or Excel Online

Select PDF File

TCP-IP-Attacks.pdf

Convert to

Microsoft Word (*.docx)

Document Language: English (U.S.) Change

Convert

Edit PDF

Create PDF

Comment

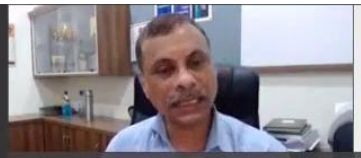
Combine Files

Organize Pages

Compress PDF

Create, edit, and e-sign PDF forms & agreements

42:59 / 59:59



Vinod | 1N | 111803083 Varun Ajit N | 1Y | 111803147 Aayush Kali | 1C | 141903003 Shravani Sh | 1B | 111803041 Mugdha Pra

TCP-IP-Attacks.pdf - Adobe Acrobat Reader DC (64-bit)

File Edit View Sign Window Help

Home Tools TCP-IP-Attacks.pdf Sign In

Session Hijacking

- Hijacking is possible when the attacker steals an HTTP session after observing and capturing the packets using a packet sniffer.
- It enables the attacker to have full access to the HTTP session and the communication changes from the client to the web server to attacker to the web server.
- Hijacking is possible when there is weak authentication between the client and the web server during the initializing of the session

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Export PDF

Adobe Export PDF

Convert PDF Files to Word or Excel Online

Select PDF File

TCP-IP-Attacks.pdf

Convert to

Microsoft Word (*.docx)

Document Language: English (U.S.) Change

Convert

Edit PDF

Create PDF

Comment

Combine Files

Organize Pages

Compress PDF

Create, edit, and e-sign PDF forms & agreements

44:39 / 59:59

Vinod | 111803083 Varun Ajit N | 111803147 Aayush Kali | 141903003 Shravani Sh | 111803041 Mugdha Pra

TCP-IP-Attacks.pdf - Adobe Acrobat Reader DC (64-bit)

File Edit View Sign Window Help

Home Tools TCP-IP-Attacks.pdf

Sign In

10 / 85 111%

Cookie Poisoning

- Cookies are used to maintain the state of a session to avoid the user to retype their credentials every time they visit a site or change web pages.
- Cookies are used by many web applications (including browsers) to save information. This information is stored permanently or temporarily on the client machine.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Search 'Insert Page'

Export PDF

Adobe Export PDF

Convert PDF Files to Word or Excel Online

Select PDF File

TCP-IP-Attacks.pdf

Convert to

Microsoft Word (*.docx)

Document Language: English (U.S.) Change

Convert

Edit PDF

Create PDF

Comment

Combine Files

Organize Pages

Compress PDF

Create, edit, and e-sign PDF forms & agreements

45:34 / 59:59

Vinod | 1N | 111803083 Varun Ajit N | 1Y | 111803147 Aayush Kali | 1C | 141903003 Shravani Sh | 1B | 111803041 Mugdha Pra

TCP-IP-Attacks.pdf - Adobe Acrobat Reader DC (64-bit)

File Edit View Sign Window Help

Home Tools TCP-IP-Attacks.pdf × Sign In

11 / 85 111%

- Cookie poisoning is the modification or theft of cookie in a user's machine by an attacker in order to release personal information.
- If the attacker gets hold of a cookie containing a password and username, they can use the cookie on their machine and the web server will not request any authentication because the cookie will issue out the username and password automatically.
- With cookie poisoning, an attacker can gain access to unauthorized information about a user and possibly steal their identity

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Search 'Insert Page'

Export PDF

Adobe Export PDF

Convert PDF Files to Word or Excel Online

Select PDF File

TCP-IP-Attacks.pdf

Convert to

Microsoft Word (*.docx)

Document Language: English (U.S.) Change

Convert

Edit PDF

Create PDF

Comment

Combine Files

Organize Pages

Compress PDF

Create, edit, and e-sign PDF forms & agreements

46:37 / 59:59

Vinod | 1N | 111803083 Varun Ajit N | 1Y | 111803147 Aayush Kali | 1C | 141903003 Shravani Sh | 1B | 111803041 Mugdha Pra

TCP-IP-Attacks.pdf - Adobe Acrobat Reader DC (64-bit)

File Edit View Sign Window Help

Home Tools TCP-IP-Attacks.pdf × Sign In

12 / 85 111%

Counter Measure

- Web Application Firewalls (WAF) are able to detect and block cookie poisoning attacks.
- Web Application Firewalls are able to inspect the HTTP sessions and can trace down the parameters set in the cookies that have been issued by the web server

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Search 'Insert Page'

Export PDF

Adobe Export PDF

Convert PDF Files to Word or Excel Online

Select PDF File

TCP-IP-Attacks.pdf

Convert to

Microsoft Word (*.docx)

Document Language: English (U.S.) Change

Convert

Edit PDF

Create PDF

Comment

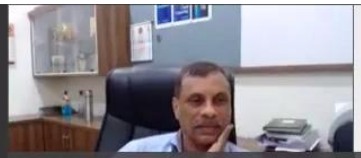
Combine Files

Organize Pages

Compress PDF

Create, edit, and e-sign PDF forms & agreements

47:21 / 59:59



Vinod | 1N | 111803083 Varun Ajit N | 1Y | 111803147 Aayush Kali | 1C | 141903003 Shravani Sh | 1B | 111803041 Mugdha Pra

TCP-IP-Attacks.pdf - Adobe Acrobat Reader DC (64-bit)

File Edit View Sign Window Help

Home Tools TCP-IP-Attacks.pdf × Sign In

13 / 85 111%

Replay Attack

- This involves man-in-the-middle attack in which the sent data is repeatedly sent to the server.
- This is more than a hijack. The data resent can be modified and can bring different results.
- Furthermore, the attacker can spoof the IP address of a client and thus redirect his/her machine.

Counter measure:

- The web browser should be able to tell that replayed traffic is not legitimate.

Search 'Insert Page'

Export PDF

Adobe Export PDF

Convert PDF Files to Word or Excel Online

Select PDF File

TCP-IP-Attacks.pdf

Convert to

Microsoft Word (*.docx)

Document Language: English (U.S.) Change

Convert

Edit PDF

Create PDF

Comment

Combine Files

Organize Pages

Compress PDF

Create, edit, and e-sign PDF forms & agreements

47:51 / 59:59

Vinod | 1N | 111803083 Varun Ajit N | 1Y | 111803147 Aayush Kali | 1C | 141903003 Shravani Sh | 1B | 111803041 Mugdha Pra

TCP-IP-Attacks.pdf - Adobe Acrobat Reader DC (64-bit)

File Edit View Sign Window Help

Home Tools TCP-IP-Attacks.pdf × Sign In

14 / 85 111%

Cross-Site Scripting

- Hacker injecting malicious code in a web application or browser and is executed at the client side.
- The essence of this attack is to perform a session hijack by stealing session tokens and cookies of a legitimate user's session.

Counter measure:

- Disable scripts to run on the website. However, this control means that some functions and features on the website will not be available.
- Another alternative is to enhance the security controls when dealing with cookie based user authentication

Search 'Insert Page'

Export PDF

Adobe Export PDF

Convert PDF Files to Word or Excel Online

Select PDF File

TCP-IP-Attacks.pdf

Convert to

Microsoft Word (*.docx)

Document Language: English (U.S.) Change

Convert

Edit PDF

Create PDF

Comment

Combine Files

Organize Pages

Compress PDF

Create, edit, and e-sign PDF forms & agreements

+101

Vinod | 1N | 111803083 Varun Ajit N | 1Y | 111803147 Aayush Kali | 1C | 141903003 Shravani Sh | 1B | 111803041 Mugdha Pra

TCP-IP-Attacks.pdf - Adobe Acrobat Reader DC (64-bit)

File Edit View Sign Window Help

Home Tools TCP-IP-Attacks.pdf ×

Sign In

15 / 85 111%

DNS Protocol Attacks

- There are following common attacks:
  - DNS cache poisoning
  - DNS spoofing

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Search 'Insert Page'

Export PDF

Adobe Export PDF

Convert PDF Files to Word or Excel Online

Select PDF File

TCP-IP-Attacks.pdf

Convert to

Microsoft Word (*.docx)

Document Language: English (U.S.) Change

Convert

Edit PDF

Create PDF

Comment

Combine Files

Organize Pages

Compress PDF

Create, edit, and e-sign PDF forms & agreements

49:58 / 59:59

Vinod | 1N | 111803083 Varun Ajit N | 1Y | 111803147 Aayush Kali | 1C | 141903003 Shravani Sh | 1B | 111803041 Mugdha Pra

TCP-IP-Attacks.pdf - Adobe Acrobat Reader DC (64-bit)

File Edit View Sign Window Help

Home Tools TCP-IP-Attacks.pdf × Sign In

16 / 85 111%

DNS Cache Poisoning

- It is an integrity attack that involves manipulating the information saved in the DNS cache giving it wrong information.
- This false information will offer a name to IP; mapping it to a wrong IP address.
- The objective is to divert the requests to another web site.
- This new web site might be bogus and offers the same or similar products and services as the real web site.
- If the user does not notice anything, he enters the user name and password.
- Then the attacker can steal the user credentials.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Search 'Insert Page'

Export PDF

Adobe Export PDF

Convert PDF Files to Word or Excel Online

Select PDF File

TCP-IP-Attacks.pdf

Convert to

Microsoft Word (*.docx)

Document Language: English (U.S.) Change

Convert

Edit PDF

Create PDF

Comment

Combine Files

Organize Pages

Compress PDF

Create, edit, and e-sign PDF forms & agreements

50:35 / 59:59

Vinod | 1N | 111803083 Varun Ajit N | 1Y | 111803147 Aayush Kali | 1C | 141903003 Shravani Sh | 1B | 111803041 Mugdha Pra

TCP-IP-Attacks.pdf - Adobe Acrobat Reader DC (64-bit)

File Edit View Sign Window Help

Home Tools TCP-IP-Attacks.pdf × Sign In

17 / 85 111%

DNS Spoofing

- DNS spoofing refers to faking the IP address of a computer to match the IP address of the DNS server so that requests can be directed to that wrong computer.
- In this attack, the hacker's computer is considered to be a legitimate DNS server by clients and other servers.
- It will impersonate the DNS server and reply to all incoming requests from the clients thus misdirecting them
- DNS server spoofing attacks are often used to spread computer worms and viruses

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Search 'Insert Page'

Export PDF

Adobe Export PDF

Convert PDF Files to Word or Excel Online

Select PDF File

TCP-IP-Attacks.pdf

Convert to

Microsoft Word (*.docx)

Document Language: English (U.S.) Change

Convert

Edit PDF

Create PDF

Comment

Combine Files

Organize Pages

Compress PDF

Create, edit, and e-sign PDF forms & agreements

51:29 / 59:59

Vinod | 1N | 111803083 Varun Ajit N | 1Y | 111803147 Aayush Kali | 1C | 141903003 Shravani Sh | 1B | 111803041 Mugdha Pra

TCP-IP-Attacks.pdf - Adobe Acrobat Reader DC (64-bit)

File Edit View Sign Window Help

Home Tools TCP-IP-Attacks.pdf Sign In

18 / 85 111%

Counter Measure

- **Avoid trust relationships:** Organizations should develop protocols that rely on **trust relationships as little as possible**. It is significantly easier for attackers to run spoofing attacks when trust relationships are in place because trust relationships only use IP addresses for authentication.

Search 'Insert Page'

Export PDF

Adobe Export PDF

Convert PDF Files to Word or Excel Online

Select PDF File

TCP-IP-Attacks.pdf

Convert to

Microsoft Word (*.docx)

Document Language: English (U.S.) Change

Convert

Edit PDF

Create PDF

Comment

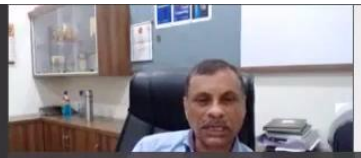
Combine Files

Organize Pages

Compress PDF

Create, edit, and e-sign PDF forms & agreements

+99



Vinod | 1N | 111803083 Varun Ajit N | 1Y | 111803147 Aayush Kali | 1C | 141903003 Shravani Sh | 1B | 111803041 Mugdha Pra

TCP-IP-Attacks.pdf - Adobe Acrobat Reader DC (64-bit)

File Edit View Sign Window Help

Home Tools TCP-IP-Attacks.pdf Sign In

19 / 85 111%

DHCP Starvation Attack

- It is the consuming of IP address space allocated by the DHCP server.
- An attacker broadcasts large number of DHCP REQUEST messages with spoofed source MAC addresses.
- If the legitimate DHCP Server in the network start responding to all these bogus DHCP REQUEST messages, then available IP Addresses in the DHCP server scope will be depleted within a very short span of time.

Search 'Insert Page'

Export PDF

Adobe Export PDF

Convert PDF Files to Word or Excel Online

Select PDF File

TCP-IP-Attacks.pdf

Convert to

Microsoft Word (*.docx)

Document Language: English (U.S.) Change

Convert

Edit PDF

Create PDF

Comment

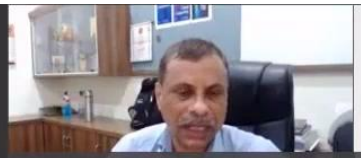
Combine Files

Organize Pages

Compress PDF

Create, edit, and e-sign PDF forms & agreements

52:21 / 59:59



Vinod | 1N | 111803083 Varun Ajit N | 1Y | 111803147 Aayush Kali | 1C | 141903003 Shravani Sh | 1B | 111803041 Mugdha Pra

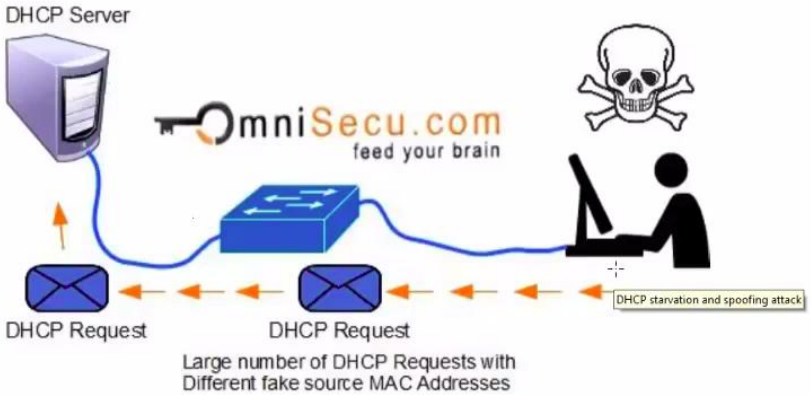
TCP-IP-Attacks.pdf - Adobe Acrobat Reader DC (64-bit)

File Edit View Sign Window Help

Home Tools TCP-IP-Attacks.pdf × Sign In

20 / 85 111%

- When a genuine user wants to access the network, the server will not offer an IP address automatically and the user will not be granted access into the network. This is a denial of service attack



Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Search 'Insert Page'

Export PDF

Adobe Export PDF

Convert PDF Files to Word or Excel Online

Select PDF File

TCP-IP-Attacks.pdf

Convert to

Microsoft Word (*.docx)

Document Language: English (U.S.) Change

Convert

Edit PDF

Create PDF

Comment

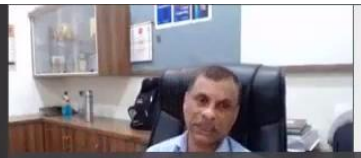
Combine Files

Organize Pages

Compress PDF

Create, edit, and e-sign PDF forms & agreements

56:23 / 59:59



Vinod | 1N | 111803083 Varun Ajit N | 1Y | 111803147 Aayush Kali | 1C | 141903003 Shravani Sh | 1B | 111803041 Mugdha Pra

TCP-IP-Attacks.pdf - Adobe Acrobat Reader DC (64-bit)

File Edit View Sign Window Help

Home Tools TCP-IP-Attacks.pdf × Sign In

21 / 85 111%

- Once the available number of IP Addresses in the DHCP server is depleted, network attackers can then set up a rogue DHCP server and respond to new DHCP requests from network DHCP clients. By setting up a rogue DHCP server, the attacker can now launch DHCP spoofing attack.

Counter Measure:

- To prevent DHCP starvation, port security can be used because it only allows a specified number of MAC addresses per port

Search 'Insert Page'

Export PDF

Adobe Export PDF

Convert PDF Files to Word or Excel Online

Select PDF File

TCP-IP-Attacks.pdf

Convert to

Microsoft Word (*.docx)

Document Language: English (U.S.) Change

Convert

Edit PDF

Create PDF

Comment

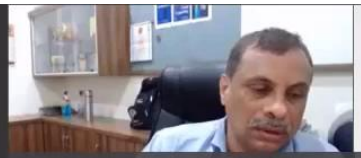
Combine Files

Organize Pages

Compress PDF

Create, edit, and e-sign PDF forms & agreements

57:25 / 59:59



Vinod | 1N | 111803083 Varun Ajit N | 1Y | 111803147 Aayush Kali | 1C | 141903003 Shravani Sh | 1B | 111803041 Mugdha Pra

TCP-IP-Attacks.pdf - Adobe Acrobat Reader DC (64-bit)

File Edit View Sign Window Help

Home Tools TCP-IP-Attacks.pdf Sign In

22 / 85 111%

DHCP spoofing attack

- After a DHCP starvation attack and setting up a rogue DHCP server, the attacker can start distributing IP addresses and other TCP/IP configuration settings to the network DHCP clients.
- TCP/IP configuration settings include Default Gateway and DNS Server IP addresses.
- Network attackers can now replace the original legitimate Default Gateway IP Address and DNS Server IP Address with their own IP Address.

Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Search 'Insert Page'

Export PDF

Adobe Export PDF

Convert PDF Files to Word or Excel Online

Select PDF File

TCP-IP-Attacks.pdf

Convert to

Microsoft Word (*.docx)

Document Language: English (U.S.) Change

Convert

Edit PDF

Create PDF

Comment

Combine Files

Organize Pages

Compress PDF

Create, edit, and e-sign PDF forms & agreements

58:38 / 59:59