Zero Knowledge Proof: Fiat-Shamir Heuristic

Prof Bill Buchanan OBE, The Cyber Academy

http://asecuritysite.com

CYBER ACADEMY

Existing Method

How To Prove Yourself: Practical Solutions to Identification and Signature Problems

Amos Fiat and Adi Shamir
Department of Applied Mathematics
The Weizmann Institute of Science
Rehovot 76100, Israel

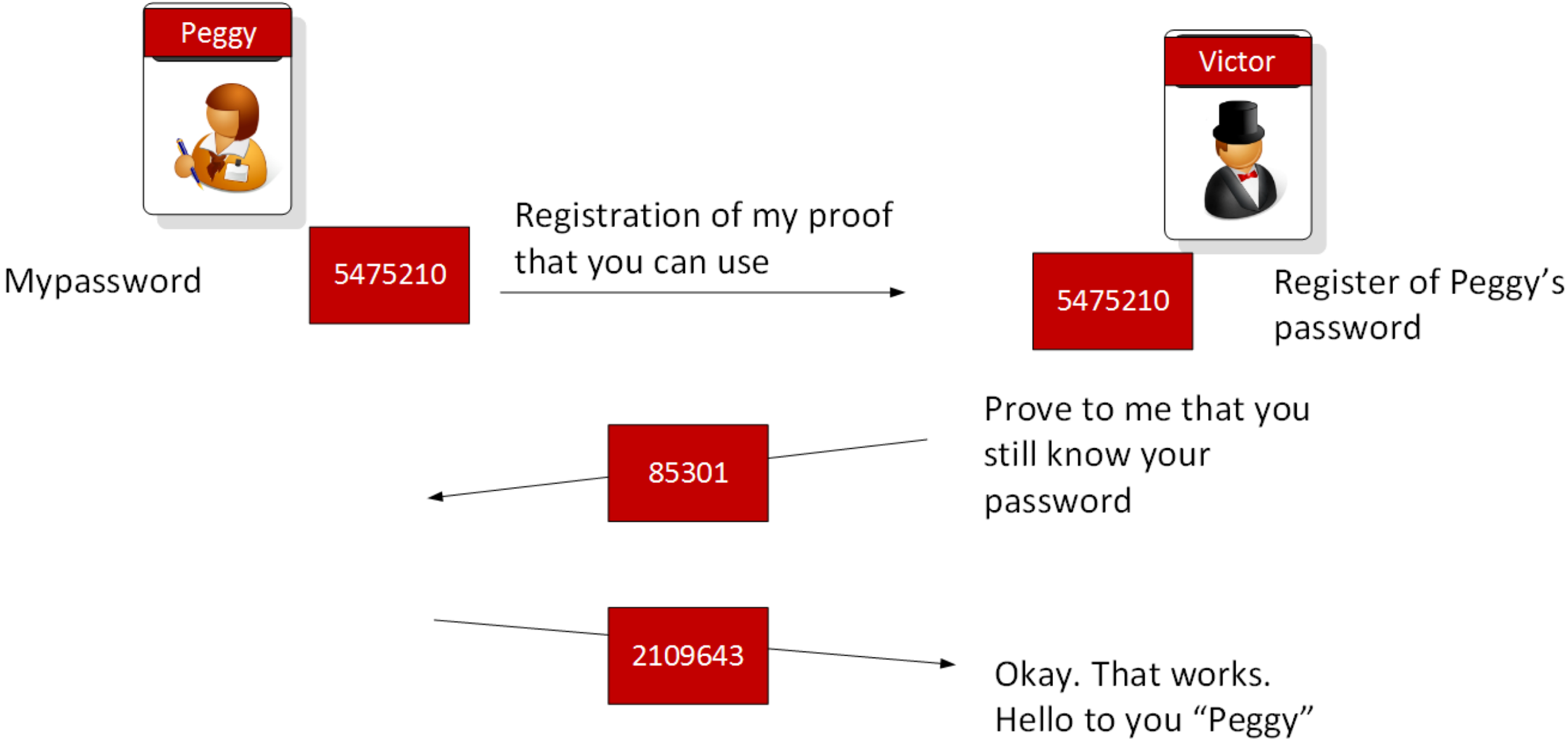
Mypassword

5k63A

salt

red hash of password

Zero-knowledge Proof



Fiat-Shamir heuristic - Non-interactive random oracle access

pass= Mypassword
x = Hash(pass)
$y = g^x$

$y = g^x$

$y = g^x$

Peggy select *v*

$t = g^v$

Victor generates a random value (c)

c

$r = v - c\,x$

r

Victor computes: $g^r y^c$

If same as t, Peggy is verified

Peggy and Victor agree on
g and *n* (prime)

```
x = int(hashlib.md5(pass).hexdigest()[:8], 16) % n
y= g**x % n
```

Fiat-Shamir heuristic - Non-interactive random oracle access

$$g^r y^c = g^{v-cx} (g^x)^c$$
$$= g^{v-cx} g^{xc}$$
$$= g^{v-cx+cx}$$
$$= g^v$$

pass= Mypassword
x = Hash(pass)
$y = g^x$

$y = g^x$

$y = g^x$

Peggy select *v*

$t = g^v$

Victor generates a random value (c)

c

$r = v - c\,x$

r

Victor computes: $g^r y^c$

If same as t, Peggy is verified

Fiat-Shamir heuristic - Non-interact

```
n=997

text="Hello"

g= 3

print "Password:\t",text

x = int(hashlib.md5(text).hexdigest()[:8]

y= pow(g,x,n)

t = pow(g,v,n)

r = (v - c * x)

Result = ( pow(g,r,n) * pow(y,c,n))  % n
```

```
Password:       hello

======Agreed parameters=============
P= 997   (Prime number)
G= 7     (Generator)

======The secret==================
x= 149   (Alice's secret)

======Random values===============
c= 3     (Bob's random value)
v= 2000          (Alice's random value)

======Shared value===============
g^x mod P=       116
r=               1553

=========Results===================
t=g**v % n =            147
( (g**r) * (y**c) )=    147
Alice has proven she knows password
```

Fiat-Shamir heuristic - Non-interactive r

```
n=997

text="Hello"

g= 3

print "Password:\t",text

x = int(hashlib.md5(text).hexdigest()[:8], 16

y= pow(g,x,n)

t = pow(g,v,n)

r = (v - c * x)

Result = ( pow(g,r,n) * pow(y,c,n))  % n
```

```
if (r<0):
 Result = ( inverse
else:
 Result = ( pow(g,r
```

```
Password:       hello

======Agreed parameters============
P= 997   (Prime number)
G= 7     (Generator)

======The secret==================
x= 149   (Alice's secret)

======Random values===============
c= 531   (Bob's random value)
v= 321   (Alice's random value)

======Shared value===============
g^x mod P=       116
r=               -78798

=========Results==================
t=g**v % n =            458
( (g**r) * (y**c) )=    458
Alice has proven she knows password
```

Fiat-Shamir heuristic – Picking g

```
def pickg(p):
 for x in range (1,p):
  rand = x
  exp=1
  next = rand % p
while (next <> 1 ):
   next = (next*rand) % p
   exp = exp+1

  if (exp==p-1):
   return rand
```

ss= Mypassword
= Hash(pass)
= g^x

$y = g^x$

$y = g^x$

Peggy select v

$t = g^v$

Victor generates a random value (c)

c

r = v – c x

r

Victor computes: $g^r y^c$

If same as t, Peggy is verified

Zero Knowledge Proof: Fiat-Shamir Heuristic

Prof Bill Buchanan OBE, The Cyber Academy

http://asecuritysite.com

CYBER ACADEMY