RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: SPO1-R03

Random Numbers – The Key to Security

Aidan Gogarty

Technology Evangelist
HOB Gmbh & Co KG

#RSAC

Presentation Areas

- Security – what is it?
- Threats – what to look out for
- Encryption – how does it work
- Random Numbers – what and why?

Security – Why You Need It

What Security Means

- Keep it safe or keep it private?
- Share only what needs to be shared

Keeping it Safe

- Not all attacks are malicious (human error, spam, data farming)
- Malicious attacks are to take data/to cause damage to system

What About The Bad Guys?

Threats

- Threat to Confidentiality
- Threat to Integrity
- Threat to Availability

Types of Harm

- Interception

- Interruption

- Modification

- Fabrication

Sender And Destination

- Verify identity

Sender
Destination

- Identification & authentication

Matter of Trust

- Can you trust the hardware?
- Can you trust the software?
- Can you trust your users?

Attackers

- Amateurs
- Hackers & crackers
- Commercial crime
- Cyber terrorism
- State-supported information gathering

Multi-Layered Defense

Medieval Castle

- Location (hill, river)
- Moat
- Wall & gatehouse
- Watchtowers
- Guards

Computer Data

- Physical
- Technical
- Policies & procedures
- Software & hardware

What About Encryption?

Encryption Through the Ages...

- Trusted couriers
- Hidden messages
- Early cryptography - readable to unreadable
- Using codewords

Spot the Connection?

First Randomizer - Enigma

The Enigma Machine

- From three rotors of a set of five, the rotor settings with 26 positions, and the plugboard with ten pairs of letters connected, the military Enigma had 158,962,555,217,826,360,000 settings

Breaking Encryption

- Break single message – look for patterns
- Infer knowledge without breaking encryption
- Predict the key to break future messages
- Find vulnerabilities in the encryption algorithm

Breakable Encryption?

- Message with 25 characters: INFORMATION SECURITY TALK
  - 26^{25} ($=10^{35}$) possibilities
- Brute force attack:
  - 10^{10} decryptions per second on 10^{35} possibilities

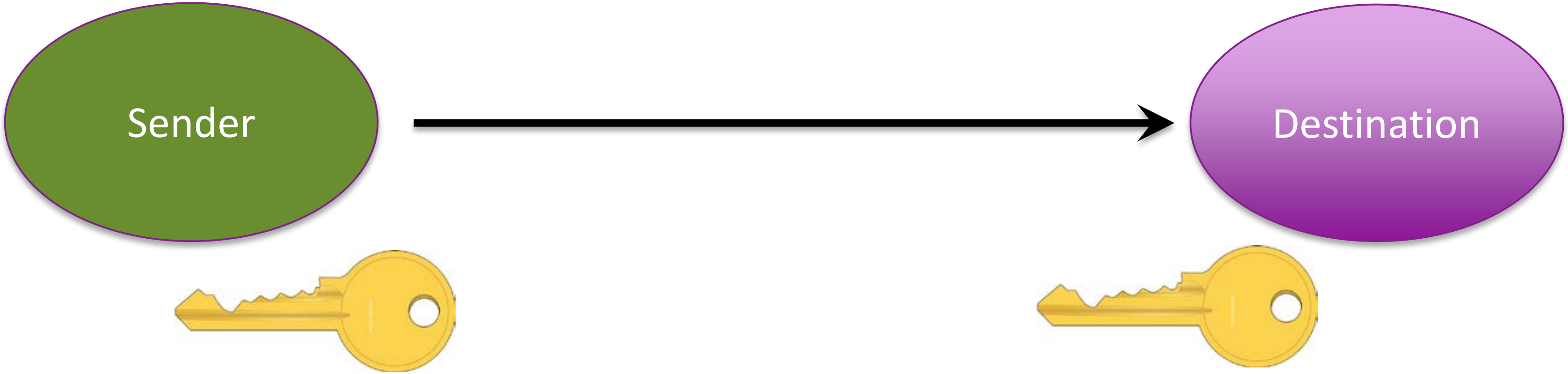
    $= 10^{25}$ seconds (10 billion years)
- Statistical analysis
  - $= 10^{5}$ seconds (1.2 days)

Using Encryption Today

- Computer = deterministic, operations can be predicted
- Public key = random number
- Random number = non deterministic, cannot be predicted

Symmetric Encryption

- Only sender and receiver know the key



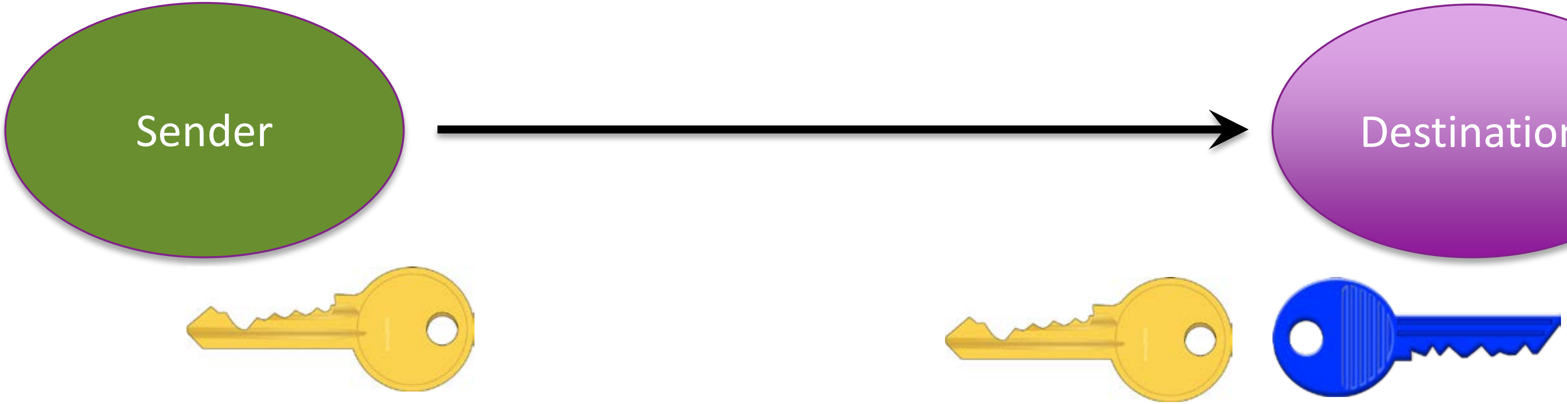
Sender

Destination

- Need to keep the connection secure

Asymmetric Encryption

- Public key – encryption key
- Private key – decryption key



Sender

Destination

So How Are Random Numbers Used?

What are Random Numbers?

- Random numbers cannot be normally predicted
- Pseudorandom numbers – pattern repeats over time
- Be careful: no discernible pattern – might not be apparent to users

Entropy

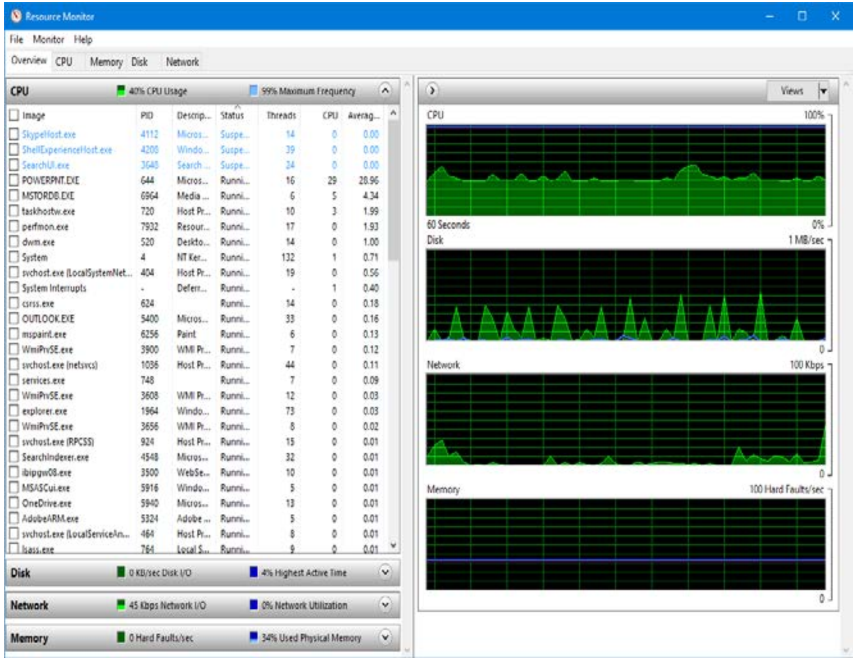
- Measure of uncertainty in the information
  - 01010101010101010101010101010101010101010101010101010101
  - 01011010010101010101010011000100110010010001010101101011
- Entropy in language
  - English vs. German/French – reasonably similar
  - English Vs. Chinese – Chinese has approximately 3 times more entropy than English

How Random Numbers are Used

- All encryption needs a key
- More random the key, the harder to crack the encryption
- All encryption starts with a seed

Where Can You Get Entropy?

- Truly random sequence –
  - Electrical current of TV signals
  - Internet radio
  - CPU load measurements
- ENIAC – first random number collector



CPU — 40% CPU Usage — 99% Maximum Frequency

Image	PID	Descrip...	Status	Threads	CPU	Averag...
SkypeHost.exe	4112	Micros...	Suspe...	14	0	0.00
ShellExperienceHost.exe	4208	Windo...	Suspe...	39	0	0.00
SearchUI.exe	3648	Search ...	Suspe...	24	0	0.00
POWERPNT.EXE	644	Micros...	Runni...	16	29	28.96
MSTORDB.EXE	6964	Media ...	Runni...	6	5	4.34
taskhostw.exe	720	Host Pr...	Runni...	10	3	1.99
perfmon.exe	7932	Resour...	Runni...	17	0	1.93
dwm.exe	520	Deskto...	Runni...	14	0	1.00
System	4	NT Ker...	Runni...	132	1	0.71
svchost.exe (LocalSystemNet...	404	Host Pr...	Runni...	19	0	0.56
System Interrupts	-	Deferr...	Runni...	-	1	0.40
csrss.exe	624		Runni...	14	0	0.18
OUTLOOK.EXE	5400	Micros...	Runni...	33	0	0.16
mspaint.exe	6256	Paint	Runni...	6	0	0.13
WmiPrvSE.exe	3900	WMI Pr...	Runni...	7	0	0.12
svchost.exe (netsvcs)	1036	Host Pr...	Runni...	44	0	0.11
services.exe	748		Runni...	7	0	0.09
WmiPrvSE.exe	3608	WMI Pr...	Runni...	12	0	0.03
explorer.exe	1964	Windo...	Runni...	73	0	0.03
WmiPrvSE.exe	3656	WMI Pr...	Runni...	8	0	0.02
svchost.exe (RPCSS)	924	Host Pr...	Runni...	15	0	0.01
SearchIndexer.exe	4548	Micros...	Runni...	32	0	0.01
ibipgw08.exe	3500	WebSe...	Runni...	10	0	0.01
MSASCui.exe	5916	Windo...	Runni...	5	0	0.01
OneDrive.exe	5940	Micros...	Runni...	13	0	0.01
AdobeARM.exe	5324	Adobe ...	Runni...	5	0	0.01
svchost.exe (LocalServiceAn...	464	Host Pr...	Runni...	8	0	0.01
lsass.exe	764	Local S...	Runni...	9	0	0.01

Disk — 0 KB/sec Disk I/O — 4% Highest Active Time

Network — 45 Kbps Network I/O — 0% Network Utilization

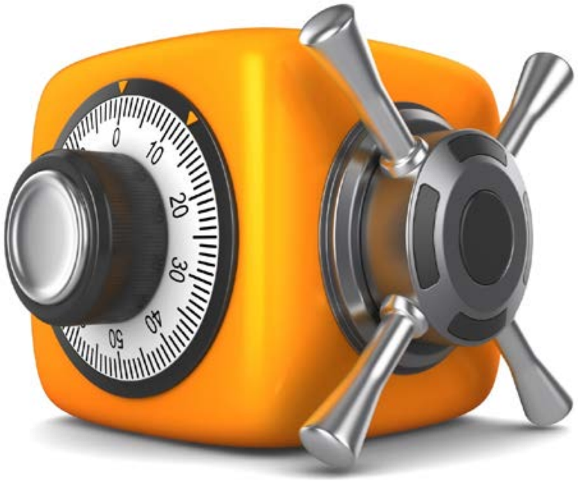
Memory — 0 Hard Faults/sec — 34% Used Physical Memory

HOB

After All That, What Do YOU Need To Do?

Methods of Protection

- Prevent Attack
- Deter Attack
- Deflect
- Mitigate
- Detect
- Recover



Improve Your Encryption

- Get a good random number generator
- Gather highest possible entropy
- Secure source of entropy
- Multiple and constant sources of entropy
- Remember Confidentiality, Integrity & Availability

And That‘s It

- Thank you for your attention
- Any questions?

Copyrights

- Slide 4 - http:// cdn.images.express.co.uk/img/dynamic/1/590x/pickpocket-381435.jpg
- Slide 8 - http://images.google.de/imgres?imgurl=https%3A%2F%2Fbib.kuleuven.be
- Slide 10 - https://c1.staticflickr.com/7/6056/6239670686_65fdd9e0eb_b.jpg
- Slide 15 – http://images.google.de/imgres?imgurl=hollywoodmoviecostumesandprops.blogspot.com
- Slide 15 - http://images.google.de/imgres?imgurl=primetime.unrealitytv.co.uk
- Slide 16 - http://images.google.de/imgres?imgurl=http%3A%2F%2Fwww.colossus-computer.com
- Slide 19 - http://lifehacker.com/5856506
- Slide 21 - https://openclipart.org/detail/204232/cylinder-lock-key
- Slide 28 - http://www.contractorsassociation.org/wp-content/uploads/2012/12/asset-protection-contractors.jpg
- Slide 30 – http://www.clipartpanda.com