Center for Distributed Computing and Security

Current activities:

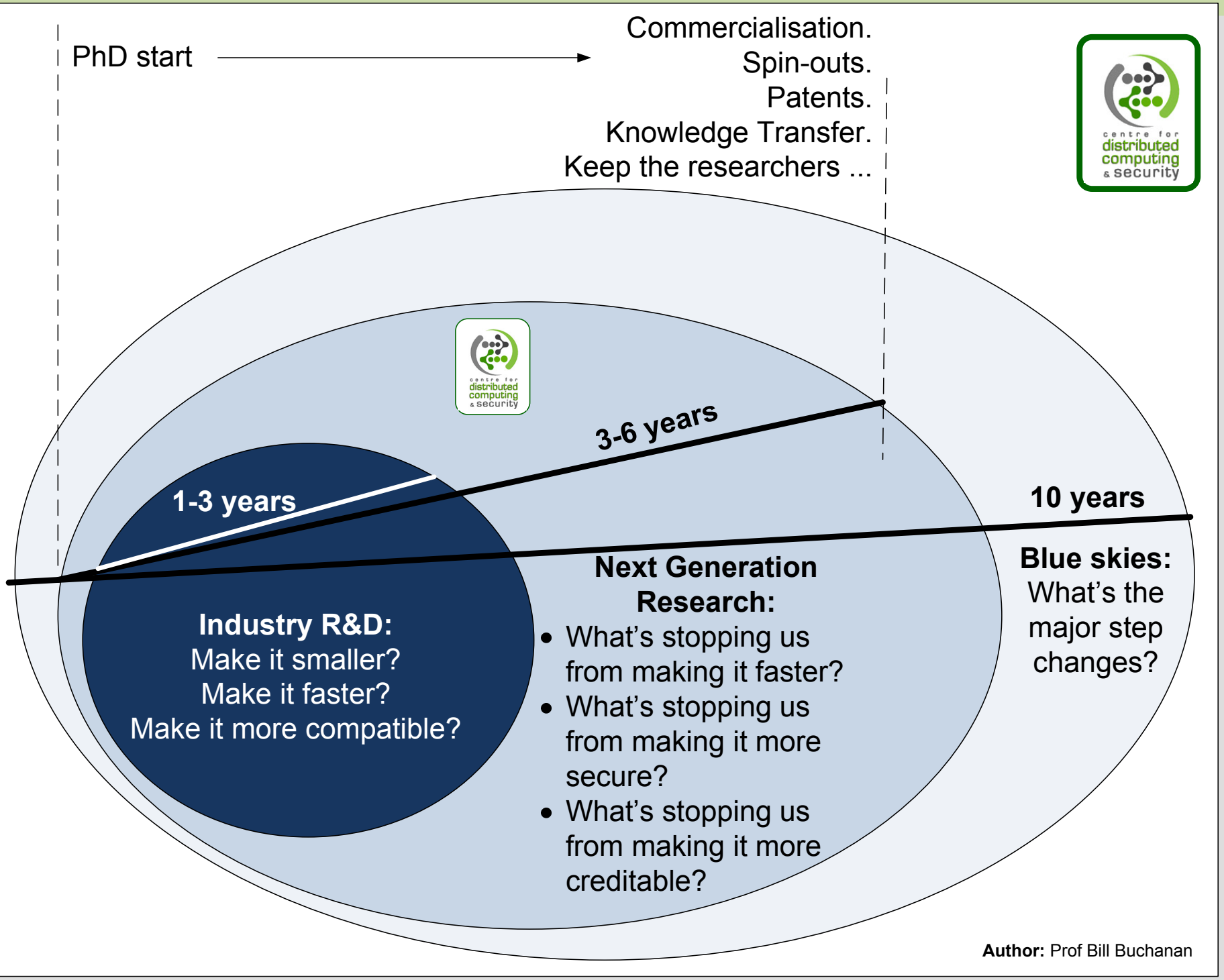
Digital DNA, Performance Evaluation of Security, Oblivious Transfer Methods ...

Prof Bill Buchanan

Leader, Centre for Distributed Computing and Security

http://www.cdcs.soc.napier.ac.uk/

Author: Prof Bill Buchanan



Why do we exist ...

Mobile Systems
Mesh/Ad-hoc Networks. **Dr N.Migas**
Mobile IP.**Dr I.Romdhani**
Group communications. **Dr A.Al-Dubai/Liang Zhao**

Security
Intrusion Detections Systems
Performance Evaluation **(Dr) L.Saliou**
Intelligence-sharing frameworks **Omair Uthmani**
Risk Analysis in e-Crime **Mat Miehling**
Next generation systems **A.Kwecha**
Privacy preserving algorithms **Z.Kwecha**

Digital Forensics
Digital DNA **Dr J.Graves/Niladri Bose**

Simulators/Educational Frameworks
Network Simulators **Prof B.Buchanan**
Linux Zoo **Dr G.Russell**

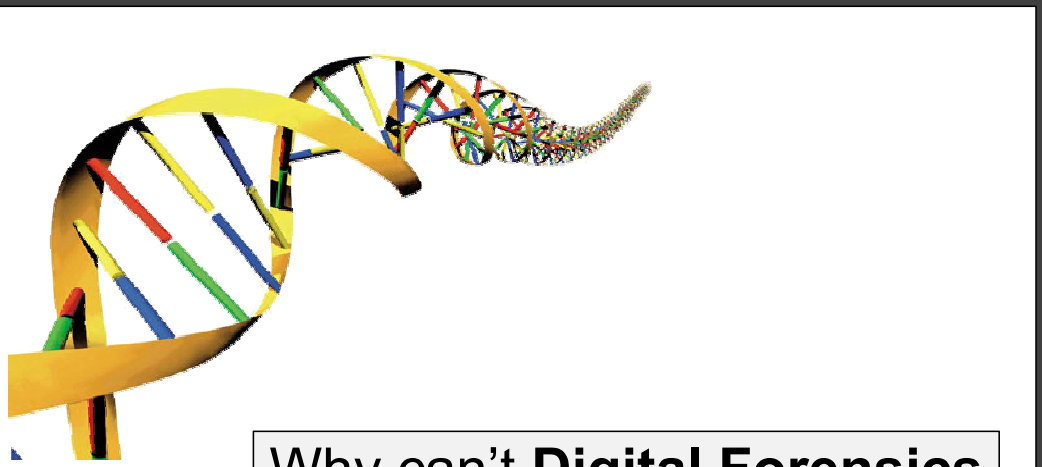
e-Health/Speech Analysis
RFID. **Dr C.Thuemmlar, MD**
Infection Tracking. **Prof Nick Christophi**
Patient Risk Assessment.
Patient-centric systems.
Speech Analysis. **A.Lawson/Dr John Old**

Imperial College London

Performance Improvements (PI) Group Ltd

Author: Prof Bill Buchanan

Center for Distributed Computing and Security



Why can't **Digital Forensics** be more like Forensic Science?

centre for distributed computing & security

Digital DNA

Jamie Gravies

Author: Prof Bill Buchanan

Existing Digital Evidence is generally not fit for purpose

- Legacy
- Not designed for current needs

"Digital DNA" conceived as a new form of metadata:

- Digital Forensics
- Auditing/Compliance
- Monitoring user/process interaction
- Provides SIEM vendors with technical edge

centre for distributed computing & security

- **Unique Metadata Collection and Analysis Suite**
  - Complete, Accurate, Authentic
  - Patent Pending (0816556.5)
  - Data Collection
    - Continuous recording, or time line, of activity
  - Data Analysis
    - Provides probability that activity occurred, akin to the use of DNA evidence in court

- **Unique form of host-based metadata**
  - Details of file-access history and process interaction
  - Offline analysis abilities
- **Compliance, eDiscovery, and Digital Forensics ready**
  - Easily integrates into multiple strategic activities
- **Patent-Pending fingerprinting technology**
  - Robust form of evidence
- **Compliments existing audit data**
  - Adds value to existing SIEM audit sources

Dr Jamie Graves

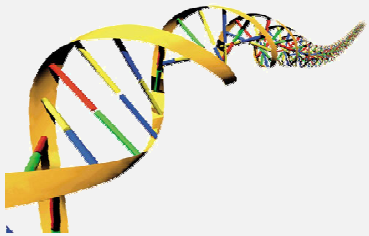
Fingerprint of Activity

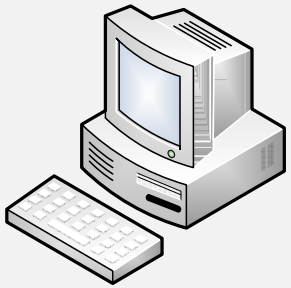
[DALLLQAFCCLPHLILLILPHLPF]

USER ACCESSES SALES DATA

Fingerprint of Activity

[DALLLQAFCCLPHLILLILPHLPF]





LILILILILILILILLQFFMMQQMMMPMDLADLALILLILLILLILLILLILPMMMMMMMMLILILLPEEEQC
CADLDLALADDLLALADLALADANLLILLPLILLPQMLLILILLPMFQMPMMPMPFEPFEELPHLILILL
QFCDFLPHLPHLILLPKFDRLILLPKFDRLILLPLILLPLILLPLILLPLILLPLILLPLILLPLILLPLILLPLIL
LPQLDQCCALADADLDLLALNLLILILLQFCDFLILLPKFDRLLPKFDRLILLPKFDRLILILLQFCDFLI
LLPKFDRLLPKFDRLILLPKFDRLILILLQFCDFLILLPKFDRLLPKFDRLILLPKFDRLILILLQFCMDL
DFLILILLQFCDFLILILLQFCDFLADLLPLIPFLAFPPFQCCADLDLALADDLLALADLALADALILLPLI
LLPLILLPNLFPPFLILPHLPHLILPHLPHLPHLILILLQFMMPPFQFCDFLILILLQFCDFFPPFLILILP
HHLILILLQFCDFFPPFFLILILLQFCDLILLQFLILLQFLILILFPPFLLQFCDFHLPSSLDLLLAFAPPFL
PHLPHLILPHLPHLPHLILLPKFDRFPPFPPFPPFPPFPPFPPFPPFPPFPPFPPFPPFPPFPPFPPFPPFPPF
PPFPMLLPLPHLPHLLPLQLQLPFCLLPELSLPHLPHLPHSLDALLLQAMDCLPHLILLILPHLPFCLI
LLPFEQLDQCCALADADLDLLALNLLQEFLSLELLPPELILILQAFFDLFLAFFFLILPHLPHLPHLPH
LILLPKFDRLILLPKFDRFFFFFFFFFLPFCLILLPFEQLDQCCALADADLDLLALNLLQEFLELLPP
ELILILQAMMMMDLAPMLILILDLILLLAILPLLIDLILLAMMMLLPELILIILILLQFCDFLLILPHLPHLIDL
ADLADLADLAPMDLADLALPFELILLDLILILPHLPFCHSLADLAPFPPFPPFPPFPPFPPFPPFPPFPPF
PPFPPFPPFPPFPPFPPFPPFPPFPPFPPFPPFPPFPPFPPFPPFPPFPPFPMDLAPMDLAMMMMMMMM
DL

Author: Prof Bill Buchanan

Dr Jamie Graves

Digital DNA

Fingerprint of Activity

[DALLLQAFCCLPHLILLILPHLPF]

USER ACCESSES SALES DATA

Fingerprint of Activity

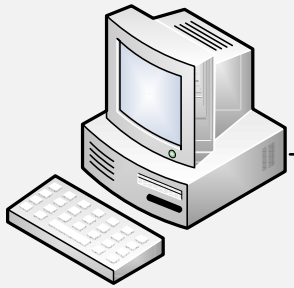
[DALLLQAFCCLPHLILLILPHLPF]

MATCH REPORT

Probability
of user opening
sales data: High
(2.9e-5)

DALLLQAFCCLPHLILLILPHLPF

DALLLQA----CLPHLILLILPHLPF

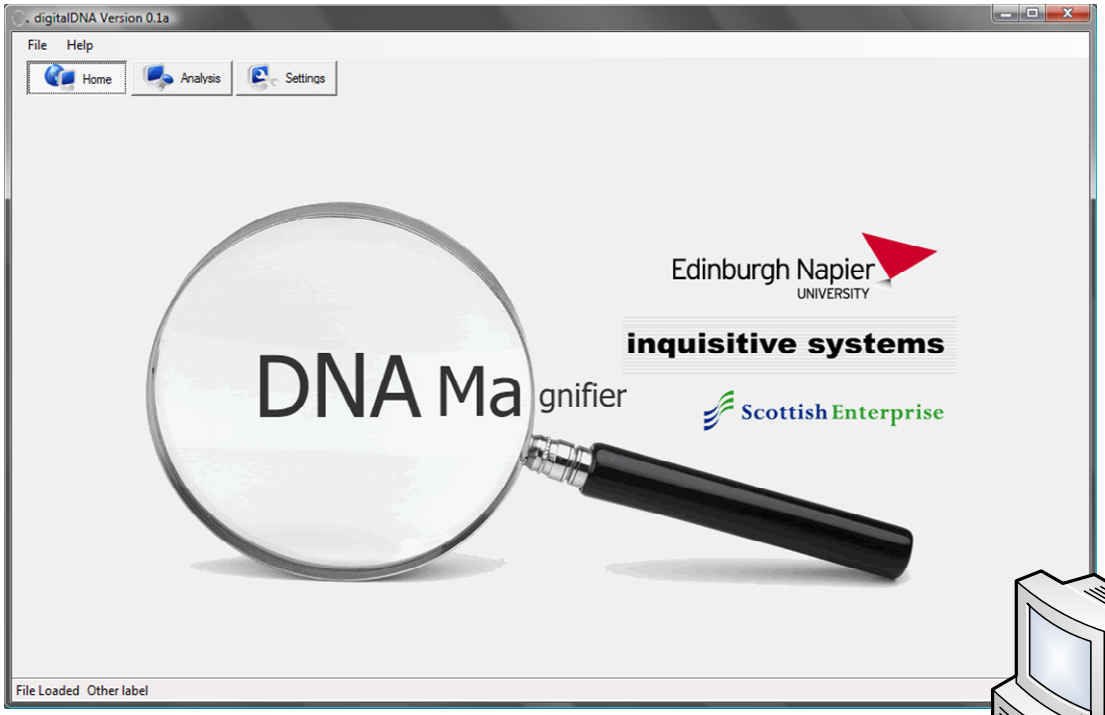


LILILILILILILILLQFFMMQQMMMPMDLADLALLLLLLLLLLLLLPMMMMMMMLILILLPEEEQCC
ADLDLALADDLLALADLALADANLLILLPLILLPQMLLILILLPMFQMPMMPMPFEPFEELPHLILLLQ
FCDFLPHLPHLILLPKFDRLILLPKFDRLILLPLILLPLILLPLILLPLILLPLILLPLILLPLILLPLILLP
QLDQCCALADADLDLLALNLLILILLQFCDFLILLPKFDRLLPKFDRLILLPKFDRLILILLQFCDFLILLP
KFDRLLPKFDRLILLPKFDRLILILLQFCDFLILLPKFDRLLPKFDRLILLPKFDRLILILLQFCMDLDFLI
LILLQFCDFLILILLQFCDFLADLLPLIPFLAFPPFQCCADLDLALADDLLALADLALADALILLPLILLPL
ILLPNLFPPFLILPHLPHLILPHLPHLPHLILILLQFMMPPFQFCDFLILILLQFCDFFPPFLILILPHHLILI
LLQFCDFFPPFFLILILLQFCDLILLQFLILLQFLILILFPPFLLQFCDFHLPSSLDLLLAFAPPFLPHLPH
LILPHLPHLPHLILLPKFDRFPPFPPFPPFPPFPPFPPFPPFPPFPPFPPFPPFPPFPPFPPFPPFPPFPM
LLPLPHLPHLLPLQLQLPFCLLPELSLPHLPHLL[DALLLQAMDCLPHLILLILPHLPF]CLILLPFE
QLDQCCALADADLDLLALNLLQEFLSLELLPPELILLQAFFDLFLAFFFLILPHLPHLPHLPHLILLPK
FDRLILLPKFDRFFFFFFFFFLPFCLILLPFEQLDQCCALADADLDLLALNLLQEFLELLPPELILILQ
AMMMMDLAPMLILILDLILLLAILPLLIDLILLAMMMLLPELILIILILLQFCDFLLILPHLPHLIDLADLADL
ADLAPMDLADLALPFELILLDLILILPHLPFCHSLADLAPFPPFPPFPPFPPFPPFPPFPPFPPFPPFPPFP
PFPPFPPFPPFPPFPPFPPFPPFPPFPPFPPFPPFPPFPPFPMDLAPMDLAMMMMMMMMDL

Author: Prof Bill Buchanan

Dr Jamie Graves

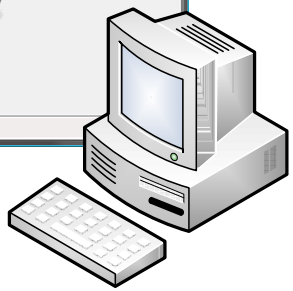
Digital DNA



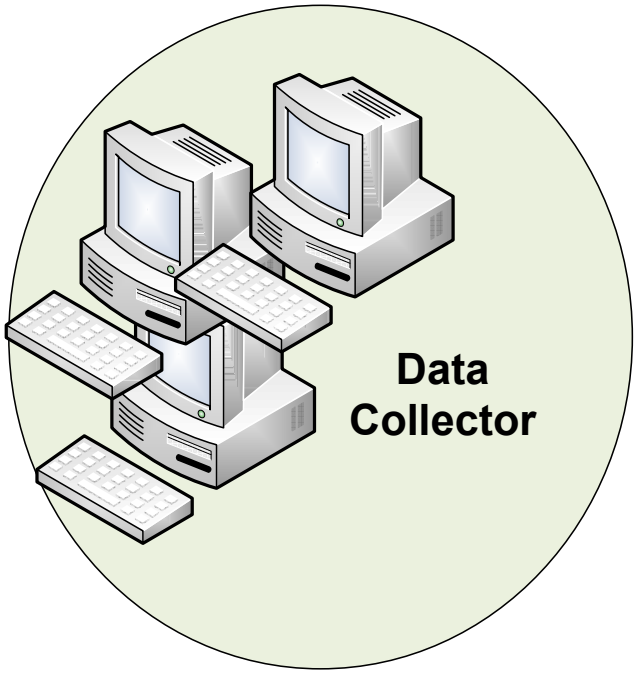
centre for distributed computing & security

Dr Jamie Graves

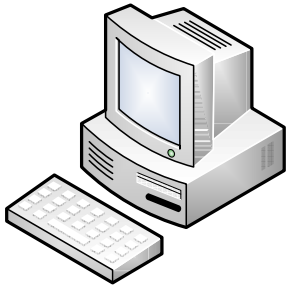
Digital DNA



Data Analysis (DNA Magnifier)



Data Collector



Data Storage

Author: Prof Bill Buchanan

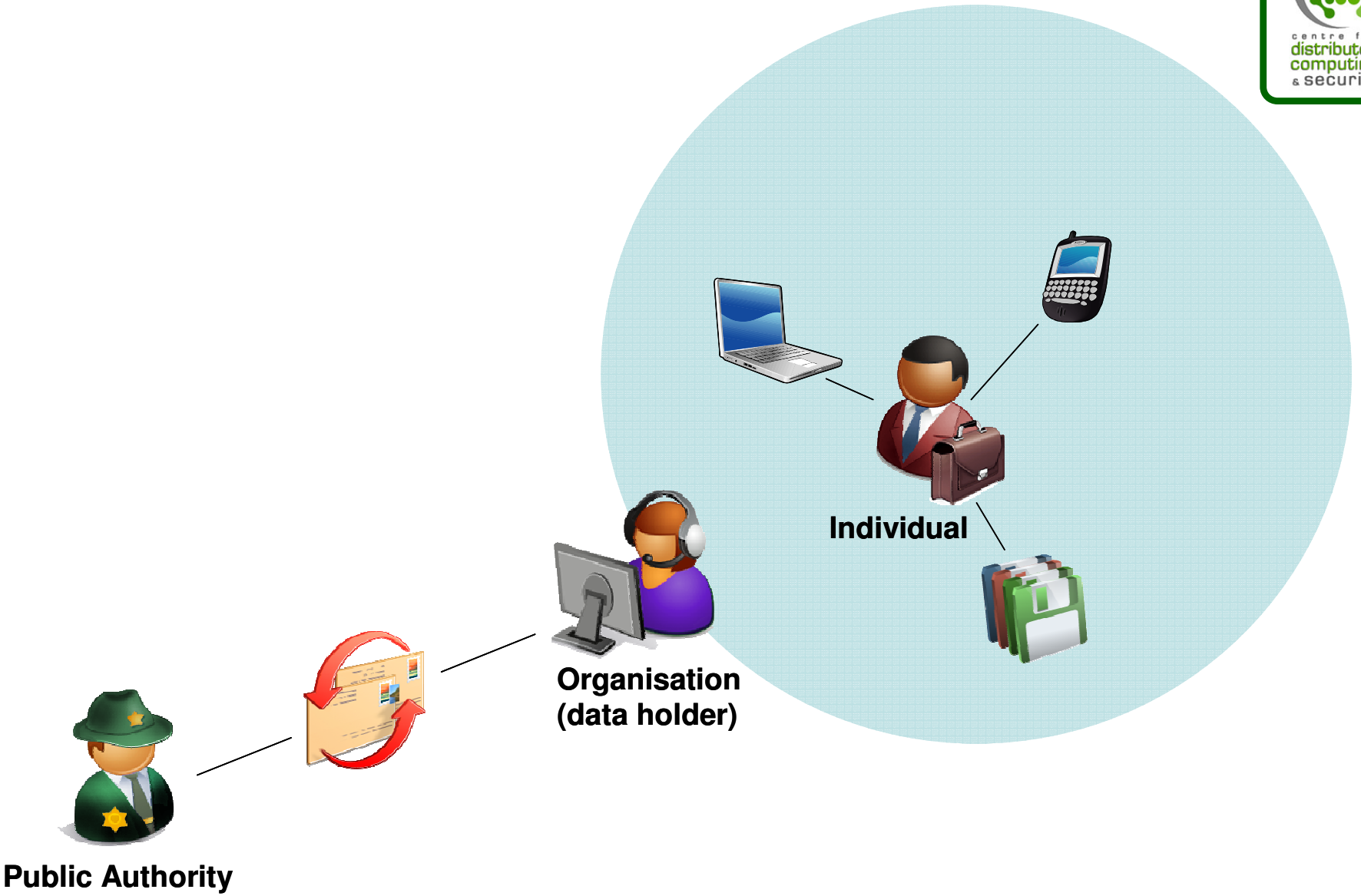
Center for Distributed Computing and Security

How do you balance the rights of the **individual** against the rights of the **investigator**?

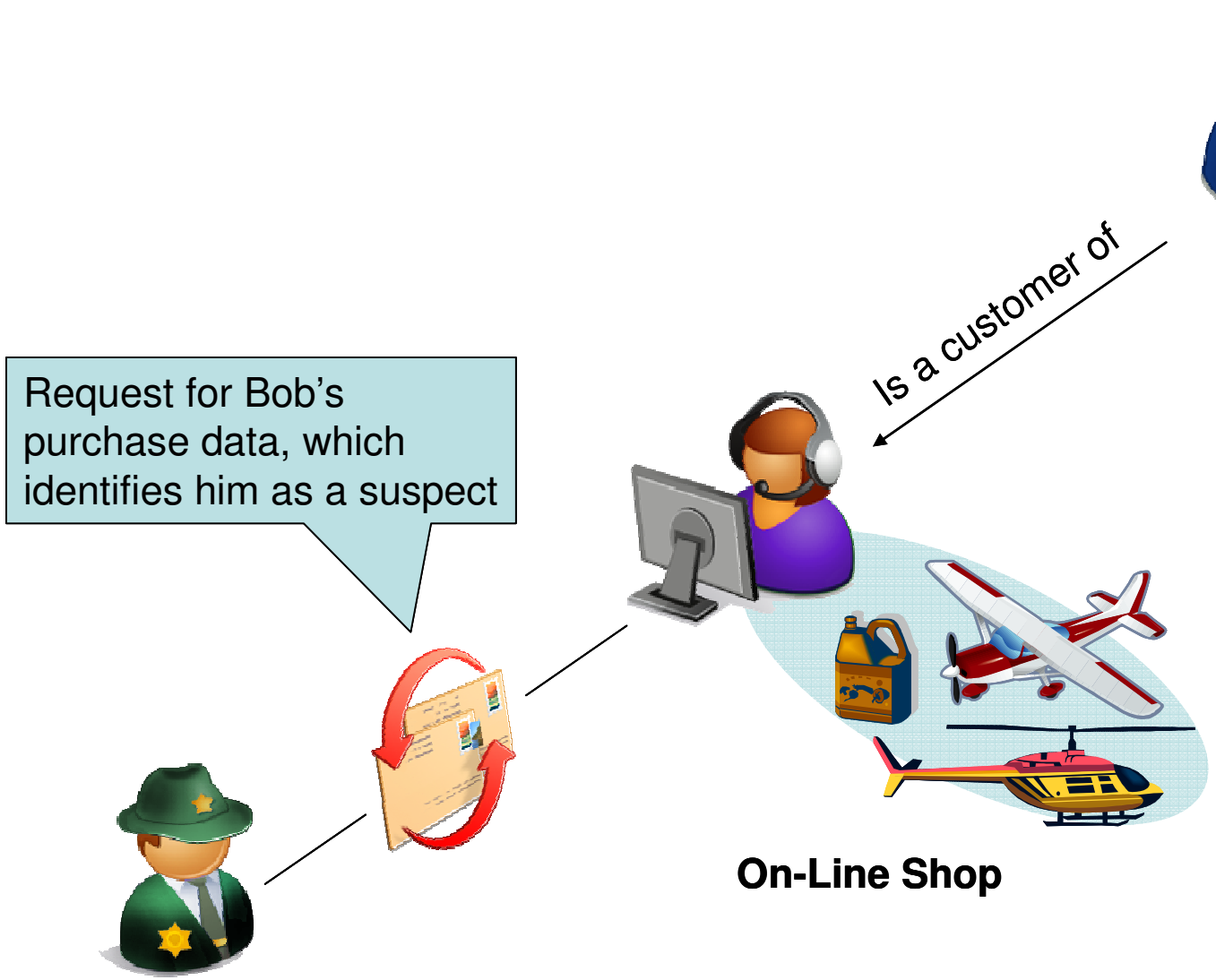
1-N Oblivious Transfer Algorithms in Privacy-Preserving Investigations

Zbigniew Kwecka

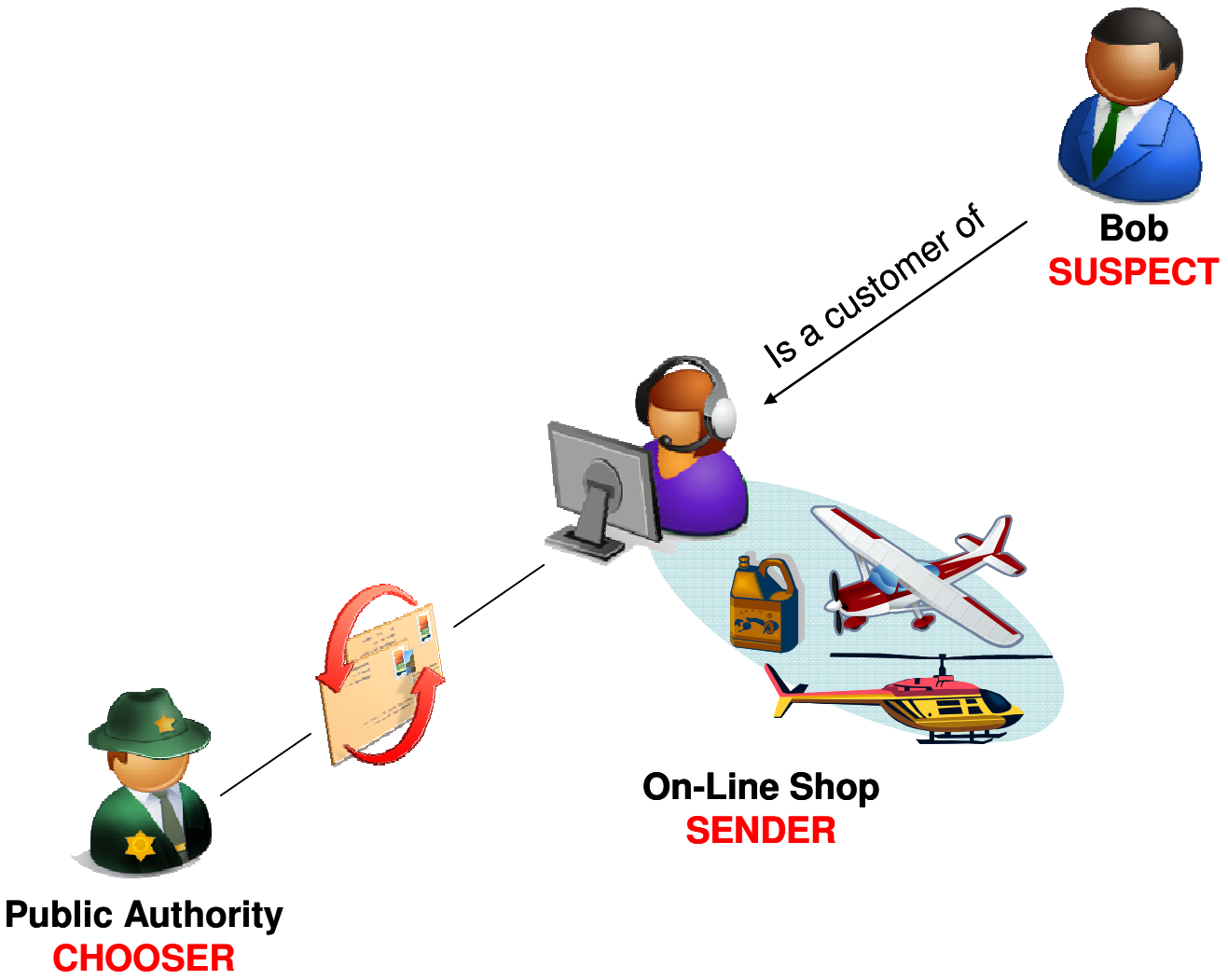
Author: Prof Bill Buchanan



Author: Prof Bill Buchanan



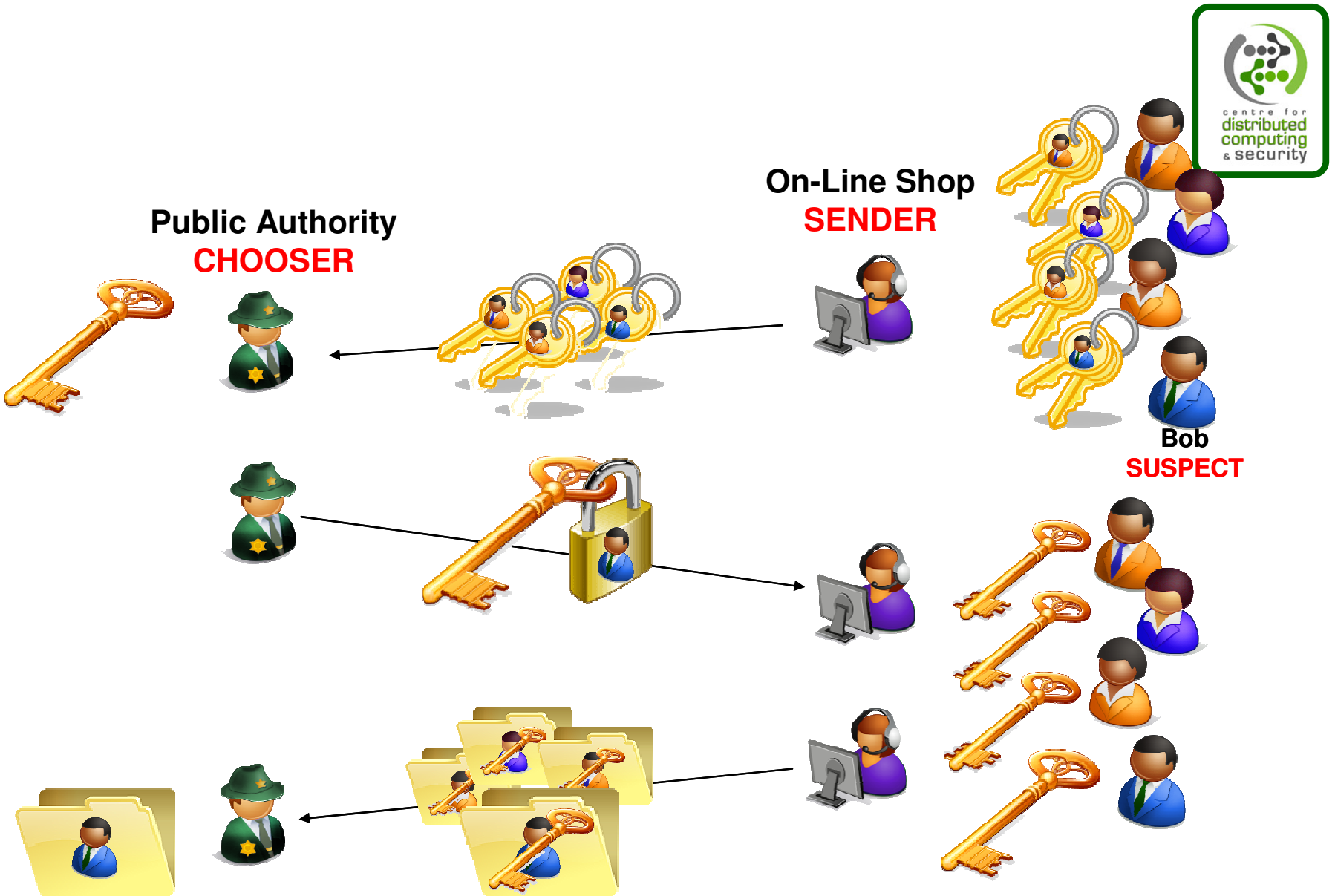
Author: Prof Bill Buchanan



Zbigniew Kwecka

Privacy Preserving

Author: Prof Bill Buchanan



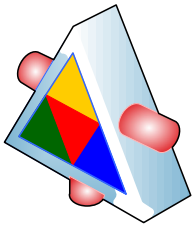
Privacy Preserving

Zbigniew Kwecka

Author: Prof Bill Buchanan

1-n **O**T **A**ccess for **P**rivacy-**P**reserving **I**nvestigations

Center for Distributed Computing and Security



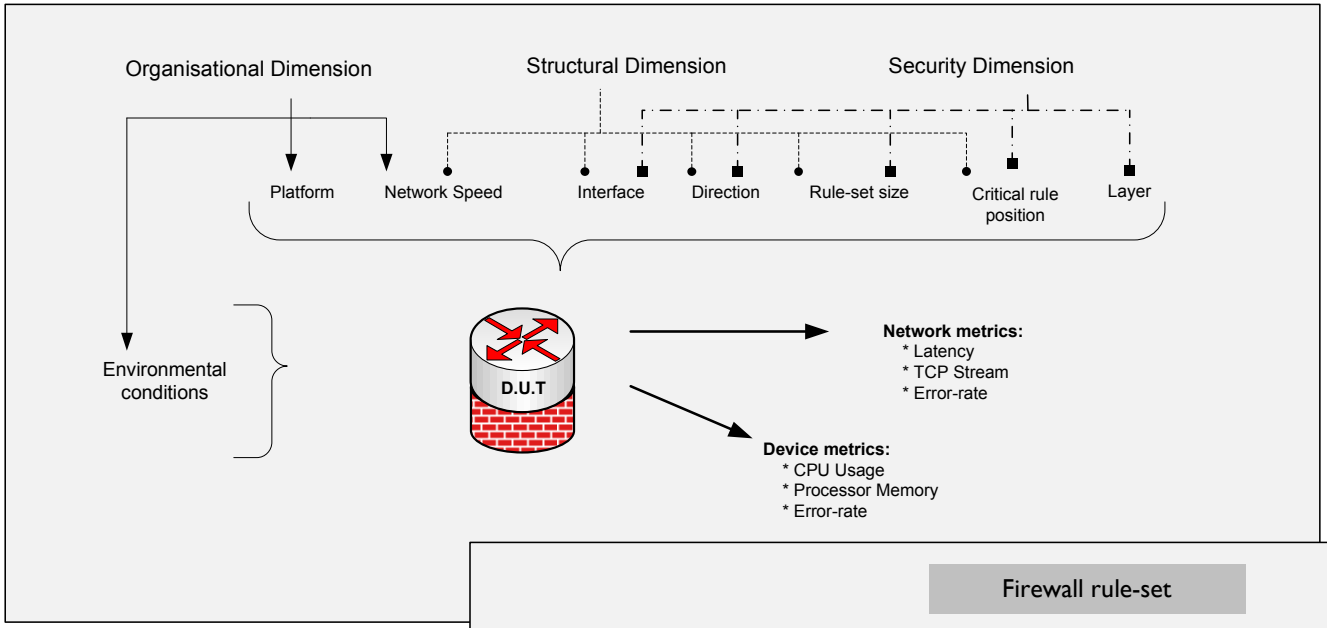
How do you **assess** the affect of security on networked devices?

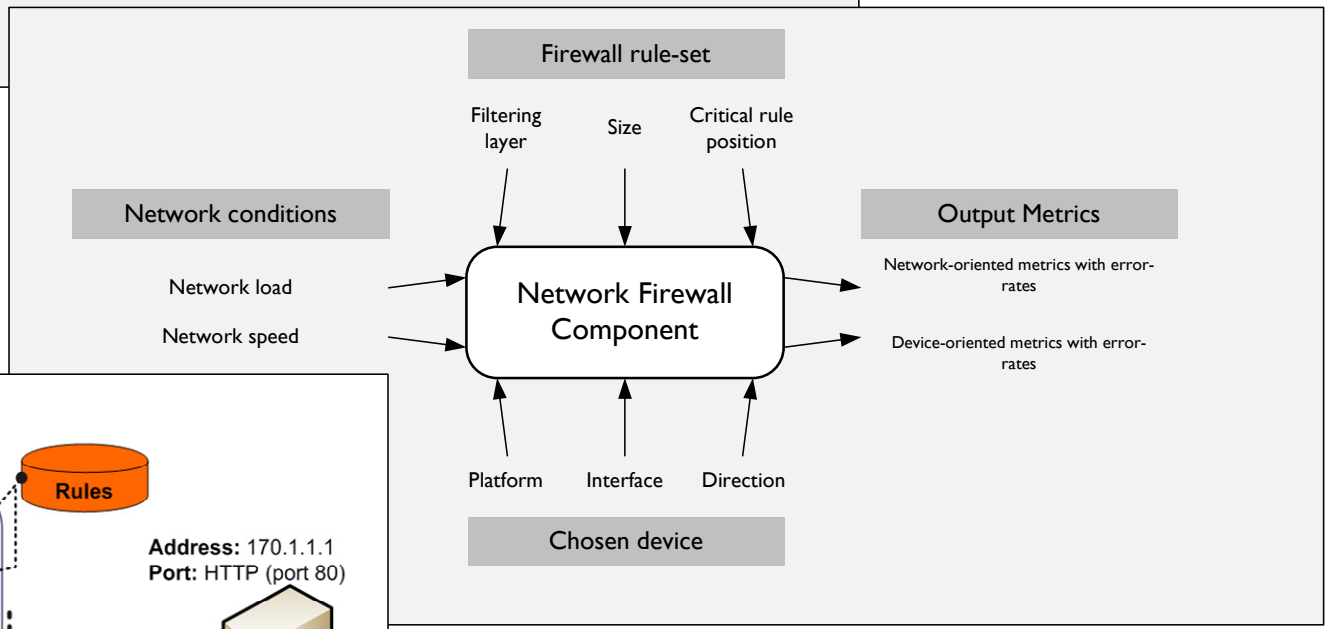
Dynamic Performance Modelling for Network Devices

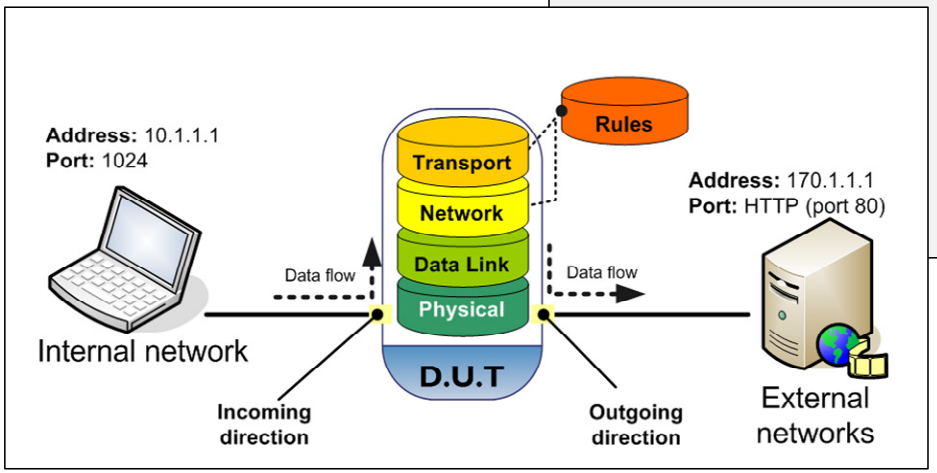
Lionel Saliou

centre for distributed computing & security

Author: Prof Bill Buchanan





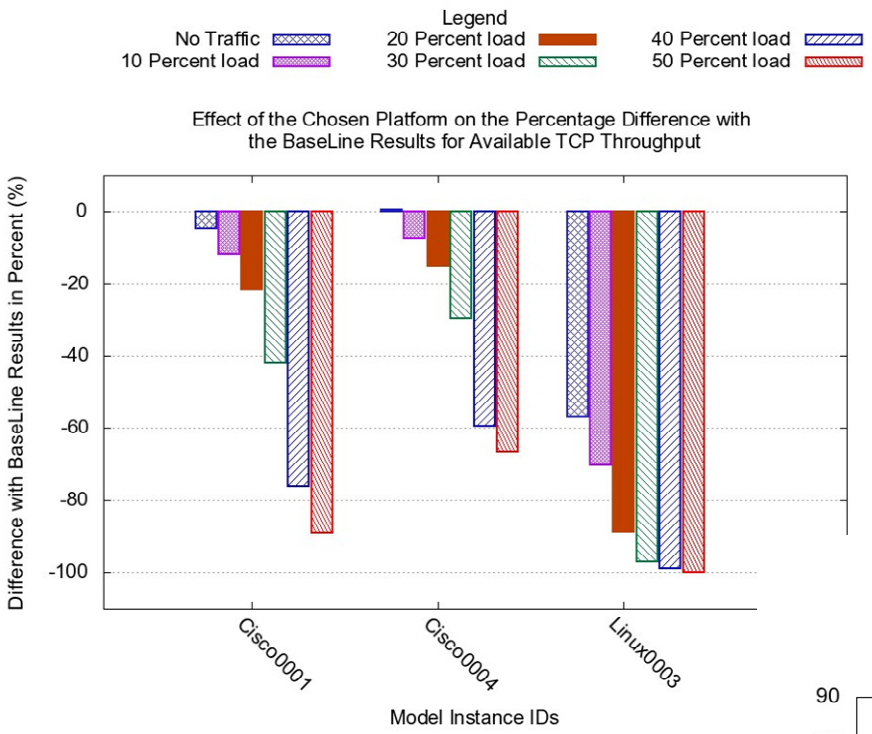


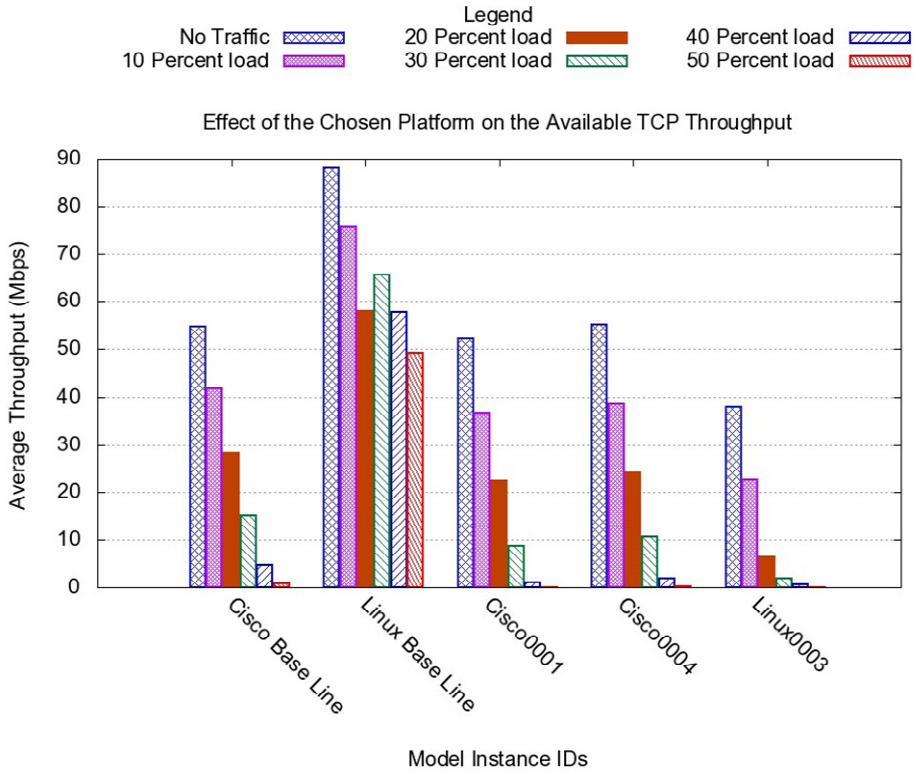
Lionel Saliou

Security Perf.

Author: Prof Bill Buchanan

Dynamic Performance of Security Devices





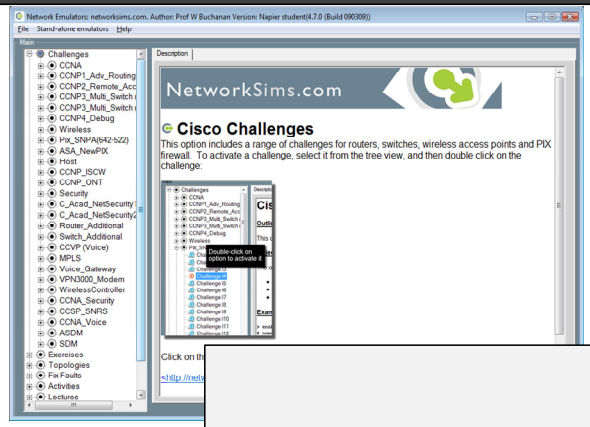
Author: Prof Bill Buchanan

Lionel Saliou

Security Perf.

Dynamic Performance of Security Devices

Center for Distributed Computing and Security

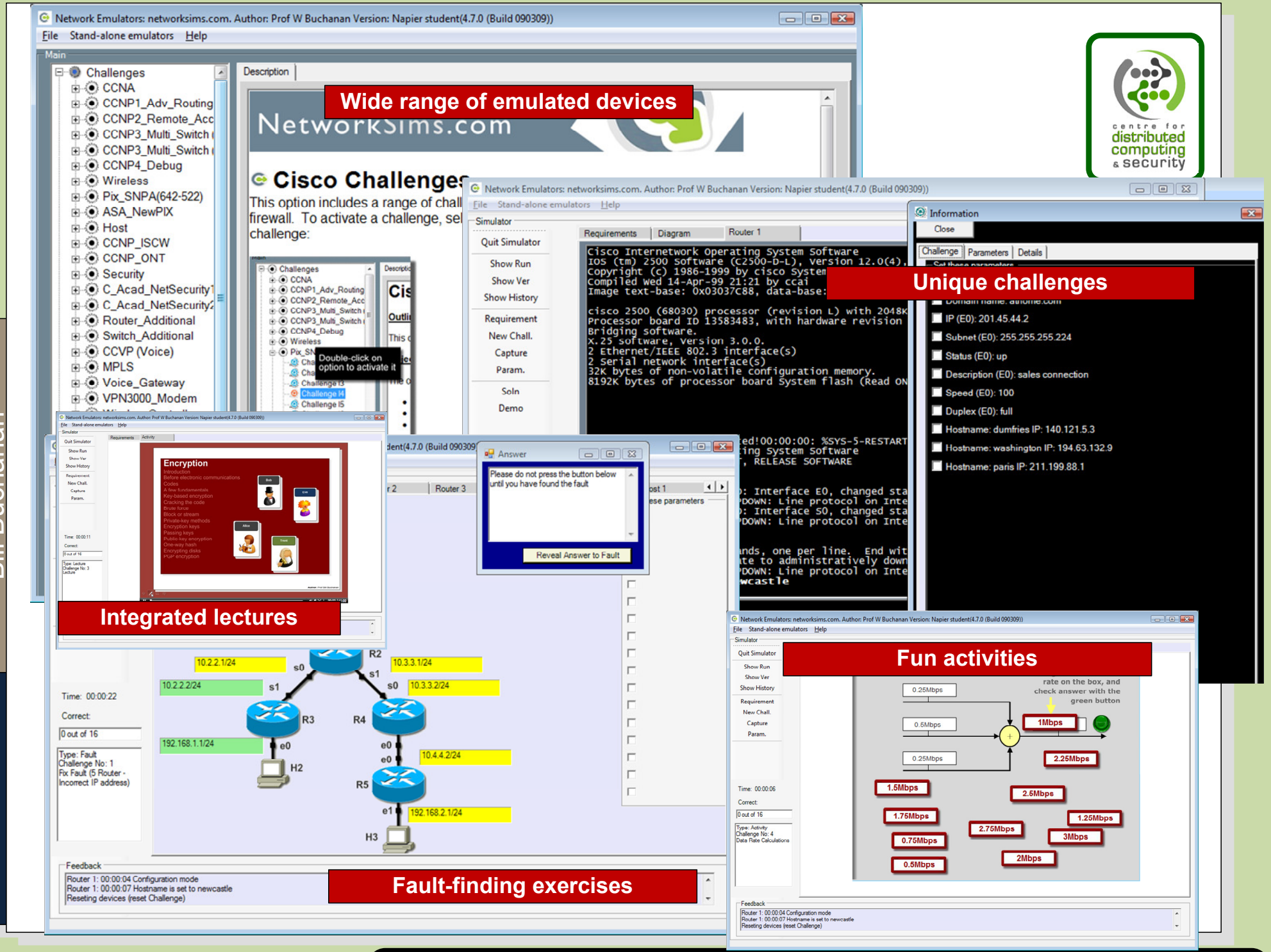


Why can't learning networking be more **fun**?

NetworkSims.com

Bill Buchanan

Author: Prof Bill Buchanan


Network Emulators: networksims.com. Author: Prof W Buchanan Version: Napier student(4.7.0 (Build 090309))
File Stand-alone emulators Help
Main
Challenges
CCNA
CCNP1_Adv_Routing
CCNP2_Remote_Acc
CCNP3_Multi_Switch
CCNP3_Multi_Switch
CCNP4_Debug
Wireless
Pix_SNPA(642-522)
ASA_NewPIX
Host
CCNP_ISCW
CCNP_ONT
Security
C_Acad_NetSecurity1
C_Acad_NetSecurity2
Router_Additional
Switch_Additional
CCVP (Voice)
MPLS
Voice_Gateway
VPN3000_Modem
Description
NetworkSims.com
Cisco Challenges
This option includes a range of chall
firewall. To activate a challenge, sel
challenge:
Wide range of emulated devices
Double-click on option to activate it
Network Emulators: networksims.com. Author: Prof W Buchanan Version: Napier student(4.7.0 (Build 090309))
File Stand-alone emulators Help
Simulator
Quit Simulator
Show Run
Show Ver
Show History
Requirement
New Chall.
Capture
Param.
Soln
Demo
Requirements Diagram Router 1
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-D-L), Version 12.0(4),
Copyright (c) 1986-1999 by cisco System
Compiled Wed 14-Apr-99 21:21 by ccai
Image text-base: 0x03037C88, data-base:
cisco 2500 (68030) processor (revision L) with 2048K
Processor board ID 13583483, with hardware revision
Bridging software.
X.25 software, Version 3.0.0.
2 Ethernet/IEEE 802.3 interface(s)
2 Serial network interface(s)
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read ON
Unique challenges
Information
Close
Challenge Parameters Details
IP (E0): 201.45.44.2
Subnet (E0): 255.255.255.224
Status (E0): up
Description (E0): sales connection
Speed (E0): 100
Duplex (E0): full
Hostname: dumfries IP: 140.121.5.3
Hostname: washington IP: 194.63.132.9
Hostname: paris IP: 211.199.88.1
Encryption
Integrated lectures
Answer
Please do not press the button below until you have found the fault
Reveal Answer to Fault
Router 3
10.2.2.1/24
10.2.2.2/24
10.3.3.1/24
10.3.3.2/24
10.4.4.2/24
192.168.1.1/24
192.168.2.1/24
R2
R3
R4
R5
H2
H3
s0
s1
e0
e1
Time: 00:00:22
Correct:
0 out of 16
Type: Fault
Challenge No: 1
Fix Fault (5 Router - Incorrect IP address)
Feedback
Router 1: 00:00:04 Configuration mode
Router 1: 00:00:07 Hostname is set to newcastle
Reseting devices (reset Challenge)
Fault-finding exercises
Fun activities
0.25Mbps
0.6Mbps
0.25Mbps
1Mbps
2.25Mbps
1.5Mbps
2.5Mbps
1.75Mbps
1.25Mbps
2.75Mbps
3Mbps
0.75Mbps
2Mbps
0.5Mbps
rate on the box, and check answer with the green button
Time: 00:00:06
Correct:
0 out of 16
Type: Activity
Challenge No: 4
Data Rate Calculations
centre for distributed computing & security
Bill Buchanan
NetworkSims.com
NetworkSims.com

Center for Distributed Computing and Security

Risk Analysis in e-Commerce

Matthew Miehling

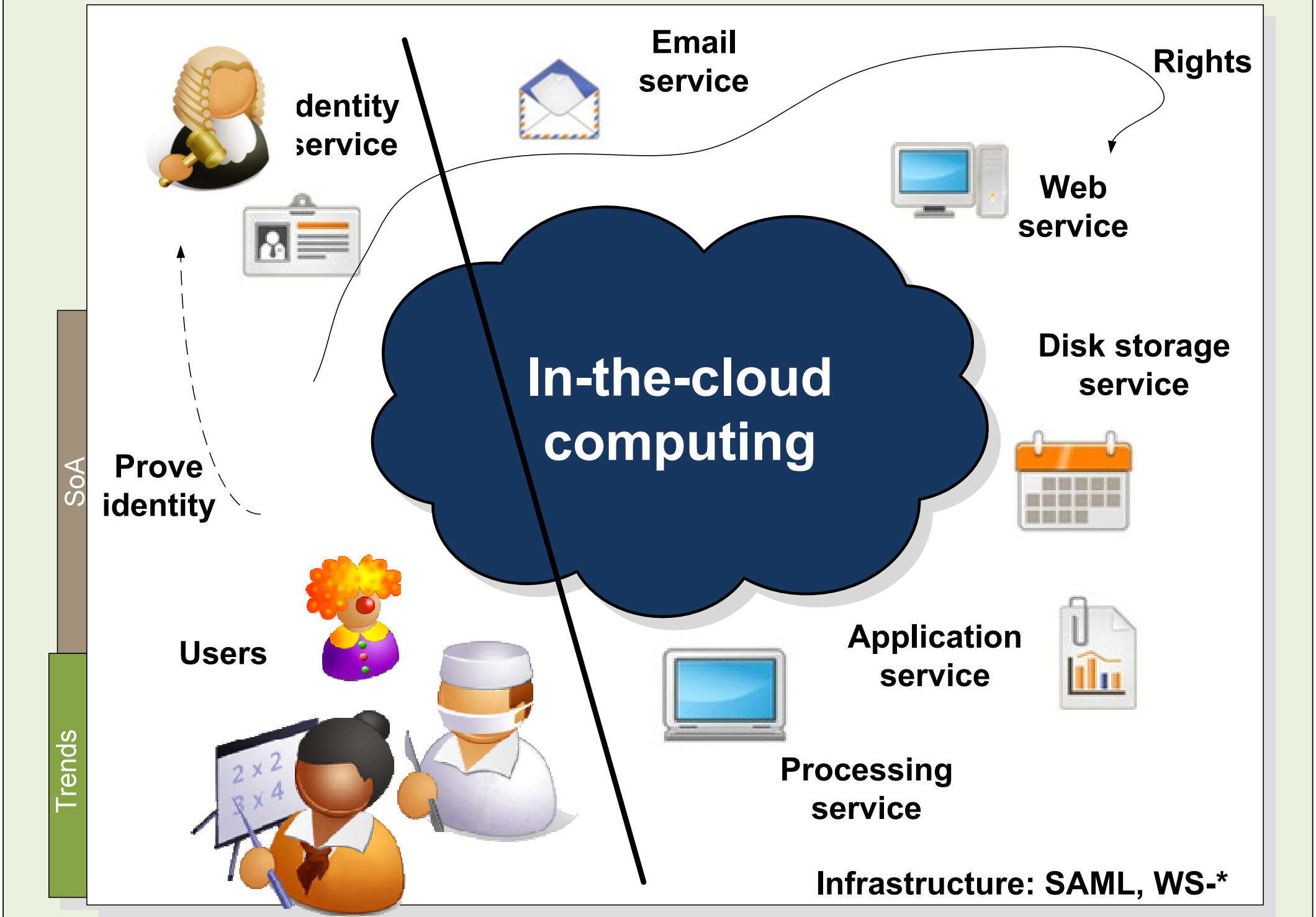
Author: Prof Bill Buchanan

Center for Distributed Computing and Security

Next-Generation Intelligence Gathering Framework

Omair Uthmani

Author: Prof Bill Buchanan


dentity
service
Email
service
Rights
Web
service
In-the-cloud
computing
Disk storage
service
Prove
identity
Users
Application
service
Processing
service
Infrastructure: SAML, WS-*
SoA
Trends
In-the-cloud computing

External access

Data sharing policy/ intelligence

centre for distributed computing & security

Role In domain

Data rights within domain based on role

Domain (Health)

SPoC (Single point-Of-contact)

Domain (Social Services)

Role-based

Federated Identity Provider (Strong – dns)

CDCS

Federated Identity Provider (Weak – google)

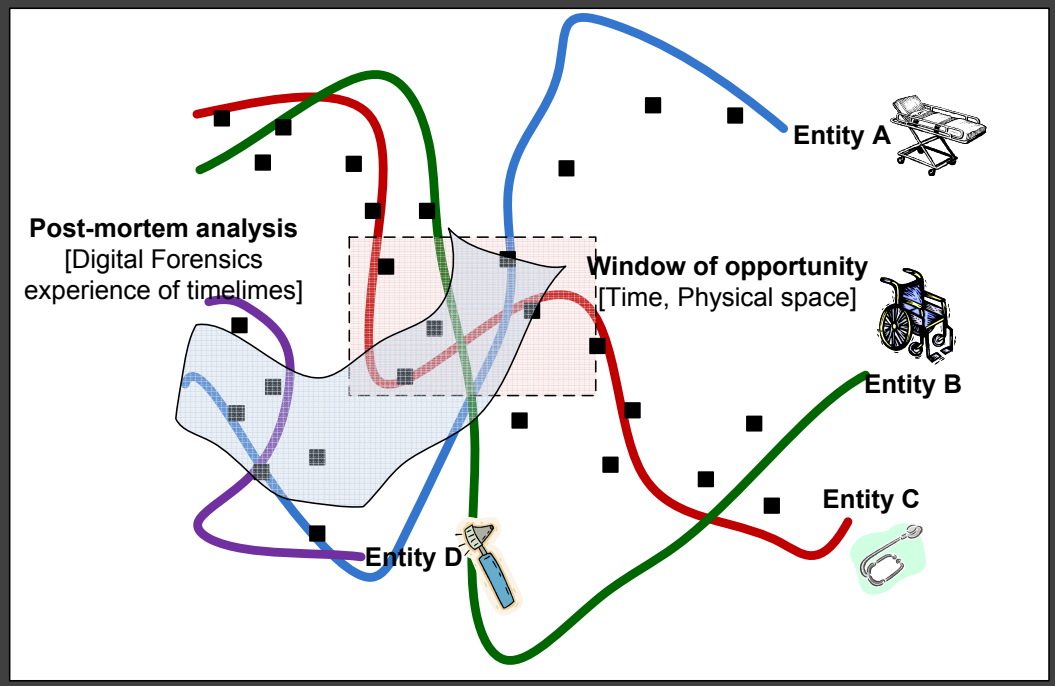
Sub-domain

Domain (Police)

Author: Prof Bill Buchanan

Enhanced data security infrastructure

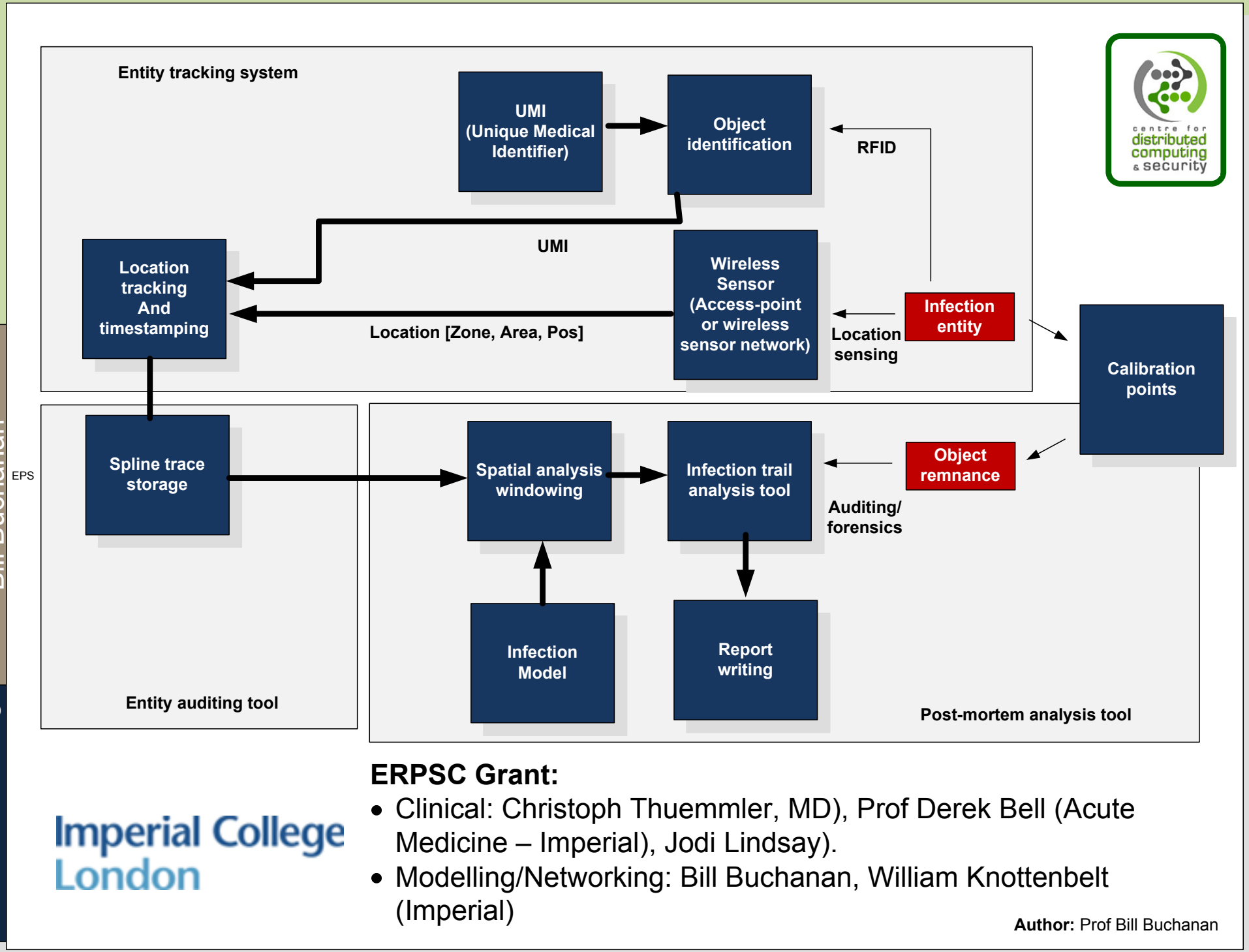
Center for Distributed Computing and Security



Infection Tracking/Modelling Infrastructure

Christoph Thuemmler

Author: Prof Bill Buchanan



Bill Buchanan

EPS

Infection Tracking

Imperial College London

ERPSC Grant:

- Clinical: Christoph Thuemmler, MD), Prof Derek Bell (Acute Medicine – Imperial), Jodi Lindsay).
- Modelling/Networking: Bill Buchanan, William Knottenbelt (Imperial)

Author: Prof Bill Buchanan

Center for Distributed Computing and Security

Current activities:

Digital DNA, Performance Evaluation of Security, Oblivious Transfer Methods ...

Prof Bill Buchanan

Leader, Centre for Distributed Computing and Security

http://www.cdcs.soc.napier.ac.uk/

Author: Prof Bill Buchanan