BCNET ANNUAL HIGHER EDUCATION IT CONFERENCE

LEARN
ENGAGE
SHARE

Teaching a Practical Ethical Hacking Course: Challenges and Solutions

Haytham El Miligi
Assistant Professor, Computing Science Dept.,
Thompson Rivers University

BCNET
Conference 2016

ETHICAL HACKING

When art meets science

BCNET
Conference 2016

Ethical Hacking

Assessing the security of computer systems or networks using penetration testing techniques.

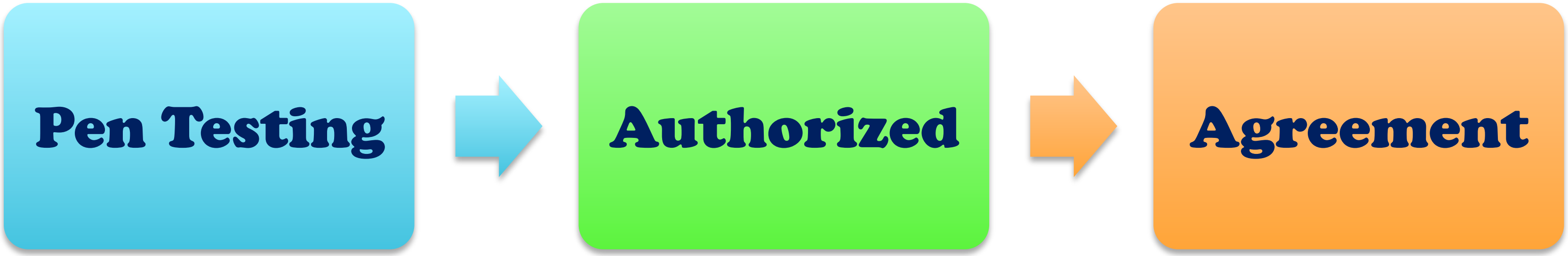
Ethical Hacking

Penetration testing of computer systems or networks must be authorized by owners.

Ethical Hacking

Authorization is granted by signing a written agreement that details the objectives, procedures, and expected impacts on target systems for each test.

Ethical Hacking



Pen Testing

Authorized

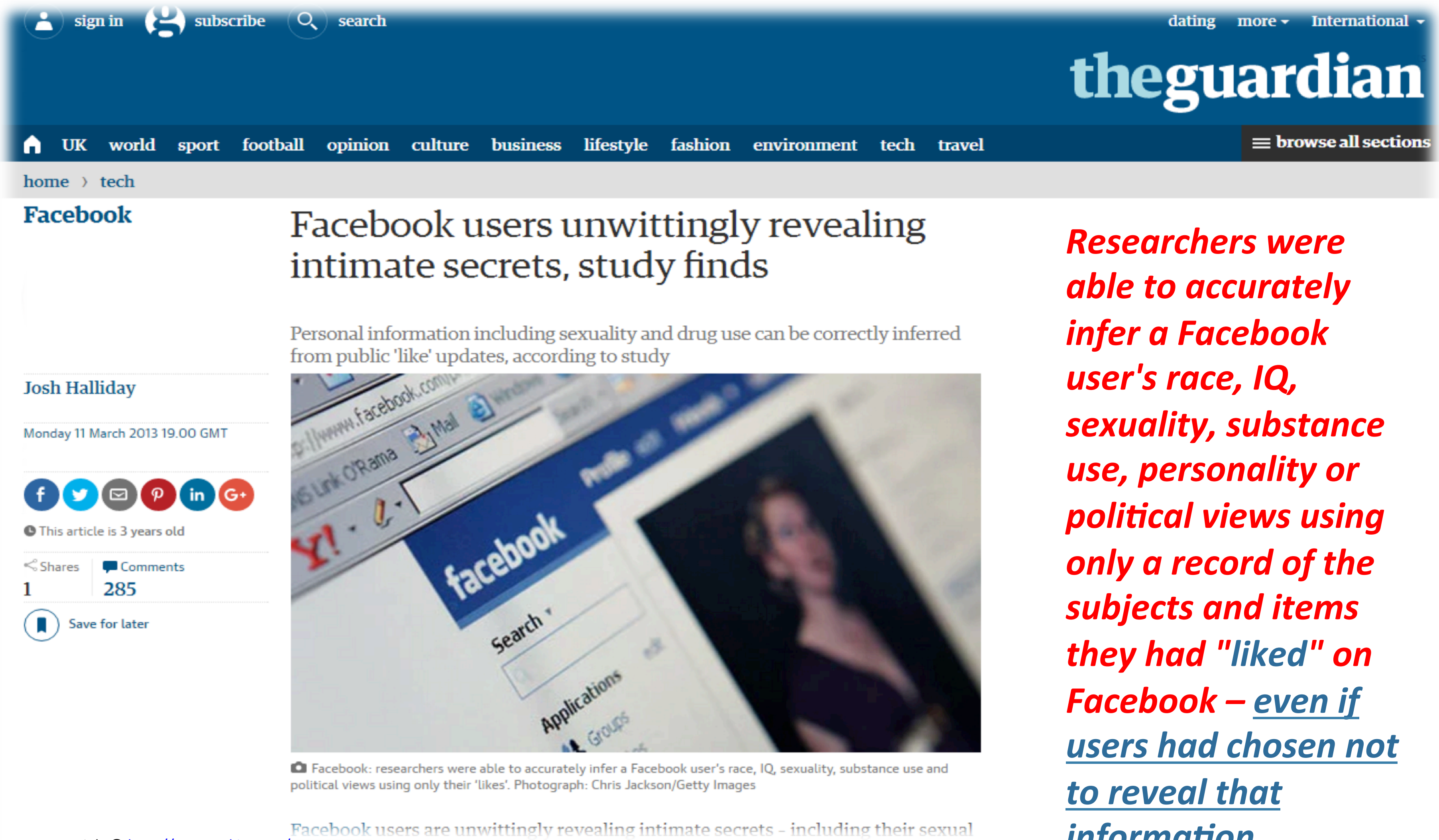
Agreement

What do Pen-Testers do?

A pentester’s evaluation of a system’s security seeks answers to three basic questions:

1. **What can an intruder see on the target systems?**
2. **What can an intruder do with that information?**
3. **Can anyone at the target notice the intruder’s attempts or successes?**

Pen-Testing Process



Facebook

Facebook users unwittingly revealing intimate secrets, study finds

Personal information including sexuality and drug use can be correctly inferred from public 'like' updates, according to study

Josh Halliday

Monday 11 March 2013 19.00 GMT

This article is 3 years old

Shares	Comments
1	285

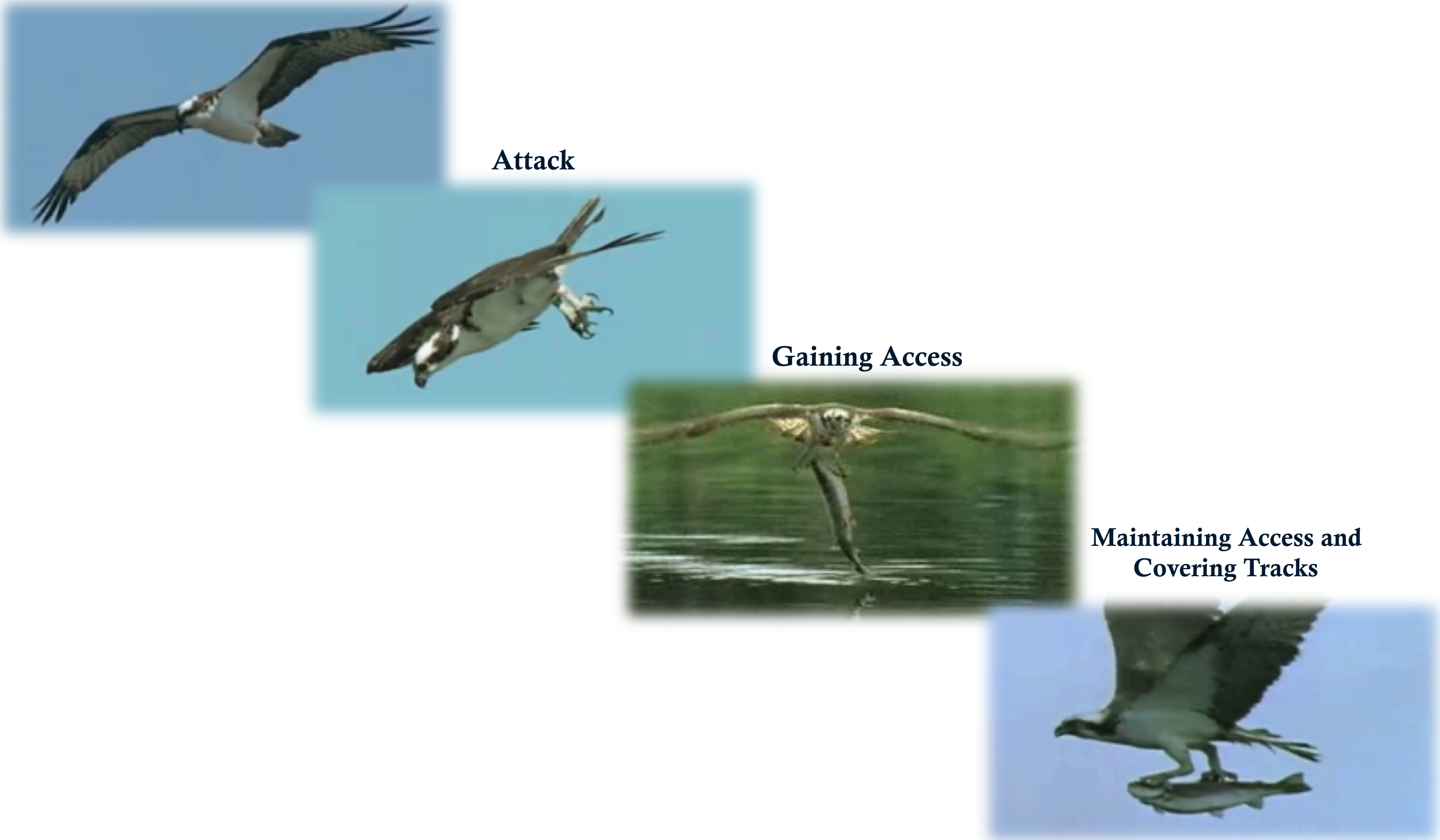
Facebook: researchers were able to accurately infer a Facebook user's race, IQ, sexuality, substance use and political views using only their 'likes'. Photograph: Chris Jackson/Getty Images

Facebook users are unwittingly revealing intimate secrets – including their sexual

Researchers were able to accurately infer a Facebook user's race, IQ, sexuality, substance use, personality or political views using only a record of the subjects and items they had "liked" on Facebook – even if users had chosen not to reveal that information.

Image copyright© http://www.arkive.org/
Educational license under http://www.arkive.org/about/terms-of-use
Target Article: http://www.forbes.com/
The Guardian article: www.theguardian.com

Pen-Testing Process



Reconnaissance and Target Scanning

Attack

Gaining Access

Maintaining Access and
Covering Tracks

Image copyright© http://www.arkive.org/
Educational license under http://www.arkive.org/about/terms-of-use

Vulnerability Scanning vs Pen-Testing

Vulnerability Scan

- Looks for known vulnerabilities in your systems and reports potential exposures.
- Focus: Breadth over depth.
- Vulnerability scans are list-oriented.
- Vulnerability scans depend primarily on tools.

Pen-Testing

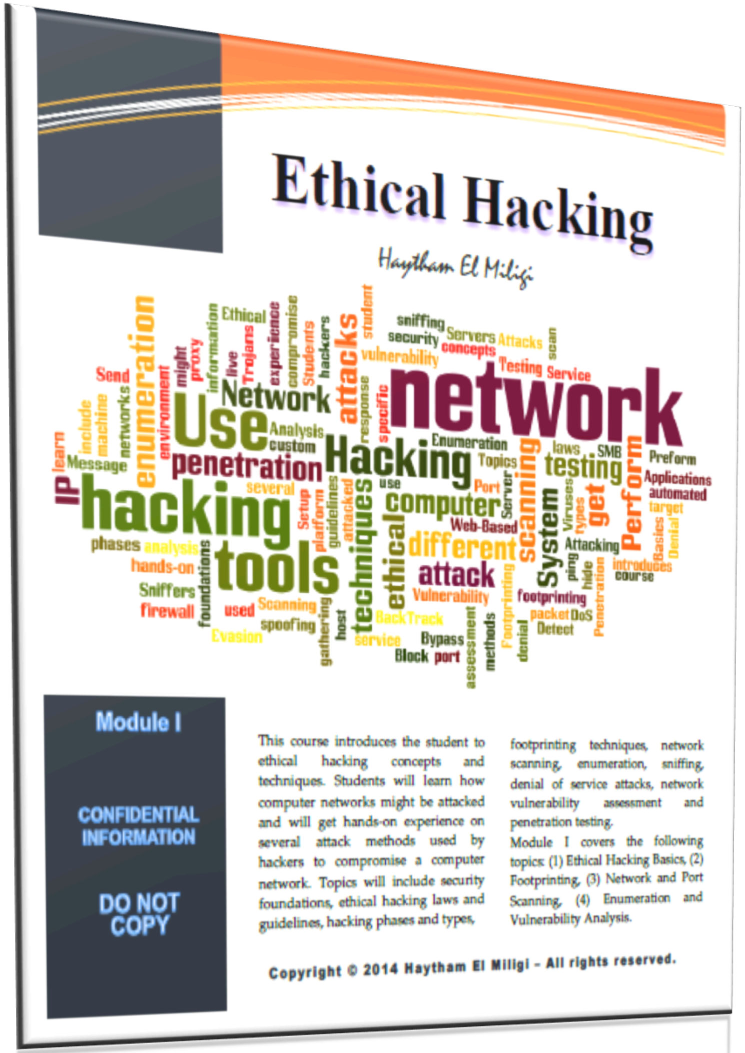
- Is designed to actually exploit weaknesses in the architecture of your systems.
- Focus: Depth over breadth.
- Penetration tests are goal-oriented.
- Penetration tests depend primarily on skills.

TEACHING COMP 4980: ETHICAL HACKING

Challenges and Solutions

BCNET
Conference 2016

COMP 4980: Ethical Hacking



Ethical Hacking

Haytham El Miligi

Module I

CONFIDENTIAL INFORMATION

DO NOT COPY

This course introduces the student to ethical hacking concepts and techniques. Students will learn how computer networks might be attacked and will get hands-on experience on several attack methods used by hackers to compromise a computer network. Topics will include security foundations, ethical hacking laws and guidelines, hacking phases and types, footprinting techniques, network scanning, enumeration, sniffing, denial of service attacks, network vulnerability assessment and penetration testing.

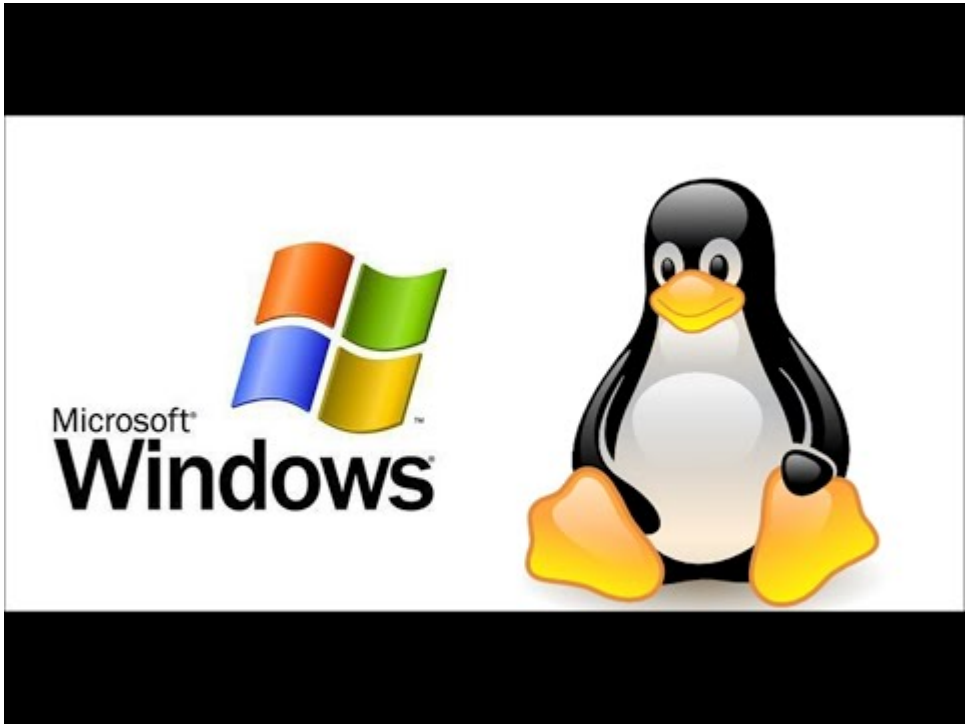
Module I covers the following topics: (1) Ethical Hacking Basics, (2) Footprinting, (3) Network and Port Scanning, (4) Enumeration and Vulnerability Analysis.

Copyright © 2014 Haytham El Miligi - All rights reserved.

Ethical Hacking Topics

- Ethical Hacking Basics
- Footprinting
- Network and Port Scanning
- Enumeration and Vulnerability Analysis
- Hacking Through the Network
- Attacking a System (DoS attacks)
- Web-Based Hacking: Servers and Applications
- Trojans, Viruses and Other Attacks
- Penetration Testing

Labs ?



Source: https://search.creativecommons.org/ -> https://www.google.ca/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=0ahUKEwjN99iTgIfMAhUJKWMKHb3CAV4QjhwIBQ&url=https%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3D-QsN-57bx8E&bvm=bv.119028448,d.cGc&psig=AFQjCNH13Ll_7pjOkmlkVeOZ1AsGztf3wQ&ust=1460478376277921
Labeled for reuse with modification - Creative Commons Attribution 4.0 License.
Original windows logo belong to Microsoft Windows and Linux logo by Larry Ewing.

Lab Objectives

- ✓ **Simulate Real-Life Environments**
- ✓ **Setup Flexible Network Configurations**
- ✓ **Protect TRU Network**
- ✓ **Provide Rich Hands-on Experience**

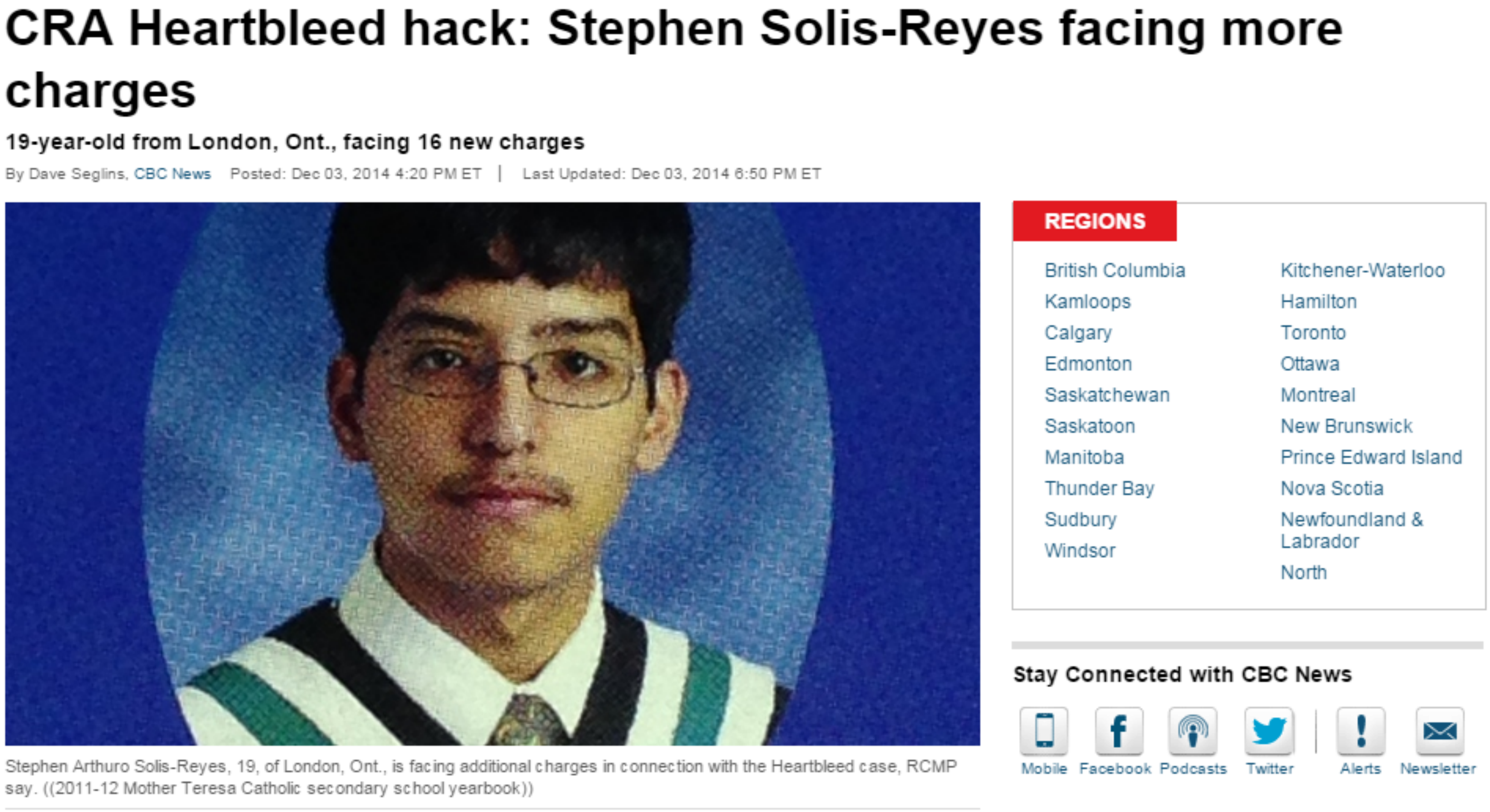
Students need to try!

Why?

HeartBleed Hack - 2014

Heartbleed Bug

HeartBleed Hack - 2014



CRA Heartbleed hack: Stephen Solis-Reyes facing more charges

19-year-old from London, Ont., facing 16 new charges

By Dave Seglins, CBC News Posted: Dec 03, 2014 4:20 PM ET | Last Updated: Dec 03, 2014 6:50 PM ET

Stephen Arthuro Solis-Reyes, 19, of London, Ont., is facing additional charges in connection with the Heartbleed case, RCMP say. ((2011-12 Mother Teresa Catholic secondary school yearbook))

REGIONS

- British Columbia
- Kamloops
- Calgary
- Edmonton
- Saskatchewan
- Saskatoon
- Manitoba
- Thunder Bay
- Sudbury
- Windsor
- Kitchener-Waterloo
- Hamilton
- Toronto
- Ottawa
- Montreal
- New Brunswick
- Prince Edward Island
- Nova Scotia
- Newfoundland & Labrador
- North

Stay Connected with CBC News

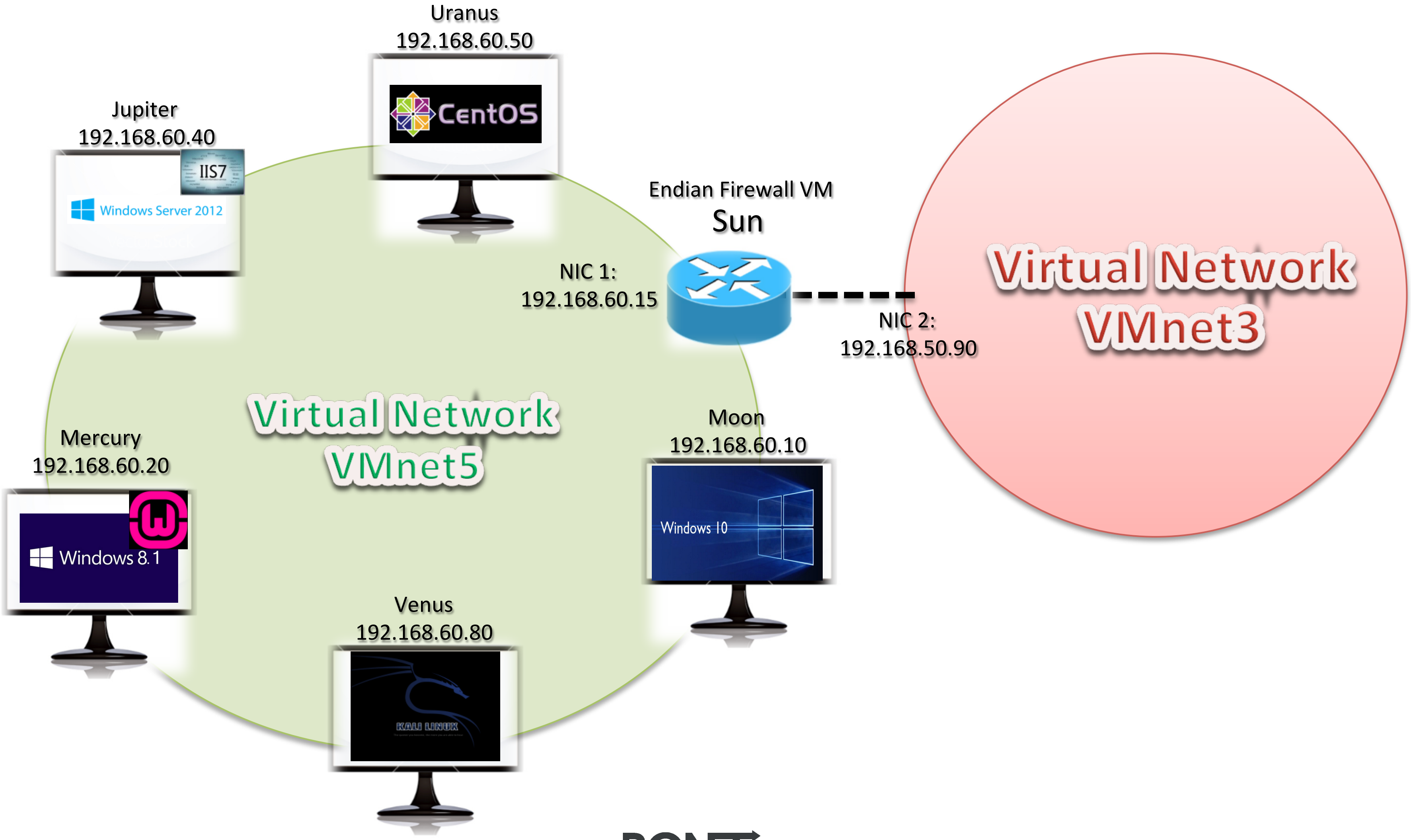
Source: http://www.cbc.ca/news/canada/cra-heartbleed-hack-stephen-solis-reyes-facing-more-charges-1.2859416

RCMP laid 16 new charges against Stephen Solis-Reyes involving alleged hacks against the CRA, as well as the computers of the University of Western Ontario, the London District Catholic School Board, and an offshore email service, Jersey Mail, among others.

Looking for an Island!

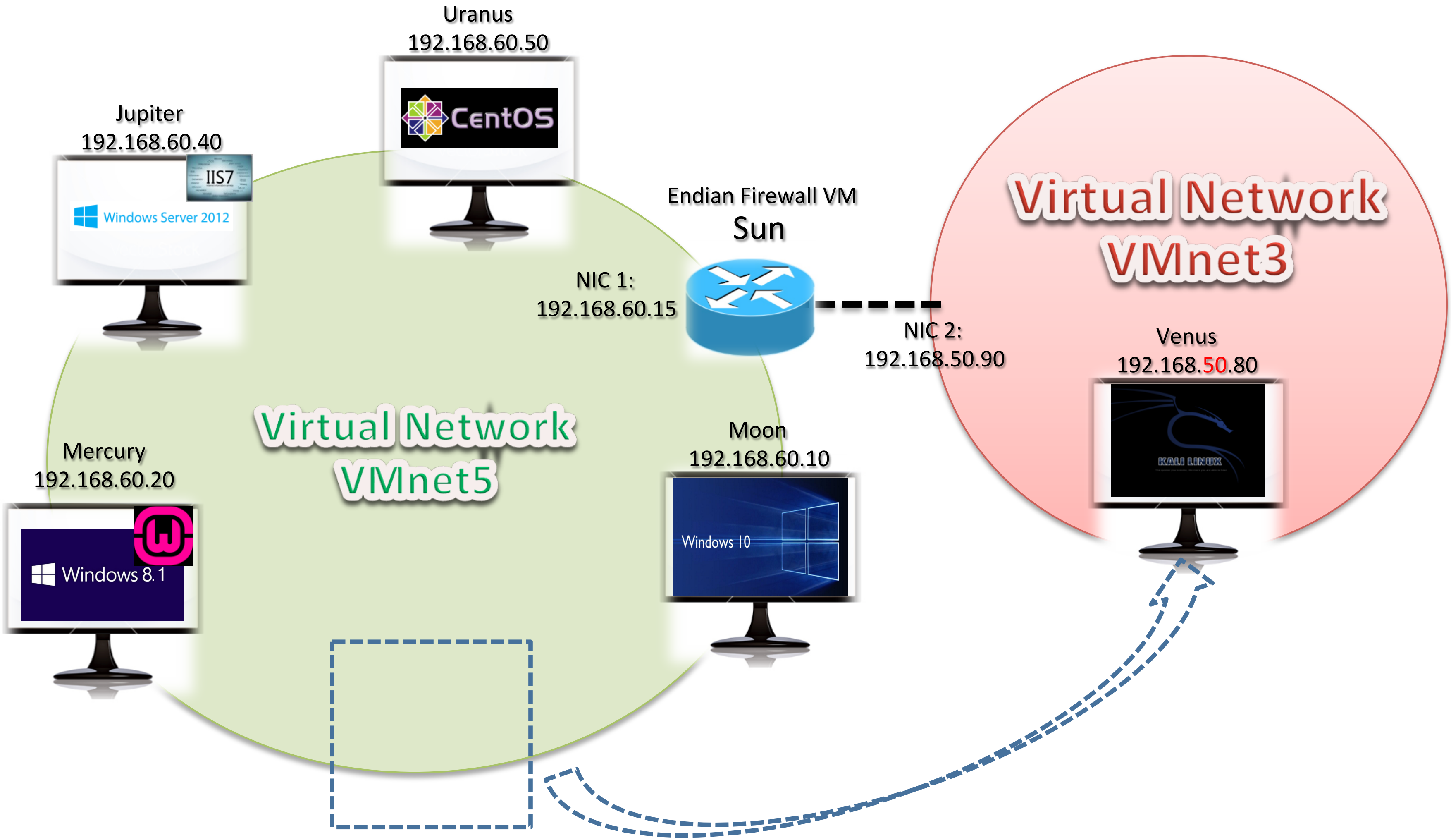
Source: https://search.creativecommons.org/ -> https://www.google.ca/search?site=imghp&tbm=isch&q=island&tbs=sur:fmc&gws_rd=cr&ei=1dQLV4PRBcSgjwORtLuIBg#gws_rd=cr&imgrc=HgLn7nW-BlOLAM%3A
Labeled for reuse with modification - Creative Commons Attribution 4.0 License.

Lab Setup



BCNET
Conference 2016

Lab Setup


Uranus
192.168.60.50
CentOS
Jupiter
192.168.60.40
IIS7
Windows Server 2012
Endian Firewall VM
Sun
NIC 1:
192.168.60.15
NIC 2:
192.168.50.90
Virtual Network
VMnet3
Venus
192.168.50.80
KALI LINUX
Virtual Network
VMnet5
Mercury
192.168.60.20
Windows 8.1
Moon
192.168.60.10
Windows 10

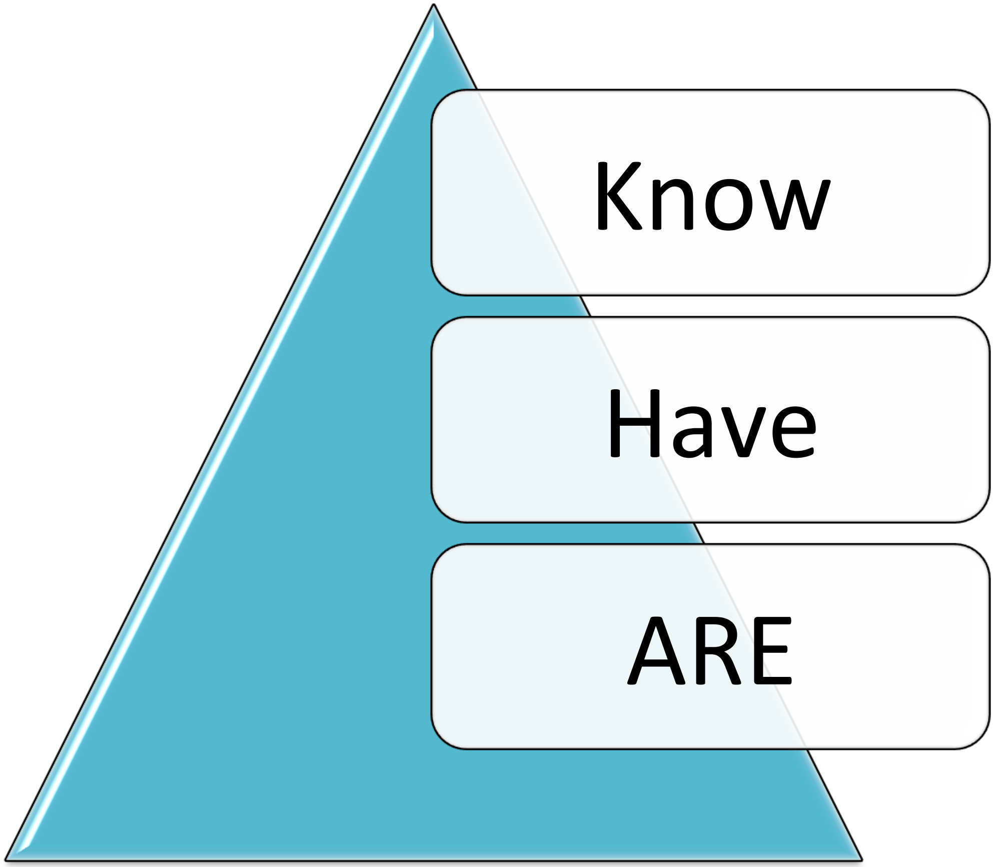
THE FUTURE OF PEN-TESTING

The end of password era

BCNET
Conference 2016

Pass~~words~~codes

Passcodes



Know

Have

ARE

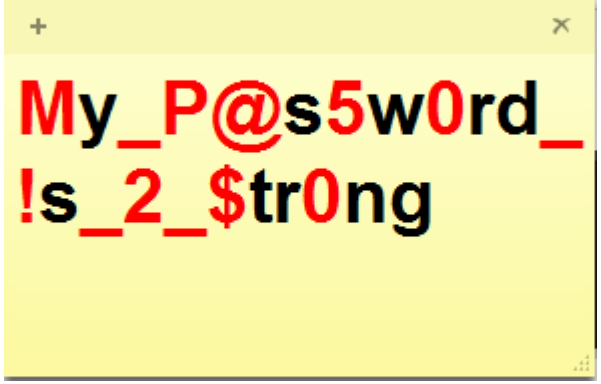
Passcodes - Passwords

mypasswordistoostrong

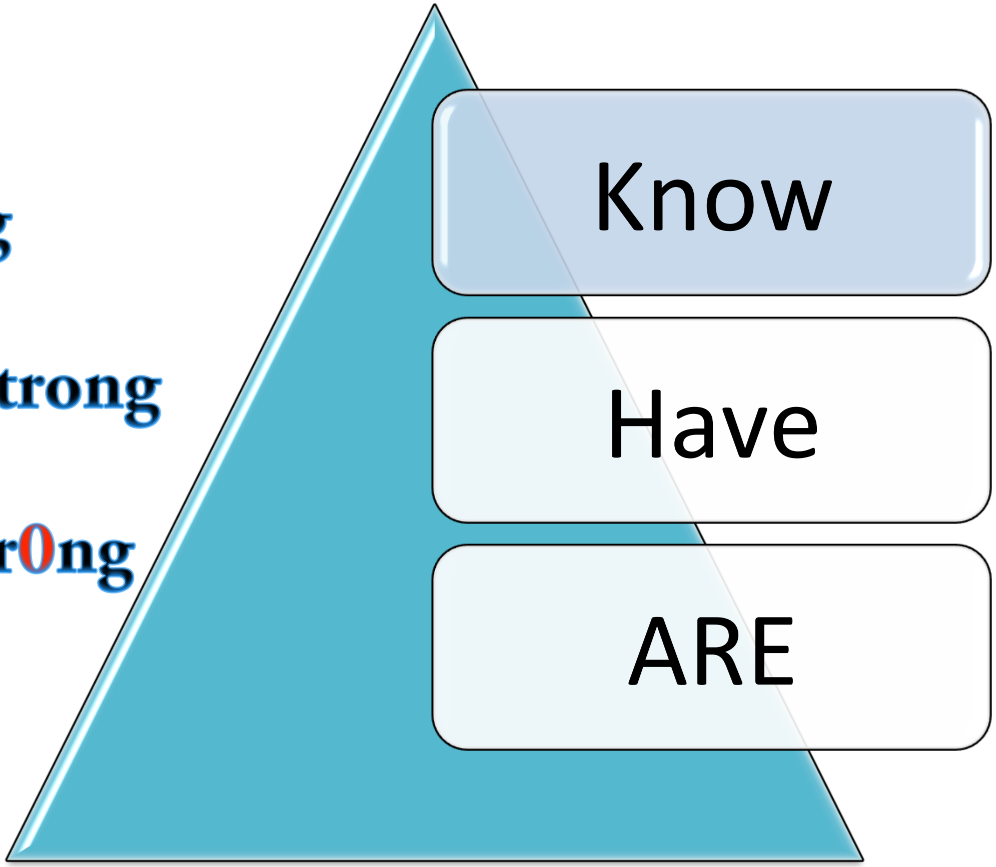
MyPasswordistooStrong

My_Password_is_too_Strong

My_P@s5w0rd_!s_2_$tr0ng



My_P@s5w0rd_!s_2_$tr0ng



Know

Have

ARE

Passcodes: Security Tokens

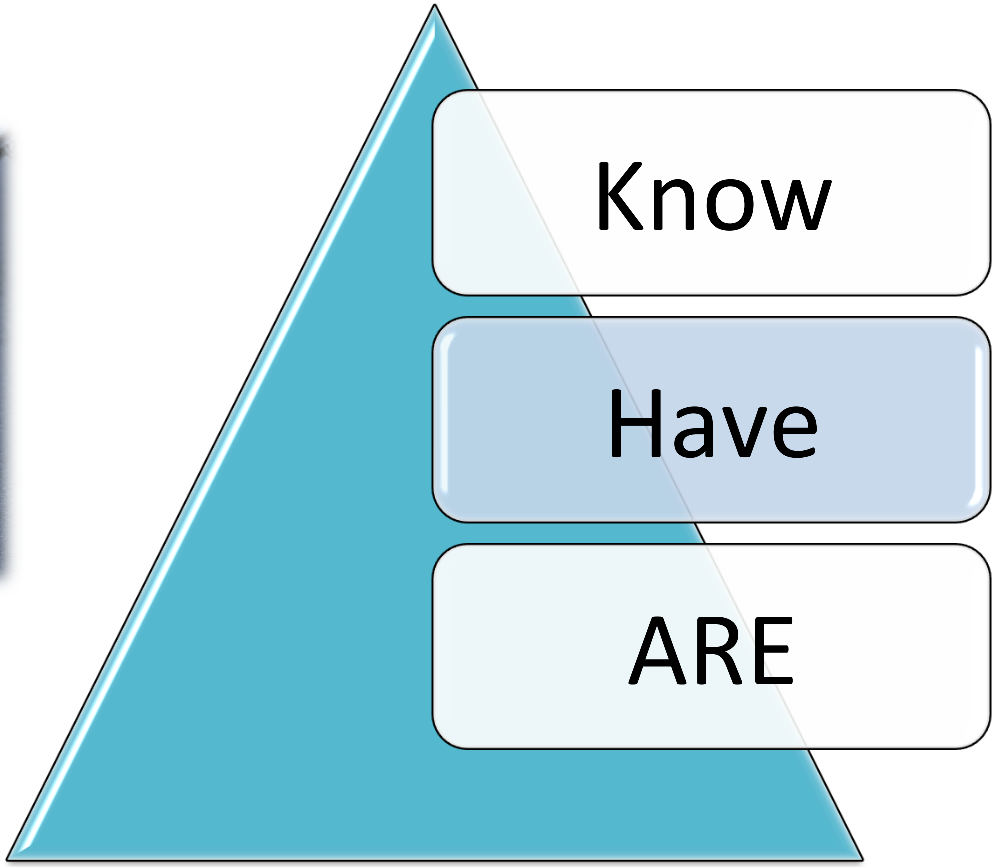


Image copyright© http://sciencestockphotos.com/
Creative Commons Attribution 4.0 License

Passcodes: Biometrics

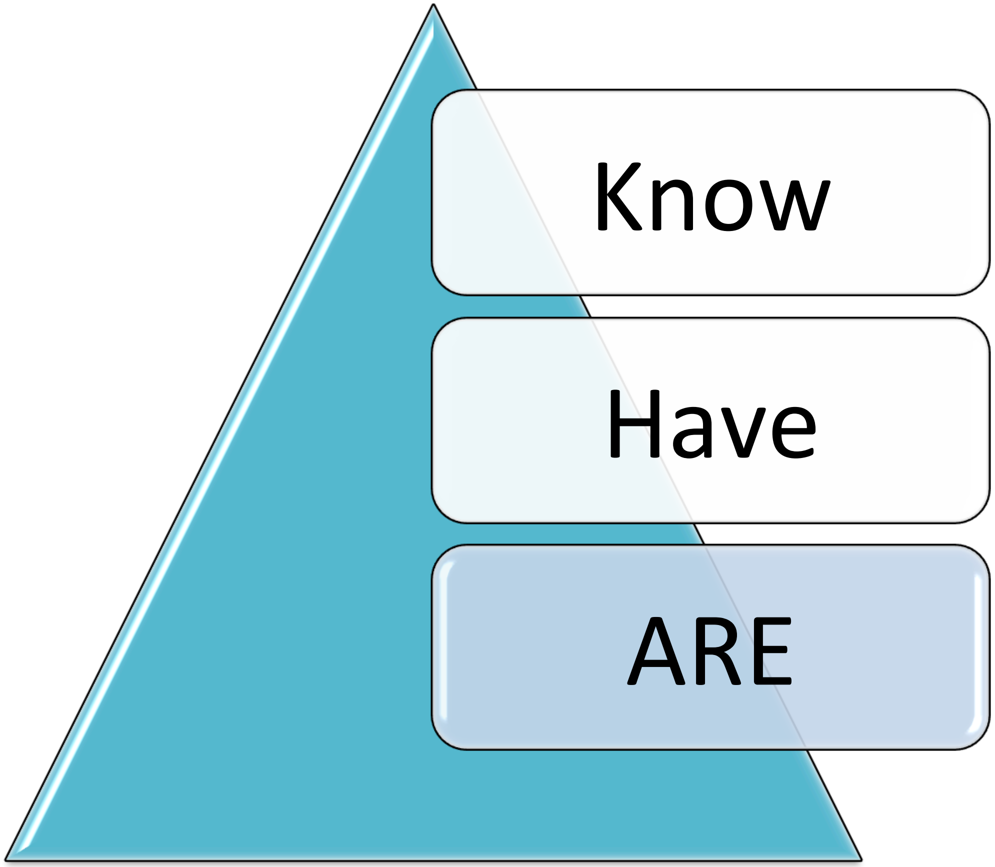
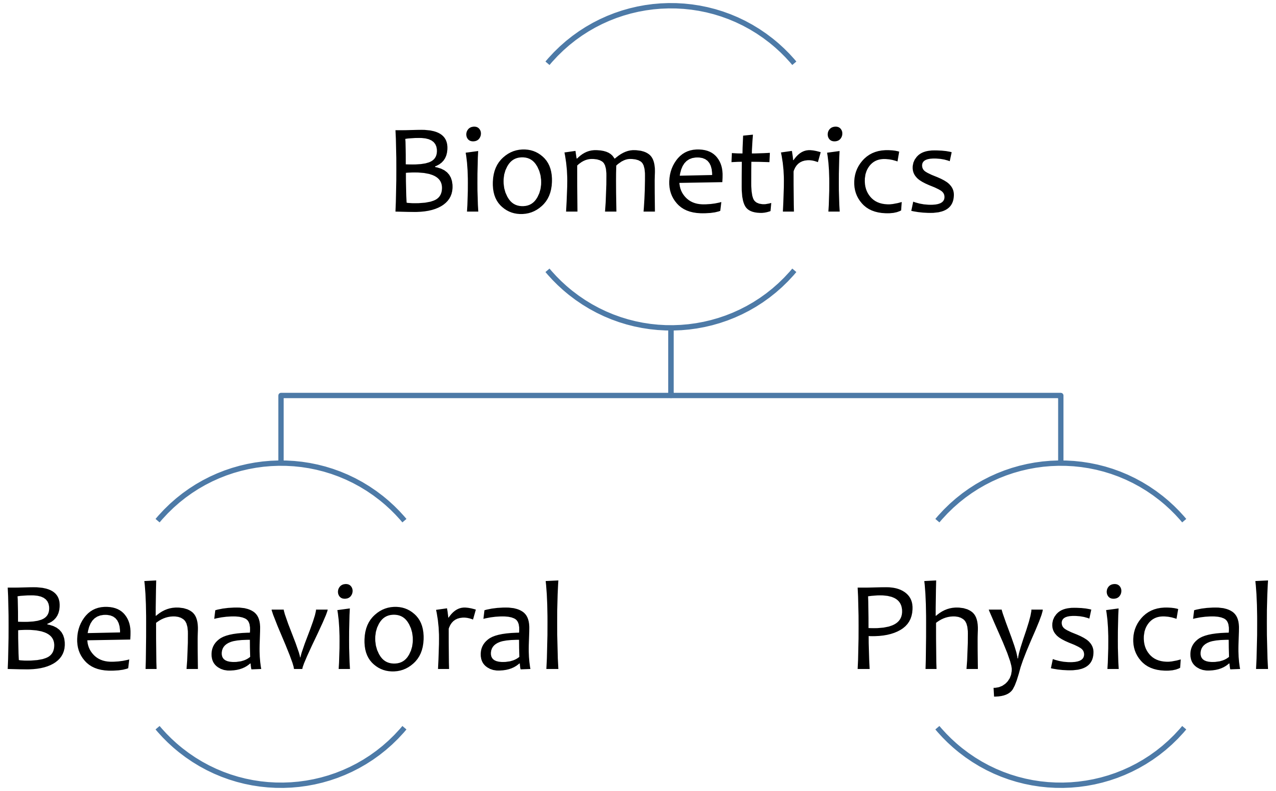
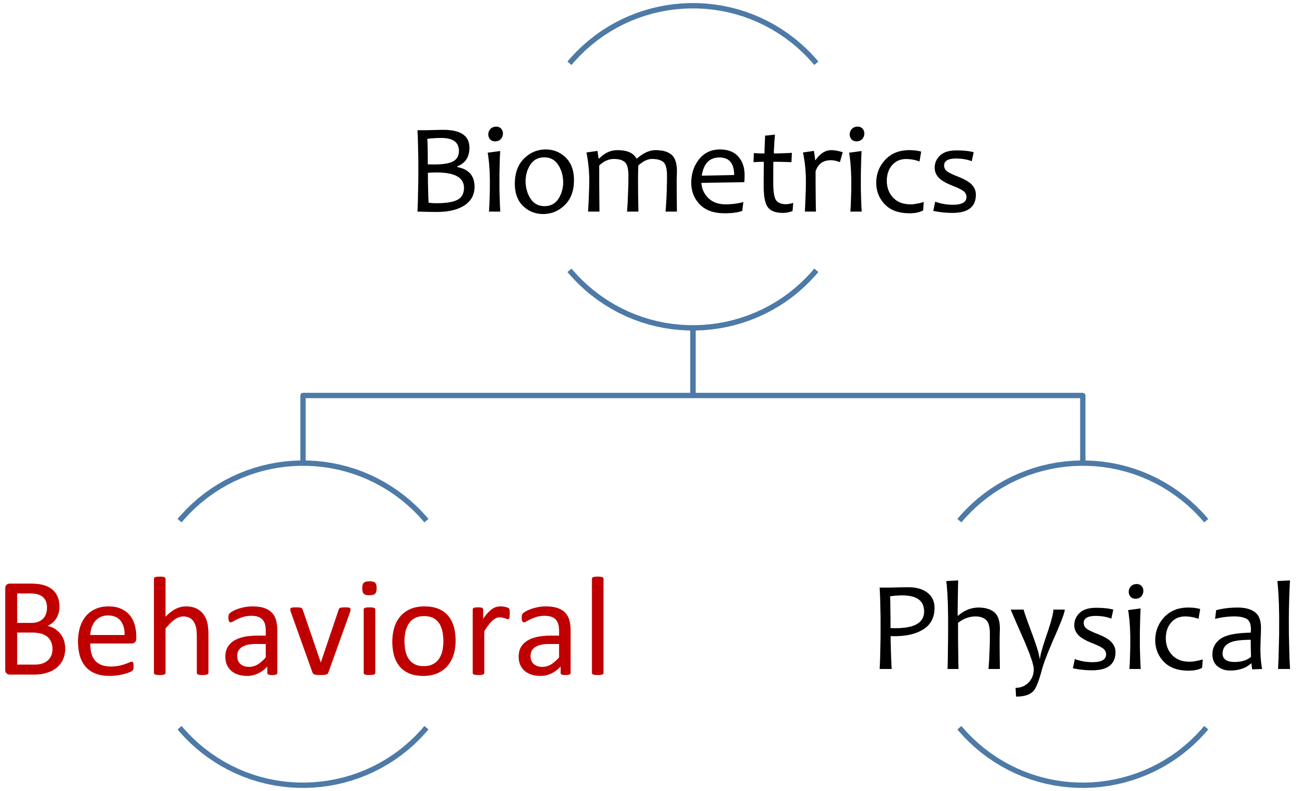


Image copyright© http://sciencestockphotos.com/, https://www.pexels.com
Creative Commons Attribution 4.0 License

Passcodes: Biometrics



Passcodes: Biometrics



Biometrics

Behavioral

Physical

Passcodes: Keystroke dynamics

Image copyright© https://www.pexels.com
Creative Commons Attribution 4.0 License

Passcodes: Behavioral Biometrics

Keystroke dynamics

Keystroke dynamics refer to the unique patterns of rhythm and timing-based features that are created when a user types on a keyboard.

Passcodes: Behavioral Biometrics

IPROFILE

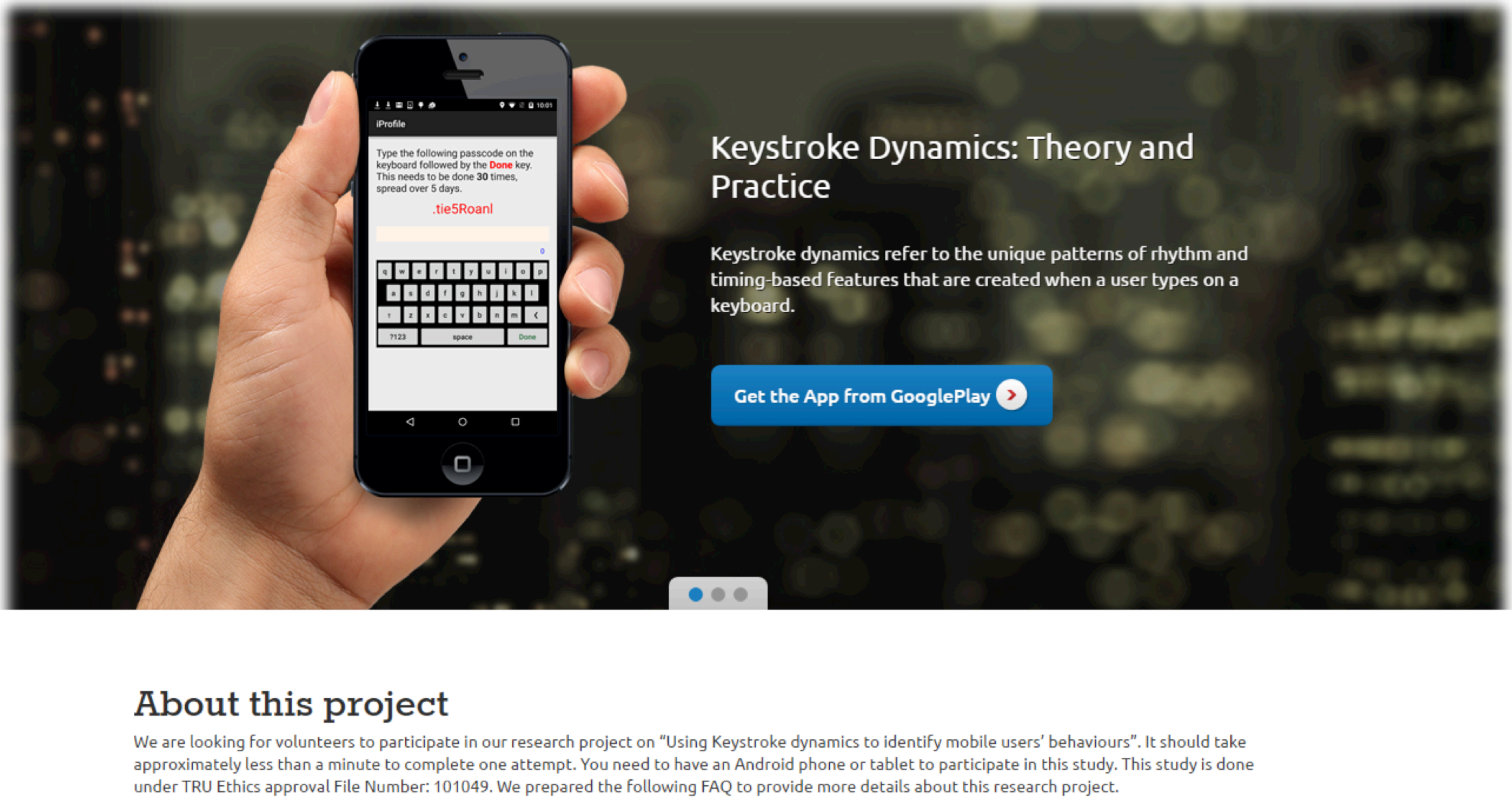
iProfile

Type the following passcode on the keyboard followed by the **Done** key. This needs to be done **30** times, spread over 5 days.

.tie5Roanl

www.iprofileapp.com

Passcodes: Behavioral Biometrics



iProfile

Type the following passcode on the keyboard followed by the **Done** key. This needs to be done **30** times, spread over 5 days.

.tie5Roanl

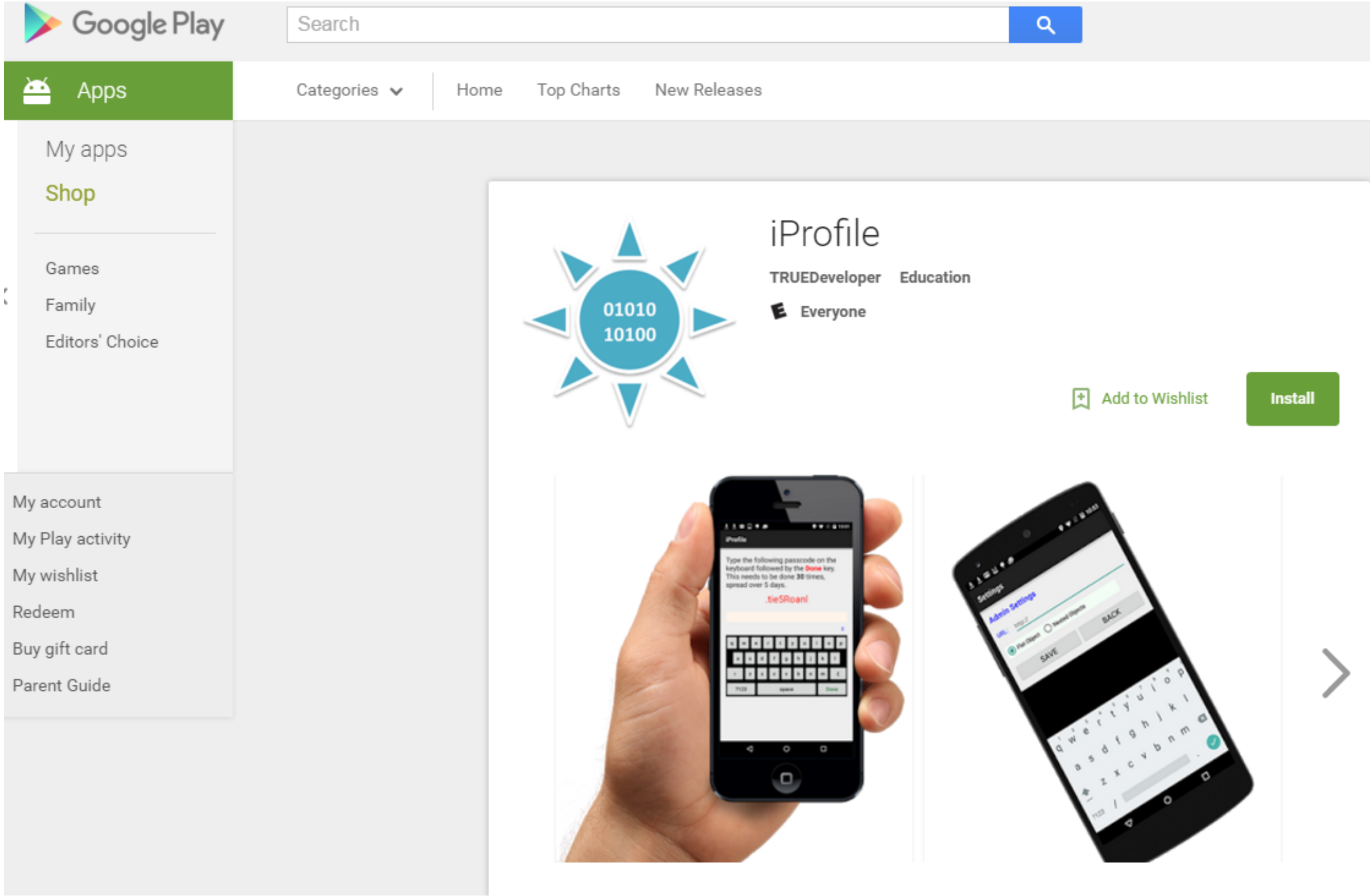
Keystroke Dynamics: Theory and Practice

Keystroke dynamics refer to the unique patterns of rhythm and timing-based features that are created when a user types on a keyboard.

About this project

We are looking for volunteers to participate in our research project on "Using Keystroke dynamics to identify mobile users' behaviours". It should take approximately less than a minute to complete one attempt. You need to have an Android phone or tablet to participate in this study. This study is done under TRU Ethics approval File Number: 101049. We prepared the following FAQ to provide more details about this research project.

Passcodes: Behavioral Biometrics



iProfile

TRUEDeveloper Education

Everyone

Type the following passcode on the keyboard followed by the Done key. This needs to be done 30 times, spread over 5 days.

.tie5Roanl

Thank You!