predict
prioritise
prevent

TREsPASS

Technology-Supported
Risk
Estimation by
Predictive
Assessment of
Socio-Technical
Security

Security Nightmare 2015 – Cloud Attack!

Cybercrime Social Engineering Analysis Challenge

TREsPASS invites you to the Social Engineering Challenge 2015. You can apply by submitting your proposal before December 15th. After selection by a professional jury, the award-winning proposal will be announced at the CPDP conference in Brussels, Belgium, on January 27-29, 2016.

Cybercrime is increasing rapidly all around the globe. Methods such as phishing, scamming, and hacking are becoming more sophisticated. At the same time, cloud computing has taken off and much of our data is stored and processed in public and corporate cloud data centers, dynamically crossing geographic borders, accessible through the network from anywhere. To counteract this pervasive problem, organisations have investigated technical solutions as well as awareness programs for employees and customers. As Social Engineering is a key factor in 92% of industrial espionage attacks (Verizon), the human factor is attracting increasing media –and attacker– attention. However, systematic analysis of the securing against attacks including Social Engineering is still rare, and scientists and practitioners from diverse research disciplines are trying to understand the mechanisms behind it more holistically.

But you can help! This year, you are invited to think of attack scenarios for a cloud-based setting. Though this might include some clever technical steps, tricking the human element of security is what this challenge is about: the ultimate security nightmare. We are not looking for new hacking tools, spam bots, phishing attacks, blackmail, etc., but rather how you, as an outsider, could gain access to the crucial and famous *fileX* stored in the cloud that would give you money and fame, if you could get your hands on it.

To make the given setting more concrete, imagine a scenario as described on www.trespass-project.eu/award.

To give you some ideas and stimulate your creativity, you may wish to visit the *Social Engineering Panel* at http://www.youtube.com/watch?v=WrdrwiTlVoo.

Describe your Social Engineering cloud attack idea and include a suitable countermeasure to prevent your scenario from taking place: think of policies, access controls, etc. It would be ideal if you also provide a short outline of an experiment/research proposal that could be used to test the feasibility or relevance of your attack scenario.

Submit your 2-page proposal and a 1-page CV **before December 15th 2015** to http://easychair.org/conferences/?conf=trespasssec15.

The proposals will be evaluated and judged based on creativity, feasibility and deceivability. The best proposal will be awarded with €750 and the winner will be invited to the CPDP 2015 conference to receive the award. A maximum of €800 travel costs will be reimbursed.

Good luck,

TREsPASS project (Contact TREsPASS@zurich.ibm.com).

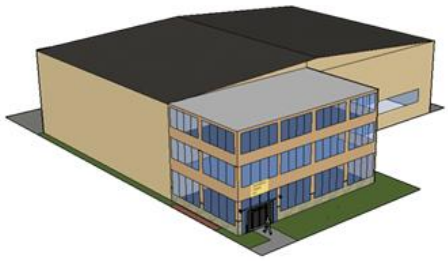
European Commission

SEVENTH FRAMEWORK PROGRAMME

This project receives funding from the European Commission's Seventh Framework Programme under Grant Agreement No.

International Traders Ltd. (ITL)

Imagine the medium sized company called **International Traders Ltd. (ITL)**.
ITL's is a commodity trader – they buy and sell oil and gas related investments around the world for an international set of clients. They own an office with a co-located datacenter.



Much of their trading is automated and they have a large IT department.
The key company asset *fileX* is a list of international clients with the following details

1. The clients names and address
2. Bank Account details
3. Clients Investment portfolio
4. Details of investment transactions dating back 5 years

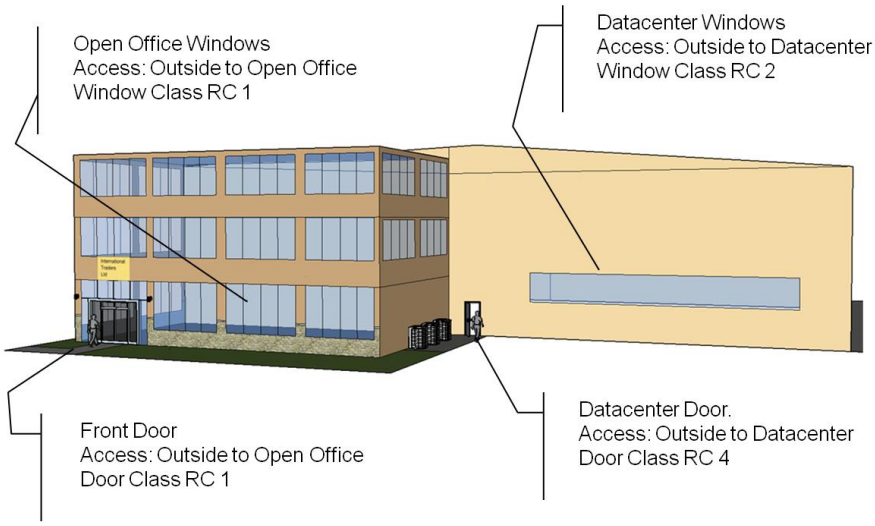
ITL has a number of departments including:

- A **marketing and sales** department that is responsible for developing investment packages
  - The marketing data is informational in nature and not considered sensitive
  - The marketing and sales data is stored with all other non sensitive data on the marketing computer system
- A **trading** department that handles all transaction with clients
  - The client data and financial transactions are considered sensitive information and are stored on a separate trading computer system
- An **IT** department that is responsible for the companies computing infrastructure. This includes:
  - Networks, switches, routers etc
  - Servers
  - Applications

Some key people in the company are

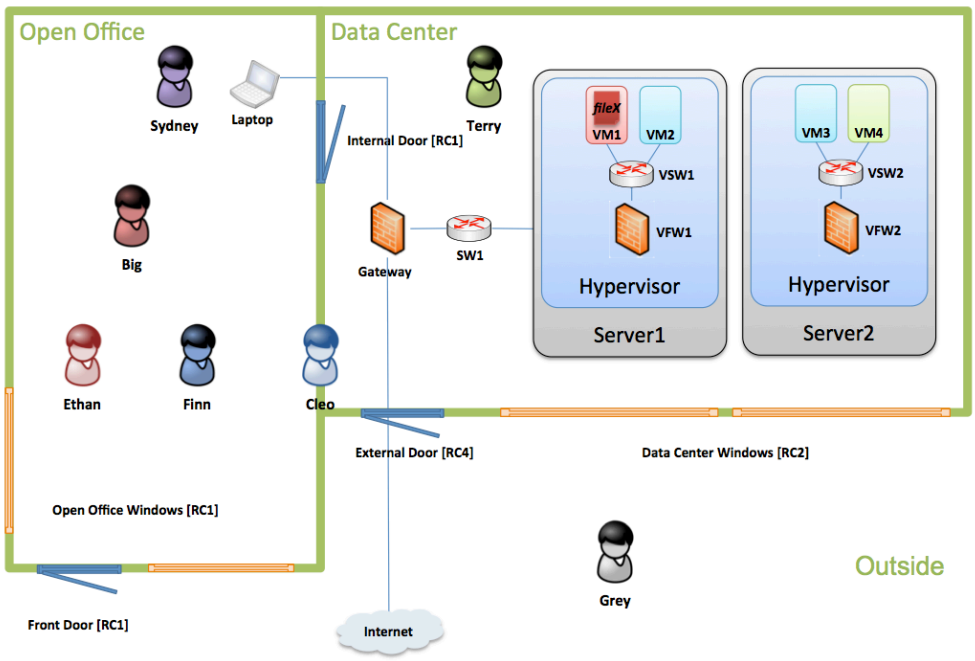
Actor	Job/Role	Department	Physical Access	Logical Access
Ethan	Fraud investigator	Trading dept	Up to Open Office	To VM1
Finn	Finance manager	Marketing dept	Up to Open Office	To VM3
Terry	Technician	IT department	Everywhere	No access
Sydney	IT system administrator	IT department	Everywhere	Full access
Cleo	Cleaning personnel	External contractor	Everywhere	No access
Grey	External visitor	N/A	No access	No access
Big	CEO	N/A	Up to Open Office	Read access

Their main office building is located in a busy industrial area and consists mostly of an open office space and the data center room.



The office is open plan. On the ground floor is front door access to the office space. All employees have a badge access through the front door [Security Class RC2].
An internal door leads directly into the data center. This door is access controlled and only data center staff has access [Security Class RC1].
The bottom floor of the open office has a number of large windows [Security Class RC1].

The data center is directly attached to the office space from where it is accessible through an internal door. This door is access controlled and only data center staff has access [Security Class RC1].
There is a separate external door directly into the data center. This door is used to bring in computer supplies. It is a secure door that can only be opened from the inside [Security Class RC4].
The data center has two large windows [Security Class RC2].



The cloud infrastructure is running on two physical servers, both located in the Data Center. On each server, two virtual machines, a virtual switch and a virtual firewall are running on top of a Hypervisor. These virtual components are connected to physical network components, namely switch SW2 and a Gateway. Through this connection it is possible to reach the physical and virtual infrastructure from the Laptop.

The sensitive document ***fileX*** is located in the storage of VM1. This is currently stored together with the trading solution. The marketing department has a separate solution.
Both systems are on physically separate host systems within the data centre.

APPENDIX: Door and Window Classifications

Security class RC	Burglary type *	Use
1	Basic protection against burglary by the use of physical force	Premises without increased risk of burglary
2	Occasional burglar uses basic burglary tools	Increased protection for normal housing security
3	Experienced burglar uses heavy duty drilling and hammering tools	High level of security for the premises in view of increased risk of burglary
4	Experienced burglar additionally uses electric saws and power drilling tools	Extra high level of housing protection in view of high risk of burglary
5	Experienced burglar additionally uses power cutting and heavy duty drilling tools	Extremely high protection for military and industrial premises. Minimum door weight- 300 kg
6	Experienced burglar additionally uses power cutting and heavy duty drilling tools	Extremely high protection for military bunkers, etc. Minimum door weight- 500 kg

** see http://www.door.lt/en/security-classes for details*