Confidentiality Risks for Engineers:

5 Tools for Secure Engineering Communications

Dr. Terence Love FDRS, AMIMechE, MISI
IT Coordinator, IMechE Australian Branch
Director, Love Services Pty Ltd
admin@loveservices.com.au

Event notes:

The following presentation is for educational purposes and was presented on 16 April 2015 as a joint technical lecture of the *Institution of Mechanical Engineers*, *Engineers Australia*, the *American Society of Mechanical Engineers* and the *Australian Society for Bulk Solids Handling* at the Engineers Australia Auditorium, West Perth.

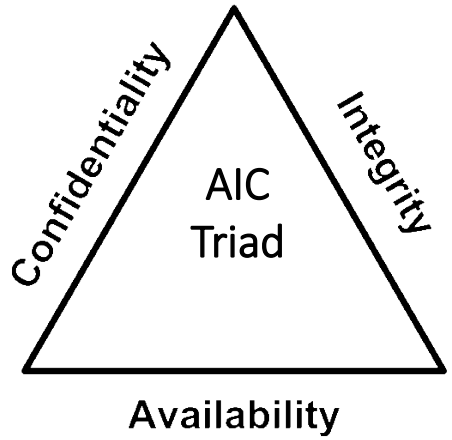
The presenter was Dr Terence Love, IT Coordinator of the Institution of Mechanical Engineers Australian Branch.

Confidential

Confidential *means:*

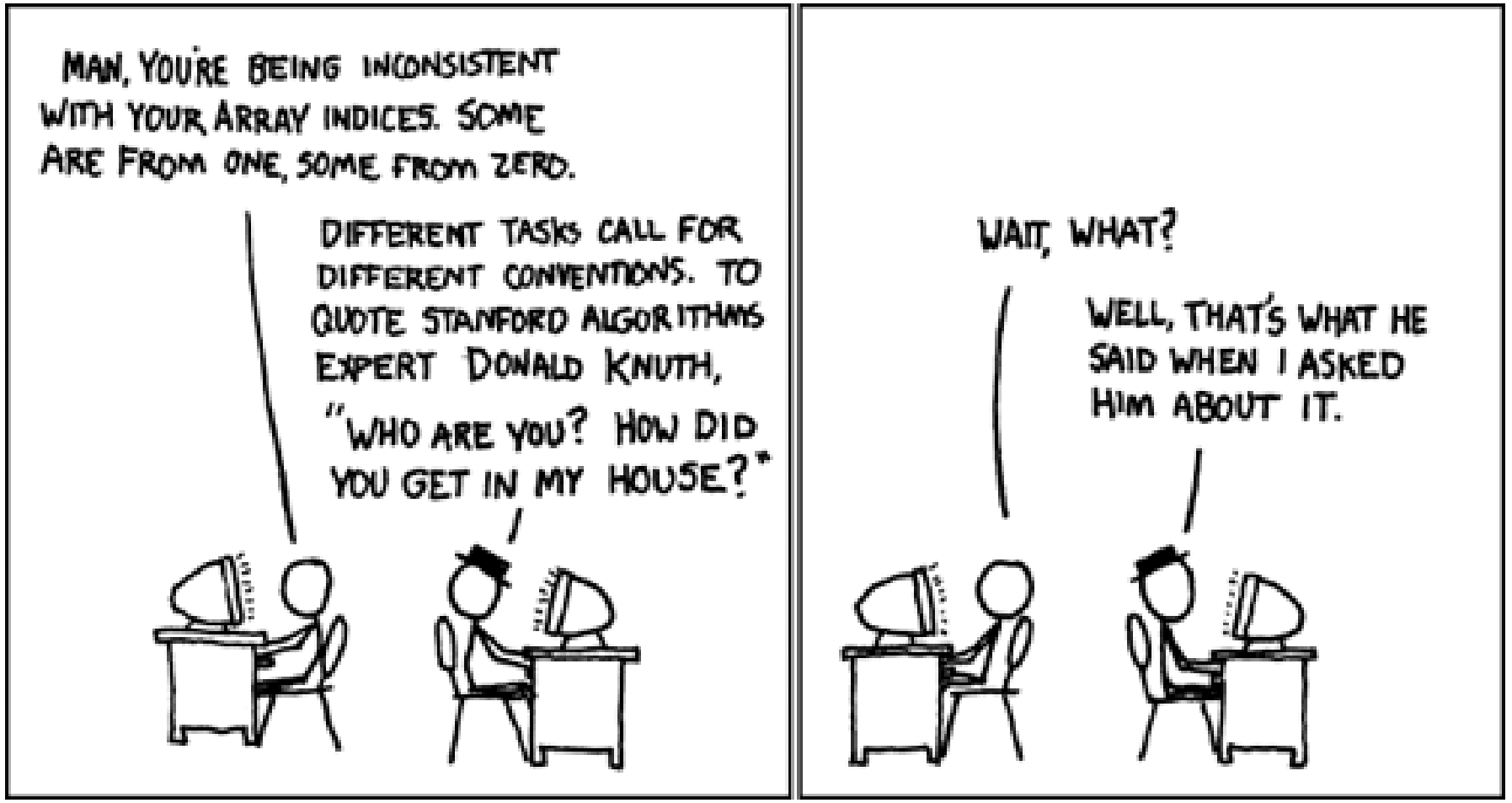
Intended to be kept secret

Entrusted with private or restricted information



Confidentiality *is an arrangement to prevent sensitive information from reaching the wrong people while ensuring the right people can access it.*

Confidentiality



Xkdc –donal-knuth

Confidential Content

Content is the **knowledge and information** you see or hear in:

Word documents
Emails
Websites
Excel files
Databases
Audio & video recordings
Books
Messages
Phone calls
….

Content is the ***content***

Metadata

Metadata is **information about data** and is often attached to that data.

- ***Document metadata*** includes author, time and date, who edited it, etc.
- ***Image metadata*** includes owner, how it was created, exposure info, where it was created, keywords etc.
- ***Video metadata*** can include information about creator, where created, what is in the video at different points
- ***Communication metadata*** records who sent which information to who, what you did when, where and with who.

Attacks on confidential content & metadata

Attacks on your *confidential content* and *meta-data* typically have different purposes:

Confidential content attacks – *someone wants to know what someone else knows*

Confidential metadata attacks – *someone wants to put pressure on someone else*

Confidentiality of communication

Confidentiality of engineers communication is at risk when:

- **Information is sat on servers** – hacking of computers
- **Information is moving** – hacking of networks, wireless, cables
- **Password are recorded** – passwords enable access to other information and systems
- **Engineers and their behaviours are *indirectly* identified** – meta-data collection
- **Engineers and their activities are *directly* recorded** – surveillance
- **Communication and data modification -** records are intercepted and changed

Scenario 1: Terrorism risks

SCADA systems ***remotely*** monitor & control essential services - electricity, gas, water, waste treatment and transport systems.

Mary is an engineering manager whose computer has software to make SCADA changes.

SCADA changes can result in loss of life, loss of services to a city, and high-levels of environmental contamination.

Mary also needs access to confidential information, technical documentation, online discussions with colleagues, password access to secure systems and software updates.

What are the terrorism risks associated with Mary's position?

Scenario 2: National economic risks

A small 3rd world nation has significant amounts of oil within its territorial boundaries. A powerful nearby 1st world country believes it is justified to claim the oil and attempts to redraw its territorial boundaries so all the oil is on its side.

During negotiations, discussions about the oil, technology and territory are compromised by bugging the smaller nation's cabinet room by the larger nation.

The result is3$Bn/ year loss from the smaller 3rd world nation to the larger 1st world nation. The issue is now with the ICJ in the Hague.

What are the national economic risks due to lack of confidentiality?

Scenario 3: Password shoulder surfing

Peter is a senior engineering designer for a large corporation collaborating with engineers overseas.

His hotel room is often his workspace and he uses the chair, table and light provided.

Peter is unaware of tiny video camera in the ceiling above his keyboard recording all his key presses, especially passwords.

He is also unaware all sounds are recorded, phone is intercepted, internet communications are recorded. When he leaves his computer in the safe, it is accessed and the data copied.

What are the risks associated with Peter's position?

Scenario 4: Engineer whistle-blowers

Many whistle-blowers are engineers, and historically one of the reasons engineering societies formed was to protect such members.

Engineers shall '*act appropriately, and in a professional manner, when you perceive something to be wrong'* (Engineers Australia); and '*shall conduct their professional work … with due regard for the welfare of the people*' (IMechE).

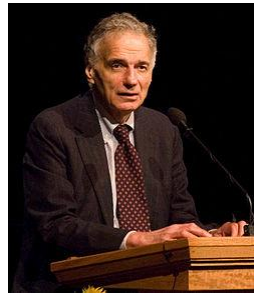
2 main confidential communication issues:

How to protect a whistle-blower, and keep them anonymous?

How to protect others from release of confidential information when the whistle is blown?

How can confidential communications be done achieved for engineer whistle-blowing?

A **whistleblower** is a person who exposes misconduct, alleged dishonest or illegal activity in an organization.



US vehicle safety campaigner **Ralph Nader** coined the phrase in the early 1970s

Scenario 5: Engineers in volatile places

James, an expat mechanical engineer working in a volatile country risks kidnapping, violence, disease, accidents, blackmail, corruption, terrorism, computer & information theft.

Confidentiality risks include:

- Details of James' location and timetable
- Confidential technical data
- Compromised communication with base
- Operational weaknesses (including illness)Censorship and local law-related risks

What other kinds of risks from poor confidentiality of communication does James have?

Reminder: Confidentiality targets for attacks

Data or content at rest *– on servers , computers, hard drives, cloud, phones, repositories*

Data or content in motion – *in networks, wireless, the Internet, phonelines*

Messages at rest *– on servers , computers, hard drives, cloud, phones*

Messages in motion – *in networks, wireless, the Internet, phonelines*

Metadata about content or communications at rest or in motion

Creating a Threat Model

Use the following questions for all ‘at risk’ information and communications to create a **Threat Model**:

- *What do you want to protect? (can be people, information, company, physical things…)*
- *Who is trying to do something I don’t want? Why?*
- *What can they do?*
- *What happens if they succeed?*

Then **create a security plan** by asking:

*What **security processes** will protect against the above?*

5 Tools for Secure Engineering Communications

Purpose: use tools to secure engineering communications to protect engineers, businesses, the public.

Five tool areas are:

1. ***Protect data*** (moving and at rest)
2. ***Protect messages*** (moving and at rest)
3. ***Protect personal metadata***
4. ***Protect passwords***
5. ***Preserve anonymity where necessary for engineers' safety***

Note: In most cases, it is identity that needs to be confirmed rather than

Virtual Private Networks (VPN)

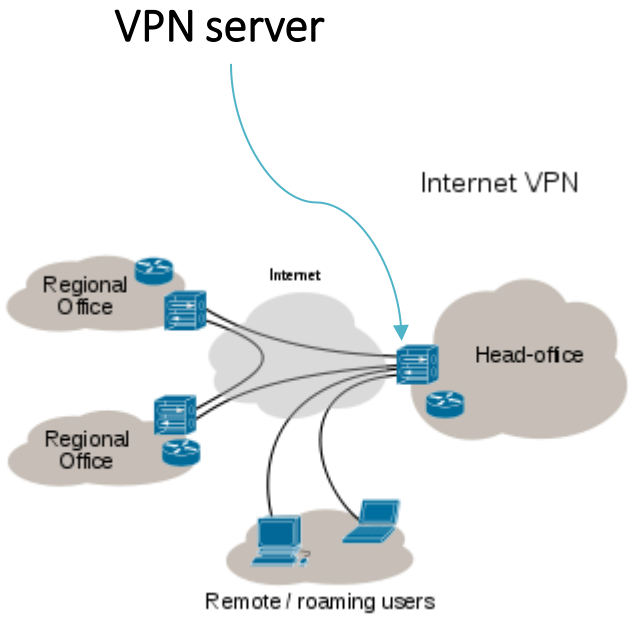
Private networks are those that exist within a trusted company and are secured and inaccessible to outsiders.

Virtual Private Networks (VPN) are outside networks that behave as if they were securely inside.

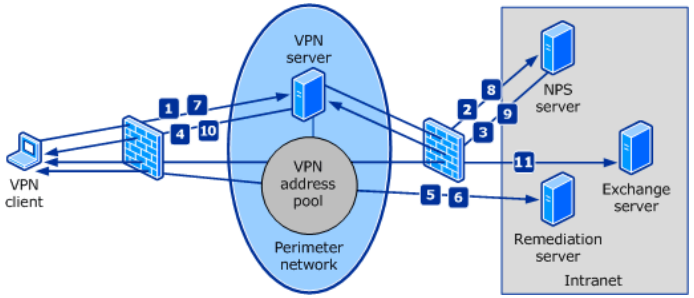
All external communications go via the internal **VPN server**

VPN's external communications are encrypted, including requests for webpages, which go through the VPN server

Using a **VPN** provides some security on public open wifi (see the *wifi pineapple* problem, later)



VPNs and engineers' travel



VPNs offer good information security whilst travelling

- All communications are encrypted to your VPN server
- Good protection for using insecure wifi while travelling
- Data can be on server in office rather than on laptop/tablet/phone
- Assume ALL public wifi is attacked and recorded

Where possible use a company VPN when travelling.

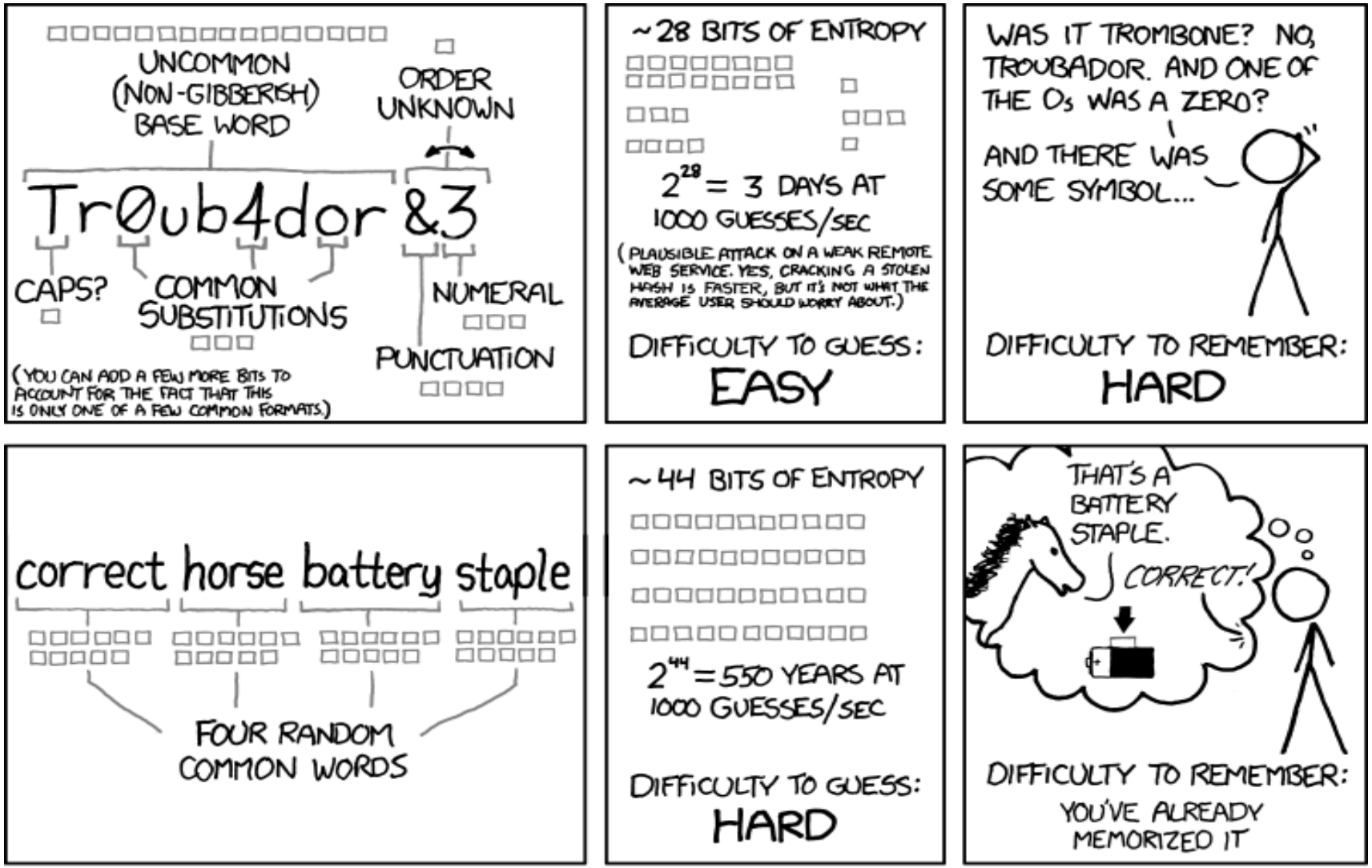
If not, and it is necessary to use public wifi then buy traffic at a VPN – eg *Private Tunnel* (www.privatetunnel.com/home/) at 500Gb/$50

Attacks on VPN communications

Three attacks on confidentiality of VPNs are:

- **Poor password management** (use password manager)
- **Shoulder surfing /video surveillance** (use a towel or hood if necessary to securely enter passwords)
- **WiFi Pineapples** are a man-in-the-middle attack (disable 'connect to remembered access points' on your computer, or, better, use a 3G modem rather than wifi)

Passwords



https://xkcd.com/936/

Password Managers

Good passwords are:

- A random long mix of lower/upper case, numbers and symbols (@ # $ % ^ etc)
- Used for only one login
- Changed often

Most engineers are likely to have dozens or ***hundreds*** of passwords.

Passwords are difficult to remember, and easy for computers to guess.

The only satisfactory solution at this point seems to be:

Use a secure password manager

Password managers

Password managers store passwords securely

You need remember one very secure password and copy the others as needed from the password manager.

You can layer security protection and keep the password data off your computers or the cloud.

Secure your password manager on encrypted USB and remove when not in use. Use a hardware-encrypted USB, e.g. IronKey in preference to software-encryption or layer them

Backup your password database and put it somewhere secure!

Password Safe
KeepassX
KeyChain
LastPass
and many others

Private and Public Key encryption

Many kinds of security use private and public key encryption – emails, VPN, SSH, Instant messaging

Private and Public Keys are large random numbers =>>

Private key – You keep very safe

Public key – you give to everyone

Bob has: **Bob's** Private key and **Alice's** Public key

Alice has **Alice's** Private Key and **Bob's** Public Key

-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEA3Tz2mr7SZiAMfQyuvBjM9Oi..Z1BjP5CE/Wm/Rr500P
RK+Lh9x5eJPo5CAZ3/ANBE0sTK0ZsDGMak2m1g7..3VHqIxFTz0Ta1d+NAj
wnLe4nOb7/eEJbDPkk05ShhBrJGBKKxb8n104o/..PdzbFMIyNjJzBM2o5y
5A13wiLitEO7nco2WfyYkQzaxCw0AwzlkVHiIyC..71pSzkv6sv+4IDMbT/
XpCo8L6wTarzrywnQsh+etLD6FtTjYbbrvZ8RQM..Hg2qxraAV++HNBYmNW
s0duEdjUbJK+ZarypXI9TtnS4o1Ckj7POfljiQI..IBAFyidxtqRQyv5KrD
kbJ+q+rsJxQlaipn2M4lGuQJEflxELFDyd3XpxP..Un/82NZNXlPmRIopXs
2T91jiLZEUKQw+n73j26adTbteuEaPGSrTZxBLR..yssO0wWomUyILqVeti
6AkL0NJAuKcucHGqWVgUIa4g1haE0ilcm6dWUDo..fd+PpzdCJf1s4NdUWK
YV2GJcutGQb+jqT5DTUqAgST7N8M28rwjK6nVMI..BUpP0xpPnuYDyPOw6x
4hBt8DZQYyduzIXBXRBKNiNdv8fum68/5klHxp6..4HRkMUL958UVeljUsT
BFQlO9UCgYEA/VqzXVzlz8K36VSTMPEhB5zBATV..PRiXtYK1YpYV4/jSUj
vvT4hP8uoYNC+BlEMi98LtnxZlh0V4rqHDsScAq..VyeSLH0loKMZgpwFEm
bEIDnEOD0nKrfT/9K9sPYgvB43wsLEtUujaYw3W..Liy0WKmB8CgYEA34xn
1QlOOhHBn9Z8qYjoDYhvcj+a89tD9eMPhesfQFw..rsfGcXIonFmWdVygbe
6Doihc+GIYIq/QP4jgMksE1ADvczJSke92ZfE2i..fitBpQERNJO0BlabfP
ALs5NssKNmLkWS2U2BHCbv4DzDXwiQB37KPOL1c..kBHfF2/htIs20d1UVL
+PK+aXKwguI6bxLGZ3of0UH+mGsSl0mkp7kYZCm..OTQtfeRqP8rDSC7DgA
kHc5ajYqh04AzNFaxjRo+M3IGICUaOdKnXd0Fda..QwfoaX4QlRTgLqb7AN
ZTzM9WbmnYoXrx17kZlT3lsCgYEAm757XI3WJVj..WoLj1+v48WyoxZpcai
uv9bT4Cj+lXRS+gdKHK+SH7J3x2CRHVS+WH/SVC..DxuybvebDoT0TkKiCj
BWQaGzCaJqZa+POHK0klvS+9ln0/6k539p95tfX..X4TCzbVG6+gJiX0ysz
Yfehn5MCgYEAkMiKuWHCsVyCab3RUf6XA9gd3qY..fCTIGtS1tR5PgFIV+G
engiVoWc/hkj8SBHZz1n1xLN7KDf8ySU06MDggB..hJ+gXJKy+gf3mF5Kmj
DtkpjGHQzPF6vOe907y5NQLvVFGXUq/FIJZxB8k..fJdHEm2M4=
-----END RSA PRIVATE KEY-----

Public—Private Key secure email

Bob sends Alice an email encrypted with Alice's Public key

Alice decrypts it with her private key and reads it.

Alice sends Bob a reply encrypted with Bob's Public key

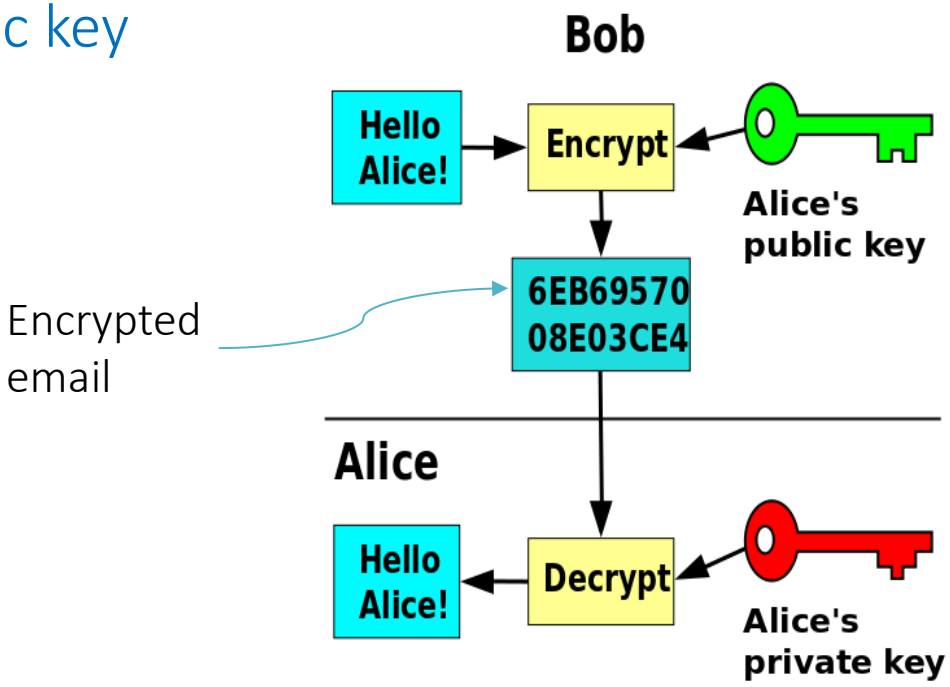
Bob decrypts it with his private key and reads it.

General rule:

Encrypt with PUBLIC KEY

Decrypt with PRIVATE Key

Can be managed automatically in email software



Institution of MECHANICAL ENGINEERS
Improving the world through engineering

Other public-private key encryption uses

- Instant messaging
- Https in web browsers
- SSH (basis of some VPNs)
- Digital signing of documents
- GPG support for email such as Outlook
- Secure file transfer

Public--private key software

GPG software is perhaps most common to manage public and private keys.

History: PGP of Phil Zimmerman was the standard public-private key encryption method. Commercially it is now available via Symantec. GPG was created as the open source free equivalent of PGP and is fully compliant with the OpenPGP standard.

GPG4Win – for Windows
GPGSuite – for Mac
Gnu Privacy Assistant - for Linux

https://www.gnupg.org/

See also Putty and PuttyGen

And for Mac and Linux use terminal and ssh-keygen

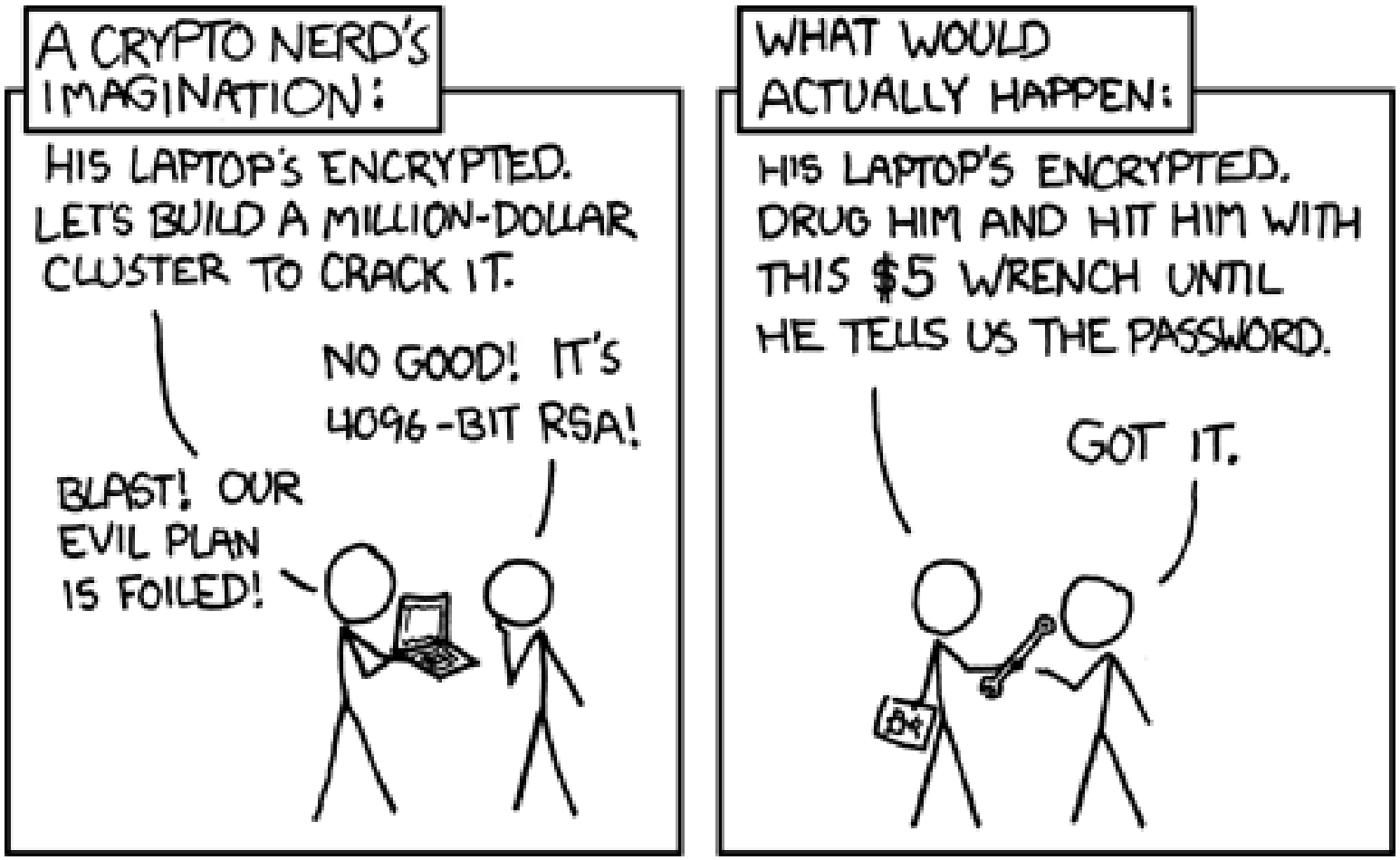
Drive encryption

Hard drives that are not fully encrypted can be removed and files accessed

Full-drive encryption *secures data and messages at rest* (examples include: Bitlocker (Win), Filevault (OSX), cryptsetup (Linux)

USBs and memory cards can be encrypted via *software* or *hardware*. *Hardware encrypted* USBs are more secure, more expensive and slower (Ironkey, Kingston, Sandisk, Kanguru)

TrueCrypt (use only 7.1a) can create hidden volumes for situations where personal security and data are both important.



For engineers working in personally highly dangerous situations, expert advice should be sought on information securing.

It may be better to have passwords held by a different person or secure information managed in a different manner.

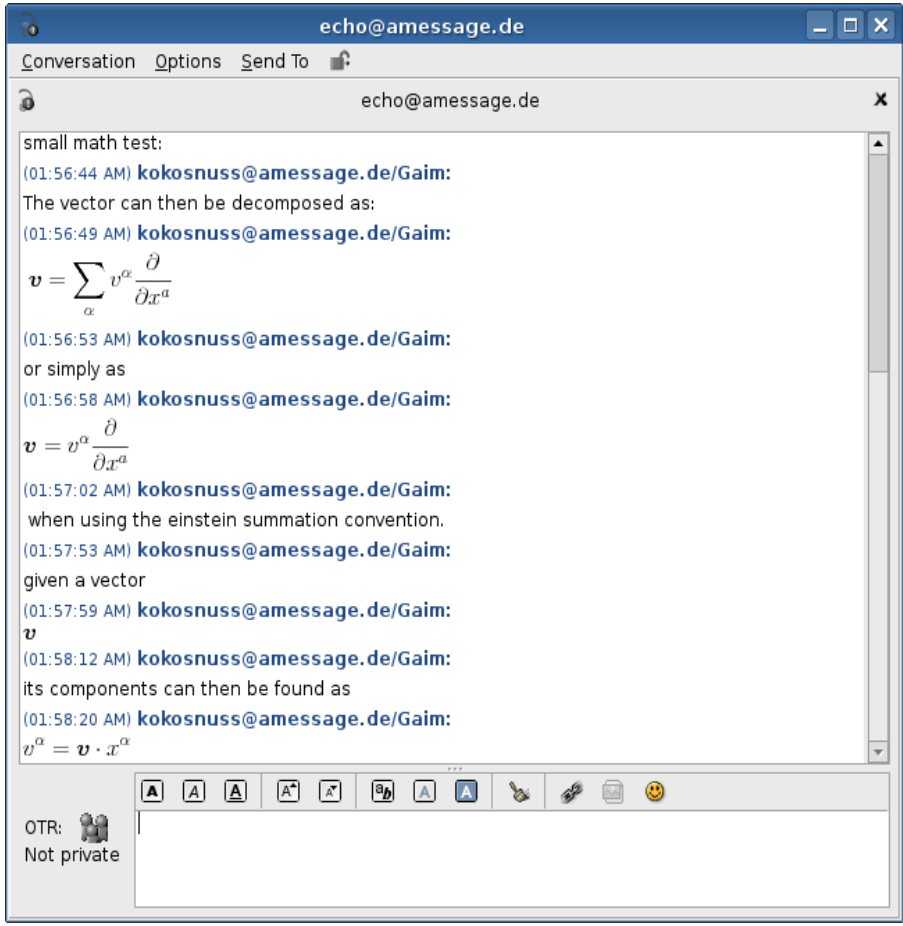
Secure instant messaging

Secure instant messaging is an effective communication tool.

- Provides 'stealth' online presence
- Messages are encrypted
- Does not log or store ANY information about messages or contents or sessions
- Does not rely on 3rd party servers

For Windows - **Pidgin** (https://pidgin.im/), **TorChat**
For Mac – **OfficeChat**, **OTR** and **Pidgin**
For Linux – **Pidgin**, **OTR**

Skype texts are also encrypted



File encryption software

File encryption, especially ‘on-the-fly’ encryption, can protect files and folders at rest and in motion.

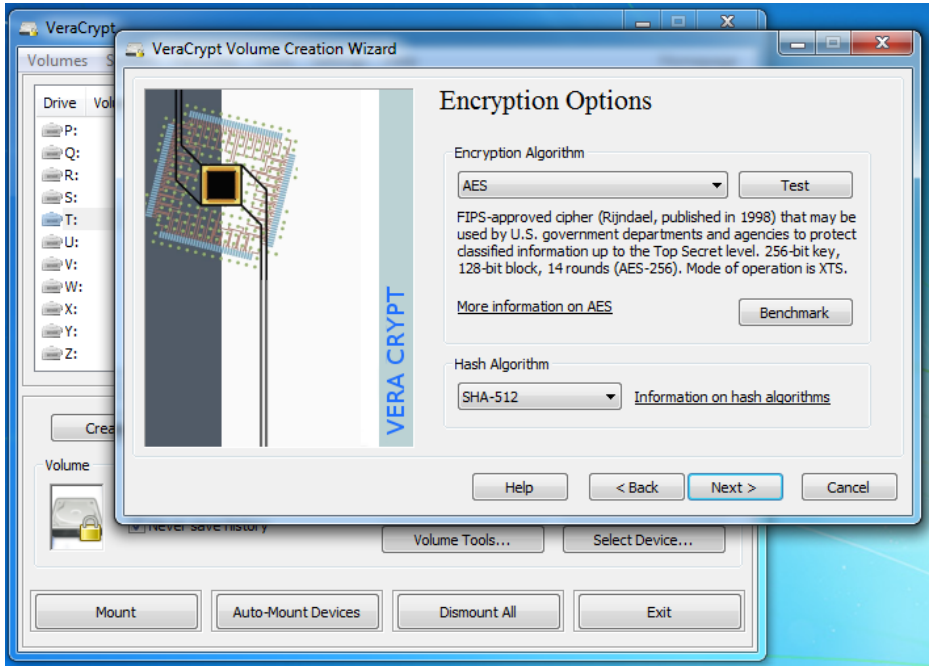
Examples include:

Windows: Bitlocker, Truecrypt 7.1a, Veracrypt, GnuPG, 7-Zip

Mac: FileVault, Disk Utility, AESCrypt, Veracrypt

Linux: GnuPG, gensfsm, openSSL, AESCrypt, Veracrypt

File encryption depend on strong passwords (usually necessary to use a password manager)



TAILS – amnesic incognito secure system

Tails is a live operating system that runs on most laptops from a DVD, USB, or SD card.

Tails contains state-of-the-art cryptographic tools to encrypt your files, emails and instant messaging and anonymise web browsing.

Tails aims preserve privacy and anonymity, add confidentiality protection, enable you to use the Internet anonymously, and in some regimes, to circumvent censorship.

All connections to the Internet go through the Tor network;

No trace left on computer being used.

Tails can provide additional security for engineers in field.

In most cases, however, VPN, secure email and file transfer, and good password management are preferred solutions

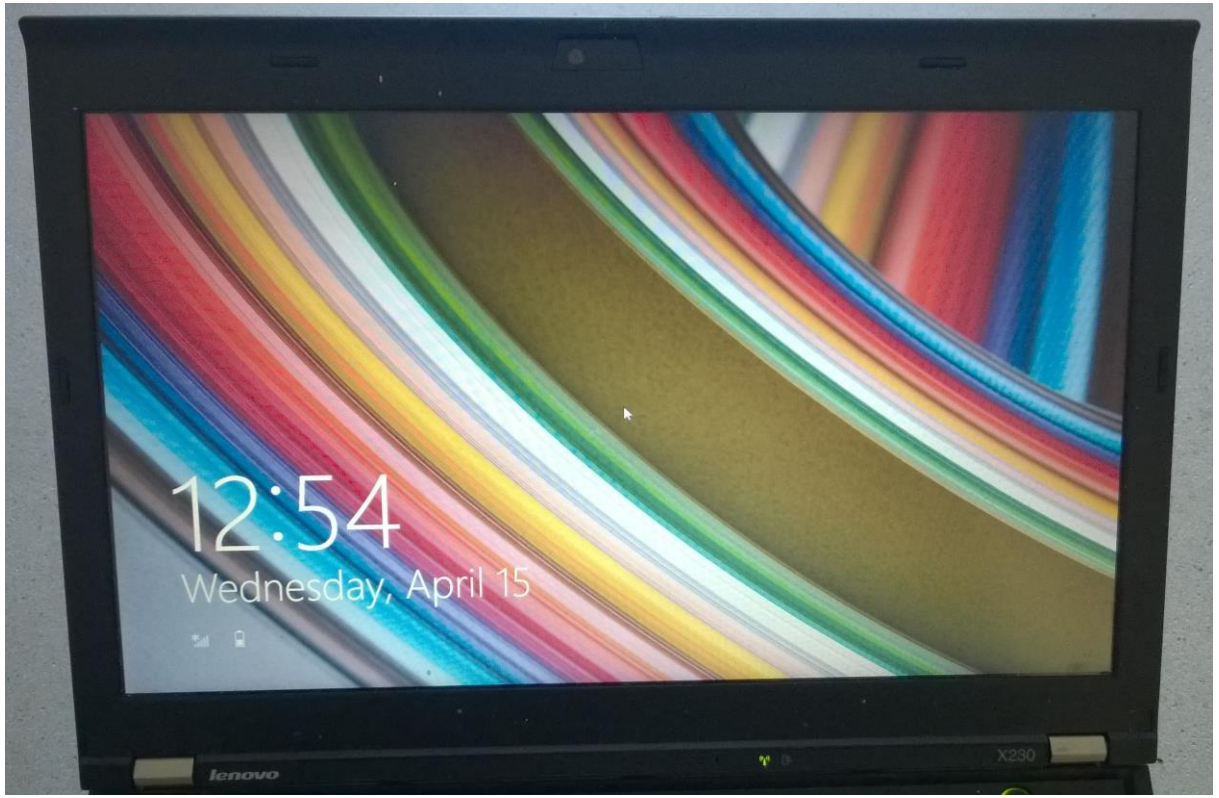
Using Tails

- Install Tails on a USB, CDROM or memory card (See, https://tails.boum.org/)
- Insert into a computer and boot from it
- Use Tails for work
- Shut down and computer memory is erased and no confidential file details are left

Some care is needed! (see, https://tails.boum.org/doc/about/warning/index.en.html)

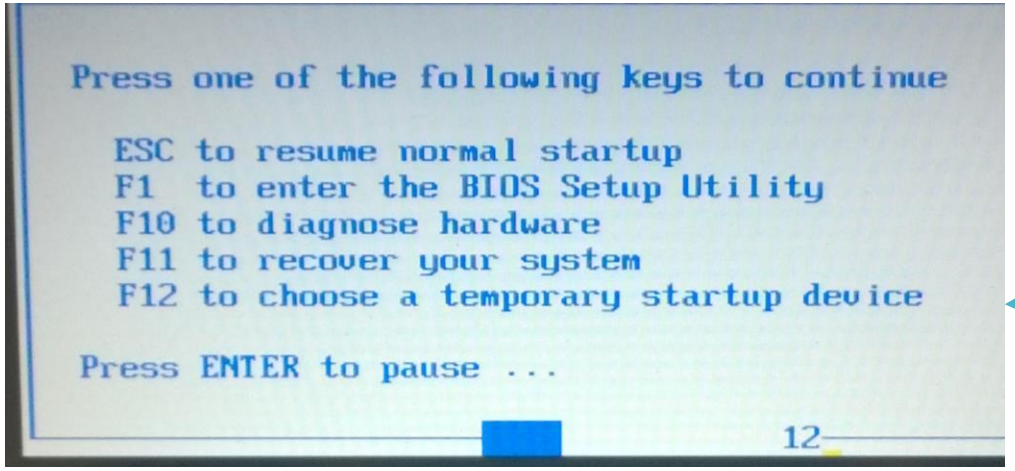
Institution of MECHANICAL ENGINEERS
Improving the world through engineering

Take a computer and shut down

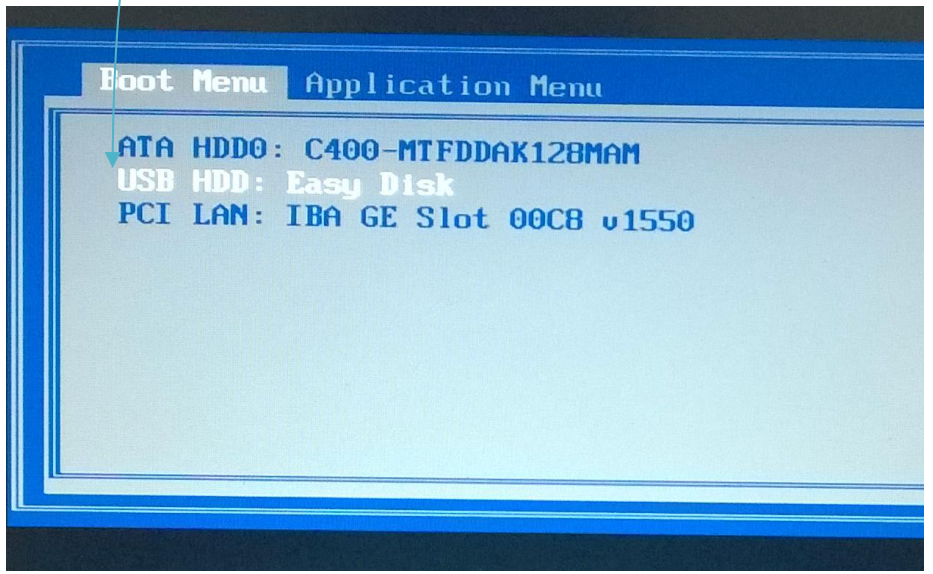


Standard Lenovo X230 with Win 8.1

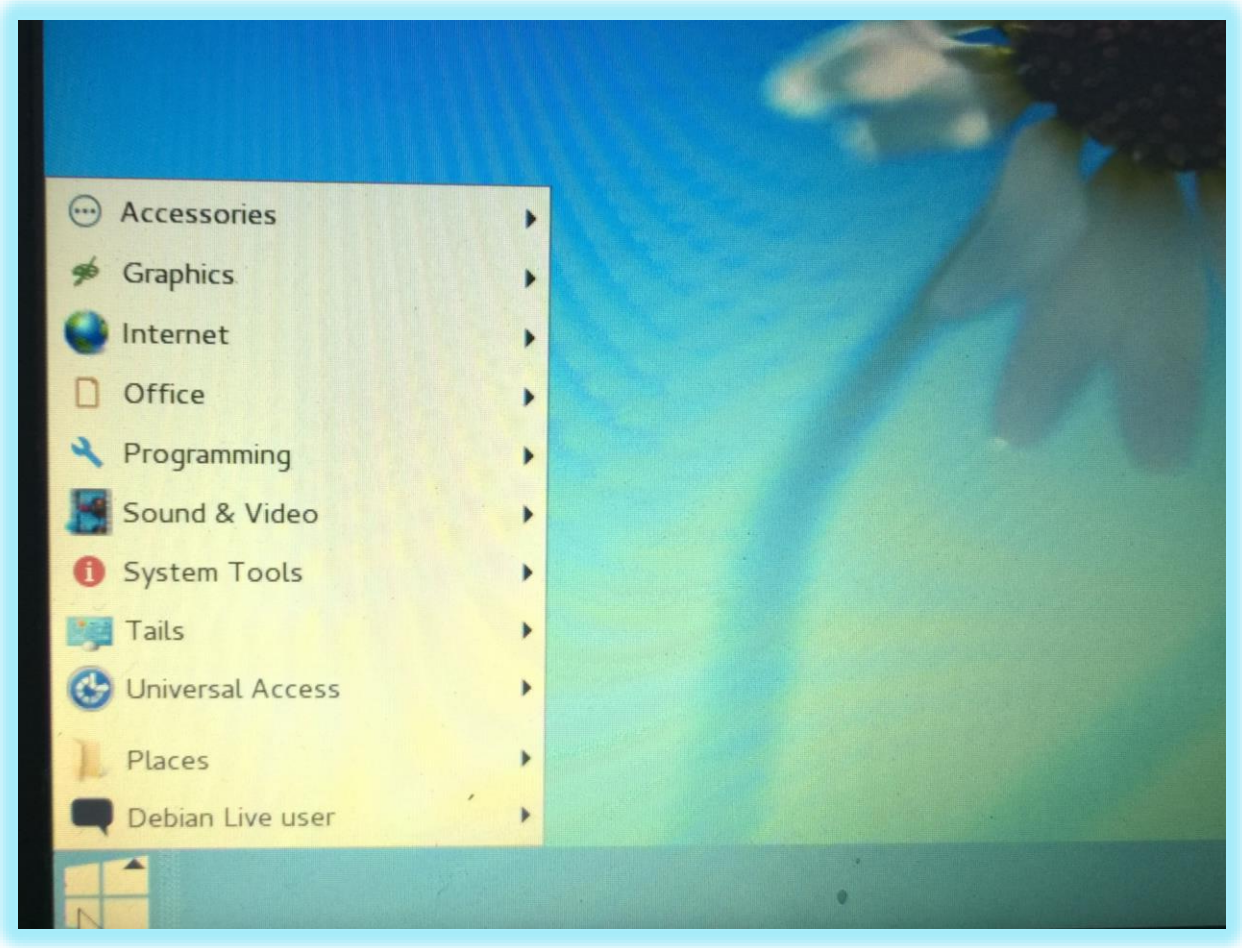
Insert Tails USB and boot from it



Choose boot device



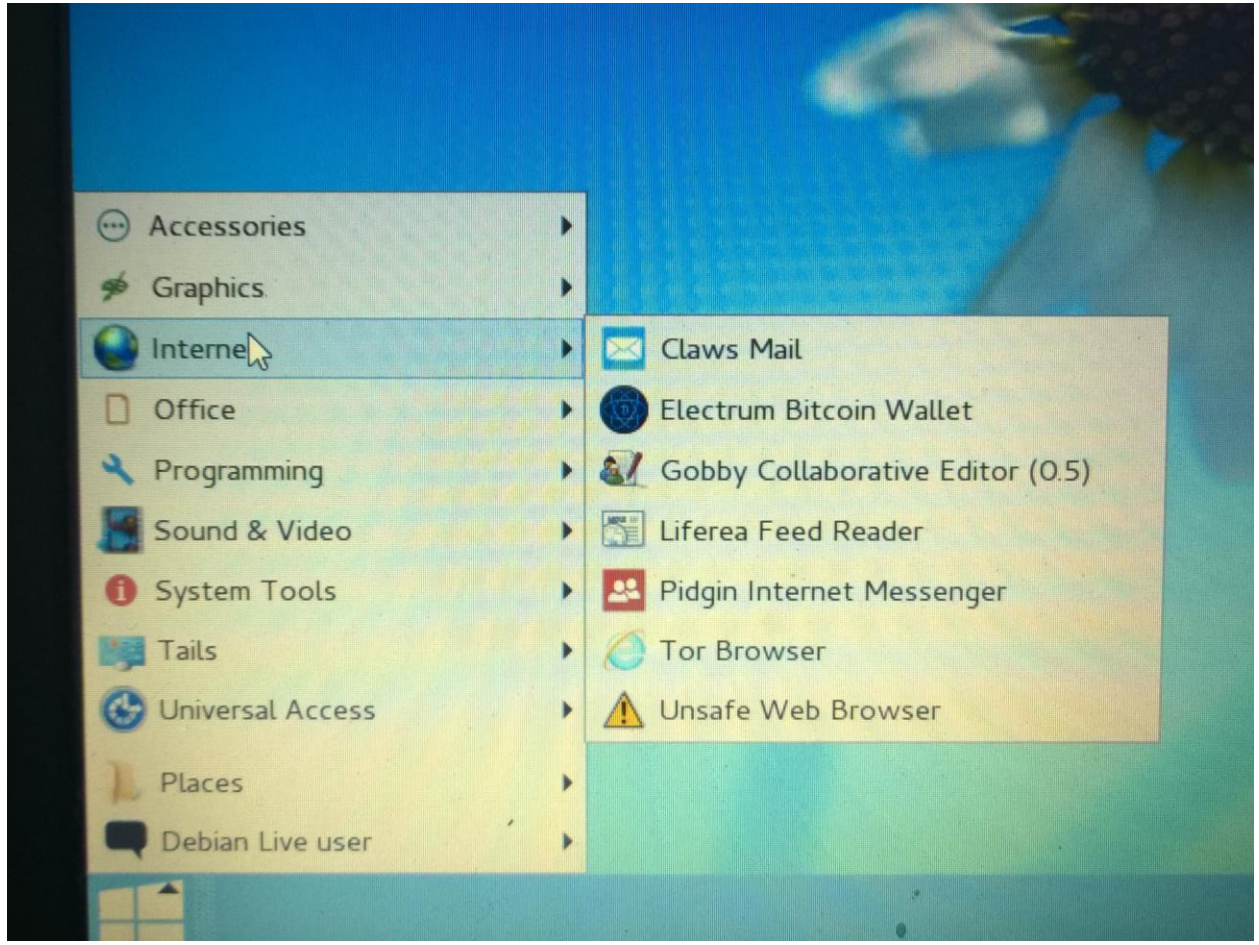
Tails on Lenovo



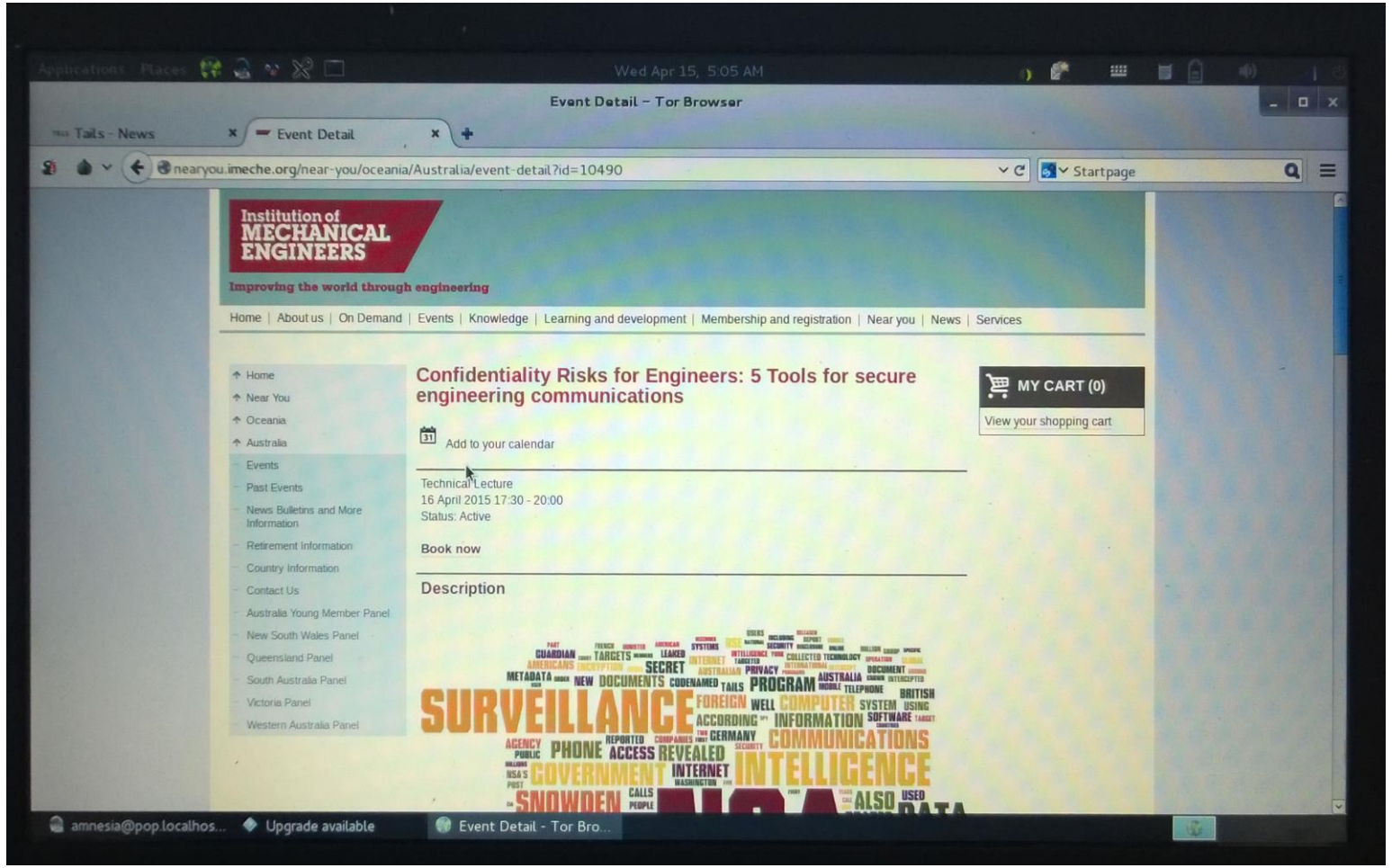
Shows general list of Tails software

Institution of MECHANICAL ENGINEERS
Improving the world through engineering

Tails secure internet software



Tails using Tor Browser



Viewing IMechE Near You website events via the Tor Browser

Web searches are via search engines that do not record your details:

StartPage

DuckDuckGo

Tails
theamnesicincognitolivesystem

Installing Tails on a new USB

Use new blank 4Gb USB

Easiest is to clone usb using a computer already running Tails

Otherwise:

- Download ISO file and create a Tails DVD
- Use DVD to run Tails
- Using computer running Tails, use Tails Installer to create new Tails USB

(https://tails.boum.org/doc/first_steps/installation/manual/index.en.html)

In conclusion

Step 1: Create a **Threat Model** for your situation

Step 2: Create a **security plan** that addresses the threats appropriately

Step 3: Install necessary software and use your security plan

In volatile situations, you may find it useful to carry Tails.

Institution of MECHANICAL ENGINEERS
Improving the world through engineering

Questions?

Dr. Terence Love
admin@loveservices.com.au

Online courses on security

Interested in short online courses on security, confidentiality and privacy?

Sign up for the free ***Courses news*** at www.praxiseducation.com