CS3235:1 - Computer Security
First topic - Introduction to IT security

Hugh Anderson

National University of Singapore
School of Computing

August, 2019

Isolation...

Outline

Outline

Outline

Your teaching staff

Lecturer	Hugh Anderson
Teaching assistants	Ang Ray Yan
	Mr Blobby
Guest speaker	Prof Neko Kanochi

Information and contact details

Please call me Hugh, and visit me in my room if you have any questions. I have an open door policy, and my room is COM2 #03-24, Telephone 6516-4262, Email hugh@comp.nus.edu.sg.

Mr Blobby likes to be called Mr Blobby, and will be here to assist in pointing out things on slides.

Prof Kanochi, and Mr Blobby can be contacted using my contact details. Ray Yan through e0003682@u.nus.edu.

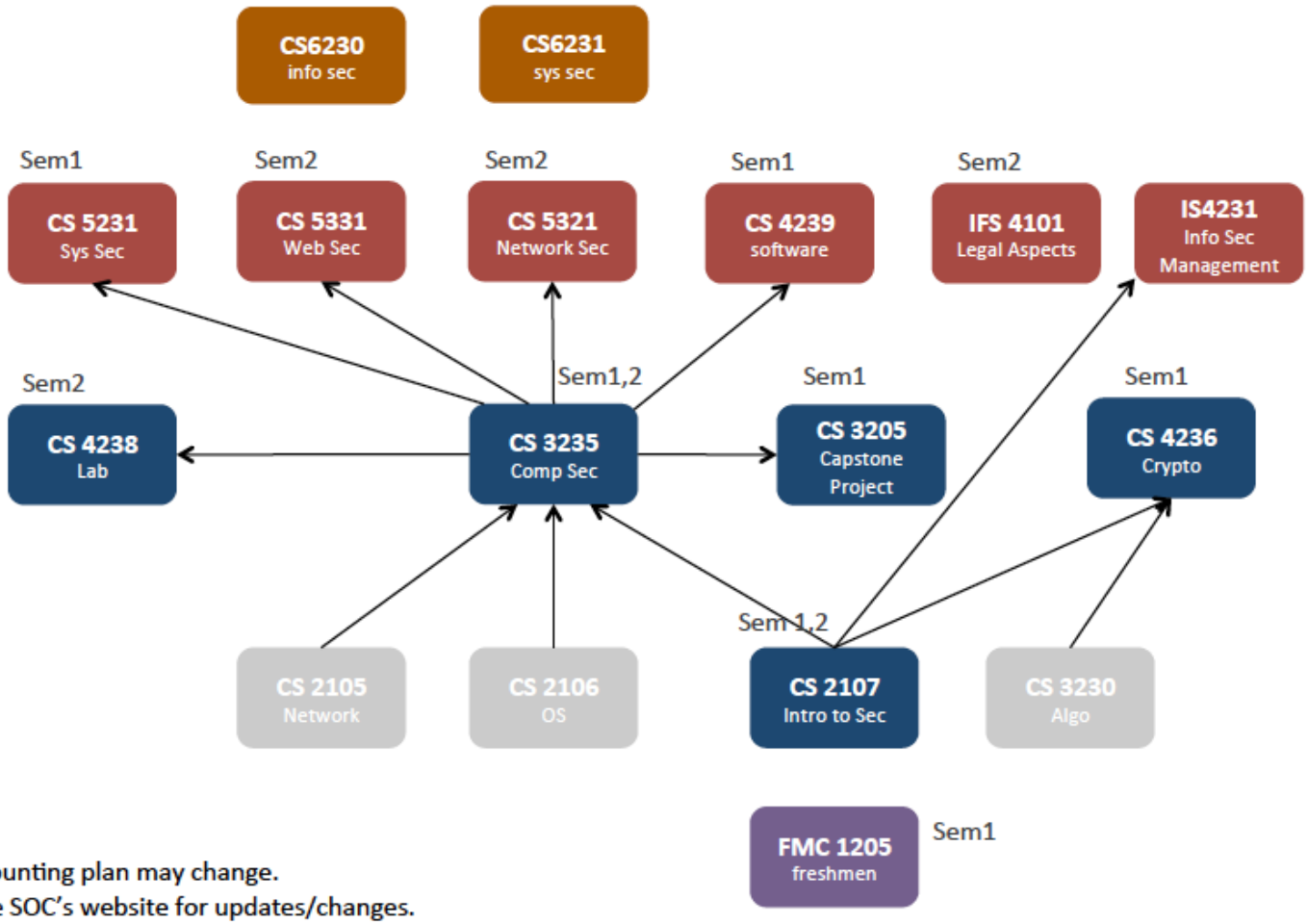
Official SOC description

From the official course description...

The objective of this module is to provide a broad understanding of computer security with some indepth discussions on selected topics in system and network security.
This module covers the following topics: intrusion detection, DNS security, electronic mail security, authentication, access control, buffer overflow, memory and stack protection, selected topics in application security, for instance, web security, and well-known attacks.

Where CS3235 lies...

In the middle :)...



Note:
1. Mounting plan may change.
2 See SOC's website for updates/changes.

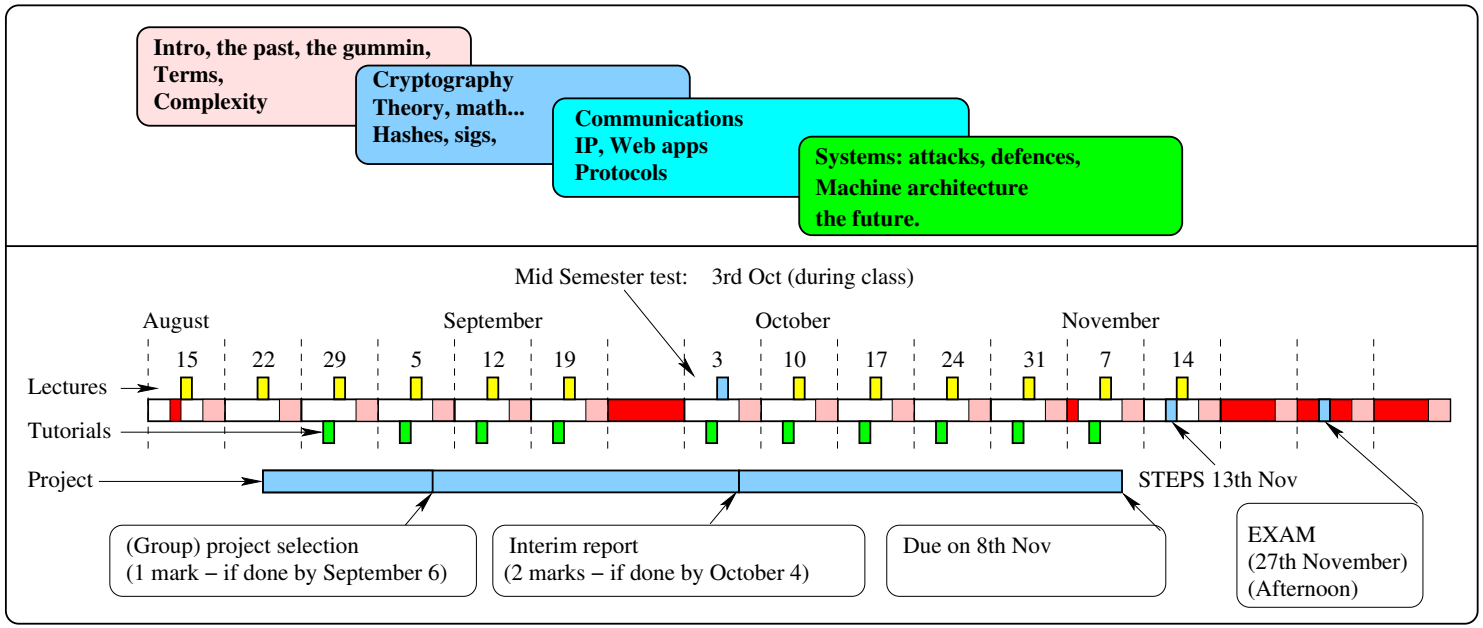
Assessment

Assessment		Grade
Tests	Closed book	10%
Lab/Homework		15%
Group project		35%
Final Exam	Open Book	40%
Total marks		**100%**

The group projects this year will be presented at the STEPS showcase (On the 13th Nov). This year your project must contain a significant development of your own (this most likely would be software) - projects made by collating google sourced information will not be acceptable.

Timetable

Lectures, tutorials and project...



The tutorials will be a mix of labs, demos, and assessed tutorials. The project will be a group one (5 members in each group, chosen by me).

Tut/labs and ITSEC/OS laboratory

Tutorial/laboratories start the third week...

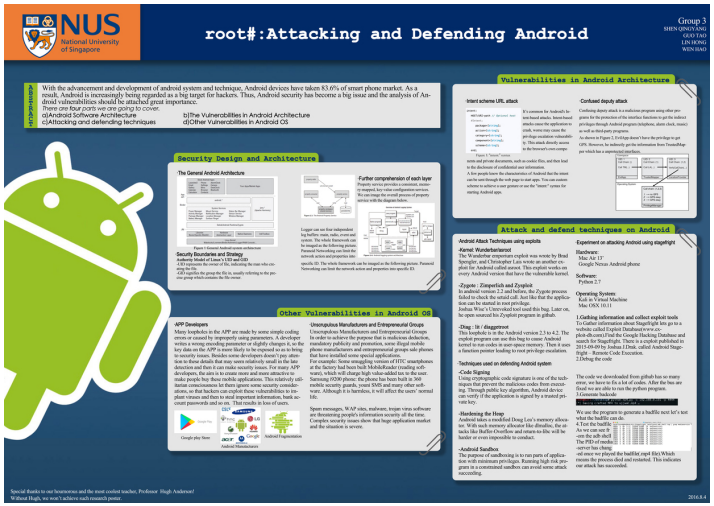
The first lab can be done whenever you have time, and is just for familiarizing yourself with the ITSEC/OS lab. Later, your tutor will be me, and if there is homework, give your written/printed answers to the homework as you enter the tutorial room for assessment.

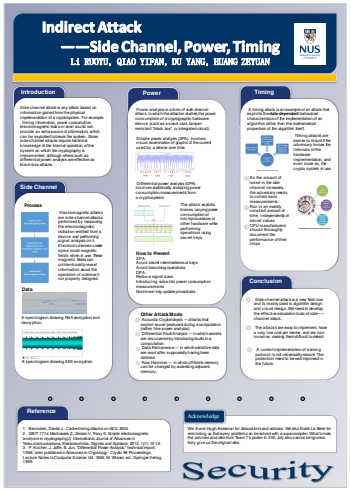
ITSEC/OS laboratory at COM1-B-13 (open 24hrs)

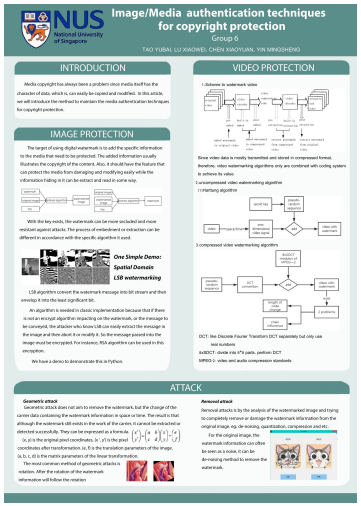
The lab has a separate Internet connection, so the NUS restrictions (about use of, say, scanners) are lifted, however, note the following three points...

1. Breaking into computers is fun, but breaking into someone else's computer is illegal.
2. However, using these techniques on your own systems helps you build more secure systems.
3. Use your powers for good, not evil.

Project







Project is soon to be under way...

The project will be published soon. The groups will be selected for you. As a result, your group members may be from different tutorial groups.
Elect a leader. We have the following important dates for the project:

- September 6 - Group/leader selection (1 mark)
- October 4 - Progress (2 marks)
- November 8th - Final submission

20% of mark is for extra - above and beyond work.

Resources

Resources

There is no textbook, but you may find the “Computer security” textbooks by Anderson, Gollman, Liska, Pfleeger, Bishop useful. I will put a PDF of Anderson/Security Engineering in the Luminus (Same book as has been used in cs2107 - it also covers a fair amount of CS3235 as well). From time to time I may give you directed readings - all available on the Internet.

- Luminus at https://luminus.nus.edu.sg/
- Join the NUS Greyhats, NUS Hackers, and attend a few sessions. Take part in the NUS bug bounty programme, hackthissite.org, get immersed in this world. If someone is giving a security talk, go and attend it...
- CS2107 at https://www.comp.nus.edu.sg/~hugh/presentations/cs2107/index.html

What you should already know...

You should already be familiar with all of CS2107.

FAQ

A random set of answers to faqs...

1. Marked to a bell curve? Not so much. Last time I taught it, 28% got As, before that 36%, before that 32%.
2. The CS2107 URL is in the previous slide.
3. Extra material, media and links will be put at https://www.comp.nus.edu.sg/~hugh/presentations/cs3235/index.html
4. Late? If you have to, but there will be penalties.
5. Mid-semester is in here, during lecture time, after the mid-sem break.
6. Yes STePs. Money can be made.
7. Yes - plagiarism detecters are used. Please do not.
8. No webcast.
9. No, No, No, Yes, and “only if they are in order”.

What you should learn...

What you are expected to know...

1. To be able to put security systems in context.
   For example: history, understanding of the “big picture”.
2. To describe “security related” things using technical terms.
   For example: keysize, PK, man-in-the-middle.
3. To understand the roles of the components of security systems, understanding the underlying reasons for their properties.
   For example: certifying authorities, SSL, VPN.
4. To characterize the effectiveness of different security systems, understanding the underlying reasons for their properties.
   For example: wireless vs wired, WEP versus WPA, symmetric vs asymmetric.
5. To aquire some practical skills that would help in securing (networked) computer systems.
   For example: firewall rules, IDS setup.

Why should you learn...

...and why should you care?

1. Reason #1: Pick up these skills and pass the final exam :)
2. Reason #2: It is fun in a kind of geeky way.
3. Reason #3: Knowing the issues, and underlying mechanisms, helps you configure systems to be safer; build better systems in future; explain to the person on the helpdesk why their system is flawed, and what needs to be done to fix it; avoid being the victim of (computer) fraud; realistically assess threats to you, your organization, your country, and of course become a better person - rich, good-looking, the recipient of unexpected gifts, and somewhat paranoid.

Please, please, please....

Attend classes and lab/tutorials. Ask if you don't know. Read references and handouts. Get interested in the subject
Dont do anything you know is plain wrong...

Outline

Aspects of IT security

A wide range of distinct subject areas...

- **Secrecy.** Encryption of documents...
- **Insecurity.** Not just secrecy, sometimes things like non-repudiation.
- **Safety/control software and hardware.** Complex software systems should be examined.
- **Assurance.** Confirm, specify and verify the behaviour of systems.
- **Networks and protocols.** The way in which we do things.
- **Mathematical, physical and legal.** Actual bounds/constraints.
- **Security models.** Formal (read *mathematical*) ways of looking at things.

The History of Herodotus

Now ... the marks on the head ...

For Histiæus, when he was anxious to give Aristagoras orders to revolt, could find but one safe way, as the roads were guarded, of making his wishes known; which was by taking the trustiest of his slaves, shaving all the hair from off his head, and then pricking letters upon the skin, and waiting till the hair grew again.
Thus he did; and as soon as ever the hair was grown, he despatched the man to Miletus, giving him no other message than this- "When thou art come to Miletus, bid Aristagoras shave thy head, and look thereon."
Now the marks on the head, ..., were a command to revolt...

The History of Herodotus

Histiæus

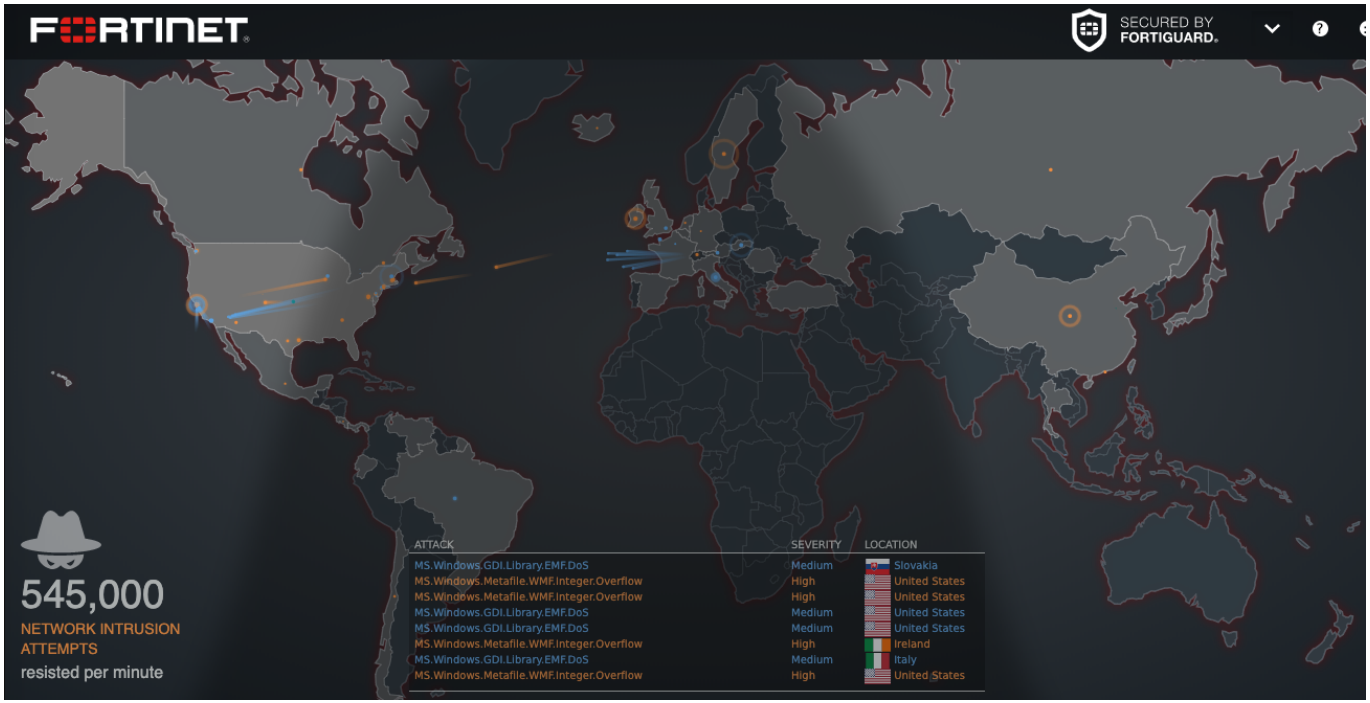
This technique was used by Histiæus to ensure *confidentiality.* It was used again by Germany in the 1914-1918 European war. This is now called steganography (hiding information amongst other stuff).

More history...

Warfare, warfare, warfare

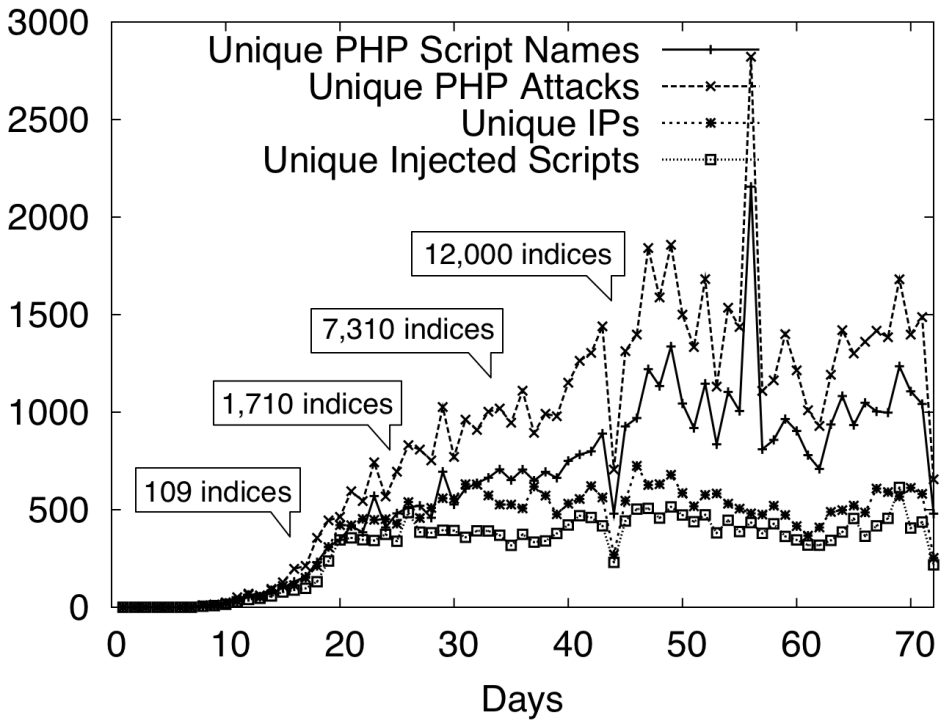
In the field of computer security, it is often common to see examples taken from the world of warfare.
We will see how Cæsar encoded messages - an early example of cryptography.
We might also examine computer protocols. In the real world, some of the earliest protocols were to ensure the correct conduct of a war (back when wars had conduct).
Do not be worried by this obsession with wars.

Information warfare



24 hours a day, 365 days a year, the attacks go on...

Attacks per day



After about 10 days, the site got discovered, and the attacks started, growing quickly until stabilizing at about 1000 attackers per day.

$100 million dollar heist

Big news in 2016...

2016 Bangladesh Bank heist

From Wikipedia, the free encyclopedia

> It has been suggested that *Tanvir Hassan Zoha* be merged into this article. (Discuss) *Proposed since June 2016.*

In February 2016, instructions to steal US$951 Million from Bangladesh Bank, the central bank of Bangladesh, were issued via the SWIFT network. Five transactions issued by hackers, worth $101 million and withdrawn from a Bangladesh Bank account at the Federal Reserve Bank of New York, succeeded, with $20M traced to Sri Lanka (since recovered) and $81M to the Philippines. The Federal Reserve Bank of NY blocked the remaining 30 transactions, amounting to $850 million, at the request of Bangladesh Bank.[1]

The Federal Reserve Bank of New York

Contents [hide]

Java Insecurity?

Big news at the time...

TECH | 1/11/2013 @ 10:33PM | 87,327 views

US Department of Homeland Security Calls On Computer Users To Disable Java

8 comments, 2 called-out + Comment Now + Follow Comments

Concerns about the susceptibility of the Java programming language to cyberattacks culminated Thursday night, with a warning posted on the Department of Homeland Security's Computer Emergency Readiness Team (US-Cert) calling on the public to temporarily disable Java on their personal computers.

Photo credit: devdsp

The call came in response to the discovery of a new vulernability that lets an attacker execute code on a PC running Java. The vulnerability is reportedly already being used in "exploit kits" which are pre-packaged, for-sale tool kits that can be used to commit online crimes such as stealing someone's identity.

Java Insecurity?

But this is nothing new...

Security Alerts

Oracle will issue Security Alerts for vulnerability fixes deemed too critical to wait for distribution in the next Critical Patch Update. The Security Alerts released since 2005 are listed in the following table. Click here for Security Alerts released before 2006. Security Advisory Notifications prior to July 2008 for BEA products are located here. Security Sun Alert notifications prior to April 2010 for Sun products are located here.

Security Alert Number And Description	Latest Version/Date
Alert for CVE-2015-3456 QEMU "Venom"	Rev 1, 15 May 2015
Alert for CVE-2014-7169 Bash "Shellshock"	Rev 5, 30 September 2014
Alert for CVE-2014-0160 OpenSSL "Heartbleed"	Rev 1, 18 April 2014
Alert for CVE-2013-1493	Rev 1, 04 March 2013
Alert for CVE-2013-0422	Rev 1, 13 January 2013
Alert for CVE-2012-4681	Rev 1, 30 August 2012
Alert for CVE-2012-3132	Rev 1, 10 August 2012
Alert for CVE-2012-1675	Rev 3, 20 June 2014
Alert for CVE-2011-5035	Rev 2, 29 March 2012
Alert for CVE-2011-3192	Rev 1, 15 September 2011
Alert for CVE-2010-4476	Rev 1, 08 February 2011
Alert for CVE-2010-0886	Rev 2, 18 May 2010
Alert for CVE-2010-0073	Rev 1, 04 February 2010
Alert for CVE-2008-3257	Rev 3, 05 March 2009

DBS/POSB attacks in 2012

Big news at the time...

A SINGAPORE PRESS HOLDINGS PORTAL

asiaone NEWS

HOME | NEWS | BUSINESS | FORUM | YOURHEALTH | MOTORING | EDVANTAGE | PLUSH | WOMEN

S'PORE | M'SIA | CASE FILES | SPORTS | REGIONAL | CONTEST | HELPDESK

ASIAONE » NEWS » SINGAPORE

DBS/POSB customers hit by unauthorised ATM withdrawals

Photo: AsiaOne, Stomp

Share: 495 46

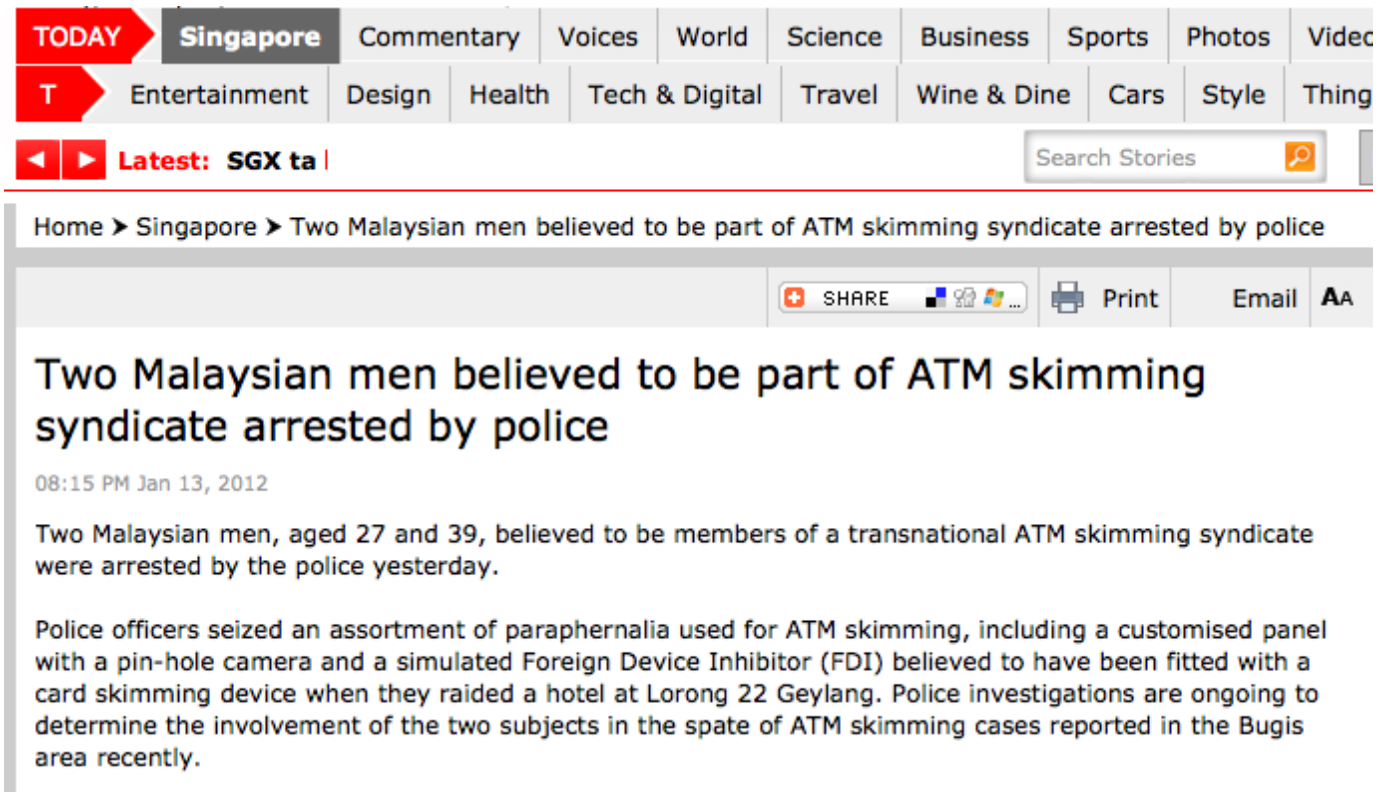
Share Tweet Share

AsiaOne
Thursday, Jan 05, 2012

SINGAPORE - DBS is investigating several hundred cases of unauthorised withdrawals from POSB/DBS accounts allegedly made from Malaysia in what could be a large scale bank fraud.

And a few days later...

Tracked down...



TODAY | Singapore | Commentary | Voices | World | Science | Business | Sports | Photos | Videc

T | Entertainment | Design | Health | Tech & Digital | Travel | Wine & Dine | Cars | Style | Thing

Latest: SGX ta

Search Stories

Home ➤ Singapore ➤ Two Malaysian men believed to be part of ATM skimming syndicate arrested by police

SHARE | Print | Email | AA

Two Malaysian men believed to be part of ATM skimming syndicate arrested by police

08:15 PM Jan 13, 2012

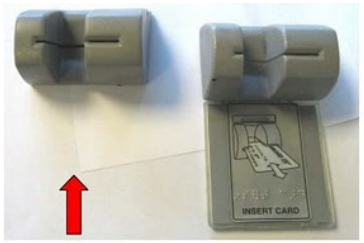
Two Malaysian men, aged 27 and 39, believed to be members of a transnational ATM skimming syndicate were arrested by the police yesterday.

Police officers seized an assortment of paraphernalia used for ATM skimming, including a customised panel with a pin-hole camera and a simulated Foreign Device Inhibitor (FDI) believed to have been fitted with a card skimming device when they raided a hotel at Lorong 22 Geylang. Police investigations are ongoing to determine the involvement of the two subjects in the spate of ATM skimming cases reported in the Bugis area recently.

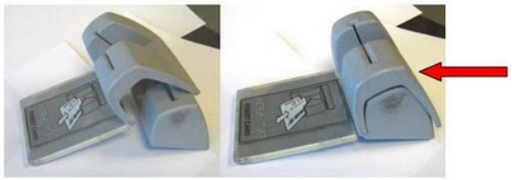
DBS/POSB attacks

How was it done?

It was done through the use of card skimmers on two machines in Bugis. Card skimming involves trying to collect your card details from the magnetic strip:



The real card reader slot. The capture device



The side cut out is not visible when on the ATM.

DBS/POSB attacks

Card skimmers

The Magnetic strip is read as it passes through the capture “shell”.
The electronics includes a magnetic strip reader head, a small amount of electronics, a battery, a microcomputer and storage (an SD card).

DBS/POSB attacks

Getting the PIN?

Common methods are to either use a small (pinhole) camera looking down on the keypad, with an SD card memory, or an overlay over the keyboard, with a small microcomputer and memory.

DBS/POSB attacks

Sometimes getting the PIN is REALLY easy!

Installing a skimmer...

Here is another skimmer...

A quick quiz...

Which of these two vehicles has a door lock?

Value SING$ 20,000

Value SING$ 350,000,000

Answer?

Outline

Hard to find the boundaries of “Security”

It is not "one thing"...

Security is complex:

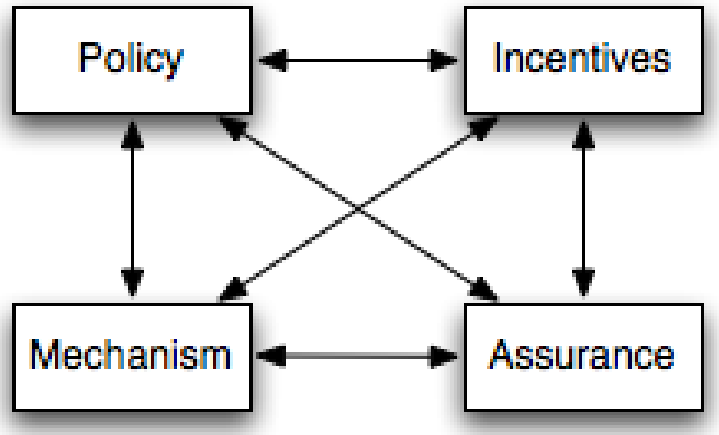
> Security can involve elements such as computers, people, locks, communication links and so on.
> The goals of security might involve authentication, integrity, accountability, and so on.
> A security system may involve an arbitrary combination of these elements and goals.

Security is everyone’s poor relation...

> It is not perceived as a benefit until something goes wrong, and requires regular monitoring.
> Too often, security is an after-thought, and regarded as an impediment to using the system.

Framework to hang our understanding on...

Ross Anderson's book suggests this framework:



Differentiate between security policies and mechanisms

policy: what is allowed/disallowed. What you are supposed to do.
mechanism: ways of enforcing a policy. Ciphers, controls...
assurance: how much reliance you place on each mechanism.
incentives: motives of the people guarding and maintaining the system, and the attackers.

Airport security - 2001 attacks and afterwards

Consider the 911 attacks...

There was actually not any failure of the security systems in place at the time: knives with blades less than 3 inches were OK in 2001. It was a failure of policy, not mechanism.

Since 911? There are still poor policy choices:

1. passenger screening is aggressive and costly, (approx $15 billion), whereas strongly reinforced cockpit doors could remove most risk (est $100 million).
2. Ground staff are seldom screened, planes do not have locks.

Why are such poor policy choices made? Because the incentives for policy makers favour visible controls over effective ones.

Assurance? System screening picks up less than half the weapons.

Bank security

Policy in banks: "The bank never loses!"

Mechanism:
Banks maintain a kind of distributed bookkeeping system, with customer accounts, and (daily) transactions.

Internal:
The main threats to banks are internal - their own staff! The main defences are double-entry bookkeeping (First described in the 15th century), controls on large transactions, and staff required to take vacations.

External:
Buildings are built to look imposing, but just a facade - “security theatre” - (a thief with a gun wins). ATMs (as we have seen) are susceptible to attacks. Bank websites use a mix of techniques - 2-factor authentication, HTTPS. Phishing attempts to bypass this by attacking clients. Banks have been leaders in the use of cryptography for communication.

Military security

In all sorts of areas... Four examples...

1. Electronic warfare and defence - jamming of radar, so opponent cannot see your planes; jamming trigger systems for IEDs.
2. Military communications - not just encryption, but also hiding the source (the location of a transmitter can be attacked, so the military use LPI - low probability of intercept - radio links).
3. Military logistics - who can mobilize 10,000 people and 30,000 meals in a day? Management systems for the military have different requirements from commercial systems - basic rule is that restricted information cannot flow to an unrestricted area.
4. Weapons control (eg nuclear weapons) need much higher levels of assurance than (say) commercial areas.

Hospital security

Policies mostly to ensure patient safety and privacy

Consider patient record systems:

> A mechanism might be that "Nurses can see the patient record for patients cared in their own department over the last 90 days". However, this might be tricky to implement given that Nurses can move departments - the patient record system would become dependent on the hospital personnel system.
> Record anonymizing for research can be tricky. Consider the next slide on database attacks.

There is an extreme requirement for accuracy of web based data (reference texts, drug side effects).

During the SARS outbreak...

Releasing (unexpected) information from databases

Day's average temperature of NUS SoC staff by nationality:

Singaporean	PRC	Poland	German	Australian	NZ	....
36.8	36.9	37.1	36.5	38.2	38.1	....

Numbers of NUS SoC staff by nationality...

Singaporean	PRC	Poland	German	Australian	NZ	....
23	14	3	5	2	1	....

By inference you can deduce that Hugh's temperature was too high!

Home security

Really? Consider...

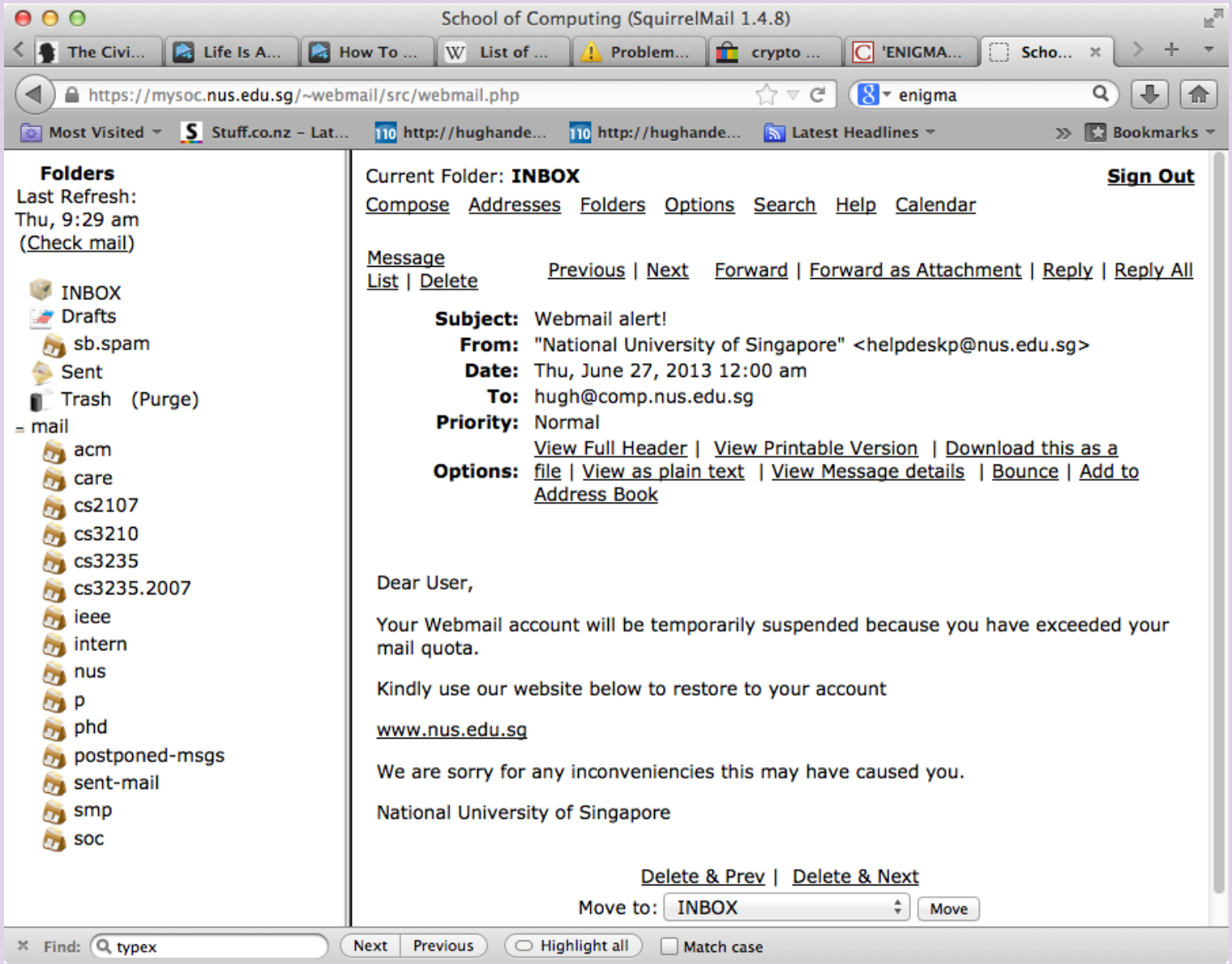
- Web-based banking, over your home wifi.
- Your car key/immobilizer.
- Your (GSM) phone (much harder to clone now than it was five years ago). No unexpected charges.
- Your TV set-top box, electronic gas/electricity meter and so on.
- In some Condos, burglar alarm, lock and security systems.

Summary:

- Policy, mechanism, assurance and incentives
- Controls, visible and effective controls, security theatre
- 2-factor authentication, HTTPS, Phishing
- Database attacks

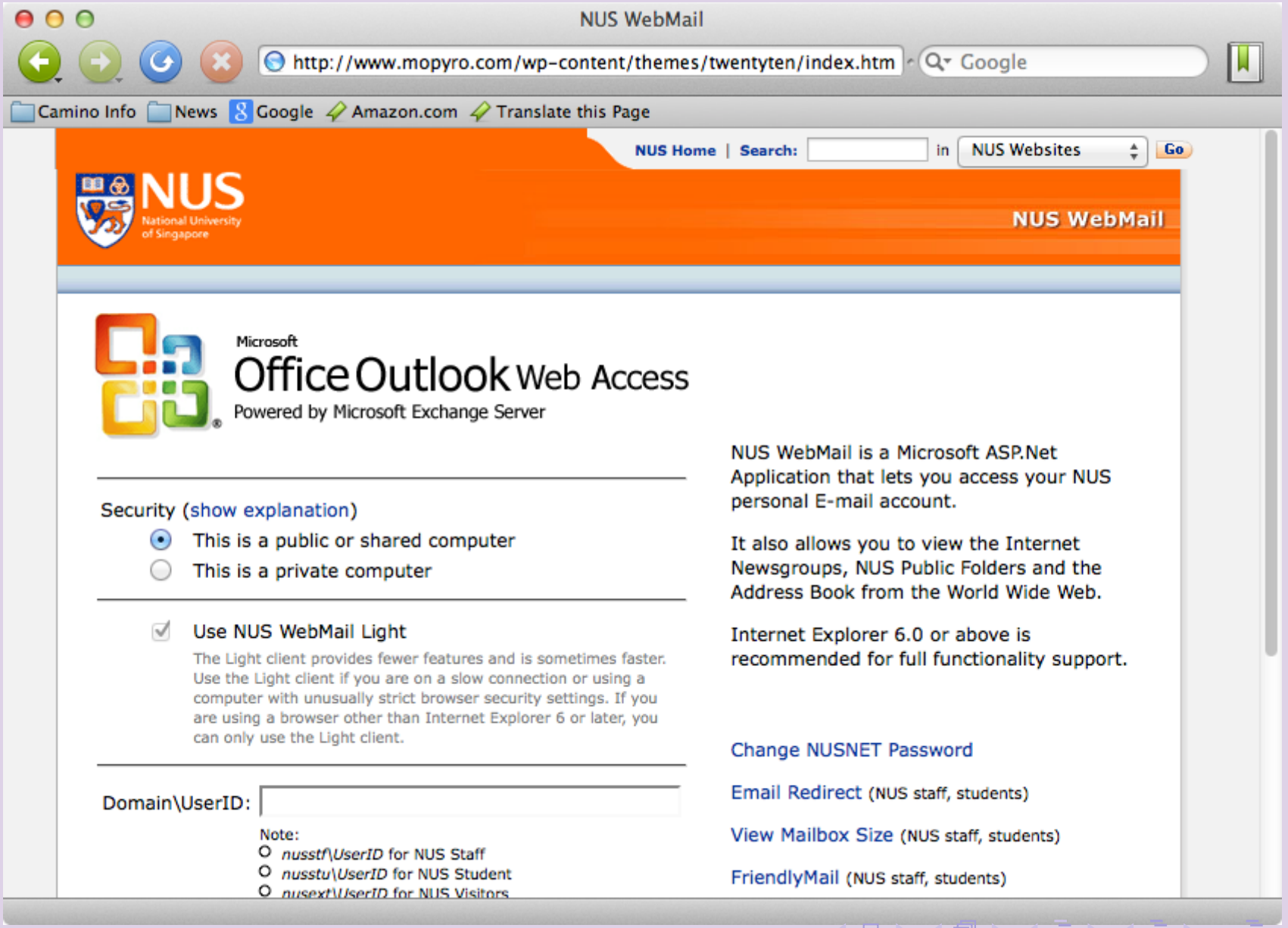
Personal security

Normal mail: click on the link...



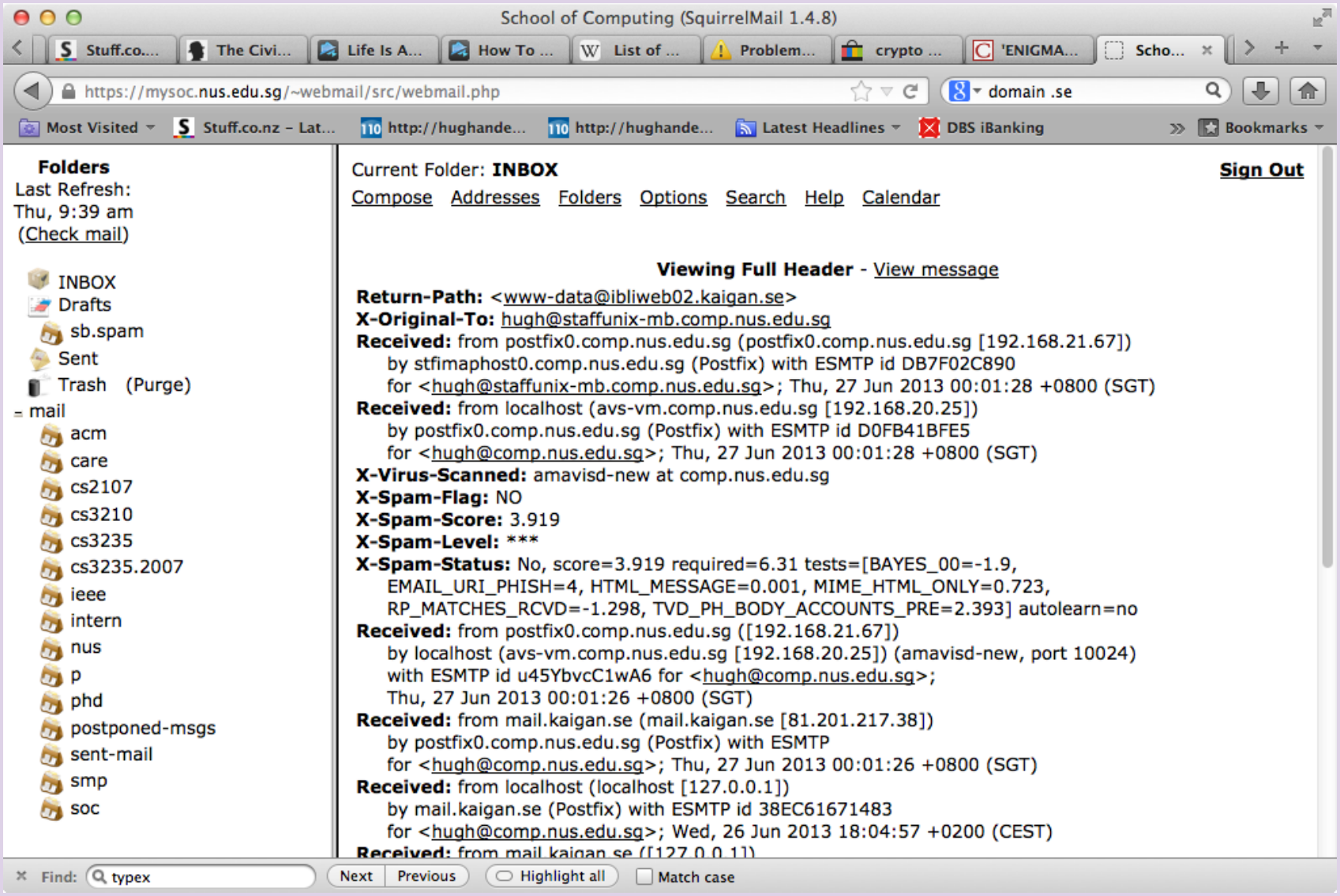
Normal looking login

I clicked on the link! (Just for you :)



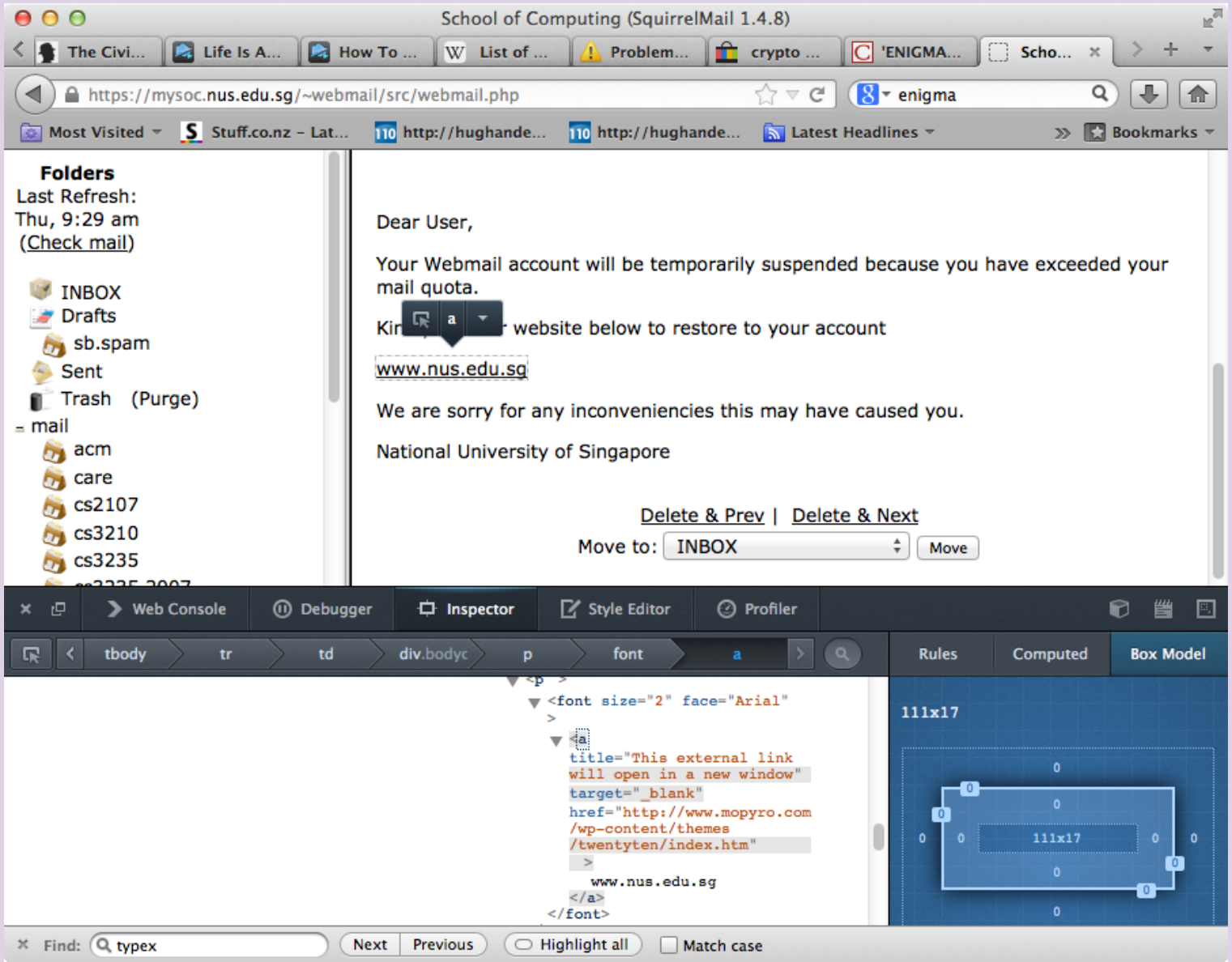
Detail in the mail

Where did it come from?



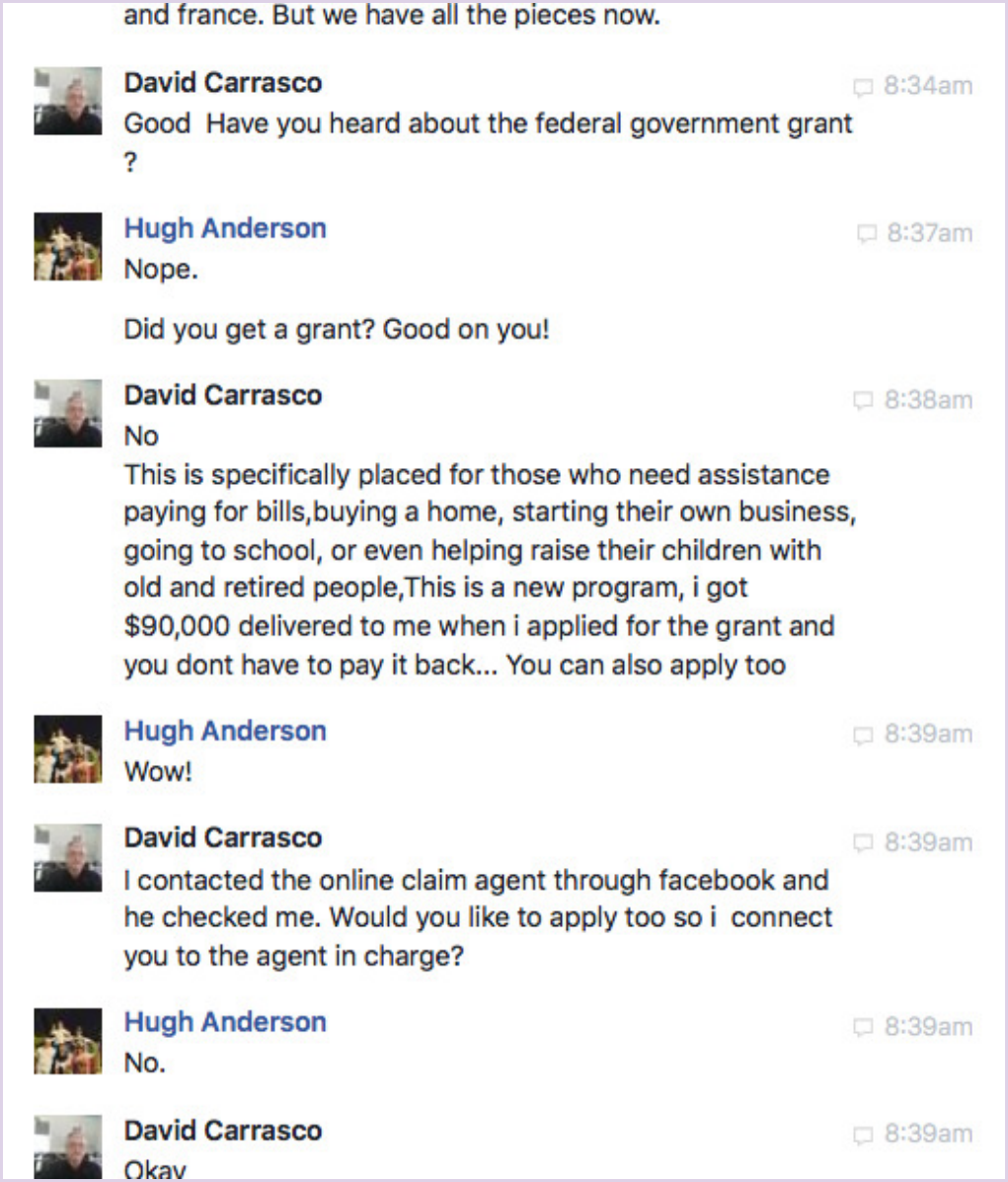
Detail in the mail

Why does the link not match the URL?



My brother-in-law messaged me recently

Except it was not him...



and france. But we have all the pieces now.

David Carrasco 8:34am
Good Have you heard about the federal government grant ?

Hugh Anderson 8:37am
Nope.

Did you get a grant? Good on you!

David Carrasco 8:38am
No
This is specifically placed for those who need assistance paying for bills,buying a home, starting their own business, going to school, or even helping raise their children with old and retired people,This is a new program, i got $90,000 delivered to me when i applied for the grant and you dont have to pay it back... You can also apply too

Hugh Anderson 8:39am
Wow!

David Carrasco 8:39am
I contacted the online claim agent through facebook and he checked me. Would you like to apply too so i connect you to the agent in charge?

Hugh Anderson 8:39am
No.

David Carrasco 8:39am
Okay

Outline

Systems/Services/Goals, Attacks and Threats

What is a system? It can vary...

1. **Product or component**: such as a smartcard, a PC, a protocol...
2. **Collection**: some products/components, and an OS, network, making up an organization's infrastructure.
3. **Application**: the above and some set of applications.
4. **Composite**: the above and IT staff, and perhaps users, management, clients, customers...

A system can thus refer to small things or big things. This indeterminacy about even basic words leads to confusion, and errors.

Basic terms

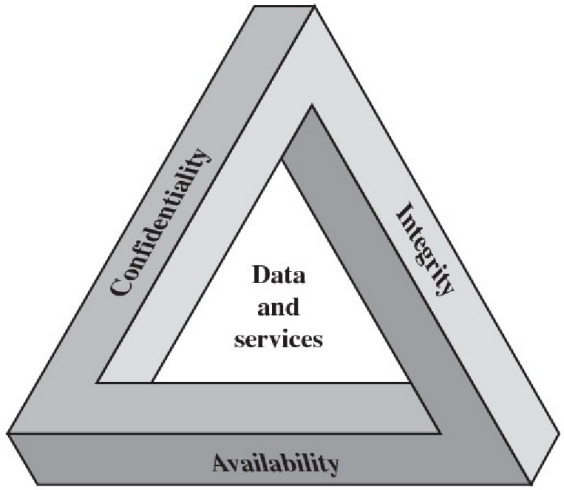
Vulnerability/Threats: If there is a weakness (vulnerability), then a potentially harmful situation (threat) may occur.

Services/Goals: ensuring adequate service in a computer system. CIA! Good guys need 'em.

Attacks/Controls: An attack=threat+vulnerability. A control is a way of reducing the effect of a vulnerability. MOM! Bad guys need 'em.

The CIA triad...

FIPS specify three objectives/goals:



- **confidentiality**: concealing information - resources may only be accessed by authorized parties;
- **integrity**: trustworthiness of data - resources may only be modified by authorized parties in authorized ways;
- **availability**: preventing DOS/denial-of-service - resources are accessible in a timely manner.

Attacks and threats

Three aspects of attacks: MOM

- **Method**: tools, knowledge;
- **Opportunity**: time, access;
- **Motive**: what advantage is there?

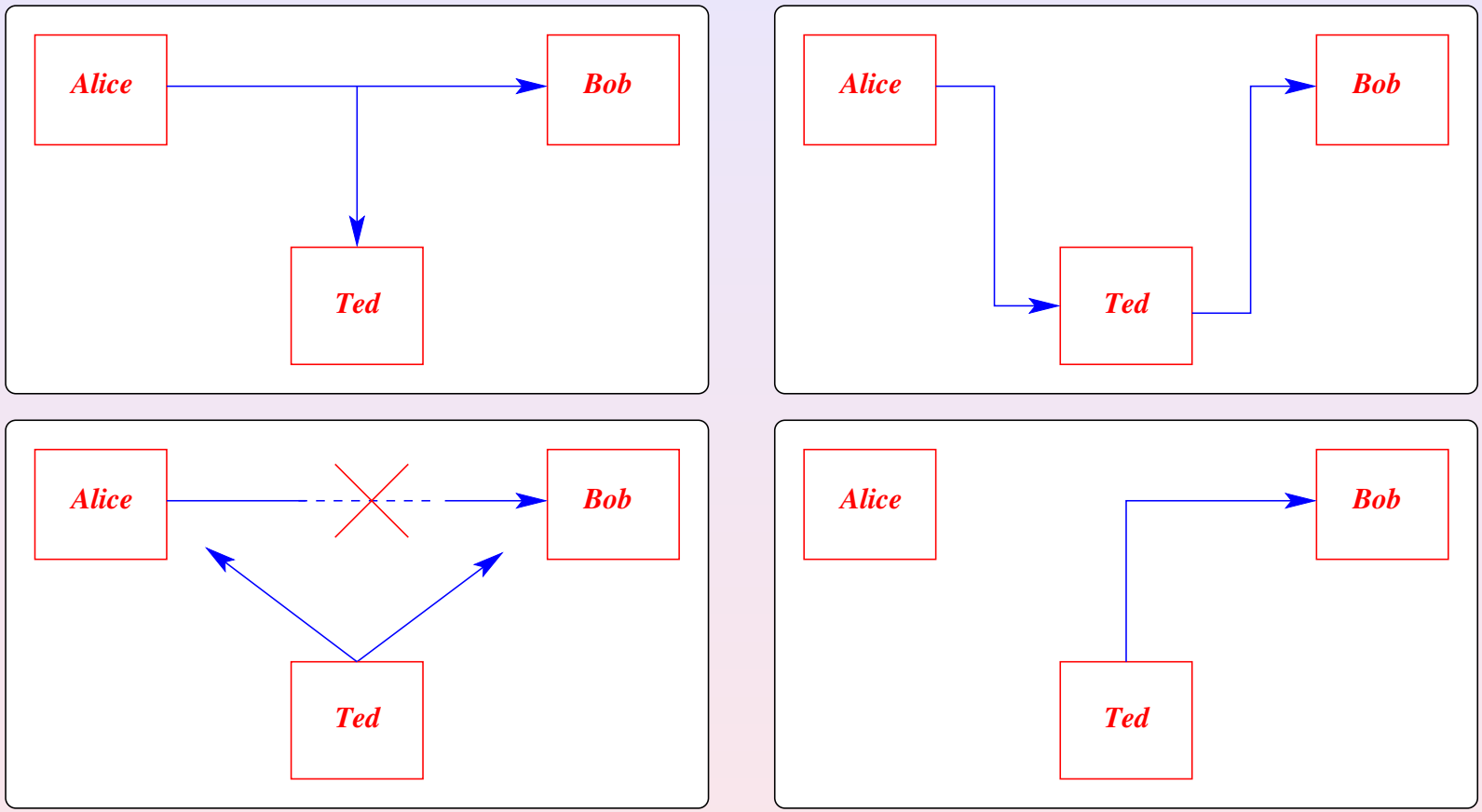
An important basic principle for attacks:

- **The weakest link**: An attacker only needs one small flaw in a system

Threats

- **disclosure**: unauthorized access (snooping/interception);
- **deception**: accept false data (man-in-the-middle/modification);
- **disruption**: prevent correct operation (denial-of-service/interruption);
- **usurpation**: unauthorized control (spoofing/fabrication).

Types of attacks

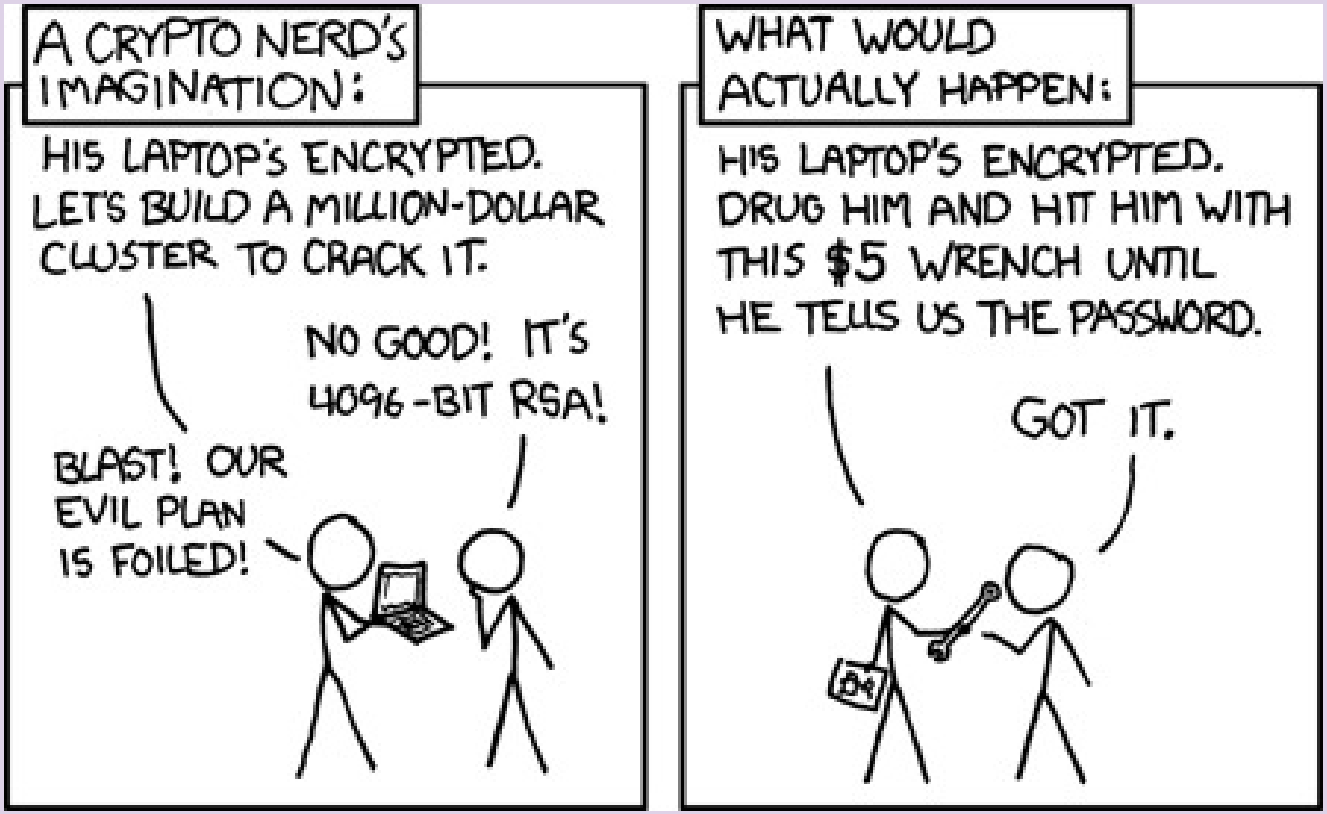


(... or ... Interception, Modification, Interruption, Fabrication)

Types of attacks

And persuasion

human factors and **social engineering**:



Attack “surfaces” for CS3235

We will not look (any more) at human factors on its own...

1. **people**: the ways in which people are manipulated. (But dont minimize this, consider Emmanuel Nwude - $242M)

But we will look at these...

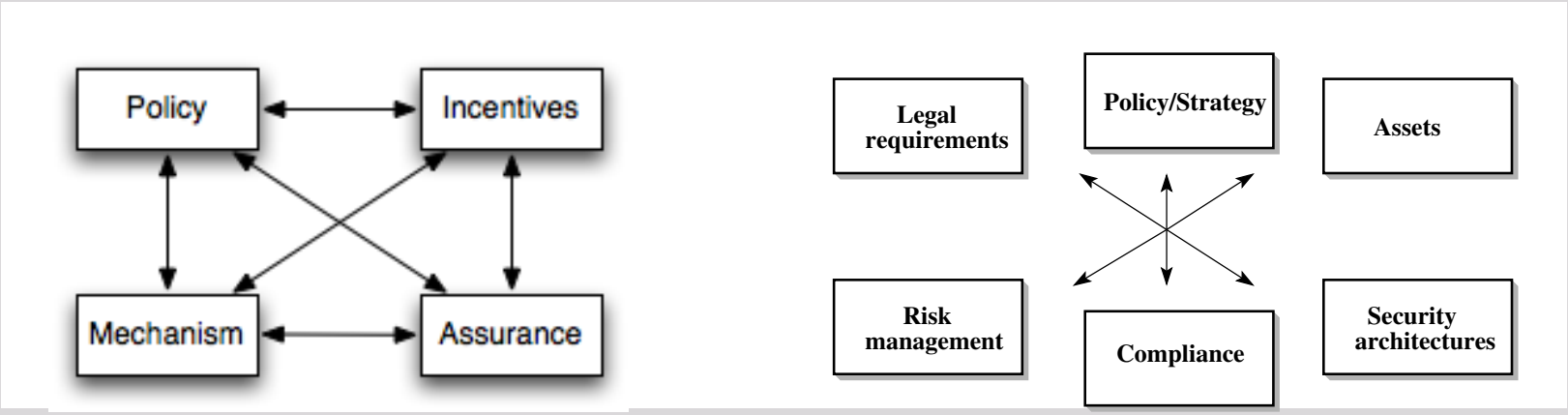
1. **complexity**: complex systems - large number of attack vectors.
2. **cryptography**: underpinning much of the IT world.
3. **communication systems**: communication between them may be attacked.
4. **high level IP**: the Internet was not designed with security in mind.
5. **web applications**: a range of attack vectors,
6. **machine architecture**: machine hardware, operating systems.

The new computer based landscape

Information and system security...

...can apply to governments, infrastructure, organizations, businesses personal security... What is a framework for thinking about this?

Frameworks: Ross Anderson's PIMA and Jeff Carr's:



Information warfare...

You can view the landscape as that of "Information warfare", and there are a wide range of activities (and hence jobs): Information Security Engineer, IT Security Architect, IT Security Specialist, IT Security Analyst, Business Security Manager, Security Research (Technical)....