DOTA2024:1
Defense of the Ancients
First topic - Introduction to IT security

Hugh Anderson

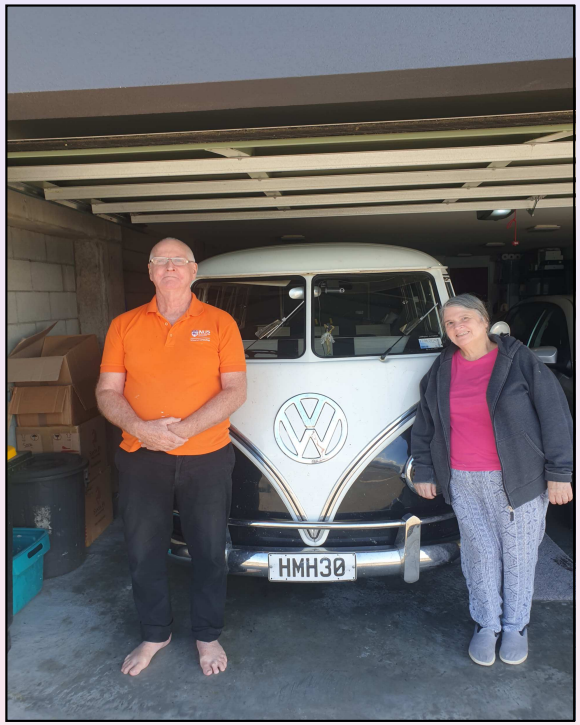
National University of Singapore
School of Computing

May 19, 2024

Family ... ... and development ...

1997

2016



2024

Isolation...

Outline

Outline

Outline

Your teaching staff

Lecturer		Hugh Anderson
Teaching assistant		Shen Jiamin

Information and contact details

Please call me Hugh, and email me at hugh@comp.nus.edu.sg. Other, faster, contact details will be given on 2nd July.

Jiamin is now a 3rd-year PhD student specializing in security and confidentiality computing. Before this, he completed his B.Eng in Information Security from Shanghai Jiao Tong University (SJTU) and obtained an M.Comp from NUS. In addition to his research focus on security, Jiamin has amassed valuable experience as a teaching assistant for Operating Systems courses. While he is typically active in the afternoons and evenings, Jiamin prefers to recharge during the mornings. Feel free to call him Jiamin.

Assessment

Assessment	Grade
MCQ - Short answer questions test on Thursday 18th (?)	12%
Laboratories	20%
Incentive marks	8%
Group project	60%
Total marks	**100%**

Laboratories/Project ...

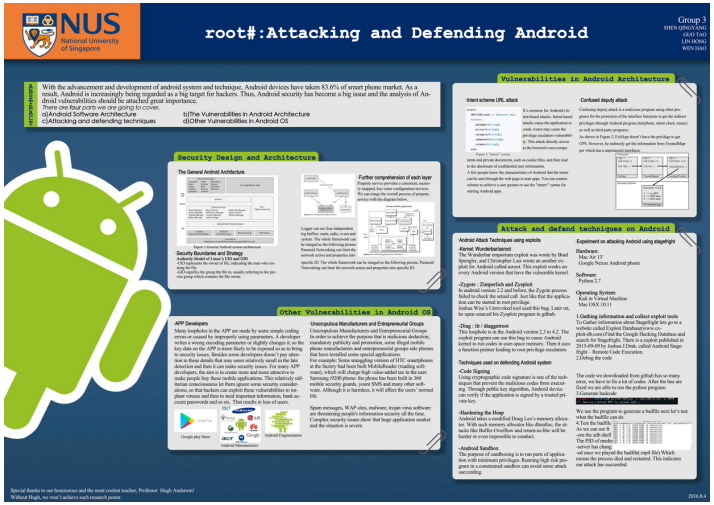
If you become one of the DOTA project people, an introductory session will be held in the first week to introduce you to the labs, and to introduce the projects.

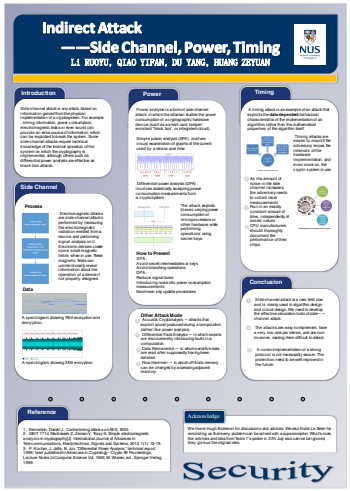
Some parts of the laboratories are done individually, some parts may be done in pairs - two of you team up to do a part of a laboratory. In some labs you will assess yourself, and can give yourself whatever mark you want - if you think you deserve 100 points, give yourself 100 points. If you think “Over 9000!”, then it is “Over 9000!”.

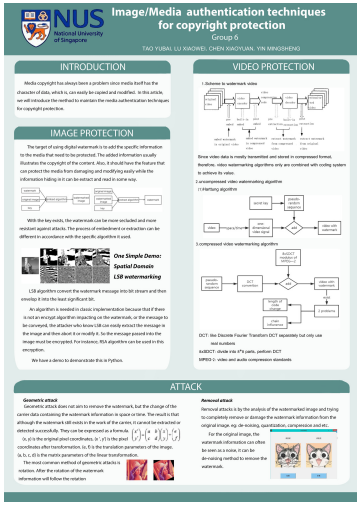
The course outline (approximately)...

Monday	Tuesday	Wednesday	Thursday	Friday	Sat/Sun
1	2	3	4	5	6/7
	LT1	LT2		LT3	
	SystemComplexity	*Crypto*		*IPnetworks*	
	Crypto				
	Consult	Lab 1	Consult	Consult	
8	9	10	11	12	13/14
	LT4	LT5		LT6	
	OtherNetworks	*WebApplications*		*Infrastructure*	
Consult	Lab 2	Consult	Consult	Lab 3	
15	16	17	18	19	20
	LT7	LT8		Posters	Showcase
	MachArchitecture	*RainbowShor*			
		MCQ test			
Consult	Lab 4	Consult	Consult		

The Project...







The project starts in July!

You will find the project specifications in Canvas well before 2 July, and examples of similar projects at `https://www.comp.nus.edu.sg/~hugh/DOTA2021/`.

The projects will each take the form of a video, a supporting poster, and a paper. The projects are underspecified, and you should talk to Jiamin and me.

Outline

Aspects of IT security

What are the issues?

The term "IT security" hides a worrying reality. The issues are wide ranging:

- *It is **warfare**! Large scale, small scale, **all** scale. Risks can be to your bank account, your peace of mind, your life, your friends, your country.*
- *There are no **truces**. There is no white flag to wave. It is **relentless**.*
- *It is not just a matter of an IT system having an exploitable error. **All** the systems which we use have **structural** issues.*

Not just "software"; Many distinct subject areas...

- **Secrecy.** Encryption of documents...
- **Insecurity.** Not just secrecy, sometimes things like non-repudiation.
- **Safety/control software and hardware.** Complex (SW/HW) 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

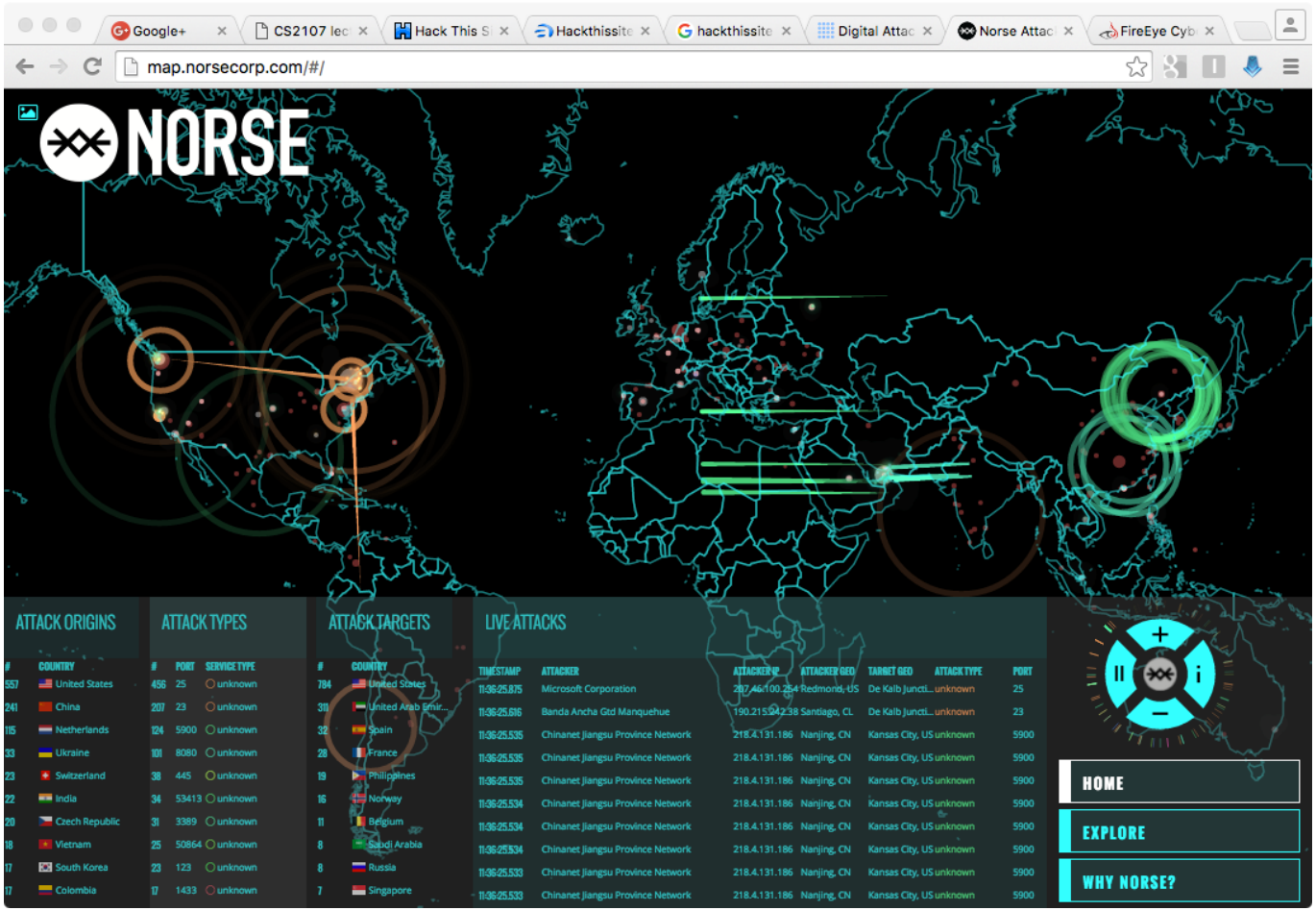
This technique was used by Histiæus to ensure *confidentiality.* It was used again by Germany in the 1914-1918 European war. This is now called steganography (hiding information amongst other stuff).

More history...

Warfare, warfare, warfare

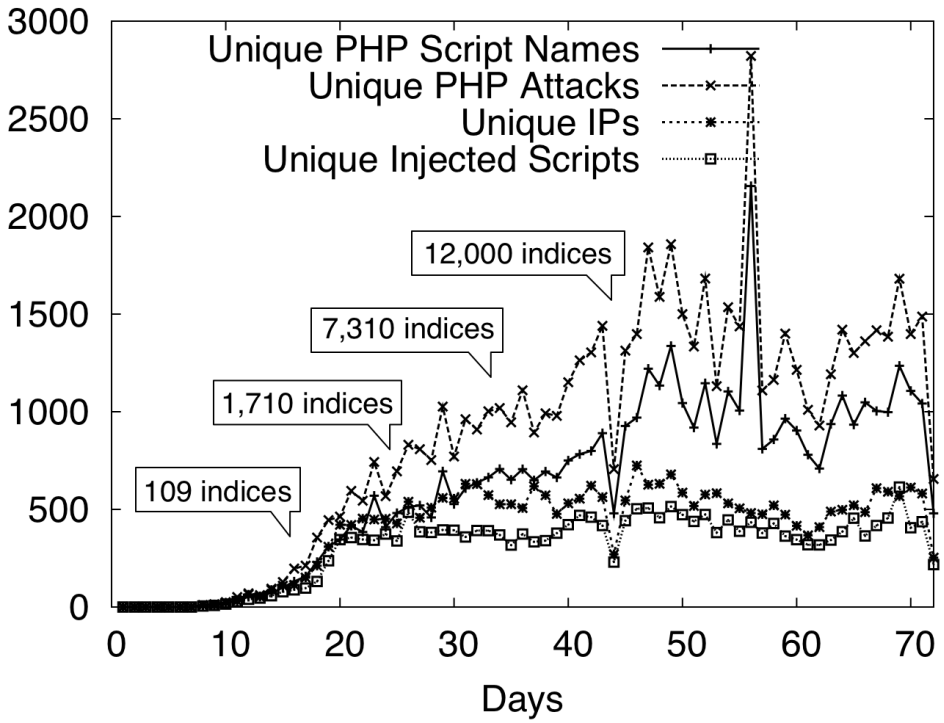
In the field of computer security, it is often common to see examples taken from the world of warfare.
We will see how Cæsar encoded messages - an early example of cryptography.
We might also examine computer protocols. In the real world, some of the earliest protocols were to ensure the correct conduct 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.

DBS/POSB attacks in Singapore 12 years ago

Big news at the time...

sph A SINGAPORE PRESS HOLDINGS PORTAL
asiaone NEWS

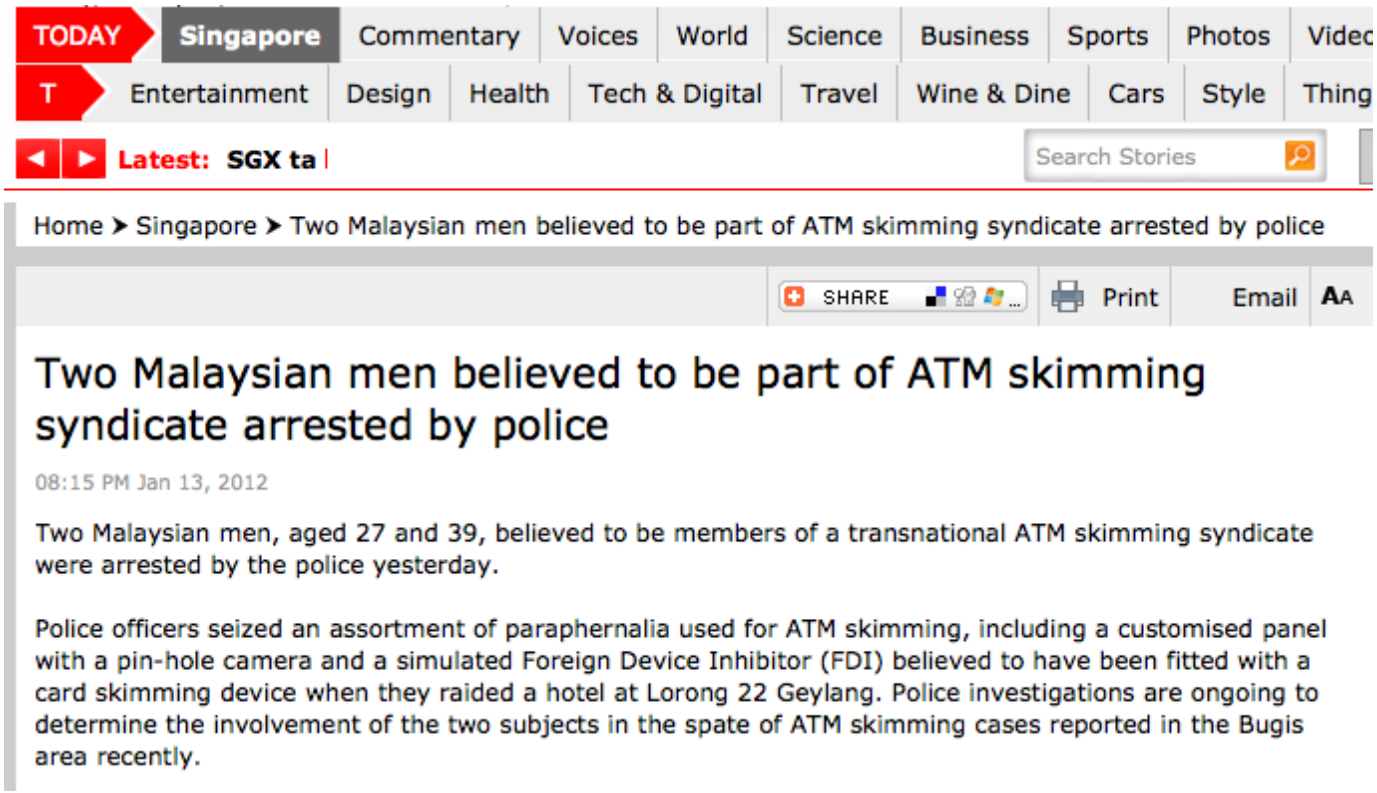
DBS/POSB customers hit by unauthorised ATM withdrawals

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

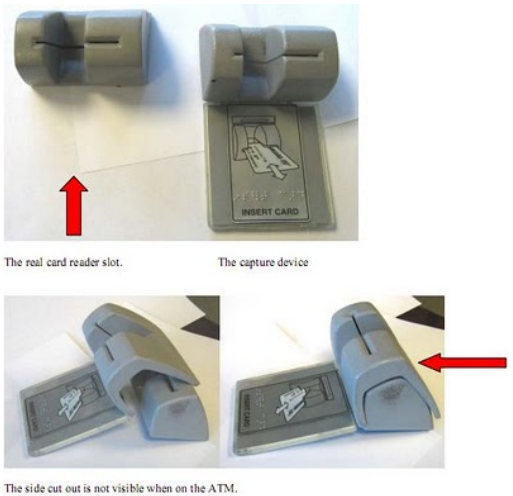
Two Malaysian men, aged 27 and 39, believed to be members of a transnational ATM skimming syndicate were arrested by the police yesterday.

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.

ATM attacks (Small scale warfare)

How was it done?

It was done through the use of card skimmers on two ATM machines. 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.

ATM 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).

PIN attacks

Getting the PIN?

A (pinhole) camera or an overlay over the keyboard.

Sometimes getting a gate PIN is REALLY easy!

Installing a skimmer...

Here is another skimmer...

LARGE SCALE theft...

$1B dollar attempt - big news a few years ago...

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]

A quick quiz...

Which of these two vehicles has a door lock?

Value US$ 15,000

Value US$ 250,000,000

Answer?

Waikato (NZ) District Health Board: #1 (10yrs ago)

Car Park gate-controller machines...

In a DHB building in NZ, the machines that controlled the gates in the car park were connected to the (internal) DHB network. These machines were running an old version of an operating system, and had not been updated in years. They were infected with the Conficker worm from a USB stick plugged in by a car-park technician.

- The worm propagated through the building, and eventually to most of the DHBs regional (internal) network, including servers and PCs.

Consequences...

Much of the DHB network was down for two days, while administrators removed the infection, and identified the source of the infection

- Though there was not much direct damage to the systems at DHB (The payload of the worm was targetted at setting up a botnet) the consequences were very personal, involving delays on medical records, operations and other health related issues.

Waikato (NZ) District Health Board: #2 (recently)

In May 2021 - ransomware via an email!

Consequences...

DHB network down for months, records lost, patient operations cancelled etc. At one time the chief officer claimed that no machines were damaged, choosing to ignore the social and health damage!

Work and Income NZ (WINZ)

Another Trojan Horse?

Work and Income NZ provide public access terminals in all of their offices around NZ. Most towns have WINZ offices. The public can use these terminals for various uses, including to look for, and apply for jobs.
Keith Ng blogged that you could go into any WINZ office and use them to access the WINZ, and Ministry for Social Development corporate networks.

- Keith was a citizen reporter, not a hacker, but said that they had some basic features disabled - you couldn't just open up File Manager...
- However, by using "Open File" in Microsoft Office, you could map any unsecured computer at WINZ, and then open up accessible files.
- He carried on to expose a wide range of information that appeared to be easily accessable.

Consequences...

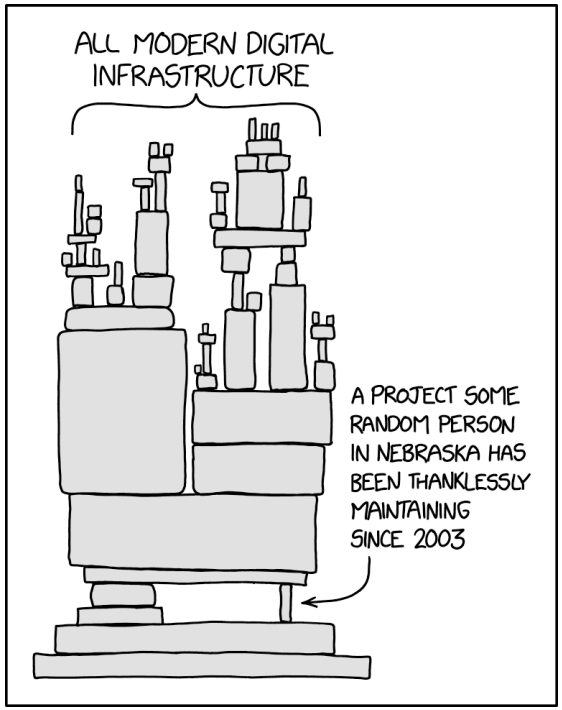
Keith became a real journalist!

Consequences: 1MW Diesel generator blown up

In 2000 I worked at the University of the South Pacific in Suva, Fiji during a coup, and some villagers sabotaged the Monasavu dam, cutting power to the entire country. For over three months we lived without power, although the electricity department did manage to get some small generators going to provide 20 minutes of electricity to Suva every day. No phones, no shops open, no lights, eventually no water, no news, no Internet.

Structure: attack on open source software

Open source compression library: xz-utils!



Relied on in Linux and the open source community (updates, the kernel, browsers etc). In February 2024, malicious code which allowed for remote execution *of code was injected into at least two official distributions. This was discovered accidentally in March, and we will revisit this story when we look at Social Engineering.*

Note that this was a successful injection of malicious code in an "open source" project.

Summary...

Case studies show us...

Warfare: All the stories remind us that there are unannounced “IT” wars going on. Not missiles and bombs, but the effect can be equally challenging.

Relentless: The Waikato DHB stories show that even when there has been considerable effort to protect systems, attacks continually re-occur, and the arbitrary infections can have serious consequences.

Structural: The WINZ corporate network was so flat, that anybody anywhere on the network could access anything. In building a large system we should design in multiple authority checks. The xz story reminds us how interconnected our systems are.

These stories remind us of the interconnected nature of the systems we rely on. It is not just PCs.

Outline

Hard to find the boundaries of “Security”

It is not "one thing"...

Security is complex:

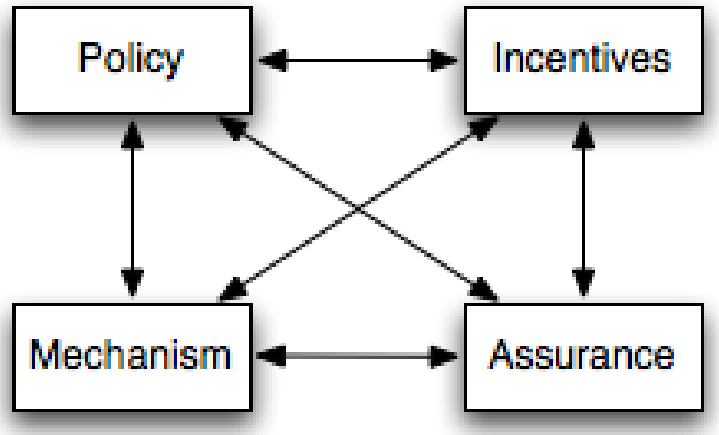
> Security can involve elements such as computers, people, locks, communication links and so on.
> The goals of security might involve authentication, integrity, accountability, and so on.
> A security system may involve an arbitrary combination of these elements and goals.

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 9/11 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 9/11? 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 disease 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/LTE) phone (harder to attack now than it was five years ago, but not really hard...). 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
- Multi-factor authentication, HTTPS, Phishing
- Database attacks

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

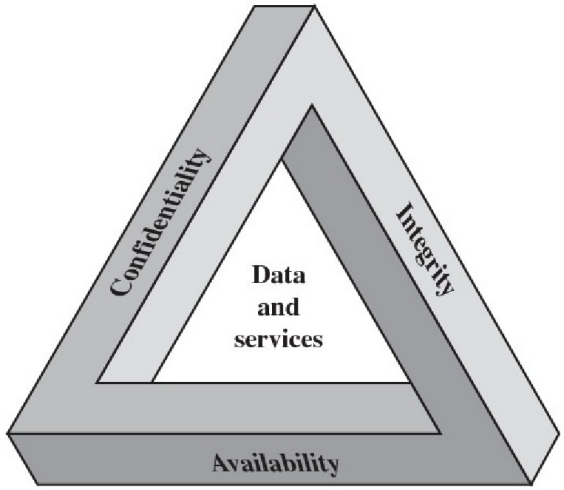
Vulnerability/Threats: If there is a weakness (vulnerability), then a potentially harmful situation (threat) may occur.

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?

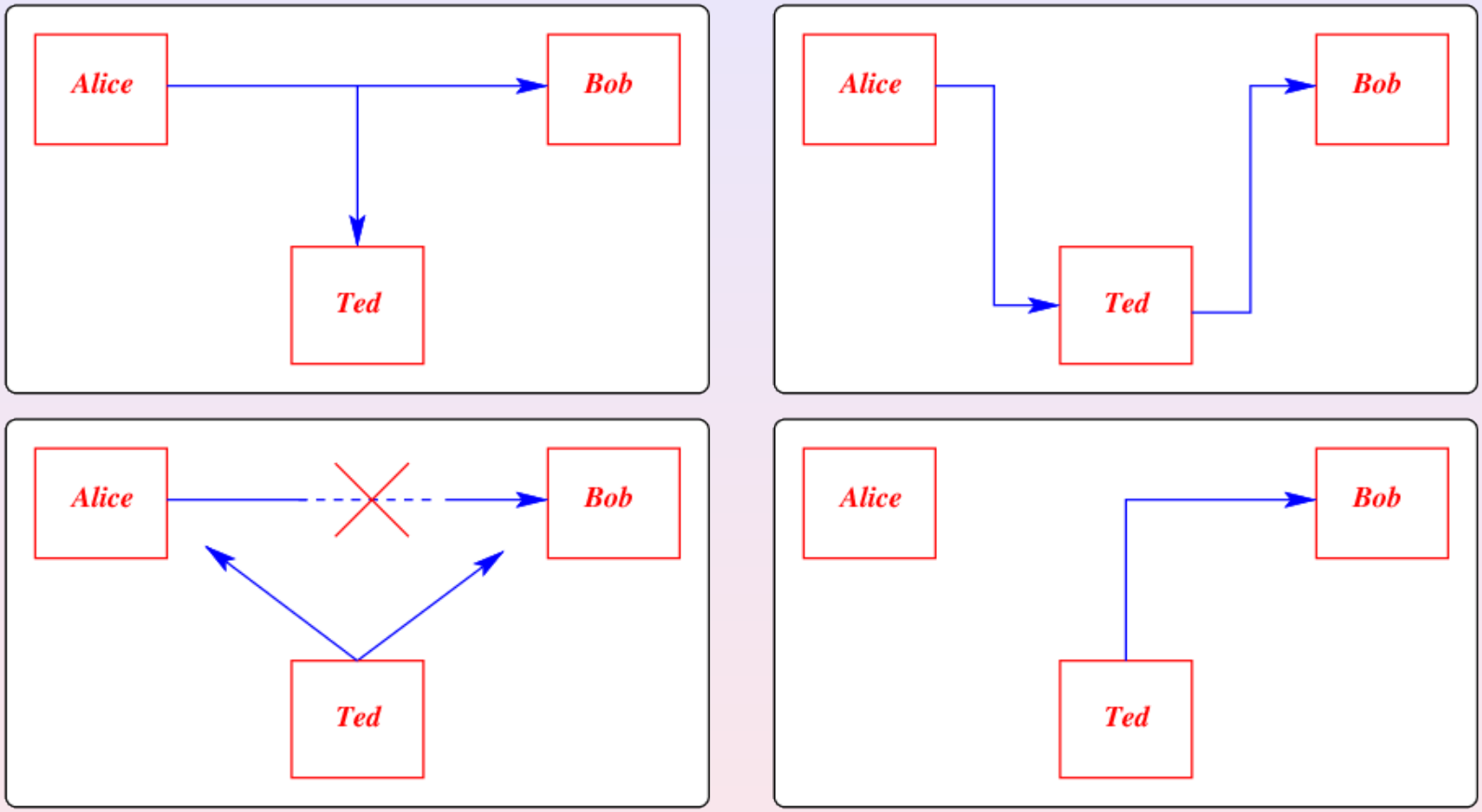
An important basic principle for attacks:

- **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

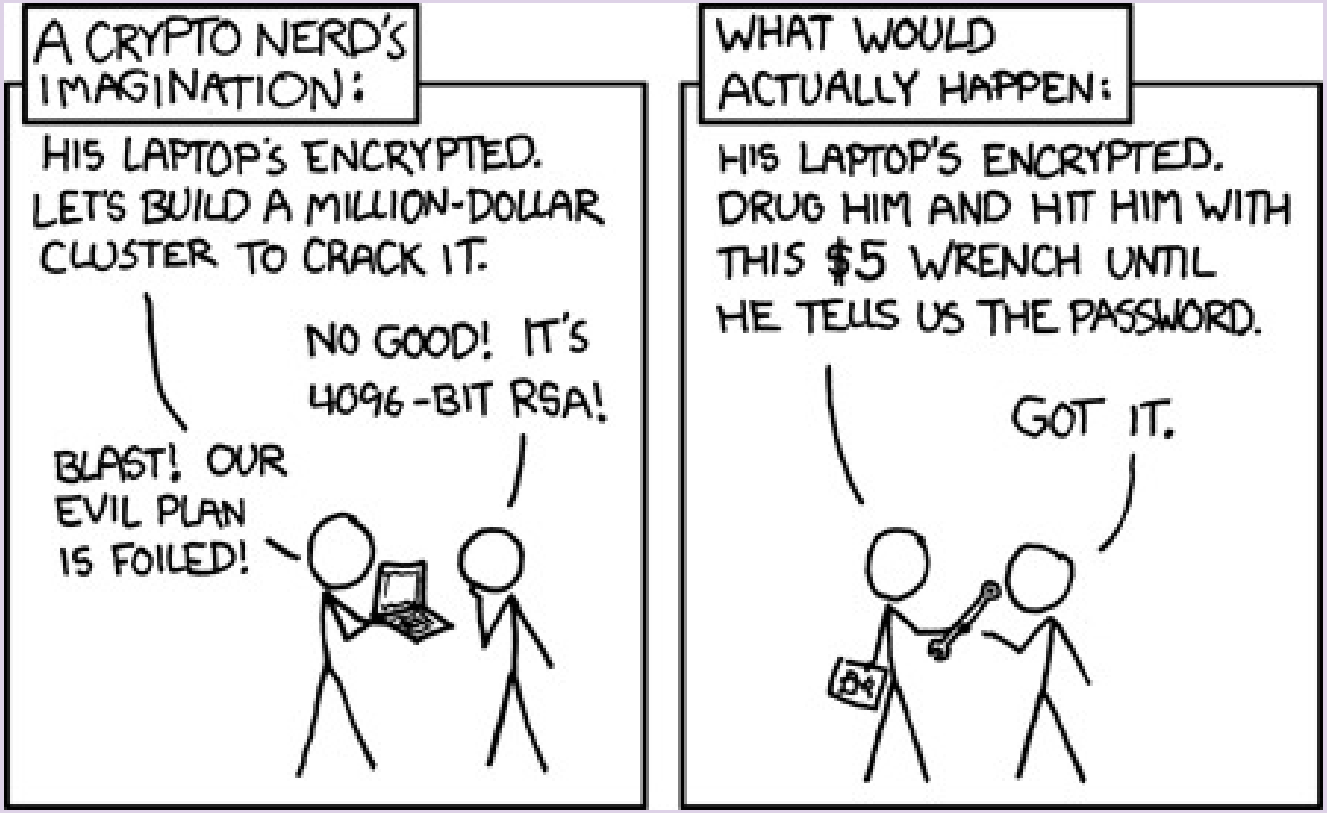


(... or ... Interception, Modification, Interruption, Fabrication)

Types of attacks

And persuasion

human factors and **social engineering**:



Attack “surfaces” for DOTA2024

We will look at these...

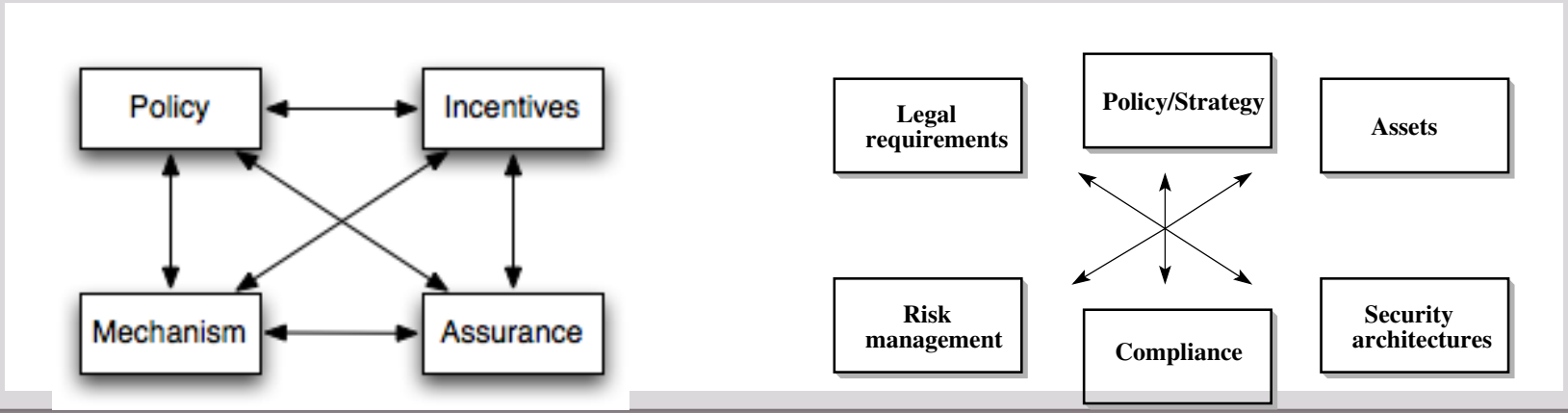
1. **people**: the ways in which people are manipulated.
2. **complexity**: complex systems - large number of attack vectors.
3. **cryptography**: underpinning much of the IT world.
4. **communication systems**: communication between them may be attacked.
5. **high level IP**: the Internet was not designed with security in mind.
6. **web applications**: a range of attack vectors,
7. **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)....