Fundamentals of Information Security

Lecture 1: Threats, Vulnerabilities and Attacks

Outline

- Introduction
- Threats
  - Threat sources
  - Threat types
- Vulnerabilities
- Attacks
  - Passive attacks
  - Active attacks
- Summary

Introduction

- Information is an important asset for
  - People
  - Organisations
- Information security is about protecting information assets from damage or harm
- Questions to consider are:
  - *What are the assets to be protected?* and
  - *How could they possibly be harmed?*

Introduction

- For a particular information asset, the security goal may be:
  - **Confidentiality**: preventing the unauthorised disclosure of information
  - **Integrity**: preventing the unauthorised modification or destruction of information
  - **Availability**: ensuring resources are accessible when required by an authorised entity
- This lecture considers some possible
  - threats, vulnerabilities and attacks

Outline

- Introduction
- Threats
  - Threat sources
  - Threat types
- Vulnerabilities
- Attacks
  - Passive attacks
  - Active attacks
- Summary

Challenges of Securing Information

- Security figures prominently in 21st century world
  - Personal security
  - Information security
- Securing information
  - No simple solution
  - Many different types of attacks
  - Defending against attacks often difficult

What Is Information Security?

- Before defense is possible, one must understand:
  - What information security is
  - Why it is important
  - Who the attackers are

Defining Information Security

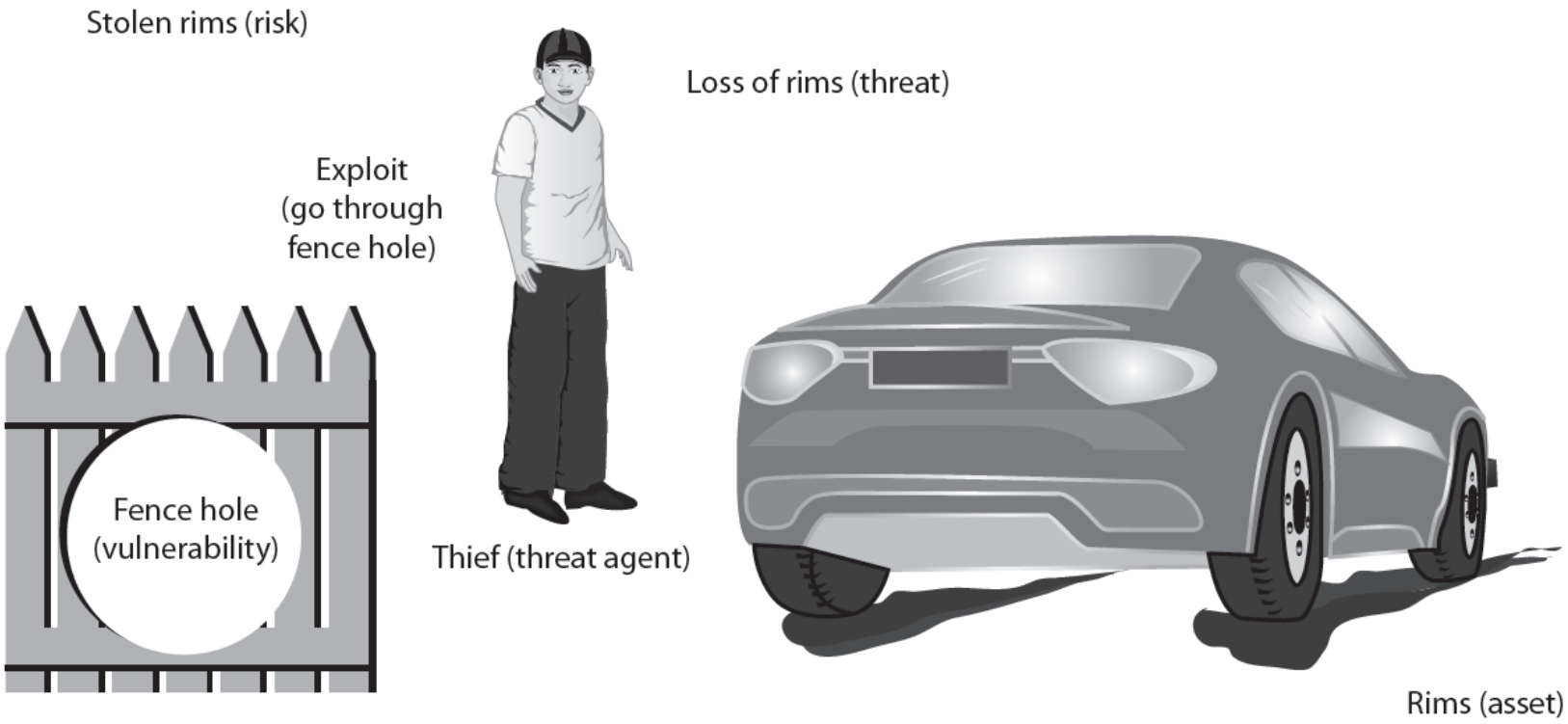
- Security
  - Steps to protect person or property from harm
    - Harm may be intentional or nonintentional
  - Sacrifices convenience for safety
- Information security
  - Guarding digitally-formatted information:
    - That provides value to people and organizations

Defining Information Security (cont'd.)

- Three types of information protection: often called CIA
  - Confidentiality
    - Only approved individuals may access information
  - Integrity
    - Information is correct and unaltered
  - Availability
    - Information is accessible to authorized users

Defining Information Security (cont'd.)

- Protections implemented to secure information
  - Authentication
    - Individual is who they claim to be
  - Authorization
    - Grant ability to access information
  - Accounting
    - Provides tracking of events



Information security components analogy

Threats

- A set of circumstances with *potential* to cause harm to an information asset by compromising stated information security goals.
  - **A breach of confidentiality**: information is disclosed to unauthorised entities
  - **A breach of integrity**: information assets have been modified or destroyed by unauthorised entity
  - **A breach of availability**: information assets are not accessible when required by an authorised entity

Threats

- How seriously should you consider possible threats?
- 2012 Australian Computer Crime and Security Survey – Systems of National Interest
  - Responses from 255 organisations (sent to approx 450)
  - Respondents from 11 industry sectors
  - 22% reported experiencing a cyber attack in past 12 months
    - 9% answered did not know
  - No. of attacks reported by the organisations who did report attacks:

# of incidents	Reported by
1-5	65%
6-10	9%
More than 10	21%
Don’t know	5%

Threats

- Threat sources:
  - External:
    - Source of threat lies outside of the organisation
    - Example:
      - People who are not authorized to use information systems - commercial competitor, cyber-criminal, political activist, terrorists
  - Internal:
    - Source of threat lies within the organisation
    - Example:
      - people who are authorized to use information systems - employees, contractors, clients, visitors

Threats

- Threat sources: external and internal
  - 2012 Australian Computer Crime and Security Survey – Systems of National Interest, p18
  - Of the respondents who knew they had suffered electronic attack,
    - 71% reported they experienced 1 - 5 external attacks
    - 44% reported they experienced 1 - 5 internal attacks
  - Need to consider both internal and external threat sources

Threats

- Threat sources:
  - External sources
    - May need to gain access to information assets used in an organisation in order to harm them
      - Physical access
      - Logical access
    - Increasing dependence on information and communications technologies (ICT) operating over internet expands potential external sources with logical access
      - Common threats: malware (virus, trojan, worm, spyware)

Threats

- Threat sources:
  - Internal sources:
    - Insiders are familiar with information systems used in an organisation:
      - Have knowledge of asset values
      - Know processes and procedures in use
      - May be aware of system vulnerabilities
    - Have opportunity to access assets
    - May misuse systems or exceed their authorization
    - Potential to cause harm is high
  - Outsourcing (cleaners, catering, support services) without security assurance brings outsiders in!

Threats

- Threat type:
  - Natural event
    - Examples: Earthquake, Fire, Flood, Storm, Tornado, Tidal Wave
  - Human action
    - Deliberate (intended to cause harm)
      - Examples: Espionage, fraud, sabotage, theft
    - Accidental (no intent to cause harm)
      - Examples: acts of negligence, errors, omissions

Threats

- Natural events:
  - Potential for threat to occur may depend on physical location of the information asset
    - Historical data may be useful indicator
    - Recent examples:
      - Brisbane: January 2011 floods – lots of data to indicate areas of concern (comparisons to 1974 flood levels)
      - Christchurch NZ: February 2011 earthquake
      - Indiana, US: March 2012 tornadoes
  - Most likely results in
    - availability of information asset being compromised
    - may also compromise confidentiality

Threats

- Examples: Brisbane floods - power outage

Floodwaters cause power outages across southeast Queensland, with more than 22,000 properties affected

James O'Loan and Kate Higgins | The Courier-Mail | January 11, 2011 5:00PM

Recommend 10 people recommend this. 5 retweet Share

THERE are now more than 20,000 southeast Queensland homes without power as floods force communities to shut down.

Energex has advised crews are on standby to switch off electricity to low-lying areas of Brisbane and Ipswich.

The outages could impact about 100,000 customers with restoration dates yet to be determined.

While crews from both Energex and Ergon were scrambling to restore electricity in horrendous conditions, both providers were unable to power would be reconnected tonight.

In many areas, access to critical repair sites remain blocked by flooded roads and power stations.

Threats

- Example: *Haitian earthquake* January 2010
  - Amnesty International report: "*Haiti: After the Earthquake* Initial Mission Findings March 2010".
  - Source: www.amnesty.org/en/library/asset/AMR36/.../amr360042010en.pdf
- Report claims related to files held at the Palais de Justice of Port-au-Prince include that:
  - Haitian authorities failed to:
    - protect sensitive files and evidence held at the Palais de Justice
    - restrict access to other buildings of the judiciary after the quake.
  - Amnesty International received reports that criminal files and judicial archives had been stolen or burnt on site.

Threats

- Tornado damage, US March 2012:
  - **“Deadly tornadoes leave U.S. towns wrecked”**
  - http://www.cbc.ca/news/world/story/2012/03/02/tornadoes-us-south.html

Mindy Nye, 18, of Henryville, Ind., looks through debris on March 4, after a tornado destroyed her home. (Brynn Anderson/Lincoln Journal Star/AP)

Threats

- Human action – deliberate
  - Actions intended to cause harm to information assets
    - Examples include:
      - Eavesdropping, Espionage, Extortion, Fire, Fraud, Industrial action, Malicious code, Sabotage, Social engineering, Theft, Vandalism
  - Consider physical and logical assets
  - Security goals compromised depend on the actions that were taken and the asset involved
    - possible to compromise all security goals

Threats

- Example: Human action – deliberate
  - Malware
    - Malicious software deliberately designed to breach security of computer based information systems
    - Depending on the payload action, malware could compromise:
      - Confidentiality: For example, logging keystrokes to obtain passwords
      - Integrity: For example, by writing a message, or corrupting data files
      - Availability: For example, by deleting data or application files

Threats

- Human action – deliberate
  - Common malware types:
    - Viruses – programs with ability to replicate
      - Spreads by copying itself into other files (infecting) and is activated when these files are open or executables are run
    - Worms – programs with ability to self replicate
      - Spreads from computer to computer without human interaction
    - Trojan horses – programs with known desirable properties and hidden undesirable property.
      - User downloads the program and knowingly uses desirable features
      - Undesirable feature runs without user knowledge

Threats

- Example: Human action – deliberate
  - April 2010
    - San Francisco Network Administrator Terry Childs found guilty of tampering with network
      - Administrator in Department of Telecommunications and Information Services
      - Had sole control over many administrative procedures
    - July 2008 locked up access to city's FiberWAN network
      - Reset administrative passwords to switches and routers
      - Would not reveal them to others
    - San Francisco city lost control of network for over 10 days
    - City spent hundreds of thousands of dollars to recover

Threats

- Example: Human action – deliberate
  - Theft of Michael Jackson back catalogue from Sony
  - Source: http://www.mtv.ca/news/article.jhtml?id=39963

Threats

- Human action – accidental
  - No intention to cause harm, but actions do have potential for harm
    - Examples include: accidental damage to equipment, change management errors, configuration errors, loss of personnel, loss of property, misdirecting messages, operational errors (such as inadvertent deletion of files or incorrect data entry), programming errors, etc
  - Consider physical and logical assets
  - Security goals compromised depend on accidental action and information asset
    - possible to compromise all goals

Threats

- Example: Human action – accidental
  - Optus outage: July 2008
  - Contractor using backhoe to excavate for water grid pipes severed a fibre optic cable in the Optus network
  - At same time, transmission card in backup line was faulty
  - Result:
    - loss of mobile, landline and Internet services for over 4 hours,
    - for more than 1 million Queenslanders who use Optus and networks that lease Optus hardware, including iiNet, 3 Mobile and Virgin
  - Affected organizations included:
    - Hospitals, Medicare,
    - Financial systems (ATMs and EFTPOS systems were affected)
    - Brisbane airport (electronic check-in and baggage handling offline)
    - Public transport systems.

Threats

- Example: Human action – accidental
- Source: http://www.businessinsider.com/cnbc-a-citigroup-trader-made-the-big-fat-finger-error-2010-5

CNBC: A Citigroup Trader Made The Big Fat Finger Error

Joe Weisenthal | May 6, 2010, 4:08 PM | 24,857 | 62

Share Tweet 1 Email A A A

Vikram!

Reports from CNBC and our own sources suggest that it was a Citigroup (C) trader that accidentally entered a sell BILLION-size sell trade, when they meant to do million.

Since the market came back and only ended down over 3%, all the focus now is on what happened. There's going to be an investigation into Proctor & Gamble (PG) trading, Accenture (ACN) and the market as a whole.

In addition to the fat finger error, there will be a lot of talk about high-frequency trading and its affect.

Threats to Privacy

Samsung Television Spies on Viewers

Earlier this week, we learned that Samsung televisions are eavesdropping on their owners. If you have one of their Internet-connected smart TVs, you can turn on a voice command feature that saves you the trouble of finding the remote, pushing buttons and scrolling through menus. But making that feature work requires the television to listen to everything you say. And what you say isn't just processed by the television; it may be forwarded over the Internet for remote processing. It's literally Orwellian.

This discovery surprised people, but it shouldn't have. The things around us are increasingly computerized, and increasingly connected to the Internet. And most of them are listening.

Our smartphones and computers, of course, listen to us when we're making audio and video calls. But the microphones are always there, and there are ways a hacker, government, or clever company can turn those microphones on without our knowledge. Sometimes we turn them on ourselves. If we have an iPhone, the voice-processing system Siri listens to us, but only when we push the iPhone's button. Like Samsung, iPhones with the "Hey Siri" feature enabled listen all the time. So do Android devices with the "OK Google" feature enabled, and so does an Amazon voice-activated system called Echo. Facebook has the ability to turn your smartphone's microphone on when you're using the app.

Even if you don't speak, our computers are paying attention. Gmail "listens" to everything you write, and shows you advertising based on it. It might feel as if you're never alone. Facebook does the same with everything you write on that platform, and even listens to the things you type but don't post. Skype doesn't listen -- we think -- but as *Der Spiegel* notes, data from the service "has been accessible to the NSA's snoops" since 2011.

Outline

- Introduction
- Threats
  - Threat sources
  - Threat types
- Vulnerabilities
- Attacks
  - Passive attacks
  - Active attacks
- Summary

Vulnerabilities

- Weaknesses in a system
  - that could be used to cause harm to information assets
- Need to consider components of information system:
  - Property
  - People
  - Procedures

Vulnerabilities

- Property includes:
  - **Physical assets**: buildings and contents
  - **Hardware**: computer systems, data communications devices, data storage devices
  - **Software**: Operating system, applications
  - **Data**: Files, databases, passwords,
- Consider possible vulnerabilities for each
  - This list is by no means exhaustive, just some of the possibilities…

Vulnerabilities

- Property – physical assets
- Aspects to consider include:
  - Location of information assets
    - In a geographical area that is:
      - Susceptible to natural disaster
      - Near storage of flammable or corrosive materials
      - Close to targets for disruption (may be collateral damage if neighbouring building is target) embassy, military site
      - Easily accessed by outsiders?
  - Physical security mechanisms
    - Fences, walls, locks, gates, partitioning of internal space

Vulnerabilities

- Property – physical assets
- Aspects to consider (continued) include:
  - Maintenance
    - of assets and perimeter protection
  - Monitoring and logging physical access
    - Use of suitable equipment for monitoring access to facilities and environmental conditions
      - Examples:
        - » CCTV, Intrusion Detection/Alarm system,
        - » Fire detection and automatic fire suppression system, etc

Vulnerabilities

- Property – ICT hardware and software
- Aspects to consider include:
  - Reliability and robustness of:
    - Asset
      - Susceptibility to environmental conditions (dust, heat, humidity)
    - Supporting infrastructure
      - Power supply, air conditioning, etc.
  - Redundancy
    - What happens if/when equipment fails?
    - Is there sufficient alternative resources?
      - Uninterruptible Power Supply (UPS),
    - What fail state does equipment revert to? (Open/closed?)

Vulnerabilities

- Property – ICT hardware and software
- Aspects to consider include:
  - Source of software: legitimate, vendor supported?
    - Downloading and installing
  - Testing of software
    - Flaws (bugs) in software
      - Example: common input problems: buffer overflows, injections
    - Need for patching and upgrading
  - Configuration/misconfiguration
  - Unprotected communications channels
    - Wired
    - Wireless

Vulnerabilities

- People – aspects to consider include:
  - Employees:
    - Recruiting staff suitable for the position
      - Failure to check background is common
    - Monitoring access of people to property and processes
      - Disgruntled employees, clients or contractors can be threat source
    - Inadequate education of staff with respect to threats: for example, are staff aware of policies regarding:
      - providing information by email or over phone
      - downloading software,
      - use of mobile devices, etc

Vulnerabilities

- Example: People – recruiting failure

THE AUSTRALIAN NATIONAL AFFAIRS BUSINESS AUSTRALIAN IT HIGHER EDUCATION VIDEO

Breaking News | The Nation | The World | Features | Opinion & Blogs | Galleries | Sport | Health & Science

New Zealand spy agency skipped basic procedures when hiring British fantasist

By staff writers | NewsCore | January 28, 2011 9:12PM

Recommend 15 people recommend this. 0 tweet Share

NEW Zealand's spy agency failed to follow basic procedures when it granted security clearance to a top defence official who turned out to be a fantasist, Prime Minister John Key said today.

British-born Stephen Wilce was recruited in 2005 and appointed as chief defence scientist and director of New Zealand's Defence Technology Agency - after he provided a series of elaborate and extravagant lies about his past during the recruitment process, news website stuff.co.nz reported.

Wilce's false claims and vast exaggerations included that he served as a helicopter pilot with Britain's Prince Andrew, worked for British security services MI5 and MI6, played international rugby for Wales, was on a hit list for Irish terrorist group the IRA and competed against the Jamaican "Cool Runnings" bobsled team in the 1988 Winter Olympics.

Vulnerabilities

- Example: People – recruiting failure:
  - Source: Brisbane Business News - January 2012

EMPLOYERS WARNED: RUN CHECKS OR RISK CRIMINALS

< Previous Next >

By Jason Oxenbridge Jan, 2012

QUEENSLAND companies are leaving themselves open to fraud risk by not performing criminal history checks on their prospective employees, according to a leading recruiter.

In light of the weekend's revelations of a Queensland Health employee allegedly defrauding the State Government of $16 million, it has been revealed that only a fraction of employers conduct police background checks as part of the hiring process.

It is alleged Hohepa Morehu-Barlow had a history of fraud related offences in New Zealand, however his criminal background was not uncovered as checks were not performed.

Related News

RBA UNDER FIRE FOR NOT LOWERING INTEREST RATES
Volume 5, 06-02-2012

THIESS SECURES $325M CSG CONTRACT
Volume 5, 06-02-2012

BATTERY WORLD CHARGED UP
Volume 5, 06-02-2012

LIGHTS OUT FOR SLEEP CITY
Volume 5, 06-02-2012

BRISBANE AGENCY CLEANS UP AT REAL ESTATE 'OSCARS'
Volume 5, 06-02-2012

Vulnerabilities

- People – aspects to consider include:
  - Employees:
    - Are there key personnel critical to organisation?
      - May be unavailable due to accident or illness, or other event (transport failure, natural disaster)
    - Vulnerable if no back-up for these people
      - If procedures are undocumented
  - Others:
    - Are security conditions included in contracts with consultants, contractors, outsourcing?

Vulnerabilities

- Processes – aspects to consider include:
  - Access control and privilege management
    - Including keys, cards, passwords
  - Backup of files and systems
  - Business continuity plans
    - for recovery of information assets after disaster
  - Communications
    - Policy for acceptable use of communications
    - Example: confirmation for sending/receiving messages

Vulnerabilities

- Processes – aspects to consider include:
  - Checks and balances:
    - People make mistakes: are there processes to detect, correct or reduce the impact of errors?
      - Example: Separation of duties
  - Processes associated with staff joining/leaving organisation
    - Clear statement of duties
    - Nondisclosure/confidentiality agreements
  - Software management processes and auditing

Outline

- Introduction
- Threats
  - Threat sources
  - Threat types
- Vulnerabilities
- Attacks
  - Passive attacks
  - Active attacks
- Summary

Attacks

- Attacks:
  - occur when vulnerabilities are deliberately exploited
- Attacker:
  - person who deliberately attempts to exploit a vulnerability to
    - gain unauthorized access, or
    - perform unauthorized actions

Attacks

- Attack Types:
  - Passive
    - Attacker's goal is to obtain information
    - Attacker does not alter information system resources
      - No interaction by the attacker other than listening or observing
    - Difficult to detect; usually try to prevent the attack.
  - Active
    - Attacker's goal may be to obtain, modify, replicate or fabricate information
    - Requires some action or interaction with the information system by the attacker
    - Usual approach is to try detect attackers actions, recognise them as signs of attack and recover

Passive Attacks

- Eavesdropping:
  - Listening to the conversations of others without their knowledge or consent
  - Wiretapping
    - Eavesdropping over telephone network
    - May be harder to detect in wireless network
  - Information can be obtained from:
    - the content of the conversations, and
    - knowing who is talking to who and when (traffic analysis)

Passive Attacks

- Shoulder surfing
  - Watching the actions of others (especially at data entry) without their knowledge or consent
  - Usually connected with entry of confidential information
    - PIN (for financial access at ATM)
    - Security code or password
  - Can also be for greater amounts of data
    - Use of mobile devices in insecure surroundings is vulnerability that can be exploited for this attack

Passive Attacks

- Network monitoring and eavesdropping
  - A packet sniffer or network analyzer can monitor network traffic
    - can be used for network maintenance (finding faults and traffic problems)
    - But can also be used to gain knowledge of confidential information
    - e.g passwords corresponding to user names
  - Confidential information should not be sent over untrusted networks without protection
    - Example: when logging on to a remote resource, passwords should not be sent ‘in the clear’

Active Attacks

- Denial of Service (DoS) Attack
  - Objective is to make an information asset or resource unavailable to authorized users
  - Common methods are:
    - To overload the resource, so it cannot respond to legitimate requests
    - To damage the resource, so that it can not be used
    - To deliberately interrupt communications between users and resource, so that it can not be accessed

Active Attacks

- Distributed Denial of Service (DDoS) Attack
  - Objective is same as DoS attack:
    - Breaches availability of information asset
  - Method:
    - Use multiple sources to make resource requests
    - Hope to overload resource, so it cannot respond to legitimate requests
    - Malware (e.g.virus) may be used to compromise many machines
      - all have same target, and payload is activated at same time, to make simultaneous resource request

Active Attacks

- Example: Denial of Service (DoS) Attack
- DoS and DDoS commonly applied to websites:
  - November 2010 ‘Wikileaks’ website unavailable for several hours
  - December 2010 ‘Anonymous’ retaliation - launched DDoS attacks against Mastercard, Visa and Amazon with varying levels of success
  - Many DDoS Attacks by Anonymous in last few years
    - Including Jan 2012 Attacks in retaliation for Megaupload shut down
- Can also be applied to telecommunications (TDoS)
  - May be used to prevent verification by phone of other actions (linked to other attacks)

Active Attacks

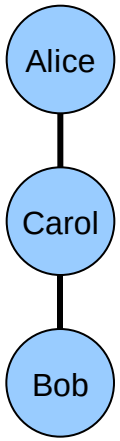
- Masquerade/Spoofing:
  - Where one entity pretends to be another in order to deceive others
- Common spoofing attacks include:
  - Email address spoofing
    - Altering the sender information on email to trick recipients into thinking the message is from another source
  - Webpage spoofing
    - Creating a fake webpage that looks like the page for a legitimate business to trick users
      - into giving the credentials they would use at legitimate site
      - Into downloading materials from an alternative site

Active Attacks

- Phishing:
  - Attempts to gain credentials to enable access to other resources by masquerading as a legitimate organisation (Bank, eBay, PayPal)
    - Example: account details, PIN number, password
  - Usually involves
    - spoofed emails and/or spoofed web pages
    - social engineering

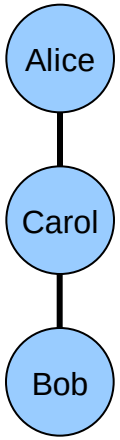
Active Attacks

- Man-in-the-Middle Attack (MITM)
  - An attacker (Carol) positions herself between two entities who wish to communicate, say Alice and Bob.
  - Carol pretends to Alice she is Bob, and pretends to Bob she is Alice (spoofing).



Active Attacks

- Man-in-the-Middle Attack (MITM)
  - Alice and Bob think they are communicating with each other.
  - However, all messages between them go via Carol, so Carol can control the conversation
    - Could just monitor conversation (breach confidentiality)
    - Can also insert or modify information (breach integrity)



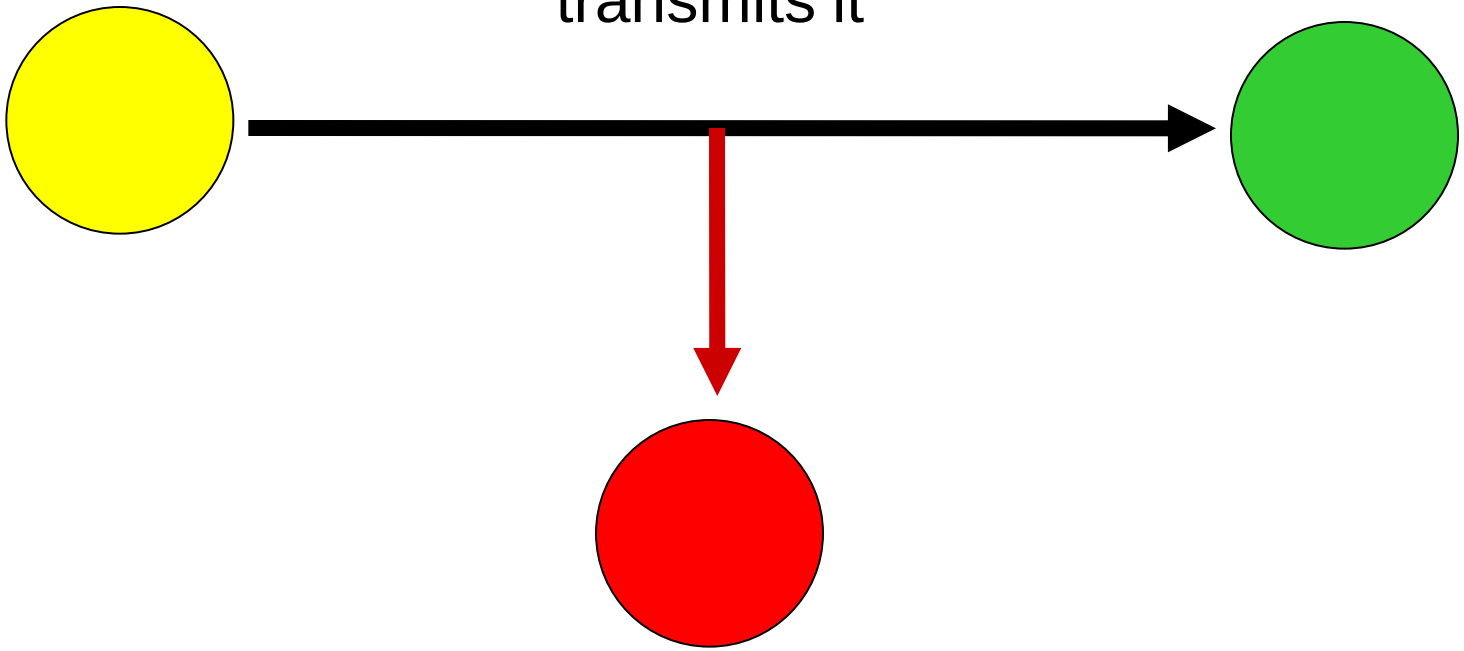
Normal information flow

Information Source (Alice)

Information Destination (Bob)

Interception

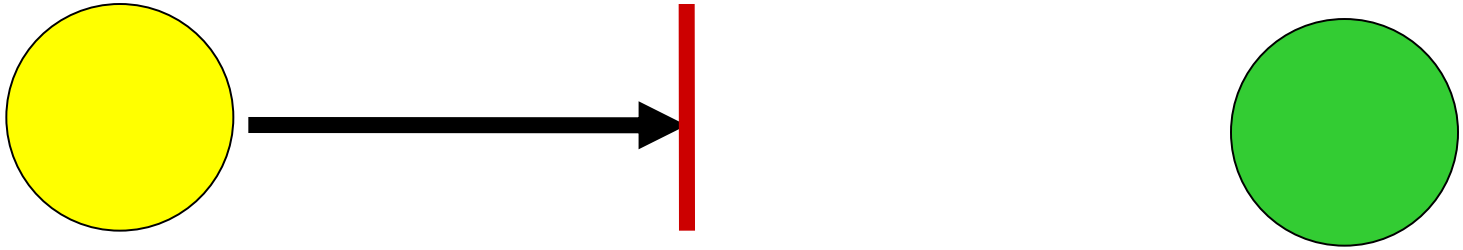
The unauthorized MITM observes the information and transmits it



Breaches confidentiality

Interruption

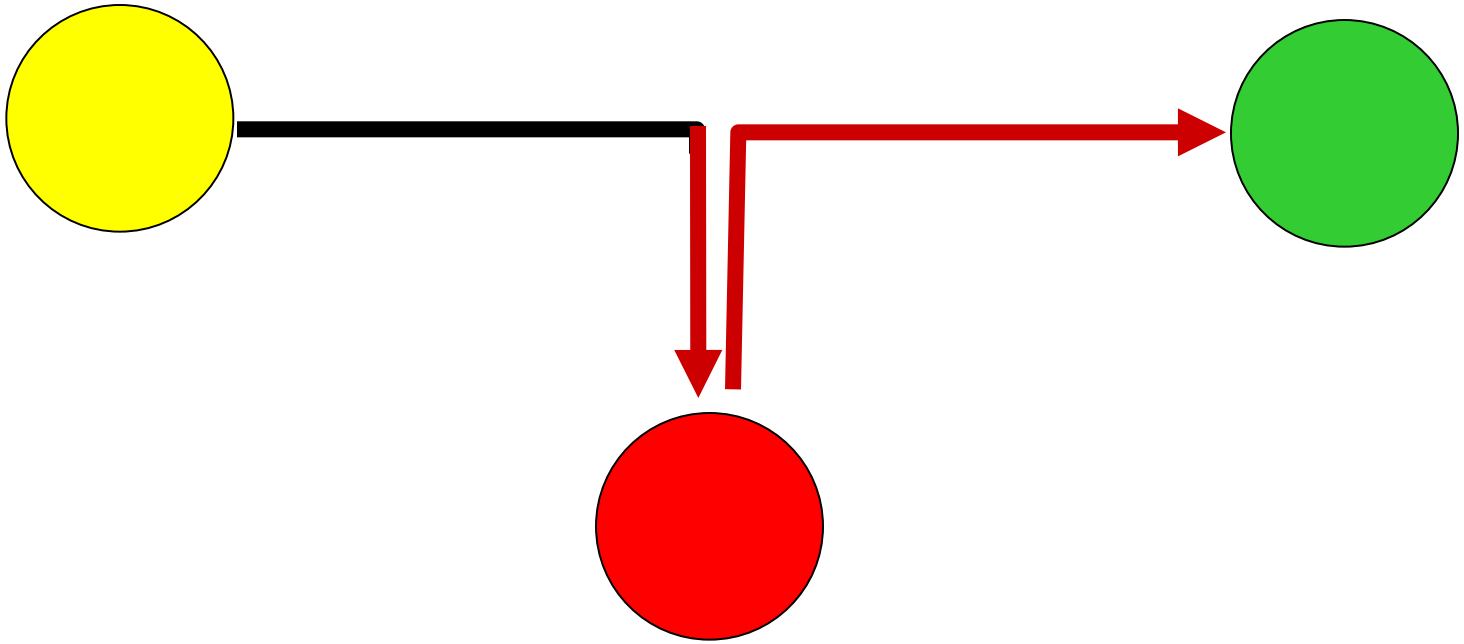
The unauthorized MITM prevents transmission, so information assets are unavailable to Bob



Breaches availability

Modification

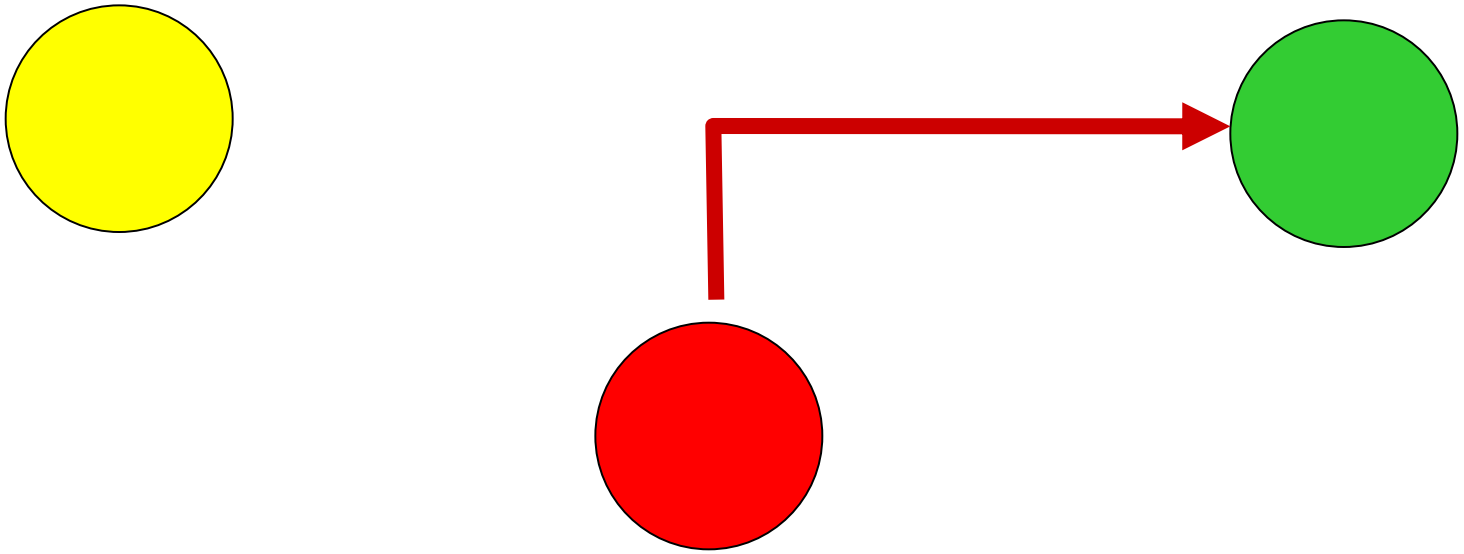
The MITM modifies the information and then sends to Bob



Breaches integrity

Fabrication

The MITM creates information asset and sends to Bob but claims it is from Alice



Breaches authenticity

Active Attacks

- Social Engineering:
  - Using social skills to convince people to reveal information or permit access to resources
  - Examples:
    - Claim to be new employee, manager's assistant, maintenance person, etc and ask for assistance in accessing resource to complete an urgent task:
      - I've lost my password and I have to finish this today …
      - My swipe card doesn't work/left at home …
    - Tailgating – follow another person closely so that when they go into secure area you can also get in without providing appropriate credentials

Active Attacks

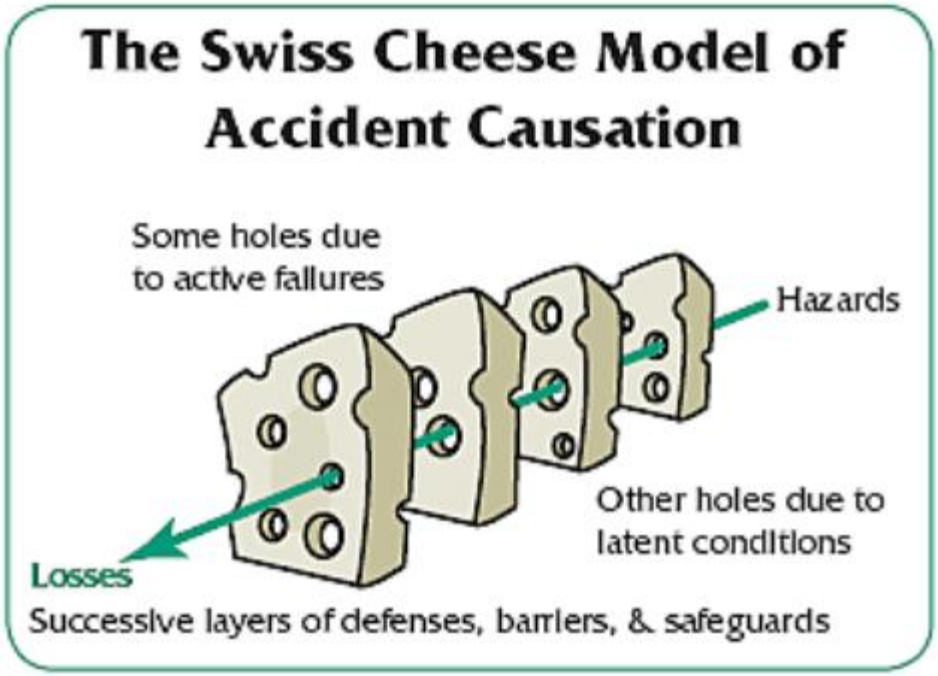
- Replay attack:
  - This is where a valid data transmission is recorded, and retransmitted at a later date
  - Example:
    - Access to a system requires use of password, but password is encrypted during transmission
    - Attacker records encrypted password, and replays this information in order to gain access
    - Doesn’t matter that attacker doesn’t know the password – they could provide the expected credential on request.

Outline

- Introduction
- Threats
  - Threat sources
  - Threat classes
  - Examples
- Vulnerabilities
- Attacks
  - Passive attacks
  - Active attacks
- Summary

Putting it all together

- When threats interact with vulnerabilities, information assets can be harmed
- Similar to Reason's model for accident causation:



Summary

- When threats and vulnerabilities coincide, security incidents occur
  - If the threat involves deliberate human action, then incident is referred to as an attack
  - Even if threat is not deliberate, the damage from the security incident can still be extensive
- Providing effective security for information assets requires understanding threats and vulnerabilities
  - so that appropriate security measures can be used

ANY QUESTIONS??

Lab Setup

- Linux Server
- Windows Server
- Linux and Windows Clients (Dual Booted)

Lets have a walk…

Security Tools

Applications

- Network Reconnaissance
- Password Cracking
- Encryption
- Data Hiding
- Forensics

Eg: -Wireshark, nmap, Nessus, John The Ripper, Cryptool, Stegag and many more

Security Tools

Frameworks

- Metasploit – (Armitage GUI)
  - Very Popular
  - Free and Commercial Version ($15,000 per year)
- Core Impact
  - Very Powerful
  - Expensive ($30,000 per year)
- Canvas
  - Good
  - Only Commercial version less expensive

Security Tools

Operating Systems

Kali Linux – used to be BackTrack

- Advanced Penetration Testing OS
- Included numerous Hacking or Penetration Testing tools
- Can be installed on Mobile Devices
- Free

More Features: https://www.kali.org/kali-linux-features/

Cool Websites

News Websites

- theregister.co.uk
- Wired
- Naked security

Resourceful Website

- Owasp.org
- sectools.org