

A background pattern of a network diagram consisting of various sized grey circles (nodes) connected by thin grey lines (edges). The nodes are scattered across the white background, creating a complex, interconnected web-like structure.

NETWORK SECURITY

PREVALENT SECURITY PROBLEMS

PHISHING

Masquerading as a well-known site such as a bank to obtain a user's personal information, typically an account number and access code

PHISHING


From Professor Bjarne Graabech Sørensen(via The Conference Alerts) <no-reply@theconferencealerts.com> ☆
Subject **Professor Bjarne Graabech Sørensen's invitation is waiting for your response** 10/28/18, 4:34 AM
To Me <jamik@imada.sdu.dk> ★

The Conference Alerts

[Professor Bjarne Graabech Sørensen](#) invites you to connect in The Conference Alerts.

Join to [The Conference Alerts](#) and get notifications for upcoming conferences.

[Accept](#)

 **Professor Bjarne Graabech Sørensen**
Professor And Pro-Rector, University Of Southern Denmark
[University of Southern Denmark](#)

PHISHING

*Beware of fraudulent emails! A number of SDU email addresses received an email in which our Pro-Vice Chancellor ostensibly invited staff to join a conference alert system. This was a phishing email. According to IT-service, **48 out of the 80** recipients of the email at IMADA on the link and registered for a profile in the system. It is not known how many used their SDU password for this...*

from his newsletter to IMADA Employees
— Martin Svensson

MISREPRESENTATION

Making false or exaggerated claims about goods or services, or delivering fake or inferior products

MISREPRESENTATION



Ophavsretlig krænkelse af rettighederne til And So It Goes

Som advokat for Scanbox Entertainment A/S, der har eksklusiv distributionsret over den ophavsretligt beskyttede film "**And So It Goes**" ("Filmen") i blandt andet Danmark, skal jeg hermed rette henvendelse til dig, idet min klient har konstateret en ulovlig kopiering af Filmen via en IP-adresse.

Faktuelle omstændigheder

IP-adressen [REDACTED] har været aktiv i et BitTorrent-netværk (herefter benævnt "BitTorrent-netværket") den [REDACTED] 2015 kl. [REDACTED] hvor det er konstateret, at den pågældende IP-adresse har downloadet og delt Filmen uden min klients samtykke.

SCAMS

Various forms of trickery intended to deceive naive users into investing money or abetting a crime

SCAMS

From Richard K. <oficina@multimarcas.cl> ☆ Reply Forward Archive Junk Delete More ▾

Subject **Tomorrow you can get a rich man!** 2017-10-30 12:46

To Me <jacob.mikkelsen@roskilde-festival.dk> ☆

Yesterday I made a crazy deal to buy a new house with garden and swimming pool. Now I'm just sitting in cafes and drinking flavored lattes with the idea that it is unfair to hide the happiness from the world.

So [I share this link with you and a few randomly selected people](#) me, as once shared with me my German friend.

The incredible achievement of scientists from Germany, the program, which making successful trades in the exchange market, it has changed the lives of people like me forever.

As long as man is prone to impulsive decisions and makes errors in anticipation of profit, BankBot operates on the market based on thorough market analysis. It does everything for you, you're just enjoying the growth of your income. If it's not a miracle, what is it?

DENIAL OF SERVICE

Intentionally blocking a particular internet site to prevent or hinder business activities and commerce

LOSS OF CONTROL

An intruder gains control of a user's computer and uses the computer to perpetrate a crime

LOSS OF DATA

Loss of intellectual property or other valuable proprietary business information

LOSS OF DATA



Equifax says data breach may have exposed personal info of 143 million consumers

September 9, 2017 *by: Alex Thomas Sadler*

Equifax, one of the nation's three main credit reporting agencies, has announced a "cybersecurity incident" that could potentially impact roughly...

TECHNIQUES USED IN SECURITY ATTACKS

WIRETAPPING

Making a copy of packets as they traverse a network to obtain information



REPLAY

Sending packets captured from a previous session (e.g. sending a password packet from a previous login)

BUFFER OVERFLOW

Sending more data than a receiver expects in order to store values in variables beyond the buffer



ADDRESS AND NAME SPOOFING

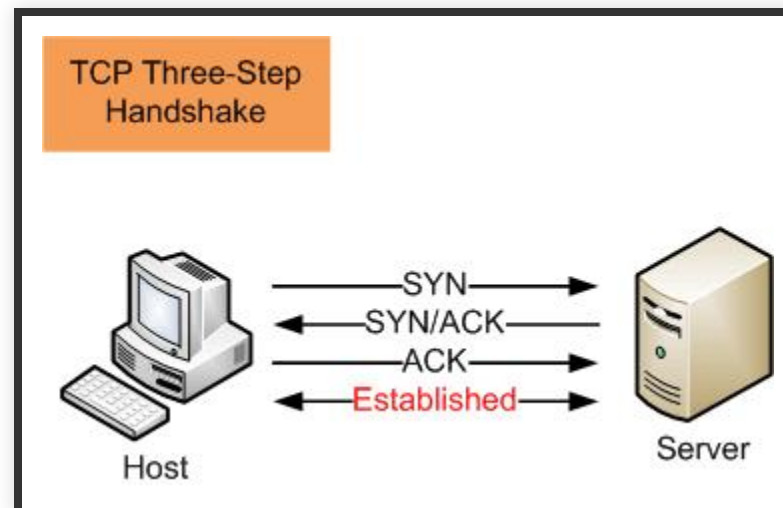
Fake the source IP address in a packet to trick a receiver into processing the packet

DOS AND DDOS

Flooding a site with packets to prevent the site from successfully conducting normal business

SYN FLOOD

Sending a stream of random TCP SYN segments to exhaust a receiver's set of TCP connections



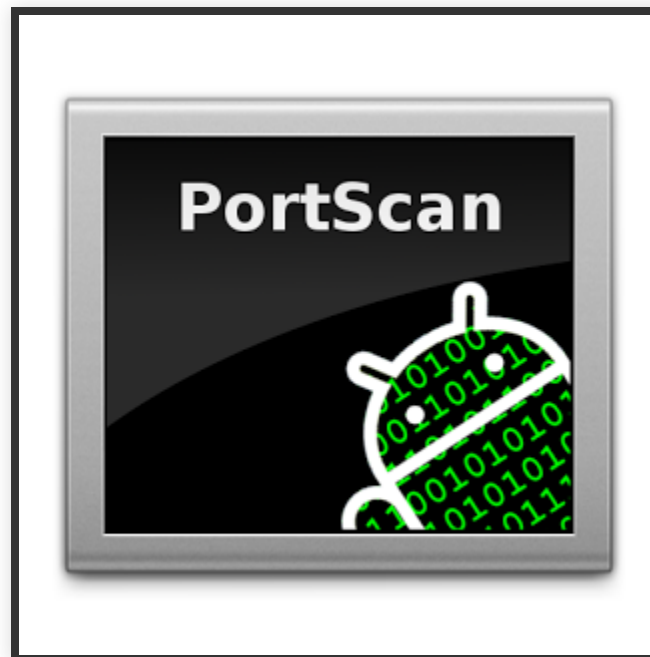
PASSWORD BREAKING

Automated systems that guess a password or a decryption key or to gain unauthorized access



PORT SCANNING

Attempting to connect to each possible protocol port on a host to find a vulnerability



PACKET INTERCEPTION

Removing a packet from the internet which allows substitution and man-in-the-middle attacks

SECURITY POLICY

Devising a network security policy can be complex because a rational policy requires an organization to relate network and computer security to human behavior and to assess the value of information

SECURITY POLICY

- **Data integrity** - Is the data that arrives identical to the data sent?
- **Data availability** - Does the data remain accessible for legitimate users?
- **Data Confidentiality** - Is data protected against unauthorized access?
- **Privacy** - Is the senders' identity revealed?

TECHNIQUES (1)

Technique	Purpose
Hashing	Data integrity
Encryption	Privacy
Digital Signatures	Message Authentication
Digital Certificates	Sender authentication

TECHNIQUES (2)

Technique	Purpose
Firewalls	Site integrity
Intrusion Detection Systems	Site integrity
Virtual Private Networks (VPN)	Data confidentiality

BEST PRACTICES

SECURITY PLANNING

- Security Team/Responsible when planning larger feature
- Ensure security features are added to user stories

DEFENCE

- Multiple layers are sometimes necessary
 - Firewalls
 - Updated OS/Frameworks etc.
 - Good programming practices



Adds more friction for attackers

UPDATE SOFTWARE

💡 Make sure all software, frameworks and technologies are updated.

- Newer versions get the most attention
- Patches more often in new version

USE HARD PASSWORDS

- Reset when someone leaves

INSTALLATION

💡 Principle of least privilege

- Employee termination
- Mistakes
- Vulnerabilities
- Don't install redundant software

SECRETS



Never hardcode secrets in source code

- Config file
- Keep it secure/restrict access
- Templating when deploying

INPUT VALIDATION

 Never trust user input

- Clean up on first entry

ERROR HANDLING



Don't show stacktraces etc

- Least information disclosure
- Make a token and save stacktrace (if needed for debug)

LOGGING

- Important to identify threats
 - Look for unusual patterns in your logs

QUESTIONS