İTÜ

BLG113E

Cyber Security

Dr. Şerif Bahtiyar

bahtiyars@itu.edu.tr

Motivation

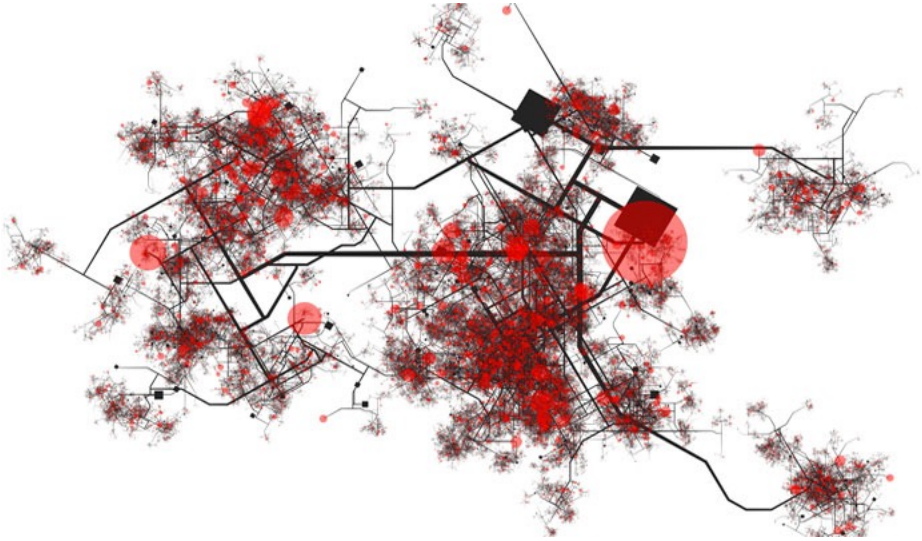
Zoom boss apologises for security issues and promises fixes

Zoom is to pause the development of any new features to concentrate on safety and privacy issues, in the wake of criticism from users of the app ….

https://www.bbc.com/news/technology-52133349

Motivation

COVID-19 Contact Tracing Apps Spotlight Privacy, Security Rights



As tech giants like Microsoft, Google, and Apple move to craft the APIs behind COVID-19 contact tracing apps, privacy advocates rush to ensure the protection of privacy and cybersecurity rights ….

https://healthitsecurity.com/news/covid-19-contact-tracing-apps-spotlight-privacy-security-rights

Motivation

UK, US warn of state-backed coronavirus hacks

Hackers attempting to steal intelligence on Western responses to coronavirus, including vaccines, say cyber security bodies ….

https://www.aa.com.tr/en/europe/uk-us-warn-of-state-backed-coronavirus-hacks/1830102

Motivation

Yahoo 'state' hackers stole data from 500 million users

http://www.bbc.com/news/world-us-canada-37447016

Motivation

Could a hacker hijack your connected car?

In 2015, 15% of car recalls in the US were related to software errors, up from 5% four years before.

Hackers showed two years ago that they could remotely take control of a Chrysler Jeep.

http://www.bbc.com/news/business-41367214

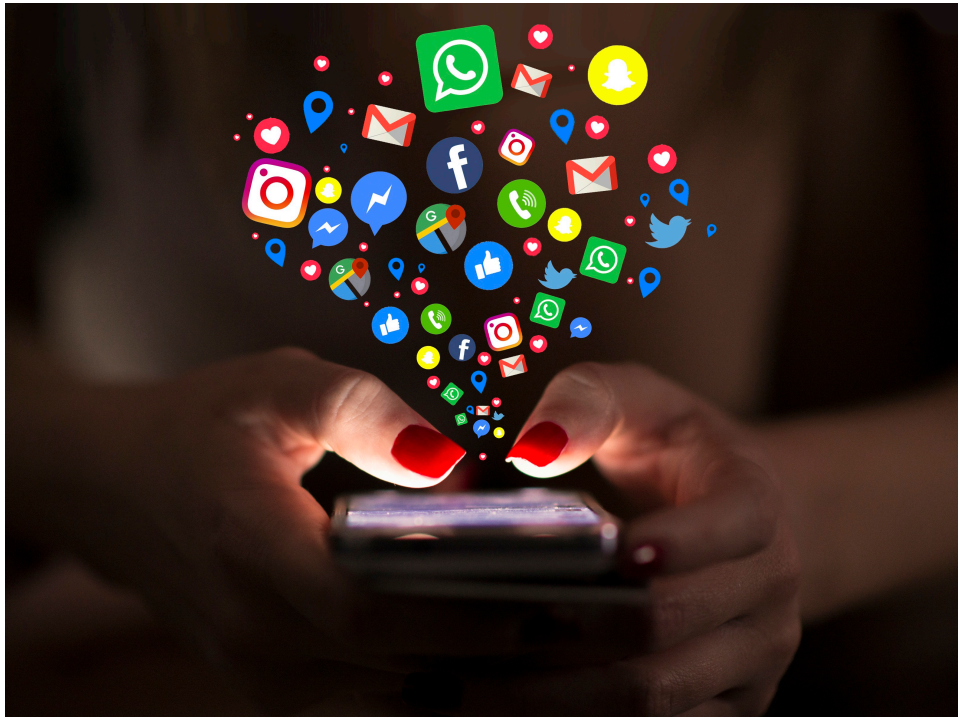
Motivation

Russian Hacking Attacks Could ‘Flood Us Cities With Sewage’ And Cause Deadly Explosions

https://www.independent.co.uk/life-style/gadgets-and-tech/news/russian-hacking-attacks-us-power-grid-sewage-explosions-a8462691.html

Motivation

Stalkerware: The software that spies on your partner



Amy says it all started when her husband seemed to know intimate details about her friends.

https://www.bbc.com/news/technology-50166147

Before Starting

Elon Musk quits AI ethics research group

Technology billionaire Elon Musk has quit the board of the research group he co-founded to look into the ethics of artificial intelligence.

http://www.bbc.com/news/43154732

Before Starting

Barclays scraps 'Big Brother' staff tracking system

Barclays says it has scrapped a system that tracked the time employees spent at their desks and sent warnings to those spending too long on breaks.

https://www.bbc.com/news/business-51570401

Motivation

Security vulnerabilities and attacks

Item	2014 Cost
1,000 Stolen Email Addresses	$0.50 to $10
Credit Card Details	$0.50 to $20
Scans of Real Passports	$1 to $2
Stolen Gaming Accounts	$10 to $15
Custom Malware	$12 to $3500
1,000 Social Network Followers	$2 to $12
Stolen Cloud Accounts	$7 to $8
1 Million Verified Email Spam Mail-outs	$70 to $150
Registered and Activated Russian Mobile Phone SIM Card	$100

Value of Information Sold on Black Market

Economic losses

We need secure systems!

What security is about in real world?

Protection of assets

What security is about in real world?

How?

Prevention: prevent your assets from being damaged or stolen, such as hire a guard

What security is about in real world?

How?

Detection: detect when, how, and by whom an asset has been damaged, such as alarms

What security is about in real world?

How?

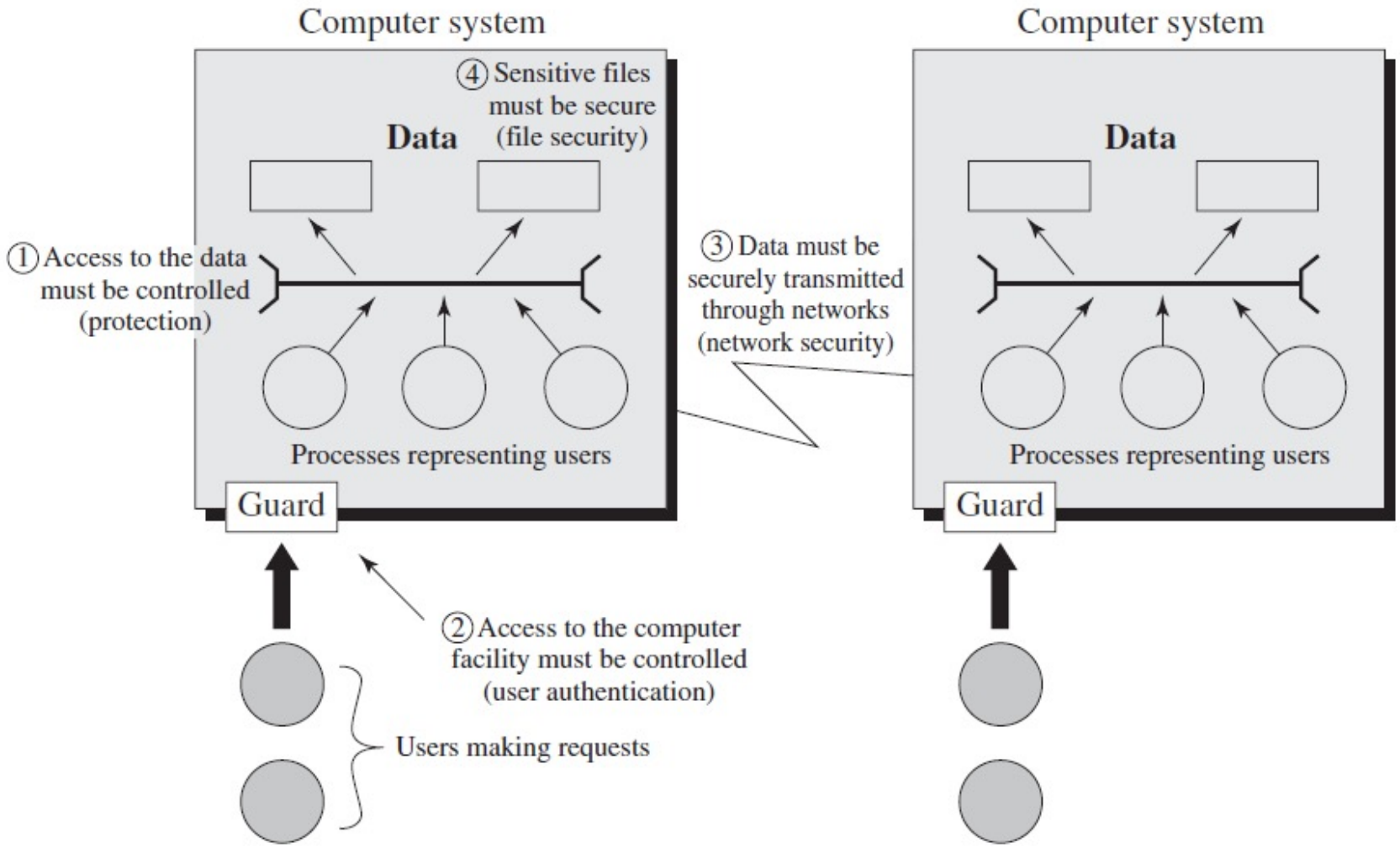
Reaction: recover your assets, such as call police or make an insurace claim.

What is computer security?

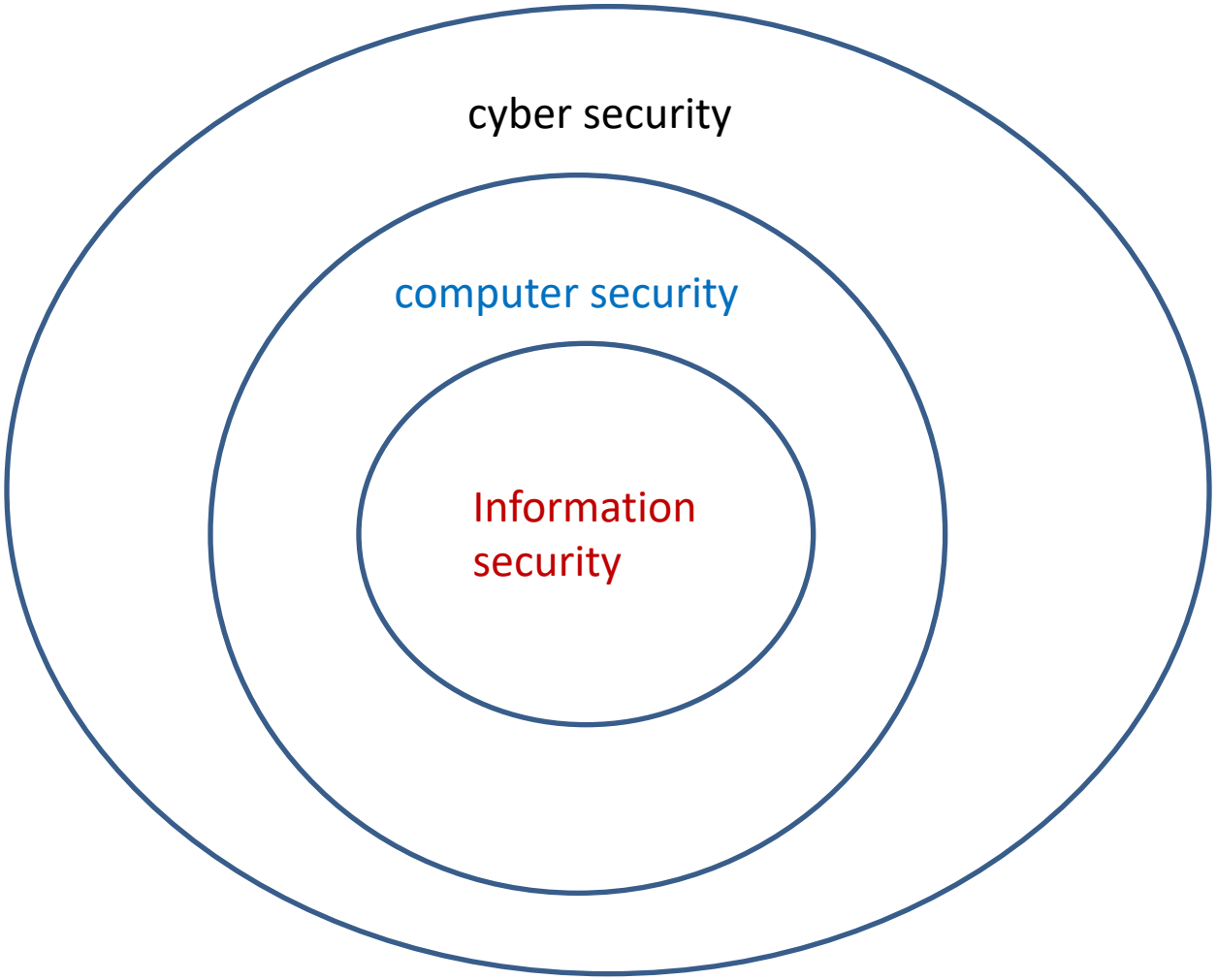
- It deals with computer related assets that are subject to a variety of threats and for which various measures are taken to protect those assets. (Stallings and Brown)

- The protection afforded to an automated information system in order to attain the applicable objectives of preventing the integrity, availability, and confidentiality of information system resources. (NIST Computer Security Handbook)

What is computer security?

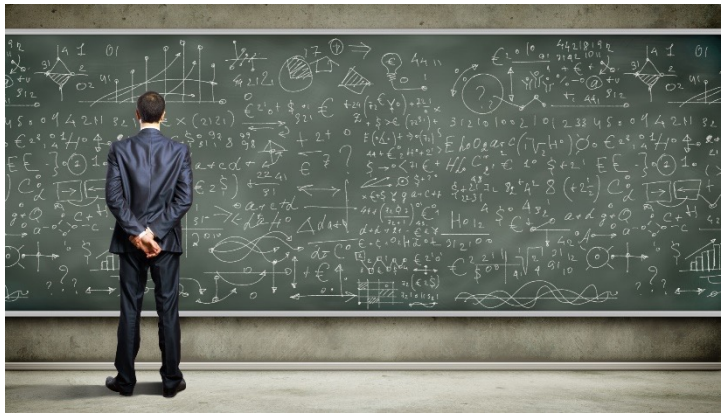


Cyber Security



Assets

- Hardware
- Software
- Data



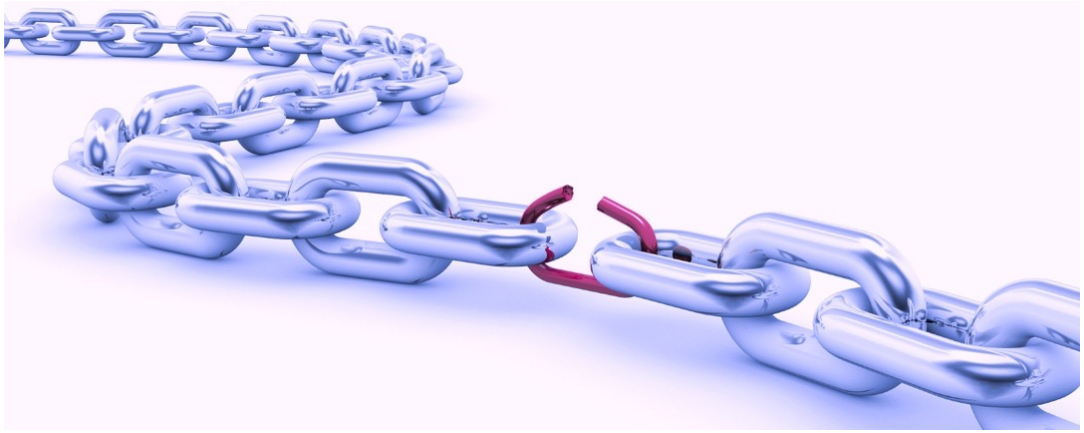
- Communication lines and networks

Threat

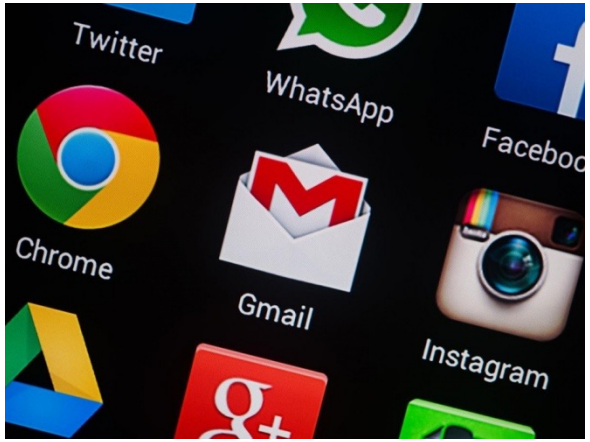
- A potential for violating security.
- A threat is a possible danger that might exploit a vulnerability.

Vulnerability

A flaw or weakness in a system's design, implementation, or management that could be exploited to violate the system's security policy.



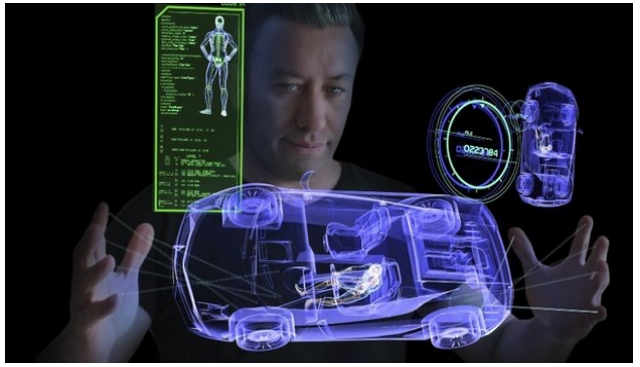
Attacks



- Destroy information
- Steal information

- Blocking to operate properly (denial of service)
- Physical damage
  - Hi-tech cars are security risk, warn researchers

(http://www.bbc.com/news/technology-28886463)



Countermeasure

An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack.

How?

- Eliminating or preventing
- Minimizing the harm
- Discovering and reporting

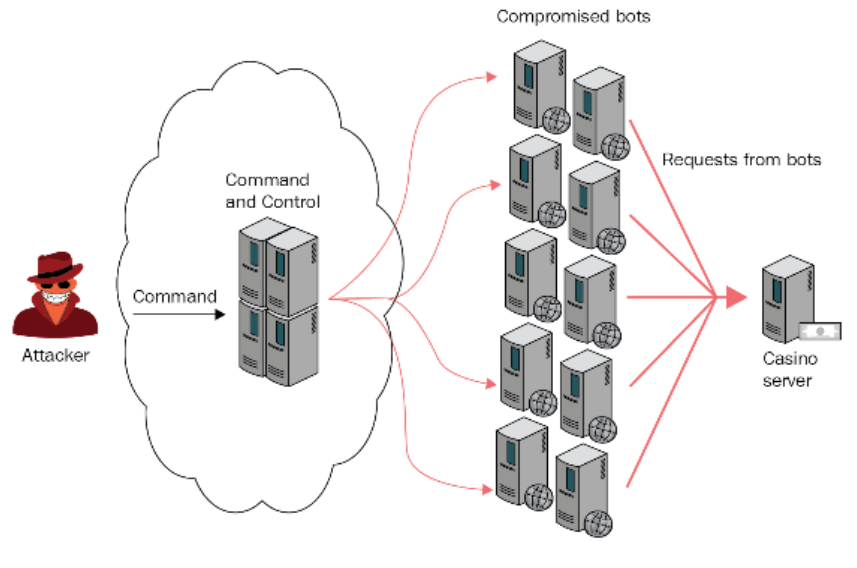
- Thus: corrective action can be taken.

Some Security Courses

- Computer Security
- Cryptography
- Network Security
- Software Security
- Secure Programming
- Security and Privacy
- Security in Financial Information Systems
- **Hacking**
- More….

Research

Machine Learning and Security



Attack detection/prediction/defense applications

- DOS/DDOS attacks
- XSS attacks
- Targeted attacks
- Attacks on connected vehicles
- Attacks on Unmanned Aerial Vehicle (UAV)
-

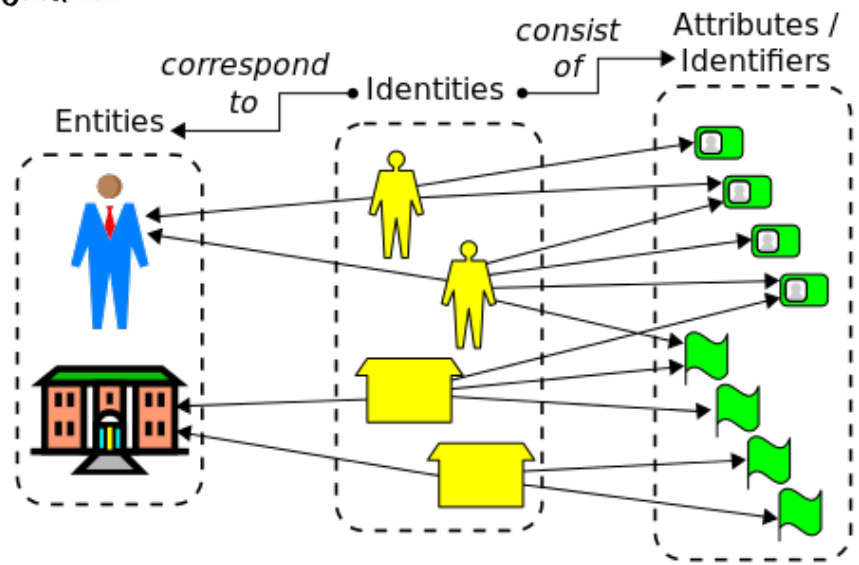
Malware Analysis and Detection

- Virus
- Trojan
- Spyware
- Ransomware
- Rootkit
- Botnet
- Worm
- …

```
push    offset aGlobalMswinzon ; "Global\\MsWinZonesCacheCounterMutexA"
lea     eax, [ebp+Dest]
push    offset aSD             ; The sprintf format "%s%d" appends a "0" to the end of the mutex name
push    eax                    ; Dest
call    ds:sprintf             ; Global\\MsWinZonesCacheCounterMutexA0
xor     esi, esi
add     esp, 10h
cmp     [ebp+arg_0], esi
jle     short loc_401F4C

                               ; CODE XREF: check_mutex+4B↓j
lea     eax, [ebp+Dest]
push    eax                    ; lpName
push    1                      ; bInheritHandle
push    100000h                ; dwDesiredAccess
call    ds:OpenMutexA          ; Check for existence of mutex
test    eax, eax
jnz     short loc_401F51 ; If this mutex exists, the malware exits
push    1000                   ; dwMilliseconds
call    ds:Sleep
inc     esi                    ; Increment the counter
cmp     esi, [ebp+arg_0] ; Compares the incrementer to the value 60, effectively
                               ; performing this mutex check each second for one minute
jl      short loc_401F26
```

Trust, Privacy, and Identity Management



More on Research

https://web.itu.edu.tr/bahtiyars/SB-Research.html

Questions