INFORMATION SECURITY

"Aut viam inveniam aut faciam"
Hannibal Barca

SCOPE – SECURITY PRO

- Almost all the major / critical networks like:
  - Defense,
  - Communication,
  - Financial,
  - Infra networks, (Power Grids,)
  - anywhere & everywhere....

Cybersecurity Skills Crisis

Too Many Threats

62% INCREASE IN BREACHES **IN 2013**[1]

1 IN 5 ORGANIZATIONS HAVE **EXPERIENCED AN APT ATTACK**[4]

US **$3 TRILLION** TOTAL GLOBAL IMPACT OF **CYBERCRIME**[3]

8 MONTHS IS THE AVERAGE TIME **AN ADVANCED THREAT GOES UNNOTICED** ON VICTIM'S NETWORK[2]

2.5 BILLION **EXPOSED RECORDS** AS A RESULT OF A DATA BREACH IN THE PAST 5 YEARS[5]

Too Few Professionals

62% OF ORGANIZATIONS **HAVE NOT INCREASED SECURITY TRAINING IN 2014**[6]

1 OUT OF 3 SECURITY PROS ARE **NOT FAMILIAR WITH ADVANCED PERSISTENT THREATS**[7]

<2.4% **GRADUATING STUDENTS HOLD COMPUTER SCIENCE DEGREES**[8]

1 MILLION UNFILLED SECURITY JOBS WORLDWIDE[9]

83% **OF ENTERPRISES** CURRENTLY LACK THE RIGHT SKILLS AND HUMAN RESOURCES TO PROTECT THEIR IT ASSETS[10]

Enterprises are under siege from **a rising volume of cyberattacks.**

At the same time, the global demand for skilled professionals sharply outpaces supply. Unless this gap is closed, organizations will continue to face major risk. Comprehensive educational and networking resources are required to meet the needs of everyone from entry-level practitioners to seasoned professionals.

SOURCES: 1. *Increased Cyber Security Can Save Global Economy Trillions*, McKinsey/World Economic Forum, January 2014; **2.** *M-Trends 2013: Attack the Security Gap*, Mandiant, March 2013; **3.** *Increased Cyber Security Can Save Global Economy Trillions*, McKinsey/World Economic Forum, January 2014; **4.** *ISACA's 2014 APT Study*, ISACA, April 2014; **5.** *Increased Cyber Security Can Save Global Economy Trillions*, McKinsey/World Economic Forum, January 2014; **6.** *ISACA's 2014 APT Study*, ISACA, April 2013; **7.** *ISACA's 2014 APT Study*, ISACA, April 2014; **8.** *Code.org*, February 2014; **9.** *2014 Cisco Annual Security Report*; **10.** *Cybersecurity Skills Haves and Have Nots*, ESG, March 2014

CSX CYBERSECURITY NEXUS

ISACA® Trust in, and value from, information systems

THE MONEY FACTOR

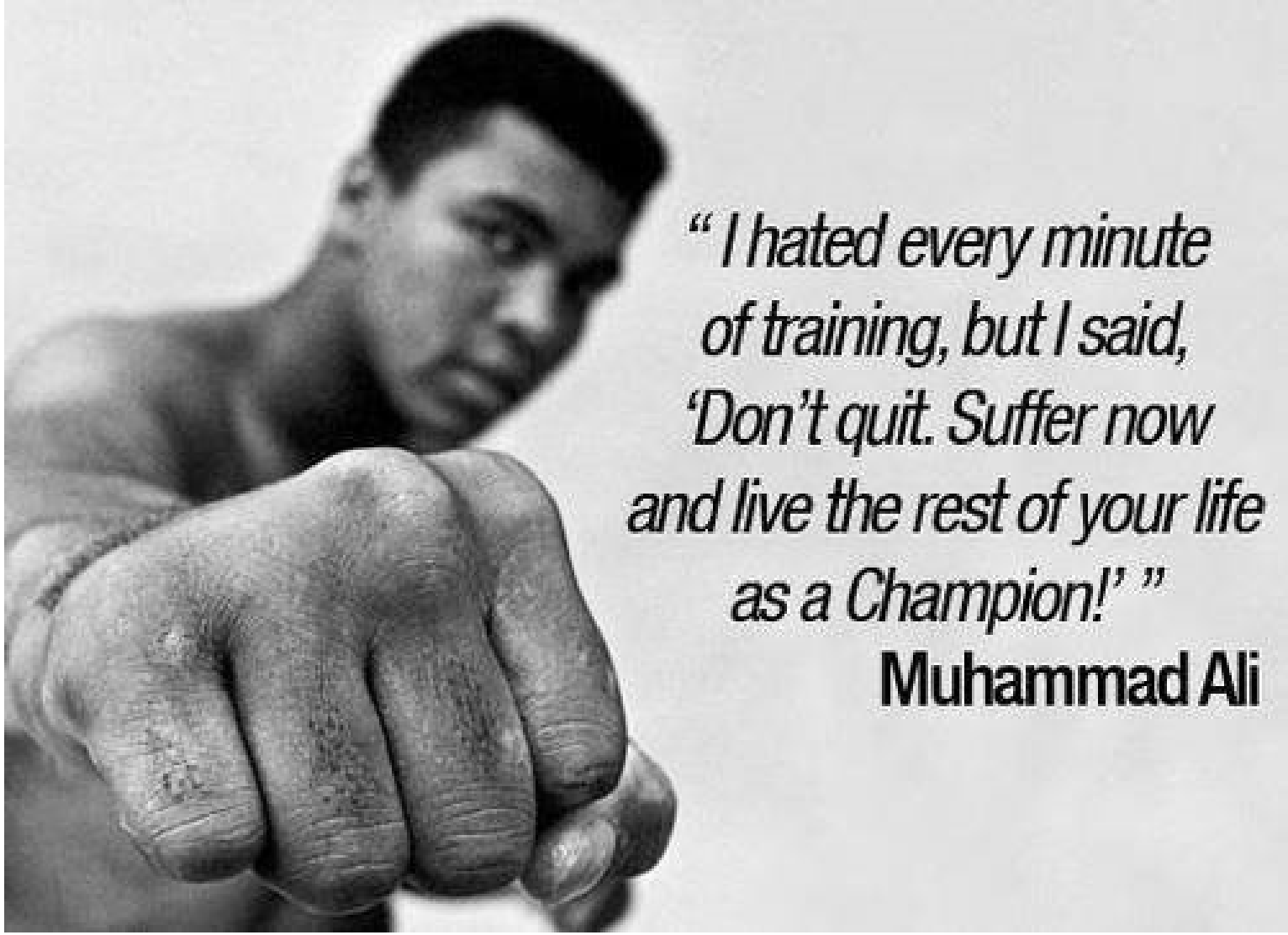
FINANCIALS – SKILLED "PRO"

- Average hourly rate – $40 – $60
- Skilled Security Pro's – $100 – $120 - $150
- 100 X 8 hrs = 800
- 800 X 5 days = 4000
- 4000 X 4 weeks = 16,000
- $ 16,000 to INR (Rs 60) = 9,60,000/-

CHALLENGES – GETTING INTO INFOSEC

- It’s challenging
- You need to have the “stuff”
- Responsibility
- Integrity
- Very vast domain.
- Consistency / Persistence

REMEMBER


" I hated every minute
of training, but I said,
'Don't quit. Suffer now
and live the rest of your life
as a Champion!' "
Muhammad Ali

SOME STATISTICS

INTERNET – THE BIG PICTURE

World wide internet usage

2008 - 694 Million

2010 - 1.97 Billion

2011 - 6,930,055,154 (6.93 Billion)

2012 - 7,017,846,922 (7.01 Billion)

2013 - 7,181,858,619 (7.18 Billion)

LIVE STATS

- http://www.internetlivestats.com/
- http://www.internetlivestats.com/watch/internet-users/

EMAIL STATISTICS - 2010

- 107 trillion – Emails sent on the Internet
- 294 billion – Average # of email per day.
- 1.88 billion – # of email users worldwide.
- **89.1%** – The share of emails that were **spam**.
- 262 billion – The number of spam emails per day

THE INTERNET

- www – ~~World Wide Web~~
- www – wild wild west

POSSIBILITIES?

So what are the possibilities when you get connected to the internet?

POSSIBILITIES?

- The 7.01 Billion users (or the Internet Population) can communicate with your system,

or

- Your system can communicate with 7.01 Billion users (or the Internet Population) .

POSSIBILITIES?

- Out of the 7.01 Billion users, some can rattle your computer to see if it is locked or not
  - locked – Its fine
  - not locked – not fine

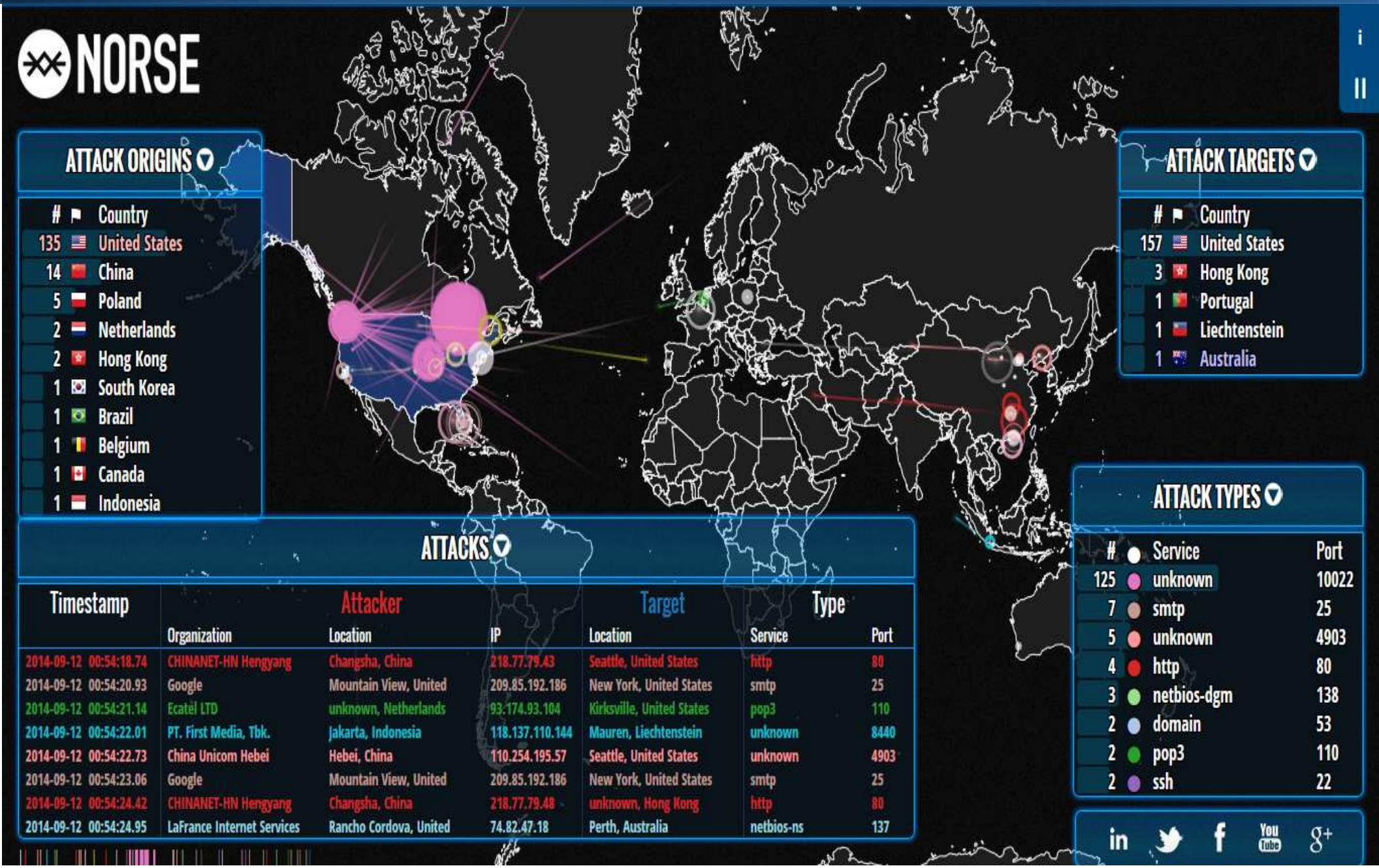
MALICIOUS TRAFFIC VISUALIZATION

- http://map.norsecorp.com/#/
- http://threatmap.fortiguard.com/
- https://cybermap.kaspersky.com/
- https://www.checkpoint.com/ThreatPortal/livemap.html

MALICIOUS TRAFFIC VISUALIZATION

- https://www.fireeye.com/cyber-map/threat-map.html
- https://www.akamai.com/us/en/solutions/intelligent-platform/visualizing-akamai/real-time-web-monitor.jsp

REAL TIME ATTACK STATISTICS



INFORMATION SECURITY

TRADITIONAL SECURITY DEFENITION

- **Protecting** the resources under the lock and key

CURRENT SECURITY CONCEPT

- Security is a **state of well being**
- Security is all about **being prepared for the unexpected**.

INFORMATION SECURITY

The

- **policies**, **procedures**, and **practices**

required to maintain and provide assurance of the

- **confidentiality**, **integrity**, and **availability**

of information

TECHNICAL JARGONS

INFORMATION SECURITY

- Policy - tells you what to do.
- Procedure – tells you how to do it.
- Practice - methodology that is proven to reliably lead to a desired result

CONFIDENTIALITY

- Restrictions on
  - the accessibility, and
  - dissemination of information.

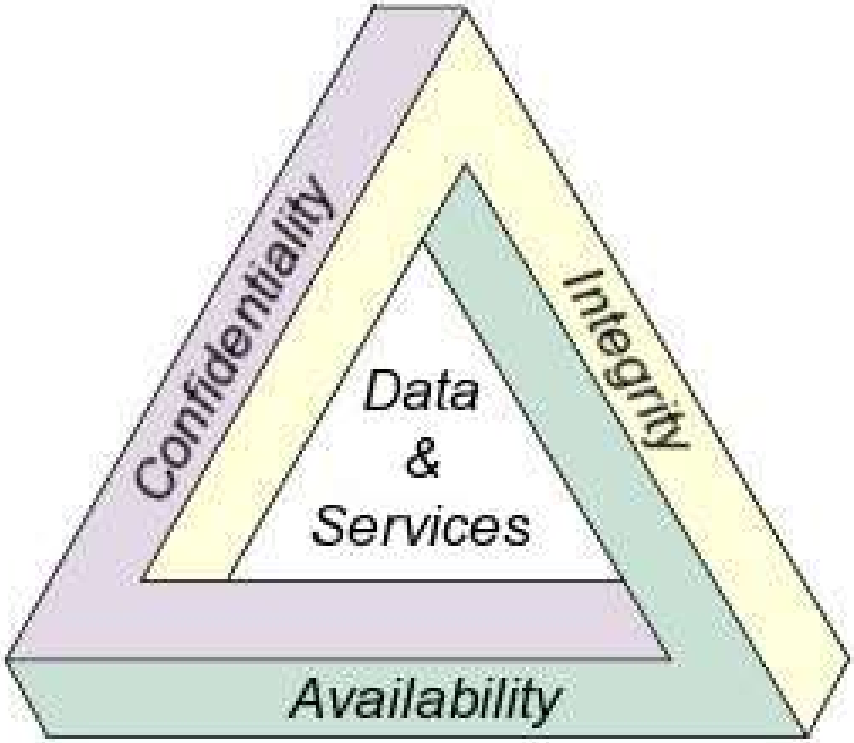
INTEGRITY

- Protecting data from **modification** or **deletion** by unauthorized parties, and
- Ensuring that when authorized people make changes, that shouldn't have been made, the damage can be **undone**.

AVAILABILITY

- Ensuring that information or resources are available when required.

CIA TRIAD



CASE STUDY – ARIANE 5

- European Space Agency
- Ariane 5 Rocket – 10 years and $ 7 million
- Capable of placing a pair of three-ton satellites into the orbit.
- Launched on 04 Jun 1996

CASE STUDY – ARIANE 5

- Immediately after launch, Ariane 5 exploded
- Cause of the explosion:
  - a very small computer program trying to stuff a 64-bit number into a 16-bit space

References: http://s.freissinet.free.fr/videos/ariane5.wmv

VULNERABILITY

- Weakness in a mechanism that can threaten the Confidentiality, Integrity, or Availability of an asset.

- Lack of countermeasure

VULNERABILITY CLASSIFICATION

- Design Vulnerability
- Implementation Vulnerability
- Operational / Configuration Vulnerability

DESIGN VULNERABILITY

- When the vulnerability is said to be inherent to the project or design
- Very difficult to detect and eliminate as it is inherent to the project

DESIGN VULNERABILITY

DESIGN VULNERABILITY

DESIGN VULNERABILITY

DESIGN VULNERABILITY

- Proper implementation of the product will not get rid of the flaw
- Example - TCP/IP protocol stack vulnerability

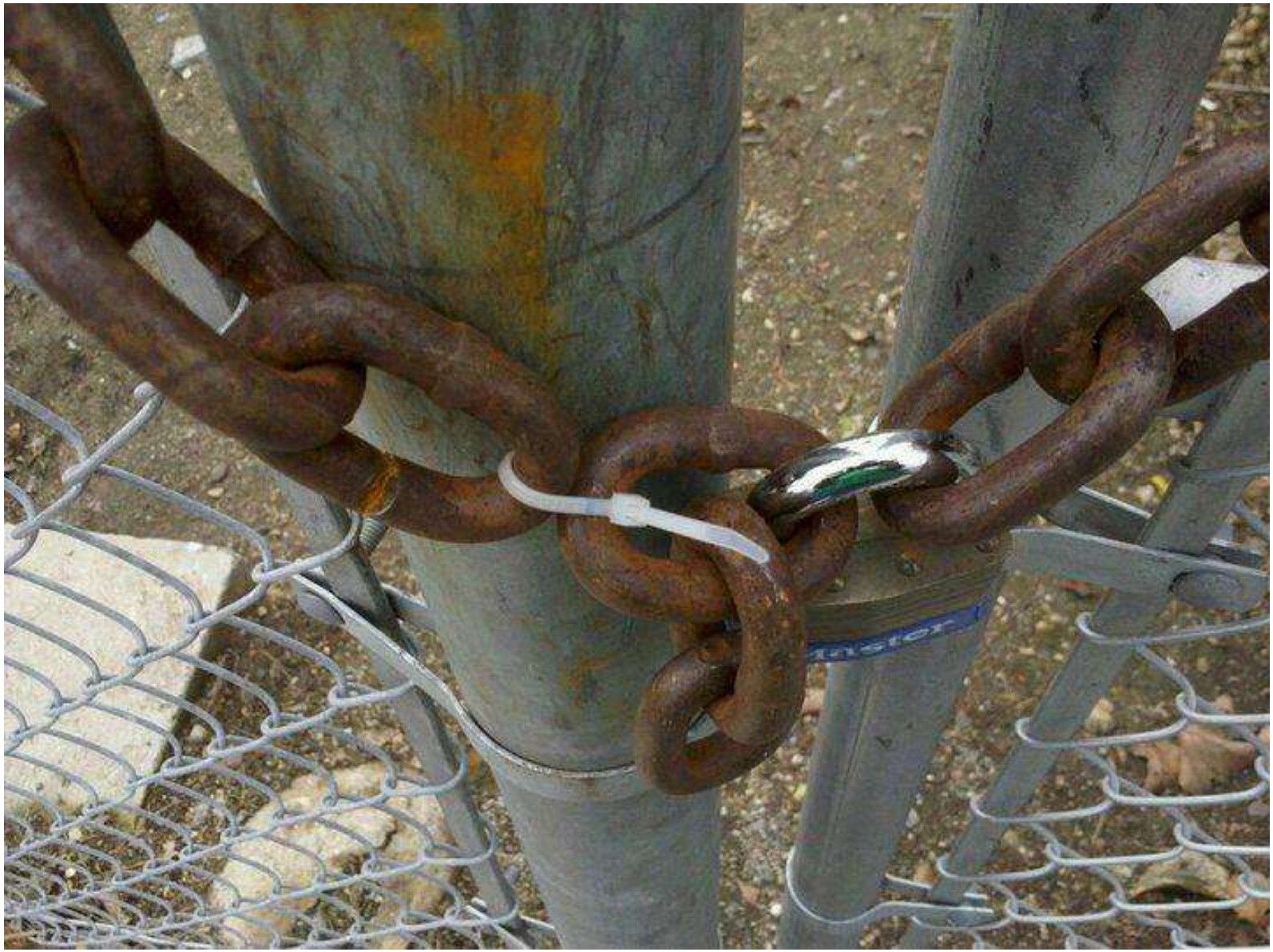
IMPLEMENTATION VULNERABILITY

- When an error is introduced into the components of a system, during the implementation stage of a project or algorithm.
- Example – Buffer Overflows

CONFIG / OPS VULNERABILITY

- When proper configuration is not performed.
- Example –
  - Not disabling unwanted services,
  - allowing weak passwords

CONFIG / OPS VULNERABILITY



THREAT

- Any potential danger to information or systems

or

- Someone uncovering a vulnerability and exploiting it

EXAMPLES

THREAT - EXAMPLES

- An un-authorized person getting into a system that is configured with a weak password or default password.
- A ransomware encrypting the user files.

DENIAL OF SERVICE (DoS) ATTACK

- Flooding the bandwidth of the victim's network so that he cannot use the internet or other services

or

- Spamming the victim mail box

RISK

- Risk is the business impact and the **probability** of that vulnerability being exploited.

RISK - EXAMPLES

- If backup's are not carried out then the data is under risk from corruption or other damages.

RISK MANAGEMENT

- **Identification**, **assessment**, and **prioritization** of risks, followed by -
- **coordinated** and **economical** application of resources to -
- **minimize**, **monitor**, and **control** the **probability** and/or **impact** of unfortunate events.

RISK MANAGEMENT PROCESS

Image Source - http://www.suwcounty.org/images/stories/risk-management-process.jpg

RISK MANAGEMENT MODEL

Risk Management Model		Probability		
		Low	Medium	High
Impact	Severe/Critical	Substantial management required	Must monitor and manage risks	Extensive management crucial
	Moderate	May accept risks but monitor them	Management effort useful	Management effort required
	Limited/Minor	Accept risks	Accept risks but monitor them	Monitor and manage risks

http://www.learner.org/courses/envsci/visual/img_lrg/risk_management_model.jpg

QUALITY OF SERVICE (QOS)

- Feature that prioritizes internet traffic for applications, online gaming, Ethernet LAN ports, or specified MAC addresses to minimize the impact of busy bandwidth.

https://kb.netgear.com/24266/How-to-enable-Quality-of-Service-QoS-on-routers-with-NETGEAR-genie

EXPOSURE

- Represents a state in a computing system which is not a universal vulnerability, but either:
  - Allows an attacker to conduct information gathering activities or to hide activities
  - Allows an attacker to hide activities

Reference:https://security4web.org/glossary.php?w=Exposure

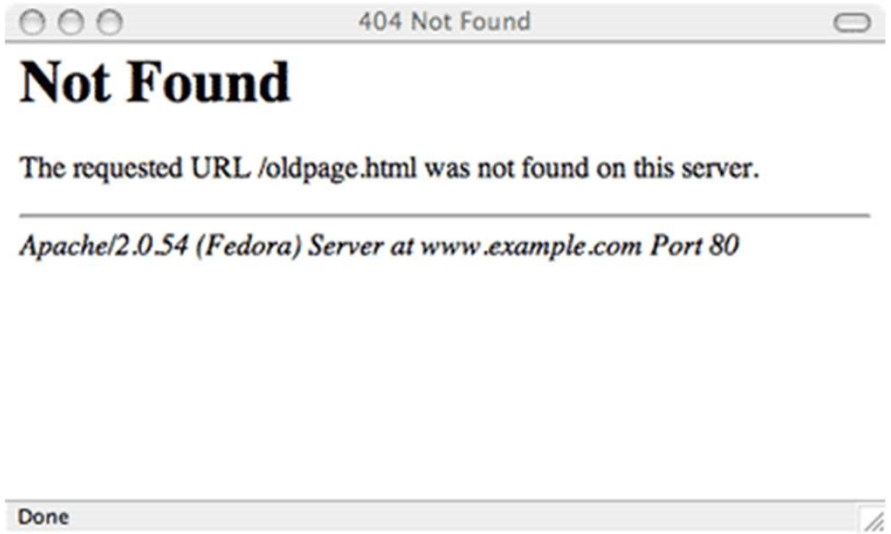
EXPOSURE

- Includes a capability that behaves as expected, but can be easily compromised
- Is a primary point of entry that an attacker may attempt to use to gain access to the system or data

Reference:https://security4web.org/glossary.php?w=Exposure

EXPOSURE

- Is considered a problem according to some reasonable security policy.
- Example - Service banner



Reference:https://security4web.org/glossary.php?w=Exposure

COUNTER MEASURE

- The deployment of a set of security services to protect against a security threat.

http://searchsoftwarequality.techtarget.com/definition/countermeasure

https://en.wikipedia.org/wiki/Countermeasure_%28computer%29

FUS TRIANGLE

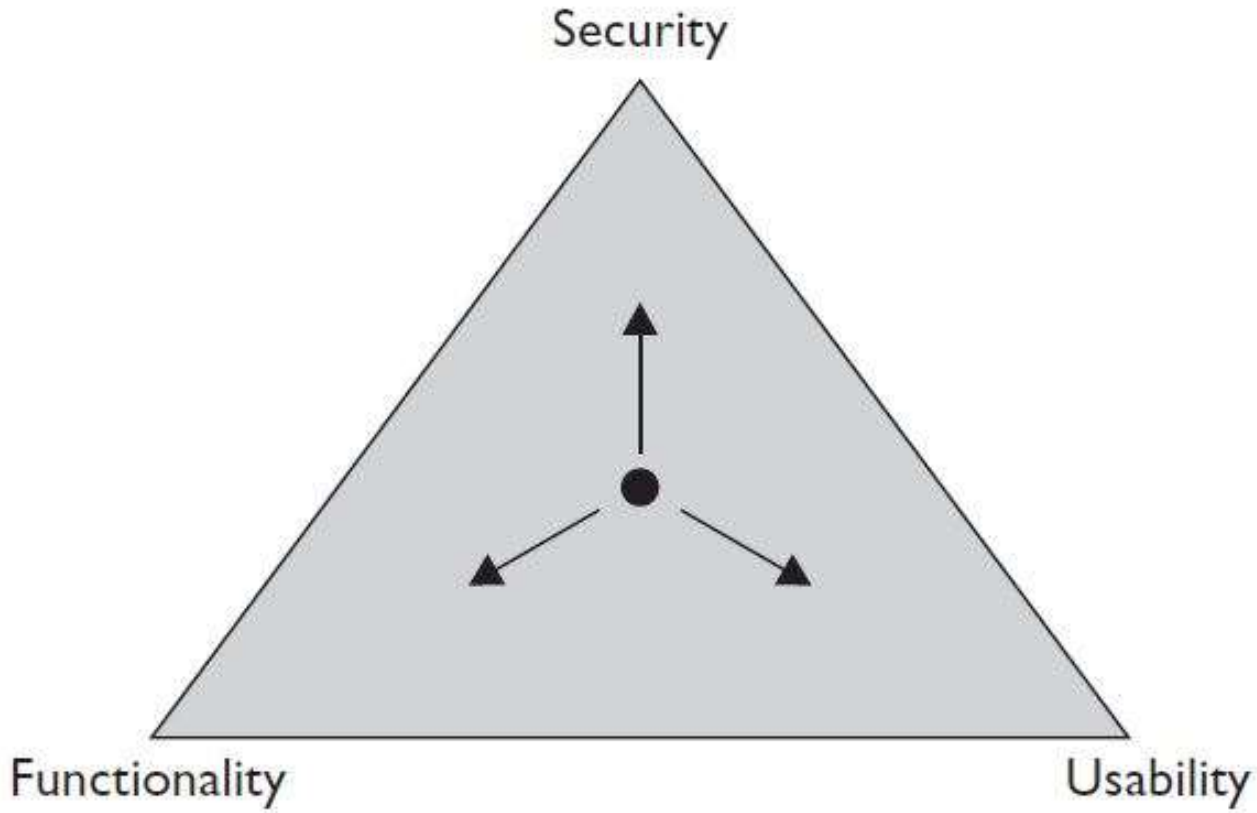


Image Source -

http://static1.squarespace.com/static/531e0c31e4b0f741e5df2ce2/t/53ff3b4ce4b085ab0d3b2a04/1409235789720/21ceb9f.jpg?format=750w

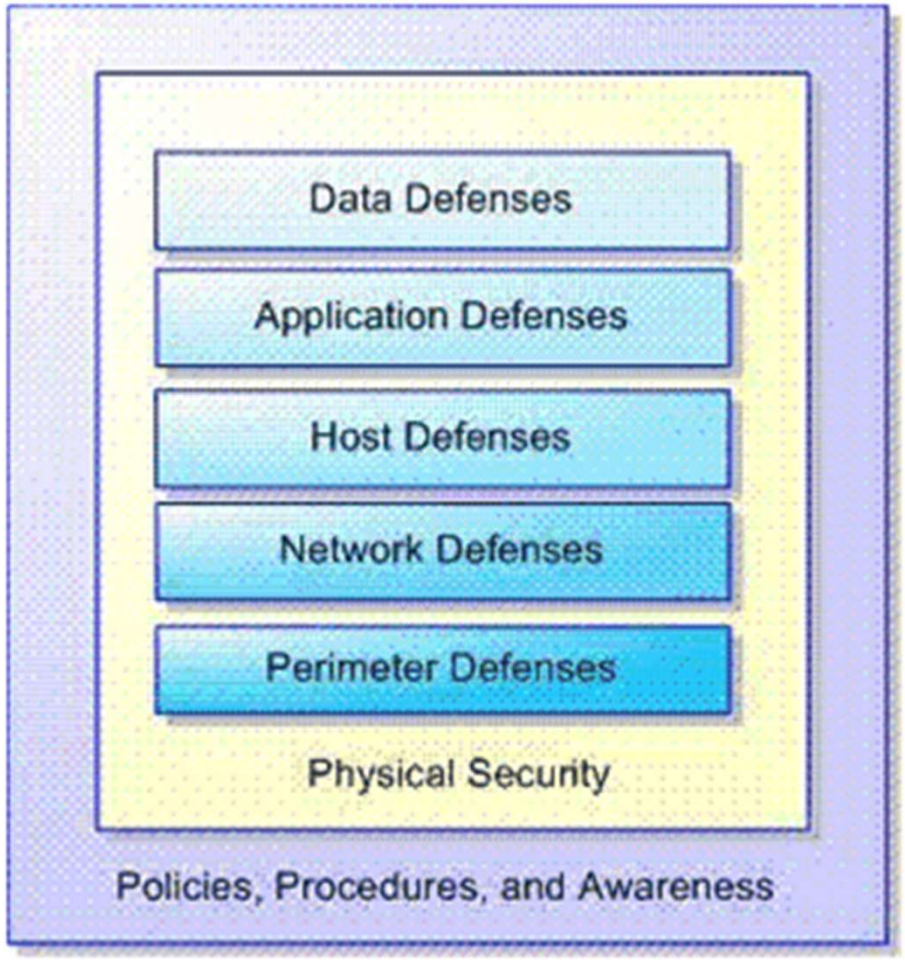
FUS TRIANGLE

- Represents the relationship between Functionality, Usability and Security.
- The more a system is secured, the less usable and functional it becomes

http://blog.infosanity.co.uk/2010/06/12/infosec-triads-securityfunctionalityease-of-use/

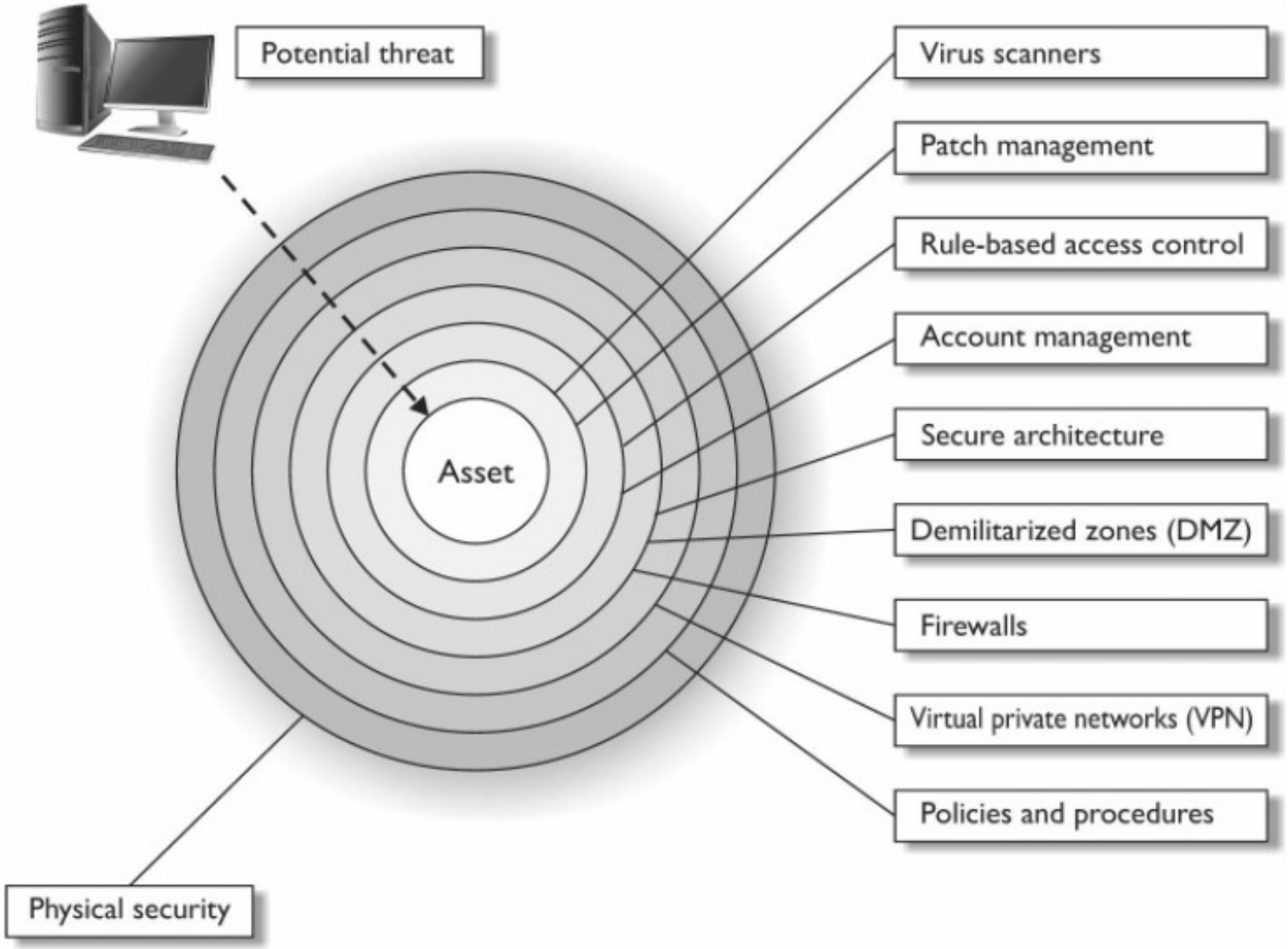
https://emilonsecurity.wordpress.com/2010/10/17/security-functionality-usability/

DEFENCE IN DEPTH



https://i-msdn.sec.s-msft.com/dynimg/IC59619.gif

DEFENCE IN DEPTH



http://3.bp.blogspot.com/-ftVrJYqsubc/UWCVA30CcuI/AAAAAAAAAZ8/9eOMREOeAqk/s1600/Defence+in+Depth.png

DEFENCE IN DEPTH

- Also known as Elastic defense / Castle Approach.
- Military strategy that seeks to delay rather than prevent the advance of an attacker.

DEFENCE IN DEPTH

- Represents the use of multiple computer security techniques to help mitigate the risk of one component of the defense being compromised or circumvented.

DEFENCE IN DEPTH

- Attacker has to penetrate a series of layered defenses
- Each layer is equipped with the suitable defense
- The delay provides the security staff with the time to respond to the attack.

THANK YOU !!!