DDoS defense challenges: The most effective factors in defending against DDoS Attacks

Esam Alzahrani

05/02/2012

Outlines

(1) Background Information

(2) Research Motivation

(3) Research Objective

(4) Reseach Question

(5) DDoS Attacks Defense Difficulties

(6) DDoS Attacks Solutions

(7) Current Defense Mechanisms Deficiencies

(8) Observations of DDoS Challenges

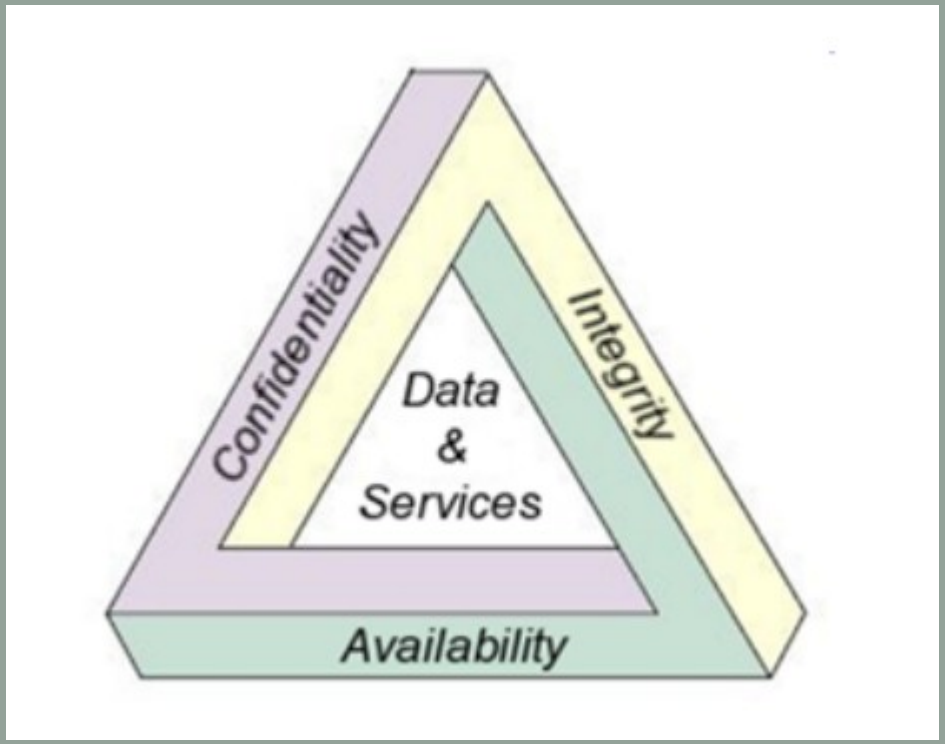
(9) Implications for Mechanisms Implementation

(10) Conclusion

(1)Background Information

- Information Security depends on three fundamental aspects
  - Confidentiality C
  - Integrity I
  - Availability A
- The three components of security are together referred to as the Security Triangle or the CIA of security

CIA- Security Triangle

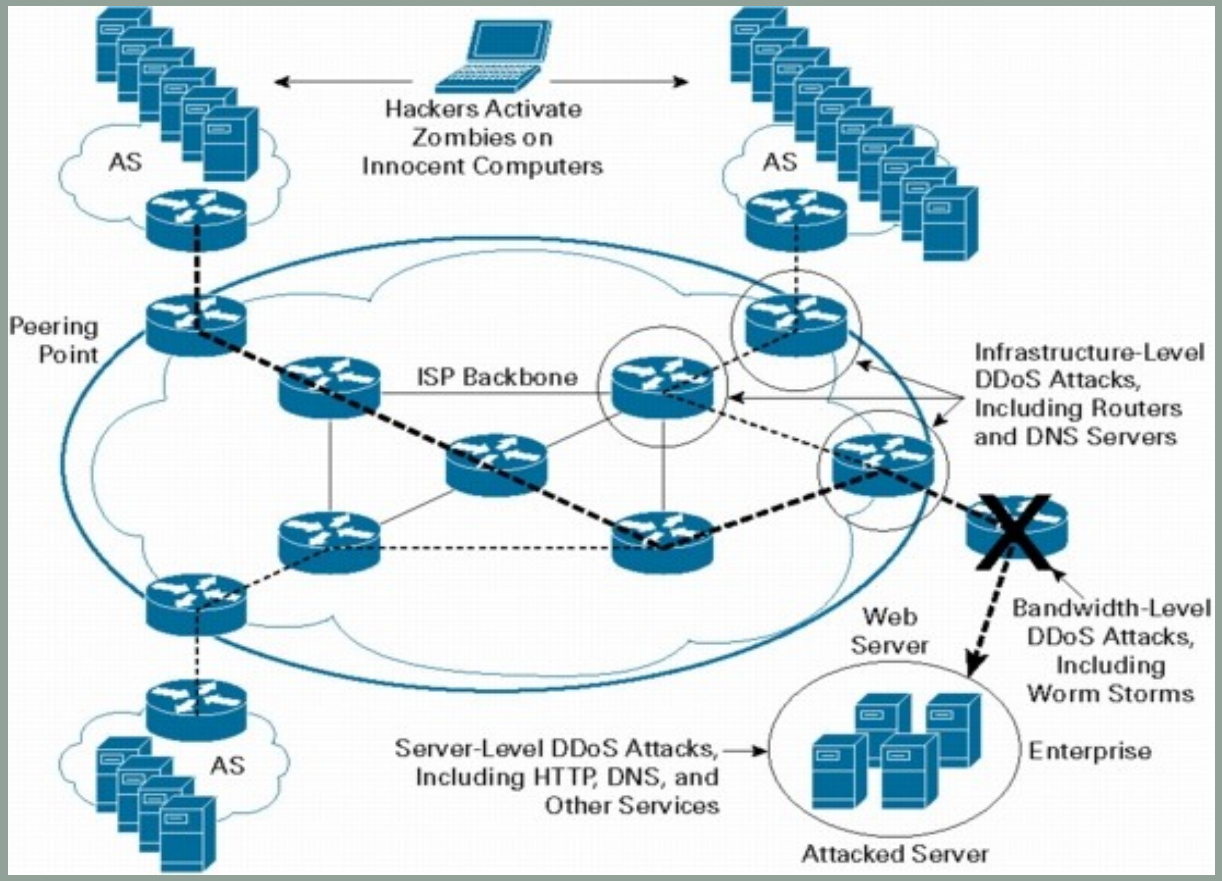


Usurpation

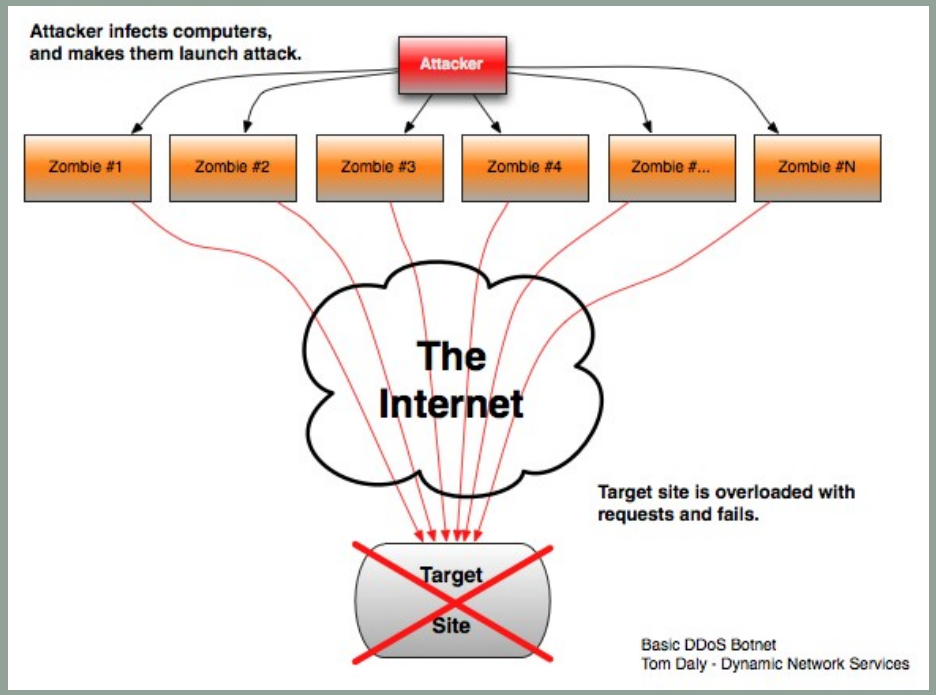
Usurpation is a class of attack in which the attacker has unauthorized control of some part of the system [11]

- Distributed Denial of Service (DDoS):
  - Inhibition of service for long term
  - Attacker prevents server from providing service
  - Availability mechanisms counter this threat

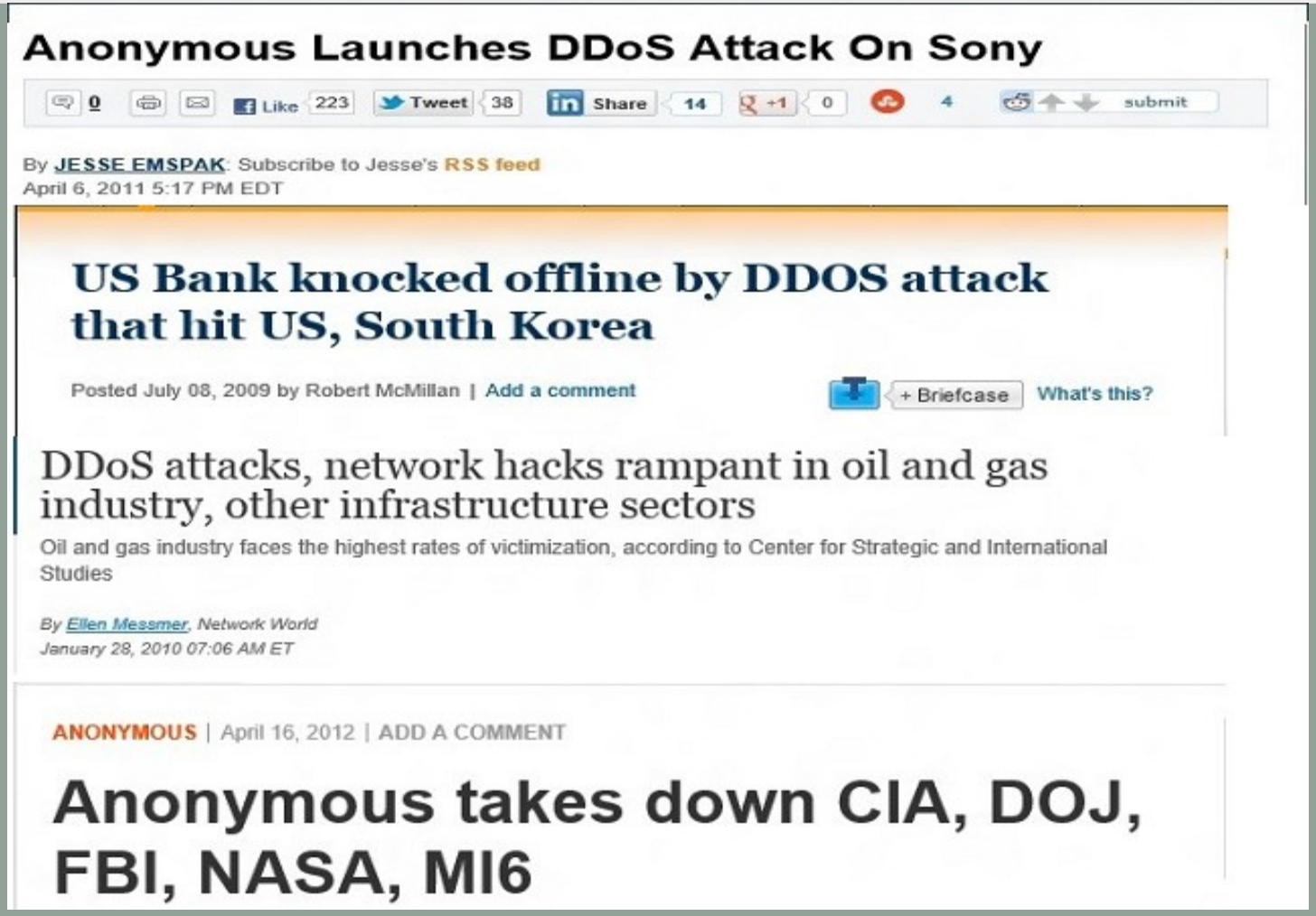
DDoS attacks Initialization



Simplified DDoS attacks Initialization



(2)Research Motivation



Anonymous Launches DDoS Attack On Sony

0 Like 223 Tweet 38 Share 14 +1 0 4 submit

By JESSE EMSPAK: Subscribe to Jesse's RSS feed
April 6, 2011 5:17 PM EDT

US Bank knocked offline by DDOS attack that hit US, South Korea

Posted July 08, 2009 by Robert McMillan | Add a comment

+ Briefcase What's this?

DDoS attacks, network hacks rampant in oil and gas industry, other infrastructure sectors

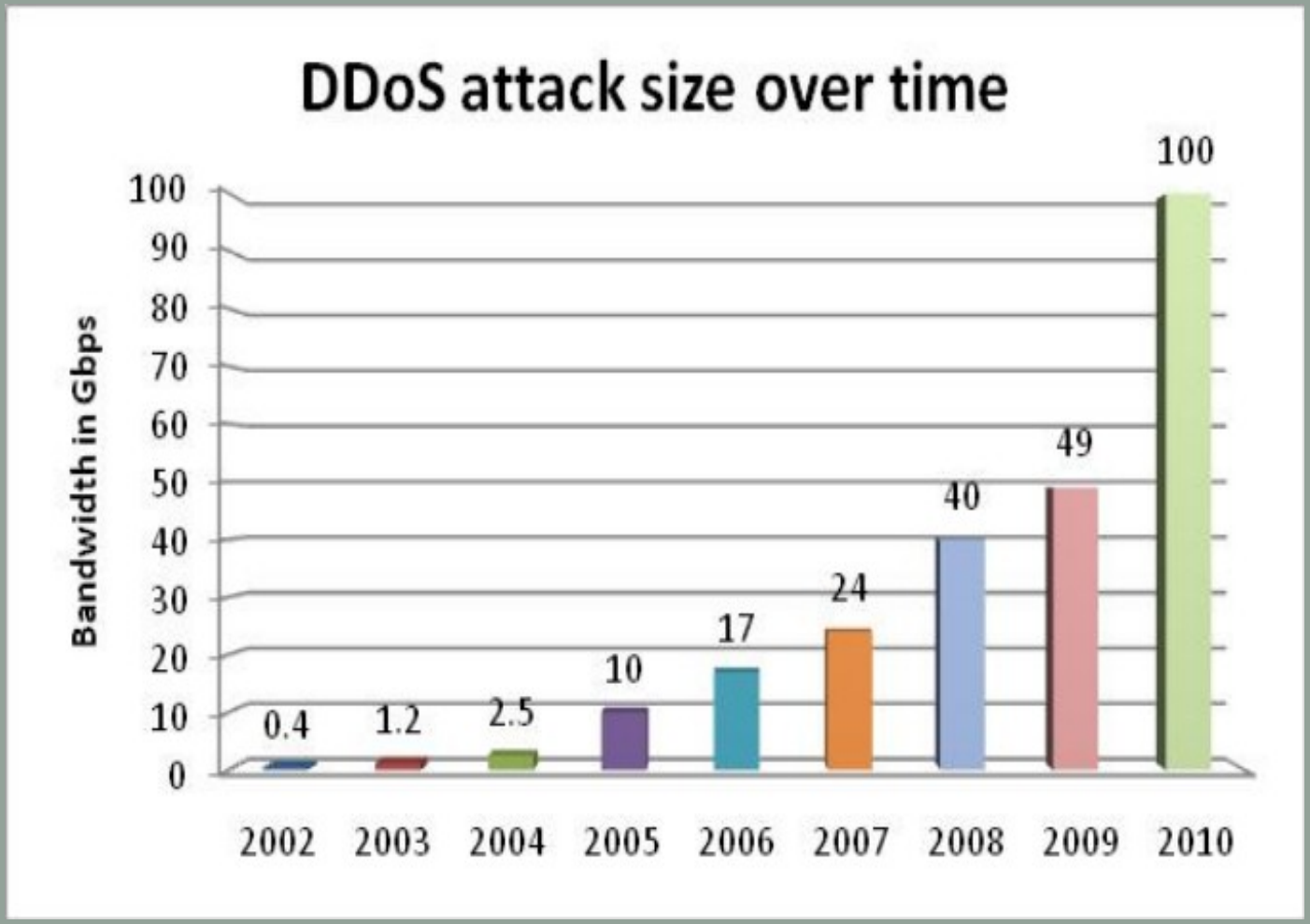
Oil and gas industry faces the highest rates of victimization, according to Center for Strategic and International Studies

By Ellen Messmer, Network World
January 28, 2010 07:06 AM ET

ANONYMOUS | April 16, 2012 | ADD A COMMENT

Anonymous takes down CIA, DOJ, FBI, NASA, MI6

Research Motivation
SANS Institute Report DDoS attacks Size



Research Motivation

- Internet security is still vulnerable.
- Security defense systems are still unreliable.
- There is a big gap between networking development and network security development.
- DDoS attacks are completely uncontrolled.

(3)Research Objective

- Assess the level of risk for Internet security issues.
- Point out the most effective factors in defense mechanisms against DDoS attacks.
- Suggest possible solutions for future work.

(4)Research Question

Why do we not have an optimal solution for DDoS attacks?

(5) Difficulties to defend DDoS

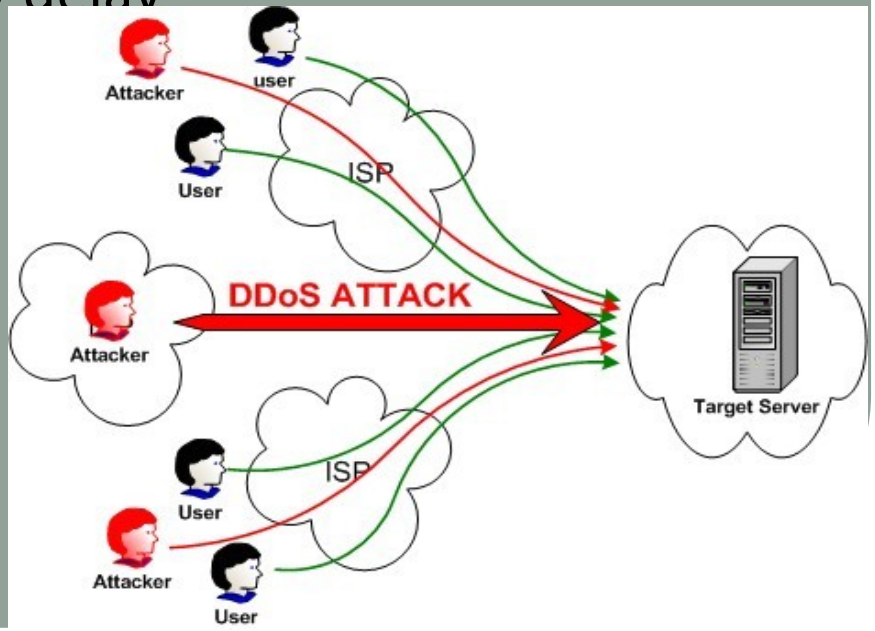
- Difference between normal traffic and attack traffic
- Levels of defense should be distributed

(6) DDoS Solutions

Solutions	Drawbacks
Firewalls	End-Defense
Routers	Inefficient
Switches	Inefficient
Intrusions preventions systems	Content should be known
Clean Pipe	Delay
Blackholing and sinkholing	Legitimate traffic could be discarded

(7) Deficiencies in current mechanisms

- No systems can distinguish legitimacy of traffic
- Available systems not 100% accurate
- Popular websites are affected by delay
- Inefficient trace-back systems



(8) Observations of DDoS Challenges

- Spoofing
- Broadcast Amplification
- Lack of Appropriate Response To Attacks
- Computers are unprotected

(9) Implications for Mechanisms Implementation

- Avoid randomness in security solutions
- Activate the role of trace-back
- Apply Security Requirements Engineering

(10) What can be done soon?

- Security is mandatory for any proposed systems
- Web developers should be aware of Internet security role
- Analysis of recent attacks
- Standards for Cyber security should be established

References

- **Xie Y., Yu S.; Monitoring the Application-layer DDoS Attacks for Popular Websites; Transaction on Networking Magazine, Vol.17, No.1; Feb 2009.**
- **Jayashree P., Easwarakumar K., Anandharaman V., Aswin K., Vijay R.; A Proactive Statistical Defense Solution for DDOS Attacks in Active Networks; ICETET 2008.**
- **You Y., Zulkernine M., Haque A.; A Distributed Defense Framework for Flooding-Based DDoS Attacks; ARES 2008.**
- **Chang R.; Defending against Flooding-Based Distributed Denial-of-Service Attack: A tutorial; IEEE Communication Magazine 2002.**

References

- **Giseop N., Ilkyenu R.; an Efficient and Reliable DDoS Attacks Detection Using Fast Entropy Computation Method; ISCIT 2009.**
- **Park P., Yi H., Hong S, Ryu J. ; An effective Defense Mechanism against DoS/DDoS Attacks in Flow-based routers; MoMM 2010.**
- **Kanmani S., Salini P., A model based Security Requirements Engineering Framework applied for Online Trading System, ICRTIT 2011.**
- **Kim So, Hong Soonjwa. Study on the development of early warning model for Cyber-Attack. IEEE 2011.**
- **Yang, S.J. ; Holsopple, J. ; Sudit, M. Evaluating Threat Assessment for Multi-Stage Cyber Attacks. IEEE 2006.**

References

- **Jongho R., Jungchan N.; Security Requirement for Cyber Attack Trace- back, NCM 2008.**

Thank You & Questions

Esam Alzahrani

ealzahr@gmu.edu