Open Source Software & Key Challenges

Selvaraj K, SAP Labs India
CyberSecurity India 2016 Conference
February 19th, 2016

Agenda

#1 Introduction

#2 Recent cases

#3 Challenges

#4 Key Takeaways

Disclaimer: Views expressed in this presentation has nothing to do with my current employer and it is my personal view as a security expert…

#1 Intro

Ramayan – A case study in Security

Video and image source: youtube.com

Ramayan – A case study in Security

Panchvati

- ✓ The target system

- ✓ Protected by Ram and Laxman

- ✓ Houses Sita, the perfect woman

Sita

- ✓ The Prize!

- ✓ Vulnerable

- ✓ Lacks basic Security Awareness!

Ramayan – A case study in Security

Laxman

- ✓ Administrates the target system
- ✓ Sets up a firewall to protect it
- ✓ Forced to trust a help-call spoofed as Ram
- ✓ Gives clear instructions to Sita

Mareecha

- ✓ Accomplice of criminal
- ✓ Master of Deception
- ✓ Spear-pfishes Ram, succeeds

Ramayan – A case study in Security

Rama

- ✓ Victim
- ✓ Loses key asset 'Sita'
- ✓ Life changes forever

Ravana

- ✓ Social Engineer par excellence
- ✓ An advanced persistent threat
- ✓ Compromised the perfect man, Rama

Ramayan – A case study in Security

That was a 9000 year old story, demonstrating:

- ✓ A Firewall in the form of Laxman Rekha

- ✓ A Spear Pfishing Attack in the form of a golden deer

- ✓ Social Engineering that compromises a seemingly secure system

- ✓ Advanced Persistent Threats are nothing new!

#2 Recent Cases

Recent Cases

✓ **Side-Channel Attack**
  Type of attack: Stealing decryption key from Air-Gapped computer in another room by analyzing the pattern of memory utilization or the electromagnetic outputs of the PC that are emitted during the decryption process
 **Impact:** Extracts the secret cryptographic key from a system.
  Source: http://thehackernews.com/2016/02/hacking-air-gapped-computer.html

✓ **Java Deserialization attack**

✓ **Open Source Software (OSS) not free of security vulnerabilities**
e.g. Heartbleed, Poodle, Shellshock…..

Risks

✓ Threat – Attackers, Hackers, Cyber Terrorists, etc.

✓ Vulnerability – Weakness in software applications (On-premise, Cloud, Mobile, IoT)

✓ Impact – Confidentiality, Integrity and Availability
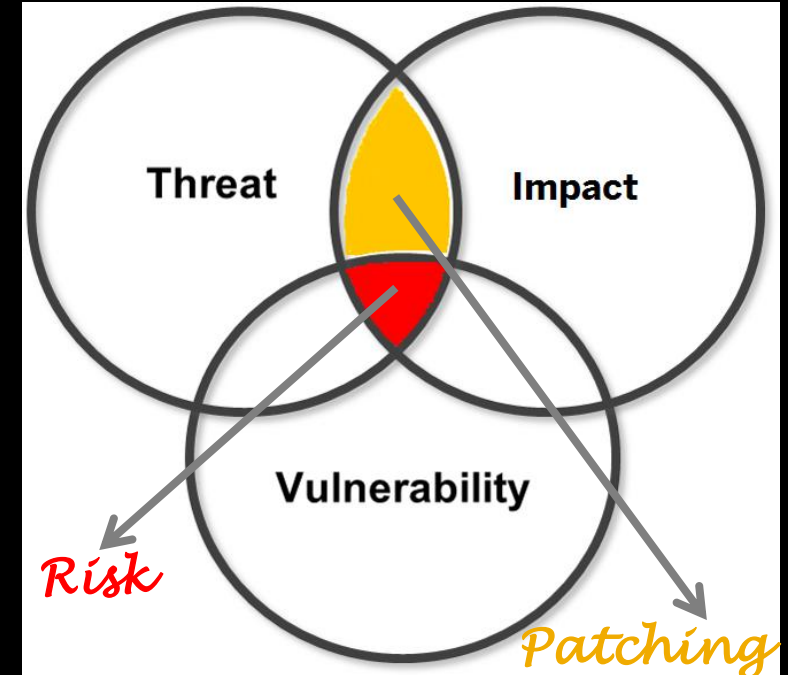
#3 Challenges

Challenges

- ✓ Open Source vulnerabilities reported in public, but to provider of OSS component

- ✓ We learn about them when issue fixed and published, effectively like a zero-day for us

- ✓ No guarantee that it is free of vulnerabilities

- ✓ AND: You are responsible for open source components as if it was your own code

- ✓ YOU need to keep it secure and fix known vulnerabilities

#4 Key Takeaways

Key Takeaways

✓ A chain is as strong as its 'weakest' link and toughen the weakest links

✓ Move from protecting the perimeter to protecting data

✓ Refresh security strategies to address rapidly evolving business needs and threats

✓ Take responsibility for OSS components, they more risky

✓ Finally, Protect your Self, Family, Organization and Nation !!

Thank you

Contact information:

Selvaraj K

Email: selvaraj.k@sap.com

Mobile: 94498 35907