Process for Attack
Simulation and Threat
Analysis

Engineering Attack Resilient Software & Applications

15 October 2014
Executive Summary

This document details to information security and risk managers the importance of focusing on releasing application software and web applications that are resilient to cyber threats. Application and software security relies on trained people following processes and provided with tools and technology. This paper focuses on a new process, the “Process for Attack Simulation and Threat Analysis (PASTA)” and details how this process can help organizations and businesses build applications that are resilient in the face of emerging and evolving cyber-threats.
Introduction to (PASTA) Process for Attack Simulation and Threat Analysis

The increased exposure to emerging cyber-threats targeting web and mobile applications for financial gain and reputational damage represent a challenge for traditional application security measures and require businesses to shift their focus from defensive measures to detective measures. From the defensive perspective, the focus of traditional application security has been the identification and prioritized remediation of vulnerabilities based on their risk/severity hence reducing the opportunity for threat agents/actors to exploit them when conducting an attack.

Because of the sophistication of today’s cyber-threats, the application assets such as sensitive data and business critical functionality can still be compromised by targeted and sophisticated cyber-threats beyond the opportunistic exploit of vulnerabilities. For example by compromising the user’s browser with malware it is possible for an attacker to direct this malware against the application to steal confidential data, bypass authentication controls and control business critical functionality to commit fraudulent transactions. Today’s cyber threats also exploit weaknesses of the human element by social engineering the application users as well as weaknesses in the design of application security controls including gaps in countermeasures that can be effective in detecting and preventing cyber-attacks as these occur and before sensitive data and critical functionality is being compromised.

The identification of design flaws in application architecture as well as of countermeasures to detect and protect from targeted and sophisticated cyber-attacks requires businesses to focus on specific threats and attacks rather then on common vulnerabilities. Specifically it is important to be able to analyze cyber-threats, model the attacks, derive the attack vectors for security testing and determine the risk in the case of a potential attack. This risk can be determined as a factor of likelihood of a threat and the potential impact in the case the threat is realized in an attack that might produce a technical and business impact on the application’s assets such as business sensitive data and critical business functionality.

This type of cyber-threat analysis, attack modeling, security testing and identification of risks posed by design flaws and lack of countermeasures in the application is covered by a specific application security assessment known as both “threat modeling” and “architecture risk analysis”. These types of assessments are manual assessments and executed by experienced security consultants knowledgeable of the application architecture design and the business context and functionality. The quality of these manual assessments mostly relies on the skills and experience of the consultants conducting these assessments. When executed by knowledgeable consultants and senior application security architects, threat modeling and architecture risk analysis produce a set of security requirements for the secure design of the application, a report with design flaws that can be remediated before implementation and a set of attack vectors and abuse cases for security testing the application before releasing it into the production environment.
By comparing with other application security assessments threat modeling allow for a more in-depth analysis of risks of the application design and analysis of the risks of the application assets being attacked by specific threat agents. As new cyber-threats emerge and as new more sophisticated attacks are devised to attack corporate assets such as confidential data it is important for businesses to adopt a process that keeps up with these new threats by analyzing the threat scenarios and by deriving a set of attack vectors that can be used to test the resilience of the application/system as being the target by the attacker.

To address this shortcomings of Minded Security Director Marco Morana developed a new process for threat modeling, the “Process For Attack Simulation and Threat Analysis (PASTA)” that is co-authored by Minded Security director Marco Morana and published in the book Application Threat Modeling by Wiley. The PASTA process is designed to integrate with security engineering and risk management process including security incident response and vulnerability management process that are used by most business today. The main objective of PASTA is to help organizations to engineer applications and systems that are resilient to targeted cyber attacks such as Distributed Denial of Service (DDoS) and malware automated/botnet based attacks.

The PASTA process leverages existing compliance processes with information security requirements and regulations, alignment of security requirements with business requirements, identification of the technical scope of the assessment, the analysis of data flows and exposure to threats, the gathering of threat intelligence and the analysis of emerging threats targeting the various business assets, the attack simulation and the security testing of the effectiveness of security controls in protecting the application assets (e.g. sensitive data and business critical functions-transactions) from the threats and attacks targeting them and the identification of design flaws and vulnerabilities and the instrumentation of countermeasures (e.g. protective and detective security controls).

To help businesses roll out PASTA internally, Minded Security consultants provide the training and an initial remotely managed risk management and threat modeling service. This service is initially to conduct the initial overhead technical risk management work starting with the identification of the business’s digital assets such as sensitive data and critical functionality and ending with the identification of design flaws and countermeasures that can be instrumented within the application to protect from future attacks targeting the application. Once the process has been rolled out Minded Security consultants will help to internal client information security and risk management teams to set up the internal architectural risk analysis and threat modeling as internal service and continue to provide feeds with real threat intelligence as well as updates of threat and attack libraries and security control frameworks for mitigate risk posed by the introduction of new technology stack and architectural components.
PASTA Activities

At high level the PASTA process consists in several activities performed at each of the seven stages of the process that are outlined in the figure herein:
Goals & Benefits of Using PASTA

Application security requires people, process and technology and commitment by the organization in training, consistent process execution and deliverables and use of tools and technologies to manage risks. In order for an organization to adopt PASTA it is important to focus on this essential elements In regarding of people, Minded Security will perform a dedicated training workshop on PASTA and help your organization in training a professionally educated workforce with expertise in conducting threat analysis, application security risk analysis, attack driven testing and cyber security risk management. In regarding of process, Minded Security will provide application security architects and information security/risk managed a process that focuses on analyzing emerging and evolving cyber-threats against application software, identifying vulnerabilities that these threats seek to exploit and simulate attacks to identify the exposure to the assets and the countermeasures to mitigate these impacts.

The main goals of PASTA process are:

1. **Improving visibility of cyber-threat risks**: by providing risk management and information security with an holistic view of the company assets and the risk exposure from the perspective of the attackers/threat actors

2. **Extending the organization protection domains**: the compliance domain is considered as a factor in documenting security requirements but PASTA focuses beyond the traditional compliance driven security domains by focusing on cyber threats as today compliance driven security controls can be bypassed by advanced and emerging threats

3. **Leveraging existing application security processes**: PASTA stages and activities leverage data and processes used today for traditional security compliance assessments such as vulnerability assessment, security tests/pen testing and secure code analysis but widen the focus to threats and attacks

4. **Integrating with the SDLC** by providing an application threat modeling process that organizations can follow to address security issues from the inception of the software development lifecycle to the production delivery

5. **Increasing the maturity of the organization in software security** by evolving from vulnerability assessments to threats and attack analysis as the drivers for determining the risk mitigation strategy

These goals are reached by using Minded Security consultants to train an internal workforce provided by the right tools and process to execute consistently and efficiently. An initial assessment will provide immediate benefits for the organization such as:

- **Risk reduction**: analyze the threat’s likelihood and technical and business impacts to identify countermeasures and propose risk mitigation strategy;
- **Knowledge of your threats**: Looking first and for most at cyber threat mitigation as a business problem, integrate threat information from what does/did happen (e.g. fraud, incidents, security events);
- **Engineer for Resilience** conceptualize likely attacks based upon motives and identified attack vectors, thinking like an attacker across the app environment and during the SDLC to build attack
resilient applications and products

**Improve Software Security:** integrate threat and risk analysis in the SDLC by leveraging security risk, governance and software security processes such as secure design reviews, secure code reviews and pen testing

**Collaboration among application/product stakeholders:** such as those who focus is information security, compliance and risk management and those who focus on engineering secure software

Ultimately the following application stakeholders in the organization will benefit by the adoption of the PASTA process:

- **Developers** are helped to understand which components are vulnerable and their exposure to attacks
- **Security/Pen-Testers** rely on abuse cases to create positive and negative tests of the application
- **Project managers** can manage security defects more efficiently by setting the right priorities
- **Architects** understand implications of threats and attacks at the design level and how countermeasure protect data assets
- **CISOs** can make informed risk management decisions
- **Business managers** can determine which business objectives have impact on security
Introduction to Minded Security

Minded Security is the Software Security Company supporting you to build, deliver and use more secure software.

Minded Security helps businesses and organizations to build secure products and services.

Minded Security main goals are:
- Helping customers to develop, maintain and buy Secure Web and Mobile Applications;
- Training and awareness in Application Security;
- Release of ad-hoc security testing tools to identify high risk vulnerabilities;
- Release of innovative web fraud detection tools for protecting organizations from specific threats.

Contacts:

To start building attack resilient applications using PASTA contact Minded Security UK Limited Marco M. Morana, Partner, Minded Security UK Limited One Canada Square Canary Wharf, E14 5AB London:
Office +44 (0) 203 725 7615
Mobile +44 (0) 7732 234 694
Mail: marco.m.morana@mindedsecurity.com

To stay informed about cyber-threats exploiting insecure software and how you can prevent cyber-attacks exploit weaknesses in web applications and software visit Minded Security web pages:
Minded Security Corporate Site: http://www.mindedsecurity.com
Minded Security Twitter: http://www.twitter.com/mindedsecurity