

Sryas Network and Security Standards

What are standards?

- They may be called specifications
- Some call them as "de facto" standards
- But they are not necessarily open standards
- They are distinguishable, published and clear rules

Web Application Securities

Securing a company's web applications is today's most overlooked aspect of securing the enterprise. Hacking is on the rise with as many as 75% of cyber attacks done through the web and via web applications.

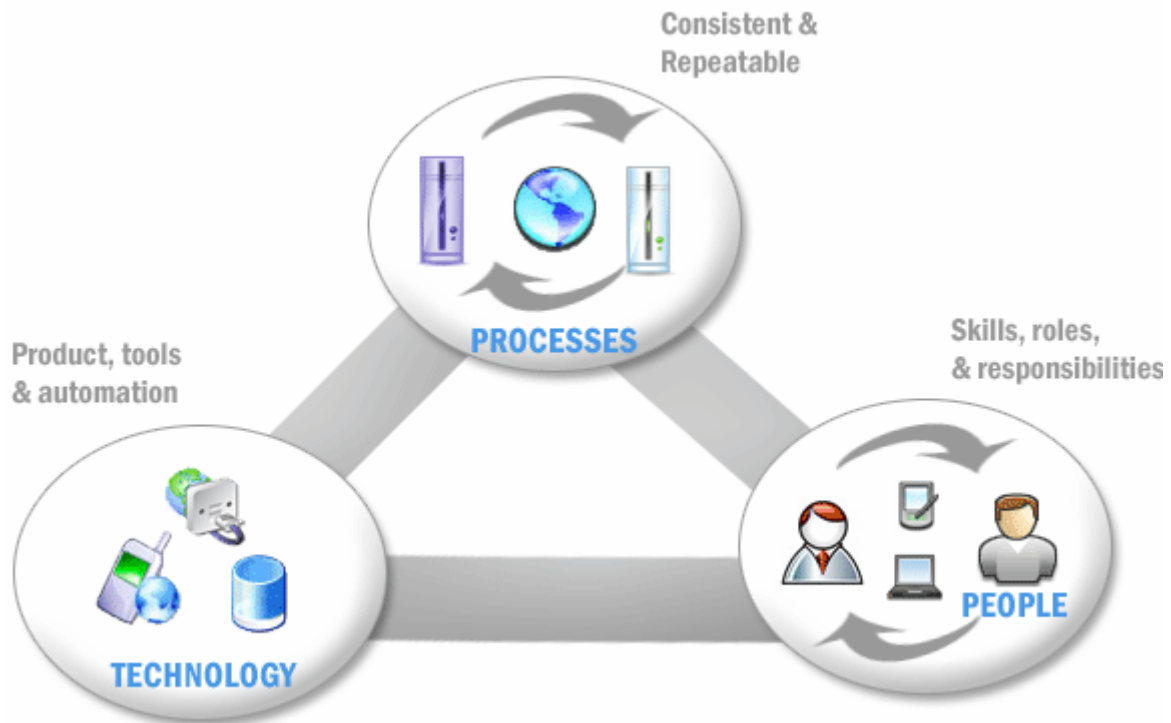
- Most corporations have secured their data at the network level, but have overlooked the crucial step of checking whether their web applications are vulnerable to attack.
- Web applications raise certain security concerns.
- To deliver the service (intended by design) to customers, web applications must be online and available 24x7x365.
- This means that they are always publicly available and cannot discriminate between legitimate users and hackers.
- To function properly, web applications must have direct access to backend databases that contain sensitive information.
- Most web applications are custom-made and rarely pass through the rigorous quality assurance checks of off-the-shelf applications.
- Through a lack of awareness of the nature of hack attacks, organizations view the web application layer as part of the network layer when it comes to security issues.

Approaches

- Holistic approach – involves people, technology and information
- A tier-ed (Layered) approach to address different audiences
- Framework approach
- Leverage existing standards, guidance and best practices and evolve own standards

Holistic Approach

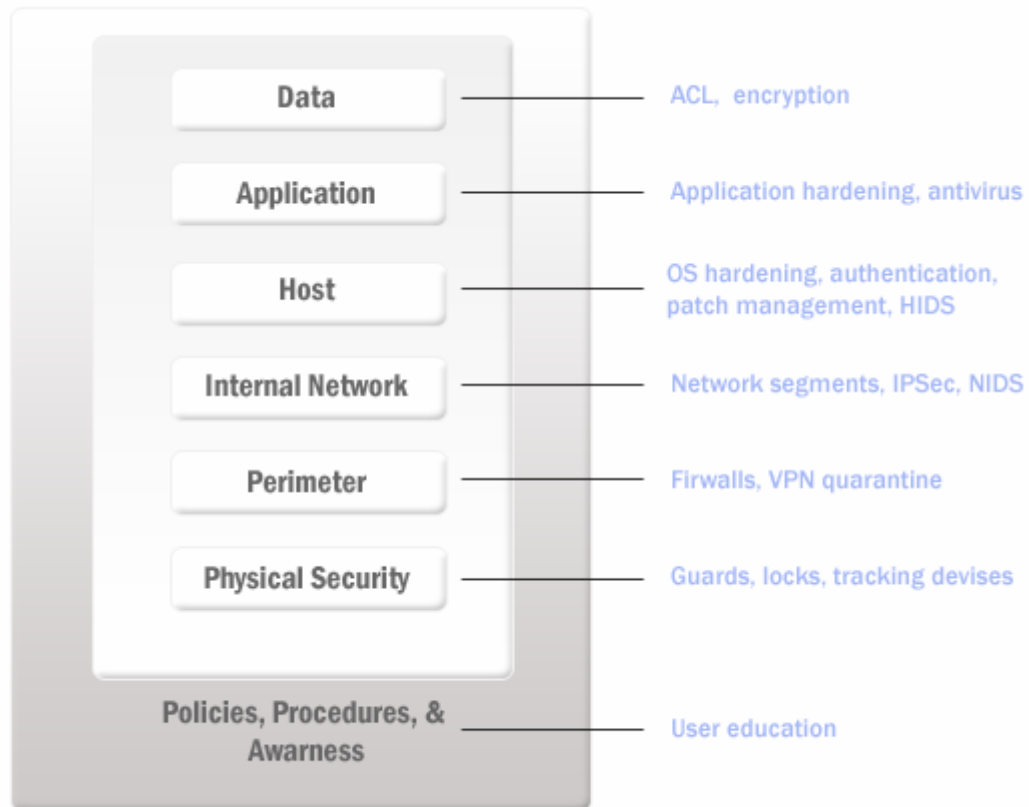
- Security challenges continue to increase
- Security is only as strong as the weakest link
- Awareness and Skills in IT security are critical to success in security



Layered Approach

Using a layered approach

- Increases attacker's risk of detection
- Reduce attackers chance of success



Framework Approach

- Firewalls, SSL and locked-down servers are futile against web application hacking
- Any defense at network security level will provide no protection against web application attacks
- Security software's for web applications for protection against SQL Injection, XSS & other web vulnerabilities
- Intelligent framework's to locate CRLF injection, Code execution, Directory Traversal, File inclusion and Authentication vulnerabilities
- Monitor traffic and view detailed reports about attackers and attack attempts
- Customize security settings for each Web site or application and Protect intranet applications against application attacks
- Analyzes websites including flash content, SOAP and AJAX
- Easily integrate application security with monitoring and management systems

Security Policy (Business & Organization Rules)									
Best Practices (Security Organization, Physical Security, Personnel Security, Operational Security)									
Architecture & Mechanisms					Security Services		Processes & Methods		
Security Infrastructure	Network Security	Security Techniques	Security APIs	Security Tokens	Authentication	Risk Assessment	Security Monitoring & Incident Management	Business Continuity & Disaster Recovery Planning	Security Assurance & Accreditation
					Authorization				
					Confidentiality				
					Integrity				
					Non-repudiation				
					Accountability				
					Availability				
Legal & Regulatory Environment									

Web application security tools

- N-Stalker – Web application security scanner
- Sandcat suite – Security Assessment Software's
- Acunetix – Web Vulnerability software tool, Industries' most advanced and in-depth SQL injection and Cross site scripting testing