Computer Network Defense Approaches

Cyril Onwubiko

Intelligence & Security Assurance
Research Series
London, United Kingdom
Email: cyril.onwubiko@research-series.com

13th December 2011

Abstract: Defenses to cyber attacks become very efficient when appropriate defense approaches are deployed accordingly to protect valued assets. Inappropriate application of defenses to treat risk in information systems will result to weakened defenses and consequently lead to significant impact on the confidentiality, integrity or availability of these assets when compromised. This paper presents defense approaches to computer network that assist information asset owners in deciding on appropriate defense approaches to adequately protect their valued assets.

Keywords: cybersecurity, defense approaches, computer network, threats, risk

1 Cybersecurity Approaches

Computer networks have now become an essential utility such as electricity or telephone access because of their importance to society in general. For example, organisations rely on computer networks for their administration and secure business transactions; while defense agencies use computer networks to disseminate classified information, national cyber intelligence and defense. Hence the reliability of computer computers and their offered services becomes critical. Unfortunately, no computer network can be absolutely secured. As new advancements emerge, for example cloud computing, new and unfamiliar risks become prevalent. Therefore, organisational security protection strategy must constantly evolve and re-visited. The underlying is not the protection mechanisms used by organisations to protect their investments, but understanding the strength and limitation of each security approach is pertinent. So that appropriate security mechanisms are used for proportionate risk treatments. In this paper, computer network Defense approaches are discussed with the aim to explaining their place in the overall organisational cybersecurity strategy.

Security defense approaches to detect, prevent and mitigate security threat and attack targeting computer networks can be classified into three main categories: *Preventive*, *Reactive* and *Retrospective* (see Figure 1).

1.1 Preventive Approaches

These are techniques distinctively used to prevent threats and attacks from penetrating into monitored networks. These include access control mechanisms, admission control methods, biometrics and cryptography that are used as the first line of defense.

1.1.1 Access Control

Access control mechanisms are used to control both physical and logical access to valued assets. These mechanisms include physical access controls such as locks and gates, fence and buildings, network nodes and infrastructure building blocks. Logical access controls such as authentication systems, identity management systems, firewalls, and access control lists are used to offer network-level and user-level access restrictions to information systems and networks. While physical access control mechanisms control physical-level access (reacheability); logical access controls provide network-level or traffic-level and user-level access restrictions to controlled or ‘monitored’ environments. Examples of access control systems include authentication and authorisation protocols such as TACACS or RADIUS servers, firewalls, locks, cabinets, and network nodes.

1.1.2 Admission control

Admission control is a higher-level access control mechanism used mainly to control logical access to user-level, system-level and network-level access to valued asset. Two well-known admission control mechanisms are system-level admission control, such as the network access protection by Microsoft and network-level admission control such as the network admission control by Cisco Systems Inc.

Network access protection (NAP [1]) is a governance policy compliance enforcement platform built into recent iterations of the Microsoft Windows operating system. It allows security policies to be set, such as requirements for the operating system patches and anti-virus updates, and restricts clients from accessing network services until the client demonstrates compliance.

Network admission control (NAC [2]) is a policy compliance authentication-based network enforcer that validates software credentials running on a client (PC, PDA and other devices) seeking access to a network. NAC's validation includes checking operating system type, patch level, service packs and anti-virus installed on the client as defined in the security policy.

1.1.3 *Cryptography*

Cryptography is used to protect information resource and asset from threats such as misuse, traffic analysis, and replay attacks by preserving the confidentiality and integrity of communications. For example, cryptographic applications such as Internet Protocol Security (RFC 4303 [3]) are used to encrypt packets being transported among trusted parties. Cryptography provides secure communications among trusted parties, such that foreign or eavesdropping adversaries cannot identify the transported payload. And also assists to transport shared secret keys securely among trusted parties.

1.1.4 *Biometrics*

Biometric security is a verification-based preventive security approach aimed to identify entities by authenticating them. This may involve series of physical identification process, such as iris and rental scans, speech, facial feature comparison and facial thermograms, and hand geometry or behavioural characteristic of the entity. Biometric security is preferred over pin-chip, password or token-based identification methods because biometrics is believed to offer stronger verification security.

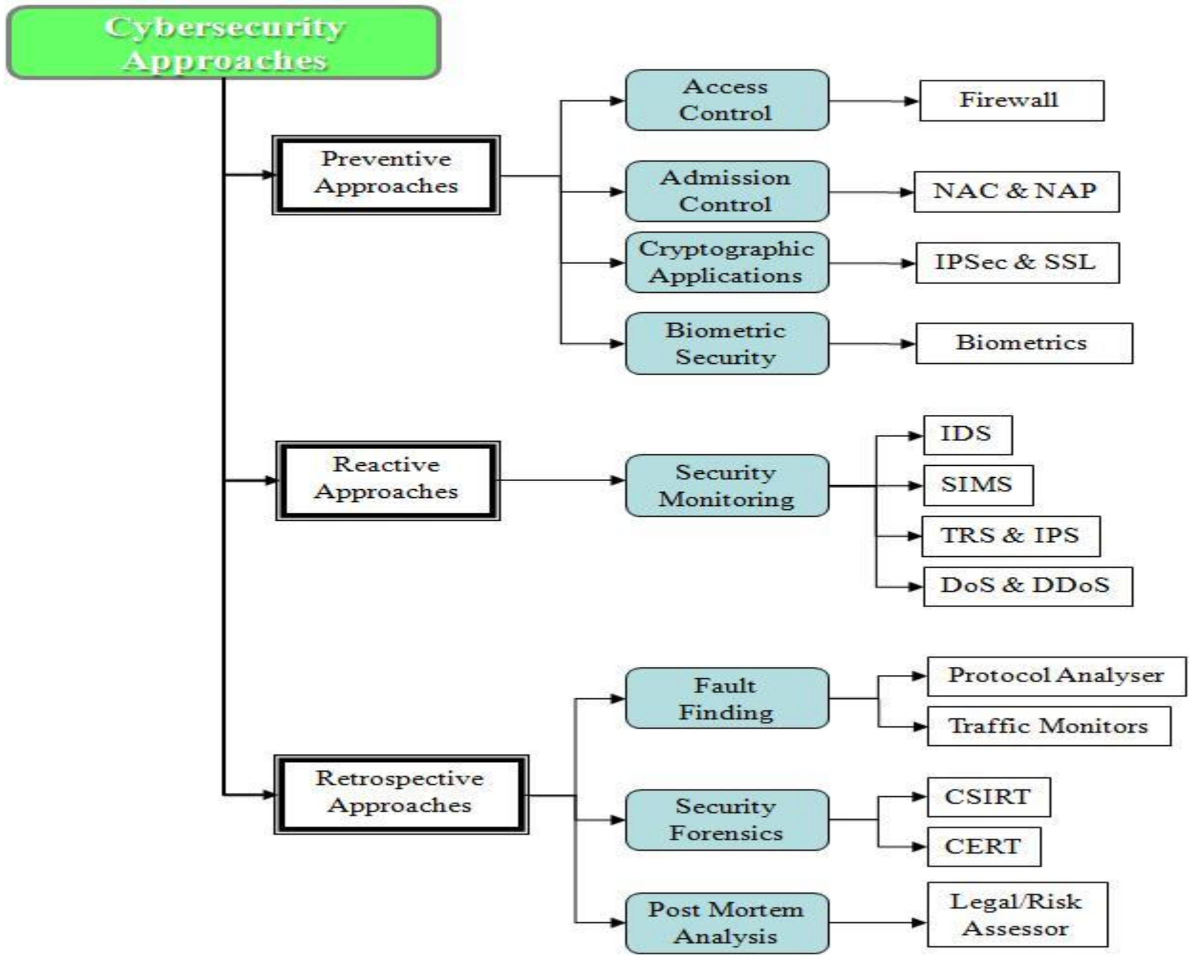

Figure 1: *High-level Classification of Approaches to Detect, Prevent and Mitigate Attacks to Computer Networks*

1.2 *Reactive Approaches*

These are techniques used in detecting and mitigating attacks that the preventive methods could not exclusively prevent. It is important to note that not all types of attacks can be prevented, for example, denial of service (DoS) or distributed denial of service attack (DDoS).

Reactive approaches complement the preventive approaches to adequately protect information assets. In security monitoring for example, a collection of both preventive and reactive defense components are used to protectively monitor the network, comprising intrusion detection systems (IDS), security information and event management systems (SIEM), integrity file checkers, threat response systems, and DoS mitigation, (see Figure 1).

1.2.1 Security Information and Event Management

Security information and event management (SIEM) are systems used to proactively monitoring computer networks for the enterprise. Their main functions are to correlate, normalise and analyse security events from varying network sources to provide a unified actionable logic for protecting an enterprise network. *Correlation* is a technique applied to show the relationship of security events coming from different sources in the network. This enables the system to compare and analyse sequences of security events, thereby allowing for improved detection capabilities. *Normalisation* is a technique applied to format the correlated security events in a particular pattern, which helps in prioritising events in a given context.

The relevance of SIEM is seen in areas such as, Enterprise Network Monitoring, Alert Correlation, Attack Identification and Tracking, and Vulnerability Assessment. For example, in the security provider arena, SIEM market is very competitive with commercial offerings such as, Arcsight's Enterprise Security Management [4], Cisco's Security Information Management System [5]. From the open source community, there are the Open Source Security Information Management [6] and the Analyst Console for Network Security Monitoring [7].

1.2.2 Threat Response Systems

Threat response systems (TRS) are in-line intrusion detection systems that provide active response to perceived attacks. Responses provided by TRS are automated, active and able to provide instant mitigation to perceived attacks. TRS are synonymous to intrusion prevention systems (IPS). When an IPS is not functioning in an in-line mode, they default to normal IDS. Most intrusion prevention systems work in simulation mode because current IDS still struggle with appropriately classifying threats (for example, false positives and negatives).

1.3 Retrospective Approaches

Retrospective techniques are fundamentally used when evaluating security breaches aimed at post-mortem examination and litigation purposes. Retrospective security methods focus on investigating break-ins after attacks had happened, comprising post-mortem analysis, network fault finding, and security forensic (see Figure 1).

1.3.1 Network Fault Finding

Network fault finding is an ethical process of analysing networks and systems to detect, diagnosis and resolve system and network related faults. The process may require the use of tools and techniques that are capable of sniffing, monitoring and analysing user-level, system-level and network-level traffic that aids to detect system and network related faults. Examples of such tools include protocol analyser, traffic monitors and passive operating system fingerprints.

1.3.2 Security Forensics

Computer and network security forensic investigates retrospective security breaches (break-in), focusing on gathering crime evidence from electronic media and network appliances. This comprises both the legal proceedings for liability and technical aspects of investigative searches, which encompasses digital crime scene investigation, authorisation, crime reconstruction and crime prosecution. It is important that every organisation has forensic readiness capability. This task can be provided in-house or off-shored to another provider organisation to carryout. There are also government agencies and public organisation that provide forensic advisory that are very pertinent such as the US-CERT (US Computer Emergence Readiness Team [8]), FIRST (Forum of Incidents Response and Security Teams [9]), CSIRT (Computer Security Incidents Response Team). These organisations provide forensic advisory and some offer early warning alerting capability toward potential incidents.

1.3.3 Post-Mortem Analysis

Security post-mortem analysis is traditionally associated with fault management and process longevity, where a roll-back examination is conducted to investigate a possible cause of fault, error or failure in systems before a back-out procedure. To avoid recurrent faults, errors or failures in the process, a post-mortem examination is essential.

2 CONCLUSION

As organisations seek to protect their information technology investments, it is important they understand associated risks to their valued assets. More importantly, they must understand the strength and limitation of protection mechanisms they deploy, bearing in mind that inappropriate choice of security mechanisms may lead to an asset either being inadequately unprotected in line with risks that may exist with that asset, consequently leading to security exploit, compromise or abuse; or overspending in the protection plan of that asset. While it is possible to combine these different security defense approaches together, there are cases when one approach is sufficient in protecting valued organisational assets.

3 REFERENCES

[1] Microsoft Inc., ‘Network Access Protection’, http://technet.microsoft.com/en-us/network/bb545879.aspx

[2] Cisco Systems Inc., ‘Network Admission Control’, http://www.cisco.com/en/US/netsol/ns466/networking_solutions_package.html

[3] S. Kent, ‘IP Encapsulating Security Payload (ESP)’, RFC 4303, December 2005

[4] Arcsight SIM - http://www.arcsight.com

[5] Cisco SIEM - http://www.cisco.com/en/US/products/sw/cscowork/ps5209/index.html

[6] OSSIM - www.ossim.net

[7] Analyst Console for NSM -http://sguil.sourceforge.net/

[8] US Computer Emergence Readiness Team, http://www.us-cert.gov/

[9] FIRST – Forum of Incident Response and Security Teams - http://www.first.org/