SCTE ISBE CABLE-TEC EXPO '16
SEPTEMBER 26-29 PHILADELPHIA

SECURITY CONSIDERATIONS IN A WI-FI FIRST NETWORK

A Technical Paper prepared for SCTE/ISBE by

RAM SRIDHARAN
CTO, Application, Analytics & Cloud (MSO Segment)
NOKIA
601 DATA DRIVE, PLANO, TEXAS, 75035
972-477-9849
ram.sridharan@nokia.com

Table of Contents

List of Figures

Introduction

With their Wireless strategies in place, MSOs are planning to use Wi-Fi First solutions to provide differentiated wireless services in order to level the playing field with converged Telco service providers in their respective markets. To achieve this level of competition, MSOs will likely form MVNO relationships with mobile operators to provide ubiquitous network coverage. These MVNO relationships can take many forms, from a complete white label service where MSOs deploy very little equipment on their side (mainly OSS/BSS integration), to a model where MSOs have a RAN sharing model with the mobile network operator. MSOs may deploy their own Evolved Packet Core (EPC) infrastructure and integrate that EPC to their existing IMS network elements. They may also deploy application/messaging servers and media servers to provide a comprehensive wireless service offering. These components will most likely be running as virtual network functions in a cloud environment. Then, there are the devices themselves - which MSOs can either sell directly or leverage in a Bring Your Own Device (BYOD) model. Security becomes an issue across all domains – the network, the cloud (where the network functions and other applications are hosted) and the devices. This paper first analyzes the security issues that need to be addressed and proposes generic solutions across these domains. Network security aspects addressed in this paper include preventing unauthorized access, malicious traffic injection, eavesdropping, assured interworking with network elements, roaming security, critical domain perimeter security (value added service, charging, OSS/BSS), etc.. Carrier Grade NAT (CGN) and Secure DNS also become key requirements. This paper goes on to highlight cloud security considerations, including automating the deployment of cloud security polices, life cycle management of the Virtual Network Functions (VNFs), enterprise security compliance, security policy management across hybrid network functions, identity management, security analytics and audits. And finally, network-based endpoint security are analyzed in detail, in the areas of malware detection and qualification, threat analysis and trending analytics.

Content

The recent increase in sophisticated, targeted security threats by both insiders and external attackers has increased the awareness and urgency from communication service providers for comprehensive security strategies. Service provider networks are particularly vulnerable given the vital role they provide in interconnecting all aspects of society.

Inadvertent actions or malicious abuse by an insider are the most common source of security breaches. Insiders are generally trusted users such as employees, contractors and business partners. Often, well-intentioned insiders are responsible for costly service disruptions and security vulnerabilities (as a result of inadvertent network configuration changes). Malicious insiders are often disgruntled employees or contractors driven by financial or personal motives and often seek valuable or sensitive information that can be used to harm the organization.

Advanced threats from external attackers are increasingly being led by organized groups such as professional criminals attempting to gain access to valuable or sensitive information, state-sponsored groups engaged in industrial espionage or cyber warfare, and “hacktivists” pursuing a variety of social causes. These groups are all highly motivated, technically advanced, and are often well funded. Threats can be targeted towards the service providers, the wireless network (including the cloud platform where

applications run), or even the end devices. network (in this case wireless networks, the cloud platform where applications are destined to run or the end devices.

1. NETWORK SECURITY

CORE Network Security

As MSOs look into implementing a wireless strategy, it is important to understand that their networks could become a conduit for malicious online attackers to execute their exploits. The all-IP nature of LTE networks potentially reduces the strong security reputations that service provider networks once had with 2G and 3G networks. The online behavior and consumption of mobile apps by users exposes the network to malware attacks. Heavy Reading's October 2013 global survey of mobile operators showed that in a period of twelve months. around 60 percent of mobile operators had experienced malicious attacks that caused an outage or degradation in a major part of their network lasting at least one hour Examples of key vehicles used to target service provider networks include DoS attacks from external networks, GTP protocol anomaly attacks and attacks using reflexive and amplification. Other trends that impact an operator's network security include moving to the cloud, utilizing software-defined networks (SDN), implementing network functions virtualization (NFV) and joining the emerging Internet-of-Things market. The entry points of attacks into service provider networks continue to evolve but, among various core network interfaces, Gi/SGi and Gp/S8 interfaces have always been at the forefront of attackers' targets. The Gi/SGi interface is where the GPRS/LTE network connects to packet data networks including the internet. Since the subscriber's internet browsing patterns and deployed applications on the subscriber's device are outside the operator's span of control, operators inevitably expose their network at the Gi/SGi interface to all types of network traffic. Subscribers are then exposed to viruses, worms, Trojans, denial-of-service (DoS) attacks, botnets and other malicious network traffic. Exploitation of these vulnerabilities may result in network compromise which further causes loss of customer loyalty and trust, negative publicity and possible loss of sensitive data. Implementing security at the Gi/SGi interface as part of the mobile network infrastructure is imperative for maintaining a positive subscriber experience, brand reputation, as well as customer loyalty.

In addition to the issues listed above, Core networks are exposed to various security issues as a direct result of connecting to GRX/IPX networks via Gp/S8 interfaces. The GRX network, in theory, is a private network that functions as a hub that connects different mobile providers' internal networks but, in reality, a GRX network is accessible from the internet. These networks are exposed to attacks and network intrusions by unauthorized entities that can overtake hosts connected to the GRX network and use them to attack other connected nodes. On the other hand, GTP (GPRS Tunnel Protocol), which is considered to be the most important protocol in Core networks and carries almost all user operations and data, is itself not designed to have embedded security schemes. It has glaring security vulnerabilities which can be easily exploited by attackers. For example 'GTP over GTP' is s a typical attack which may result in the attacker's traffic reaching nodes in the Core network that should be inaccessible to roaming partners. Needless to say, that deployment of security controls is of paramount importance to enforce valid behavior of roaming partners and to protect Core network from malicious GTP traffic.

Generally speaking, reasonable organizational security measures are implemented inside the Core network. All network elements and links controlled by operators are not malicious or 'trusted' ; however, there is still a slight probability that an external attacker gains control of a network element inside the

PLMN. If so, they would then be able to abuse this network element for further "internal" attacks. Perimeter delineation of various domains (such as OAM, IMS, Charging, Value Added Services and S/Gi & S8/Gp) is a usual practice from a network point of view. Deploying security controls such as domain perimeter firewall & access control mechanisms are highly recommended to contain such internal attacks. Physical separation, which entails the separation and deployment of security devices at each domain perimeter, is considered more desirable than logical separation,. However, due to capital and operational costs, it is not generally implemented and is considered an ideal approach. A common strategy adopted consolidating these domain perimeter firewalls and various other mechanisms like virtualization, security zones, virtual routers and VLANs are leveraged to achieve adequate level of security.

Hence a security solution to protect the CORE network has to be optimized to provide robust security across each of the 3GPP interfaces or domains within Core networks, without affecting network performance. The solution should bring together best security practices to protect an operator's Core networks from attacks. The recommendation is to deploy next generation firewalls on the S/Gi interface, the S8/Gp interface & on other internal network domain perimeters. Any solution has to be developed by conducting continuous carrier-specific traffic pattern analysis and performance assessment testing in lab environments, as this allows for a performance-optimized and scalable Core Network Security solution.

The key elements of a well-thought-out CORE Network Security solution include:

- Pre-validated configurations to reduce deployment time and assure carrier- grade stability.
- Solutions designed specifically for service providers to ensure performance and interworking with other Core network elements.
- A Scalable solution which can be leveraged to offer revenue- generating security services to Enterprise and residential customers
- A Field- proven and blueprinted solution which has been benchmarked against Industry Standards and validated best practices.

Access Security:

The introduction of IP into Radio Transport networks and Mobile Backhaul networks has led to the deployment of an architecture that is inherently open. Unless this is addressed, an operator's core network is vulnerable to various known threats. These threats include risks of eavesdropping and unauthorized access to operator systems and worst of all denial of service attack that could pull down the whole operator network. For example; a malicious intruder may gain access to the Core or RAN from an Ethernet or optical port at an eNodeB site. This could be quite easily achieved as not all RAN equipment is located in a physically secure location. In a report by Gartner (Aug 13th 2014) on "LTE/VoLTE, Software-Defined Networks and the Internet of Things: Security Implications for Communications Service Providers" Gartner stated that by 2016, at least 50% of LTE networks will become key communication interception targets for organized crime, hactivists, casual attackers and fraudsters This represents a 5% increase from today's statistic."

The use of secure IP protocols (e.g. IPSec, TLS) is vital to ensure the confidentiality and integrity of the network traffic (payload and control data) as well as the availability of the mobile service. Authentication & Authorization of genuine networks nodes is also Furthermore, brand and regulatory compliance and other policies require tighter security controls when IP is used and the number of known attack vectors increase.

In LTE networks (LTE being the driver), the traffic between base stations and core network (S1 traffic) is all IP unencrypted traffic. This makes the mobile network vulnerable to several well-known threats. These threats can be categorized into five main categories:

- Eavesdropping on Subscriber Data.
- Unauthorized access to Operator core network
- Injection of malicious traffic (e.g. Signaling)
- Heightened Denial of service attack against EPC
- UE traffic interception and 'man in the middle' attacks

Nokia Networks Security Practice recommends the encryption of all traffic planes (User, Control and Management planes) from the base station to the core network. In order to achieve this, a specific Security Gateway (SEG) is placed in front of the operator's core network to act as a gate keeper, allowing only authenticated and authorized traffic into the core network, as shown in the figure below:

A time consuming scalability challenge for any operator is the management of thousands, possibly tens of thousands of IPSec within the operator network. The security solution has been designed to comply fully to the 3GPP (TS 33.310) and includes the mandated use of digital certificates via purpose built carrier-grade PKI to manage the connection of base stations to the SEG's. As seen in the figure below, the solution includes the PKI (Public Key Infrastructure) solution (also referred to as CA solution, Certificate Authority) that fulfills both the 3GPP requirements and the automation necessary in a service provider environment.

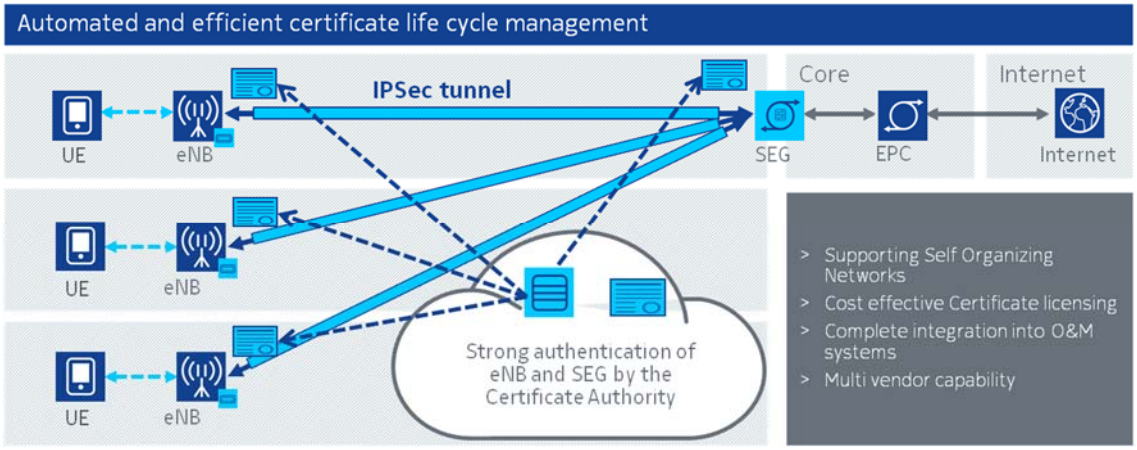

Figure 1 - Public Key Infrastructure Implementation

The deployment of a PKI system in a service provider environment can be regarded as a full green field for the operational teams of a mobile operator. It is imperative to tackle the technological aspect of a PKI , while also defining the processes required to operate this PKI in a RAN environment. PKI solutions are typically deployed in enterprise environments (such as Defense, Finance and Governmental), and transforming the PKI to run in a service operator environment presentments certain challenges. These challenges and their mitigations can be seen below. ..

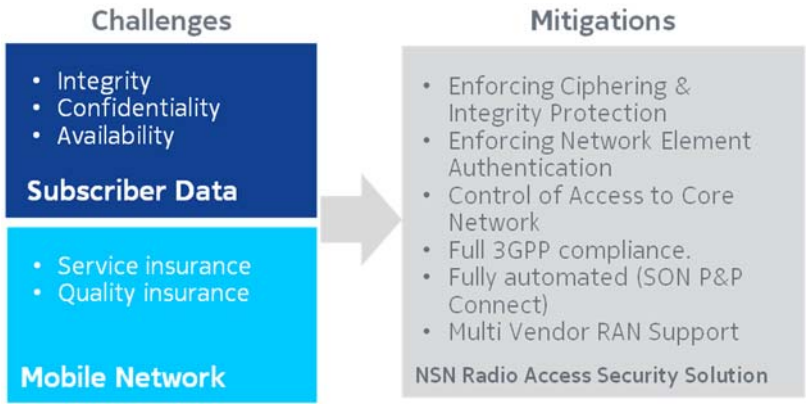

Figure 2 - Security Challenges and Mitigation

As MSOs look into the deployment of Small cells in licensed, lightly licensed (3.5G, GAA) or unlicensed mode, these networks are prone to similar security exposures. The closer a network element is deployed to the end subscribers, the higher the security risk, because the operators' physical security standards and security processes cannot be controlled as shown in the figure below. . Hence, small cells' access into mobile operator networks must be secured.

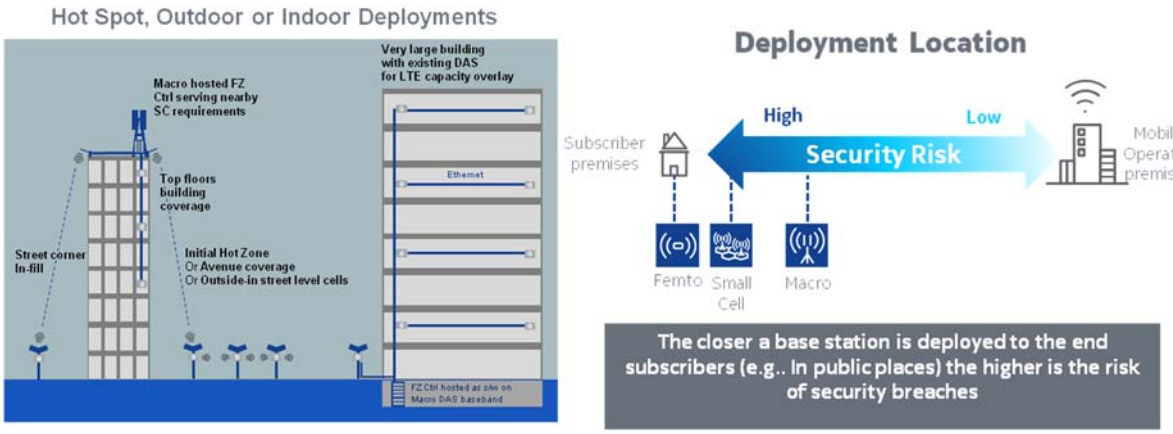

Figure 3 - Small Cell Deployment and Security Risks

The Access security solution should offer comprehensive protection combined with high performance and availability. The 3GPP-compliant solution secures data between the base station and core network with IP security (IPSec). In addition, strong certificate authority using Public Key Infrastructure (PKI) ensures that only operator-authorized base stations can access the network. The solution should include Certificate Authority and Security Gateways as hardware/software components as well as services covering the solution's full life cycle, from architecture and design, to implementation and support.

The key elements of a well thought out access Security solution includes:

- Complete end-to-end security solution with live deployment experience
- Built-in IPSec in the eNodeBs with high throughput ensuring highest performance.
- Pre-validated LTE RAN solutions
- Efficient operation through fully automated certificate life cycle management for both eNodeB, Small Cells, and Security Gateway.

For certificate and key management, a it is essential to deploy GPP standards-compliant Public Key Infrastructure and Certificate Authority (CA) Solution, which generally have the following key features & capabilities as highlighted below:

- Per 3GPP requirements, X.509 certificates are employed to authenticate Security Gateways and eNodeB's for enrollment and IPSec communications in the network.
- Nokia's INSTA PKI solution is fully automated, with support for Secure Self Organizing Networks (SON) functionality and centralized certificate management procedures.
- Nokia's INSTA PKI solution employs tamper-resistant FIPS 140-2 compliant hardware security modules to secure the private cryptographic elements used to authenticate all eNodeB's and IPSec tunnels in the radio network.

1.1. Virtual Firewalls

Virtualization is increasingly seen as a way to meet the constant pressures for cost and requirements for agility. It is vital that a security solution can support this direction. A key decision required is whether to use technology created for the physical world or to deploy a solution that has been designed to meet the new challenges virtualization brings.

Deploying a virtualized solution offers many advantages. The model for redundancy and failover can be ; different; a plethora of hardware can be used to create a solution with which one can turn up instances of virtual infrastructure across the network very rapidly., It is optimal to implement a firewall solution that only incurs cost for the traffic that passes thought it and a firewall that encourages the adoption of the best design practice of segregating the security zones onto different physical infrastructure. Above all, it is imperative to implement firewall solution that has been designed for a service provider environment with the emphasis on reliability and scalability rather than a range of features aimed at Medium Sized Enterprises.

The basic security principles remain when deploying a virtual firewall. It is important to separate data plane and control plane traffic to ensure that device management is separated from through traffic to make sure network traffic does not compromise the firewall. This model can then allow for cores to be scaled in and out independently for data plane and control plane traffic. A dynamic deployment model will allow virtual CPU's to be allocated to each plane to meet the operator capacity needs.

A side benefit of dynamic vCPU deployment is that the firewall can be optimized for the characteristics of the traffic at that point in the network. For example, allocating more cores to the control plane can increase IKE negotiation rate capabilities while more cores allocated for the data plane functions typically increase packet forwarding performance. When looking at a virtual firewall it is important to check that the behavior is generic so that all cores can perform any type of work. This way, if there is an unexpected load of a certain type of traffic it can be handled better using the resources available. An example would be if all cores having the ability to handle fragmented traffic compared to if only one, or few cores can handle specific types of traffic.

To implement these design principles quickly within one's environment there are certain aspects that need to be considered. First, the NFV infrastructure must be able to instantiate VNFs in the right locations at the right time. Then the security functions must be dynamically implemented and adjusted based on topology information coming from Cloud Orchestrator. Thus integration with an Orchestrator becomes a fundamental requirement. This is where it is important that the device you choose has been designed for a cloud environment.

One of the downsides of an agile network deployment is that the firewalls may not have been thoroughly tested in a service provider environment. Given the importance of reliability to any operator they cannot accept the level of risk that an enterprise can. To reduce time taken by the traditional testing method it is worth ensuring that the device one chooses has been subject to extensive testing in a service provider environment from an organization with a pedigree in this field.

The architecture of the Firewall helps one to adopt a more agile deployment methodology resulting in quicker time-to-market. It should integrate into orchestration and hypervisor solutions. Not only does it let one determine how many cores are allocated to control and data plane functions but it allows to dynamically alter the number of cores as the needs change and the service provider's network grows. To achieve faster throughput than the traditional virtualized system provides, Virtual Firewall can supports

packet acceleration technologies: Single Root Input Output Virtualization (SR IOV) and PCI-pass through or DirectPath I/O. With SR-IOV, Virtual Functions have near-native performance and provide better performance than para-virtualized drivers and emulated access, without the need to dedicate a separate physical NIC to each individual virtual machine. PCI-pass through or DirectPath I/O allows the direct assignment of a PCI device (i.e. NIC) to a VM instance which bypasses hypervisor. While both behavior types are supported to allow for maximum deployment options, SR-IOV offers more flexibility than PCI pass through or DirectPath I/O.

Careful design of the firewall allows for robust optimization, performance and security. First, CPU isolation allows for direct and exclusive assignment of vCPU cores to the Virtual Firewall. Inside the VNF, CPU pinning enables direct core access for specific threads (e.g. Control Plane, scheduler, Data Plane).

The CPUs are isolated so that neither the OS nor the hypervisor will use isolated cores for its own tasks. Furthermore they will not share isolated cores among other VMs. This end result is a significant improvement in robustness, memory access (two times faster) and the overall speed of VNF. These are some of the core principles when implementing a virtual firewall strategy.

1.2. Domain Names System (DNS) Security

The increasing number of IP addresses required by network elements and devices, along with increasing security threats to networks, has put an increased emphasis on the need to deliver IP addressing and management mechanisms that are both automated as well as secure. Hence comprehensive, secure, and highly available DNS/DHCP solution for network IP address assignment and resolution becomes a key requirement.

A secure DNS solution protects the network by providing Secure Response Policy Zones (RPZ's) for listed domains, including Transport, EPC, Roaming, and SGi. In addition, Secure DNS Solution should provide comprehensive protection from multiple avenues of DNS-based attacks, including Volumetric & D/DoS attacks (e.g., DNS Reflection, DNS Amplification), as well as DNS-specific exploits (e.g., DNS cache poisoning, DNS tunneling). The Secure DNS solution should also provide centralized DNS management, along with in-service security upgrades, enhancing the overall reliability and resiliency.

Hence a comprehensive DNS/DHCP solution provides multiple features, capabilities, and benefits for the service provider, including:

- Built-in support for DNS, DNS-SEC, DHCP, FTP, TFTP, HTTP, HTTPS, and NTP
- Advanced DNS Protection and DNS Firewalling mechanisms to protect against DNS-Based DoS/DDoS attacks
- Full support for IPv4, IPv6, and dual-stack IPv4/IPv6
- Centralized management of distributed DNS/DHCP appliances
- Synchronization of distributed DNS/DHCP appliances
- Highly efficient and automated IP address management
- Secured role-based administration and hardened OS to prevent root access and reduce vulnerability to network attacks

1.3. IP Multi-Media System (IMS) Security

As MSOs look into implementing a converged IMS strategy, where a single IMS implementation can provide services across both the cable broadband network and wireless networks, securing the IMS Domain becomes even more critical. Network Perimeter and Domain Firewall Solutions will provide complete security, protecting against multiple cyber attack vectors including D/DoS, Protocol Encapsulation, Fragmentation, IP spoofing, and malformed packet attacks. IDS/IPS, security logging, and content inspection/filtering are also supported in the firewall solutions.

A Secure DNS Solution, when implemented as described above, will also protect the IMS Domain by providing Secure Response Policy Zones (RPZ's). In addition, a Secure DNS Solution provides comprehensive protection from multiple avenues of DNS-based attacks, including Volumetric & D/DoS attacks (e.g., DNS Reflection, DNS Amplification), as well as DNS-specific exploits (e.g., DNS cache poisoning, DNS tunneling). A typical Secure DNS solution also provides centralized DNS management, along with in-service security upgrades, enhancing the overall reliability and resiliency.

1.4. End to End Security Management and Logging

Securing large, multi-vendor, multi-technology networks is a daunting task and requires a consistent set of security procedures and policies that are diligently followed. Hundreds of network operations personnel as well as external contractors and equipment vendors are required to access, manage and maintain large networks. These consist of hundreds of thousands of physical and virtual network functions, and operations systems.

Simple tasks like changing default passwords, or rotating passwords, become cumbersome. As networks change and expand, service providers find it challenging to respond to the business priorities that require frequent configuration changes. The potential for committing errors increases dramatically. Moreover, a simple error in a configuration could introduce serious security vulnerabilities. Typically, there is no way to control access device configurations based on user role, and checking or preventing unauthorized configuration changes is problematic. When something goes wrong due to a faulty configuration change or when a security breach occurs it is possible to trace the actions to a particular individual in the absence of audit trails. The sheer scale of service provider networks compounds these challenges. There are simply so many disparate network elements, such as small cells in mobile networks, customer premise devices, and now virtual machines and network functions. Keeping track of which systems may have modified configuration data has become almost unachievable. But as networks continue to expand and change, and as the conventional definitions of a perimeter disappear, cyber-security attack surfaces and attack vectors continue to grow.

Hence, the elements for end-to-end security management solution should include :

- An Access Guard solution that provides protection and security management of network elements, through multiple mechanisms, including:
    - Multifactor authentication for NOC personnel login
    - Bulk password rotation and common password format enforcement
    - Role-based workflows, which define specific network elements NOC personnel may access based on security policy

- Comprehensive audit trails, with logging of accesses into all network elements in the network, including video logging of GUI access

- A NetGuard Security Management Center solution that is typically compliant to ITU-T M.3410-compliant security management system implementation for Next Generation Telecommunications Networks. Such a solution would include comprehensive system-wide security management capabilities, including but not limited to:
  - Security status visualization
  - Incident management
  - Vulnerability management
  - Security policy management
  - Network access management
- And finally a Security Information and Event Management (SIEM) solution that supports comprehensive data and flow-based collection and analysis capabilities. Such a solution should also provide multiple security management capabilities in the network, including Log Management, Threat Management, and Compliance Management.

To mitigate insider threat, the security solution should provide protection against insider attacks at the Networks Operations Center level through advanced security features, including:

- Fully traceable per-user single-sign-on, preventing sharing of login credentials
- Multifactor authentication for login
- Consolidation of multi-vendor network management security policies into a single coherent policy (e.g., standardized password structures and password renewal timeframes)
- Role-based workflows which restrict access to network elements based on assigned credentials and role for the user in the network
- Bulk password rotations, preventing attacks to the system from compromised login credentials
- Standardized and comprehensive logging of access into all network elements in the network, including video logging of GUI access.

2. CLOUD SECURITY

The business challenges faced by communication service providers are well known: revenues remain threatened by increasing competition from both traditional and new competitors. There are urgent needs to develop new service offerings to drive new revenue growth while improving operational efficiencies, and shrinking costs. As a result, service providers are turning to new technologies such as Network Function Virtualization (NFV) and Software Defined Networking (SDN) along with new business models as mechanisms to increase revenue while reducing operating costs.

As part of their MVNO strategy MSOs may deploy their own Evolved Packet Core (EPC) infrastructure and integrate that EPC to their existing IMS network elements. They may also deploy application/messaging servers and media servers to provide a comprehensive wireless service offering. In the past, networks were built on customized and purpose-built hardware and software. The technical knowledge required to compromise a given network was contained within a very small community, and there were limited motivating factors to encourage hacking. Similarly, network equipment and associated functionality was vendor- and domain-specific, with a small number of entry points, further limiting its exposure to external security risks. Today, the move to all-IP networks has resulted in mobile and wireline networks becoming more vulnerable and exposed to the same types of threats that afflict any server reachable over the Internet.

SDN, like many new technologies, introduces security challenges. SDN involves the functional separation of control and forwarding planes. Securing the interfaces between centralized SDN controllers and the underlying network elements or network functions is crucial to ensure that rogue, malicious instructions dictating how traffic flows across networks are not injected.

NFV completely changes how networks are designed, built and managed. It pulls the functions necessary to run networks off of proprietary hardware and places it on servers that can be deployed where they are needed most – in data centers, mobile base stations, as well as customer premise locations. This combination reduces cost but also dramatically increases the attack surface for security attacks, and increases security administration costs and complexity.

NFV is a transformational technology being embraced by service providers. Cost improvements, operational efficiency, and accelerated new service introduction times are some of are some of the market drivers as to why NFV is an integral evolutionary step for most service providers. Some of these efficiencies are achieved by optimizing equipment and infrastructure costs through consolidation of network functions, while exploiting economies of scale from the IT industry.

The standards body ETSI has defined a generic architecture for NFV including management and orchestration (MANO), virtual network functions (VNFs) and virtual network infrastructure (NFVI) which allows service providers to deploy network functions as virtualized software instances instead of dedicated hardware appliances. These software-based network functions can then be driven off of industry-standard high-volume servers, network, and storage platforms. These can be located in data centers, distributed central offices or points of presence, mobile base stations and customer premise locations.

Multiple Administrative Domains

Unlike traditional hardware-based networks, with NFV the hard boundaries that existed between physical network functions are now blurred, making defining and administering security roles and responsibilities

more complex. There are multiple levels/domains that need to be addressed, such as the NFVI (including the hypervisor), VNFs, and VNF managers and orchestrators, as well as external systems such as OSS and policy systems. Administration of roles, responsibilities and privilege levels will become more critical and challenging in this complex environment

NFV purists believe that management of virtual networks will be simpler. In some ideal, future state, humans will never have to log into networks. The network and communications will be automated, resulting in improved security outcomes. Conversely, pragmatists believe this is unlikely and humans will continue to control processes and resulting changes to networks. The likely reality is that automation will increase but humans will still need to access network resources manually. Configuration errors will continue to occur, provisioning issues will continue, and troubleshooting complex issues will still require human correlation. The definition of identity access management needs to evolve to encompass both people and processes. Administration of who, or which system can view, set, or change configuration parameters and effect network policies becomes vital. This is especially important given the interdependencies between NFVIs and VNFs, and overall service performance and availability. Moreover, as multiple automated software systems access the same shared pool of network resources, assuring that security permissions and policies do not conflict will be crucial. Software enabled provisioning processes can lead to orchestration vulnerabilities including network configuration exploits and malicious configurations.

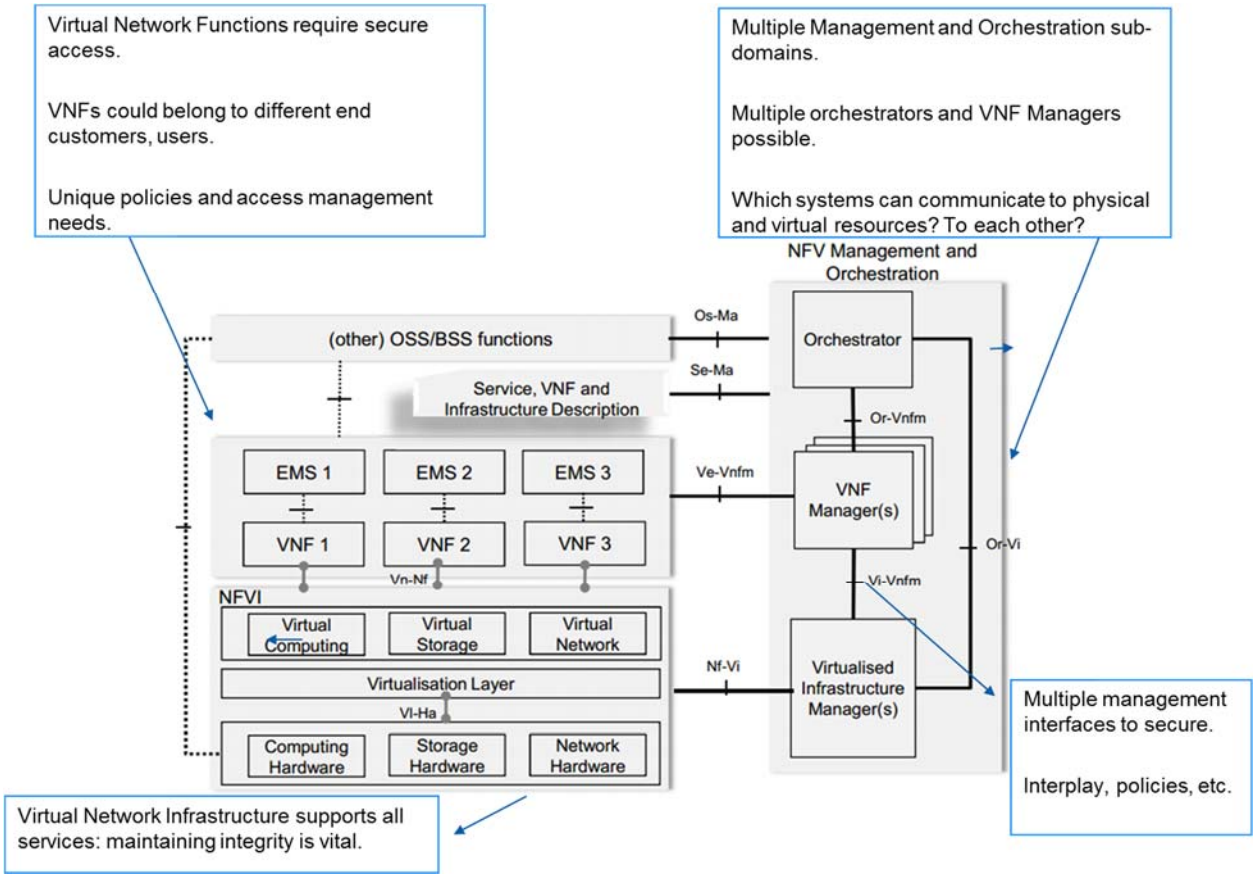

Figure 4 - Potential NFV Security Vulnerability Points

Maintaining Virtualized Infrastructure Configuration Integrity with Multi-tenancy

Multi-tenancy environments pose significant challenges when trying to maintain configuration integrity, and common cloud infrastructure could easily have hypervisor vulnerabilities introduced as a result of integrity failures. Virtual Machine, guest OS, or VNF manipulation could also compromise the integrity of the hypervisor. It will be important to log and monitor hypervisor activities. Similarly, it will be important that VNF configurations themselves are audited to understand whether configuration or operating system changes may have an impact to security integrity.

An important driver for NFV is to create a more flexible and elastic network to enable new service provider business models and revenue opportunities. VNFs will be instantiated, retired, or moved in a more dynamic fashion in order to meet the service delivery requirements. New business models could include VNF, or VNF-as-a-Service, whereby service providers could host different 3rd party VNFs within their own distributed, virtualized infrastructures. Some NFV implementations may involve hosting VNFs from different 3rd parties within a common service provider virtualized infrastructure. Without periodic integrity auditing, VNFs could be arbitrarily instantiated by Virtual Infrastructure Managers on suitable or available hypervisors. This could create vulnerable co-residency scenarios should the hypervisor become exploited or the security policies not be applied properly to the respective VNFs.

Retiring or removing VNFs is equally critical as some VNFs inadvertently left instantiated could result in security breaches or result in susceptibility to Denial of Service attacks. For instance, VNFs may be instantiated for temporary troubleshooting or service testing during service activation. These may include virtual test agents, traffic generators, virtual taps, and packet analysis. If they are mistakenly left instantiated or fail to be retired by an automated process, they can be exploited maliciously or inadvertently during routine network maintenance, resulting in service disruption and extended operational expenses.

Clearly, maintaining configuration integrity will be necessary in order to meet regulatory and compliance requirements, which will be increasingly challenging and potentially expensive in virtualized networks.

Expanded Attack Surface

The aforementioned scenario becomes even more challenging when multi-cloud or multi-site NFV is considered. Technology miniaturization and cost improvements, combined with latency sensitive application requirements, results in a network-wide distribution of virtualized computing and storage assets. The virtual network may span from data centers, remote points-of-presences, to mobile base stations, and to customer premise locations. Not all VNFs are suitable to be centrally hosted for a variety of reasons, including latency, bandwidth and performance. The resulting architecture is very effective and practical for hosting various types of VNFs and changes the conventional definition of a security perimeter.

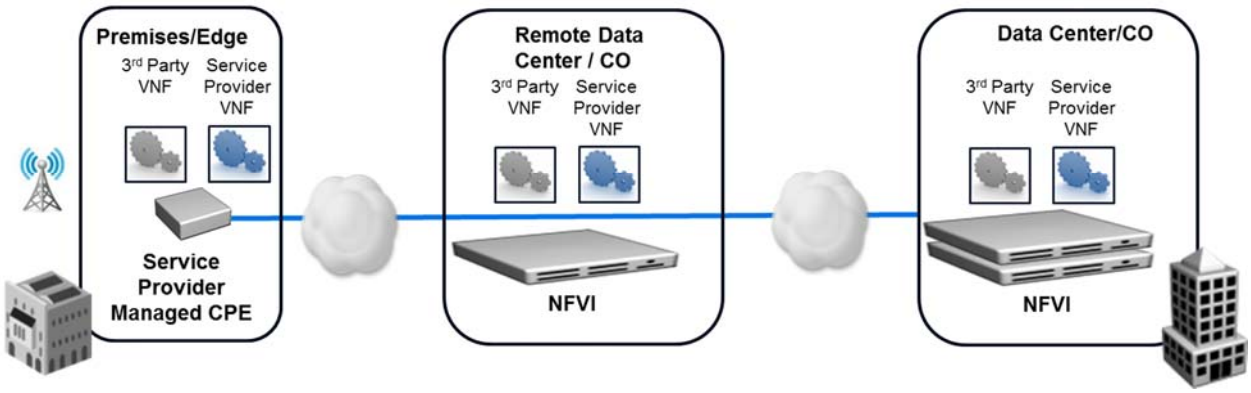

Figure 5 - Distributed Cloud's Expanded Attack Surface

Perimeter-based threat protection approaches such as network, web and endpoint security will be insufficient in these increasingly complex and sophisticated network environments

Hybrid and Distributed Networks

In the ETSI NFV model, part of the Management and Orchestration (MANO) role is to provide lifecycle and VNF management. Many VNFs themselves will be security virtual appliances. While it is clear that a NFV orchestrator will manage these like any other class of VNF, it is less obvious how security orchestration may be implemented for the VNFs, for NFVI, as well as for the OSS, BSS, EMS and MANO components themselves including orchestrators, VNF managers, and Virtual Infrastructure Managers. For instance, many service providers are envisioning domain-specific orchestrators (e.g. mobile/wireline or business/consumer services may have their own unique orchestration implementations) or a federation of orchestrators may be necessary simply because of scale (e.g. metro, regional, national and global networks may have unique orchestrators).

Ultimately, end-user services will traverse a combination of networks (e.g. mobile and wireline), regions (e.g. metro, regional, national and global) and technologies (e.g. traditional physical networks and virtual networks). Services and service chains will be complex, spanning shared infrastructures, physical networks, locations, and clouds. It will be important to administer and maintain service-oriented security privileges and policies to ensure that the right systems, processes, and people have the appropriate access end-to-end in order to turn on, manage, optimize, and troubleshoot services.

Maintaining security integrity needs to be part of a holistic service assurance strategy, requiring a service-driven and contextual view of security access control policies.

Organizational and Business Processes Complexity

Service provider networks are inherently complex and heterogeneous, and could consist of the following:

- Multiple services: consumer, commercial
- Multiple markets: metro, regional, national, global
- Multi-domain: mobile, wireline, content

- Multi-technology: cable, fiber, copper, 3G/4G/5G, Wi-Fi
- Multi-vendor: many unique hardware and software suppliers per domain, per technology
- Multi-generational: legacy technologies and products
- Multi-protocol: IP, MPLS, Ethernet and legacy protocols such as TDD, ATM and Frame Relay

The network complexity is often mirrored by complex operations and business processes, with distinct management and operation silos. Compounding this is the financial pressure to reduce operational costs. As a result, outsourced managed network services are increasing in popularity. Increasingly, service providers are outsourcing network installation, field operations, and network operating centers. In some cases, application and service delivery are also outsourced. As a result service provider networks, equipment, and systems are being accessed not only by employees, but also by third parties including partners, suppliers, and customers.

Dynamic Access Policy Management

Granting user access to a wide range of resources through strong authentication measures still poses risks. Once granted access, a user may be logged in for an extended period of time. If the user is a partner, supplier or other third party, it may be more challenging to enforce security best practices-at a minimum, it will increase the cost of creating, maintaining and enforcing SLA's in the future. Maintaining the integrity of the security policies requires role based identity management. Identity access management policies are necessary to control access to resources depending on the type of user and the context of the user access request. Possible factors to consider include the identity of the user, the location of the user's access, and the user's roles and privileges.

Rapid Provisioning and De-provisioning of Users

Given the fluid and dynamic nature of modern software defined networks, the management of user accounts and privileges must also become agile. User and system access cannot be persistent. It will be important to be able to grant access privileges rapidly and even more critical to disable all access when the association ends. Examples of this situation include an employee resigning, a 3rd party completing maintenance or troubleshooting, or an automated management and orchestration system completing its tasks.

Recommendations

An integrated Identity and Access Management solution that spans physical and virtual networks, and the associated OSS, BSS and management and orchestration systems is needed. Virtualization introduces multi-tenancy with the need to establish flexible role-based security policies for both humans and autonomous systems. There are now multiple layers of interdependencies (e.g. MANO, VNFs, NFVI, physical network functions), which will drive more complex policies. Domain isolation between these different slices will be needed, along with flexibility to create access management rules as needed. Network implementations, services, and operations practices will vary by operator, service, and region, so access management solutions must be adaptable and flexible.

Single sign-on (SSO) is a critical need. SSO facilitates both ease of use and administration simplicity, but also allows for rapid response and control to change and revoke access. SSO supporting role based identity management is crucial.

Service providers must rank scalability and availability requirements highly as they operate mission-critical networks. Identity access management strategies need to accommodate a variety of network equipment, multiple generations of technologies, scale to support thousands wide variety of equipment types, virtual infrastructure, virtual network functions, servers, and systems. Conventional systems designed for enterprise applications often lack the scale, performance, and availability needed for service provider networks.

Network behavior analysis will be an integral part of next generation security strategies. Autonomous management and orchestration processes will result in more dynamic and fluid networks. Virtual network infrastructure configuration changes will be frequent, and virtual network functions will be instantiated, retired, changed, and moved more dynamically. The automated systems and humans accessing network resources used to activate, change, monitor and troubleshoot services will grow. It will be vital to correlate network configuration and service parameter changes with security events. This will be crucial to pin-point configuration changes which may create security risks and to rapidly identify network access resulting in malicious attacks.

3. END-POINT SECURITY

With the growth of smart devices, the threats known from the IT world are moving to the mobile world. People have their devices with them everywhere they go, with all sorts of private information stored on them.

Unlike in the IT world, mobile subscribers have low awareness of the security threats coming from malware. For example, subscribers are often interested in getting free premium applications, offered by the multiple existing app stores. They are unaware, however that the probability of malware infection ranges between 2% and 63%, as cybercriminals can inject malware such as Trojans on legitimate apps which continue to work normally, but perform malicious activities alongside.

This lack of awareness leads to low installation rate of antivirus systems on mobile devices. Moreover, for some types of devices there is no antivirus available, either due to the vendor not allowing the installation (e.g. on iOS devices), or because the devices are not powerful enough to host an antivirus system (e.g. IoT devices).

Smart phones have added to the challenge, as they have become the main interface to the Internet, through which social networks and mobile applications can act as a route for mobile malware. The billing association between the operator and the subscriber makes a particularly attractive target for criminals, intent on introducing fraudulent malware.

The “McAfee Labs Threats report 2015” states that mobile malware doubles year-on-year, while “Kaspersky Security Bulletin 2014” claims a 4-fold increase on Android malware, peaking in a 9-fold increase in mobile banking Trojans. Clearly, security threats to mobile broadband operators and their subscribers are to be taken seriously, especially in the transition to all-IP networks, which require dedicated measures to protect both networks and subscribers.

Providing an effective protection requires the end-to-end integration of network-based and device-based solutions that take into account the specific aspects of the mobile domain. According to Nokia’s Acquisition and Retention Study 2013, security was one of the top priorities (#3) for new services. Also services such as m-commerce and m-health require security, so securing the network and end users becomes an avenue for new business.

Operators have a close relationship with their customers, who have a high level of trust in their providers and high expectations for security. This unique position gives operators the chance to provide security and differentiate by protecting their customers from security risks. Service providers have the option to provide a network- based device security solution which would protect subscribers against fraud, even when they do not have any anti-malware software installed on their smart devices.

Such a network based solution uses data on the use of services such as voice, SMS and mobile broadband, and analyzes network traffic patterns, working faster than conventional systems that employ signature mechanisms and other generic methods to detect malware. Once detected the solution also notifies the user, blocks the affected services on the network, and helps subscribers cleanse their smart devices. One of the key capabilities is to correlate suspicious network traffic patterns to known threats, building on trusted malware intelligence. Self learning techniques are used to detects new malware earlier than conventional signature recognition, enabling immediate action to improve protection of smart devices.

After detection, the solution can automatically contain the malware's activities, for example by preventing premium rate SMS messages from being sent, or blocking unauthorized mobile payments. The subscriber will then be alerted of this contamination, and can optionally opt in to software to disinfect the device and provide further protection to complement the network-based defense.

Key Deliverables

The two main components of this network-based solution are a security dashboard and an Action Engine

The Security Insight dashboard gives the operator a view into the status of the malware on its network. The real-time dashboard shows which were the most relevant malwares e.g. in the last minutes or hours, as well as the most affected locations, device types, and IP destinations. It also shows the "malware" events (each time that a malware activity is detected) and various statistics such as who are the infected subscribers, which are the key premium SMS malwares, etc. The monitoring dashboard is typically customized for mobile broadband operators to provide detailed infection data in real-time, as well as the list of infected subscribers and several statistics correlated with Telco information, such as the most affected locations or phone models.

The other component is an automated Action Engine. For each infected subscriber, there will be a workflow in order to help the subscriber in an automated way. It may, for example, send an SMS informing the subscriber about the infection, block his/her access to VAS (value added services) or advise a one-time scan to clean the malware. When employed to protect corporate customers, the solution can also provide a view of the infection state of this customer's mobile device and reports across the entire corporation.

Such a network-based solution can optionally provide a device antivirus program that is able to clean the malware and reduce the probability of infection in the future. To address data privacy issues relevant in many countries, the solution should support 'white lists' of subscribers that have opted in for the service to be monitored. For all other subscribers, only statistical data should be collected, but no trace-back of findings to individual subscribers should be made possible. All privacy related information about such events should be either irreversible hashed, or not stored or displayed at all.

A network-based device security solution should also provide support for detecting malware on IOT devices, by comparing communication patterns of these devices against associated profiles. For example, in the case of an electric vehicle charger, the device in the car should communicate to the charging station via a central middleware server. Any deviation from that traffic pattern, such as . sending notifications to other destinations should be considered as malicious activity.

A Device-Independent Solution

A device independent solution allows operators to see the security status of the device on the network, while also enabling them to provide proactive support for infected subscribers.

The other advantage for operators is the chance to increase revenue by selling device security packages. It also helps to avoid misuse and fraud, cuts the number of support calls the operator needs to answer, and protects the reputation of the brand.

The chance to address new markets such as mobile payment,; achieving reduced time between infection and mitigation; and gaining a cleaner network are all further advantages of such a solution.

For subscribers, the solution offers the best available protection against malware, combining network and anti-virus protection. By providing immediate information to users when their device is infected, the solution prevents bill shock and gives users peace of mind

The traditional device antivirus uses signatures to detect malware. A signature is a set of characteristics that identifies malware, such as filename, size, pieces of code, etc. The inconvenience with signature-based detection on the device is that one type of malware might have thousands of variants (e.g. another filename, small changes on the code), meaning that when a new variant appears, there is a time gap until the antivirus DBs are updated. It is during this time gap that the malwares are particularly dangerous, as they are not detected by the device anti-virus.

Thus, best-in-class protection can be achieved by combining network-based fraud detection (device-independent prevention) and the classic antivirus approach on devices.

Overview of a Network Based Solution

The following provides details of a network based solution as described above. The solution provides real-time analysis and insight into active malware within the Operator's network. It is based on a Correlation Engine, receiving information from network data taps, a Dashboard presenting correlated data related to malware events, and an Automated Action Engine that can take proactive actions to help infected subscribers.

The Correlation Engine uses external Context Data to provide intelligence on current threats in combination with operator specific data, to inspect network traffic from standard interfaces on core elements such as GTP data flows from the GGSN and Short Messages from the SMSC.

The solution also typically offers an optional device antivirus package that is able to clean the malware and reduce the probability of an infection in the future.

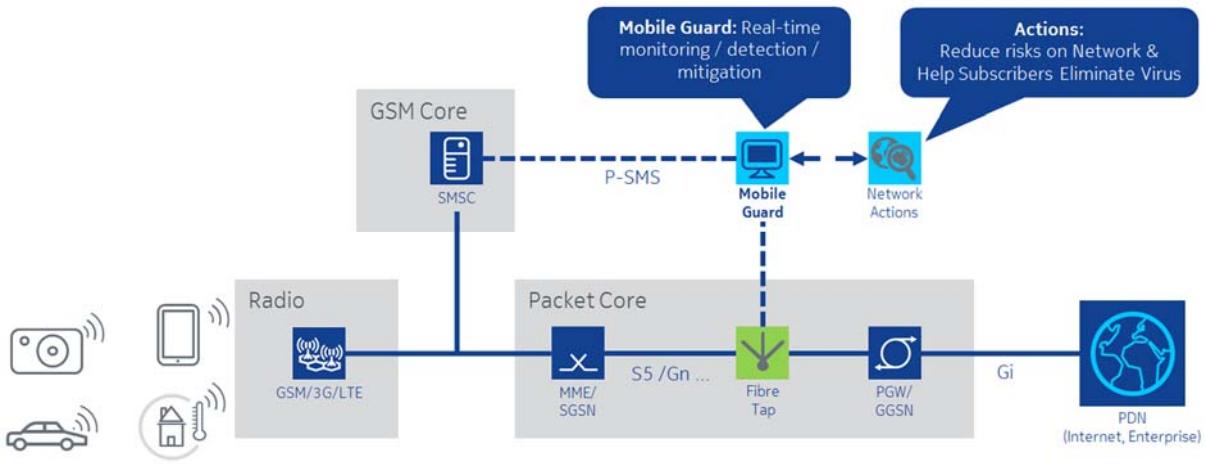

Figure 6 - Network Based End-Point Security Implementation

The malware intelligence database is updated by evaluating multiple information sources to build specific knowledge for the identification of malware activities. Malware samples are typically collected by honeypots, which are specific computers that emulate vulnerable systems to attract malware to infect them. The analysis tries to extract various types of information about the collected malware samples such as IP addresses and communication capabilities between bots and malicious hosts such as command and control servers, drop zones and servers offering fraudulent services (including phone calls and premium SMS messages). Other factors including data mining metadata received from various sources, and closely monitoring the attacker's activities are considered while building the threat database.??

A simplified sample analysis would be as follows:

1. The system receives files and metadata related to malware and benign objects.
2. The system automation engine processes this data by using static and dynamic means and the facts are extracted.
3. The facts go through various clustering algorithms.
4. The rules engine, operated by analysts and researchers, makes millions of automatic decisions per day to give a verdict whether an object is good or bad.
5. The clients in the devices query these verdicts from Security Cloud to get instant protection, or in some cases part of these verdicts are distributed to clients locally to provide protection even in situations where no network connectivity is available.

Correlation of traffic patterns (detection)

The "Correlation of traffic patterns" recognizes both known and new attacks by identifying anomalies, e.g. characteristic patterns in the network operation associated with malware attacks. Amongst others, anomalies include suspicious DNS requests, large amount of email (spam), frequent sms messages, etc. The monitoring process includes packet inspection and the evaluation of traffic attributes.

Potential new attacks will be reported in a feedback loop to the Analysis building block and may lead to the definition of new malware samples, thus providing continuous improvement of the detection capabilities.

The Dashboard is responsible for the orchestration of all tasks requiring interaction between the building blocks. It is the central point for managing the solution and can be implemented as a remote or local installation – depending on the operator's needs.

The Dashboard presents the Operators Security teams with an up-to-date, real-time view on current active threats within the network. The information is categorized by types of malware, Operating Systems, subscriber location, destination and device types. It is possible to drill down further into the displayed information and gain access to several types of statistics.

Threat Mitigation

The Mitigation limits the impacts of malware and BotNet attacks by using an automated actions workflow for each infected subscriber. This approach includes:

- Identification of infected devices and the subscribers owning these devices.
- Notification of the subscribers via email, sms, phone or web re-directs.
- Quarantining the rogue devices.

- Inhibiting the communication between the bots and the command and control infrastructure of the BotNet by blocking of IP addresses, domains or protocols.
- Providing information related to disinfection.
- Activating automated disinfection tools.
- Warning the customer care about the infected subscribers.

Threat Prevention

The Prevention building block aims to avoid new malware infections by using a device antivirus. Besides the antivirus protection, the following functionalities are also available:

- **Antitheft:** protects the device and the data by offering a remote lock, wipe, alarm, and possibility to locate over an SMS or from a web portal.
- **Browsing protection:** protects end-users from malicious websites and phishing attacks.
- **Parental control:** allows parents to control the type of websites that children can browse as well as to query their location.
- **Safe Applications:** widens the parent's ability to control the applications; new applications can be used only after the user has been authorized by the parent.
- **Anti-spam:** blocks unwanted calls and messages.
- **Anti-virus/anti-spyware:** keeps the device clean of harmful viruses and applications.
- **Backup** (optional): protects the irreplaceable content on the device, like pictures and videos.
- **Messaging agent:** gives promotional capabilities to the operator.
- **Automatic updates:** keep the mobile security always up-to-date.

Conclusion

As described in this paper, a comprehensive security strategy as part of the overall wireless strategy has to include three domains: Network, Cloud Platforms and End-Point. A security solution to protect the CORE network has to be optimized to provide robust security across multiple interfaces or domains within Core networks, without affecting network performance. The solution should bring together the best security practices to protect the operator's Core networks from attacks, and the recommendation is to deploy next generation firewalls within and across other internal network domain perimeters.

MSO's are in the process of deploying cloud platforms with SDN/NFV as they move towards a virtualized world where most physical network functions will run as virtual network functions on those platforms. In order to realize the full commercial benefits of new technologies such as NFV, identifying and overcoming some of the practical and critical operational considerations will be required. Security is one critical operational aspect that will quickly come into focus. Securing NFV must not be an afterthought if full benefits are to be realized. The definition of Identity Access Management must evolve, extend to systems, as well as people, and take into account the expanded and fluid attack surface.

Finally, service providers have the option to provide a network based device security solution which would protect subscribers against fraud, even when they do not have any anti-malware software installed on their smart devices. A device independent solution allows operators to see the security status of the device on the network while also enabling them to provide proactive support for infected subscribers. The other advantage for operators is the chance to increase revenue by selling device security packages. It also helps to avoid misuse and fraud, cuts the number of support calls the operator needs to answer and protects the reputation of the brand. For subscribers, such a solution offers the best available protection against malware, combining network and anti-virus protection. Providing immediate information to subscribers when their device is infected, the solution prevents bill shock and gives users peace of mind.

Abbreviations

AP	access point
bps	bits per second
DoS	Denial of Service
EPC	Evolved Packet Core
FEC	forward error correction
HFC	hybrid fiber-coax
HD	high definition
Hz	hertz
IMS	IP Multimedia System
ISBE	International Society of Broadband Experts
GPRS	General Packet Radio Service
GTP	GPRS Tunneling Protocol
LTE	Long Term Evolution
MSO	Multiple System Operator
MVNO	Mobile Virtual Network Operator
NAT	Network Address Translation
NFV	Network Function Virtualization
RAN	Radio Access Network
SEG	Security Gateway
SDN	Software Defined Network
SCTE	Society of Cable Telecommunications Engineers
TLS	Transport Layer Security

Bibliography & References

1. Heavy Reading's on global survey of mobile operators. October 2013
2. Gartner on “LTE/VoLTE, Software-Defined Networks and the Internet of Things: Security Implications for Communications Service Providers”, August 2014
3. The “McAfee Labs Threats Report, 2015”
4. Kaspersky Security Bulletin, 2014

