

IPTV



Security and Reliability Challenge

IPTV is susceptible to the same attacks and reliability problems that plague other IP-based data and VoIP services. Codenomicon DEFENSICS for IPTV preemptively analyzes your IPTV systems and services for security flaws and vulnerabilities, protecting you from outages and malicious attacks.

Introduction

While the threat landscape for IPTV is similar to other IP-based services, securing IPTV has other, special challenges. Due to the streaming nature of the content and the quality of service customers have become to expect with traditional TV, there is little tolerance for packet loss, latency, or jitter. Even worse, customers experiencing problems are quick to change channels and restart playback in an attempt to improve quality, which only worsens any ongoing problems with the service. This makes IPTV highly sensitive to Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. These kind of conditions are not always caused by malicious hackers, but may result simply from faulty memory or bad connectors in set-top boxes or other equipment in the IPTV network.

Protecting the Content Source and Management Network is an important aspect of the IPTV security that presents even more challenges. Video-on-Demand (VoD) servers can never be completely isolated, as they have to interact with the Home Network and are therefore open to attacks from that direction. Firewalls and IDS/IPS systems are deployed for protecting IPTV servers. However, these devices can only protect from threats for which they have signatures, and they can also be attacked and taken down. Due to their multilayered, highly complex protocol stacks, Content Source and Management Network servers offer a large attack surface for hackers trying to steal content or perform other illegal activities. Initiating attacks against them is relatively straightforward for a malicious hacker - just spoof the IP address and behaviour of a standard set-top box and start scanning for services available in the network.



Summary of IPTV security and reliability challenges

- Protect against service disruption, DoS and DDoS
- Provide content security, prevent theft of video streams
- Ensure integrity of service and prevent rogue redistribution
- Block attempts to abuse network to spread viruses and worms

IPTV Security and Reliability Challenge

DEFENSICS for IPTV

Due to the special requirements of IPTV, pre-emptive security and robustness testing is needed to ensure the quality, reliability and availability of IPTV services. In robustness testing, a system under test (SUT) is subjected to invalid and malformed protocol traffic that simulates various attack and malfunction scenarios. Robustness testing can ensure that the protocol stacks in servers and protection devices such as firewalls and IPS/IDS systems are up to the task of delivering high-quality content reliably for users.

Codenomicon DEFENSICS is the most comprehensive negative testing solution in the market today. Codenomicon DEFENSICS for IPTV can be applied to testing the complete IPTV infrastructure, including IPTV Content Source systems, Delivery and Management networks and Home Networks.

DEFENSICS Benefits

- Eliminates downtime and costly patching in production environments. DEFENSICS finds and fixes problems before deployment.
- Covers the whole IPTV infrastructure with built-in server and client tests. Testing the server side of the infrastructure, such as VoD servers, ensures only one half of security. DEFENSICS provides the other half by testing the client direction in devices such as set-top boxes.
- Tests static security mechanisms with thorough end-to-end testing. Firewalls and IDS/IPS devices can only protect against threats that are known to them, but they have to be able to process any kinds of malicious traffic. DEFENSICS can be used to ensure the first lines of static protection are up to the task.
- Provides the broadest protocol coverage in the market. DEFENSICS offers unparalleled protocol coverage, enabling customers to test any protocols and interfaces systematically and comprehensively.
- Uses a stateful, model-based approach. DEFENSICS doesn't just test the initial message in a protocol sequence and stop there. Fully stateful testing combined with a unique mini-simulation approach helps DEFENSICS find vulnerabilities deep within the internals of any tested system.

DEFENSICS for IPTV Protocol Coverage

- IPv4
- IPv6
- TLS/SSL
- IPSec
- RTP/RTCP/SRTP
- RTSP
- HTTP
- TFTP
- FTP
- PIM-SM/DM
- RSVP
- IGMP
- MPEG4

Security and Robustness Problems Cost Real Money

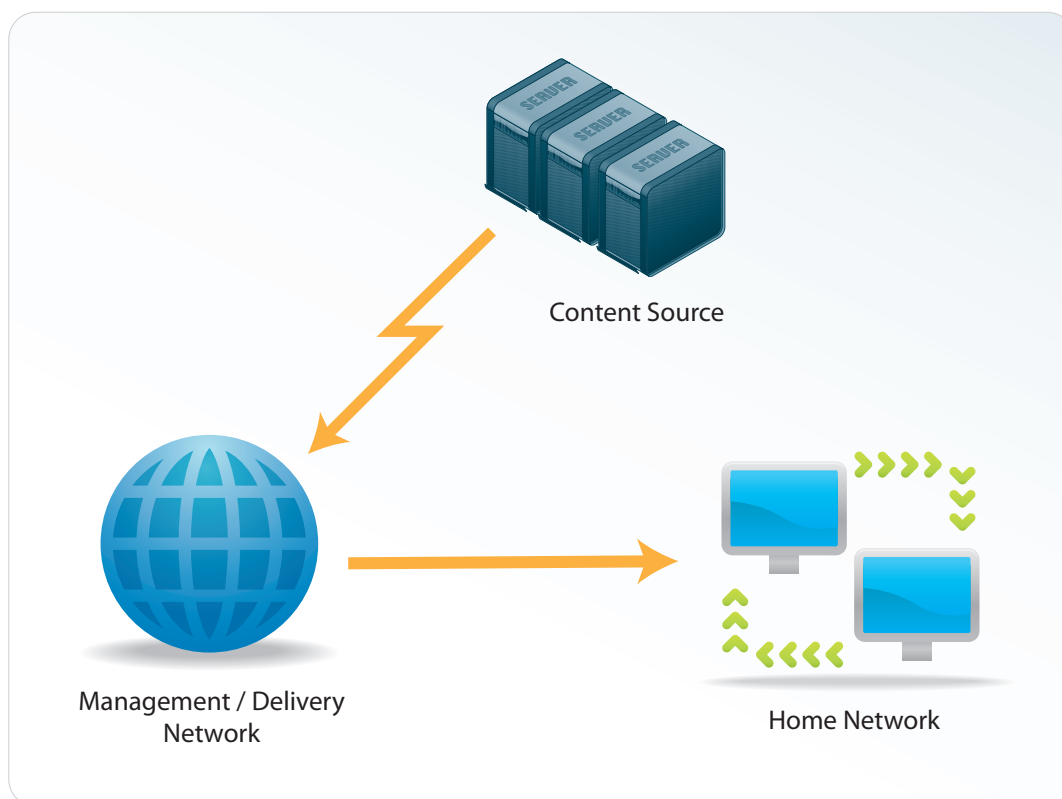
The average revenue per user (ARPU) of bundled triple-play is approximately \$100 / month today, with the target for many operators hanging as high as \$125 / month. The amount of IPTV subscribers is growing rapidly. As an example, during the first quarter of 2008, BT reported adding 91,000 new subscribers to their service, Telefonica 43,000, and Telecom Italia 56,000. As noted earlier, quality of service and user experience are critical factors for services like IPTV to succeed.

If security, reliability and robustness issues are found from software in a production environment, they can potentially affect thousands of users. Not only are these problems costly to fix, but they can also lead to decreased customer satisfaction and affect the public image on service quality and reliability. With a fast-growing user base and wide availability of equivalent services, the threshold to change service providers may be low if services are perceived to be inadequate. For a service provider with a user base of 500,000, a net loss of only 1% of subscribers would mean \$6M in lost revenues annually.

Covering All the Bases - Home Network Security

Home network security is often overlooked in IPTV security discussions, although it should be seen as critical as infrastructure security. Set-top boxes and other home network equipment may at first glance seem like any consumer devices, in which security and robustness problems are easily perceived as annoyances rather than critical failures in infrastructure security and integrity. The picture becomes bleaker when viewed through the motives and goals of a modern network criminal. Home network security threats can nowadays involve taking over a massive amount of home devices through a single vulnerability and harnessing them as zombie hosts for mounting further attacks against the IPTV network or against third-party services. This kind of scenario may lead to customer networks suddenly being used for DDoS attacks or for spreading rogue content. An attacker might also simply use the home equipment to steal content and to watch free transmissions, or to find more vulnerabilities in the network.

Codonomicon DEFENSICS is the only negative testing solution today to comprehensively offer also client-side testing for home network devices. Applicable protocols include e.g. IP, UDP, HTTP, RTSP, RTP, TLS, SIP, DNS, DHCP, WLAN, UPnP, etc. Practical testing with Codonomicon DEFENSICS has proven that all of the above concerns are valid. Many vendors and service providers have already benefited from securing their set-top boxes and other home network devices with DEFENSICS solutions.



DEFENSICS Advantage

Codenomicon DEFENSICS preemptive security and robustness testing solutions empower customers to mitigate unknown and published threats in products and services prior to release or deployment - before systems are exposed, outages occur and zero-day attacks strike.

Founded in 2001, the company was spun out of the successful PROTON test tools research of the Oulu University Secure Programming Group. Years later, the world-proven Codenomicon DEFENSICS platform remains unmatched in its ability to quickly find quality, resiliency and security flaws within the broadest array of applications. Thousands of developers and security analysts across telecommunications, networking, manufacturing, financial services and defense industries rely on Codenomicon to reduce costly reputation, quality and compliance risks.

Headquartered in Oulu, Finland, with offices in Silicon Valley and Hong Kong, the company markets its testing software and services directly and through international partners. Codenomicon's customers include Adobe, Alcatel-Lucent, AT&T, Cisco Systems, Nortel, Microsoft and Siemens AG among many others. The company is privately held with investments from Eqvitec Partners and Prime Technology Ventures.

The Issue: Greater attack velocity, organized cybercrime and service disruptions have elevated the need for more extensive security and robustness assessment of devices, applications and systems. Security and quality testing at all levels has become a best practice. However, barriers towards developing and maintaining adequate testing methods that help customers stay ahead of the threat still persists in the market. This is due to:

- Flawed commercial, consumer and corporate applications
- Increased development and deployment release pressures
- Shortage of security resources and expertise
- Unpredictable zero-day attacks, patches and system availability issues

Codenomicon's objective is to ensure the security and robustness of any application or service implementation. Development and security personnel in a lab or staged environment use Codenomicon DEFENSICS to fortify quality and security assurance – quickly, easily and reliably. The test software offers a systematic blackbox and negative test methodology uniquely capable of revealing undesired behavior and issues in protocol implementations. Codenomicon teams its Protocol Modeling Engine and Attack Simulation Engine with the industry's broadest protocol support covering network, wireless, and digital media. Thousands of pre-built, highly targeted and well-documented test cases allow users to start seeing results as soon as the platform is connected to the target system, accelerating time-to-value. In short, if a product or service under test passes DEFENSICS inspection – risk management and quality assurance is strong.

Summary

The past has shown that any new services are attractive targets for malicious hacking attempts. Immature technologies and lack of established best practices can provide an opportunity for illegitimate activities. Studies of IPTV show several technology areas that are vulnerable.

DEFENSICS for IPTV can be used proactively to mitigate threats and ensure safety for critical infrastructure. Preemptive elimination of security vulnerabilities and software flaws help organizations to save significant amounts in remediation costs. For further details on DEFENSICS, please visit www.codenomicon.com.

CODENOMICON Ltd.

info@codenomicon.com | www.codenomicon.com

Europe:

Tutkijantie 4E | FIN-90570 OULU
FINLAND

Tel. +358 424 7431

CODENOMICON Ltd.

info@codenomicon.com | www.codenomicon.com

USA:

10670 North Tantau Avenue | Cupertino, CA 95014
UNITED STATES

Tel. +1 408 252 4000