www.crysys.hu

Network Security (BMEVIHIMB00)

Integrated Security Solutions

Gergő Ládi
Laboratory of Cryptography and System Security
Department of Networked Systems and Services
Gergo.Ladi@CrySyS.hu

Outline

- Introduction
- Typical features
- Choosing a solution

- Some products

Introduction

- Integrated security solution
  - Hardware or software that combines several networking, security, and network security related features (hence 'integrated')
  - Filters, inspects traffic in some way

- A common misconception: an integrated security solution is a small, low-performance device for home/SOHO networks
  - This is wrong!

Introduction

- These integrated solutions are available in three different forms
  - Physical hardware
    - » You get a rack-mountable (rarely desktop) machine/device upon purchase
    - » Has all the software that is needed to operate and usually runs a custom OS
    - » More expensive but is guaranteed to be compatible with the software
  - Software
    - » You get a software package that you can install on your own hardware
    - » Cheaper, but there may be compatibility issues
  - Virtual appliance
    - » You get a virtual appliance to be run as a virtual machine on VMware ESXi, Microsoft Hyper-V, or at a cloud infrastructure provider
    - » Cheaper, but consumes resources on the host machine
      - If the host is overloaded, performance might suffer -> network issues!
    - » No compatibility issues

TYPICAL FEATURES

Typical features – Basic network services

- These are usually used at the edge of the network as a gateway or to isolate and filter traffic among network segments or VLANs
- Therefore, basic network services are often provided
  - DNS
  - DHCP
  - NAT
  - Routing
  - (NTP)
- Even routing protocols may be supported

Typical features – Traffic filtering

- Their main role is traffic filtering
  - As such, at the very least, they operate as a L4 stateful firewall
  - Nowadays, all of them work as L7 application firewalls
    - » Actual L7 features vary

- Typical L7 filtering features
  - URL filtering
    - » Based on categories and premade lists of "bad" domains
  - Keyword filtering
  - Spam and phishing filtering (discussed on another lecture)
  - Malware filtering
  - Protocol filtering

Typical features – SSL/TLS decryption

- Some security solutions are capable of intercepting and decrypting SSL/TLS traffic
  - This might not seem very secure, but this can actually improve security by being able to look into and filter encrypted traffic
  - This can be very powerful when combined with other filtering methods

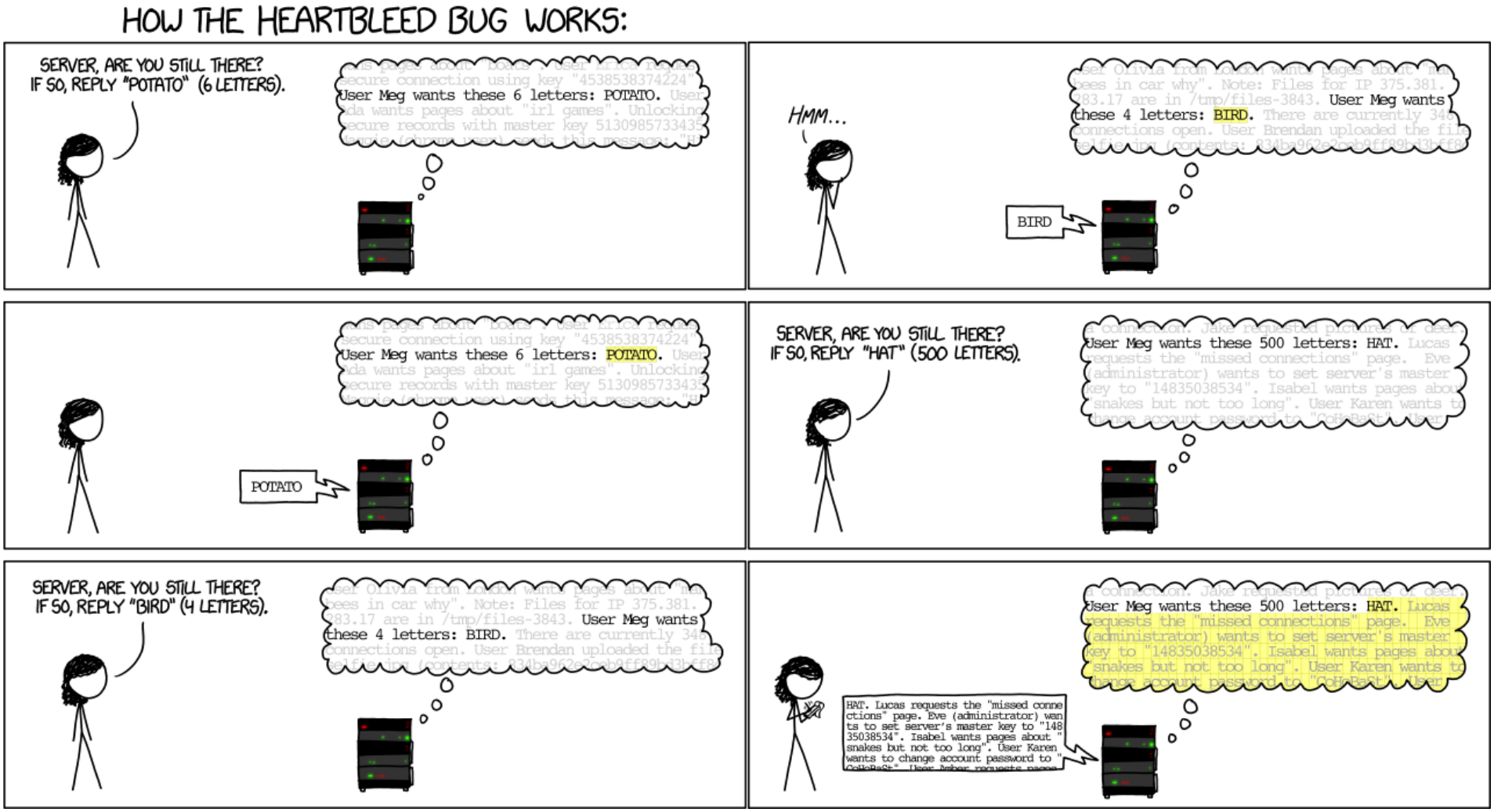
- The interception is essentially a man-in-the-middle attack
  - The firewall detects a TLS handshake
  - It checks the domain name, and uses a local CA to create a certificate for that domain (if one does not already exist)
  - The firewall acts as a client to the original service, and as a server to the local client
  - The local CA is set as trusted by the company's devices, therefore no TLS errors or warnings are triggered by the browsers

Typical features – Protocol validation

- Newer solutions are also capable of verifying whether the seen protocols' messages meet the specifications, and may fix or drop non-conformant or out-of-sequence messages

- Most of the security vulnerabilities in networked applications stem from improper message parsing and message handling
  - E.g.: Heartbleed

Typical features – Protocol validation



(https://xkcd.com/1354/)

Typical features – Advanced traffic filtering

- DLP: data loss prevention
  - 'Data leak prevention' would be a better term…
  - Aims to prevent confidential data from being exfiltrated
    - » By e-mail
    - » By web uploads
    - » …
- Filter evasion detection
  - Malware or malicious users may attempt to perform tricks to evade filters
    - » DNS tunnels, ICMP tunnels, etc.
  - Security solutions with evasion detection attempt to find and block these methods as well

Typical features – Misc. & convenience

- Integration with identity management solutions
  - Makes it possible to see not just the network flows, but also which user a given flow belongs to
  - This can be used for more fine-grained policies
    - » E.g. members of the Marketing department may access Facebook (they need it for work), but no one else may
  - This also helps investigate network incidents faster

- VPN
  - Most integrated security solutions can act as a VPN server
  - The supported protocols vary, but typically IPSec or DTLS-based protocols are chosen
  - Users often need to install 3rd party software to connect

Typical features – Misc. & convenience

- DDoS mitigation
  - Some solutions may have protections against (D)DoS attacks
  - They can't help against volumetric attacks (the external link will be flooded)
  - But they may protect against protocol-based or request-based attacks

- WiFi, captive portals, guest logins
  - Some solutions can act as captive portals for WiFi devices
    - » Users may get access to a restricted (guest) network after providing information about themselves and agreeing to the company policy
  - Some can also detect unauthorized (rogue) APs

Typical features – Performance & reliability

- High availability (HA)
  - Solutions may make it possible for 2 or more instances to cooperate in a way that ensures that if one of them malfunctions, the other one can still provide the necessary services
  - Implementations
    - » Active-active
    - » Active-passive (active-standby)

- Clustering
  - 2 or more instances may cooperate such that the cluster can handle more load than a single instance alone
  - Clustering does not always imply HA, but usually, both can be achieved

CHOOSING A SOLUTION

Choosing a solution

- When choosing a solution, it is imperative to consider all the requirements that the solution must meet in the present **and in the foreseeable future**
  - Making the wrong choice can be painfully expensive

Choosing a solution

- Basic services (if needed)
  - NAT
  - DNS, DHCP
  - Routing

- Traffic filtering
  - Maximum throughput
  - Maximum connection count (new and total)
  - What layer does it operate in? 4 or 7?
    - » Malware filtering (AV engines, means of detection?)
    - » URL filtering (categories, URL count, how often is it updated?)
    - » Spam and phishing filtering
    - » Protocol filtering
    - » SSL/TLS decryption?

Choosing a solution

- VPN
  - Maximum user count
  - Maximum throughput
  - Supported protocols
  - Does it require the installation of additional client software to work?
- IPv6 support
- WiFi (if needed)
  - Guest logins, captive portal
  - Rogue AP detection
  - Roaming support

Choosing a solution

- Support
  - Is support available?
    - » How? By phone? By e-mail?
    - » What is the maximum response time?
  - Priority tickets/premium support available? (Is it needed?)
  - How much does it cost?
    - » Is it included in the license fee?
  - How long is the product supported?
    - » When is it going to be End of Sale (EoS), and End of Life (EoL)?
    - » How long do we plan to use it?
  - How long are firmware/software/security updates provided?

Choosing a solution

- Licensing
  - Cost
    - » Is it free? Paid?
  - How is it licensed?
    - » One-time fee?
    - » Per-user? Per-device?
    - » Per feature?
    - » Per-<X>?
  - How long is the license valid for?
  - Upgrade options available?

Choosing a solution

- Management – How is it managed?
  - Web interface?
  - CLI?
  - SNMP?
  - Something else?
- Interoperability with existing hardware from other vendors?
- (How) can it be integrated with SIEM (logging and alerting) systems?
- High availability options
- Clustering options

Choosing a solution

- Ask friends at similar companies
  - What do they use?
  - Are they satisfied?
- Read reviews
  - Beware: some reviews are "sponsored", so take everything you find with a grain of salt

SOME PRODCUTS

Balasys Zorp Gateway

- Software-based

- Key features
  - Basic services
  - Firewall
  - Virus scanning
  - TLS decryption
  - Protocol validation
  - HA/clustering support
  - VPN support (OpenVPN)

- Has its own management framework
- Extensible functionality through custom Python scripts

Balasys Zorp GPL

- Software-based

- Key features
  - Basic services
  - Firewall
  - Virus scanning
  - TLS decryption
  - Protocol validation (some proxies are missing)
  - VPN support (OpenVPN)

- Free and open source
- No centralized management
- Extensible functionality through custom Python scripts

Cisco Adaptive Security Appliance (ASA)

- Hardware-based or virtual appliance (ASAv)

- Key features
  - Firewall
  - Dynamic routing
  - TLS decryption (some models)
  - HA/clustering support (not in ASAv)
  - VPN support (SSL VPN, Cisco AnyConnect)

- Supports multiple security contexts
- Newer versions have IDS/IPS features and protocol validation

Cisco Meraki MX Firewall

- Hardware-based or virtual appliance (vMX)

- Key features
  - Firewall
  - Content filtering
  - HA/clustering support
  - IDS/IPS features
  - VPN support (IPSec)

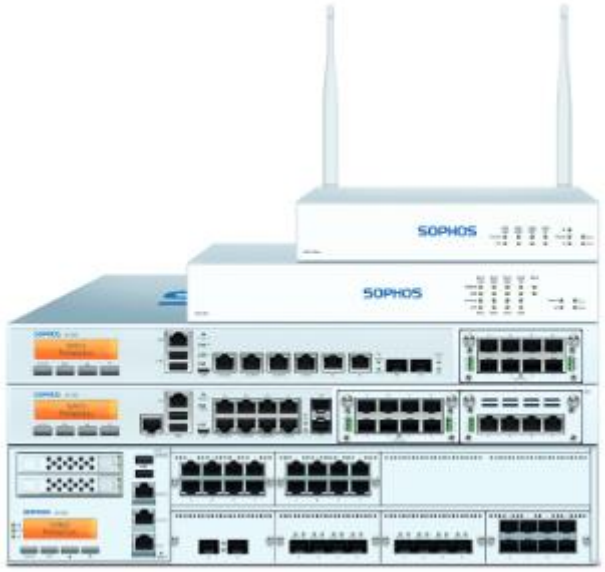
- Cloud-managed
- TLS decryption as a beta feature
  - Still in beta as of 2022
  - Removed as of 2023?

pfSense

- Hardware, software, or virtual appliance
- Key features
  - Basic services
  - Firewall
  - Web filtering
  - VPN (IPSec, OpenVPN)
- Open source
- Captive portal support

Sophos UTM

- Hardware-based or virtual appliance
- Key features
  - Firewall
  - Web filtering
  - Spam filtering
  - VPN (SSL, IPSec)
- WiFi support, incl. captive portals



Other solutions

- Barracuda CloudGen Firewall
- Check Point CloudGuard
- Fortinet FortiGate
- Juniper (v)SRX
- PaloAlto Firewalls
- Untangle NG Firewall
- …

www.crysys.hu

Thank you for your attention!

Questions?

Gergő Ládi
Laboratory of Cryptography and System Security
Department of Networked Systems and Services
Gergo.Ladi@CrySyS.hu

MISCELLANEOUS

Control Questions

- What is an integrated security solution? Why are they called 'integrated'?
- In what three forms are integrated solutions usually available? Describe each of these forms.
- What typical features are integrated solutions expected to provide? Name at least 4.
- What is the purpose and benefit of SSL/TLS decryption?
- What is the purpose and benefit of protocol validation?
- (Optional: What is Heartbleed? How did it work?)

Control Questions

- What is DLP (Data Loss Prevention)?
- Why might it be a good idea to integrate a firewall with an identity management service?
- What Wi-Fi related security benefits are offered by integrated solutions?
- Why is performance and reliability important for integrated solutions? How are they achieved?
- List at least 5 questions that are important to answer before purchasing an integrated security solution.