Bezbedni komunikacioni kanali

Informaciona bezbednost

Fakultet tehničkih Nauka, Univerzitet u Novom Sadu

Imre Lendak, 2020

Sadržaj današnjeg predavanja

- Uvod
- Medijumi
- Protokoli
- Perimetar sistema
- Firewall
- IDS/IPS

Razlozi slabosti distribuiranih sistema

- Mnoge potencijalne tačke slabosti kod velikih sistema sa puno elemenata
- Anonimnost – napad sa bilo kog mesta
- Deljenje resursa – pristup više korisnika nego kod jedne neumrežene radne stanice
- Kompleksnost i heterogenost sistema
- Nepoznate granice mreže
- Nepoznata putanja u mreži

Motiv

- Izazov – “da li mogu da upadnem u mrežu?”
- Slava – “drugi (hakeri) će me više ceniti”
- Novac – “koliko ću biti u plusu upadom?”
- Špijunaža – “koliko plaća „Organizacija X“ za upad?”
- Međunarodni organizovani kriminal
- Ideologija: hektivizam i kiber terorizam

Bezbedne komunikacione mreže

MEDIJUMI

Žičani komunikacioni sistemi

- Žičane mreže na bazi: kabl, parica, optika
- Kodiranje podataka: analogno, digitalno
- Zaštita: upotreba skrivača, čuvanje mrežnih dijagrama u tajnosti
- Metod napada: fizički pristup, merenje zračenja
  - Kod optike fizički pristup na ripiterima
  - Optika ne zrači (!)

Bežični komunikacioni sistemi

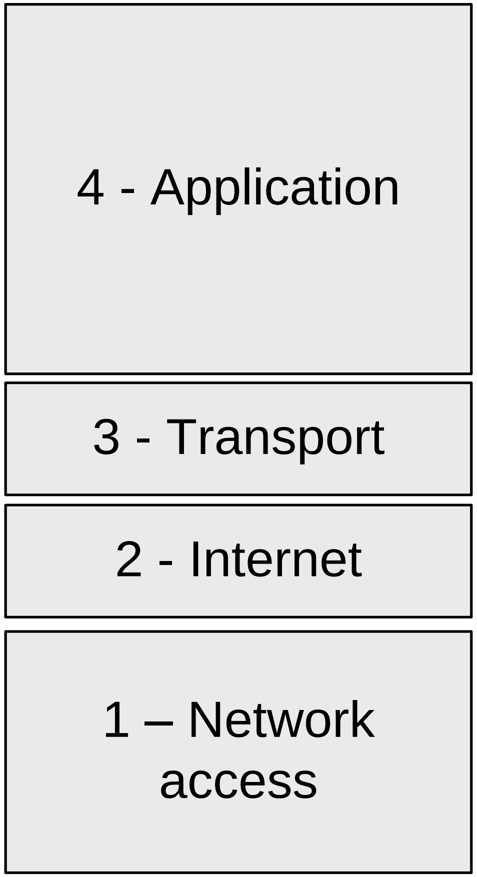
- Bežične mreže na bazi:
  - WiFi
  - Bežične mobilne mreže – GSM, GPRS, 3G, 4G
  - Bluetooth
  - Near-field communication (NFC)
  - Infracrveni – infrared (IR)
  - Satelitska veza
  - Radio-frequency identification (RFID)
  - Mikrotalasni radio
- Sa stanovišta bezbednosti je kod žice potreban fizički pristup, dok kod bežični komunikacionih sistema nije

Bezbedne komunikacione mreže

PROTOKOLI

TCP/IP

- 4 – aplikacije, enkripcija, sesije, itd.
- 3 – uspostavlja i održava virtualna kola između dva računara, pouzdanost prenosa podataka
- 2 – logičko adresiranje i nalaženje putanje
- 1 – binarni prenos & kontrola linka – parice, konektori, naponski nivoi, fizičko adresiranje, mrežna topologija, redosled isporuke, upravljanje tokom

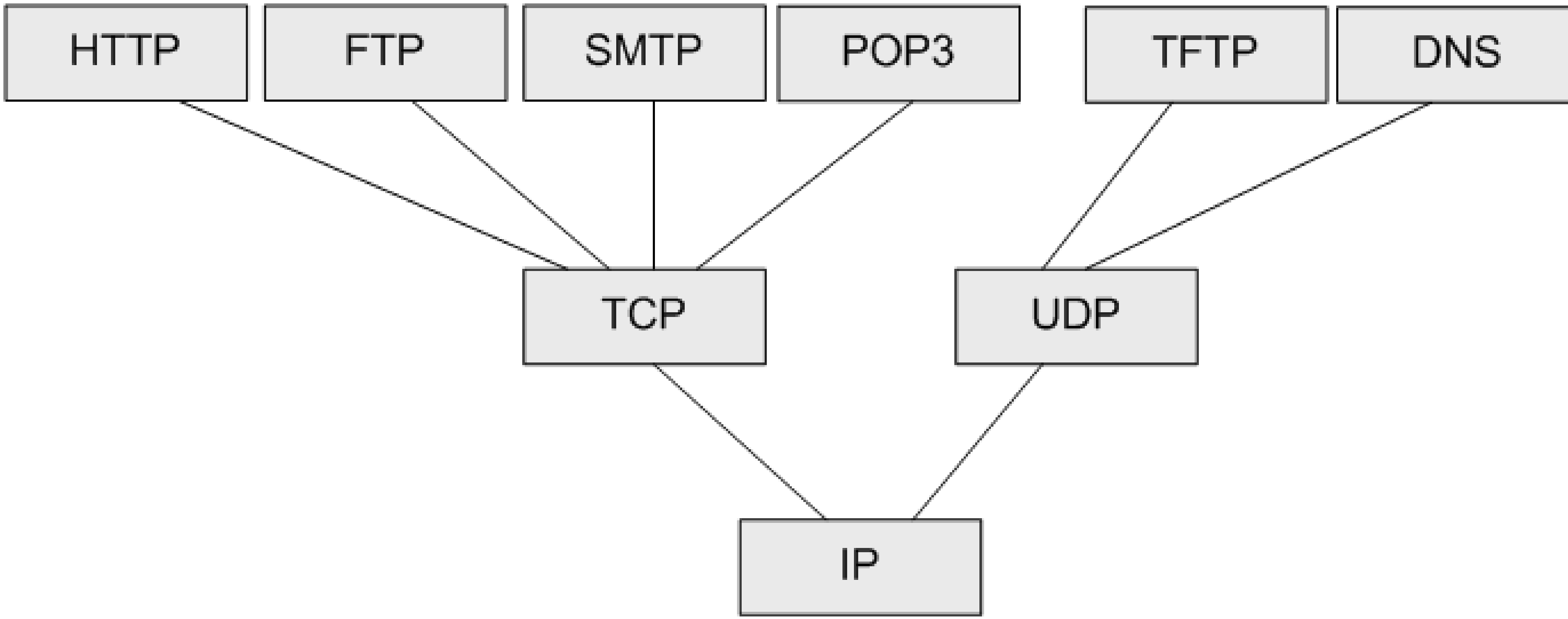


Mere bezbednosti u TCP/IP steku

Network Security Role

OSI Model	TCP/IP Model	
Application Layer	Application	Access control, hashing, checking digital signatures
Presentation Layer		Translation, encryption, decryption
Session Layer		Maintains open communication line
Transport Layer	Transport	Transmission and retransmission
Network Layer	Internet	Data network routing, IPv4, IPv6
Data Link Layer	Network Access	Data directing, MAC address, L2 switches
Physical Layer		Data transmission methods

Protokoli



Bezbedne komunikacione mreže

PERIMETAR KOMUNIKACIONOG SISTEMA

Perimetar

- Perimetar je administrativna granica sistema (engl. Electronic Security Perimeter – ESP)
- Perimetar se sastoji od elektronskih tačaka pristupa (engl. Electronic Access Point – EAP)
- Najčešći elementi elektronskih tačaka pristupa:
    - Web server
    - Granični ruteri
    - Komunikacioni uređaji (antene, ripiteri i sl.)
    - Mobilni elementi, npr. laptop, službeni mobilni
- U kontekstu kritičnih infrastruktura je (i) oprema na terenu jeste deo perimetra, npr. oprema u transformatorskoj stanici na IP mreži
    - Zbog velikog broja taj tip opreme se selektivno štiti
- Enklava (*enclave*) ili zona je logički i/ili fizički odvojen deo sistema

Mobilni elementi

- Razni tipovi mobilnih uređaja se takođe mogu smatrati činiocima perimetra sistema:
  - Službeni laptop
  - Personalni asistenti, npr. tablet, smartphone, Google Glass
  - Prenosni mediji, npr. USB disk
- Metodi napada na i preko mobilnih elemenata:
  - Zaraza malware-om van kompanije i ubacivanje u zaštićene enklave
  - Krađa
  - Neutorizovane dizanje sistema, npr. sa USB diska

Bezbedne komunikacione mreže

ZAŠTITA PERIMETRA – FIREWALL

Firewall

- *Firewall* je alat koji filtrira saobraćaj između zaštićene unutrašnje i spoljašnje zone
  - Softver: filtriranje, inspekcija, aplikativni proksi, lični
  - Hardver: aplikativni, prenosni sloj
- Mesta upotrebe:
  - Na perimetru sistema,
  - Između enklava sistema,
  - Na serverima i radnim stanicama
- Pristup podešavanju:
  - *Default deny – preporučljiv i selektivniji*
  - *Default permit – korišćen ranije, ne preporučuje se*
- Minimalni: minimum servisa i korisnika na *firewall*-u

FW1: Packet filtering firewall

- Koristi se da bi rasteretio granične rutere
- Nalazi se iza graničnih rutera
- Filtrira saobraćaj na bazi pravila
  - Izvorna adresa, npr. SSH iz određene mreže
  - Odredišna adresa, npr. za odlazne konekcije
  - Tip protokola, npr. HTTP
- Ne tumači sadržaj paketa, tj. odluke donosni na osnovu zaglavlja IP paketa
- Loša strana je složenost konfiguracije
- Softverske implementacije, npr. iptables na Linux OS

FW2: Stateful inspection firewall

- Packet filtering firewall sa dodatnim opcijama
- Pored filtriranja paketa pamti informacije (tzv. kontekst) o otvorenim konekcijama
- Može da detektuje napad koji se sastoji od fragmentovanih malih paketa

FW3: Application proxy

- Aplikativni proxy je složeniji tip firewall-a
    - Aplikativni proxy je dodatni čvor između izvora i odredišta
    - „Zaviruje“ u podatke pored analize zaglavlja
    - Simulira obe strane koje komuniciraju prekog njega
    - Obezbeđuje da samo korektni zahtevi i podaci prođu kroz njega
    - Omogućava da se filtriraju komande protokola na višim nivoima (SMTP, FTP, itd.)
- Primer: proxy.uns.ac.rs

FW4: Lični firewall

- Koristi se od strane individualnih korisnika sa direktnim pristupom Internetu
  - Kod kuće ne postoji kompanijski firewall stručno podešen od strane profesionalaca
- Poseban firewall bi imao loše strane kod kuće: skup, zauzima prostor, troši struju, itd.
- Realizuje se kao softverski *firewall*
- Primeri:
  - Microsoft Windows Firewall
  - PC Tools Firewall
  - Comodo Firewall, itd.

Bezbedne komunikacione mreže

ZAŠTITA PERIMETRA – IDS/IPS

Nadzor u bezbednosti informacionih sistema

- **DEF:** The goal of Network Security Monitoring (NSM) is to analyze various data types and generate (security) alerts.
- The alert is presented to a security analyst → detection ends and analysis begins
- Detection mechanisms which might raise alerts
  - Network and Host-based Intrusion Detection/Prevention Systems (IDS/IPS)
  - Anti-malware solutions
  - Data loss prevention (DLP)
  - Behavioral monitoring systems
- Detection mechanism types:
  - Signature-based
  - Anomaly-based

IDS

- **DEF:** An **intrusion detection system** is an appliance (i.e. piece of hardware) or software which monitors a host or a system for malicious activity or policy violations.
  - A policy violation might be downloading a multimedia file or watching videos during working hours
  - Historically, most intrusion detection solutions were relying on indicators of compromise found in network traffic
  - Input: network traffic, host level logs, host-level user activity
  - Output: alert sent to an administrator or a Security Information and Event Management (SIEM) solution
- **DEF:** Systems with active response capabilities (e.g. able to terminate a TCP connection) are called **Intrusion Prevention Systems (IPS)**

Short IDS history

- 1980: J. Anderson defined the preliminary IDS concept for analyzing audit logs (user & file access, system events)
- 1986: D. Denning & P.G.Neumann published an IDS model named Intrusion Detection Expert System (IDES) which analyzed both network and user activity
  - Rule-based detection of known intrusions
  - Statistical anomaly detection of users and hosts
- 1986: National Security Agency research program on IDS
  - R. Bace, “Intrusion Detection” paper in 2000
- 1991: Distributed Intrusion Detection System (DIDS) prototype developed by the University of California – Davis
- 1998: Bro developed at the Lawrence Berkeley National Laboratory with its own language for pcap analysis
- 1998: Snort IDS developed – monitors local hosts and remote capture points via TZSP – it is the most widely used signature-based IDS
- 2010: Suricata IDS developed by the Open Information Security Foundation (OISF) – (mostly) shares the Snort signature format

Signature-based detection

- Signature-based detection steps

1. Analyze available NSM data
2. Look for known elements of known malicious behavior:
   - IP address
   - Uniform Resource Locator (URL)
   - Malware file hash

- **DEF:** Platform-independent descriptions of known malicious behavior are indicators of compromise (IOC)
- **DEF:** Signatures are IOCs described in a platform-specific language of a detection platform
  - E.g. specific IP address-based rule in a NIDS
- Reputation-based detection is a subset of signature-based detection

Anomaly-based detection

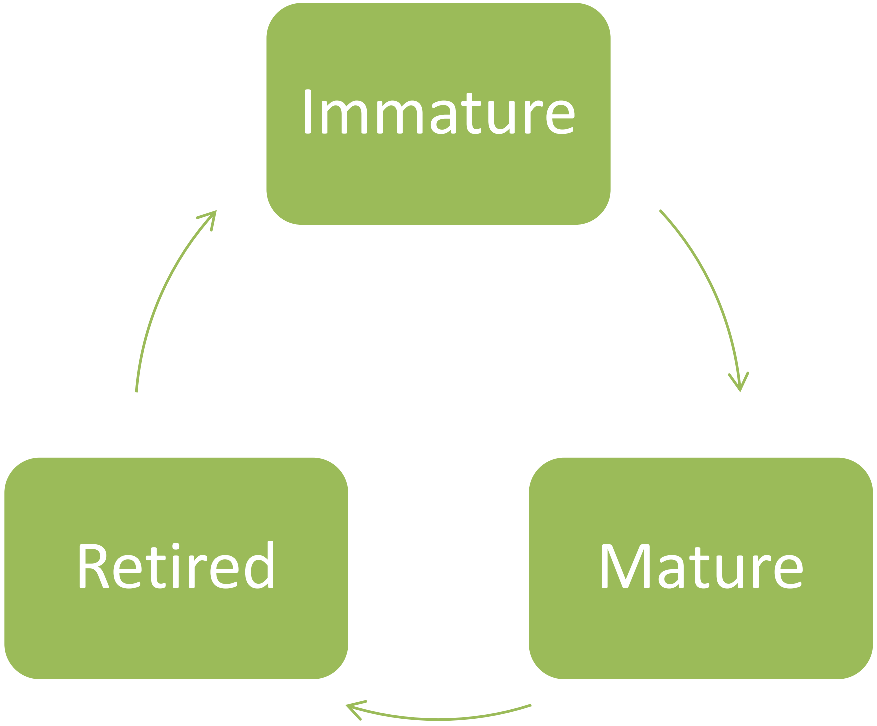
- **DEF:** Anomaly-based detection relies on observing and 'learning' normal network traffic and detecting out-of-ordinary patterns in NSM data
- The goal is to detect any pattern in NSM data that deviates from normal behavior
  - E.g. administrator logs in with valid credentials at 02:00 AM from a foreign country
- Statistical or heuristics-based analysis
- Anomaly-based detection is a newer form of detection in NSM analysis
- Anomaly-based detection is usually applied after signature-based, i.e. when the security analyst team gains confidence and experience

IOC

- **DEF:** An IOC is a single piece or a complex set of information which describe a network intrusion in a platform-independent manner
  - IOCs are usually referred to as just ‘indicators’
- IOC types:
  - Simple indicators = consist of a single piece of information
  - Behavioral indicators = a set of information which describe events which occur jointly and define an unwanted activity in a distributed information system
- IOC storage modes:
  - CSV files,
  - SQL databases
- **DEF:** The IOCs when converted into the configuration format of a specific IDS solution is a **signature**
  - Signatures are released and updated by IDS vendors, i.e. producers in platform-specific formats

Indicator lifecycle phases

- IOCs and signatures usually pass through 3 stages in the lifecycle
  - **Immature** = in testing mode, if in operation, then alerts assigned to higher level analysts
  - **Mature** = well-tested and used in real-time or offline NSM
  - **Retired** = not in use, but maintained
- Note: IOCs should be stored in a versioning system



IOC step-by-step lifecycle

- Step 1: A security analyst (SA) analyzes a malicious activity, e.g. insider exfiltrating a file via DNS
- Step 2: The SA derives an IOC for the incident
- Step 3: The SA develops the IOC into a signature for a specific IDS solution
- Step 4: The signature is tested in a test environment
- Step 5: The signature is tested in a live, real-time environment and alerts are sent to higher level SA only
- Step 6: If the signature is approved by the higher level (e.g. 2/3) SA, then it is deployed in the real-time environment
- Step 7: The signatures alert when the activity occurs
- (Optional) Step 8: The signature is shared with the community

Signatures

- **DEF:** Signatures are platform-dependent IOC descriptions
- Signatures are directly usable by specific detection solutions:
  - NIDS/HIDS: Suricata, Snort
  - Anti-malware: Avast, Kaspersky
  - Behavioral analytics
  - Data loss prevention

Signature relevance

- **True Positive (TP)** = an alert was raised after a correct identification of an event
- **False Positive (FP)** = an alert was raised after an incorrect identification
- **True Negative (TN)** = no alert, no unwanted event
- **False Negative (FN)** = no alert, undetected unwanted event

- **Precision** is the ability to identify positive results

$$Precision = \frac{TP}{(TP + FP)}$$

- **Confidence** is the level of trust security analyst put into an alert received
- High precision signatures have higher confidence (!)

Challenges

- **Network traffic encryption** disallows IDS to inspect payloads, i.e. TCP/IP header analysis only
- **Signature lag** is the time between the emergence of a new known threat and a signature created by the IDS vendor and deployed by the IDS user
- **Noise** is any unwanted network or other NSM activity which is non-malicious but might raise an alert. Possible sources: software bugs → malformed packets, LAN packets on the WAN
- In a **high false positive environment** the real alerts can be very rare and might be missed by security analysts who are overwhelmed by the false positives

Evasion techniques

- **Spoofed IP addresses:** might lead to false negatives
- **Port modification:** the attacker might reconfigure the malware to use a different TCP/UDP port, e.g. backdoor to C&C server communication
- **Payload modification:** the attackers slightly change the payload itself, e.g. reordering the binary code of the malware
- **Payload fragmentation:** the payload (e.g. malware) is fragmented into multiple packets → signature is not matched
- **Coordinated attacks:** the attackers might fragment their activities between different hosts and/or different IP addresses in a coordinated fashion

IDS izlazi

- Fast: alerts are displayed in a simple one-line format

```
08/05-15:58:54.524545 [**] [1:2100498:8] GPL ATTACK_RESPONSE id check returned
root [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 217.160.51.31:80 -
>172.16.16.20:52316
```

- Syslog: standard logging format on *nix systems

```
Aug 5 15:58:54 lakota snort: [1:2100498:8] GPL ATTACK_RESPONSE id check
returned root [Classification: Potentially Bad Traffic] [Priority: 2]:
{TCP} 217.160.51.31:80 ->172.16.16.20:52316
```

- Full: Fast + packet header data

```
[**] [1:2100498:8] GPL ATTACK_RESPONSE id check returned root [**]
[Classification: Potentially Bad Traffic] [Priority: 2] 08/05-15:58:54.524545
217.160.51.31:80 ->172.16.16.20:52316
TCP TTL:40 TOS:0x20 ID:44920 IpLen:20 DgmLen:299 DF
***AP*** Seq: 0x6BD4465B Ack: 0xE811E4E6 Win: 0x36 TcpLen: 20
```

Rezime

- Uvod
- Medijumi
- Protokoli
- Perimetar sistema
- Firewall
- IDS/IPS

Hvala na pažnji!