

# Beveiliging van netwerken en computers

Bert De Saffel

Master in de Industriële Wetenschappen: Informatica Academiejaar 2018–2019

Gecompileerd op 10 november 2018

# Inhoudsopgave

<b>1</b>	<b>Basisconcepten</b>	<b>2</b>
<b>2</b>	<b>Netwerk en communicatiebeveiliging</b>	<b>3</b>
2.1	SSH . . . . .	3
2.1.1	Architectuur . . . . .	4
<b>3</b>	<b>Encryptiealgoritmen</b>	<b>7</b>
3.1	Geschiedenis . . . . .	7
3.2	Moderne cryptografie . . . . .	9
3.2.1	Symmetrische algoritmen . . . . .	9
<b>4</b>	<b>Software- en systeembeveiliging</b>	<b>10</b>

# Hoofdstuk 1

## Basisconcepten

Computerbeveiliging

## Hoofdstuk 2

# Netwerk en communicatiebeveiliging

Voorlopig hebben we enkel de basisconcepten gezien zoals: symmetrische encryptie, asymmetrische encryptie, hashfuncties en message authentication codes. Dit hoofdstuk zal deze concepten toepassen om beveiligingsprotocollen te ontwikkelen voor netwerken.

### 2.1 SSH

SSH (Secure Shell) is een **applicatielaagprotocol**. Ondanks deze naamgeving bevat SSH ook een **transportlaagprotocol**, met als bedoeling een veilige connectie te maken tussen andere OSI applicatielaagprotocollen (bv HTTP) en de werkelijke OSI transportlaag. SSH kan draaien op zowel workstations als routers en switches. Routers en switches volgen de OSI laag namelijk niet strict, zodat zij ook een applicatielaag hebben. Vroeger werd het programma **telnet** gebruikt om remote configuratie toe te passen. Deze manier van werken is **onveilig** aangezien verkeer tussen de local host en remote host niet geëncrypteerd wordt, zodat deze door eender wie kunnen bekeken worden. SSH verhelpt dit probleem door de informatie te encrypteren. Vrijwel alle UNIX en Linux distributies komen met een versie van SSH geïnstalleerd. SSH laat onder andere toe om:

- een veilige remote verbinding op te zetten vanuit eender welke local host naar eender welke remote host. Het protocol maakt gebruik van erkende algoritme voor zowel encryptie (sleutels van ten minste 128 bits), data-integriteit, sleuteluitwisselingen en public key management. Tijdens het leggen van een connectie worden algoritmen tussen de local host en remote host afgesproken, op basis van welke ze al dan niet ondersteunen,
- TCP te tunnelen via een SSH connectie,
- bestanden te verplaatsen, gebruik makend van bijhorende protocols zoals SCP (Secure Copy) of SFTP (SSH File Transfer Protocol),
- zowel X-sessions als poorten te forwarden.

### 2.1.1 Architectuur

SSH kan opgesplitst worden in drie elementen: Transport Layer Protocol, User Authentication Protocol en het Connection Protocol.

#### Transport Layer Protocol

Dit protocol heeft onder andere de verantwoordelijkheid om: authenticeren van servers, sleuteluitwisselingen en perfect forward privacy implementeren. Perfect forward privacy wil zeggen dat, indien een sleutel gecompriemd wordt tijdens een sessie, deze geen invloed kan hebben op de beveiliging van vorige sessies. Dit protocol loopt uiteraard op de transportlaag, en in de meeste gevallen zal dit TCP zijn. Vooraleer de cliënt kan connecteren moet hij de **public host key** van de server bezitten. Hiervoor kunnen er twee modellen gebruikt worden (cfr. RFC 4521) waarbij:

1. de cliënt een lokale databank bevat die de mapping beschrijft van elke hostnaam naar de corresponderende public host key. Op deze manier is er geen centrale entiteit nodig, maar het beheer van deze databank kan, indien deze groot genoeg wordt, lastig zijn om te onderhouden.
2. de mapping bevestigd wordt door een **CA (Certification Authority)**. De cliënt kent in dit geval enkel de CA root key waarmee de geldigheid van elke host key kan nagaan die getekend zijn door deze CA. In dit geval moet de cliënt slechts één of enkele CA root keys bevatten.

Wanneer er een connectie kan gelegd worden van een cliënt tussen een server, is het eerste proces altijd het **onderhandelen van de algoritmen**. Deze stap zal algoritmen selecteren die compatibel zijn met zowel de cliënt als de server. Wanneer de cliënt een TCP connectie heeft met de server worden volgende pakketten verstuurd:

- **Identification string exchange.** Dit is een string dat zowel het protocolversie als de softwareversie van SSH bevat. Deze string wordt ten eerste van de cliënt naar de server verstuurd, waarop de server dan antwoord met zijn protocol en softwareversie. Indien hieruit blijkt dat de machines niet compatibel zijn met elkaar, wordt de connectie onderbroken (**SSH2 is bv niet compatibel met SSH**) en worden volgend stappen bijgevolg niet meer uitgevoerd.
- **Algorithm Negotiation.** In deze fase sturen zowel de server als de cliënt een SSH\_MSG\_KEXINIT bericht, die een lijst van alle ondersteunde algoritmen bevat, in volgorde van voorkeur. Elk type van algoritme zoals sleuteluitwisseling, encryptie, MAC algoritme en compressiealgoritme heeft zo zijn eigen lijst. Elk type moet dan ook een algoritme toegekend krijgen en wordt bepaald door het eerste algoritme dat de cliënt goed vindt dat ook beschikbaar is op de server.
- **Key Exchange.** Indien de vorige fase goed gelukt is, start nu de sleuteluitwisseling. Voor de sleuteluitwisseling worden er momenteel slechts twee versie van **Diffie-Helman** ondersteund (cfr. RFC 2409). Het einde van de sleuteluitwisseling wordt gesignaleerd door een SSH\_MSG\_NEWKEYS pakket, met als gevolg dat zowel de cliënt als de server de gegenereerde sleutels mag gebruiken.
- **Service Request.** De laatste stap, dat eigenlijk het begin is van een volgend proces, wordt gesignaleerd door een SSH\_MSG\_SERVICE\_REQUEST pakket. Dit pakket vraagt ofwel de start van het User Authentication Protocol of van het Connection Protocol. Alle verkeer

tussen server en cliënt wordt op dit moment getransporteerd als de payload van een SSH Transport Layer pakket, beveiligd met encryptie en een MAC.

Een SSH Transport Layer pakket heeft de volgende vorm, waarbij elementen met een  $\delta$ -symbool geëncrypteerd en geauthenticeerd zijn en elementen met een  $\Delta$ -symbool ook optioneel gecomprimeerd kunnen zijn:

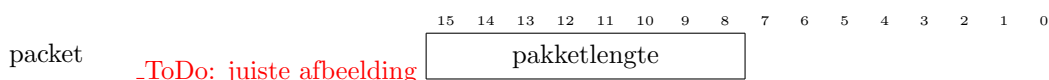
$\delta$  **Pakketlengte (4 bytes)**. De lengte van het pakket in bytes, zonder de lengte van de pakketlengte zelf en het MAC veld in beschouwing te nemen.

$\delta$  **Paddinglengte (1 byte)**. Dit is de lengte van het random padding veld.

$\Delta$  **Payload**. De eigenlijke informatie van het pakket.

$\delta$  **Random padding**. Dit veld dient om cryptanalyse moeilijk te maken. Kleine pakketten zijn op deze manier minder veel minder voorspelbaar en algoritmen, die vaak een kenmerkende vaste lengte hebben, worden ook moeilijker te achterhalen.

/ **MAC veld**. Dit veld wordt enkel gegenereerd indien dit zo in de onderhandeling besproken werd. Dit veld wordt berekend over het hele pakket en krijgt ook nog een bijhorend sequentienummer. Het sequentienummer start op 0, en wordt telkens met 1 geïncrmenteerd voor elk pakket. Een aanvaller kan dit sequentienummer niet achterhalen aangezien een MAC een onomkeerbaar proces is.



Het **sleuteluitwisselingsproces** vraagt wat enige uitleg, er is echter nog niet nagegaan of deze sleutels op een **veilige** manier uitgewisseld worden. Op het moment van sleuteluitwisseling is er helemaal nog geen SSH connectie. Het uitwisselingsproces verloopt in twee fasen: eerst wordt er een gedeelde sleutel gegenereerd met Diffie-Helman, daarna wordt deze gedeelde sleutel gesigneerd met de publieke sleutel van de cliënt voor authenticatie. Sleutels kunnen ook heruitwisseld worden, hierbij gelden volgende regels:

- Mogelijk op elk moment, behalve tijdens het sleuteluitwisselingsproces.
- Kan aangevraagd worden door beide partijen.
- Sessie identificaties blijven ongewijzigd.
- Cryptografische algoritmen kunnen gewijzigd worden.
- Sessiesleutels worden vervangen.

Meestal worden sleutels vervangen na het behalen van een bepaalde quota zoals een tijdslimiet of het aantal totaal verstuurd bytes.

### User Authentication Protocol

Dit protocol specificeert **hoe** een cliënt zich moet authenticeren aan een server. Meerdere methoden zijn mogelijk waaronder de drie belangrijkste ervan: Public Key Authentication, Password Authentication en Host Based Authentication:

- **Public Key Authentication.** De implementatie van deze methode is afhankelijk van het gebruikte public-key algoritme. Een cliënt verstuurt berichten, dat gesigneerd is door de cliënt zijn private sleutel, naar de server, die de publieke sleutel van de cliënt bevat. De server gaat na of deze publieke sleutel nog geldig is en zoja, of dat de signatuur correct is.
- **Password Based Authentication.** De cliënt verstuurt zijn paswoord, dat geëncrypteerd wordt door het SSH Transport Layer Protocol naar de server, die nagaat of het paswoord correct is.
- **Host Based Authentication.** **\_ToDo:**

### Connection Protocol

**\_ToDo:** vanaf slide 26

## Hoofdstuk 3

# Encryptiealgoritmen

### 3.1 Geschiedenis

Encryptiemethoden worden al eeuwenlang gebruikt om informatie onleesbaar te maken voor partijen die deze informatie niet mogen achterhalen. Deze inleiding bespreekt de basismethoden om encryptie toe te passen.

Zogenaamde **substitution ciphers** zijn de meest eenvoudigste vorm van encryptie. De originele versie, ook wel Caesar cipher genoemd, vervangt elke letter van het alfabet met een voorgedefiniëerde shift in positie. Een shift van 3 zal het originele alfabet (in kleine letters) afbeelden op het verschoven alfabet (in grote letters): Het duidelijke nadeel is dat er slechts 25 verschillende encryp-

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

tiemogelijkheden zijn. Een verbeterde versie mapt elke letter met een willekeurige andere (nog niet gebruikte) letter: waardoor er nu  $26! \approx 4 \cdot 10^{26}$  mogelijkheden zijn. Deze manier is daarom niet meer

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
D	K	V	Q	F	I	B	J	W	P	E	S	C	X	H	T	M	Y	A	U	O	L	R	G	Z	N

secur, aangezien de onderliggende frequentie van letters nog steeds dezelfde is. Een eenvoudige decryptiemethode is om de relatieve frequenties van de ciphertekst te tellen, waardoor er statistisch kan achterhaald worden met welke gedecrypteerde letter elke geëncrypteerde letter overeenkomt.

Een encryptiealgoritme wil ook de relatieve frequenties verbergen. Een methode dat dit implementeert is de Vigenère Cipher. Deze bevat een sleutel  $K = k_1 k_2 \dots k_d$  waarbij  $k_i$  het  $i$ -de alfabet specificeert dat gebruikt moet worden. Na  $d$  letters start ment terug vanaf  $k_i$ .

Een laatste voorbeeld van een substitutiecipher is de Playfair cipher. Hier wordt er een  $5 \times 5$  matrix opgesteld, waarbij eerst het sleutelwoord ingevuld wordt, gevolgd door de niet gebruikte letters in alfabetische volgorde. Dit wordt uitgewerkt met de sleutel **MONARCHY** in Tabel 3.1. Een bericht wordt in paren van letters geëncrypteerd. Stel dat we het woord **ballon** willen encrypteren, de paren letters



M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

Tabel 3.1: Playfair cipher.

worden: ba lx lo nx. Er wordt een x toegevoegd indien er twee dezelfde letters achter elkaar komen, en als het eindpaar uit slechts één letter bestaat. Er kunnen zich drie gevallen voordoen bij elk paar:

1. Als beide letters in dezelfde rij voorkomen, wordt elke letter vervangen door de letter die er rechts van ligt: (on  $\rightarrow$  na).
2. Als beide letters in dezelfde kolom voorkomen, wordt elke letter vervangen door de letter die er onder van ligt: (ba  $\rightarrow$  ib).
3. Anders wordt elke letter vervangen door de letter van de kolom van de andere letter: (lx  $\rightarrow$  su).

Er zijn  $26 * 26 = 676$  mogelijke diagrammen die gemaakt kunnen worden.

Na de **substitution ciphers** zijn er ook **transposition ciphers**. Zulke ciphers gaan letters niet vervangen, maar gaan ze echter verplaatsen. Dit heeft natuurlijk als nadeel dat de relatieve frequentie van de letters behouden wordt. Twee eenvoudige voorbeelden zijn:

1. Keer elke letter om:

A SIMPLE EXAMPLE  $\rightarrow$  ELPMAXE ELPMIS A

2. Keer de woordvolgorde om, en elk woord keert ook de lettervolgorde om:

A SIMPLE EXAMPLE  $\rightarrow$  A ELPMIS ELPMAXE

Een iets beter voorbeeld is de Rail Fence cipher. Deze heeft als private sleutel het aantal rijen dat gebruikt wordt. Elke letter zal diagonaal geschreven worden, uitgewerkt in Tabel 3.2 op de zin DEFEND THE EAST WALL: Geëncrypteerd is dit dus DNETLEEDHESWLXFTAAX.

D				N				E				T				L		
	E		E		D		H		E		S		W		L		X	
		F				T				A				A				X

Tabel 3.2: Rail Fence cipher.

De laatste methode die besproken wordt is de columnar transposition cipher. Een bericht wordt in rijen geschreven over een bepaald aantal kolommen. Hierna worden de kolommen gesorteerd op basis van de geheime sleutel  $K = k_i k_j \dots k_n$ . Stel  $K = k_3 k_4 k_2 k_1 k_5 k_6 k_7$  en plaintext ATTACK POSTPONED UNTIL TWO AM: Op Tabel 3.3 wordt deze plaintext uitgeschreven in rijen en kolommen. De ciphertext wordt dan TTNAAPTMTSUOAODWCOIXKNLYPETZ.

A	T	T	A	C	K	P
O	S	T	P	O	N	E
D	U	N	T	I	L	T
W	O	A	M	X	X	X

Tabel 3.3: Rail Fence cipher.

Uiteindelijk kan men ook de combinatie maken van **substitution** en **transposition** ciphers, wat de basis vormt van moderne cryptografie.

## 3.2 Moderne cryptografie

### 3.2.1 Symmetrische algoritmen

Vooraleer er in detail kan ingegaan worden op symmetrische algoritmen, moet eerst de term **block cipher** besproken worden. Een block cipher wil zeggen dat informatie in blokken zullen verstuurd worden en kan best vergeleken worden met een substitutiecipher, maar dan toegepast op blokken. Een typische blok grootte varieert van 8 tot 128 bytes en wordt door de meeste algoritmen gebruikt. De **Feistel Cipher encryptie** vormt de basis van moderne blockciphers en maakt gebruik van twee primitieve encryptieoperaties:

- Substitutie (de S-box)
- Permutatie (de P-box)

Het Feistel encryptieschema maakt gebruik van  $n$  ronden, een functie  $F$  en  $\cdot$ . In elke ronde

## Hoofdstuk 4

# Software- en systeembeveiliging