Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Prima prova scritta — temi e correzione

Mauro Brunato

Lunedì 12 giugno 2017

Contenuti

- Testi dei temi d'esame
- Traccia della soluzione del Tema 1
- Griglie di correzione dei temi

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Prima prova scritta

Mauro Brunato

Tema 1

Lunedì 12 giugno 2017

Esercizio 1

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 40 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

1.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

1.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

1.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 1.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 2

Descrivere il meccanismo della firma digitale, con particolare attenzione ai seguenti punti:

- proprietà
- funzioni utilizzate
- struttura di una firma
- procedimento di verifica
- motivazione dei vari blocchi costitutivi, in riferimento alla resistenza ai tentativi di forgiatura.

Esercizio 3

Vogliamo realizzare una rete composta da una DMZ e due Intranet (studenti e docenti).

- Requisiti della DMZ:
  - utilizza una sottorete IP pubblica;
  - contiene un server web (porta 80 TCP) e un server DNS (porta 53 UDP) su due macchine distinte;
  - le intranet devono poter accedere liberamente alle macchine della DMZ;
  - dall'esterno, solo i due servizi indicati devono essere accessibili.
- Requisiti delle due intranet:
  - condividono l'infrastruttura di livello 2, e sono fisicamente separate dalla DMZ;
  - ciascuna deve utilizzare una sottorete IP privata con netmask `255.255.0.0`;
  - possono accedere liberamente alla DMZ;
  - accedono a internet tramite NAT;
  - non devono essere contattabili dalla DMZ.
- Risorse disponibili:
  - un router con due interfacce Ethernet `e0` ed `e1`, dotato di funzionalità 802.1Q, NAT e firewalling;
  - un router con un'interfaccia Ethernet `e0` e un'interfaccia WAN `s0`, dotato di funzionalità 802.1Q, NAT e firewalling;
  - la sottorete IP pubblica `137.85.195.96/29` per la DMZ;
  - l'indirizzo fornito dall'ISP all'interfaccia `s0` del router e il corrispondente default gateway sono rispettivamente l'IP più basso e quello più alto utilizzabili nella sottorete `56.199.203.240/28`;
  - tutti gli switch necessari.

Ogni dato non fornito nell'esercizio può essere stabilito arbitrariamente (se possibile, motivando la scelta).

3.1) Disegnare uno schema di massima della rete evidenziando la posizione dei due router e delle varie reti, fisiche e virtuali.

3.2) Indicare la configurazione (indirizzo IP, netmask, default gateway) dei due server della DMZ, e di un terminale per ciascuna delle intranet.

3.3) Indicare la configurazione delle interfacce dei due router: eventuale suddivisione in interfacce logiche, indirizzo IP e netmask.

3.4) Indicare le configurazioni interne dei due router: tabelle di instradamento, NAT, ACL.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Prima prova scritta

Mauro Brunato

Tema 2

Lunedì 12 giugno 2017

Esercizio 1

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 36 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

1.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

1.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

1.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 1.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 2

Descrivere il meccanismo della firma digitale, con particolare attenzione ai seguenti punti:

- proprietà
- funzioni utilizzate
- struttura di una firma
- procedimento di verifica
- motivazione dei vari blocchi costitutivi, in riferimento alla resistenza ai tentativi di forgiatura.

Esercizio 3

Vogliamo realizzare una rete composta da una DMZ e due Intranet (studenti e docenti).

- Requisiti della DMZ:
  - utilizza una sottorete IP pubblica;
  - contiene un server web (porta 80 TCP) e un server DNS (porta 53 UDP) su due macchine distinte;
  - le intranet devono poter accedere liberamente alle macchine della DMZ;
  - dall'esterno, solo i due servizi indicati devono essere accessibili.
- Requisiti delle due intranet:
  - condividono l'infrastruttura di livello 2, e sono fisicamente separate dalla DMZ;
  - ciascuna deve utilizzare una sottorete IP privata con netmask `255.255.0.0`;
  - possono accedere liberamente alla DMZ;
  - accedono a internet tramite NAT;
  - non devono essere contattabili dalla DMZ.
- Risorse disponibili:
  - un router con due interfacce Ethernet `e0` ed `e1`, dotato di funzionalità 802.1Q, NAT e firewalling;
  - un router con un'interfaccia Ethernet `e0` e un'interfaccia WAN `s0`, dotato di funzionalità 802.1Q, NAT e firewalling;
  - la sottorete IP pubblica `168.233.162.128/29` per la DMZ;
  - l'indirizzo fornito dall'ISP all'interfaccia `s0` del router e il corrispondente default gateway sono rispettivamente l'IP più basso e quello più alto utilizzabili nella sottorete `66.160.93.208/28`;
  - tutti gli switch necessari.

Ogni dato non fornito nell'esercizio può essere stabilito arbitrariamente (se possibile, motivando la scelta).

3.1) Disegnare uno schema di massima della rete evidenziando la posizione dei due router e delle varie reti, fisiche e virtuali.

3.2) Indicare la configurazione (indirizzo IP, netmask, default gateway) dei due server della DMZ, e di un terminale per ciascuna delle intranet.

3.3) Indicare la configurazione delle interfacce dei due router: eventuale suddivisione in interfacce logiche, indirizzo IP e netmask.

3.4) Indicare le configurazioni interne dei due router: tabelle di instradamento, NAT, ACL.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Prima prova scritta

Mauro Brunato

Tema 3

Lunedì 12 giugno 2017

Esercizio 1

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 30 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

1.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

1.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

1.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 1.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 2

Descrivere il meccanismo della firma digitale, con particolare attenzione ai seguenti punti:

- proprietà
- funzioni utilizzate
- struttura di una firma
- procedimento di verifica
- motivazione dei vari blocchi costitutivi, in riferimento alla resistenza ai tentativi di forgiatura.

Esercizio 3

Vogliamo realizzare una rete composta da una DMZ e due Intranet (studenti e docenti).

- Requisiti della DMZ:
  - utilizza una sottorete IP pubblica;
  - contiene un server web (porta 80 TCP) e un server DNS (porta 53 UDP) su due macchine distinte;
  - le intranet devono poter accedere liberamente alle macchine della DMZ;
  - dall'esterno, solo i due servizi indicati devono essere accessibili.
- Requisiti delle due intranet:
  - condividono l'infrastruttura di livello 2, e sono fisicamente separate dalla DMZ;
  - ciascuna deve utilizzare una sottorete IP privata con netmask `255.255.0.0`;
  - possono accedere liberamente alla DMZ;
  - accedono a internet tramite NAT;
  - non devono essere contattabili dalla DMZ.
- Risorse disponibili:
  - un router con due interfacce Ethernet `e0` ed `e1`, dotato di funzionalità 802.1Q, NAT e firewalling;
  - un router con un'interfaccia Ethernet `e0` e un'interfaccia WAN `s0`, dotato di funzionalità 802.1Q, NAT e firewalling;
  - la sottorete IP pubblica `162.39.102.88/29` per la DMZ;
  - l'indirizzo fornito dall'ISP all'interfaccia `s0` del router e il corrispondente default gateway sono rispettivamente l'IP più basso e quello più alto utilizzabili nella sottorete `81.4.61.176/28`;
  - tutti gli switch necessari.

Ogni dato non fornito nell'esercizio può essere stabilito arbitrariamente (se possibile, motivando la scelta).

3.1) Disegnare uno schema di massima della rete evidenziando la posizione dei due router e delle varie reti, fisiche e virtuali.

3.2) Indicare la configurazione (indirizzo IP, netmask, default gateway) dei due server della DMZ, e di un terminale per ciascuna delle intranet.

3.3) Indicare la configurazione delle interfacce dei due router: eventuale suddivisione in interfacce logiche, indirizzo IP e netmask.

3.4) Indicare le configurazioni interne dei due router: tabelle di instradamento, NAT, ACL.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Prima prova scritta

Mauro Brunato

Tema 4

Lunedì 12 giugno 2017

Esercizio 1

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 30 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

1.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

1.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

1.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 1.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 2

Descrivere il meccanismo della firma digitale, con particolare attenzione ai seguenti punti:

- proprietà
- funzioni utilizzate
- struttura di una firma
- procedimento di verifica
- motivazione dei vari blocchi costitutivi, in riferimento alla resistenza ai tentativi di forgiatura.

Esercizio 3

Vogliamo realizzare una rete composta da una DMZ e due Intranet (studenti e docenti).

- Requisiti della DMZ:
  - utilizza una sottorete IP pubblica;
  - contiene un server web (porta 80 TCP) e un server DNS (porta 53 UDP) su due macchine distinte;
  - le intranet devono poter accedere liberamente alle macchine della DMZ;
  - dall'esterno, solo i due servizi indicati devono essere accessibili.
- Requisiti delle due intranet:
  - condividono l'infrastruttura di livello 2, e sono fisicamente separate dalla DMZ;
  - ciascuna deve utilizzare una sottorete IP privata con netmask `255.255.0.0`;
  - possono accedere liberamente alla DMZ;
  - accedono a internet tramite NAT;
  - non devono essere contattabili dalla DMZ.
- Risorse disponibili:
  - un router con due interfacce Ethernet `e0` ed `e1`, dotato di funzionalità 802.1Q, NAT e firewalling;
  - un router con un'interfaccia Ethernet `e0` e un'interfaccia WAN `s0`, dotato di funzionalità 802.1Q, NAT e firewalling;
  - la sottorete IP pubblica `154.75.162.112/29` per la DMZ;
  - l'indirizzo fornito dall'ISP all'interfaccia `s0` del router e il corrispondente default gateway sono rispettivamente l'IP più basso e quello più alto utilizzabili nella sottorete `126.55.130.240/28`;
  - tutti gli switch necessari.

Ogni dato non fornito nell'esercizio può essere stabilito arbitrariamente (se possibile, motivando la scelta).

3.1) Disegnare uno schema di massima della rete evidenziando la posizione dei due router e delle varie reti, fisiche e virtuali.

3.2) Indicare la configurazione (indirizzo IP, netmask, default gateway) dei due server della DMZ, e di un terminale per ciascuna delle intranet.

3.3) Indicare la configurazione delle interfacce dei due router: eventuale suddivisione in interfacce logiche, indirizzo IP e netmask.

3.4) Indicare le configurazioni interne dei due router: tabelle di instradamento, NAT, ACL.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Prima prova scritta

Mauro Brunato

Tema 5

Lunedì 12 giugno 2017

Esercizio 1

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 34 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

1.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

1.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

1.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 1.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 2

Descrivere il meccanismo della firma digitale, con particolare attenzione ai seguenti punti:

- proprietà
- funzioni utilizzate
- struttura di una firma
- procedimento di verifica
- motivazione dei vari blocchi costitutivi, in riferimento alla resistenza ai tentativi di forgiatura.

Esercizio 3

Vogliamo realizzare una rete composta da una DMZ e due Intranet (studenti e docenti).

- Requisiti della DMZ:
  - utilizza una sottorete IP pubblica;
  - contiene un server web (porta 80 TCP) e un server DNS (porta 53 UDP) su due macchine distinte;
  - le intranet devono poter accedere liberamente alle macchine della DMZ;
  - dall'esterno, solo i due servizi indicati devono essere accessibili.
- Requisiti delle due intranet:
  - condividono l'infrastruttura di livello 2, e sono fisicamente separate dalla DMZ;
  - ciascuna deve utilizzare una sottorete IP privata con netmask `255.255.0.0`;
  - possono accedere liberamente alla DMZ;
  - accedono a internet tramite NAT;
  - non devono essere contattabili dalla DMZ.
- Risorse disponibili:
  - un router con due interfacce Ethernet `e0` ed `e1`, dotato di funzionalità 802.1Q, NAT e firewalling;
  - un router con un'interfaccia Ethernet `e0` e un'interfaccia WAN `s0`, dotato di funzionalità 802.1Q, NAT e firewalling;
  - la sottorete IP pubblica `161.102.227.96/29` per la DMZ;
  - l'indirizzo fornito dall'ISP all'interfaccia `s0` del router e il corrispondente default gateway sono rispettivamente l'IP più basso e quello più alto utilizzabili nella sottorete `123.74.196.208/28`;
  - tutti gli switch necessari.

Ogni dato non fornito nell'esercizio può essere stabilito arbitrariamente (se possibile, motivando la scelta).

3.1) Disegnare uno schema di massima della rete evidenziando la posizione dei due router e delle varie reti, fisiche e virtuali.

3.2) Indicare la configurazione (indirizzo IP, netmask, default gateway) dei due server della DMZ, e di un terminale per ciascuna delle intranet.

3.3) Indicare la configurazione delle interfacce dei due router: eventuale suddivisione in interfacce logiche, indirizzo IP e netmask.

3.4) Indicare le configurazioni interne dei due router: tabelle di instradamento, NAT, ACL.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Prima prova scritta

Mauro Brunato

Tema 6

Lunedì 12 giugno 2017

Esercizio 1

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 34 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

1.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

1.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

1.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 1.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 2

Descrivere il meccanismo della firma digitale, con particolare attenzione ai seguenti punti:

- proprietà
- funzioni utilizzate
- struttura di una firma
- procedimento di verifica
- motivazione dei vari blocchi costitutivi, in riferimento alla resistenza ai tentativi di forgiatura.

Esercizio 3

Vogliamo realizzare una rete composta da una DMZ e due Intranet (studenti e docenti).

- Requisiti della DMZ:
  - utilizza una sottorete IP pubblica;
  - contiene un server web (porta 80 TCP) e un server DNS (porta 53 UDP) su due macchine distinte;
  - le intranet devono poter accedere liberamente alle macchine della DMZ;
  - dall'esterno, solo i due servizi indicati devono essere accessibili.
- Requisiti delle due intranet:
  - condividono l'infrastruttura di livello 2, e sono fisicamente separate dalla DMZ;
  - ciascuna deve utilizzare una sottorete IP privata con netmask `255.255.0.0`;
  - possono accedere liberamente alla DMZ;
  - accedono a internet tramite NAT;
  - non devono essere contattabili dalla DMZ.
- Risorse disponibili:
  - un router con due interfacce Ethernet `e0` ed `e1`, dotato di funzionalità 802.1Q, NAT e firewalling;
  - un router con un'interfaccia Ethernet `e0` e un'interfaccia WAN `s0`, dotato di funzionalità 802.1Q, NAT e firewalling;
  - la sottorete IP pubblica `151.21.49.120/29` per la DMZ;
  - l'indirizzo fornito dall'ISP all'interfaccia `s0` del router e il corrispondente default gateway sono rispettivamente l'IP più basso e quello più alto utilizzabili nella sottorete `104.234.17.240/28`;
  - tutti gli switch necessari.

Ogni dato non fornito nell'esercizio può essere stabilito arbitrariamente (se possibile, motivando la scelta).

3.1) Disegnare uno schema di massima della rete evidenziando la posizione dei due router e delle varie reti, fisiche e virtuali.

3.2) Indicare la configurazione (indirizzo IP, netmask, default gateway) dei due server della DMZ, e di un terminale per ciascuna delle intranet.

3.3) Indicare la configurazione delle interfacce dei due router: eventuale suddivisione in interfacce logiche, indirizzo IP e netmask.

3.4) Indicare le configurazioni interne dei due router: tabelle di instradamento, NAT, ACL.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Prima prova scritta

Mauro Brunato

Tema 7

Lunedì 12 giugno 2017

Esercizio 1

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 40 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

1.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

1.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

1.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 1.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 2

Descrivere il meccanismo della firma digitale, con particolare attenzione ai seguenti punti:

- proprietà
- funzioni utilizzate
- struttura di una firma
- procedimento di verifica
- motivazione dei vari blocchi costitutivi, in riferimento alla resistenza ai tentativi di forgiatura.

Esercizio 3

Vogliamo realizzare una rete composta da una DMZ e due Intranet (studenti e docenti).

- Requisiti della DMZ:
  - utilizza una sottorete IP pubblica;
  - contiene un server web (porta 80 TCP) e un server DNS (porta 53 UDP) su due macchine distinte;
  - le intranet devono poter accedere liberamente alle macchine della DMZ;
  - dall'esterno, solo i due servizi indicati devono essere accessibili.
- Requisiti delle due intranet:
  - condividono l'infrastruttura di livello 2, e sono fisicamente separate dalla DMZ;
  - ciascuna deve utilizzare una sottorete IP privata con netmask `255.255.0.0`;
  - possono accedere liberamente alla DMZ;
  - accedono a internet tramite NAT;
  - non devono essere contattabili dalla DMZ.
- Risorse disponibili:
  - un router con due interfacce Ethernet `e0` ed `e1`, dotato di funzionalità 802.1Q, NAT e firewalling;
  - un router con un'interfaccia Ethernet `e0` e un'interfaccia WAN `s0`, dotato di funzionalità 802.1Q, NAT e firewalling;
  - la sottorete IP pubblica `131.60.247.136/29` per la DMZ;
  - l'indirizzo fornito dall'ISP all'interfaccia `s0` del router e il corrispondente default gateway sono rispettivamente l'IP più basso e quello più alto utilizzabili nella sottorete `51.16.5.208/28`;
  - tutti gli switch necessari.

Ogni dato non fornito nell'esercizio può essere stabilito arbitrariamente (se possibile, motivando la scelta).

3.1) Disegnare uno schema di massima della rete evidenziando la posizione dei due router e delle varie reti, fisiche e virtuali.

3.2) Indicare la configurazione (indirizzo IP, netmask, default gateway) dei due server della DMZ, e di un terminale per ciascuna delle intranet.

3.3) Indicare la configurazione delle interfacce dei due router: eventuale suddivisione in interfacce logiche, indirizzo IP e netmask.

3.4) Indicare le configurazioni interne dei due router: tabelle di instradamento, NAT, ACL.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Prima prova scritta

Mauro Brunato

Tema 8

Lunedì 12 giugno 2017

Esercizio 1

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 40 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

1.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

1.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

1.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 1.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 2

Descrivere il meccanismo della firma digitale, con particolare attenzione ai seguenti punti:

- proprietà
- funzioni utilizzate
- struttura di una firma
- procedimento di verifica
- motivazione dei vari blocchi costitutivi, in riferimento alla resistenza ai tentativi di forgiatura.

Esercizio 3

Vogliamo realizzare una rete composta da una DMZ e due Intranet (studenti e docenti).

- Requisiti della DMZ:
  - utilizza una sottorete IP pubblica;
  - contiene un server web (porta 80 TCP) e un server DNS (porta 53 UDP) su due macchine distinte;
  - le intranet devono poter accedere liberamente alle macchine della DMZ;
  - dall'esterno, solo i due servizi indicati devono essere accessibili.
- Requisiti delle due intranet:
  - condividono l'infrastruttura di livello 2, e sono fisicamente separate dalla DMZ;
  - ciascuna deve utilizzare una sottorete IP privata con netmask `255.255.0.0`;
  - possono accedere liberamente alla DMZ;
  - accedono a internet tramite NAT;
  - non devono essere contattabili dalla DMZ.
- Risorse disponibili:
  - un router con due interfacce Ethernet `e0` ed `e1`, dotato di funzionalità 802.1Q, NAT e firewalling;
  - un router con un'interfaccia Ethernet `e0` e un'interfaccia WAN `s0`, dotato di funzionalità 802.1Q, NAT e firewalling;
  - la sottorete IP pubblica `150.170.135.88/29` per la DMZ;
  - l'indirizzo fornito dall'ISP all'interfaccia `s0` del router e il corrispondente default gateway sono rispettivamente l'IP più basso e quello più alto utilizzabili nella sottorete `41.137.95.224/28`;
  - tutti gli switch necessari.

Ogni dato non fornito nell'esercizio può essere stabilito arbitrariamente (se possibile, motivando la scelta).

3.1) Disegnare uno schema di massima della rete evidenziando la posizione dei due router e delle varie reti, fisiche e virtuali.

3.2) Indicare la configurazione (indirizzo IP, netmask, default gateway) dei due server della DMZ, e di un terminale per ciascuna delle intranet.

3.3) Indicare la configurazione delle interfacce dei due router: eventuale suddivisione in interfacce logiche, indirizzo IP e netmask.

3.4) Indicare le configurazioni interne dei due router: tabelle di instradamento, NAT, ACL.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Prima prova scritta

Mauro Brunato

Tema 9

Lunedì 12 giugno 2017

Esercizio 1

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 34 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

1.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

1.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

1.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 1.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 2

Descrivere il meccanismo della firma digitale, con particolare attenzione ai seguenti punti:

- proprietà
- funzioni utilizzate
- struttura di una firma
- procedimento di verifica
- motivazione dei vari blocchi costitutivi, in riferimento alla resistenza ai tentativi di forgiatura.

Esercizio 3

Vogliamo realizzare una rete composta da una DMZ e due Intranet (studenti e docenti).

- Requisiti della DMZ:
  - utilizza una sottorete IP pubblica;
  - contiene un server web (porta 80 TCP) e un server DNS (porta 53 UDP) su due macchine distinte;
  - le intranet devono poter accedere liberamente alle macchine della DMZ;
  - dall'esterno, solo i due servizi indicati devono essere accessibili.
- Requisiti delle due intranet:
  - condividono l'infrastruttura di livello 2, e sono fisicamente separate dalla DMZ;
  - ciascuna deve utilizzare una sottorete IP privata con netmask `255.255.0.0`;
  - possono accedere liberamente alla DMZ;
  - accedono a internet tramite NAT;
  - non devono essere contattabili dalla DMZ.
- Risorse disponibili:
  - un router con due interfacce Ethernet `e0` ed `e1`, dotato di funzionalità 802.1Q, NAT e firewalling;
  - un router con un'interfaccia Ethernet `e0` e un'interfaccia WAN `s0`, dotato di funzionalità 802.1Q, NAT e firewalling;
  - la sottorete IP pubblica `160.163.90.120/29` per la DMZ;
  - l'indirizzo fornito dall'ISP all'interfaccia `s0` del router e il corrispondente default gateway sono rispettivamente l'IP più basso e quello più alto utilizzabili nella sottorete `119.237.183.192/28`;
  - tutti gli switch necessari.

Ogni dato non fornito nell'esercizio può essere stabilito arbitrariamente (se possibile, motivando la scelta).

3.1) Disegnare uno schema di massima della rete evidenziando la posizione dei due router e delle varie reti, fisiche e virtuali.

3.2) Indicare la configurazione (indirizzo IP, netmask, default gateway) dei due server della DMZ, e di un terminale per ciascuna delle intranet.

3.3) Indicare la configurazione delle interfacce dei due router: eventuale suddivisione in interfacce logiche, indirizzo IP e netmask.

3.4) Indicare le configurazioni interne dei due router: tabelle di instradamento, NAT, ACL.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Prima prova scritta

Mauro Brunato

Tema 10

Lunedì 12 giugno 2017

Esercizio 1

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 30 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

1.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

1.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

1.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 1.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 2

Descrivere il meccanismo della firma digitale, con particolare attenzione ai seguenti punti:

- proprietà
- funzioni utilizzate
- struttura di una firma
- procedimento di verifica
- motivazione dei vari blocchi costitutivi, in riferimento alla resistenza ai tentativi di forgiatura.

Esercizio 3

Vogliamo realizzare una rete composta da una DMZ e due Intranet (studenti e docenti).

- Requisiti della DMZ:
  - utilizza una sottorete IP pubblica;
  - contiene un server web (porta 80 TCP) e un server DNS (porta 53 UDP) su due macchine distinte;
  - le intranet devono poter accedere liberamente alle macchine della DMZ;
  - dall'esterno, solo i due servizi indicati devono essere accessibili.
- Requisiti delle due intranet:
  - condividono l'infrastruttura di livello 2, e sono fisicamente separate dalla DMZ;
  - ciascuna deve utilizzare una sottorete IP privata con netmask `255.255.0.0`;
  - possono accedere liberamente alla DMZ;
  - accedono a internet tramite NAT;
  - non devono essere contattabili dalla DMZ.
- Risorse disponibili:
  - un router con due interfacce Ethernet `e0` ed `e1`, dotato di funzionalità 802.1Q, NAT e firewalling;
  - un router con un'interfaccia Ethernet `e0` e un'interfaccia WAN `s0`, dotato di funzionalità 802.1Q, NAT e firewalling;
  - la sottorete IP pubblica `138.227.89.120/29` per la DMZ;
  - l'indirizzo fornito dall'ISP all'interfaccia `s0` del router e il corrispondente default gateway sono rispettivamente l'IP più basso e quello più alto utilizzabili nella sottorete `62.224.211.192/28`;
  - tutti gli switch necessari.

Ogni dato non fornito nell'esercizio può essere stabilito arbitrariamente (se possibile, motivando la scelta).

3.1) Disegnare uno schema di massima della rete evidenziando la posizione dei due router e delle varie reti, fisiche e virtuali.

3.2) Indicare la configurazione (indirizzo IP, netmask, default gateway) dei due server della DMZ, e di un terminale per ciascuna delle intranet.

3.3) Indicare la configurazione delle interfacce dei due router: eventuale suddivisione in interfacce logiche, indirizzo IP e netmask.

3.4) Indicare le configurazioni interne dei due router: tabelle di instradamento, NAT, ACL.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Prima prova scritta

Mauro Brunato

Tema 11

Lunedì 12 giugno 2017

Esercizio 1

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 40 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

1.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

1.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

1.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 1.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 2

Descrivere il meccanismo della firma digitale, con particolare attenzione ai seguenti punti:

- proprietà
- funzioni utilizzate
- struttura di una firma
- procedimento di verifica
- motivazione dei vari blocchi costitutivi, in riferimento alla resistenza ai tentativi di forgiatura.

Esercizio 3

Vogliamo realizzare una rete composta da una DMZ e due Intranet (studenti e docenti).

- Requisiti della DMZ:
  - utilizza una sottorete IP pubblica;
  - contiene un server web (porta 80 TCP) e un server DNS (porta 53 UDP) su due macchine distinte;
  - le intranet devono poter accedere liberamente alle macchine della DMZ;
  - dall'esterno, solo i due servizi indicati devono essere accessibili.
- Requisiti delle due intranet:
  - condividono l'infrastruttura di livello 2, e sono fisicamente separate dalla DMZ;
  - ciascuna deve utilizzare una sottorete IP privata con netmask `255.255.0.0`;
  - possono accedere liberamente alla DMZ;
  - accedono a internet tramite NAT;
  - non devono essere contattabili dalla DMZ.
- Risorse disponibili:
  - un router con due interfacce Ethernet `e0` ed `e1`, dotato di funzionalità 802.1Q, NAT e firewalling;
  - un router con un'interfaccia Ethernet `e0` e un'interfaccia WAN `s0`, dotato di funzionalità 802.1Q, NAT e firewalling;
  - la sottorete IP pubblica `167.101.207.120/29` per la DMZ;
  - l'indirizzo fornito dall'ISP all'interfaccia `s0` del router e il corrispondente default gateway sono rispettivamente l'IP più basso e quello più alto utilizzabili nella sottorete `79.167.218.208/28`;
  - tutti gli switch necessari.

Ogni dato non fornito nell'esercizio può essere stabilito arbitrariamente (se possibile, motivando la scelta).

3.1) Disegnare uno schema di massima della rete evidenziando la posizione dei due router e delle varie reti, fisiche e virtuali.

3.2) Indicare la configurazione (indirizzo IP, netmask, default gateway) dei due server della DMZ, e di un terminale per ciascuna delle intranet.

3.3) Indicare la configurazione delle interfacce dei due router: eventuale suddivisione in interfacce logiche, indirizzo IP e netmask.

3.4) Indicare le configurazioni interne dei due router: tabelle di instradamento, NAT, ACL.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Prima prova scritta

Mauro Brunato

Tema 12

Lunedì 12 giugno 2017

Esercizio 1

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 40 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

1.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

1.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

1.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 1.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 2

Descrivere il meccanismo della firma digitale, con particolare attenzione ai seguenti punti:

- proprietà
- funzioni utilizzate
- struttura di una firma
- procedimento di verifica
- motivazione dei vari blocchi costitutivi, in riferimento alla resistenza ai tentativi di forgiatura.

Esercizio 3

Vogliamo realizzare una rete composta da una DMZ e due Intranet (studenti e docenti).

- Requisiti della DMZ:
  - utilizza una sottorete IP pubblica;
  - contiene un server web (porta 80 TCP) e un server DNS (porta 53 UDP) su due macchine distinte;
  - le intranet devono poter accedere liberamente alle macchine della DMZ;
  - dall'esterno, solo i due servizi indicati devono essere accessibili.
- Requisiti delle due intranet:
  - condividono l'infrastruttura di livello 2, e sono fisicamente separate dalla DMZ;
  - ciascuna deve utilizzare una sottorete IP privata con netmask `255.255.0.0`;
  - possono accedere liberamente alla DMZ;
  - accedono a internet tramite NAT;
  - non devono essere contattabili dalla DMZ.
- Risorse disponibili:
  - un router con due interfacce Ethernet `e0` ed `e1`, dotato di funzionalità 802.1Q, NAT e firewalling;
  - un router con un'interfaccia Ethernet `e0` e un'interfaccia WAN `s0`, dotato di funzionalità 802.1Q, NAT e firewalling;
  - la sottorete IP pubblica `135.224.163.112/29` per la DMZ;
  - l'indirizzo fornito dall'ISP all'interfaccia `s0` del router e il corrispondente default gateway sono rispettivamente l'IP più basso e quello più alto utilizzabili nella sottorete `66.55.242.240/28`;
  - tutti gli switch necessari.

Ogni dato non fornito nell'esercizio può essere stabilito arbitrariamente (se possibile, motivando la scelta).

3.1) Disegnare uno schema di massima della rete evidenziando la posizione dei due router e delle varie reti, fisiche e virtuali.

3.2) Indicare la configurazione (indirizzo IP, netmask, default gateway) dei due server della DMZ, e di un terminale per ciascuna delle intranet.

3.3) Indicare la configurazione delle interfacce dei due router: eventuale suddivisione in interfacce logiche, indirizzo IP e netmask.

3.4) Indicare le configurazioni interne dei due router: tabelle di instradamento, NAT, ACL.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Prima prova scritta

Mauro Brunato

Tema 13

Lunedì 12 giugno 2017

Esercizio 1

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 36 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

1.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

1.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

1.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 1.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 2

Descrivere il meccanismo della firma digitale, con particolare attenzione ai seguenti punti:

- proprietà
- funzioni utilizzate
- struttura di una firma
- procedimento di verifica
- motivazione dei vari blocchi costitutivi, in riferimento alla resistenza ai tentativi di forgiatura.

Esercizio 3

Vogliamo realizzare una rete composta da una DMZ e due Intranet (studenti e docenti).

- Requisiti della DMZ:
  - utilizza una sottorete IP pubblica;
  - contiene un server web (porta 80 TCP) e un server DNS (porta 53 UDP) su due macchine distinte;
  - le intranet devono poter accedere liberamente alle macchine della DMZ;
  - dall'esterno, solo i due servizi indicati devono essere accessibili.
- Requisiti delle due intranet:
  - condividono l'infrastruttura di livello 2, e sono fisicamente separate dalla DMZ;
  - ciascuna deve utilizzare una sottorete IP privata con netmask `255.255.0.0`;
  - possono accedere liberamente alla DMZ;
  - accedono a internet tramite NAT;
  - non devono essere contattabili dalla DMZ.
- Risorse disponibili:
  - un router con due interfacce Ethernet `e0` ed `e1`, dotato di funzionalità 802.1Q, NAT e firewalling;
  - un router con un'interfaccia Ethernet `e0` e un'interfaccia WAN `s0`, dotato di funzionalità 802.1Q, NAT e firewalling;
  - la sottorete IP pubblica `138.47.70.112/29` per la DMZ;
  - l'indirizzo fornito dall'ISP all'interfaccia `s0` del router e il corrispondente default gateway sono rispettivamente l'IP più basso e quello più alto utilizzabili nella sottorete `43.200.78.208/28`;
  - tutti gli switch necessari.

Ogni dato non fornito nell'esercizio può essere stabilito arbitrariamente (se possibile, motivando la scelta).

3.1) Disegnare uno schema di massima della rete evidenziando la posizione dei due router e delle varie reti, fisiche e virtuali.

3.2) Indicare la configurazione (indirizzo IP, netmask, default gateway) dei due server della DMZ, e di un terminale per ciascuna delle intranet.

3.3) Indicare la configurazione delle interfacce dei due router: eventuale suddivisione in interfacce logiche, indirizzo IP e netmask.

3.4) Indicare le configurazioni interne dei due router: tabelle di instradamento, NAT, ACL.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Prima prova scritta

Mauro Brunato

Tema 14

Lunedì 12 giugno 2017

Esercizio 1

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 34 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

1.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

1.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

1.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 1.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 2

Descrivere il meccanismo della firma digitale, con particolare attenzione ai seguenti punti:

- proprietà
- funzioni utilizzate
- struttura di una firma
- procedimento di verifica
- motivazione dei vari blocchi costitutivi, in riferimento alla resistenza ai tentativi di forgiatura.

Esercizio 3

Vogliamo realizzare una rete composta da una DMZ e due Intranet (studenti e docenti).

- Requisiti della DMZ:
  - utilizza una sottorete IP pubblica;
  - contiene un server web (porta 80 TCP) e un server DNS (porta 53 UDP) su due macchine distinte;
  - le intranet devono poter accedere liberamente alle macchine della DMZ;
  - dall'esterno, solo i due servizi indicati devono essere accessibili.
- Requisiti delle due intranet:
  - condividono l'infrastruttura di livello 2, e sono fisicamente separate dalla DMZ;
  - ciascuna deve utilizzare una sottorete IP privata con netmask `255.255.0.0`;
  - possono accedere liberamente alla DMZ;
  - accedono a internet tramite NAT;
  - non devono essere contattabili dalla DMZ.
- Risorse disponibili:
  - un router con due interfacce Ethernet `e0` ed `e1`, dotato di funzionalità 802.1Q, NAT e firewalling;
  - un router con un'interfaccia Ethernet `e0` e un'interfaccia WAN `s0`, dotato di funzionalità 802.1Q, NAT e firewalling;
  - la sottorete IP pubblica `149.193.251.136/29` per la DMZ;
  - l'indirizzo fornito dall'ISP all'interfaccia `s0` del router e il corrispondente default gateway sono rispettivamente l'IP più basso e quello più alto utilizzabili nella sottorete `30.231.26.176/28`;
  - tutti gli switch necessari.

Ogni dato non fornito nell'esercizio può essere stabilito arbitrariamente (se possibile, motivando la scelta).

3.1) Disegnare uno schema di massima della rete evidenziando la posizione dei due router e delle varie reti, fisiche e virtuali.

3.2) Indicare la configurazione (indirizzo IP, netmask, default gateway) dei due server della DMZ, e di un terminale per ciascuna delle intranet.

3.3) Indicare la configurazione delle interfacce dei due router: eventuale suddivisione in interfacce logiche, indirizzo IP e netmask.

3.4) Indicare le configurazioni interne dei due router: tabelle di instradamento, NAT, ACL.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Prima prova scritta

Mauro Brunato

Tema 15

Lunedì 12 giugno 2017

Esercizio 1

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 38 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

1.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

1.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

1.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 1.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 2

Descrivere il meccanismo della firma digitale, con particolare attenzione ai seguenti punti:

- proprietà
- funzioni utilizzate
- struttura di una firma
- procedimento di verifica
- motivazione dei vari blocchi costitutivi, in riferimento alla resistenza ai tentativi di forgiatura.

Esercizio 3

Vogliamo realizzare una rete composta da una DMZ e due Intranet (studenti e docenti).

- Requisiti della DMZ:
  - utilizza una sottorete IP pubblica;
  - contiene un server web (porta 80 TCP) e un server DNS (porta 53 UDP) su due macchine distinte;
  - le intranet devono poter accedere liberamente alle macchine della DMZ;
  - dall'esterno, solo i due servizi indicati devono essere accessibili.
- Requisiti delle due intranet:
  - condividono l'infrastruttura di livello 2, e sono fisicamente separate dalla DMZ;
  - ciascuna deve utilizzare una sottorete IP privata con netmask `255.255.0.0`;
  - possono accedere liberamente alla DMZ;
  - accedono a internet tramite NAT;
  - non devono essere contattabili dalla DMZ.
- Risorse disponibili:
  - un router con due interfacce Ethernet `e0` ed `e1`, dotato di funzionalità 802.1Q, NAT e firewalling;
  - un router con un'interfaccia Ethernet `e0` e un'interfaccia WAN `s0`, dotato di funzionalità 802.1Q, NAT e firewalling;
  - la sottorete IP pubblica `138.149.62.96/29` per la DMZ;
  - l'indirizzo fornito dall'ISP all'interfaccia `s0` del router e il corrispondente default gateway sono rispettivamente l'IP più basso e quello più alto utilizzabili nella sottorete `55.191.94.192/28`;
  - tutti gli switch necessari.

Ogni dato non fornito nell'esercizio può essere stabilito arbitrariamente (se possibile, motivando la scelta).

3.1) Disegnare uno schema di massima della rete evidenziando la posizione dei due router e delle varie reti, fisiche e virtuali.

3.2) Indicare la configurazione (indirizzo IP, netmask, default gateway) dei due server della DMZ, e di un terminale per ciascuna delle intranet.

3.3) Indicare la configurazione delle interfacce dei due router: eventuale suddivisione in interfacce logiche, indirizzo IP e netmask.

3.4) Indicare le configurazioni interne dei due router: tabelle di instradamento, NAT, ACL.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Prima prova scritta

Mauro Brunato

Tema 16

Lunedì 12 giugno 2017

Esercizio 1

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 38 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

1.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

1.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

1.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 1.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 2

Descrivere il meccanismo della firma digitale, con particolare attenzione ai seguenti punti:

- proprietà
- funzioni utilizzate
- struttura di una firma
- procedimento di verifica
- motivazione dei vari blocchi costitutivi, in riferimento alla resistenza ai tentativi di forgiatura.

Esercizio 3

Vogliamo realizzare una rete composta da una DMZ e due Intranet (studenti e docenti).

- Requisiti della DMZ:
  - utilizza una sottorete IP pubblica;
  - contiene un server web (porta 80 TCP) e un server DNS (porta 53 UDP) su due macchine distinte;
  - le intranet devono poter accedere liberamente alle macchine della DMZ;
  - dall'esterno, solo i due servizi indicati devono essere accessibili.
- Requisiti delle due intranet:
  - condividono l'infrastruttura di livello 2, e sono fisicamente separate dalla DMZ;
  - ciascuna deve utilizzare una sottorete IP privata con netmask `255.255.0.0`;
  - possono accedere liberamente alla DMZ;
  - accedono a internet tramite NAT;
  - non devono essere contattabili dalla DMZ.
- Risorse disponibili:
  - un router con due interfacce Ethernet `e0` ed `e1`, dotato di funzionalità 802.1Q, NAT e firewalling;
  - un router con un'interfaccia Ethernet `e0` e un'interfaccia WAN `s0`, dotato di funzionalità 802.1Q, NAT e firewalling;
  - la sottorete IP pubblica `132.242.13.112/29` per la DMZ;
  - l'indirizzo fornito dall'ISP all'interfaccia `s0` del router e il corrispondente default gateway sono rispettivamente l'IP più basso e quello più alto utilizzabili nella sottorete `25.202.41.224/28`;
  - tutti gli switch necessari.

Ogni dato non fornito nell'esercizio può essere stabilito arbitrariamente (se possibile, motivando la scelta).

3.1) Disegnare uno schema di massima della rete evidenziando la posizione dei due router e delle varie reti, fisiche e virtuali.

3.2) Indicare la configurazione (indirizzo IP, netmask, default gateway) dei due server della DMZ, e di un terminale per ciascuna delle intranet.

3.3) Indicare la configurazione delle interfacce dei due router: eventuale suddivisione in interfacce logiche, indirizzo IP e netmask.

3.4) Indicare le configurazioni interne dei due router: tabelle di instradamento, NAT, ACL.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Prima prova scritta

Mauro Brunato

Tema 17

Lunedì 12 giugno 2017

Esercizio 1

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 32 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

1.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

1.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

1.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 1.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 2

Descrivere il meccanismo della firma digitale, con particolare attenzione ai seguenti punti:

- proprietà
- funzioni utilizzate
- struttura di una firma
- procedimento di verifica
- motivazione dei vari blocchi costitutivi, in riferimento alla resistenza ai tentativi di forgiatura.

Esercizio 3

Vogliamo realizzare una rete composta da una DMZ e due Intranet (studenti e docenti).

- Requisiti della DMZ:
  - utilizza una sottorete IP pubblica;
  - contiene un server web (porta 80 TCP) e un server DNS (porta 53 UDP) su due macchine distinte;
  - le intranet devono poter accedere liberamente alle macchine della DMZ;
  - dall'esterno, solo i due servizi indicati devono essere accessibili.
- Requisiti delle due intranet:
  - condividono l'infrastruttura di livello 2, e sono fisicamente separate dalla DMZ;
  - ciascuna deve utilizzare una sottorete IP privata con netmask `255.255.0.0`;
  - possono accedere liberamente alla DMZ;
  - accedono a internet tramite NAT;
  - non devono essere contattabili dalla DMZ.
- Risorse disponibili:
  - un router con due interfacce Ethernet `e0` ed `e1`, dotato di funzionalità 802.1Q, NAT e firewalling;
  - un router con un'interfaccia Ethernet `e0` e un'interfaccia WAN `s0`, dotato di funzionalità 802.1Q, NAT e firewalling;
  - la sottorete IP pubblica `169.163.193.88/29` per la DMZ;
  - l'indirizzo fornito dall'ISP all'interfaccia `s0` del router e il corrispondente default gateway sono rispettivamente l'IP più basso e quello più alto utilizzabili nella sottorete `38.203.186.224/28`;
  - tutti gli switch necessari.

Ogni dato non fornito nell'esercizio può essere stabilito arbitrariamente (se possibile, motivando la scelta).

3.1) Disegnare uno schema di massima della rete evidenziando la posizione dei due router e delle varie reti, fisiche e virtuali.

3.2) Indicare la configurazione (indirizzo IP, netmask, default gateway) dei due server della DMZ, e di un terminale per ciascuna delle intranet.

3.3) Indicare la configurazione delle interfacce dei due router: eventuale suddivisione in interfacce logiche, indirizzo IP e netmask.

3.4) Indicare le configurazioni interne dei due router: tabelle di instradamento, NAT, ACL.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Prima prova scritta

Mauro Brunato

Tema 18

Lunedì 12 giugno 2017

Esercizio 1

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 30 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

1.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

1.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

1.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 1.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 2

Descrivere il meccanismo della firma digitale, con particolare attenzione ai seguenti punti:

- proprietà
- funzioni utilizzate
- struttura di una firma
- procedimento di verifica
- motivazione dei vari blocchi costitutivi, in riferimento alla resistenza ai tentativi di forgiatura.

Esercizio 3

Vogliamo realizzare una rete composta da una DMZ e due Intranet (studenti e docenti).

- Requisiti della DMZ:
  - utilizza una sottorete IP pubblica;
  - contiene un server web (porta 80 TCP) e un server DNS (porta 53 UDP) su due macchine distinte;
  - le intranet devono poter accedere liberamente alle macchine della DMZ;
  - dall'esterno, solo i due servizi indicati devono essere accessibili.
- Requisiti delle due intranet:
  - condividono l'infrastruttura di livello 2, e sono fisicamente separate dalla DMZ;
  - ciascuna deve utilizzare una sottorete IP privata con netmask `255.255.0.0`;
  - possono accedere liberamente alla DMZ;
  - accedono a internet tramite NAT;
  - non devono essere contattabili dalla DMZ.
- Risorse disponibili:
  - un router con due interfacce Ethernet `e0` ed `e1`, dotato di funzionalità 802.1Q, NAT e firewalling;
  - un router con un'interfaccia Ethernet `e0` e un'interfaccia WAN `s0`, dotato di funzionalità 802.1Q, NAT e firewalling;
  - la sottorete IP pubblica `148.209.146.128/29` per la DMZ;
  - l'indirizzo fornito dall'ISP all'interfaccia `s0` del router e il corrispondente default gateway sono rispettivamente l'IP più basso e quello più alto utilizzabili nella sottorete `71.19.17.192/28`;
  - tutti gli switch necessari.

Ogni dato non fornito nell'esercizio può essere stabilito arbitrariamente (se possibile, motivando la scelta).

3.1) Disegnare uno schema di massima della rete evidenziando la posizione dei due router e delle varie reti, fisiche e virtuali.

3.2) Indicare la configurazione (indirizzo IP, netmask, default gateway) dei due server della DMZ, e di un terminale per ciascuna delle intranet.

3.3) Indicare la configurazione delle interfacce dei due router: eventuale suddivisione in interfacce logiche, indirizzo IP e netmask.

3.4) Indicare le configurazioni interne dei due router: tabelle di instradamento, NAT, ACL.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Prima prova scritta

Mauro Brunato

Tema 19

Lunedì 12 giugno 2017

Esercizio 1

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 30 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

1.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

1.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

1.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 1.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 2

Descrivere il meccanismo della firma digitale, con particolare attenzione ai seguenti punti:

- proprietà
- funzioni utilizzate
- struttura di una firma
- procedimento di verifica
- motivazione dei vari blocchi costitutivi, in riferimento alla resistenza ai tentativi di forgiatura.

Esercizio 3

Vogliamo realizzare una rete composta da una DMZ e due Intranet (studenti e docenti).

- Requisiti della DMZ:
  - utilizza una sottorete IP pubblica;
  - contiene un server web (porta 80 TCP) e un server DNS (porta 53 UDP) su due macchine distinte;
  - le intranet devono poter accedere liberamente alle macchine della DMZ;
  - dall'esterno, solo i due servizi indicati devono essere accessibili.
- Requisiti delle due intranet:
  - condividono l'infrastruttura di livello 2, e sono fisicamente separate dalla DMZ;
  - ciascuna deve utilizzare una sottorete IP privata con netmask `255.255.0.0`;
  - possono accedere liberamente alla DMZ;
  - accedono a internet tramite NAT;
  - non devono essere contattabili dalla DMZ.
- Risorse disponibili:
  - un router con due interfacce Ethernet `e0` ed `e1`, dotato di funzionalità 802.1Q, NAT e firewalling;
  - un router con un'interfaccia Ethernet `e0` e un'interfaccia WAN `s0`, dotato di funzionalità 802.1Q, NAT e firewalling;
  - la sottorete IP pubblica `134.254.13.136/29` per la DMZ;
  - l'indirizzo fornito dall'ISP all'interfaccia `s0` del router e il corrispondente default gateway sono rispettivamente l'IP più basso e quello più alto utilizzabili nella sottorete `29.254.52.240/28`;
  - tutti gli switch necessari.

Ogni dato non fornito nell'esercizio può essere stabilito arbitrariamente (se possibile, motivando la scelta).

3.1) Disegnare uno schema di massima della rete evidenziando la posizione dei due router e delle varie reti, fisiche e virtuali.

3.2) Indicare la configurazione (indirizzo IP, netmask, default gateway) dei due server della DMZ, e di un terminale per ciascuna delle intranet.

3.3) Indicare la configurazione delle interfacce dei due router: eventuale suddivisione in interfacce logiche, indirizzo IP e netmask.

3.4) Indicare le configurazioni interne dei due router: tabelle di instradamento, NAT, ACL.

Reti Avanzate e Sicurezza dei Dati, A.A. 2016–2017

Prima prova scritta

Mauro Brunato

Tema 20

Lunedì 12 giugno 2017

Esercizio 1

Alice distribuisce il pacchetto di installazione m di un proprio applicativo su una CDN, alcuni nodi della quale sono però controllati da Charlie. Per cautelarsi da possibili modifiche del pacchetto da parte di terzi, Alice utilizza una funzione hash crittografica per ottenere un riassunto di m che pubblica sul proprio sito web (che Charlie non è in grado di attaccare).
La funzione hash genera un riassunto a 30 bit; Alice, Bob e Charlie possono calcolare un milione di hash al secondo.

1.1) Come può Bob verificare l'integrità del pacchetto m dopo averlo scaricato, ovviamente confidando che la lunghezza del riassunto sia sufficiente? Quanto tempo impiega a effettuare la verifica?

1.2) Charlie vuole diffondere nei nodi della CDN da lui controllati una versione modificata dell'applicativo contenente un virus. Quanto tempo impiegherà Charlie a generare una versione m' del pacchetto di installazione che Bob considererà autentica?

1.3) Supponiamo ora che Alice decida di appendere al pacchetto m un nonce che azzera i 20 bit più significativi del suo riassunto hash.
Quanto impiega Alice a trovare un nonce adeguato?
Data questa proof-of-work di Alice, il disegno fraudolento di Charlie, descritto al punto 1.2, si è complicato o no? Se sì, quanto?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 2

Descrivere il meccanismo della firma digitale, con particolare attenzione ai seguenti punti:

- proprietà
- funzioni utilizzate
- struttura di una firma
- procedimento di verifica
- motivazione dei vari blocchi costitutivi, in riferimento alla resistenza ai tentativi di forgiatura.

Esercizio 3

Vogliamo realizzare una rete composta da una DMZ e due Intranet (studenti e docenti).

- Requisiti della DMZ:
  - utilizza una sottorete IP pubblica;
  - contiene un server web (porta 80 TCP) e un server DNS (porta 53 UDP) su due macchine distinte;
  - le intranet devono poter accedere liberamente alle macchine della DMZ;
  - dall'esterno, solo i due servizi indicati devono essere accessibili.
- Requisiti delle due intranet:
  - condividono l'infrastruttura di livello 2, e sono fisicamente separate dalla DMZ;
  - ciascuna deve utilizzare una sottorete IP privata con netmask `255.255.0.0`;
  - possono accedere liberamente alla DMZ;
  - accedono a internet tramite NAT;
  - non devono essere contattabili dalla DMZ.
- Risorse disponibili:
  - un router con due interfacce Ethernet `e0` ed `e1`, dotato di funzionalità 802.1Q, NAT e firewalling;
  - un router con un'interfaccia Ethernet `e0` e un'interfaccia WAN `s0`, dotato di funzionalità 802.1Q, NAT e firewalling;
  - la sottorete IP pubblica `135.99.232.128/29` per la DMZ;
  - l'indirizzo fornito dall'ISP all'interfaccia `s0` del router e il corrispondente default gateway sono rispettivamente l'IP più basso e quello più alto utilizzabili nella sottorete `11.235.151.176/28`;
  - tutti gli switch necessari.

Ogni dato non fornito nell'esercizio può essere stabilito arbitrariamente (se possibile, motivando la scelta).

3.1) Disegnare uno schema di massima della rete evidenziando la posizione dei due router e delle varie reti, fisiche e virtuali.

3.2) Indicare la configurazione (indirizzo IP, netmask, default gateway) dei due server della DMZ, e di un terminale per ciascuna delle intranet.

3.3) Indicare la configurazione delle interfacce dei due router: eventuale suddivisione in interfacce logiche, indirizzo IP e netmask.

3.4) Indicare le configurazioni interne dei due router: tabelle di instradamento, NAT, ACL.

Traccia della soluzione al tema 1

Esercizio 1 — Funzioni hash

1.1 — Verifica dell'integrità del pacchetto

Bob deve semplicemente calcolare l'hash $H(m)$ del pacchetto scaricato e confrontarlo con il valore pubblicato da Alice. Il tempo di verifica (al netto dello scaricamento del pacchetto e del valore di confronto) consiste nel milionesimo di secondo necessario a calcolare il valore hash.

1.2 — Generazione di un pacchetto fraudolento

Charlie deve generare una serie di pacchetti alternativi $m_1, m_2, \ldots, m_i, \ldots$ finché uno di questi non ha lo stesso valore hash del pacchetto originale: $H(m_i) = H(m)$. La probabilità di collisione è pari a 2^{-40} per ogni nuovo pacchetto.

Di conseguenza, Charlie dovrà generare in media $2^{40} \approx 10^{12}$ pacchetti, impiegando un tempo pari a $10^{12-6} = 10^6$ secondi (10–15 giorni).

1.3 — Proof of effort

La probabilità che un nonce azzeri i primi 20 bit della funzione hash è 2^{-20}, quindi il numero atteso di tentativi da parte di Alice è $2^{20} = 10^6$, e il tempo atteso è un secondo.

Indipendentemente dal numero di bit pari a zero, Charlie è ancora alla ricerca di un preciso valore hash, quindi il suo tempo atteso non cambia.

Esercizio 2 — Firma elettronica

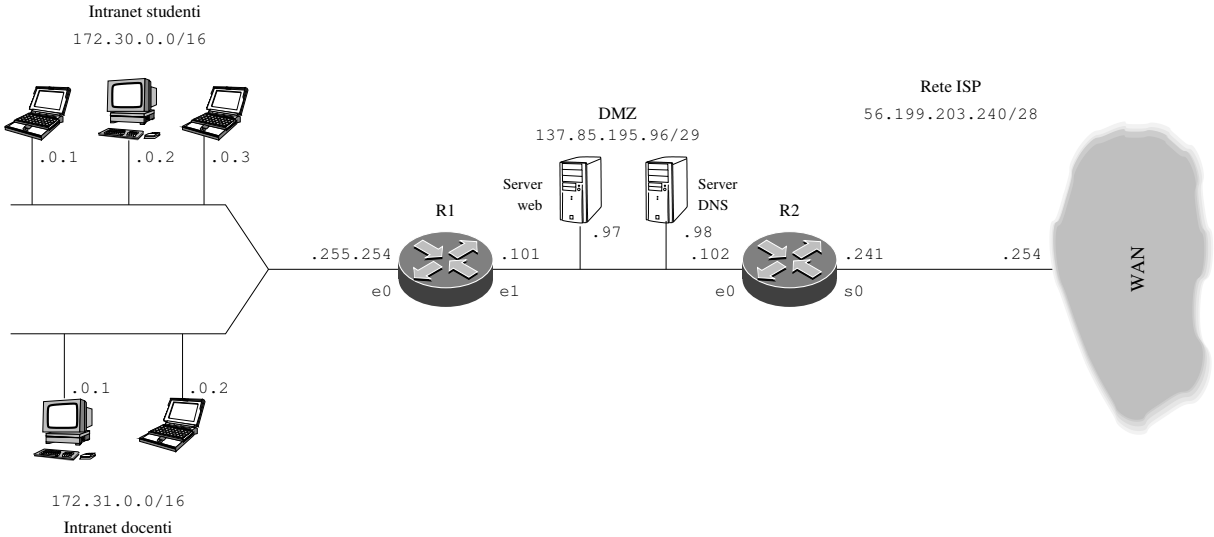
Osservazioni

L'esercizio non chiedeva di parlare delle Certification Authorities, né della Web of Trust, ma solo del meccanismo di base.

Esercizio 3 — Progettazione di una rete locale

Progettazione della rete

Vista la disponibilità di due router con due sole interfacce, e il requisito di mantenere fisicamente separata la DMZ dalle intranet, la soluzione più immediata è la seguente:



Le sottoreti IP delle intranet sono scelte arbitrariamente nell'intervallo pubblico `172.16.0.0/12`, mentre gli indirizzi IP della DMZ e dell'ISP sono dettati dall'esercizio. Le due VLAN fanno capo alla stessa interfaccia fisica di R1, `e0`, che va suddivisa in due interfacce virtuali (vedi più avanti).

Configurazione degli host

Host	IP	Netmask	Default gateway
Terminale Studenti	172.30.0.1	255.255.0.0	172.30.255.254
Terminale Docenti	172.31.0.1	255.255.0.0	172.31.255.254
Server web	137.85.195.97	255.255.255.248	137.85.195.102
Server DNS	137.85.195.98	255.255.255.248	137.85.195.102

Si noti come i due server della DMZ potrebbero beneficiare di una regola di routing che indirizza verso il router R1 i pacchetti diretti verso le intranet, ma tale regola non è strettamente necessaria (anzi, diventa inutile se le intranet sono nattate da R1).

Configurazione delle interfacce dei router

L'interfaccia e0 di R1 va suddivisa in due interfacce logiche, che chiameremo e0.30 ed e0.31. Nei casi in cui siamo liberi di decidere, scegliamo (arbitrariamente) gli indirizzi più alti a disposizione nella sottorete.

Router	Interfaccia reale	Interfaccia virtuale	IP	Netmask
R1	e0	e0.30	172.30.255.254	255.255.0.0
		e0.31	172.31.255.254	255.255.0.0
	e1		137.85.195.101	255.255.255.248
R2	e0		137.85.195.102	255.255.255.248
	s0		56.199.203.241	255.255.255.240

Altre configurazioni

Ecco le tabelle di instradamento di R1, che utilizza l'interfaccia e0 di R2 come default gateway, e di R2:

Destinazione	Interfaccia	Gateway
172.30.0.0/16	e0.30	
172.31.0.0/16	e0.31	
137.85.195.96/29	e1	
0.0.0.0/0		137.85.195.102

Destinazione	Interfaccia	Gateway
137.85.195.96/29	e0	
56.199.203.240/28	s0	
172.30.0.0/15		137.85.195.101
0.0.0.0/0		56.199.203.254

Possiamo assumere che gli IP delle intranet possano viaggiare liberamente all'interno di tutta la rete locale, e che il router R2 si incarichi di effettuare il NAT. I parametri del NAT, applicati a R2, sono dunque i seguenti:

Interfaccia interna: e0
Pool di indirizzi interni: 172.30.0.1–172.30.255.253, 172.31.0.1–172.31.255.253
Interfaccia esterna: s0
Pool di indirizzi esterni: 56.199.203.241

Un'altra possibile soluzione consiste nel far applicare il NAT al router R1.

Per quanto riguarda le ACL, R2 deve occuparsi di bloccare tutti i pacchetti entranti che non siano diretti verso i due servizi della DMZ o appartenenti a connessioni già aperte dall'interno. Ad esempio, la seguente tabella può essere applicata in ingresso all'interfaccia s0:

Protocollo	Provenienza	Destinazione	Flag	Azione	Spiegazione
TCP	0.0.0.0/0:*	137.85.195.97/32:80	*	allow	Server www
UDP	0.0.0.0/0:*	137.85.195.98/32:53	*	allow	Server DNS
*	0.0.0.0/0:*	0.0.0.0/0:*	ESTABLISHED	allow	Iniziati da interno
*	0.0.0.0/0:*	0.0.0.0/0:*	*	deny	Default

Infine, i pacchetti della DMZ (ma, per precauzione, anche delle reti esterne) debbono entrare nelle intranet solamente se "invitati", quindi impostiamo le seguenti regole in ingresso su `e1`:

Protocollo	Provenienza	Destinazione	Flag	Azione	Spiegazione
*	`0.0.0.0/0:*`	`0.0.0.0/0:*`	ESTABLISHED	allow	Iniziati da interno
*	`0.0.0.0/0:*`	`0.0.0.0/0:*`	*	deny	Default

Osservazioni

Sono ovviamente possibili molte soluzioni diverse.

Attenzione: non ha senso spezzare la DMZ in due VLAN come hanno fatto molti.

Griglie di soluzione

Sono elencati, per ogni tema:

- il numero di tentativi N e il tempo richiesto T per l'esercizio 1;
- gli indirizzi IP del ramo ISP e l'intervallo di indirizzi utilizzabili per la DMZ.

```
1
 bit = 40; Nhash = 1.1e+12; Tcharlie = 1.1e+6
 ISP --- IP router: 56.199.203.241; Default gateway: 56.199.203.254
 DMZ --- Intervallo IP 137.85.195.97 - 137.85.195.102

2
 bit = 36; Nhash = 6.9e+10; Tcharlie = 6.9e+4
 ISP --- IP router: 66.160.93.209; Default gateway: 66.160.93.222
 DMZ --- Intervallo IP 168.233.162.129 - 168.233.162.134

3
 bit = 30; Nhash = 1.1e+9; Tcharlie = 1.1e+3
 ISP --- IP router: 81.4.61.177; Default gateway: 81.4.61.190
 DMZ --- Intervallo IP 162.39.102.89 - 162.39.102.94

4
 bit = 30; Nhash = 1.1e+9; Tcharlie = 1.1e+3
 ISP --- IP router: 126.55.130.241; Default gateway: 126.55.130.254
 DMZ --- Intervallo IP 154.75.162.113 - 154.75.162.118

5
 bit = 34; Nhash = 1.7e+10; Tcharlie = 1.7e+4
 ISP --- IP router: 123.74.196.209; Default gateway: 123.74.196.222
 DMZ --- Intervallo IP 161.102.227.97 - 161.102.227.102

6
 bit = 34; Nhash = 1.7e+10; Tcharlie = 1.7e+4
 ISP --- IP router: 104.234.17.241; Default gateway: 104.234.17.254
 DMZ --- Intervallo IP 151.21.49.121 - 151.21.49.126

7
 bit = 40; Nhash = 1.1e+12; Tcharlie = 1.1e+6
 ISP --- IP router: 51.16.5.209; Default gateway: 51.16.5.222
 DMZ --- Intervallo IP 131.60.247.137 - 131.60.247.142

8
 bit = 40; Nhash = 1.1e+12; Tcharlie = 1.1e+6
 ISP --- IP router: 41.137.95.225; Default gateway: 41.137.95.238
 DMZ --- Intervallo IP 150.170.135.89 - 150.170.135.94

9
 bit = 34; Nhash = 1.7e+10; Tcharlie = 1.7e+4
 ISP --- IP router: 119.237.183.193; Default gateway: 119.237.183.206
 DMZ --- Intervallo IP 160.163.90.121 - 160.163.90.126

10
 bit = 30; Nhash = 1.1e+9; Tcharlie = 1.1e+3
 ISP --- IP router: 62.224.211.193; Default gateway: 62.224.211.206
 DMZ --- Intervallo IP 138.227.89.121 - 138.227.89.126
```

11
 bit = 40; Nhash = 1.1e+12; Tcharlie = 1.1e+6
 ISP --- IP router: 79.167.218.209; Default gateway: 79.167.218.222
 DMZ --- Intervallo IP 167.101.207.121 - 167.101.207.126

12
 bit = 40; Nhash = 1.1e+12; Tcharlie = 1.1e+6
 ISP --- IP router: 66.55.242.241; Default gateway: 66.55.242.254
 DMZ --- Intervallo IP 135.224.163.113 - 135.224.163.118

13
 bit = 36; Nhash = 6.9e+10; Tcharlie = 6.9e+4
 ISP --- IP router: 43.200.78.209; Default gateway: 43.200.78.222
 DMZ --- Intervallo IP 138.47.70.113 - 138.47.70.118

14
 bit = 34; Nhash = 1.7e+10; Tcharlie = 1.7e+4
 ISP --- IP router: 30.231.26.177; Default gateway: 30.231.26.190
 DMZ --- Intervallo IP 149.193.251.137 - 149.193.251.142

15
 bit = 38; Nhash = 2.7e+11; Tcharlie = 2.7e+5
 ISP --- IP router: 55.191.94.193; Default gateway: 55.191.94.206
 DMZ --- Intervallo IP 138.149.62.97 - 138.149.62.102

16
 bit = 38; Nhash = 2.7e+11; Tcharlie = 2.7e+5
 ISP --- IP router: 25.202.41.225; Default gateway: 25.202.41.238
 DMZ --- Intervallo IP 132.242.13.113 - 132.242.13.118

17
 bit = 32; Nhash = 4.3e+9; Tcharlie = 4.3e+3
 ISP --- IP router: 38.203.186.225; Default gateway: 38.203.186.238
 DMZ --- Intervallo IP 169.163.193.89 - 169.163.193.94

18
 bit = 30; Nhash = 1.1e+9; Tcharlie = 1.1e+3
 ISP --- IP router: 71.19.17.193; Default gateway: 71.19.17.206
 DMZ --- Intervallo IP 148.209.146.129 - 148.209.146.134

19
 bit = 30; Nhash = 1.1e+9; Tcharlie = 1.1e+3
 ISP --- IP router: 29.254.52.241; Default gateway: 29.254.52.254
 DMZ --- Intervallo IP 134.254.13.137 - 134.254.13.142

20
 bit = 30; Nhash = 1.1e+9; Tcharlie = 1.1e+3
 ISP --- IP router: 11.235.151.177; Default gateway: 11.235.151.190
 DMZ --- Intervallo IP 135.99.232.129 - 135.99.232.134