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.