WHITE PAPER

TECNOLOGIA CLEARSIGHT COATING

Sistemi di videosorveglianza

Panasonic

Panasonic

1. Introduzione

La videosorveglianza esterna oggi è necessaria in una varietà di Aree urbane – come stazioni ferroviarie, aeroporti, strade, e porti.
Le telecamere per questo tipo di videosorveglianza stanno avendo una risoluzione sempre più alta, passando dalla tecnologia analogica a quella IP.
Tuttavia, anche se le telecamere stanno ottenendo una risoluzione sempre più elevata, una scarsa visibilità delle immagini registrate stà diventato un problema.
Questi problemi in particolare nella sorveglianza in ambienti esterni si presentano quando le immagini di scarsa qualità non possono essere utilizzate a causa di fattori esterni, quali le coperture degli obiettivi che si sporcano a causa della pioggia (gocce d'acqua) e della polvere.
Per superare questo tipo di problema Panasonic ha sviluppato una nuova tecnologia unica e originale chiamata "ClearSight" Coating.
Tutte le nuove telecamere H.265 da esterno PTZ, Dome e Bullet utilizzano questa tecnologia di rivestimento sulla copertura degli obiettivi, per ottenere una migliore qualità dell'immagine.

2. Tecnologia Panasonic "ClearSight" Coating

Panasonic ha sviluppato la tecnologia Rain-Wash Coating per alcune telecamere PTZ da esterno H.264 per migliorare la visibilità anche in presenza di pioggia, sporcizia, ecc., ed ottenere una buona visibilità in ambienti esterni.
Con questa tecnologia, i costi di manutenzione per la pulizia della copertura dell'obiettivo sono ridotti al minimo. Tuttavia, nel campo dell'installazione e manutenzione, c'è spazio di miglioramento sulla facilità di installazione e manutenzione come di seguito descritto:

① La resistenza del rivestimento Rain Wash Coating è scarsa e si deteriora quando viene pulita con un panno o toccata con le mani.
Il rivestimento se accidentalmente viene toccato, lo sporco delle impronte digitali aderiscono al rivestimento e ciò non può essere ripristinato con una semplice pulizia.

② Analogamente, il rivestimento protettivi non può essere applicato sulle cupole perché non si può toccare.

Per superare questo problema, Panasonic ha introdotto una nuova tecnologia di rivestimento per le proprie telecamere facili da installare e manutenere.

3. Tecnologia di rivestimento

3.1 Rainwash Coating

Il Rain-Wash Coating è una tecnologia sviluppata da Panasonic per ridurre la stagnazione di gocce e ottenere una auto pulizia della calotta come mostrato nel diagramma.
Grazie a questa caratteristica, si ottiene una buona visibilità e resistenza alla sporcizia causata dalla pioggia.
Ciò consente di ottenere una videosorveglianza ad alta risoluzione in ambienti esterni in ogni condizione.

☞ *figura* 1

Questa tecnologia di rivestimento è applicata anche ai modelli IR LED.
Come mostrato di seguito, l'impatto della riflessione dall' illuminatore IR è ridotta anche in caso di piogge, consentendo una ottima videosorveglianza.

☞ *figura* 2

3.2 Tecnologia "ClearSight" Coating

Al fine di migliorare la resistenza meccanica del rivestimento, che era un problema nella precedente tecnologia Rain Wash Coating, è stato sviluppato il nuovo rivestimento "ClearSight" che facilita l'installazione e la manutenzione.

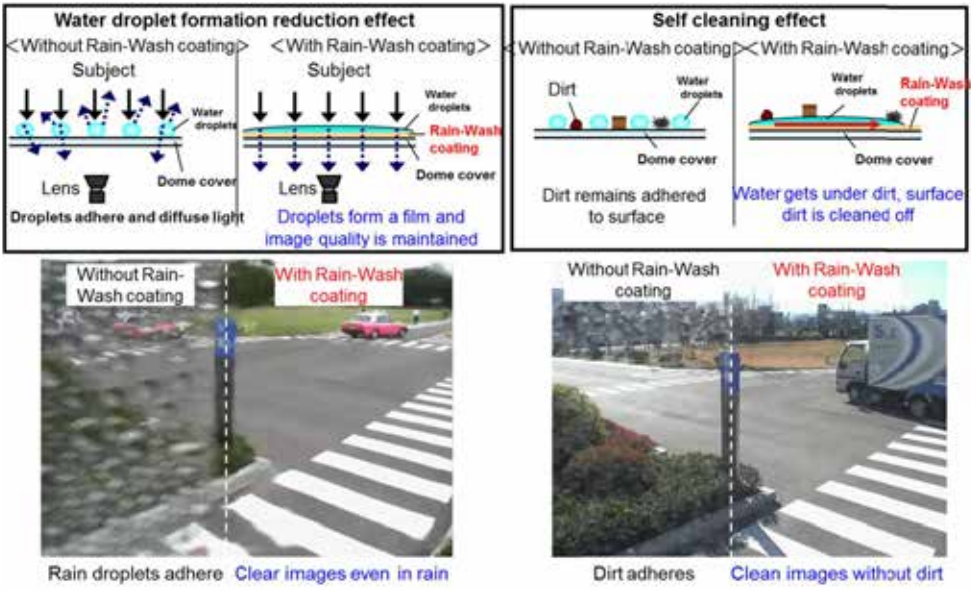
- Diverso materiale di rivestimento
- Aumento dello spessore del rivestimento, maggiore adesione al substrato della cupola

Grazie a un metodo di rivestimento totalmente originale con un maggior spessore della pellicola, si garantisce la qualità, uniformità e prevenzione delle irregolarità del rivestimento. Con questa tecnologia di rivestimento, le impronte digitali e la sporcizia possono essere tolte con una spugna bagnata anche se la cupola è stata accidentalmente toccata durante l'installazione o la manutenzione.
La copertura può anche essere lavata con un detergente neutro. In questo modo, i problemi che c'erano con la tecnologia precedente Rain-Wash Coating sono ora superati. Inoltre, questo trattamento protettivo può essere utilizzato allo stesso modo nei modelli precedenti, migliorando la facilità di installazione.

☞ *figura* 3

4. Conclusione

Tutte le nuove telecamere H.265 da esterno PTZ, Dome e Bullet sono dotate di questa tecnologia "ClearSight" di rivestimento sulla copertura degli obiettivi contribuendo ad aumentare la qualità dell'immagine grazie alla migliore resistenza alla sporcizia, ma anche a ridurre i costi operativi e di manutenzione.



☞ *figura* 1

☞ *figura* 2

☞ *figura* 3

WHITE PAPER

TECNOLOGIA STABILIZZATORE ZOOM INTELLIGENTE

Sistemi di videosorveglianza

Panasonic

Panasonic

1. Introduzione

Le richieste di prestazioni delle telecamere di sorveglianza sono costantemente in aumento negli ultimi anni a causa delle maggiori preoccupazioni sociali sul terrorismo, oltre alle preoccupazioni in materia di sicurezza stradale e ferroviaria.
Le prestazioni richieste, includono una maggiore risoluzione tra cui il 4K, una maggiore compressione dei dati basata su tecnologia H.265 e la sorveglianza in ambienti con bassa luminosità all'aperto. In particolare, l'impossibilità di ottenere immagini soddisfacenti, come ad esempio da immagini mosse, a causa dell'ambiente in cui è installata la telecamera, è diventato un problema in particolare in ambienti esterni critici, inclusi quelli di sorveglianza urbana.
Per superare questo problema, Panasonic ha sviluppato una nuova telecamera PTZ H.265 di alto livello, ottimizzata per la sorveglianza di ambienti esterni.

2. Tecnologia Stabilizzatore Zoom Intelligente

Le telecamere PTZ sono state equipaggiate negli ultimi anni con funzioni di ingrandimento zoom per usi esterni di sorveglianza, consentendo la sorveglianza da punti sempre più lontani. D'altra parte, le telecamere sono installate in punti alti per consentire la sorveglianza da una distanza più elevata con la problematica della stabilità dell'immagine a causa degli effetti del vento, soprattutto quando si utilizza il massimo dell' ingrandimento. Questo problema è superato con l'utilizzo di due tecnologie combinate tra loro:

① Tecnologia per rilevare l'instabilità meccanica della telecamera e la relativa correzione delle immagini;
② Tecnologia per rilevare elettronicamente il movimenti dell'immagine e la relativa correzione.

Panasonic ha sviluppato telecamere PTZ dotate delle due tecnologie appena descritte. Quest'ultime consentono di ottenere un video stabilizzato con vibrazioni ridotte anche con lo zoom al massimo dell' ingrandimento, consentendo una sorveglianza in ampi spazi esterni.

3. Tecnologia Stabilizzatore Zoom Intelligente

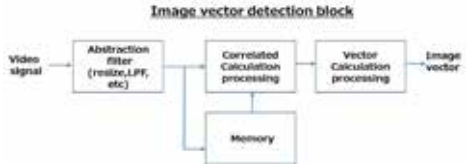
Un livello più elevato di stabilizzazione delle immagini viene raggiunto combinando le due tecnologie: rilevazione del movimento fisico dai sensori giroscopici e rilevamento vettoriale della instabilità dell' immagine ripresa.

3.1 Rilevamento giroscopico

Acquisendo i dati dai sensori giroscopici ad alta velocità, viene rilevata una vibrazione fino a 30 Hz, e combinata in base alla instabilità della ripresa video (cropping) per ottenere la migliore stabilizzazione dell'immagine.
Ciò è molto efficace nella riduzione delle vibrazioni verticali, orizzontali e della distorsione "rolling shutter", principalmente nelle riprese a distanze medie e lunghe.

3.2 Rilevamento vettoriale di immagini

Con la tecnologia di elaborazione dell'immagine di Panasonic, studiata per l'elaborazione delle immagini dei circuiti LSI, è possibile rilevare vibrazioni minime fino a 15 Hz e l'instabilità del video viene regolata in base alla quantità di movimento tra i fotogrammi per ottenere una stabilizzazione dell'immagine.



3.3 Stabilizzazione Zoom Intelligente

In precedenza, era stato adottato un metodo di rilevamento giroscopico o un metodo di rilevazione vettoriale di movimento dalle immagini (rilevazione vettoriale), ma non entrambi. Tuttavia, ognuno di questi metodi ha le proprie problematiche, come sottolineato di seguito.

♦ Rilevazione giroscopica

C'è un limite al rapporto S/N nel rilevamento delle vibrazioni. In alcuni casi, la sfocatura video dovuta a lievi vibrazioni non possono essere sufficientemente corrette (questo si verifica frequentemente ad un alto ingrandimento.)

♦ Rilevamento vettoriale

Le immagini vengono utilizzate per rilevare le vibrazioni, in questo caso la precisione di rilevazione potrebbe non essere stabile in alcuni casi a causa delle condizioni di ripresa con il soggetto in movimento.
Per superare questi problemi, Panasonic ha sviluppato la tecnologia di "Stabilizzazione Zoom Intelligente". Questa tecnologia è basata sul metodo di rilevazione giroscopica e combinata con il metodo di rilevazione vettoriale.
Utilizzando le informazioni del sensore giroscopico, la precisione di rilevazione vettoriale è stabilizzata e alla minima vibrazione che non può essere completamente corretta con il rilevamento giroscopico, può essere rilevato dal vettore dell'immagine e corretto e in questo caso si ottiene una immagine stabile anche con il massimo ingrandimento dello zoom.

4. Conclusione

Le nuove Telecamere PTZ H.265 di Panasonic dotate della nuova funzione di stabilizzazione dello zoom intelligente, possono ottenere immagini stabili anche con l'utilizzo di super teleobiettivi. Questa funzione può essere impiegata per la sorveglianza urbana di ampi spazi come le autostrade per ottenere immagini stabili in abbinamento alle applicazioni di analisi video, creando così soluzioni di sorveglianza esterne di alto livello.

WHITE PAPER

SECURE COMMUNICATION

Quanto è sicuro il tuo sistema di videosorveglianza?

Sistemi di videosorveglianza

Panasonic

Panasonic

1. Introduzione

Gli attacchi informatici contro i dispositivi IoT sono in aumento negli ultimi anni, anche i sistemi di videosorveglianza connessi ad Internet possono essere oggetto di questo genere di attacchi.
La resistenza all'attacco informatico sta dunque diventando un fattore importante nella scelta di un sistema di videosorveglianza appropriato.
Per scegliere correttamente un sistema di videosorveglianza IP bisognerebbe porsi alcune semplice domande:

- "Perché ho bisogno di sistema di videosorveglianza IP?"
- "Quali metodi sono attualmente utilizzati?"
- "Perché dovremmo prestare maggiore attenzione alla sicurezza nelle reti informatiche?"

Durante le visite ai nostri clienti abbiamo notato frequentemente che gli utenti non prendono alcuna precauzione per proteggere le loro reti dati dove transitano i segnali del sistema di videosorveglianza.
Vediamo password mantenute a default di fabbrica, impostazioni DHCP, reti aperte non protette connesse ad Internet e molto altro ancora.
I recenti fatti di cronaca dovrebbero far riflettere su i danni che puoi provocare un attacco informatico su larga scala anche a chi pensa di non aver nulla di così importante da proteggere.
Nessuna rete IT professionale viene ormai progettata e realizzata senza un adeguata protezione.
I dipartimenti IT hanno appreso, talvolta a loro spese, quanto sia importante la sicurezza delle reti.
Tuttavia, questo "modus operandi" è ancora raramente utilizzato nell'ambito della trasmissione video su IP dei sistemi di sorveglianza.
Le impostazioni di protezione esistenti vengono semplicemente ignorate e non configurate.
Gli aggiornamenti sulla sicurezza delle telecamere vengono ignorati ed i contratti di manutenzione non vengono stipulati per risparmiare sui costi di esercizio.
Spesso può essere fuorviante credere di godere di una totale sicurezza senza aver messo in atto le adeguate contromisure.
Esiste una grande varietà di metodi per attaccare i sistemi di videosorveglianza, in questo documento verranno messi in evidenza i rischi che si possono correre se non si attivano i dovuti livelli di protezione.

2. Rischi nell'utilizzo delle credenziali di accesso di default

Tramite il sito internet http://www.insecam.org è possibile visualizzare le immagini live di migliaia di telecamere IP in tutto il mondo di cui altre 1300 solo in Italia. Queste trasmissioni includono tutto ciò che riguarda le vedute delle aziende, la sorveglianza della città, le residenze private, le stalle di cavalli, i garage, gli uffici, i negozi, ecc..

Tutto in chiaro senza richiesta di credenziali e senza alcun controllo da parte degli utenti proprietari delle immagini. Tutto ciò è possibile grazie al fatto che queste camere sono connesse e pubblicate su Internet senza password o mantenendo le credenziali di default del fabbricante. Le stime affermano che le credenziali di default sono state modificate in più del 60% dei sistemi di videosorveglianza installati nel mondo.Questa mancanza li rende molto facili da manipolare.
Come dimostrano gli esempi provenienti da Internet, le telecamere IP possono essere viste da chiunque su qualsiasi piattaforma che si collega al Web, incluso i normali SmartPhone.
I rischi che si possono correre in questi casi sono notevoli, vediamo alcuni esempi:

- Telecamere che controllano un'area pubblica che senza autorizzazione esplicita vengono trasmesse tramite Internet (cloud, etc..) per semplicità di utilizzo da parte dell'utilizzatore o per motivi legati alle tipologie di connessioni di rete disponibili in quella zona. La mancata impostazione o modifica delle credenziali di accesso rende le immagini visibili a tutti anche ad utenti non autorizzati. Questa grave inosservanza alla vigente norma sulla Privacy può portare a sanzioni anche penali sia verso il titolare dell'impianto che verso l'azienda che si è occupata dell'installazione e della programmazione dello stesso.

- Telecamere che controllano magazzini, negozi o abitazioni private, liberamente accessibili via Internet. Qualsiasi potenziale delinquente può vedere esattamente quando gli uffici di una società sono chiusi, quando un magazzino è pieno di merce di valore, le abitudini del proprietario della casa o del negozio, ecc.. Grazie a queste informazioni, il delinquente può pianificare il momento migliore per eseguire una rapina o un furto, magari manomettendo il sistema di videosorveglianza prima di agire così da non essere ripreso.

- Le telecamere possono anche mostrare la posizione precisa delle aree di allarme impostate sulle immagini, o dove sono presenti sensori di prossimità o barriere ad infrarossi. I delinquenti possono sfruttare queste informazioni per agire evitando queste zone oppure disattivandole prima di entrare nell'area allarmata.
- Ancora più critici sono i casi di immagini rubate nella sfera privata (da appartamenti, giardini, piscine, ecc.) che diventano pubblici. Queste informazioni potrebbero essere utilizzate anche impropriamente da persone senza scrupoli per causare danni a minori, alla propria famiglia o ad i propri conoscenti.

Questi sono solo alcuni esempi dei rischi che si possono correre sottovalutando gli aspetti legati alla sicurezza dei sistemi di videosorveglianza.

3. Cosa può accadere in caso di accesso non autorizzato ad una telecamera?

Sono possibili vari scenari. Prima di tutto, una telecamera di sicurezza dovrebbe naturalmente aumentare la sicurezza in aree che richiedono protezione.
Se uno sconosciuto ottiene accesso non autorizzato alla telecamera la può disattivare, manipolare o trasmettere false informazioni in tutta inclusi virus e software malware.
In passato con i vecchi sistemi analogici era quasi impossibile il verificarsi di un problema simile, le connessioni con cavi coassiali o doppino telefonico erano praticamente inattaccabili ed anche in caso di manomissione potevano provocare danni limitati e soprattutto non diffondibili ad altri sistemi come invece accade per le connessioni su reti telematiche.
La sempre maggiore proliferazione delle telecamere IP rende la necessità di proteggere i sistemi di videosorveglianza e la rete a cui sono collegati, in quanto che i metodi per attaccarli sono diventati sempre maggiori e di facile reperibilità, anche con tutorial presenti su comuni siti Internet.
Inoltre, i sistemi video vengono sempre più interconnessi con gli altri sistemi di sicurezza come l'antincendio, l'antintrusione ed il controllo accessi.

Possibili effetti di un attacco hacker sulle telecamere IP:

1. L'accesso IP alle telecamere può essere utilizzato per infiltrarsi nell'intera rete dati
2. Le telecamere wireless possono essere attaccate tramite la rete WLAN (wifi)
3. I dati video possono essere manipolati
4. È possibile leggere i dati rilevanti dell'intera rete (indirizzi IP, dati sui server, database ...)
5. Le telecamere possono essere dotate di backdoor lasciate volutamente aperte dal produttore, che vengono utilizzate per scopi di spionaggio industriale ed altro.

4. Chi puoi essere interessato a carpire informazioni e perché?

La maggior parte delle aziende o dei privati che sono dotati di sistemai di videosorveglianza crede che le immagini che essi riprendono siano di scarsa rilevanza a livello generale e che siano importanti solo per un uso interno.
Nella realtà dei fatti non è così.
I criminali stanno imparando ad usare gli strumenti informatici sempre più diffuso nel mondo di oggi per poter pianificare con cura le loro azioni.
Immagini che sembrano innocue per alcuni possono essere molto importanti per altri, le telecamere spesso riprendono non sono la zona a cui sono asservite ma molto altro, sconfinando in un ambiente privato vicino oppure inquadrando aree pubbliche.

Per esempio una telecamere di un negozio che inquadra per caso anche l'ingresso di una banca può essere monitorata per capire se e quando l'ingresso e sorvegliato, senza accedere alla rete della banca (sicuramente protetta) ma accedendo a quella nel piccolo negozio, dei criminali potrebbero pianificare una rapina senza la necessità di eseguire sopraluoghi in campo.
Il pericolo non deve sempre arrivare da criminali incalliti o servizi segreti collegati a livello globale come si vede nei film.
Frequentemente lavoratori frustrati o disonesti, ex dipendenti o piccoli delinquenti, sono le persone che possono carpire ed usare in modo illegale queste informazioni, in modo diretto o vendendole ad altri che possono essere interessati.

Informazioni dalla telecamera	Conclusioni
Presenza o meno di personale all'interno del sito monitorato.	• Capire il momento migliore per entrare. • Capire dove e quando si trova il personale di sicurezza dell'edificio. • Capire se ci sono momenti in cui è meno rischioso entrare. (Ambito privato: la persona va a lavorare da ... a ...)
Monitoraggio di un punto vendita.	• Capire se ci sono scaffali con oggetti di valore non inquadrati dalle telecamere. • Capire quali sono le lacune nel sistema di sorveglianza e di allarme in generale.
Monitoraggio di un punto cassa o di uno sportello bancomat.	• Capire se le immagini possono essere manipolate per mascherare eventuali furti. • Capire come operare per installare dispositivi per la clonazione delle carte. • Leggere codici di sicurezza digitati dall'utente sul tastierino del bancomat.
Monitoraggio di un magazzino.	• Capire come le rampe di carico sono controllate. • Capire dove le merci rubate possono essere portate all'esterno senza essere visti (ad esempio, porte non supervisionate). • Presenza o meno di materiale nel magazzino.
Monitoraggio aree esterne e perimetri.	• Capire se ci sono zone non controllate. • Capire dove sono le zone più idonee per accedere e per uscire senza essere visti. • Capire se le telecamere possono essere spostate o oscurate. (PTZ, ecc..) • Capire se sono installati sistemi di allarme perimetrale o di altro genere.
Area informatica - Sala server	• Capire se e quando il personale è presente. • Capire se informazioni importanti per accedere ai server possono essere visualizzate dalle telecamere (modelli server, password, ecc.)

5. Opportunità di hacking tramite una telecamera IP

5.1. Ogni telecamera IP è un client della rete

Poiché le telecamere si trovano nella rete proprio come qualsiasi PC o altro dispositivo e dispongono di indirizzi IP, rappresentano anche possibili punti di accesso alla rete stessa. Ogni telecamera deve essere considerata come un client o un utente di rete e può, come qualsiasi altro dispositivo della rete, essere attaccato. Ciò significa che se in una rete vengono già protetti PC o altri dispositivi, è necessario proteggere allo stesso modo anche le telecamere.

5.2. Errori nel sistema operativo della telecamera

Le telecamere IP sono oggi processori ad alte prestazioni in miniatura con i propri sistemi operativi e software per l'elaborazione delle immagini. Potenziali errori e lacune di sicurezza nel software di una telecamera possono essere sfruttate per lanciare attacchi informatici.

5.3. Backdoors presenti nelle telecamere

Backdoors (conosciute anche come trapdoors) si riferiscono a parti del software (spesso introdotte consapevolmente dal produttore) che consentono agli utenti di evitare il controllo di sicurezza di accesso standard per ottenere l'accesso ad un dispositivo IP (per esempio una telecamera) o ad una funzione altrimenti protetta di un'applicazione informatica (per esempio i software di gestione video per la sicurezza).
È emerso di recente che il più grande produttore mondiale di telecamere IP ha inserito in tutti i propri prodotti un sistema che consente di accedere alle immagini sfruttando proprio una di queste backdoor. Tale scoperta a messo a rischio migliaia di impianti in tutto il mondo con particolare attenzione di quelli collegati ad Internet. Vedi articolo del 24 novembre 2016 sul sito Inglese di informazione Newsgram:
http://www.newsgram.com/imagine-a-world-where-everyone-can-be-tracked-is-the-worlds-biggest-surveillance-camera-maker-sending-footage-to-china/

Rilevamento e rimozione dei virus

5.4. Manipolazione delle immagini

L'accesso alla tecnologia delle telecamere ovviamente significa che anche i dati video associati possono essere manipolati e modificati. Ad esempio: i preset (viste specifiche che possono essere configurate in una telecamera motorizzata) possono essere modificati o rimossi lasciando scoperte completamente intere aree precedentemente sorvegliate; gli allarmi possono essere disattivati o spediti a destinatari differenti; nelle telecamere con ottica motorizzata le immagini possono essere sfocate, e molto altro ancora. In molti casi le modifiche effettuate non verranno immediatamente notate dagli utenti poiché la telecamera, in linea di massima, continua a funzionare normalmente e quanto lo si nota è ormai troppo tardi. Oppure anche se lo si nota subito, l'intervento del manutentore potrebbe non essere immediato e questo darebbe il tempo ad i malintenzionati di agire indisturbati.

5.5. Attacchi verso i software di gestione e i sistemi di registrazione

I sistemi di gestione video implementati come soluzioni software stanno diventando sempre più popolari, poiché solo un PC è in grado di dare la flessibilità necessari per soddisfare le richieste degli utenti finali . Il software è spesso anche offerto gratuitamente per piccoli impianti fino a 15 o 20 telecamere, il che significa che un sistema funzionale può essere ottenuto ad un prezzo molto attraente. La gestione del sistema è molto semplice in quanto il know-how per i sistemi basati su PC (di solito Windows o Linux) è già conosciuto o disponibile internamente nel reparto IT dell'azienda. Di contro un sistema basato su PC sarà anche più a rischio di attacchi informatici, poiché le falle nella sicurezza dei sistemi operativi commerciali sono ben note facilmente sfruttabili. In linea generale con i sistemi basati su PC si possono incontrare i seguenti problemi:

- Non sono dotati di un software di protezione appropriato.
- Gli aggiornamenti del sistema operativo non vengono eseguiti con continuità.
- I processi di backup potrebbero non essere attivi o insufficienti a proteggere i dati.
- Il collegamento di tali PC alla rete aziendale, può facilitare l'accesso degli hacker ad i dati sensibili dell' azienda.
- Altri software potrebbero venire installati sul PC creando problemi all'applicazione di gestione e registrazione del sistema di sicurezza.
- Instabilità e periodici riavvii richiesti tipicamente dai sistemi operativi tradizionali che potrebbero bloccare il sistema in modo casuale ed inaspettato.

6. Cosa deve essere fatto per proteggere il proprio sistema di sorveglianza

Le misure di protezione sono sempre essenziali nei sistemi di monitoraggio video e devono essere inserite urgentemente se non sono già state pianificate in anticipo livello adeguato. Purtroppo, la grande maggioranza di produttori di telecamere, aziende specializzate e integratori, non sono oggi in grado di affrontare tutte le possibili minacce e non riescono ad informare i propri clienti in modo adeguato.

- I dati video continuano per essere trasmessi in forma non crittografata sulla rete.
- L'accesso da parte di utenti non autorizzati, persone, ecc. non viene monitorato e rilevato.
- Le modifiche nella struttura della rete, nella configurazione della telecamera, nei dati trasmessi, ecc. non possono essere rilevate o quando vengono rilevate è troppo tardi.
- I metodi di crittografia non vengono offerti affatto o solo in forma OpenSSL.
- Le password rimangono nell'impostazione predefinita o vengono inserite in forma semplice come "1234" "Admin / admin".
- I dati video vengono memorizzati in forma non crittografata, facilitando l'accesso e consentendo la manipolazione o l'eliminazione degli stessi dagli hard disk.
- L'assenza di protezione antivirus significa che virus, trojan e altri malware non vengono rilevati dal sistema.
- Gli aggiornamenti dei dispositivi non vengono eseguiti in modo adeguato.
- Le telecamere funzionano per anni senza alcuna manutenzione sia hardware che software.

Le nostre raccomandazioni

1. Modificare immediatamente le credenziali standard quando si installa un dispositivo.
2. Informare gli utenti finali sulla necessità di eseguire aggiornamenti periodici al proprio sistema includendoli per esempi in un contratto di manutenzione.
3. Crittografare tutti i dati trasferiti tra telecamere, registratori e VMS.
4. Installare uno scanner antivirus in tutti i sistemi video basati su PC per individuare e rimuovere immediatamente eventuali minacce. Gli antivirus devo essere adeguatamente configurati per non interferire con corretto funzionamento del sistema di videosorveglianza.
5. Controllare le politiche del firewall, aprire le porte, ecc., anche per i sistemi video, mai disabilitare completamente i firewall di rete.
6. Utilizzare sistemi attivi per monitorare eventuali modifiche all'interno della rete.

7. Le soluzioni Panasonic per proteggere i propri clienti

Noi di Panasonic stiamo lavorando da molti anni sui nostri prodotti per essere in grado di offrire ai nostri clienti una soluzione per salvaguardare i loro sistemi da tutte le possibili minacce interne ed esterne. Con l'ultima generazione di dispositivi IPro Extreme, i clienti hanno ora la possibilità, senza alcun costo aggiuntivo, di proteggere il loro sistema dagli attacchi informatici. I dispositivi Panasonic possiedono le seguenti caratteristiche principali:

1. Le nuove telecamere non hanno più credenziali di accesso di default impostate dalla fabbrica, l'utente alla prima accensione imposta le sue credenziali seguendo un criterio obbligato di scelta delle chiavi per garantire una alto livello di sicurezza.
2. I trasferimenti di dati tra telecamere, registratori e VMS sono completamente crittografati.
3. I certificati firmati da Symantec vengono preinstallati sulle telecamera in fabbrica, il metodo crittografico utilizzato da Panasonic utilizza il protocollo SSL ma con un metodo proprietario. Tale metodo consente una crittografia dei dati molto veloce (17ms rispetto a 43ms con lo standard OpenSSL).
4. Sono utilizzati registratori con un sistema operativo proprietario che garantisce la massima affidabilità e la totale sicurezza non essendo soggetto al rischio legato a virus informatici. Inoltre essendo slegato dai PC che visualizzano le immagini, nel caso questi si spengano o si resettino a causa di problemi legati ai loro sistemi operativi, il registratore continuerà autonomamente a registrare le immagini.

8. Conclusioni

Come già accennato, ci sono potenzialmente numerose minacce per sistemi di videosorveglianza, la resistenza a tali minacce diventerà probabilmente ancora più importante in futuro con i progressi nello IoT.
Panasonic lavora continuamente per migliorare la sicurezza dei propri prodotti identificando ed eliminando rapidamente queste minacce, concentrandosi su i quattro aspetti principali per ottenere il massimo livello di sicurezza all'interno del proprio sistema.

1. Crittografia dei dati.
2. Crittografia delle comunicazioni, e delle registrazioni.
3. Monitoraggio e verifica contro l'alterazione dei dati.
4. Analisi delle vulnerabilità del sistema.

Con i nostri prodotti avrete la certezza della massima protezione e riservatezza dei dati nel vostro sistema di Videosorveglianza, e del rischio quasi azzerato di subire attacchi informatici sia dall'interno che dall'esterno della vostra rete.
Inoltre le immagini registrate potranno essere utilizzate sempre in sede di giudizio con la garanzie di non poter essere mai contestate.

WHITE PAPER

TECNOLOGIA SECURE COMMUNICATION

Sistemi di videosorveglianza

Panasonic

Panasonic

1. Introduzione

Gli attacchi informatici contro i dispositivi IoT sono in aumento negli ultimi anni, anche i sistemi di videosorveglianza connessi ad Internet possono essere oggetto di questo genere di attacchi.
La resistenza all'attacco informatico sta dunque diventando un fattore importante nella scelta di un sistema di videosorveglianza appropriato.
I modelli di telecamere della serie i-PRO Extreme di Panasonic possono inviare le immagini con certificati digitali preinstallati, crittografare le comunicazioni verso i server di registrazione e rilevare alterazioni nei dati trasmessi, prevenendo l'attacco prima che questo danneggi il sistema.
Dotando il proprio sistema di tali funzioni vengono messe in atto tutte le contromisure contro la perdita ed il furto dei dati in un architettura end-to-end.
Questo white paper spiega le funzioni di sicurezza presenti nelle telecamere della serie i-PRO Extreme riguardanti la crittografia delle comunicazioni e la protezione dei dati con l'uso di certificati digitali e chiavi di cifratura.

2. Cifratura dei Dati e Certificati Digitali

Chiavi di cifratura, firme digitali e certificati digitali sono solo alcune delle tecnologie di base della sicurezza informatica.
Questo capitolo spiega le caratteristiche principali di queste tecnologie.

2.1. Tecnologie di Cifratura dei dati

Crittografia significa riorganizzare le informazioni di "testo" dei dati digitali seguendo delle regole prestabilite per evitare che il contenuto venga compreso da terzi.
La crittografia moderna è di solito separata in algoritmi che vengono liberamente scambiati e dati, chiamati chiavi ed applicati a tali algoritmi, che vengono mantenute segrete.
I sistemi di cifratura sono classificati nei due principali tipi secondo le proprietà delle chiavi ed il loro modo di utilizzo.

- Crittografia a chiave simmetrica
- Crittografia a chiave pubblica (o asimmetrica)

La crittografia a chiave simmetrica può essere paragonata a una chiave di casa, dove la chiave per la crittografia e la chiave per la decodifica sono essere la stessa cosa.
Nel cyberspazio i dati possono essere intercettati con relativa facilità all'interno di un percorso di comunicazione, quindi condividere una chiave crittografica tra il mittente ed il destinatario diventa un grosso problema.

DES, 3DES, RC4 e AES sono esempi di crittografia che utilizzando il sistema a chiave simmetrica e di solito hanno velocità più elevate rispetto alla crittografia a chiave pubblica.

Figura 1: **Crittografia a Chiave Simmetrica**

La crittografia a chiave pubblica (o asimmetrica) utilizza un paio di chiavi diverse chiamate una chiave pubblica e una chiave privata.
I dati crittografati da una delle chiavi possono essere decrittati solo dall'altra chiave, ed è estremamente complicato risalire ad una chiave conoscendo la sua corrispondente.
Il metodo di comunicazione parte dal destinatario che genera una coppia di chiavi ed invia la chiave pubblica al mittente.
Il mittente utilizza la chiave pubblica per crittografare i dati da inviare, successivamente il destinatario decodifica le informazioni ricevute con la sua chiave privata.
I dati crittografati dalla chiave pubblica possono essere decodificati solo dalla chiave privata corrispondente, pertanto sono possibili comunicazioni sicure a meno che la chiave privata non venga fisicamente sottratta al suo proprietario.
Questo metodo non richiede la condivisione della chiave privata, quindi viene superato il problema della condivisione delle chiavi presente nel metodo di crittografia simmetrica.
L'RSA è un esempio di una cifra usando il sistema di crittografia a chiave pubblica.

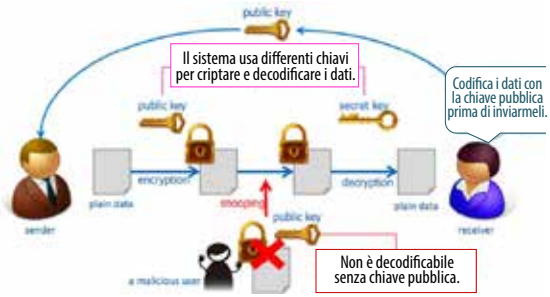


Figura 2: **Crittografia a Chiave Pubblica**

2.2. Firma Digitale

Le firme digitali sono la tecnologia per certificare che i dati sono creati dalla persona che si suppone di essere il mittente. Le specifiche del metodo di certificazione sono le seguenti:

[Alla fonte dei dati (firma digitale)]

I. Il creatore dei dati (mittente) genera chiavi pubbliche e private e invia la chiave pubblica al destinatario.
II. Il creatore calcola il valore numerico hash ("riassunto digitale" del messaggio).
III. Il valore hash viene crittografato dalla chiave privata del creatore.
Questa è quella che si definisce "firma digitale".
IV. La firma digitale viene aggiunta ai dati e i dati vengono inviati al destinatario.

[Al punto di ricezione dei dati (certificazione)]

I. Il destinatario calcola il valore hash (A) dei dati ricevuti.
II. Il destinatario estrae la firma digitale dai dati ricevuti decodificandoli usando la chiave pubblica (B) ricevuta dal creatore
III. Se A e B corrispondono, è la conferma che B è stata generata dalla chiave privata nota solo dal creatore dei dati, che sono a loro volta certificati come "creati dal creatore".

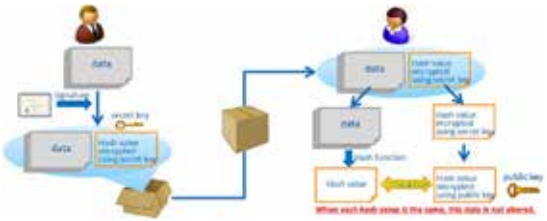


Figura 3: **Firma Digitale**

2.3. Certificati Digitali

2.3.1. Panoramica generale

Un certificato digitale utilizza la citata crittografia a chiave pubblica e le tecnologie della firma digitale ed ha i seguenti tre ruoli:

I. Memorizzare la chiave pubblica e le informazioni del proprietario della chiave privata accoppiata con quella.
II. Accreditamento da parte di terze parti che i dati sono veri.
III. Certificazione che i dati non siano stati falsificati.

I certificati soddisfano questi requisiti grazie a firme digitale di società terze che garantiscono le informazioni generata dal proprietario.

2.3.2. Tipi di certificati digitali

I certificati digitali sono classificati in due tipi principali a seconda di chi è il firmatario.

- Certificati firmati da una CA (Certification Authority)
- Certificati a firma del proprietario

La sezione seguente spiega le caratteristiche e le differenze tra le due tipologie.

2.4. Certificati con firma di una CA

2.4.1. Procedure per ricevere un certificato firmato da una CA

Un certificato con firma di una CA è un documento digitale prodotto da un'autorità di certificazione (CA= Certification Authority) riconosciuta a livello internazionale. I certificati firmati da una CA vengono generalmente generati attraverso seguente procedura:

I. Una coppia di chiavi pubbliche e private viene generata nel dispositivo.
II. Una richiesta di firma del certificato (CSR) viene generata nel dispositivo in base alla chiave pubblica e alle informazioni relative al proprietario.
III. Il proprietario del dispositivo invia la CSR alla CA tramite mezzi come la posta elettronica.
IV. La CA verifica se le informazioni della CSR ricevute sono corrette.
V. Se le informazioni sono riconosciute come corrette, viene firmata la chiave privata CA e viene generato un certificato.
VI. La CA invia il certificato al proprietario del dispositivo.
VII. Il proprietario del dispositivo installa il certificato sul dispositivo.

Durante l'installazione di certificati CA su dispositivi di sicurezza, le persone che impostano tali dispositivi devono eseguire la procedura di cui sopra per ogni dispositivo. Passaggi da III a VI richiedono alcuni minuti a poche settimane, come descritto nella sezione successiva, portando ad aumentare i costi legati al tempo durante l'installazione.

2.4.2. Tipi di certificati con firma di una CA

I certificati firmati da una CA sono classificati nei tre tipi seguenti secondo la differenza in "metodo di esame" impiegato nel passaggio IV sopra indicato.

Tipo	Metodo di verifica	Tempo richiesto per la verifica	Caratteristiche	Prezzo
Certificato a Validità Estesa (EV)	Conferma dell'esistenza dell'indirizzo web legale della società richiedente.	Alcune settimane	La barra dell'indirizzo diventa verde quando si accede via browser.	Alto
Certificato di validità dell' organizzazione	Conferma dell'esistenza della società richiedente.	Pochi giorni	Il nome della società richiedente è presente nel certificato.	Medio
Certificato di validità del Dominio	Conferma che il Dominio è stato registrato.	Pochi minuti	Basso costo e veloce da ottenere.	Basso

Le firme digitali dei certificati vengono sottoposte a screening da parte delle CA riconosciute a livello internazionale per verificare il proprietario della chiave, ma bisogna prendere in considerazione le differenze nei metodi di esame sopra riportati. Con la sola convalida del dominio, un certificato può essere rilasciato finché il richiedente ha i diritti di proprietà del dominio stesso rilevato nel certificato.
Un dominio può essere ottenuto da chiunque per un paio di decine di dollari all'anno e un CA certificato "ufficiale" può essere facilmente ottenuto anche da qualcuno con "cattive intenzioni ". Nel phishing (furto di dati) bancario online, i certificati CA ottenuti in questo modo vengono utilizzati dagli hacker per far credere all'utente di operare sul sito sicuro della propria banca quando in realtà stanno operando su un sito fasullo con un dominio simile (ma non uguale) a quello della banca, la presenza del certificato inganna molti utenti che non fanno attenzione al dominio su cui stano lavorando.

2.4.3. Affidabilità della Certification Authority

La firma digitale di un certificato prodotta da una CA è fatta utilizzando una chiave privata di proprietà della CA stessa, quindi se tale chiave privata dovesse essere hackerata tutti i certificati prodotti dalla CA, anche in passato, non saranno più attendibili. Per questo motivo, è necessario proteggere le chiavi private prodotte dalle CA. Ci sono stati casi in passato in cui le chiavi private sono state rubate a seguito di attacchi informatici e sono stati rilasciati certificati CA non autorizzati. Le autorità di certificazione ritenute altamente affidabili dedicano enormi risorse per proteggere le loro chiavi private bloccando gli attacchi informatici alle loro reti.

2.5. Certificati con firma del Produttore

Con un certificato auto-firmato, il certificato digitale viene firmato dal dispositivo stesso, non da terze parti.
I metodi ordinari di generazione sono i seguenti:

I. Una coppia di chiavi pubbliche e private viene generata nel dispositivo.
II. Una richiesta di firma del certificato (CSR) viene generata nel dispositivo in base alla chiave pubblica e alle informazioni relative al proprietario.
III. La CSR è sottoscritta dalla chiave privata sopra menzionata generata nel dispositivo.

Essere in grado di firmare da soli un certificato permette di evitare la verifica da parte di una CA, in tal modo il certificato può essere generato immediatamente e non vi sono costi da sostenere per la validazione. Ma poiché non è garantita l'identità del proprietario, non esiste alcuna funzione per accreditare le informazioni sul certificato, vale a dire uno dei tre ruoli di 2.3.1. Ciò significa che se una persona con intenti disonesti intercetta il certificato quando viene inviato all'altra parte e lo sostituisce con un altro certificato auto-firmato, non c'è alcun modo per verificarlo, quindi c'è il rischio che i dati vengano falsificati. I certificati auto-firmati devono essere utilizzati solo per le comunicazioni crittografate se l'identità del mittente dei dati è garantita da un altro metodo. Molti dispositivi di videosorveglianza hanno la funzione di generare certificati auto-firmati, ma occorre prestare attenzione ad i rischi derivanti dall'utilizzo di questo metodo che non garantisce assolutamente la sicurezza del sistema.

2.6. Conclusioni

Come dimostrato, i ruoli dei certificati digitali di memorizzare le chiavi pubbliche e le informazioni riguardanti il proprietario e di prevenire la falsificazione dei contenuti scritti nel certificato, sono uguali per tutti i tipi di certificati, ma l'affidabilità varia notevolmente tra i certificati digitali validati da una CA e quelli validati dal produttore stesso. Al fine di prevenire attacchi informatici attraverso le telecamere di rete, dovrebbe essere introdotto un certificato di convalida dedicato al settore e gestito da una CA a livello mondiale per garantirne un altissimo grado di sicurezza. Tuttavia, ciò comporterebbe costi elevati ed una lunga tempistica per l'emissione della documentazione, inoltre l'installazione di un certificato su ogni telecamera richiede del tempo e per impianti molto grandi aumenterebbero notevolmente i costo di configurazione e manutenzione.

3. Certificato pre-installato sulle telecamere Panasonic IPro Extreme

I modelli di telecamere della serie i-PRO Extreme saranno spediti con certificati preinstallati al momento della produzione. In questo modo i clienti che acquistano tali dispositivi potranno utilizzare varie funzioni di sicurezza che utilizzano questi certificati senza dover passare attraverso Il processo di richiesta e rilascio ed installazione sulla telecamera. Nelle telecamere i-PRO con funzione Secure Communication le coppie di chiavi privata e pubblica vengono generate al momento dell'uscita dalla linea di produzione e non al momento dell'istallazione.
Poiché non esiste alcun modo per ottenere la chiave privata dalla telecamera, non esiste il rischio che tale chiave venga rubata o hackerata, inoltre i certificati sono firmati da una CA riconosciuta a livello mondiale e la chiave privata utilizzata per la firma è gestita rigorosamente dalla CA stessa.
Per quanto riguarda l'esame al momento del rilascio dei certificati da parte della CA, sono firmati solo i certificati per i quali la richiesta di emissione è stata effettuata correttamente dalla fabbrica Panasonic e vengono prese misure rigorose per prevenire l'emissione di certificati non autorizzati da parte della CA stessa. Per identificare i certificati rilasciati in questo modo vengono utilizzati certificati speciali della CA (certificati digitali di proprietà del firmatario del certificato). Questi certificati CA principali vengono firmati solo per i dispositivi di videosorveglianza Panasonic, in modo da poter essere facilmente individuati quando viene verificato il certificato CA principale.

4. Livelli di sicurezza nelle telecamere Panasonic

4.1. Comunicazione SSL/TLS

Attualmente molte comunicazioni tra dispositivi di videosorveglianza (ad esempio, telecamere di rete) e i client (PC, registratori, terminali mobili) avvengono in modo non codificato. Se si possono osservare i pacchetti dati che transitano nella rete tra i server ed i client, il contenuto delle comunicazioni può essere facilmente hackerato.
Ciò include non solo i dati relativi alle immagini, ma anche gli ID / password per l'accesso ad i vari sottosistemi (telecamere, NVR, ecc). In tal modo persone con intenzioni criminose possano facilmente assumere il controllo del sistema andando a modificare i percorsi dei pacchetti dati tra le telecamere ed il sistema di gestione e registrazione oppure prendendo il controllo delle telecamere stesse oppure andando a cancellare i dati registrati nei dischi.
Tali problemi vengono risolti utilizzando i certificati digitali preinstallati nelle telecamere i-PRO e comunicando tramite protocollo SSL / TLS.

4.1.1. Protezione dei Dati

Questo paragrafo spiega il meccanismo per proteggere i dati inviati usando il protocollo SSL / TLS.
Con le comunicazioni SSL / TLS, il client riceve dal server un certificato ed un valore privato sul quale verrà basata la creazione della chiave comune, tale chiave viene poi criptata dal client con la chiave pubblica inclusa nel certificato stesso.
Il dato criptato viene quindi rispedito al server che estrae la chiave comune decriptandolo attraverso la sua chiave privata.
In seguito, i dati da trasmettere in base a questa chiave comune vengono crittografati ed inviati al client.
Per questo motivo, anche se i pacchetti vengono tracciati da qualcuno sul percorso di trasmissione, i dati non possono essere compresi da parte che non disponga della chiave privata.
Le comunicazioni SSL / TLS possono essere ottenute inserendo per esempio https: // nella barra degli indirizzi di un browser.

4.1.2. Garantire che le comunicazioni avvengano con il server corretto

Spieghiamo ora il meccanismo per garantire che il nostro interlocutore sia effettivamente quello corretto.
Il giudizio sull'affidabilità o meno del mittente è eseguita mediante la verifica della firma digitale presente nel certificato ricevuto dal server all'inizio della comunicazione SSL / TLS. Come spiegato nel punto 2.4, un certificato con firma digitale di una CA acquista maggior importanza.
Prima di tutto, con un certificato auto-firmato, la firma è creata dal proprietario del dispositivo, quindi non è possibile ottenere una conferma di identificazione e pertanto non è possibile impedire lo spooping dei dati.
Anche con i certificati firmati da una CA è necessario confermare l'identità e il metodo di valutazione utilizzato e non sempre è possibile impedire lo spooping con alcuni firmatari.
Le telecamere i-PRO utilizzano un certificato pre-installato con un metodo altamente affidabile come spiegato nel punto 3, per cui non è possibile eseguire spooping su questi prodotti.
In questo modo, la condivisione di comunicazioni SSL / TLS utilizzando certificati preinstallati con le telecamere i-PRO offre due tipi di sicurezza in quanto l'intercettazione dei dati sul percorso di comunicazione tra dispositivi e lo spooping degli stessi sono impediti.

4.2. Rilevamento delle falsificazioni

Un altro modo per utilizzare i certificati è impedire la falsificazione dei dati video e audio registrati dalle telecamere.
I dati registrati direttamente su una scheda SD o altri supporti della telecamera ed i dati esportati dai dischi sui registratori possono essere falsificati durante il download.
Nell'utilizzare i dati registrati come prova i sede legale, la necessità è di dimostrare che questi ultimi non siano stati alterati o falsificati.
Questo problema viene risolto utilizzando i certificati preinstallati nelle telecamere Panasonic i-PRO. In primo luogo, i dati registrati vengono firmati dalla chiave privata nella telecamera durante la registrazione sulla scheda di memoria SD.
Durante il processo di esportazione sul PC viene copiato anche il certificato che contiene la chiave pubblica. L'integrità del dato viene verificata dal software sul PC andando a confrontare la firma digitale contenuta nella registrazione con la chiave pubblica nel certificato. Lo stesso processo avviene per i dati esportati dai dischi di un registratore.
L'affidabilità di questo processo è garantita dal fatto che la firma digitale fine creata ed inserita nelle immagini direttamente a bordo della telecamera prima che il dato venga trasmesso in rete, in questo modo qualsiasi alterazione nei dati una volta trasmessi può essere facilmente individuata rendendo il sistema altamente affidabile.
In un sistema auto-firmato esiste il rischio di spooping nel rilevamento della falsificazione con alcuni tipi di certificati. Ad esempio, se qualcuno con intenti criminosi falsifica i dati durante il trasporto inserendo una sua firma ed aggiungendo un proprio certificato, sostituendo quello originale, la firma viene verificata con successo e si giudica che non vi sia falsificazione.
Con i certificati preinstallati nelle telecamere i-PRO Panasonic questa operazione non è possibile, in quanto che sia la firma che i certificati sono univoci e garantiti dalla CA con u livello di crittografia molto elevato.

4.3. Cifratura dei dati

Con i sistemi di telecamere di rete, esiste il rischio di perdite di informazioni private a causa di incidenti come l'intercettazione dei flussi video sulla rete e la perdita o il furto dei supporti su cui vengono registrate le immagini. Con le telecamere i-PRO Panasonic i dati vengono crittografati per proteggerli da tali minacce.

4.3.1. Protezione del flusso video

Il flusso video in H.264/H.265 viene crittografato in tempo reale e spedito via rete.
Il video viene crittografato dalla telecamera di rete che lo genera, in modo che non possa essere visualizzato anche se la trasmissione tra le periferiche collegate viene intercettata. A differenza delle comunicazioni SSL / TLS, i dati video vengono crittografati all'origine, pertanto i possono essere trasferiti da protocolli di comunicazione ordinari (RTP, UTP ecc.) senza alcuna limitazione.

4.3.2. Protezione dei dati registrati

Le telecamere i-PRO di Panasonic possono registrare le immagini su scheda SD in formato H.264/H.265, tale registrazione può essere crittografata.
Se la scheda SD in uso viene rubata o se viene persa, nessuno sarà in grado di visualizzare i video nonostante siano registrati in un formato standard MP4.*1
In un sistema dove le immagini vengo registrate da un NVR o da un server PC, i dati criptati essendo generati dalle telecamere possono essere comunque immagazzinati nei dischi anche se il sistema di registrazione non possiede un algoritmo di crittografia.
Non è necessario decriptare i dati per immagazzinarli nei dischi o per riceverli dalla rete, inoltre non potendo visualizzare i dati nel sistema di registrazione essi resteranno protetti anche nel caso in cui questo venga infettato da virus o attaccato dagli hacker.

**1: Gli utenti autorizzati possono riprodurre il video con un visualizzatore dedicato dopo essersi autenticati.*

4.3.3. Metodi Crittografici

La crittografia avviene tramite un sistema di cifratura ad alta velocità che combina uno schema di condivisione segreta usando un algoritmo ad alta velocità proprietario Panasonic con un sistema di crittografia a chiave simmetrica. Nei paragrafi successivi sono riportate le caratteristiche di tale metodo.

4.3.3.1. Metodo "Secret Sharing" a 256bit

A differenza dei semplici sistemi di cifratura semplificati per dispositivi embedded, la codifica Panasonic ha una complessità uguale o superiore a quella dei sistemi di crittografia a chiave simmetrica ordinaria. Il metodo "secret sharing" utilizzato ha un livello crittografico superiore dello standard AES-256, grazie all'utilizzo di un sistema di crittografia a chiave simmetrica con lunghezza di 256bit.

4.3.3.2. Elaborazione dei dati

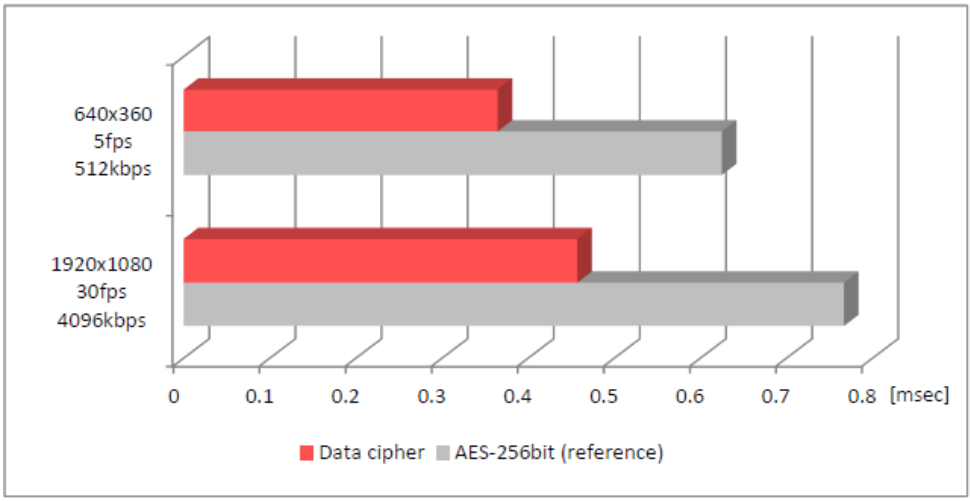


Figura 4: **Tempo di criptatura dei dati**

Il carico di elaborazione è ridotto rispetto ai sistemi di crittografia a chiave simmetrica ordinaria (AES-256 bit), per cui il ritardo dovuto alla crittografia è minimo.*2
In teoria, è possibile prevedere effetti di riduzione più elevati, più il volume dei dati aumenta a causa dell'elevato bit rate e dell'alta risoluzione, quindi questo può essere applicato anche alle telecamere 4K.
Per quanto riguarda i sistemi di archiviazione (NVR, Server PC..) non vi è alcun aumento nel carico di lavoro per registrare le immagini crittografate per cui non vi è alcuna riduzione nel numero totale di telecamere che possono gestire rispetto a una trasmissione "in chiaro".
Potranno invece esserci delle limitazioni per quei sistemi che oltre ad archiviare sono in grado di decodificare e visualizzare le immagini sia in live che in playback.
In questo caso è possibile che ci sia una riduzione sul numero totale di telecamere visualizzabili o sul numero di fps in playback.

*2: *vedi Figura 4*

4.3.3.3. Dimensione dei dati

L'aumento del volume dei dati dovuto alla crittografia è mantenuto a circa il 2%, quindi non esiste quasi nessun effetto sulla banda di comunicazione e sulla capacità di memorizzazione.

4.3.3.4. Implementazioni Software

L'elaborazione della crittografia viene implementata dal software, per cui le funzioni di crittografia sono abilitate direttamente a bordo delle telecamere i-PRO Panasonic.
Inoltre, non è necessario alcun hardware speciale per la riproduzione di dati video e i dati possono essere decifrati dal software visualizzatore. *3

* 3: *Il sistema di crittografia a chiave simmetrica usato utilizza hardware comune di cifratura per consentire un ulteriore aumento della velocità di elaborazione*

5. Conclusioni

Come già accennato, ci sono potenzialmente numerose minacce per sistemi di videosorveglianza, come l'intercettazione e la falsificazione di dati e lo spooping dei dispositivi, la resistenza a tali minacce diventerà probabilmente ancora più importante in futuro con i progressi nello IoT. Panasonic sta lavorando continuamente per migliorare la sicurezza dei propri prodotti identificando ed eliminando rapidamente queste minacce.

WHITE PAPER

PANASONIC SECURE COMMUNICATION

Sistemi di videosorveglianza

Panasonic

Panasonic

1. Introduzione

Gli attacchi informatici su dispositivi IoT sono aumentati negli ultimi anni. I sistemi di sorveglianza basati sulle telecamere analogiche e sui registratori in passato sono stati utilizzati principalmente in piccole reti chiuse come le reti interne delle aziende.
Con la migrazione di tali sistemi da analogico a digitale, l'estensione della rete sta aumentando notevolmente anche all'interno di una piccola azienda e l'accesso a Internet di tutti si sistemi, incluso la videosorveglianza, sta diventando la norma.
I sistemi di videosorveglianza sono anche riconosciuti come una parte importante dell'infrastruttura sociale mondiale con milioni di telecamere di rete installate per il controllo del traffico e dei luoghi pubblici nei centri cittadini. Questo white paper descrive le funzioni di sicurezza e le modalità per impostarle sulle telecamere ed i registratori di videosorveglianza i-PRO Panasonic.

2. Cenni descrittivi

Le misure contro le minacce alla sicurezza devono tener conto dell'ambiente ove è installato il sistema, dei beni da proteggere e delle informazioni presenti al suo interno.
Le seguenti fasi sono normalmente da prendere in considerazione quando si progetta la sicurezza informatica di sistemi di videosorveglianza su rete dati.

Fase 1: Identificare la struttura complessiva (passata, presente e futura) del sistema di videosorveglianza da proteggere.

Fase 2: Identificare informazioni, i nodi e le risorse da proteggere nel sistema.

Fase 3: Identificare le possibili minacce interne ed esterne (analisi delle minacce).

Fase 4: Identificare le migliori contromisure da applicare per contrastare le minacce.

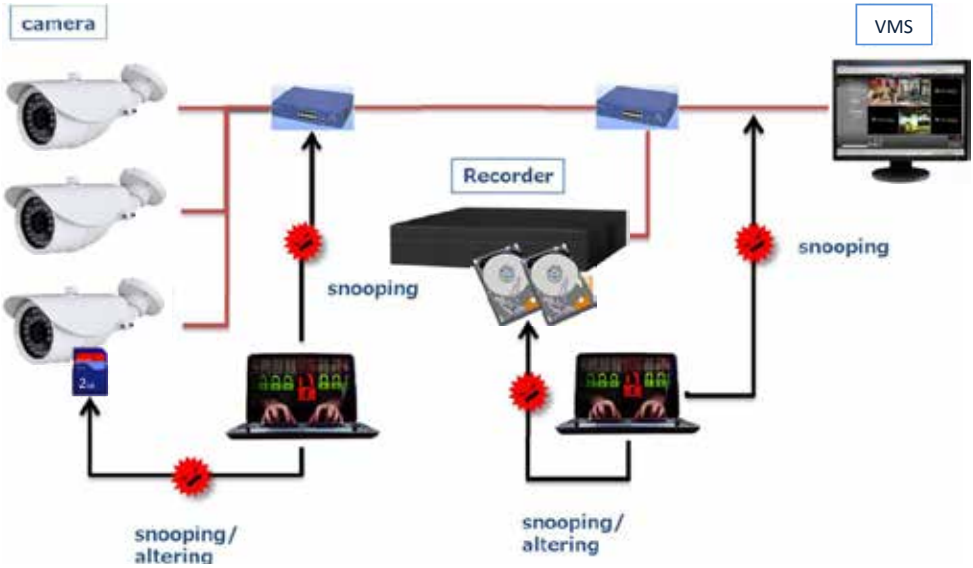
Fase 5: Selezionare le contromisure da prendere in considerazione in base al livello di minaccia, al livello di danni potenziali, ai costi, ecc.

Questo white paper descrive, nei capitoli successivi, le funzioni di sicurezza presenti nei prodotti Panasonic serie i-PRO Extreme, ma è importante far notare che l'implementazione di tutte queste funzioni può limitare alcune funzionalità dei prodotti o diminuire la facilità d'uso degli stessi.
È importante quindi fare un attenta analisi dei rischi prima di attivare tali funzioni.

3. Funzioni di Sicurezza principali delle telecamere I-Pro

3.1 Aree di competenza

Il nella figura sottostante viene mostrato un sistema che utilizza telecamere di sorveglianza senza protezioni attive.
Come viene evidenziato ci sono una serie di rischi di attacchi informatici nelle parti più deboli del sistema.
Pertanto, devono essere adottate le adeguate contromisure per prevenire e bloccare questi attacchi rendendo il sistema più sicuro.



Le minacce potenziali e le contromisure efficaci sono mostrate nella seguente tabella.

Minaccia	Contromisura
Accesso da client non autorizzati	Autenticazione con password (digest)
	Autenticazione dell'Host (indirizzo IP)
	Rimozione di servizi non necessari
	802.1X
Snooping: alterazione dei dati trasmessi via rete	Comunicazione crittografata (HTTPS)
Falsificazione dei dati registrati	Registrazione crittografata
Falsificazione dei dati registrati	Rilevamento dell'alterazione del dato

3.2. Nome Utente e Password

Il metodo più semplice e veloce per impedire l'accesso non autorizzato alle apparecchiature di videosorveglianza è impostare un nome utente ed una password di connessione a tutti i componenti del sistema.
In molti prodotti sul mercato nume utente e password di amministratore vengono preimpostati dal fabbricante e alcuni dispositivi dispongono di un account utente incorporato che non può essere modificato. In altri dispositivi è possibile accedere ad alcuni servizi senza necessità di autenticazione. Molti utenti mantengono invariate le credenziali impostate dal fabbricante, questo permette di iniziare subito ad utilizzare il dispositivo riducendo i tempi di istallazione. Le credenziali di default però possono essere ottenute da chiunque ricercandole sui siti Internet o più semplicemente scaricando e leggendo il manuale di istruzioni del dispositivo. Inoltre i software utilizzati per compiere attacchi informatici dispongono già di un vocabolario interno con tutti i nomi utente e password di default comunemente utilizzati dai fabbricanti (root, admin, 12345, 54321, ecc.).
I sistemi Panasonic di ultima generazione per impostazione predefinita non possiedono credenziali di default impostate dalla fabbrica. All'atto della prima accensione sarà compito dell'utilizzatore creare, nel setup menu o con un semplice tool software, le credenziali di amministratore dei propri dispositivi. È inoltre buona norma creare più utenti nei dispositivi con privilegi e livelli differenti, mantenendo sempre unico e segreto l'account di amministratore. Per quanto riguarda la tipologia di credenziali da utilizzare, solitamente il criterio di gestione viene deciso dal responsabile della sicurezza che ha in carico il sistema. I suggerimenti che si possono dare sono:

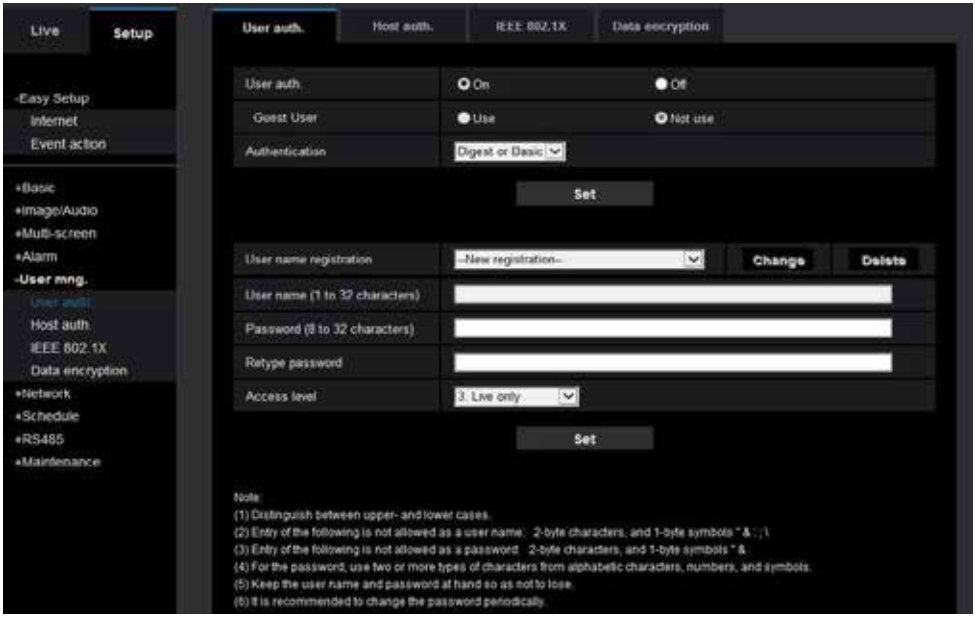
- Utilizzare due o più tipi di caratteri (lettere, numeri, simboli) per utente e password.
- Non utilizzare parole/combinazioni di senso compiuto contenute in vocabolari o elenchi.
- Modificare la password periodicamente.
- Non utilizzare combinazioni troppo brevi.

3.3. Autenticazione Digest

Anche se vengono impostati un nome utente e una password appropriati per accedere al dispositivo, la possibilità che queste informazioni vengano "catturate" via rete da parte di un hacker è sempre presente e dipende dal metodo di autenticazione e utilizzato. Per il protocollo HTTP sono definiti i seguenti due metodi di autenticazione:

- Autenticazione di base:
  Con l'autenticazione di base, il nome utente e la password vengono inviati come testo normale. Per tale motivo, non dovrebbe più essere utilizzato a meno che non sia assolutamente necessario per mantenere retro compatibilità del sistema.
- Autenticazione Digest:
  Con l'autenticazione del digest, il nome utente e la password vengono inviati in codifica MD5 basata su i valori hash delle credenziali utilizzate. Con questo metodo è difficile risalire ad i valori originali delle stringhe di testo, impedendo l'accesso non autorizzato al sistema.
  È anche vero che teoricamente chiunque può generale un valore hash di un testo per confrontarlo con quelli utilizzati nelle credenziali, quindi diventa importante l'utilizzo di combinazioni non di uso frequente (root, password: 12345) per le credenziali di accesso, come suggerito nel capitolo precedente.

Per impostare metodo e credenziali di accesso in una telecamera I-Pro Extreme seguire:
[Setup] -> [User mng.] -> [User auth.] ed impostare il metodo di [Authentication] e le credenziali.



3.4. Autenticazione dell' Host

Questo metodo di autenticazione permette di accreditare solo un PC o un gruppo di PC basandosi sull'indirizzo IP o sulla classe di rete. Tale metodo può essere utilizzato in combinazione con l'autenticazione classica basata sulla richiesta di ID e Password.

Per impostare l'accesso con controllo dell'host in una telecamera I-Pro Extreme seguire:
[Setup] -> [User mng.] -> [Host auth.] ed impostare i valore come desiderato.

Per autorizzare solo un indirizzo IP specifico, immettere un indirizzo come 192.168.0.100.
Per autorizzare l'accesso ad un intera sotto rete di indirizzi, immettere la sottorete tramite la notazione CIDR come 192.168.0.0/24.

Verificare attentamente i valori inseriti, in caso di errore non sarà più possibile accedere alla telecamera e sarà necessario eseguire un reset hardware delle stessa ad i parametri di fabbrica. Lo stesso metodo pió essere utilizzato per gli indirizzi IPv6 se tale numerazione è attiva nel menù corrispondente.

3.5. Rimozione dei servizi non necessari

Un pirata informatico può utilizzare servizi attivi (ma non utilizzati) in un dispositivo come piattaforma per lanciare attacchi. Per esempio tramite il servizio telnet è possibile accedere con semplicità ad una periferica e prenderne il controllo, una volta entrati le impostazioni del dispositivo possono essere modificate ed esso può essere utilizzato come piattaforma per attaccare altri dispositivi usando un malware.
Nelle telecamere Panasonic i-PRO, di default solo due servizi sono attivi:

- HTTP (80)
- RTSP (554)

3.6. IEEE 802.1x

IEEE 802.1x è una tecnologia che utilizza gli switch della LAN per far sì che solo dispositivi approvati possano eseguire una connessione di rete. Utilizzando questo meccanismo, è possibile impedire ad utenti non autorizzati di collegare un PC ad una porta dello switch disponibile sulla LAN, per infiltrarsi nella rete e fare snooping dei dati.

Con IEEE 802.1x, uno specifico software deve essere installato sul PC client che vuole accedere alla rete dallo switch di LAN tramite un servizio di autenticazione.
Un client che desidera accedere innanzitutto fa una richiesta di connessione allo switch di autenticazione e invia un messaggio EAP (Extensible Authentication Protocol).
Lo switch di autenticazione inoltra il messaggio EAP al server di autenticazione e il server giudica se consentire o meno la connessione.
Esistono diversi tipi di EAP, tra cui EAP-MD5, PEAP e EAP-TLS. EAP-MD5 e PEAP, sono metodi di autenticazione per ID e password e EAP-TLS utilizza certificati digitali per l'autenticazione.
Le telecamere Panasonic serie i-PRO Extreme supportano IEEE 802.1x, solo per EAP-MD5 e PEAP supportati come EAP, gli altri metodi di autenticazione verranno ampliati in futuro con aggiornamenti del firmware.

Per impostare l'autenticazione con 802.1x seguire:
[Setup] -> [User mng.] -> [IEEE 802.1x].

3.7. HTTPS

HTTPS (Hyper Transfer Protocol Secure) è un protocollo per le comunicazioni protette basato su HTTP utilizzando i protocolli SSL / TLS.
Due i due benefici principali ottenibili con HTTPS sono i seguenti:

- Prevenzione del snooping;
  Le comunicazioni vengono crittografate utilizzando HTTPS e anche se i dati vengono intercettati sulla rete non risulteranno leggibili. Utilizzando questa tecnologia, può essere impedito il snooping. Per crittografare le comunicazioni tramite HTTPS, nella telecamera/registratore deve essere presente una chiave specifica. Per questo motivo, un certificato crittografico generato dall'esterno viene scaricato in ogni telecamera singolarmente per permettere alle stesse di generare una chiave segreta specifica. Con tale metodo, c'è la possibilità che il certificato e la chiave segreta vengano "rubati" durante l'importazione. Inoltre scaricare il certificato su ogni camera e generare la relativa chiave richiede del tempo, che per impianti di medie e grandi dimensioni aumenta notevolmente i costi di istallazione.
  Panasonic è stata la prima azienda al mondo a fornire prodotti in cui sono preinstallati una chiave segreta e un certificato digitale approvati da una Certification Authority a livello internazionale. Questo lavoro viene eseguito in una fabbrica sotto stretti controlli e l'autorità di certificazione che rilascia (firma) i certificati è controllata a livello mondiale per dare il massimo livello di sicurezza possibile.

- Prevenzione dello spoofing;
  Lo Spoofing comporta l'utilizzo di un PC che, una volta inseritosi nella rete, finge di essere una telecamera/registratore a cui l'utente sta cercando di accedere ed acquisisce le credenziali del sistema o altre informazioni rilevanti. Questo, per esempio, è un metodo spesso utilizzato nella tecnica di phishing del banking online. Al fine di prevenire lo spoofing, è necessario verificare l'identità del certificato digitale inviato dal dispositivo di connessione (telecamera / registratore) durante la creazione di una comunicazione HTTPS.

  In particolare, l'emittente (firmatario) del certificato digitale deve essere affidato dal dispositivo di connessione (client). Con le telecamere di molti produttori, viene fornita una funzione per generare certificati auto-firmati come metodo crittografico per le comunicazioni HTTPS, il livello di sicurezza è però molto basso. Con i certificati preinstallati utilizzati da Panasonic, generati e firmati da una Certification Authority esterna, il livello di sicurezza è altissimo.

Per impostare l'HTTPS seguire: [Setup] -> [Network] -> Scheda [Advanced] -> [HTTPS], mettendo [Connessione] su [HTTPS] e premendo il pulsante [Set].

I certificati preinstallati sono firmati da una CA e dovrà anche essere installato e registrato nel PC client per confermare il firmatario per evitare lo spoofing.

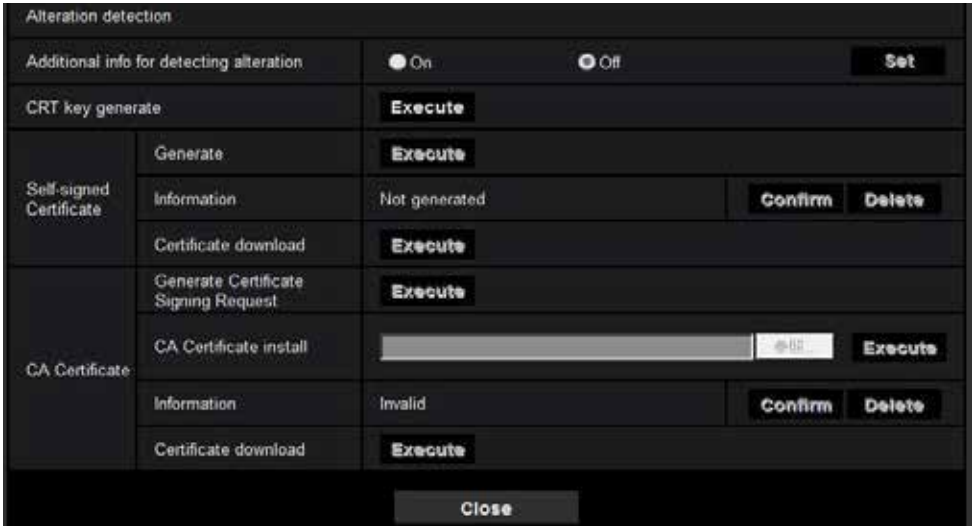
3.8. Crittografia dei dati

La crittografia dei dati, a differenza di HTTPS e VPN, comporta la crittografia solo dei dati video e audio. HTTPS e VPN crittografano il percorso di comunicazione, quindi i dati all'interno vengono trasmessi "in chiaro" e saranno visibili a chiunque riesca ad intromettersi nella rete. Con la crittografia dei dati questi sono sempre protetti e lo rimangono anche dopo essere stati immagazzinati sul supporto di archiviazione.

Quindi, anche se il disco o la scheda SD vengono rubati, i file al loro interno restano illeggibili da un urente non autorizzato. Non esiste un metodo standard di crittografia dei dati per la videosorveglianza, le telecamere della serie i-PRO Extreme gestiscono una crittografia AES-256bit proprietaria. Per impostare la crittografia dei dati:
[Setup] -> [User mng.] -> [Data encryption].

3.9. Rilevamento della falsificazione dei dati registrati

Esiste la possibilità che i dati immagazzinati nella memoria del sistema di registrazione vengano scaricati per essere visionati esternamente, inviati tramite posta elettronica o trasportati su una chiave USB.
È tecnicamente possibile modificare o sostituire tali dati sul percorso di trasporto o alla destinazione.
La funzione di rilevamento delle alterazioni (falsificazioni) verifica che ciò non sia accaduto.
In particolare, il valore hash dei dati video viene calcolato dalla telecamera, crittografato utilizzando il sistema preinstallato e aggiunto al certificato trasmesso.
Questi dati crittografati vengono chiamati "firma".
Quando si rileva la presenza di alterazioni, viene nuovamente calcolato il valore hash dei dati video esportati e confrontato con quello originale.
Se tale valore combacia può essere certificato che i dati non sono stati modificati.
La firma creata dalla chiave segreta della telecamera può essere decodificata solo con la chiave pubblica inclusa nel certificato spedito.
Come illustrato nella sezione su HTTPS, non può essere confermato oggettivamente chi ha prodotto un certificato auto-firmato, ad esempio se i dati su una scheda SD vengono firmati in questo modo non è possibile rilevare un eventuale falsificazione.
Per prevenire tali situazioni, è necessario utilizzare un certificato preinstallato sul dispositivo stesso.
Per impostare l'Ateration Detection:
[Setup] -> [Basic] -> [SD Memory card] -> [Alteration Detection]-> Additional info… su [On] e premendo [Set].



Il rilevamento dell'alterazione su SDCard gestisce solo i filmati in formato MP4 e la conferma può essere effettuata tramite un software dedicato.

3.10. Test di vulnerabilità

Il software installato sui dispositivi di rete è stato oggetto di molti attacchi informatici in passato e sono state trovate molte vulnerabilità, questa lista è stata aggregata in un database CVE (Common Vulnerabilities and Exposures) condiviso in tutto il mondo tramite Internet. Essendo pubblico questo database viene utilizzato anche dagli hacker per sviluppare nuovi virus informatici. La serie di telecamere Panasonic i-PRO Extreme è stata sottoposta a prove di verifica sulle vulnerabilità registrate presso il CVE e sono state adottate le opportune contromisure per eliminarle completamente. Con questo sforzo, la minaccia di attacchi informatici su problemi noti può essere ridotta e per certi casi eliminata. Inoltre, con il sistema i-PRO, la struttura del modulo crittografico per le comunicazioni HTTPS è proprietaria ad alto livello di sicurezza, gli algoritmi di crittografia con livello debole, come SSL3.0 e RC4, non vengono utilizzati. C'è anche la possibilità che in futuro si possano trovare vulnerabilità non note.
Panasonic controlla costantemente le nuove vulnerabilità e le azioni vengono prese immediatamente quando si giudica che siano necessarie contromisure. Per proteggersi dagli ultimi attacchi informatici, è consigliabile controllare periodicamente il sito Web di Panasonic per verificare la presenza di nuovi firmware.

3.11. Firmware

Esiste anche il rischio di presenza di virus nel firmware stesso. C'è la possibilità di essere attirati, tramite email, da siti di spoofing che suggeriscono di aggiornare il prodotto con un firmware particolare che per esempio ne migliora le prestazioni, nella realtà molti di questi firmware contengono virus o malware che sfruttano il dispositivo di rete per lanciare attacchi informatici all'insaputa del proprietario. Il firmware deve essere sempre scaricato dalla pagina ufficiale del fornitore.

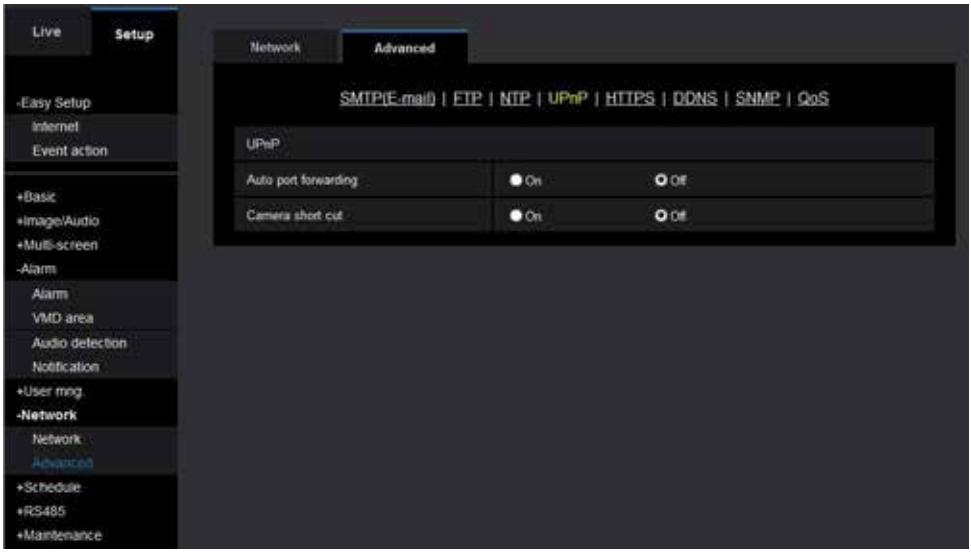
Se il firmware inviato non è crittografato, esiste il rischio che venga analizzato e ricodificato inserendo software maligno. Ci sono stati casi anche recenti in cui dispositivi di videosorveglianza sono stati vittima di attacchi DDoS che gli hanno resi inoperabili, tali attacchi hanno sfruttato una vulnerabilità del firmware nella gestione del protocollo NTP. Con telecamere e registratori i-PRO, tutti i firmware sono criptati in modo sicuro e non possono essere analizzati e modificati.

4. Consigli per in corretto utilizzo delle camera di rete

4.1. UPnP

Configurazione delle impostazioni di inoltro automatico delle porte UPnP.

Le impostazioni di inoltro automatico delle porte eseguite tra router e le telecamere tramite tabelle NAT possono rendere le reti ed i dispositivi presenti accessibili da Internet. Per bloccare l'accesso dall'esterno non controllato, l'impostazione di inoltro automatico delle porte UPnP deve essere disattivata dal menu di Setup della telecamera.

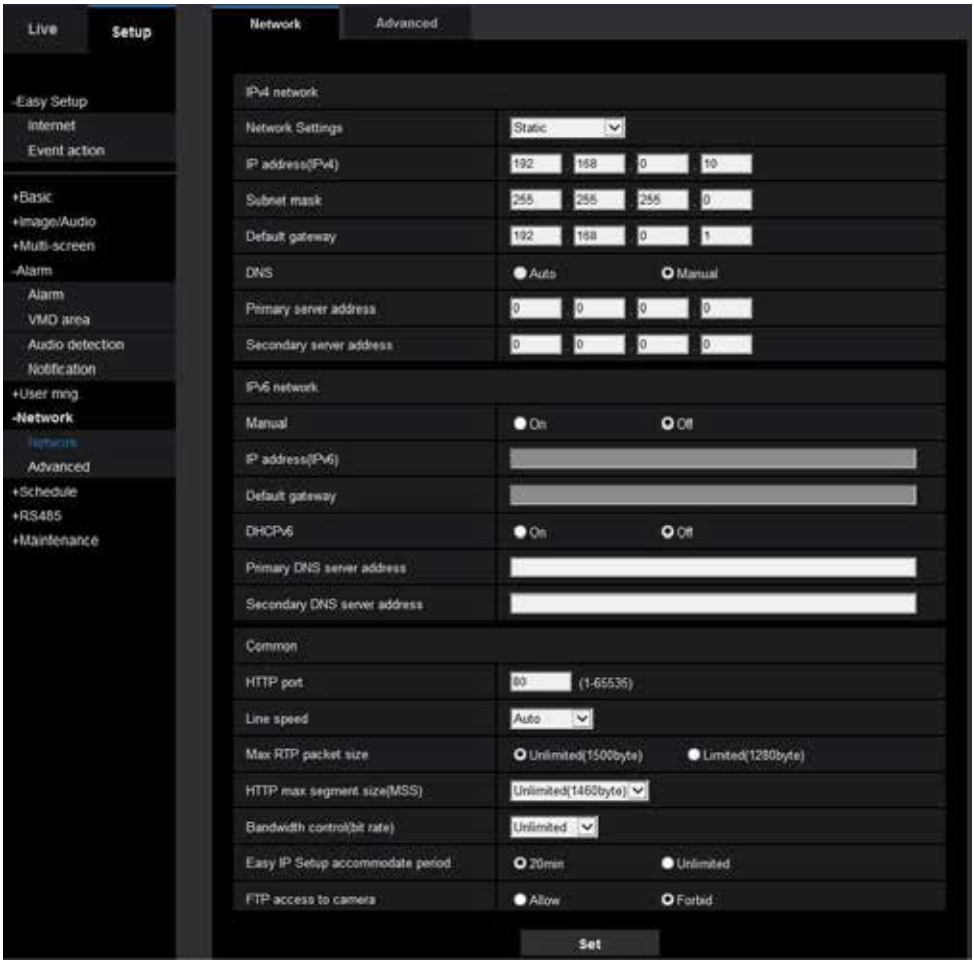


4.2. Server FTP

Attivando la funzione del server FTP, le telecamere di rete possono essere accessibili da client FTP tramite protocollo FTP. Le comunicazioni FTP non sono crittografate, pertanto è consigliabile disattivare la funzionalità del server FTP quando non la si utilizza, per impedire lo snooping su ID, password ed i dati trasferiti.

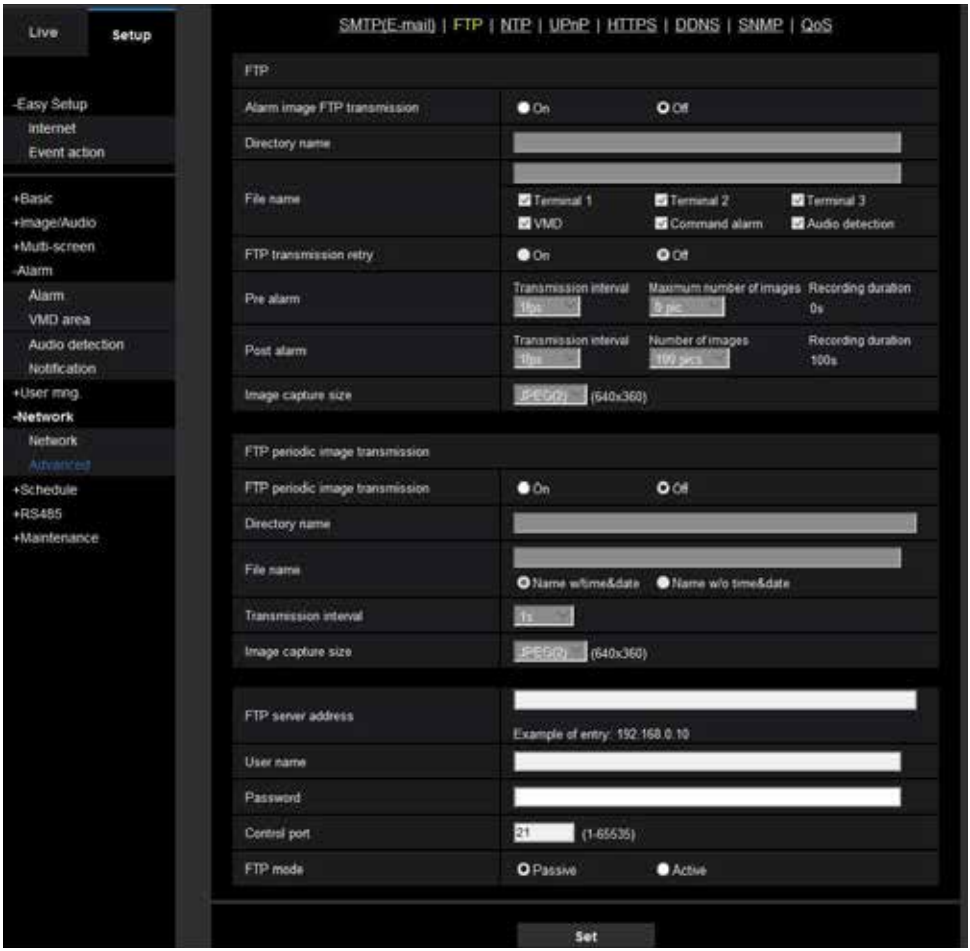
La funzione del server FTP può essere disattivata dalla schermata dedicata nelle impostazioni di rete della telecamera.

La modalità di accesso deve essere impostata su [Forbit].



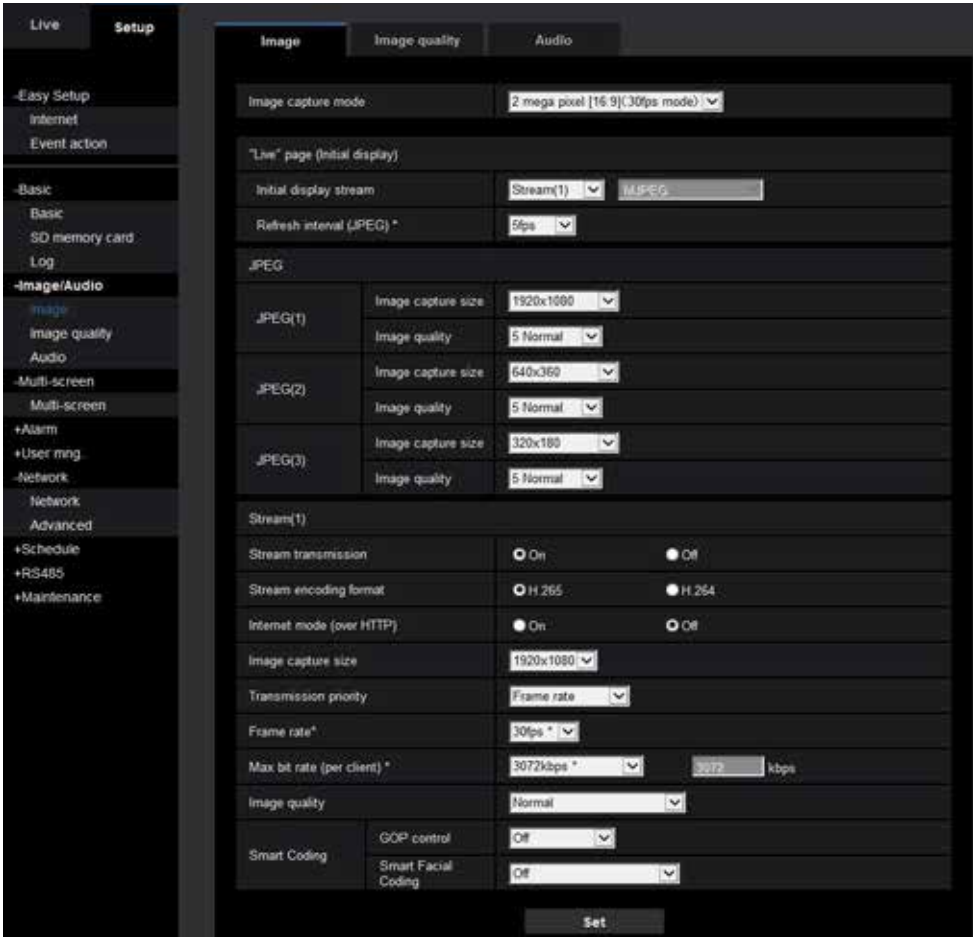
4.3. Client FTP

Attivando la funzione client FTP, le immagini possono essere trasferite ad un server FTP esterno. Le comunicazioni FTP non sono crittografate, per cui è consigliabile disattivare la funzionalità client FTP quando si utilizza in un ambiente non protetto per evitare accessi indesiderati al sistema o furto dei dati e delle immagini.



4.4. RTSP

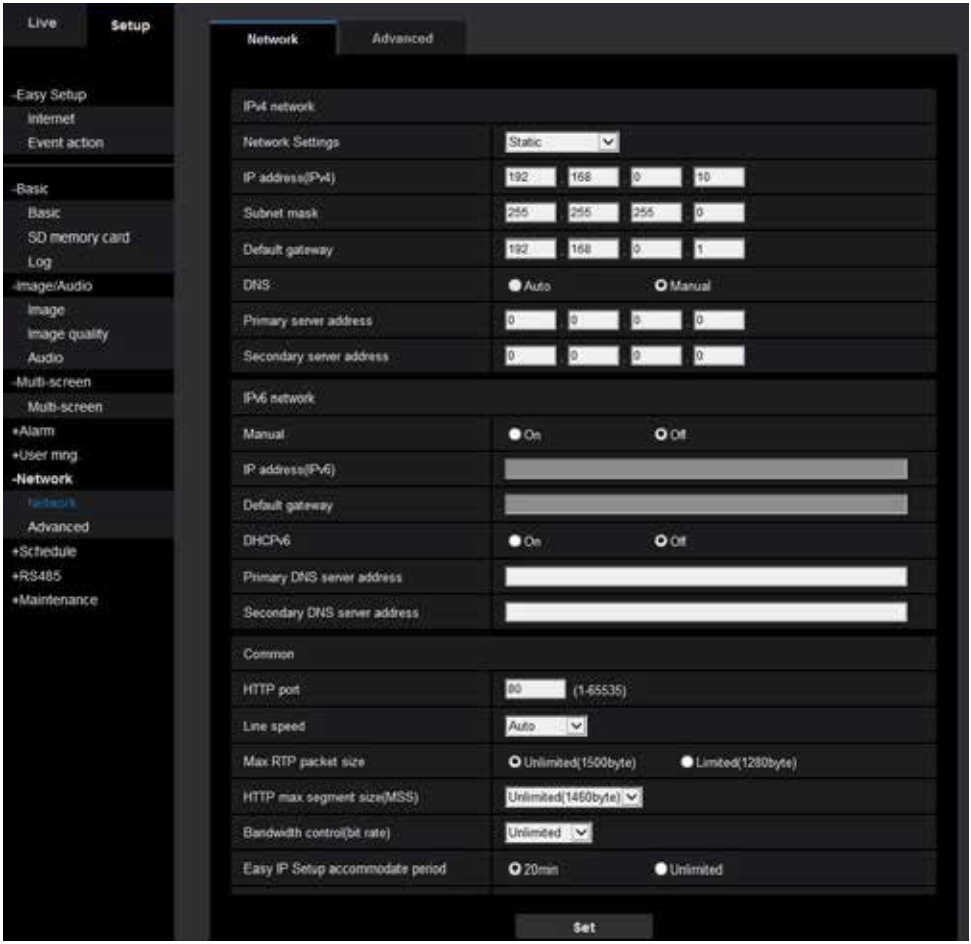
L'RTSP viene utilizzato per lo streaming video ma non gestisce le comunicazioni crittografate tramite protocollo SSL. C'è pertanto un rischio di accesso non autorizzato e furto dei dati trasmessi.
Molto spesso l'RTSP viene utilizzato per semplificare l'invio degli stream video via HTTP usando un'unica porta di comunicazione.
In questo caso è possibile ottenere lo stesso risultato in modalità criptata HTTPS attivando la funzione Internet Mode nelle impostazioni Image/Audio dello stream interessato.



4.5. Easy IP

Attivando il software Easy IP Setup di Panasonic da un PC connesso alla stessa rete delle telecamere è possibile ricercare i dispositivi Panasonic tramite indirizzo MAC per poterne configurare a piacimento l'indirizzo IP.
In questo modo utenti non autorizzati potrebbero ottenere accesso alle telecamere, aumentando il rischio di attacchi DDoS.

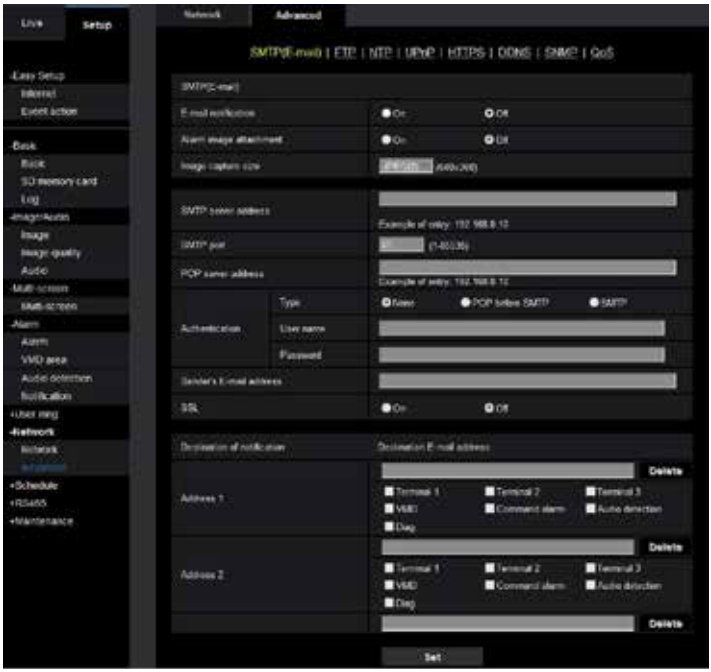
Per fare in modo che le telecamere non possano essere ricercate dallo strumento Easy IP Setup si consiglia di limitare il periodo di visibilità da Unlimited a 20 minuti.
In tal modo la telecamera sarà accessibile a tutti solo nei primi 20 minuti dopo l'accensione permettendo all'installatore di eseguire le configurazioni necessarie per poi chiudere automaticamente il servizio.
Per rete ad elevata sicurezza il servizio può essere spento.



4.6. SMTP

Quando si invia la posta elettronica tramite SMTP, l'ID e la password non vengono crittografati durante la connessione al server, quindi c'è il rischio di essere hackerati.

Pertanto, quando si invia la posta tramite SMTP, è consigliabile inviare un'e-mail a un server che supporti SMTP tramite SSL. L'SMTP over SSL può essere attivato impostando su ON la voce SSL nella schermata delle impostazioni SMTP (e-mail).



4.7. SNMP

Con l'SNMP v1 / v2, i pacchetti stessi non vengono crittografati, per cui possono essere intercettati o modificati.

Quando si utilizza una telecamera in un ambiente in cui esistono rischi di snooping da parte di terze parti, è consigliabile utilizzare SNMP v3 con funzioni di crittografia e alter detection.

L'SNMP v3 può essere utilizzato impostandolo nella schermata dedicata al SNMP.

5. Conclusioni

Ci sono potenzialmente molte minacce per i sistemi di videosorveglianza, come lo snooping, l'alterazione dei dati e lo spoofing dei dispositivi.

Quindi la resistenza a queste minacce diventerà probabilmente ancora più importante in futuro con i progressi nello IoT.

Panasonic sta lavorando continuamente per migliorare la sicurezza dei propri prodotti per raggiungere e mantenere sempre il livello più alto possibile, identificando e superando rapidamente queste minacce.